TECHNISCHE UNIVERSITÄT MÜNCHEN

Lehrstuhl für Nachrichtentechnik

Key Agreement with Physical Unclonable Functions and Biometric Identifiers

Onur Günlü

Vollständiger Abdruck der von der Fakultät für Elektrotechnik und Informationstechnik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor–Ingenieurs

genehmigten Dissertation.

Vorsitzender:		Prof. Dr.-Ing. Georg Sigl
Prüfer der Dissertation:	1.	Prof. Dr. sc. techn. Gerhard Kramer
	2.	Prof. Dr. ir. Frans M.J. Willems, Eindhoven University of Technology, The Netherlands
	3.	Prof. Dr. Amin Aminzadeh Gohari, Sharif University of Technology, Iran

Die Dissertation wurde am 24.08.2018 bei der Technischen Universität München eingereicht und durch die Fakultät für Elektrotechnik und Informationstechnik am 09.11.2018 angenommen.

Preface

Contents

Abstract

This thesis addresses security and privacy problems for digital devices and biometrics, where a secret key is generated for authentication, identification, or secure computations. A physical unclonable function (PUF) is a promising solution for local security in digital devices. A low-complexity transform-coding algorithm is developed to make the information-theoretic analysis tractable and motivate a noisy (hidden) PUF source model.

The optimal trade-offs between the secret-key, privacy-leakage, and storage rates for multiple measurements of hidden PUFs are characterized. The first optimal and low-complexity code constructions are proposed. Polar codes are designed to achieve the best known rate tuples. The gains from cost-constrained controllable PUF measurements are illustrated to motivate extensions.

Zusammenfassung

Diese Dissertation befasst sich mit Problemen der Sicherheit und des Datenschutzes für digitale Geräte und Biometrie, wobei ein geheimer Schlüssel für Authentifizierung, Identifizierung oder sichere Berechnungen erzeugt wird. Eine physical unclonable function (PUF) ist eine Lösung für die lokale Sicherheit in digitalen Geräten. Unser Algorithmus zur Transformationskodierung, der eine geringe Komplexität aufweist, macht die informationstheoretische Analyse möglich und führt zu einem verrauschten (versteckten) PUF-Quellmodell.

Der optimale Kompromiss zwischen den Geheimschlüssel-, Privacy-Leakage- und Speicherraten für Mehrfachmessungen von versteckten PUFs wird ermittelt. Erste optimale und wenig komplexe Code-Konstruktionen werden vorgeschlagen. Polar-Codes werden entworfen, um darzustellen, dass sie die besten bekannten Rate Tupeln erreichen. Die Vorteile aus kostenbeschränkten, kontrollierbaren PUF-Messungen werden veranschaulicht, um Erweiterungen zu motivieren.

1

Introduction

After World War I, the U.S. Army and Navy made fundamental advances in cryptography in secret. One exception was Claude E. Shannon's paper "The Communication Theory of Secrecy Systems" [1]. Until 1967, the literature on security was not extensive, but a book [2] with a historical review of cryptography changed this trend [3]. Since then, the amount of sensitive data that needs to be protected against attackers has increased significantly. Continuous improvements in security are needed and every improvement creates new possibilities for attacks [4].

A promising local solution to security and privacy problems is a physical unclonable function (PUF) [5, 6]. PUFs generate "fingerprints" for physical devices by using their intrinsic and unclonable properties. These functions resemble biometric features of human beings. In this thesis, we bridge the gap between the practical secrecy systems that use PUFs and the information-theoretic security limits by

1. Statistically modeling real PUF (and biometric) outputs to solve security problems with valid assumptions on the output model;

2. Proposing methods that transform PUF symbols so that the transform-domain outputs are information-theoretically tractable and result in smaller hardware area than benchmark designs in the literature;

3. Finding the information-theoretic limits for realistic PUF output models;

4. Providing optimal, practical, and future-proof code constructions to achieve these limits;

5. Designing best-in-class polar codes for realistic PUF output models by using the optimal code constructions.

In short, we start from real PUF outputs to obtain mathematically-tractable models of their behaviour and we propose optimal code constructions for these models. Using the real PUF outputs, we then illustrate that our models are realistic and, most importantly, our methods perform well in practice. Since our designs are based on information theory, any further improvements in this topic are likely to follow our steps.

The thesis is structured as follows.

- ▷ **Chapter 2** gives a general definition of PUFs. Practical motivations to use PUFs and challenges faced when extracting a uniform sequence from PUF outputs are listed.
- ▷ **Chapter 3** reviews and improves a transform-coding approach [5, 7, 8] to overcome the noise and correlation in the PUF outputs so that a secret key can be generated without leaking information about the key. A key agreement (helper data generation) method is described and error-correcting codes are designed for this method according to the modeling parameters obtained from the transform-coding algorithm. The results of this chapter were published in [9–11], where programming for the hardware implementation was done by Tasnad Kernetzky of TUM.
- ▷ In **Chapter 4**, information-theoretic rate regions are derived for a generalization of a classic two-terminal source model key agreement problem. The additions to the model are that the encoder observes a hidden, or noisy, version of the identifier, and that the encoder and decoder can perform multiple measurements. The gains from multiple measurements of a hidden source are illustrated for binary sources. The results of this chapter were published in [12, 13].
- ▷ In **Chapter 5**, two linear code constructions, previously proposed for the Wyner-Ziv (WZ) problem, are developed for two terminals to agree on a secret key hidden from an eavesdropper. The first (random) code construction achieves all points of the key-leakage-storage regions of the generated- and chosen-secret models. We design nested polar codes as the second code construction for vector quantization during enrollment and for error correction during reconstruction to illustrate that they improve on existing methods. The results of this chapter are submitted for publication in [14], where the polar code design tools of Onurcan İşcan of Huawei (previously at TUM) were used.
- ▷ **Chapter 6** considers the problem of secret-key based authentication under a privacy constraint on the source sequence. The identifier measurements during authentication are assumed to be controllable via a cost-constrained “action” sequence. Single-letter characterizations of the optimal trade-off among the secret-key rate, storage rate, privacy-leakage rate, and action cost are given for the two problems when noisy measurements of a hidden source are enrolled to generate or embed secret keys. The results of this chapter were published in [15].
- ▷ In **Chapter 7**, two further contributions are summarized. The first contribution is about characterizing the rate regions for multiple enrollments of PUF measurements, and the second considers multiple rounds of public communication for the source model key agreement problem to find sufficient and necessary conditions to obtain

a positive secret-key capacity. The results of this chapter were partially published in [16], where the proof of the general two-enrollment case is from Frans Willems and Lieneke Kusters of TU Eindhoven. The results were also partially published in [17], where the majority of the work was done by Amin Gohari of Sharif University of Technology. The extension of [17] will be submitted for publication in [18].

▷ **Chapter 8** summarizes the main contributions of this thesis. We list ongoing and future works that extend these contributions.

Parts of the material presented in this thesis appear in our papers [7–19]. Direct extensions of this thesis, defended in November 2018 and published in [20] in February 2019, include the works in [21–34].

Notation

Upper case letters represent random variables and lower case letters their realizations. A letter with superscript denotes a string of variables, e.g., $X^n = X_1 \dots X_i \dots X_n$, and a subscript denotes the position of a variable in the string. $X^{n\setminus i}$ represents the vector $(X_1, X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$. A random variable X has probability mass P_X or probability density f_X. Calligraphic letters such as $\mathcal{X}$ denote sets, and set sizes are denoted as $|\mathcal{X}|$. A set, e.g., $\mathcal{X}^n$, with superscript n denotes an n-fold Cartesian product set. $\mathcal{T}_\epsilon^n(P_X)$ denotes the set of length-n letter-typical sequences with respect to the probability mass P_X and positive number ϵ [35, Ch. 3], [36], i.e., we have

$$\mathcal{T}_\epsilon^n(P_X) = \left\{ x^n : \left| \frac{N(a|x^n)}{n} - P_X(a) \right| \leq \epsilon P_X(a), \ \ \forall a \in \mathcal{X} \right\} \tag{1.1}$$

where $N(a|x^n)$ is the number of occurrences of symbol a in x^n. $H(X)$ represents the entropy of a random variable X and $H(X|Y)$ is the conditional entropy of X given a random variable Y. $I(X;Y)$ is the mutual information of X and Y. $H_b(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function and $H_b^{-1}(\cdot)$ denotes its inverse with range $[0, 0.5]$. The $*$-operator is defined as $p * x = p(1-x) + (1-p)x$. Bold letters such as $\mathbf{H}$ represent matrices. $\mathsf{Enc}(\cdot)$ is an encoder mapping and $\mathsf{Dec}(\cdot)$ is a decoder mapping. $X - Y - Z$ indicates a Markov chain. The operator $\oplus$ represents the element-wise modulo-2 summation. The operation $\bar{x} = 1 - x$ gives the one's complement of the bit x. A binary symmetric channel (BSC) with crossover probability p is denoted by BSC(p). $X^n \sim \text{Bern}^n(\alpha)$ denotes that X^n is an independent and identically distributed (i.i.d.) binary sequence of random variables with $\Pr[X_i = 1] = \alpha$ for $i = 1, 2, \dots, n$. $\text{Unif}\,[1 : |\mathcal{X}|]$ represents a uniform distribution over the integers from 1 to $|\mathcal{X}|$. A linear error-correction code $\mathcal{C}$ with parameters (n, k, d) has block length n, dimension k, and minimum distance d.

2

Literature Review

We give a brief review of the literature on PUFs and discuss the PUF types considered in this thesis.

A PUF is a function that is embodied in a physical device and that is unclonable. In the literature, there are alternative expansions of the term PUF such as “physically unclonable function” [37], which suggests that it is a function that is only physically unclonable. Such PUFs may provide a weaker security guarantee since they allow their functions to be digitally cloned. For any practical application of a PUF, we need the property of unclonability both physically and digitally. In this thesis, we therefore consider a function as a PUF only if it is a physical function, which is embodied in a physical device, that is unclonable digitally and physically.

This chapter is organized as follows. We give a generic definition of PUFs in Section 2.1. We summarize possible application areas and basics of PUFs in Section 2.2. Four of the most important PUF types are given in Section 2.3.

2.1. PUF Definition

Physical identifiers such as PUFs are heuristically defined to be complex challenge response mappings that depend on the random variations in a physical object. Secret sequences are derived from this complex mapping, which can be used as a secret key. One important feature of PUFs is that the secret sequence generated is not required to be stored and it can be regenerated on demand. This property makes PUFs cheaper (no requirement for a memory for secret storage) and safer (the secret sequence is regenerated on demand only) alternatives to other secret generation and storage techniques such as storing the secret in a non-volatile memory (NVM) [6].

There are an immense number of PUF types, which makes it practically impossible to give a single definition of PUFs that includes all types. We provide the following definition of PUFs that includes all PUF types of interest in this thesis.

Definition 2.1 ([6])**.** A PUF is a challenge response mapping embodied by a physical device such that it is

- ▷ easy and fast for the physical device to evaluate the PUF response;
- ▷ hard for an attacker, who cannot access the PUF, to determine the PUF response to a randomly chosen challenge, even if he has access to a set of challenge-response pairs.

The terms used in Definition 2.1, i.e., easy, fast, and hard, are relative terms that should be quantified for each PUF application separately. There are physical functions, called physical one-way functions (POWFs), in the literature that are closely related to PUFs. Such functions are obtained by applying the cryptographic concept of "one-way functions", i.e., functions that are (on average) difficult to invert but easy to compute [38], to physical systems. As a first example of POWFs, the speckle pattern obtained from coherent waves propagating through a disordered medium is a one-way function of both the angle of the beam used to generate the optical waves and the physical randomness in the medium [39].

Similar to POWFs, biometric identifiers such as the iris, retina, and fingerprints are closely related to PUFs, and a PUF can be seen as a "fingerprint" of a physical device. Most of the assumptions for biometric identifiers are satisfied also by PUFs, so we can apply almost all of the results in the literature for biometric identifiers to PUFs. However, it is common practice to assume that PUFs can resist invasive (physical) attacks, which are considered to be the most powerful attacks used to obtain information about a secret in a system, unlike biometric identifiers that are constantly available for attacks. The reason for this assumption is that invasive attacks permanently destroy the fragile PUF outputs [6]. This assumption will be the basis for the PUF system models used throughout the thesis. We therefore assume that the attacker (eavesdropper) does not observe a sequence that is correlated with the PUF outputs, since physical attacks applied to obtain such a sequence permanently change the PUF outputs.

2.2. Applications of PUFs

A PUF can be seen as a source of random sequences that are hidden from an attacker who does not have access to the PUF outputs. Therefore, any security application that takes a secret sequence as input can theoretically use PUFs. We list some scenarios where PUFs fit well practically.

- ▷ Consider a fifth-generation (5G) mobile device that uses a set of static random access memory (SRAM) outputs, which are available in mobile devices, as a PUF to extract secret keys so that the messages to be sent are encrypted with these secret keys before sending the data over the wireless channel. In this way, the receiver (e.g., a base station) that previously obtained the secret keys can decrypt the data, while an eavesdropper who only overhears the data broadcast over the wireless channel cannot learn the message sent.

- ▷ Security of information in wireless networks with an eavesdropper is a physical-layer security problem. Consider Wyner's wiretap channel model introduced in [40], where a transmitter sends a message through a broadcast channel so that a legitimate receiver can reliably reconstruct the message, while the message should be kept secret from an eavesdropper. A randomized encoder helps the transmitter in keeping the message secret by confusing the eavesdropper. Therefore, one can use PUFs at the transmitter as the source of private (local) randomness for the random encoder when a message should be sent securely.

- ▷ The controller area network (CAN) bus standard used in modern vehicles is illustrated in [41] to be susceptible to denial-of-service attacks, which shows that safety-critical inputs of the internal vehicle network such as throttle and brakes can be controlled by an attacker. One countermeasure against such attacks is to encrypt the transmitted CAN frames by using block ciphers. Secret keys generated from PUF outputs can be used as inputs to the block cipher to provide security against such safety-critical attacks.

- ▷ Cloud storage requires security to protect users' sensitive data. However, securing the cloud is expensive and the users do not necessarily trust the cloud service providers. A PUF in a universal serial bus (USB) token, i.e., Saturnus®, has been trademarked by the company Intrinsic-ID to encrypt user data before uploading data to the cloud.

- ▷ Internet-of-things (IoT) devices may carry sensitive data, e.g., wearable or e-health devices, and use a PUF to store secret keys so that only a mobile device with access to the secret keys can control the IoT devices. One common example of such applications is when PUFs are used to authenticate wireless body sensor network devices [42].

- ▷ Consider system developers who want to mutually authenticate a field-programmable gate array (FPGA) chip and the intellectual property (IP) components in the chip, and IP developers who want to protect the IP. In [43], a protocol is described that achieves these goals with a small hardware area that uses one symmetric cipher and one PUF.

- ▷ Security of an item with a radio frequency identification (RFID) tag can be provided by using lightweight PUF designs as a source of secret key that protects the RFID tag from being copied [44].

Other applications of PUFs include providing non-repudiation (i.e., undeniable transmission or reception of data), proof of execution on a specific processor, and remote integrated circuit (IC) enabling. Note that every application of PUFs has different assumptions about the PUF properties, computational complexity of the cryptographic system that takes PUF outputs as input, and the specific system models. Therefore, there are different constraints and system parameters for each application. In the thesis, we focus mainly on the application where a secret key is generated from a PUF for user, or device, authentication.

2.3. Main PUF Types

We review four main PUF types, i.e., silicon, arbiter, SRAM, and ring oscillator (RO) PUFs. We consider mainly the last two PUFs for algorithm and code designs due to their common use in practice. Another emerging PUF type is the quantum readout PUF that uses a random quantum state as the challenge and a unitary transform of the quantum state as the response, which does not require trusted devices for PUF measurement [45]. Furthermore, locally enhanced defectivity PUFs are recently proposed in [46] as a completely stable PUF.

2.3.1. Silicon and Arbiter PUFs

Common complementary metal–oxide–semiconductor (CMOS) manufacturing processes are used to build silicon PUFs, where the response of the PUF depends on the circuit delays which vary across ICs [47]. Due to high sensitivity of the circuit delays to environmental changes (e.g., ambient temperature and power supply voltage), another PUF scheme, called arbiter PUF, is proposed in [48], for which an arbiter (i.e., a simple transparent data latch) is added to the silicon PUFs so that the comparison result of two different path delays generates a single bit. For instance, the difference of the path delays is mapped to the bit 0 if the upper path is faster, and the bit 1 otherwise. The difference can be small, which causes meta-stable outputs. Since the output of the mapper is generally preset to 0, the incoming signals must satisfy the setup time (t_{setup}) of the latch to switch the output to 1. This design results in a bias in the arbiter PUF outputs. Symmetrically implementable latches (e.g., set-reset latches) should be used to overcome this problem, which is difficult due to, e.g., the peculiarities of FPGA routing that does not allow the user to enforce symmetry in the hardware implementation. We discuss below that PUFs without symmetry requirements, e.g., RO PUFs, provide better results for FPGA chip authentication.

2.3.2. SRAM PUFs

There are multiple memory-based PUFs such as SRAM PUFs, Flip-flop PUFs, and Butterfly PUFs [37]. Their common feature is that they posses a small number of challenge-response pairs with respect to their sizes. As the most promising memory-based PUF type that is already used in industry, we consider SRAM PUFs. SRAM PUFs use the uncontrollable settling state of bi-stable circuits [49]. In the standard SRAM design, there are four transistors used to form the logic of two cross-coupled inverters, as depicted in Figure 2.1, and two other transistors to access the inverters.

The logically stable states of an SRAM cell are $(\overline{Q}, Q) = (1, 0)$ and $(0, 1)$. During the power-up, the state is undefined if the manufacturer did not fix it. The undefined power-up state of an SRAM cell converges to one of the stable states due to physical mismatch of the inverters, which is fixed when the cell is manufactured [50]. Furthermore, there is random electrical noise in the cell that affects the cell at every power-up. Since the physical

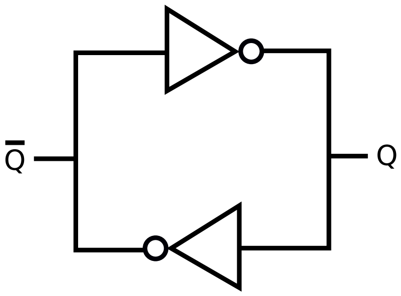

Figure 2.1.: SRAM logic circuit.

mismatch of the cross-coupled inverters is a manufacturing variation, the power-up state of an SRAM cell is considered as a PUF response with one challenge, which is the address of the SRAM cell [50].

2.3.3. Ring Oscillator PUFs

The logic circuit of an odd number of inverters serially connected with a feedback of the output of the last inverter into the first inverter is a RO, as depicted in Figure 2.2. The first logic gate in Figure 2.2 is chosen to be a NAND gate, which gives the same logic output as an inverter gate when the ENABLE signal is 1 (ON), to enable/disable the RO circuit. The manufacturing-dependent and uncontrollable component in an RO is the total propagation delay of an input signal to flow through the RO, which determines the oscillation frequency $\hat{x}$ of an RO. This component is used as the source of randomness for RO PUFs. A self-sustained oscillation is possible when the ring provides a 2π phase shift and has unit voltage gain at the oscillation frequency $\hat{x}$.

Consider an RO with m inverters. Each inverter should provide a phase shift of $\frac{\pi}{m}$ with an additional phase shift of π due to the feedback. Therefore, the signal should flow through the RO twice to provide the necessary phase shift [51]. Consider a propagation delay of τ_d for each inverter, so the oscillation frequency of a RO is

$$\hat{x} = \frac{1}{2m\tau_d}. \tag{2.1}$$

The propagation delay τ_d is affected by nonlinearities and parasitics in the circuit. Furthermore, there are deterministic noise sources such as the cross-talk between adjacent signal traces and additional random noise sources such as thermal noise and flicker noise [51]. Such effects should be eliminated to have a reliable RO output. Rather than improving the standard RO designs, which would impose the condition that all manufacturers should change their RO designs, the first proposal to fix the reliability problem was to make hard bit decisions by comparing RO pairs [52], as illustrated in Figure 2.3.

In Figure 2.3, the multiplexers are challenged by a bit sequence of length at most $\lceil \log_2 N \rceil$ so that an RO pair is selected among N of them. The counters output the number of rising edges from each RO for a fixed time duration. A logic bit decision is made by

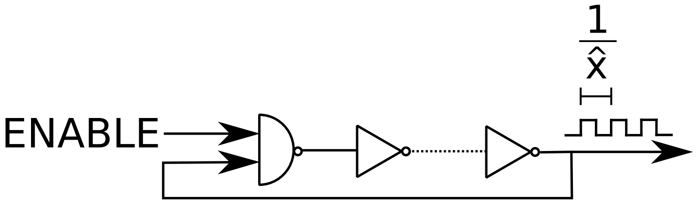

Figure 2.2.: RO logic circuit.

comparing the counter values, which are related to the oscillation frequencies. For instance, when the upper RO has a greater counter value, then a bit 0 is generated; otherwise, a bit 1. Given that ROs are identically laid out in the hardware, the differences in the oscillation frequencies are determined mainly by uncontrollable manufacturing variations. Furthermore, it is not necessary to have a symmetric layout when hard-macro hardware designs are used for different ROs [52], unlike arbiter PUFs.

The key extraction method illustrated in Figure 2.3 gives an output of $\binom{N}{2}$ bits, which are correlated due to overlapping RO comparisons. This causes a security threat and makes the RO PUF vulnerable to various attacks. Thus, non-overlapping pairs of ROs are used in [52] to extract each bit. However, there are systematic variations in the neighboring ROs due to the surrounding logic, which should also be eliminated to extract keys with full entropy [53].

Ambient temperature and supply voltage variations are the most important effects that reduce the reliability of RO PUF outputs. A scheme called 1-out-of-k masking is proposed in [52] as a countermeasure to these effects. This scheme compares the RO pairs that have the maximum oscillation frequency differences for a range of voltages and temperatures. The bits extracted by such a comparison are more reliable than the bits extracted by using previous methods [52]. The main disadvantages of this scheme are that it is inefficient due to unused RO pairs, and only a single bit is extracted from the (semi-) continuous RO outputs. We review and extend in the next chapter an RO PUF method that improves on these methods by using transforms.

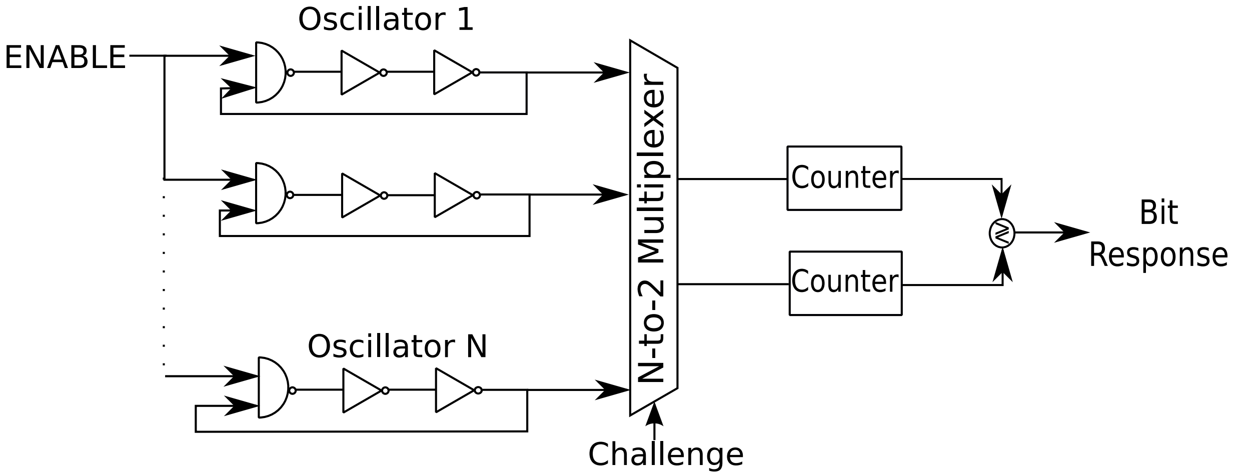

Figure 2.3.: First RO PUF method [52].

3

Transform Coding for Key Agreement with Correlated PUFs

In this chapter, we consider biased (nonuniform) and correlated (dependent) PUF outputs that are also noisy. We review and improve a transform-coding algorithm [5] to extract an almost i.i.d. uniform bit sequence from each PUF so that a helper-data generation algorithm can correct the bit errors in the bit sequence generated from the noisy PUF outputs. We give a reference hardware design to illustrate that the hardware area occupied by the proposed algorithm is small. Furthermore, from Section 3.6 on and in the next chapters, we assume that such a transform-coding algorithm is available to obtain i.i.d. bit sequences from PUFs so that we can use standard information-theoretic tools. The results of this chapter were published in [9–11], where programming for the hardware implementation was done by Tasnad Kernetzky.

3.1. Motivation

Invasive attacks to physical identifiers permanently change the identifier output so that an attacker cannot learn the secret key by using an invasive attack [39]. This property eliminates the need for continuous hardware protection. Physical identifiers such as PUFs are considered to be random sources with high entropy. Security applications that use a secret key stored in a NVM can alternatively use a PUF for the same purpose. Thus, we can use PUFs for low-complexity key storage in, e.g., IoT applications like securing a surgical robot against hacking.

There are multiple *key-generation*, or generated-secret (GS), and *key-binding*, or chosen-secret (CS), methods to reconstruct secret keys from noisy PUF outputs, where the key is generated from the PUF outputs or bound to them, respectively. A code-offset fuzzy extractor (COFE) [54] is an example of key-generation methods and the fuzzy commitment scheme (FCS) [55] is a key-binding method. Since a key should be stored in a secure database for both models, it is more practical to allow a trusted entity to choose the secret key bound to a PUF output. Thus, in this chapter, we aim at further improving reliability, privacy, secrecy, and hardware cost performance of a transform-coding algorithm that is applied to PUF outputs in combination with the FCS.

Correlation in PUF outputs leaks information about the secret key, called *secrecy leakage*, and about the PUF output, called *privacy leakage* [13,56,57]. Moreover, noise reduces the reliability of PUF outputs and error-correction codes are needed to satisfy the reliability constraints. The transform-coding approach proposed in [5,7] in combination with a set of scalar quantizers has made its way into secret-key binding with continuous-output identifiers. This approach allows to reduce the output correlation and to adjust the effective noise at the PUF output. For instance, the discrete cosine transform (DCT) is the building block in [7] to generate a uniformly distributed bit sequence from RO outputs under varying environmental conditions. Efficient post-processing steps are applied to obtain more reliable PUF outputs rather than changing the hardware architecture, so standard components can be used. This transform-coding approach improves on the existing approaches in terms of the reliability under varying environmental conditions and maximum key length [7,8]. We apply this algorithm to PUF outputs with further significant improvements by designing the transformation and error-correction steps jointly.

Information-theoretic limits for the FCS are given in [58]. We use these information-theoretic limits to evaluate error-correction codes proposed for the transform-coding algorithm. Similar analyses were conducted for biometric identifiers in [59], but their assumptions such as i.i.d. identifier outputs and maximum block-error probability constraint $P_B = 10^{-2}$ are not realistic. We therefore consider highly correlated RO outputs with the constraint $P_B \leq 10^{-9}$, which are realistic for security applications that use PUFs [60], as listed in Chapter 2.

3.1.1. Summary of Contributions and Organization

We improve the DCT-based algorithm of [7] by using different transforms and reliability metrics. We also propose error-correction codes that achieve better (secret-key, privacy-leakage) rate tuples than previous code designs. A summary of the main contributions is as follows.

- ▷ We compare a set of transforms to improve the performance of the transform coding algorithm in terms of the maximum secret-key length, decorrelation efficiency, uniqueness and security of the extracted bit sequence, and computational complexity.

- ▷ Two quantization methods with different reliability metrics are proposed to address multiple design objectives for PUFs. One method aims at maximizing the length of the bit sequence extracted from a fixed number of ROs, whereas the second method provides reliability guarantees for each output in the transform domain by fixing the decoding capability of a decoder used for error correction.

- ▷ We give a reference hardware design for the transform with the smallest computational complexity, among the set of transforms considered, in combination with the second quantization method to illustrate that our algorithm occupies a small hardware area. Our results are shown to be better than the hardware area results of previous RO PUF designs.
- ▷ Error-correction codes that satisfy the block-error probability constraints for practical PUF systems are proposed for both quantization methods to illustrate complete key-binding systems. The proposed codes operate at better rate tuples than previously proposed codes for the FCS. Our quantizer designs also allow us to significantly reduce the gap to the optimal (secret-key, privacy-leakage) rate point achieved by the FCS.

This chapter is organized as follows. In Section 3.2, we define the FCS that uses PUF outputs as the randomness source. The transform-coding algorithm proposed to extract a reliable bit sequence from RO PUFs is explained in Section 3.3. We propose two different quantization methods with different reliability metrics in Section 3.4. In Section 3.5, we illustrate the small hardware area of the proposed algorithm with a reference hardware design and show the gains in terms of reliability, security, and maximum secret-key length as compared to the existing methods. Error-correction codes are proposed, and their secrecy and privacy performance are given in Section 3.6.

3.2. System Model and the Fuzzy Commitment Scheme

Consider an RO as a source that generates a real-valued symbol $\hat{x}$. Systematic variations in RO outputs in a two-dimensional array are less than the systematic variations in one-dimensional ROs [61]. We thus consider a two-dimensional RO array of size $l = r \times c$ and represent the array as a vector random variable $\widehat{X}^l$. Suppose there is a single *PUF circuit*, i.e., a single two-dimensional RO array, in each device with the same circuit design, and it emits an output $\widehat{X}^l$ according to a probability density $f_{\widehat{X}^l}$. Each RO output is disturbed by mutually-independent additive Gaussian noise and the vector noise is denoted as $\widehat{Z}^l$. Define the noisy RO outputs as $\widehat{Y}^l = \widehat{X}^l + \widehat{Z}^l$. Observe that $\widehat{X}^l$ and $\widehat{Y}^l$ are correlated. A secret key can thus be agreed by using these outputs of the same RO array [56, 57, 62, 63].

One needs to extract random sequences with i.i.d. symbols from $\widehat{X}^l$ and $\widehat{Y}^l$ to employ available information-theoretic results for secret-key binding with identifiers. We propose an algorithm as the first quantizer that extracts nearly i.i.d. binary and uniformly distributed random vectors X^n and Y^n from $\widehat{X}^l$ and $\widehat{Y}^l$, respectively. For such X^n and Y^n, we can define a binary error vector as $E^n = X^n \oplus Y^n$. The random sequence E^n corresponds to a sequence of i.i.d. Bernoulli random variables with parameter p, i.e., $E^n \sim \text{Bern}^n(p)$. The channel $P_{Y|X}$ is thus a BSC(p), which is not required for the second quantizer design.

The FCS reconstructs a secret key by using correlated random variables without leaking any information about the secret key [55]. The FCS is depicted in Figure 3.1, where an

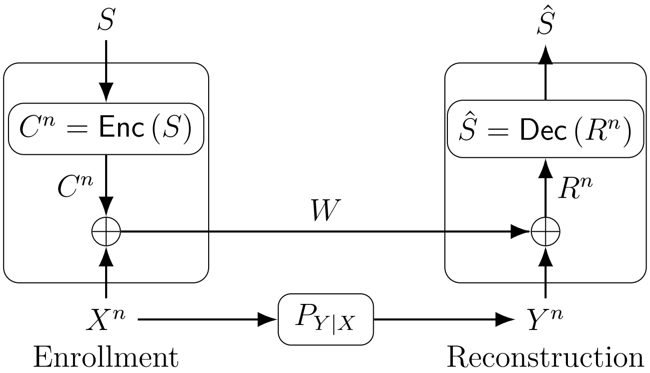

Figure 3.1.: The fuzzy commitment scheme (FCS).

encoder $\mathsf{Enc}(\cdot)$ embeds a secret key, uniformly distributed according to $\text{Unif}\,[1:|\mathcal{S}|]$, into a binary codeword C^n that is added modulo-2 to the binary PUF-output sequence X^n during enrollment. The resulting sequence is the public helper data W, which are sent through an authenticated and noiseless channel. The modulo-2 sum of the helper data W and Y^n gives the result

$$R^n = W \oplus Y^n = C^n \oplus E^n \tag{3.1}$$

which is later mapped to an estimate $\hat{S}$ of the secret key by the decoder $\mathsf{Dec}(\cdot)$ during reconstruction.

Definition 3.1. A secret-key vs. privacy-leakage rate pair (R_s, R_ℓ) is achievable by the FCS with perfect secrecy, i.e., zero secrecy leakage, if, given any $\epsilon > 0$, there is some $n \geq 1$, and an encoder and decoder for which $R_s = \dfrac{\log|\mathcal{S}|}{n}$ and

$$\Pr[S \neq \hat{S}] \leq \epsilon \qquad \text{(reliability)} \tag{3.2}$$

$$I(S;W) = 0 \qquad \text{(perfect secrecy)} \tag{3.3}$$

$$\frac{1}{n} I(X^n;W) \leq R_\ell + \epsilon \qquad \text{(privacy).} \tag{3.4}$$

Theorem 3.1 ([58])**.** The achievable secret-key vs. privacy-leakage rate region for the FCS with a channel $P_{Y|X}$ that is a BSC(p), uniformly distributed X and Y, and zero secrecy leakage is

$$\mathcal{R} = \{\,(R_s, R_\ell) : 0 \leq R_s \leq 1 - H_b(p), \quad R_\ell \geq 1 - R_s\}. \tag{3.5}$$

The region $\mathcal{R}$ suggests that any (secret-key, privacy-leakage) rate pair that sums to 1 bit/source-bit is achievable with the constraint that the secret-key rate is at most the channel capacity of the BSC. Furthermore, smaller secret-key rates and greater privacy-leakage rates than these rates are also achievable.

The FCS is a particular realization of the CS model. The region $\mathcal{R}'$ of all achievable (secret-key, privacy-leakage) rate pairs for the CS model with a negligible secrecy-leakage rate, where a generic encoder is used to confidentially transmit an embedded secret key to a decoder that observes Y^n and the helper data W, is given in [56] as

$$\mathcal{R}' = \bigcup_{P_{U|X}} \left\{ (R_s, R_\ell)\colon \quad 0 \leq R_s \leq I(U;Y), \quad R_\ell \geq I(U;X) - I(U;Y) \right\} \tag{3.6}$$

where $U - X - Y$ forms a Markov chain and the alphabet $\mathcal{U}$ of the auxiliary random variable U can be limited to have the size $|\mathcal{U}| \leq |\mathcal{X}| + 1$. The FCS is optimal, i.e., it achieves a boundary point of $\mathcal{R}'$, for a BSC $P_{Y|X}$ with crossover probability p only at the point $(R_s^*, R_\ell^*) = (1 - H_b(p), H_b(p))$ [58]. This point corresponds to the highest achievable secret-key rate; see Figure 3.7 below. Note that the region $\mathcal{R}'$ gives an outer bound for the perfect-secrecy case (see [56] for discussions).

3.3. Transform Coding Steps

The aim of transform coding is to reduce the correlations between RO outputs by using a linear transformation. We propose a transform-coding algorithm that extends the work in [5, 7]. Optimizations of the quantization and error-correction parameters to maximize the security and reliability performance, and a simple method to decrease storage are its main steps. The output of these post-processing steps is a bit sequence X^n (or its noisy version Y^n) used in the FCS. We consider the same post-processing steps for the enrollment and reconstruction. The difference is that during enrollment the design parameters are chosen as a function of the source statistics by the device manufacturer. It thus suffices to discuss only the enrollment steps. Figure 3.2 shows the post-processing steps that include transformation, histogram equalization, quantization, bit assignment, and bit-sequence concatenation.

RO outputs $\widehat{X}^l$ in an array are correlated due to, e.g., the surrounding logic [64]. A transform $T_{r\times c}(\cdot)$ of size $r \times c$ is applied to an array of RO outputs to reduce correlations. Decorrelation performance of a transform depends on the source statistics. We model each real-valued output T in the transform domain, called *transform coefficient*, obtained from an RO-output dataset in [65] by using the corrected Akaike information criterion (AICc) [66] and the Bayesian information criterion (BIC) [67]. These criteria suggest that a Gaussian distribution can be fitted to each transform coefficient T for the DCT, discrete Walsh-Hadamard transform (DWHT), discrete Haar transform (DHT), and Karhunen-Loève transform (KLT), which are common transforms considered in the literature for image processing, digital watermarking, etc. [68]. We use maximum-likelihood estimation [69] to derive unbiased estimates for the parameters of Gaussian distributions.

The histogram equalization step in Figure 3.2 converts the probability density of the i-th coefficient T_i into a standard normal distribution such that $\widehat{T}_i = \frac{T_i - \mu_i}{\sigma_i}$, where μ_i is the mean and σ_i is the standard deviation of the i-th transform coefficient for all $i = 1, 2, \ldots, l$.

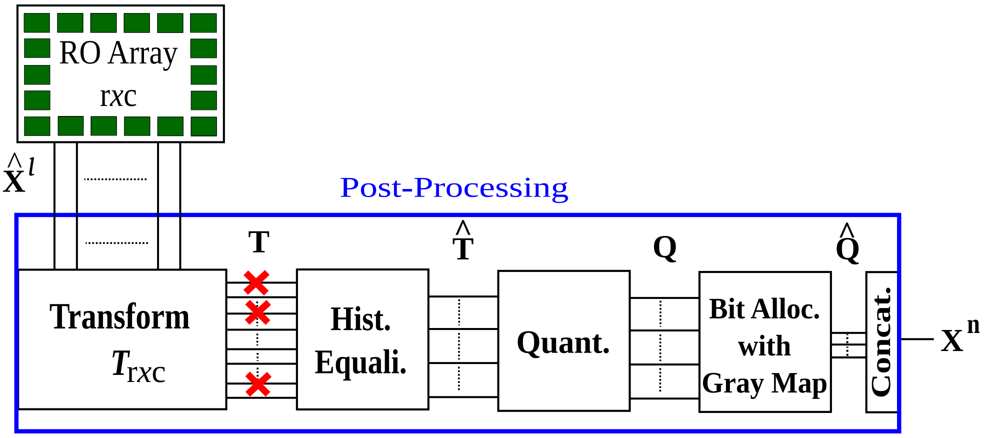

Figure 3.2.: Transform-coding steps [7].

Quantization steps for all transform coefficients are thus the same. Without histogram equalization, we need a different quantizer for each transform coefficient. Therefore, the histogram equalization step reduces the storage for the quantization steps. Transformed and equalized coefficients $\widehat{T}_i$ are independent if the transform $T_{r\times c}(\cdot)$ decorrelates the RO outputs perfectly and the transform coefficients T_i are jointly Gaussian. One can thus use a scalar quantizer for all coefficients without a performance loss. We propose scalar quantizer and bit extraction methods that satisfy the security and reliability requirements of the FCS with the independence assumption, in combination with a correlation-thresholding approach discussed below.

3.4. Quantizer and Code Designs

The aim of the post-processing steps in Figure 3.2 is to extract a uniformly-random bit sequence X^n. We use a quantizer $Q(\cdot)$ with quantization-interval values $k = 1, 2, \cdots, 2^{K_i}$, where K_i is the number of bits we extract from the i-th coefficient $\widehat{T}_i$ for $i=1,2,\ldots,l$. We have

$$Q(\hat{t}_i) = k \quad \text{if} \quad b_{k-1} < \hat{t}_i \leq b_k \tag{3.7}$$

and we choose $b_k = \Phi^{-1}\left(\frac{k}{2^{K_i}}\right)$, where $\Phi^{-1}(\cdot)$ is the quantile function of the standard normal distribution. The quantizer output k is assigned to a bit sequence of length K_i. The chosen permutation of assigned bit sequences does not affect the security performance. However, the most likely error event when we quantize $\widehat{T}_i$ is a jump to a neighboring quantization step due to zero-mean noise. We thus apply a Gray mapping when we assign bit sequences of length K_i to the integers $k = 1, 2, \ldots, 2^{K_i}$ so that neighboring bit sequences change only in one bit position.

We next propose two different reliability metrics for joint quantizer and code designs.

The first metric results in BSC measurements of each extracted bit with approximately the same crossover probability. This method extracts a different number of bits from each transform coefficient. The code design is then done for a fixed crossover probability of the BSCs. The second method fixes the maximum number of erroneous transform coefficients and considers an error-correction code that can correct all error patterns with up to a fixed number of errors.

3.4.1. Quantizer Design with Fixed Measurement Channels

Observe that with the quantizer in (3.7) and a Gray mapping, one can model the channel between a bit extracted from the enrollment outputs $\widehat{X}^l$ and the corresponding bit extracted from the reconstruction outputs $\widehat{Y}^l$ as a BSC with a fixed average crossover probability p_b. Our algorithm thus fixes an average crossover probability p_b such that the error-correction step in the FCS can satisfy the maximum block-error probability of 10^{-9}. The algorithm enforces that each output $\hat{t}_i$ results in an average bit error probability as close as possible to, but not greater than, p_b by adapting the number of bits $K_i(p_b)$ extracted from the i-th coefficient $\widehat{T}_i$ for all $i = 1, 2, \ldots, l$. We use the *average fractional Hamming distance* $D(K)$ between the quantization intervals assigned to the original and noisy coefficients as a metric to determine $K_i(p_b)$. Define

$$D_i(K)=\frac{1}{K}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\left(\sum_{k=1}^{2^K}\Pr[Q(\hat{t}+\hat{n}) = k]\mathrm{HD}_k(\hat{t})\right)\cdot f_{\widehat{T}_i}(\hat{t})f_{\widehat{N}_i}(\hat{n})\mathrm{d}\hat{t}\mathrm{d}\hat{n} \tag{3.8}$$

where $\mathrm{HD}_k(\hat{t})$ is the Hamming distance between the bit sequences assigned to the k-th quantization interval and to the interval $Q(\hat{t})$, and $\widehat{N}_i$ represents the Gaussian noise in the i-th coefficient after histogram equalization. We then determine $K_i(p_b)$ as the greatest number of bits K such that $D_i(K)\leq p_b$.

The first coefficient, i.e., DC coefficient, $\widehat{T}_1$ is not used since its value is a scaled version of the mean of the RO outputs in the array, which is generally known by an eavesdropper. Ambient-temperature and supply-voltage variations have a highly-linear effect on the RO outputs, so the DC coefficient is the most affected coefficient, which is another reason not to use the DC coefficient [8]. Therefore, the total number $n(p_b)$ of extracted bits from all transform coefficients for a fixed p_b is

$$n(p_b) = \sum_{i=2}^{l} K_i(p_b). \tag{3.9}$$

We calculate the maximum secret-key length $S_{\max}$ by using (3.5) for a BSC(p_b) with the maximum secret-key rate $R_s^*=1-H_b(p_b)$ as

$$S_{\max} = (1 - H_b(p_b)) \cdot n(p_b) \tag{3.10}$$

which is used to compare different transforms and to decide whether one can use an RO

PUF with fixed number of ROs and p_b for secret-key binding. For instance, for the Advanced Encryption Standard (AES), the minimum secret-key length is 128 bits. However, the rate region $\mathcal{R}$ in (3.5) is valid for large n. One thus needs to consider the rate loss due to a finite block length for a system design. One can alternatively combine multiple RO arrays in a device to approach the maximum secret-key rate.

3.4.2. Quantizer Design with Fixed Number of Errors

We now propose a *conservative* approach, based on the assumption that either all bits extracted from a transform coefficient are correct or they all flip, to provide reliability guarantees. The correctness probability P_c of a transform coefficient is defined to be the probability that all bits associated with this coefficient are correct. We use this metric to determine the number of bits extracted from each coefficient such that there is an encoder and a bounded minimum distance decoder (BMDD) that satisfy the block-error probability constraint $P_B \leq 10^{-9}$. This approach results in reliability guarantees for the random-output RO arrays.

For a K-bit quantizer and the quantization boundaries b_k as in (3.7) for an equalized (i.e., standard) Gaussian transform coefficient $\hat{T}$, we obtain the correctness probability

$$P_c(K)=\sum_{k=0}^{2^K-1}\int_{b_k}^{b_{k+1}}\left[Q\Big(\frac{b_k-\hat{t}}{\sigma_{\hat{n}}}\Big)-Q\Big(\frac{b_{k+1}-\hat{t}}{\sigma_{\hat{n}}}\Big)\right]f_{\widehat{T}}(\hat{t})d\hat{t} \tag{3.11}$$

where $\sigma_{\hat{n}}^2$ is the noise variance and $f_{\widehat{T}}$ is the probability density of the standard Gaussian distribution.

Suppose our channel decoder can correct all errors in up to $C_{\max}$ transform coefficients. Suppose further that coefficient errors occur independently and that the correctness probability $P_{c,i}(K)$ of the i-th coefficient $\widehat{T}_i$ for $i=1,2,\ldots,l$ is at least $\overline{P}_c(C_{\max})$. A sufficient condition for satisfying the block-error probability constraint $P_B \leq 10^{-9}$ is that $\overline{P}_c(C_{\max})$ satisfies the inequality

$$\sum_{c=C_{\max}+1}^{l}\binom{l}{c}(1-\overline{P}_c(C_{\max}))^c\overline{P}_c(C_{\max})^{l-c}\leq 10^{-9}. \tag{3.12}$$

We thus determine the number K_i of bits extracted from the i-th transform coefficient as the maximum value K such that $P_{c,i}(K) \geq \bar{P}_c(C_{\max})$. Similar to Section 3.4.1, we choose $K_1=0$ so that the total number $n(C_{\max})$ of extracted bits is

$$n(C_{\max})=\sum_{i=2}^{l}K_i. \tag{3.13}$$

In the worst case, the coefficients in error are the coefficients from which the greatest number of bits are extracted. We sort the numbers K_i of bits extracted from all coefficients in descending order such that $K'_i \geq K'_{i+1}$ for all $i=1,2,\dots,l-1$. The channel decoder thus must be able to correct up to

$$e(C_{\max}) = \sum_{i=1}^{C_{\max}} K'_i \tag{3.14}$$

bit errors, which can be satisfied by using a block code with minimum distance $d_{\min} \geq 2e(C_{\max})+1$.

Suppose a key bound to physical identifiers in a device is used in the AES with a uniformly-distributed secret key with a length of 128 bits. The block code used in the FCS should thus have a code length of at most $n(C_{\max})$ bits, code dimension of at least 128 bits, and minimum distance of $d_{\min} \geq 2e(C_{\max}) + 1$ for a fixed $C_{\max}$. The code rate should be as high as possible to operate close to the optimal (secret-key, privacy-leakage) rate point of the FCS. This optimization problem is hard to solve. We illustrate by an exhaustive search over a set of $C_{\max}$ values and over a selection of algebraic codes that there is a channel code that satisfies these constraints with a reliability guarantee for each extracted bit. Restricting our search to codes that admit low-complexity encoders and decoders is desired for IoT applications, for which complexity is the bottleneck.

Note that the listed conditions are conservative. For a given transform coefficient, the correctness probability can be significantly greater than the correctness threshold $\overline{P}_c(C_{\max})$. Secondly, due to Gray mapping, it is more likely that less than K_i bits are in error when the i-th coefficient is erroneous. Thirdly, it is also unlikely that the bit errors always occur in the transform coefficients from which the greatest number of bits is extracted. Therefore, even if a channel code cannot correct all error patterns with up to $e(C_{\max})$ errors, it can still be the case that the block-error probability constraint is satisfied. We illustrate such a case in the next section.

3.5. Performance Evaluations

Suppose the RO output $\widehat{X}^l$ is a vector random variable with the autocovariance matrix $\mathbf{C}_{\widehat{\mathbf{X}}\widehat{\mathbf{X}}}$. Consider RO arrays of sizes 8×8 and 16×16. Autocovariance matrix of such RO outputs and noise are estimated from the dataset in [65]. We compare the DCT, DWHT, DHT, and KLT in terms of their decorrelation efficiency, maximum secret-key length, complexity, uniqueness, and security.

3.5.1. Decorrelation Performance

One should eliminate correlations between the RO outputs and make them independent to extract uniform bit sequences by treating each transform coefficient separately. We use the *decorrelation efficiency* η_c [70] as a decorrelation performance metric. Consider the

Table 3.1.: The average RO output decorrelation-efficiency results.

	DCT	DWHT	DHT
η_c for 8×8	0.9978	0.9977	0.9978
η_c for 16×16	0.9987	0.9988	0.9986

autocovariance matrix $\mathbf{C_{TT}}$ of the transform coefficients, so η_c of a transform is

$$\eta_c = 1 - \frac{\sum\limits_{a=0}^{l-1}\sum\limits_{b=0}^{l-1} |\mathbf{C_{TT}}(a,b)|\mathbb{1}\{a \neq b\}}{\sum\limits_{a=0}^{l-1}\sum\limits_{b=0}^{l-1} |\mathbf{C_{\widehat{X}\widehat{X}}}(a,b)|\mathbb{1}\{a \neq b\}} \tag{3.15}$$

where the indicator function $\mathbb{1}\{a \neq b\}$ takes on the value 1 if $a \neq b$ and 0 otherwise. The decorrelation efficiency of the KLT is 1, which is optimal [70]. We list the average decorrelation efficiency results of other transforms in Table 3.1. All transforms have similar and good decorrelation efficiency performance for the RO outputs in the dataset in [65]. The DCT and DHT have the highest efficiency for 8×8 RO arrays, whereas for 16×16 RO arrays, the best transform is the DWHT. Table 3.1 indicates that increasing the array size improves η_c.

3.5.2. Maximum Secret-key Length

The maximum number of bits extracted with the method given in Section 3.4.2 depends on the fixed number of transform coefficients that are in error. Moreover, the method uses a conservative metric. However, for the method given in Section 3.4.1, we can optimize the number of bits extracted from each coefficient to maximize the secret-key length. We therefore consider only the method in Section 3.4.1 for maximum key-length comparisons.

The secret key S should satisfy the length constraints of the cryptographic primitives that use it. Consider, e.g., again the AES with a 128-bit secret key. We compare different transforms by calculating the maximum secret-key lengths $S_{\max}$, defined in (3.10), for various crossover probabilities p_b that can be obtained by applying the post-processing steps in Figure 3.2. For RO array dimensions 8×8, we show $S_{\max}$ results of the considered transforms in Figure 3.3. For $p_b \leq 0.05$, R_s^* is high but $n(p_b)$ is small, so $S_{\max}$ is mainly determined by $n(p_b)$, as depicted in Figure 3.3. For $p_b \geq 0.07$, $n(p_b)$ is high but R_s^* mainly determines $S_{\max}$, which is small.

The DHT, DWHT, and DCT have similar $S_{\max}$ results and the KLT has worse performance than the others, which is mainly determined by the signal-to-noise ratio (SNR) in the transform domain. This illustrates that a transform's η_c performance for the estimated RO output distribution, and its $S_{\max}$ performance for the estimated RO output and noise distributions can be different. We determine a crossover probability range $\mathcal{P} = [0.05, 0.07]$ such that the secret-key lengths of all transforms are close to their maximum and greater

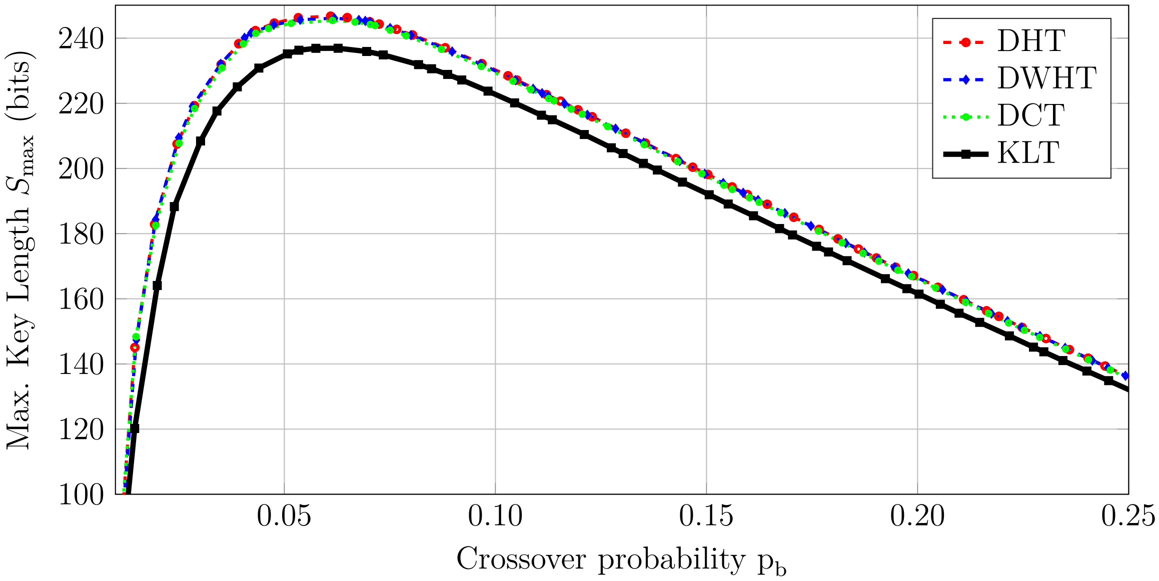

Figure 3.3.: The maximum key lengths $S_{\max}$ for 8×8 RO arrays.

than 128 bits. For a BSC with crossover probability $p \in \mathcal{P}$, we design error-correction codes such that $P_B \leq 10^{-9}$ is satisfied. The crossover probability range considered in [60] is $[0.12, 0.14]$, while 0.14 is the only value considered in [71] for the same P_B constraint. Considering a set of crossover values rather than a single value provides more flexibility in designing error-correction codes. Our crossover probability range also allows us to use higher-rate codes than the codes for the range $[0.12, 0.14]$ since the maximum key rate R_s^* of the FCS increases with decreasing p_b. The proposed transform-coding algorithm with the first quantizer method is thus beneficial for code design due to smaller crossover probability p_b.

The maximum number of extracted bits, which corresponds to n in (3.9), for an 8×8 RO array is 16 bits for the *1-out-of-8 masking* scheme [52], 32 bits for the *non-overlapping RO pairs* [52], both of which are discussed in Chapter 2 above, and 64 bits for the *regression-based distillers* [53]. Even if one assumes no errors, i.e., $R_s^* = 1$, for these methods, their $S_{\max}$ results are much smaller than the $S_{\max}$ results of our algorithm, as shown in Figure 3.3.

3.5.3. Transform Complexity

We measure the complexity of a transform in terms of the number of operations required to compute the transform and the hardware area required to implement it in a FPGA. We are first interested in a computational-complexity comparison for RO arrays of sizes $r = c = 8$ and $r = c = 16$, which are powers of 2, so that fast algorithms are available for the DCT, DWHT, and DHT. We then present an RO PUF hardware design for the transform with the minimum computational complexity.

The computational complexity of the KLT for $r = c = n$ is $O(n^3)$, while it is $O(n^2 \log_2 n)$

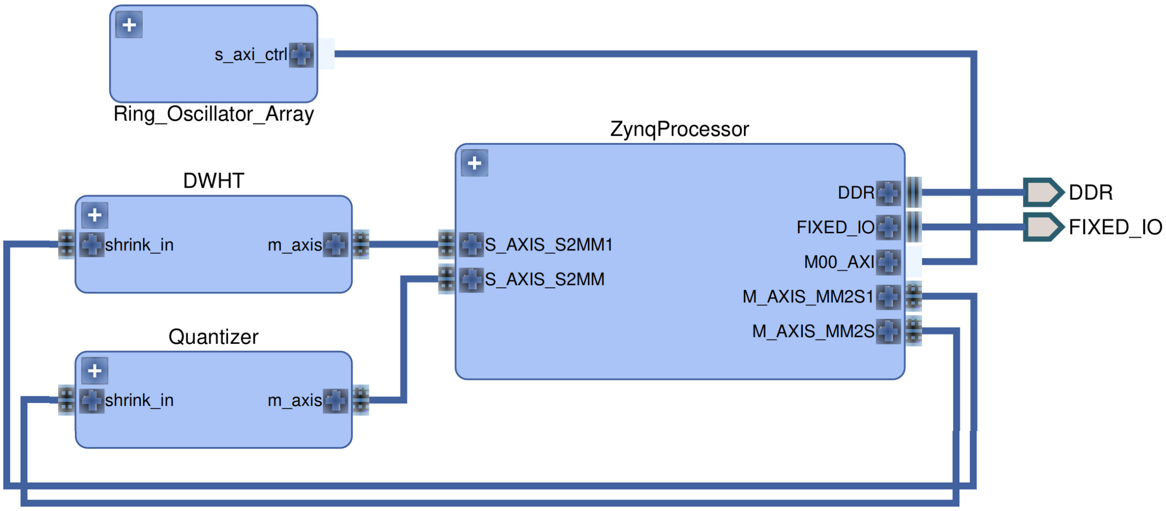

Figure 3.4.: Hardware design overview.

for the DCT and DWHT, and $O(n^2)$ for the DHT [68]. There are efficient implementations of the DWHT without multiplications [72]. The DWHT is thus a good candidate for RO PUF designs for, e.g., IoT applications.

We now give a reference FPGA implementation for the DWHT without multiplications to illustrate that the hardware area occupied by the transform-coding algorithm is small and the processing time is significantly better than previous RO PUF designs.

FPGA Implementation

We use a Xilinx ZC706 evaluation board with a Zynq-7000 XC7Z045 system-on-chip (SoC) to evaluate our DWHT design. A high level overview of the design is depicted in Figure 3.4. The Zynq SoC consists of an FPGA part and an ARM Cortex-A9 dual-core processor, connected with memory-mapped AXI4 buses [73]. The ARM processor is connected to three components: the RO array, DWHT, and quantizer. The RO array is connected via a bi-directional memory-mapped AXI bus, and the other components are connected via AXI streaming buses [74]. We first measure RO outputs with counters, give the counter values as input to the DWHT, and then quantize the transform coefficients to assign bits. This is an implementation of the transform-coding algorithm given in Figure 3.2.

We use a standard RO array of size 16 × 16. All ROs in a row are connected to a counter and they can be measured serially by using the same counter. There is an additional counter that stops the counting operations after a specified time. For the FPGA we use, it is practically necessary to use at least five inverters for each RO since using three inverters results in oscillation frequencies of about 1 GHz, which violates the timing constraints of the FPGA. Our RO designs with five inverters have oscillation frequencies in the range $[400, 500]$ MHz. Furthermore, we use 16-bit counters so that the minimum duration $T_{\min}$

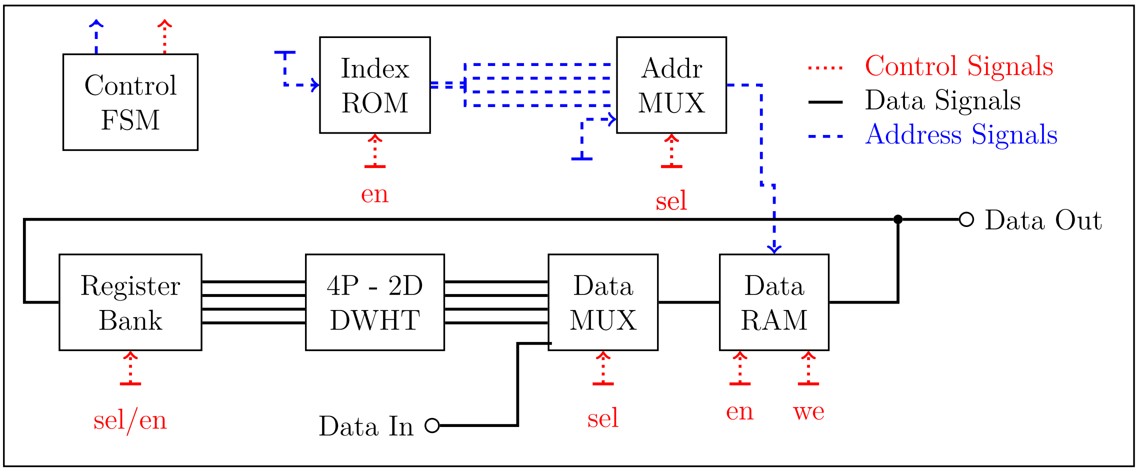

Figure 3.5.: Building blocks of the DWHT implementation with select (sel), enable (en), and write enable (we) control signals.

to have an overload in a counter is

$$T_{\text{min}} = \frac{2^{16} - 1}{500\ \text{MHz}} = 131\mu\text{s}. \tag{3.16}$$

We count each RO output for a duration of 100μs, which is less than T_{min} to avoid overloads. This results in a total counting duration of 1.6ms for all 16 columns of the RO array, which is compared below with the previous RO PUF designs.

We next implement an extended version of the algorithm in [72], proposed for an 8×8 array, to calculate the two-dimensional (2D) 16×16 DWHT without multiplications. The main block we use is the 4-point (4P)-2D DWHT [72] that takes four inputs $[x_0, x_1, x_2, x_3]$ and calculates

$$\begin{bmatrix} y_0 & y_1 \\ y_2 & y_3 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} x_0 + x_1 + x_2 + x_3 & x_0 - x_1 + x_2 - x_3 \\ x_0 + x_1 - x_2 - x_3 & x_0 - x_1 - x_2 + x_3 \end{bmatrix}. \tag{3.17}$$

We successively apply the 4P-2D DWHT to the 16×16 RO array according to an extension of the input-selection algorithm proposed in [72]. We implement a finite-state machine (FSM) to control the input and output AXI streaming interfaces as well as the input-selection algorithm. The building blocks of our DWHT implementation is depicted in Figure 3.5, which includes

- ▷ a data random access memory (RAM) to store all array elements,
- ▷ a 32-bit index read-only memory (ROM), where each word stores four 8-bit array-element addresses,
- ▷ a multiplexer (MUX) to select the RAM address to be accessed,

- ▷ a second MUX to select the ROM input,
- ▷ a register for each input to convey different RAM words to different ports.

We first store all RO outputs in the data RAM. Then, the first word of the index ROM is fetched. This word holds the addresses of four array elements to be loaded. These array elements are passed to the 4P-2D DWHT's input registers by selecting the corresponding port in the address MUX and register bank. After evaluating the 4P-2D DWHT, the new array elements $[y_0, y_1, y_2, y_3]$ are written back to the locations from where the inputs $[x_0, x_1, x_2, x_3]$ were fetched. The FSM performs the same steps for all remaining ROM words and conveys the 2D DWHT coefficients to the AXI output port.

The addition and subtraction operations on four numbers in each 4P-2D DWHT evaluation requires at most two additional bits, while the subsequent bit shift to implement the division by 2 in (3.17) removes one bit. Since the 4P-2D DWHT is applied in total four times to each RAM location, the transform requires 20-bit operations and storage in order to process the 16-bit signed numbers used for counter values.

The quantizer contains AXI stream ports, an FSM, and one ROM. The ROM holds $2^{K_i} - 1$ quantization boundaries for the i-th transform coefficient. We remark that the histogram equalization step in Figure 3.2 is useful when the number of bits K_i extracted is large, but we choose $K_i = K = 1$ for all used transform coefficients, which is illustrated in combination with an error-correction code design in Section 3.6.2. Therefore, we do not apply the histogram equalization step for this case, so the ROM contains 255 words and is of size 638 Bytes ($\geq 255 \times 20$ bits) in total. The FSM compares the quantizer input with the corresponding quantization boundary to assign a bit 1 for transform-coefficient values greater than the quantization boundary, and the bit 0 otherwise. The assigned bits are then conveyed to the output port.

Hardware Design Comparisons

We now compare our results with a benchmark RO PUF hardware design given in [60] in terms of the hardware area and processing times. The number of lookup tables (LUTs), registers, and MUXs used in [60] are not available. However, our results can be compared with their slice-count and processing-delay results since the FPGA (Spartan-6) used in [60] also has 4 LUTs, 8 registers, and 3 MUXes in each slice, the same as the FPGA used in this chapter. In addition, our quantizer and DWHT clock rate is 54 MHz, as in [60]. We list in Table 3.2 the hardware area occupied by individual components of our RO PUF design and by the RO PUF design of [60].

Table 3.2 illustrates that the RO array requires the highest hardware area and uses approximately 82% of all occupied LUTs, 62% of registers, and 86% of slices. We do not include the area for RAMs and ROMs, because we use Block RAM slices that are available in the FPGA. However, we include the control logic area required to control the Block RAM slices. Our DWHT-based design occupies an approximately 11% smaller RO PUF hardware area than the RO PUF design proposed in [60] in terms of the number of slices used. This result can be improved if we reuse the same area for different ROs, which might

Table 3.2.: Hardware area and processing delays for RO PUF designs.

Blocks	**LUT**	**Register**	**MUX**	**RAM&ROM**[B]	**Slice**	**Time**[μs]
Proposed-ROs	1632	397	65	0	729	1600
Proposed-DWHT	326	200	0	1664	99	66
Proposed-Quantizer	43	39	0	638	21	14
Proposed (ROPUF)	2001	636	65	2302	849	1680
PUFKY (ROPUF) [60]	n.a.	n.a.	n.a.	n.a.	952	4611

increase correlations in the RO outputs. In addition, the DWHT and quantizer constitute approximately 14% of the total slice count of our RO PUF design. These results illustrate that the transform-coding approach occupies a small hardware area.

The total counter duration of 1.6ms is a result of the calculation given in (3.16) to avoid overloads in the counters, and the choice of this value depends mainly on the number of inverters used for each RO and counter bit width. The overall processing time of the proposed design is approximately 1.68 ms, which is significantly better than the processing delay of the benchmark RO PUF design in [60].

3.5.4. Uniqueness and Security

The bit sequence extracted from a physical identifier should be uniformly distributed to make the rate region $\mathcal{R}$ in (3.5) valid. A common measure, called *uniqueness*, for checking randomness of a bit sequence is the average fractional Hamming distance between the bit sequences extracted from different RO PUFs [7]. We obtain similar uniqueness results for all transforms, where the mean Hamming distance is 0.500 and Hamming distance variance is approximately 7×10^{-4}. All transforms thus provide close to optimal uniqueness results due to their high decorrelation efficiencies and equipartitioned quantization intervals. These results are significantly better than the results 0.462 [52] and 0.473 [65].

The National Institute of Standards and Technology (NIST) provides a set of randomness tests that check whether a bit sequence can be differentiated from a uniformly random bit sequence [75]. We apply these tests to evaluate the randomness of the generated sequences. We observe that the bit sequences generated from ROs in the dataset [65] with the DWHT pass most of the applicable tests for short lengths for both reliability metrics, which is considered to be an acceptable result [75]. We also conclude that the KLT performs the best due to its optimal decorrelation performance. One can apply a thresholding approach such that the reliable transform coefficients from which the bits are extracted do not have high correlations, which further improves the security performance [8].

3.6. Privacy and Secrecy Analysis of Proposed Error-Correction Codes

Suppose that extracted bit sequences are i.i.d. and uniformly distributed so that the secrecy leakage is zero. We propose different codes for the transform-coding algorithm according to the two proposed reliability metrics.

3.6.1. Codes for the Quantizer Design with Fixed Measurement Channels

For the first quantizer method given in Section 3.4.1, fix an average crossover probability $p_b = 0.06$ to obtain the highest maximum secret-key length, as shown in Figure 3.3. We illustrate that there are efficient error-correction codes for the FCS with $P_B \leq 10^{-9}$ and a small privacy-leakage rate. Recall that the code dimension has to be at least 128 bits, a requirement of the AES, so the block length is in the short block-length regime for error-correction codes with high rates and $k = 128$. We expect a rate loss in our code designs due to the small block-error probability and short block length.

The basic approach to design codes for small block-error probabilities and reasonable decoding complexity is to use concatenated codes. Since the hardware complexity of a code design should be small for IoT applications, we minimize also the field sizes of the codes.

Remark 3.1. It would be natural to use iterative decoders in combination with high-performance codes like low density parity check (LDPC) and turbo codes. However, hardware complexity might increase and it is a difficult task to simulate these codes for $P_B \leq 10^{-9}$. We use concatenated algebraic codes so that we can find analytical bounds on P_B without simulations for the outer code.

The first construction uses a Reed-Muller (RM) code $\mathcal{C}(32, 6, 16)$ as the inner code and a Reed-Solomon (RS) code $\mathcal{C}(28, 22, 7)$ that operates with symbols from the Galois field $\mathbb{F}_{2^6}$ as the outer code of a concatenated code. Every symbol of the RS code can be represented by 6 bits and the code takes 22 symbols as input, which corresponds to 132 input bits which is greater than 128 bits. The maximum likelihood decoder (MLD) of the inner RM code transforms the BSC with crossover probability $p_b = 0.06$ into a channel with errors and erasures by declaring an *erasure* if there are two codewords with equal distances to a received vector and makes an *error* if a wrong codeword is selected. Simulation results show that the erasure probability after the MLD of the inner code is about 6.57×10^{-5} and the error probability is about 4.54×10^{-6}. One can correctly reconstruct the codeword of the outer code if $2 \times e + \nu < d$, where e is the number of errors and ν is the number of erasures in the received vector [76]. The block-error probability after decoding the outer RS code is approximately $P_B \approx 1.37 \times 10^{-11}$. The key and leakage rates of this code are $R_s = 0.1473$ and $R_\ell = 0.8527$ bits/source-bit, respectively.

An alternative concatenated code is a binary extended Bose-Chaudhuri-Hocquenghem (BCH) code $\mathcal{C}(256, 132, 36)$ as the outer code and a repetition code $\mathcal{C}(3, 1, 3)$ as the inner code. The MLD for the inner code transforms the BSC with crossover probability $p_b = 0.06$ into a BSC with $p_b = 0.0104$ so that the BMDD for the outer BCH code results in $P_B = 3.48 \times 10^{-10}$. The key-leakage rate pair (R_s, R_ℓ) for this code is $(0.1719, 0.8281)$ bits/source-bit, which gives better rates than the RM+RS concatenation above and the best generalized concatenated code (GCC) design with the FCS in [71] with the key-leakage rate pair $(0.1260, 0.8740)$ bits/source-bit, which is shown to be better than the previous results in [60]. The significant improvement in the rates with a low-complexity code is due to the decrease in p_b by using our transform-coding algorithm.

The FCS can asymptotically achieve the maximum secret-key rate $R_s^* = 0.6726$ bits/source-bit and corresponding minimum privacy-leakage rate $R_\ell^* = 0.3274$ bits/source-bit for a BSC($p_b = 0.06$). Better key-leakage rate pairs are thus possible, e.g., by using GCCs or by improving the decoder for the outer code. However, these constructions would result in increased hardware complexity, which is not desired for IoT applications.

3.6.2. Codes for the Quantizer Design with Fixed Number of Errors

We now select a channel code according to Section 3.4.2 to store a secret key of length 128 bits. The correctness probabilities defined in (3.11) for the transform coefficients T with the three highest and three smallest probabilities are plotted in Figure 3.6. The indices of the 16×16 transform coefficients follow the order in the dataset [65], where the coefficient index at the first row and first column is 1, and it increases columnwise up to 16 so that the second row starts with the index 17, the third row with the index 33, etc. The most reliable transform coefficients are the low-frequency coefficients, which are in our case at the upper-left corner of the 2D transform-coefficient array with indices such as $1, 2, 3, 17, 18, 19, 33, 34, 35$. The low-frequency transform coefficients therefore have the highest SNRs for the source and noise statistics obtained from the RO dataset in [65]. The least reliable coefficients are observed to be spatially away from the transform coefficients at the upper-left or lower-right corners of the 2D transform-coefficient array. These results indicate that the *SNR-packing efficiency*, which can be defined similarly as the energy-packing efficiency, of a transform follows a more complicated scan order than the classic zig-zag scan order used for the energy-packing efficiency metric [77]. Observe from Figure 3.6 that increasing the number of extracted bits decreases the correctness probability for all coefficients since the quantization boundaries get closer so that errors due to noise become more likely, i.e., the probability $P_c(K)$ defined in (3.11) decreases with increasing K.

We fix the maximum number $C_{\max}$ of transform coefficients T allowed to be in error and calculate the correctness threshold $\overline{P}_c(C_{\max})$ using (3.12), the total number $n(C_{\max})$ of extracted bits using (3.13), and the number $e(C_{\max})$ of errors the block code should be able to correct using (3.14). We observe that if $C_{\max} \leq 10$, $\overline{P}_c(C_{\max})$ is so large that $P_{c,i}(K = 1) \leq \overline{P}_c(C_{\max})$ for all $i = 2, \dots, l$. If $11 \leq C_{\max} \leq 15$, $n(C_{\max})$ is less than

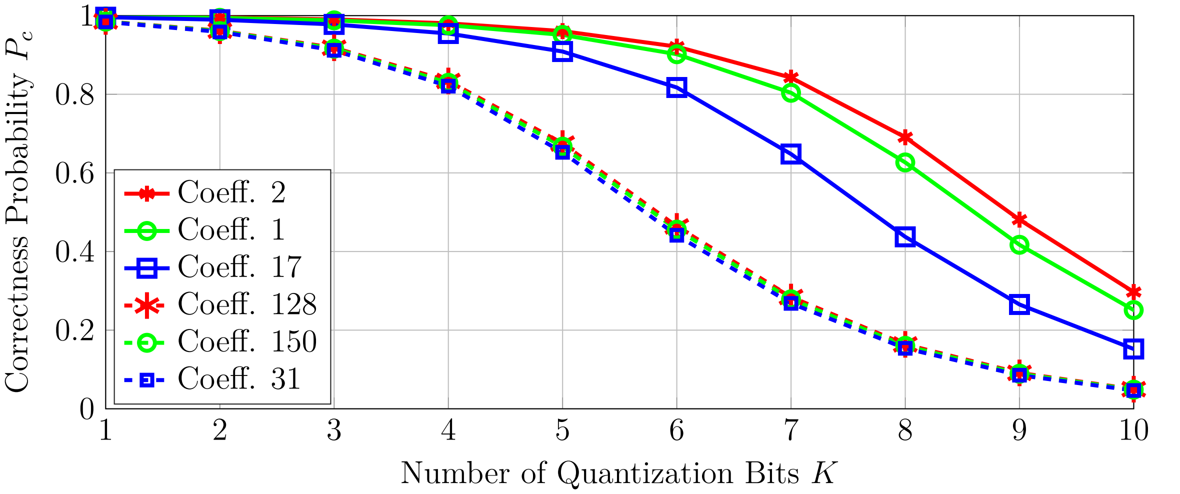

Figure 3.6.: The correctness probabilities for transform coefficients.

the required code dimension of 128 bits. Increasing $C_{\max}$ results in a smaller correctness threshold $\overline{P}_c(C_{\max})$ so that the maximum of the number $K_{\max}(C_{\max}) = K'_1(C_{\max})$ of bits extracted among the $l-1$ used coefficients increases. This result can increase hardware complexity. We thus do not consider the cases where $C_{\max}>20$. Table 3.3 shows $\overline{P}_c(C_{\max})$, $n(C_{\max})$, and $e(C_{\max})$ for the remaining range of $C_{\max}$ values, which are used for channel-code selection.

Consider again binary (extended) BCH and RS codes, which have good minimum-distance properties. An exhaustive search does not provide a code with dimension of at least 128 bits and with parameters satisfying any of the $(n(C_{\max}), e(C_{\max}))$ pairs in Table 3.3. However, the correctness threshold analysis leading to Table 3.3 is conservative. We therefore choose a BCH code with parameters as close as possible to a $(n(C_{\max}), e(C_{\max}))$ pair and then prove that even if the number e_{BCH} of errors the chosen BCH code can correct is less than $e(C_{\max})$, the block-error probability constraint is satisfied. Consider therefore the BCH code with the block length 255, code dimension 131, and a capability of correcting all error patterns with $e_{\text{BCH}} = 18$ or less errors.

We now show that the proposed code satisfies the block-error probability constraint. First, we impose the condition that exactly one bit is extracted from each coefficient, i.e., $K_i=1$ for all $i=2,3,\ldots,l$, so that in total $n=l-1=255$ bits are obtained. Note that this results in independent bit errors E_i. It follows from this condition that the chosen block code should be able to correct all error patterns with up to $e=20$ bit errors rather than $e(20)=25$ bit errors, which is still greater than the error-correction capability $e_{\text{BCH}} = 18$ of the considered BCH code.

The block error probability P_B for the BCH code $\mathcal{C}(255,131,37)$ with a BMDD corre-

Table 3.3.: Code-parameter constraints.

$\mathbf{C_{max}}$	**16**	**17**	**18**	**19**	**20**
$\bar{P}_c$	0.9902	0.9889	0.9875	0.9860	0.9844
$K_{\max}$	3	3	3	3	3
n	144	224	250	255	259
e	18	20	21	23	25

sponds to the probability of having more than 18 errors in the codeword, i.e.,

$$P_B = \sum_{j=19}^{255} \left[\sum_{A \in \mathcal{F}_j} \prod_{i \in A} (1 - P_{c,i}) \cdot \prod_{i \in A^c} P_{c,i} \right] \tag{3.18}$$

where $P_{c,i}$ is the correctness probability of the i-th transform coefficient $\widehat{T}_i$ defined in (3.11) for $i = 2, 3, \ldots, 256$, $\mathcal{F}_j$ is the set of all size-j subsets of the set $\{2, 3, \ldots, 256\}$, and A^c denotes the complement of the set A. The correctness probabilities $P_{c,i}$ are different and they represent probabilities of independent events due to the independence assumption for the transform coefficients.

One needs to consider $\sum_{j=0}^{18} \binom{255}{j} \approx 1.90 \times 10^{27}$ different cases to calculate (3.18), which is not practical. We thus use the discrete Fourier transform - characteristic function method [78] to calculate the block-error probability and obtain the result $P_B \approx 1.26 \times 10^{-11} < 10^{-9}$. The block-error probability constraint is thus satisfied by using the BCH code $\mathcal{C}(255, 131, 37)$ with a BMDD although the conservative analysis suggests that it would not be satisfied.

We now compare the BCH code $\mathcal{C}(255, 131, 37)$ with previous codes proposed for binding keys to physical identifiers with the FCS and a secret-key length of 128 bits such that $P_B \leq 10^{-9}$ is satisfied. The (secret-key, privacy-leakage) rate pair for this proposed code is $(R_s, R_\ell) = (\frac{131}{255}, 1 - \frac{131}{255}) \approx (0.514, 0.486)$ bits/source-bit. This pair is significantly better than our previous results in Section 3.6.1 proposed for a BSC ($p_b = 0.06$). The main reason for obtaining a better (secret-key, privacy-leakage) rate pair is that the quantizer in Section 3.4.2 allows us to exploit higher identifier-output reliability by decreasing the number of bits extracted from each transform coefficient.

We compare the secret-key and privacy-leakage rates of the BCH code $\mathcal{C}(255, 131, 37)$ with the region of all achievable rate pairs for the CS model and the FCS for a BSC $P_{Y|X}$ with crossover probability $p_b = 1 - \frac{1}{l-1} \sum_{i=2}^{l} P_{c,i}(K_i = 1) \approx 0.0097$, i.e., the probability of being in error averaged over all used transform coefficients with the quantizer in Section 3.4.2. We compute the boundary points of the region $\mathcal{R}'$ by using Mrs. Gerber's lemma [79], which gives the optimal auxiliary random variable U in (3.6) when $P_{Y|X}$ is a BSC. We plot the regions of all rate pairs achievable by the FCS and CS model, the maximum secret-key rate point, the (secret-key, privacy-leakage) rate pair of the proposed

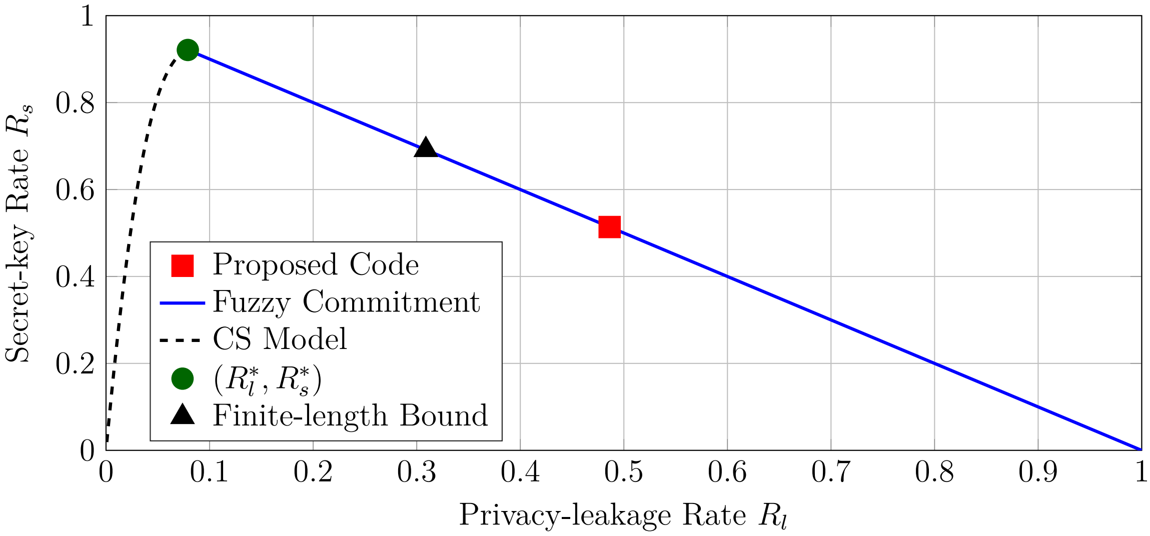

Figure 3.7.: The operation point of the proposed BCH code $\mathcal{C}(255, 131, 37)$, regions of achievable rate pairs according to (3.5) and (3.6), the maximum secret-key rate point, and a finite-length bound for $n = 255$ bits, $P_B = 10^{-9}$, and BSC (0.0097).

code, and a finite-length bound [80] for the block length of $n = 255$ bits and $P_B\!=\!10^{-9}$ in Figure 3.7.

The maximum secret-key rate is $R_s^* \approx 0.922$ bits/source-bit with a corresponding minimum privacy-leakage rate of $R_\ell^* \approx 0.079$ bits/source-bit. There is a gap between the secret-key rate of the proposed code and the only operation point where the FCS is optimal, i.e., (R_ℓ^*, R_s^*). Part of this rate loss can be explained by the short block length of the code and the small block-error probability constraint. The finite-length bound given in [80, Theorem 52] establishes that the rate pair $(R_s, R_\ell)\!=\!(0.691, 0.309)$ bits/source-bit is achievable by using the FCS, as depicted in Figure 3.7. One can therefore further improve the rate pairs by using better codes and decoders with higher hardware complexity, but this may not be possible for IoT applications. Figure 3.7 also illustrates that there exist other code constructions, e.g., the WZ-coding construction in Chapter 5, that reduce the privacy-leakage rate for a fixed secret-key rate.

4

Key Agreement with Multiple Measurements of Identifiers

In this chapter, we consider the gains from measuring an identifier multiple times during reconstruction and also during enrollment. The latter scenario suggests that the identifier output is a hidden, or remote, source whose noisy measurements are observed at the encoder unlike previous identifier models in the literature. We determine the information-theoretic rate regions for the hidden source case and quantify the reduction in the privacy-leakage rate for a hidden identifier as compared to a noise-free, or visible, identifier. More importantly, if the encoder incorrectly models the source as visible, it is shown that substantial secrecy leakage may occur and the reliability of the reconstructed key might decrease. The results of this chapter were published in [12, 13].

4.1. Motivation

Consider the key agreement model introduced in [62] and [63] where two terminals observe dependent random variables and have access to a public communication link; an eavesdropper observes the messages, called *helper data*, transmitted over this link. Similar to Chapter 3, we consider the GS and CS models, where the information through helper data about the secret key, called the *secrecy leakage*, should be negligible. Furthermore, the information leaked about the identifier, called the *privacy leakage*, should be minimized so that an eavesdropper cannot obtain information about a second secret key stored by a second encoder that uses the same or a correlated identifier.

The secret-key vs. privacy-leakage, or key-leakage, regions for the two models are given in [56] and [57]. In addition to the secret-key and privacy-leakage rates, it is important to consider the amount of storage in the public link that is required for the decoder to reliably reconstruct the secret key [81]. The storage rate is generally equal to the privacy-leakage rate when we consider the GS model. Similarly, for the CS model, the storage rate is generally equal to the sum of the secret-key and privacy-leakage rates. The storage rate is different from the privacy-leakage rate for general (non-negligible) secrecy-leakage levels [82], unlike for the negligible secrecy-leakage rate constraint considered in [56] and [57]. We show that the storage and privacy-leakage rates are different also when the identifier is a *remote* or *hidden* source [83, p. 118], [84, p. 78].

Secret-key based user or device authentication with a privacy-leakage constraint is considered in [85]. There is an assumption in [85] that the eavesdropper has side information correlated with the identifier outputs, which is reasonable for biometric identifiers because they are continuously available for attacks. However, physical identifiers like PUFs are used for on-demand key reconstruction. Invasive attacks on PUFs also permanently change the identifier output, as mentioned in Chapter 3, so we assume in this chapter that the eavesdropper cannot obtain information correlated with the PUF output. Key agreement with correlated side information at the eavesdropper has been studied in [86–88]. We remark that there can be algorithms designed for key agreement with PUFs that mistakenly do not eliminate the effects of correlation between the PUF outputs in different devices, which results in side information available to the eavesdropper. We therefore consider an eavesdropper with side information in Chapter 6 for biometric identifiers and for such algorithms.

Multiple measurements of biometric or physical identifiers at the decoder can substantially decrease the privacy-leakage and storage rates because less side information is required to reconstruct the secret key as compared to a single measurement. One obtains a diversity gain, corresponding to a gain in reliability, to combat erroneous measurements by averaging over different channels. One can also exploit the additional degrees of freedom by increasing the extracted secret-key size. The latter gain can be viewed as a multiplexing gain, in analogy to multiple antenna systems for wireless communications. Such gains in the achievable key-leakage rates are illustrated in [12] when there are multiple noisy measurements of the source at the decoder.

The above models assume that the encoder measures the “true” source. We propose that the true source, i.e., the ground truth, is instead hidden from the encoder and the encoder measures a noisy version of the source (see also discussions in [7] on key-binding with a hidden identifier, [89] where a hidden source is considered for authentication, and [90, Sec. II] for indirect rate-distortion problems with action-dependent side information). For example, many secrecy systems require multiple measurements at the encoder to obtain the “noise-free” output. As a second example, different systems may generate different sequences from the same identifier.

Consider multiple encoders with independent channels from the hidden source to the corresponding encoders. This is a valid scenario for biometric and physical identifiers due to differences in the environmental conditions when extracting secret keys by different encoders. An eavesdropper who wants to seize a secret key can use the information available from other encoders about the hidden source, which leads to privacy-leakage with respect to the hidden source rather than the noisy encoder measurements.

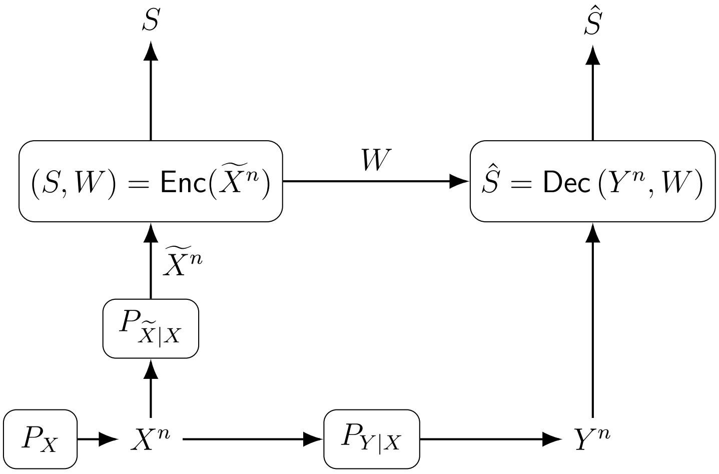

Figure 4.1.: The GS model where a secret key is generated from a noisy identifier measurement.

4.1.1. Models for Identifier Outputs

We study the physical and biometric identifier outputs that are i.i.d. according to a probability distribution with a discrete alphabet. These models are reasonable if one uses transform-coding algorithms, as given in Chapter 3, to extract almost i.i.d. bits from PUFs. Similar transform-coding based algorithms have been applied to biometric identifiers to obtain independent output symbols [91].

4.1.2. Summary of Contributions and Organization

We extend the model of [56] and [57] to include multiple noisy identifier measurements at the encoder and decoder. A summary of the main contributions is as follows.

- ▷ We derive the key-leakage-storage regions for the GS and CS models with a hidden source; see Figures. 4.1 and 4.2 for the corresponding models. Our rate regions recover several results in the literature, including various results for a visible source without eavesdropper side information in [56, 57, 62, 63, 81]. We further recover our previous results from [12] that studied the visible source model.
- ▷ We evaluate the rate region for a binary hidden source with multiple measurements at the decoder and a single noisy measurement at the encoder by applying Mrs. Gerber's lemma (MGL) [79]. The analysis differs from [56] and [57] because we need to apply MGL twice in different directions to a Markov chain rather than once. For measurement channels with a certain symmetry, we find the optimal auxiliary random variable for coding.
- ▷ We show that a significant amount of secrecy might be leaked, and the reliability of the reconstructed key might decrease, if the visible source model is mistakenly

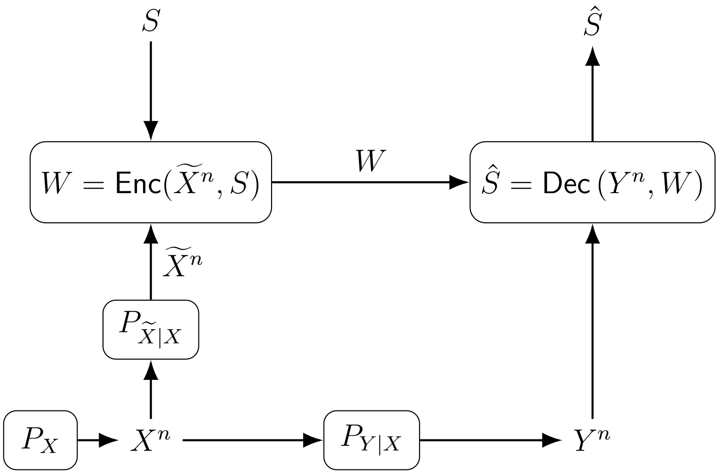

Figure 4.2.: The CS model where a secret key is given to the encoder together with a noisy identifier measurement.

used for multiple decoder measurements of a hidden source. Such a mistake leads to violations of the security and reliability constraints.

▷ Gains from having multiple measurements at the encoder are also illustrated. We show that gains in the secret-key rate can come at a large cost of storage.

This chapter is organized as follows. In Section 4.2, we describe our problem and develop the key-leakage-storage regions for the GS and CS models. The key-leakage-storage region of a binary hidden source with multiple measurements at the decoder is derived in Section 4.3. In Section 4.4, we illustrate gains from the hidden source model as compared to the visible one and depict the maximum secret-key rates achieved by having multiple encoder and decoder measurements.

4.2. System Models and Rate Regions

4.2.1. System Models

Consider a discrete memoryless source that generates i.i.d. symbols X^n from a finite set $\mathcal{X}$ according to a probability distribution P_X. Identifier outputs are noisy due to, for instance, cuts on a finger. The noise at the encoder and decoder is modeled as memoryless channels $P_{\widetilde{X}|X}$ and $P_{Y|X}$, respectively. The outputs of $P_{\widetilde{X}|X}$ and $P_{Y|X}$ are, respectively, the strings $\widetilde{X}^n$ with realizations from a finite set $\widetilde{\mathcal{X}}^n$, and Y^n with realizations from a finite set $\mathcal{Y}^n$. We thus have

$$P_{\widetilde{X}^nX^nY^n}(\tilde{x}^n, x^n, y^n) = \prod_{i=1}^{n} P_{\widetilde{X}|X}(\tilde{x}_i|x_i)P_X(x_i)P_{Y|X}(y_i|x_i). \tag{4.1}$$

The distributions $P_{\widetilde{X}|X}$ and $P_{Y|X}$ are assumed to be known for now, although we later study what happens if the encoder treats $\widetilde{X}^n$ as the true source.

In the GS model depicted in Figure 4.1, an encoder sees $\widetilde{X}^n$ and generates a secret key S and helper data W as $(S, W) = \mathsf{Enc}(\widetilde{X}^n)$, where $\mathsf{Enc}(\cdot)$ is an encoder mapping. The decoder estimates the key as $\hat{S} = \mathsf{Dec}(Y^n, W)$, where $\mathsf{Dec}(\cdot)$ is a decoder mapping. In the CS model shown in Figure 4.2, S is independent of $(X^n, \widetilde{X}^n, Y^n)$ and an encoder mapping generates the helper data as $W = \mathsf{Enc}(\widetilde{X}^n, S)$. The decoder estimates the key as $\hat{S} = \mathsf{Dec}(Y^n, W)$.

Definition 4.1. A (secret-key, privacy-leakage, storage) rate triple (R_s, R_ℓ, R_w) is *achievable* if, given any $\delta > 0$, there is some $n \geq 1$, an encoder, and a decoder for which $R_s = \dfrac{\log|\mathcal{S}|}{n}$ and

$$\Pr[S \neq \hat{S}] \leq \delta \qquad (reliability) \tag{4.2}$$

$$\frac{1}{n} I\left(S; W\right) \leq \delta \qquad (weak\ secrecy) \tag{4.3}$$

$$\frac{1}{n} I\left(X^n; W\right) \leq R_\ell + \delta \qquad (privacy) \tag{4.4}$$

$$\frac{1}{n} H(S) \geq R_s - \delta \qquad (uniformity) \tag{4.5}$$

$$\frac{1}{n} \log|\mathcal{W}| \leq R_w + \delta \qquad (storage). \tag{4.6}$$

The key-leakage-storage region is the closure of the set of achievable rate tuples. We refer to models where $\widetilde{X}^n = X^n$ as visible source model (VSM) and other cases as hidden source model (HSM).

4.2.2. Key-leakage-storage Regions

We present the key-leakage-storage regions for the GS and CS models in Theorems 4.1 and 4.2, respectively. The proofs of the theorems are given in Appendices A.1-A.2. We derive cardinality bounds for the auxiliary random variable in Appendix A.3. Using standard arguments, one can establish the convexity of the rate regions, i.e., there is no need for convexification via a time-sharing random variable.

Theorem 4.1. The key-leakage-storage region for the GS model is

$$\begin{aligned} \mathcal{R}_1 = \bigcup_{P_{U|\widetilde{X}}} \Big\{ & (R_s, R_\ell, R_w) : \\ & 0 \leq R_s \leq I(U;Y), \\ & R_\ell \geq I(U;X) - I(U;Y), \\ & R_w \geq I(U;\widetilde{X}) - I(U;Y) \Big\} \end{aligned} \tag{4.7a}$$

$$\text{where } P_{U\widetilde{X}XY} = P_{U|\widetilde{X}} \cdot P_{\widetilde{X}|X} \cdot P_X \cdot P_{Y|X}. \tag{4.7b}$$

Theorem 4.2. The key-leakage-storage region for the CS model is

$$\begin{aligned}\mathcal{R}_2 = \bigcup_{P_{U|\widetilde{X}}} \Big\{ &(R_s, R_\ell, R_w): \\ &0 \leq R_s \leq I(U;Y), \\ &R_\ell \geq I(U;X) - I(U;Y), \\ &R_w \geq I(U;\widetilde{X}) \Big\}\end{aligned} \tag{4.8a}$$

$$\text{where } P_{U\widetilde{X}XY} = P_{U|\widetilde{X}} \cdot P_{\widetilde{X}|X} \cdot P_X \cdot P_{Y|X}. \tag{4.8b}$$

Remark 4.1. The Markov conditions in (4.7b) and (4.8b) state that $U - \widetilde{X} - X - Y$ forms a Markov chain. One may restrict the cardinality of the auxiliary random variable U to $|\mathcal{U}| \leq |\widetilde{\mathcal{X}}| + 2$ for both theorems.

Remark 4.2. The converses for Theorems 4.1 and 4.2 permit randomization at the encoder (see (A.24)(b) and (A.27)(b)) and decoder (see (A.21)(a)). Since achievability requires no randomization, we may use deterministic encoders and decoders. The achievability of $\mathcal{R}_2$ follows directly from the achievability of $\mathcal{R}_1$ by using the key S of the GS model as a key of a one-time pad to secure a chosen key and storing the output at rate $I(U;Y)$.

We recover the previous results in [56] and [57] if $\widetilde{X} = X$ in both theorems so that the maximum achievable secret-key rate $I(\widetilde{X};Y)$ in these regions is at most $I(X;Y)$, which is the maximum achievable secret-key rate if the identifier X^n is observed noise-free at the encoder. The minimum achievable privacy-leakage rate in these regions decreases as compared to in [56] and [57] because $I(U;X) \leq I(U;\widetilde{X})$.

4.3. Binary Identifier Measurements

We evaluate the key-leakage-storage regions for a binary hidden source. The binary random sequence $\widetilde{X}^n$ corresponds to a single noisy measurement of the binary source X^n at the encoder, and the random sequence $Y^n_{1:M_D}$ is the output of M_D measurements of X^n for $M_D \geq 1$ at the decoder. We assume that the inverse channel $P_{X|\widetilde{X}}$ is a BSC, an assumption that is fulfilled if P_X is uniform and $P_{\widetilde{X}|X}$ is a BSC. Moreover, we assume that the channel $P_{Y_{1:M_D}|X}$ can be decomposed into a mixture of BSCs (i.e., binary-input symmetric memoryless channels [92], [93]), as illustrated below in Figure 4.3 for dependent BSCs. The former constraint lets us apply MGL to the Markov chain $U - \widetilde{X} - X$; the latter lets us apply an extension of MGL to the Markov chain $U - X - Y_{1:M_D}$. Recall that MGL is based on the result that, for any $0 \leq p \leq 1$, the function

$$f(\nu) = H_b(p * H_b^{-1}(\nu)) \tag{4.9}$$

is convex in ν for $0 \leq \nu \leq 1$ [79].

Evaluating the key-leakage-storage regions corresponds to maximizing $I(U;Y_{1:M_D})$ and minimizing $I(U;\widetilde{X})$ for a fixed $I(U;X)$. It thus requires minimizing $H(Y_{1:M_D}|U)$ and maximizing $H(\widetilde{X}|U)$ for a fixed $H(X|U)$.

Let $\tilde{p}_i\in[0,0.5]$ be the smaller transition probability from $U=u_i$ to $X=0$ or $X=1$ for $i\in\{1,2,\dots,|\mathcal{U}|\}$. We have

$$H(X|U)=\sum_{i=1}^{|\mathcal{U}|}P_U(u_i)H_b(\tilde{p}_i) \tag{4.10}$$

$$H(Y_{1:M_D}|U)=\sum_{i=1}^{|\mathcal{U}|}P_U(u_i)g(\tilde{p}_i) \tag{4.11}$$

where

$$g(\tilde{p}_i)=H(Y_{1:M_D}|U=u_i). \tag{4.12}$$

In the following, we first study dependent BSCs $P_{Y_{1:M_D}|X}$, which can be decomposed into a mixture of BSCs. We next discuss the convexity of the function $g(H_b^{-1}(\nu))$ in ν for binary-input channels $P_{Y_{1:M_D}|X}$ that can be decomposed into a mixture of BSCs to establish a tight lower bound on $H(Y_{1:M_D}|U)$ if we fix $H(X|U)$. Then, we simplify the key-leakage-storage regions of binary identifiers measured through such channels $P_{Y_{1:M_D}|X}$.

4.3.1. Measurements Through Dependent BSCs

We show that channels with multiple measurements of X through dependent BSCs can be decomposed into a mixture of independent BSCs. For simplicity, consider $M_D=3$ with

$$\begin{bmatrix}Y_1\\Y_2\\Y_3\end{bmatrix}=X\begin{bmatrix}1\\1\\1\end{bmatrix}\oplus\begin{bmatrix}B_1\\B_2\\B_3\end{bmatrix} \tag{4.13}$$

where B_1, B_2, and B_3 are mutually dependent binary random variables that are jointly independent of X. We can decompose the channel (4.13) into four independent BSCs, since we have

$$P_{Y_1Y_2Y_3|X}(y_1,y_2,y_3|x)=P_{Y_1Y_2Y_3|X}(\bar{y}_1,\bar{y}_2,\bar{y}_3|\bar{x}). \tag{4.14}$$

Define

$$q_{y_1y_2y_3}=P_{Y_1Y_2Y_3|X}(y_1,y_2,y_3|0). \tag{4.15}$$

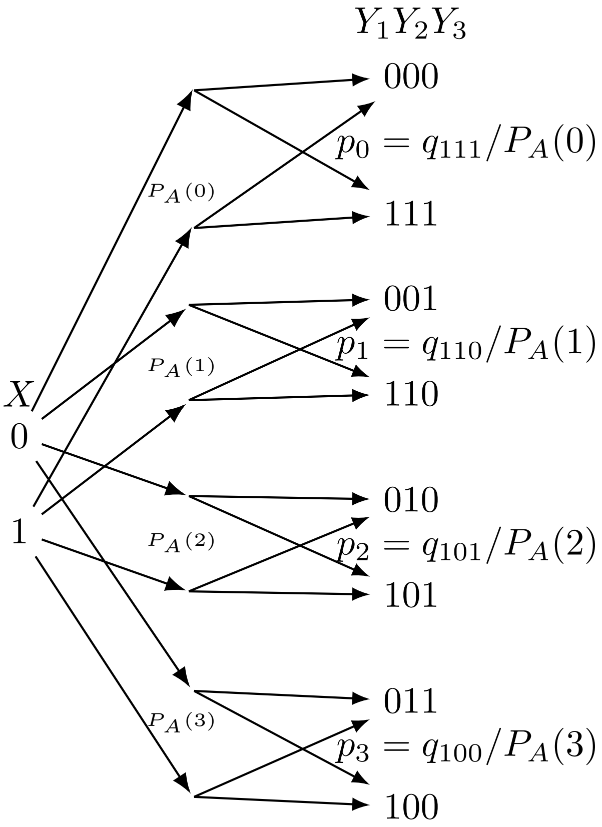

Figure 4.3.: $M_D = 3$ dependent BSCs represented as a mixture of $2^{M_D-1} = 4$ BSCs.

The decomposed channel is depicted in Figure 4.3, where the subchannel probabilities are

$$P_A(0) = q_{000} + q_{111} \tag{4.16}$$

$$P_A(1) = q_{001} + q_{110} \tag{4.17}$$

$$P_A(2) = q_{010} + q_{101} \tag{4.18}$$

$$P_A(3) = q_{011} + q_{100} \tag{4.19}$$

and the crossover probabilities are $p_0 = q_{111}/P_A(0)$, $p_1 = q_{110}/P_A(1)$, $p_2 = q_{101}/P_A(2)$, and $p_3 = q_{100}/P_A(3)$.

More generally, we can decompose a channel with M_D dependent BSC measurements into 2^{M_D-1} independent subchannels each with output symbols such that one symbol is the one's complement of the other symbol. We define

$$q_{b^{M_D}} = P_{Y_{1:M_D}|X}(b^{M_D}|0) \tag{4.20}$$

for the length-M_D binary string $b^{M_D} = b_0 b_1 \ldots b_{M_D-1}$ and

$$P_A(a) = q_{\mathsf{Bin}(a)} + q_{\overline{\mathsf{Bin}(a)}} \tag{4.21}$$

where $\overline{\mathsf{Bin}(a)}$ is the one's complement of $\mathsf{Bin}(a)$ for $a = 0, 1, \ldots, 2^{M_D-1} - 1$. The crossover probability of the a-th subchannel is $p_a = q_{\overline{\mathsf{Bin}(a)}}/P_A(a)$.

4.3.2. Mixtures of BSCs

Consider a channel $P_{Y_{1:M_D}|X}$ with a binary input and M_D binary measurements as output, i.e., the channel has 2^{M_D} possible output symbols. We decompose the channel into $L = 2^{M_D-1}$ BSCs as described above. We index these BSCs from 1 to L. Let $A = a$ represent the BSC index chosen by the channel and let p_a be the crossover probability of a-th subchannel. The conditional decoder-output entropy is

$$\begin{aligned}
H(Y_{1:M_D}|U) &\overset{(a)}{=} H(Y_{1:M_D}, A|U) \\
&\overset{(b)}{=} H(A) + \sum_{i=1}^{|\mathcal{U}|} P_U(u_i) \sum_{a=0}^{L-1} P_A(a) H(Y_{1:M_D}|A = a, U = u_i) \\
&\overset{(c)}{=} H(A) + \sum_{i=1}^{|\mathcal{U}|} P_U(u_i) \sum_{a=0}^{L-1} P_A(a) H_b(p_a * H_b^{-1}\Big(H(X|U = u_i)\Big)) \\
&= \sum_{i=1}^{|\mathcal{U}|} P_U(u_i) \sum_{a=0}^{L-1} P_A(a) \Big(H_b(p_a * \tilde{p}_i) - \log P_A(a)\Big)
\end{aligned} \tag{4.22}$$

where (a) follows because the output symbols determine A, (b) follows since A is independent of X so that U and A are independent, and (c) follows because $H_b(p_a * p)$ is symmetric with respect to $p = \frac{1}{2}$. Using (4.12) and (4.22), we have

$$g(\tilde{p}) = \sum_{a=0}^{L-1} P_A(a) \Big(H_b(p_a * \tilde{p}) - \log P_A(a)\Big). \tag{4.23}$$

Examples of channels that are mixtures of BSCs are the dependent BSCs in Section 4.3.1, the binary erasure channel (BEC) [94, p. 107], and additive white Gaussian noise (AWGN) channels with binary phase shift keying (BPSK) signals and symmetric (e.g., uniform) quantizers [94, p. 108].

The convexity property (4.9) carries over to channels $P_{Y_{1:M_D}|X}$ that can be decomposed into a mixture of BSCs [92], i.e., the function $g(\cdot)$ in (4.23) has the property that $g(H_b^{-1}(\nu))$ is convex in ν for $0 \le \nu \le 1$. To see this, note that $P_A(\cdot)$ is fixed and the following term in (4.22)(c)

$$\sum_{a=0}^{L-1} P_A(a) H_b(p_a * H_b^{-1}(\nu_i)))$$

where $\nu_i = H(X|U = u_i)$, is a weighted sum of convex functions of ν_i by MGL. An alternative proof of the convexity property for multiple independent BSCs is given in Appendix A.4. We extend this result below in Theorem 4.5 to show that the boundary points of $\mathcal{R}_1$ and $\mathcal{R}_2$ are achieved by channels $P_{\widetilde{X}|U}$ that are BSCs.

4.3.3. Two Lemmas

Consider a binary-input channel $P_{Y_{1:M_D}|X}$ that can be decomposed into a mixture of BSCs. For Theorem 4.5 below, we use the following two technical lemmas.

Lemma 4.3. We have

$$H(Y_{1:M_D}|U) \geq g\Big(H_b^{-1}\big(H(X|U)\big)\Big). \tag{4.24}$$

Proof. Since $g(H_b^{-1}(\nu))$ is convex in ν, by Jensen's inequality we have

$$H(Y_{1:M_D}|U) = \sum_{i=1}^{|\mathcal{U}|} P_U(u_i) g\Big(H_b^{-1}\big(H_b(\tilde{p}_i)\big)\Big) \geq g\left(H_b^{-1}\left(\sum_{i=1}^{|\mathcal{U}|} P_U(u_i) H_b(\tilde{p}_i)\right)\right).$$

□

Lemma 4.4. There is a unique $\tilde{p}^*$ in the interval $[0, 0.5]$ for which $H(X|U) = H_b(\tilde{p}^*) = \nu$.

Proof. The function $H_b(\cdot)$ is strictly increasing from 0 to 1 in the interval $[0, 0.5)$. We further have $0 \leq H(X|U) \leq H(X) \leq 1$. □

4.3.4. Simplified Rate Region Characterizations

We now simplify the key-leakage-storage regions for the measurement channels $P_{\widetilde{X}|X}$ and $P_{Y_{1:M_D}|X}$ considered above so that a single parameter characterizes the regions.

Theorem 4.5. Suppose $P_{X|\widetilde{X}}$ is a BSC with crossover probability p, where $0 \leq p \leq 0.5$, and $P_{Y_{1:M_D}|X}$ is a mixture of BSCs. The boundary points of $\mathcal{R}_1$ and $\mathcal{R}_2$ are achieved by channels $P_{\widetilde{X}|U}$ that are BSCs.

Proof. Consider the boundary points of $\mathcal{R}_1$ that satisfy

$$(R_s, R_\ell, R_w) = \Big(I(U;Y_{1:M_D}), I(U;X) - I(U;Y_{1:M_D}), I(U;\widetilde{X}) - I(U;Y_{1:M_D})\Big).$$

For a fixed $H(X|U)$, we obtain

$$I(U;Y_{1:M_D}) \leq H(Y_{1:M_D}) - g\Big(H_b^{-1}(H(X|U))\Big) \tag{4.25}$$

and

$$I(U;X)-I(U;Y_{1:M_D})\geq H(X)-H(X|U)-H(Y_{1:M_D})+g\Big(H_b^{-1}(H(X|U))\Big) \tag{4.26}$$

and

$$\begin{aligned} &I(U;\widetilde{X})-I(U;Y_{1:M_D}) \\ &\geq H(\widetilde{X})-H_b\left(\frac{H_b^{-1}(H(X|U))-p}{1-2p}\right)-H(Y_{1:M_D})+g\Big(H_b^{-1}(H(X|U))\Big) \end{aligned} \tag{4.27}$$

where we used Lemma 4.3 to bound $H(Y_{1:M_D}|U)$, and the MGL result in (4.9) with $\nu = H(\widetilde{X}|U)$ to bound $H(\widetilde{X}|U)$. By choosing $P_{U|\widetilde{X}}$ such that $P_{\widetilde{X}|U}$ is a BSC with crossover probability

$$\tilde{x} = \frac{H_b^{-1}(H(X|U))-p}{1-2p} \tag{4.28}$$

where $\tilde{x}\in[0,0.5]$, we achieve the right-hand sides of (4.25)-(4.27) since assigning $H(\widetilde{X}|U) = H_b(\tilde{x})$ achieves equality in (4.9) and (4.24) for the given channels. By Lemma 4.4, this $\tilde{x}$ is the unique solution. The proof for $\mathcal{R}_2$ is similar. □

The convexity property for a BSC, used in MGL, is extended to any binary channel $P_{Y_1|X}$ by Witsenhausen in [95], by Wyner as a remark in [95, Sec. III], and also by Ahslwede and Körner in [96]. Therefore, the channels $P_{Y_{1:M_D}|X}$ that can be decomposed into a mixture of *binary* channels also satisfy the convexity property. This result follows because the function $g(\cdot)$ for such channels, obtained from (4.12), also consists of a constant part and a weighted sum of functions that are convex in ν_i.

Remark 4.3. In [12, Theorem 1], we claimed that for a mixture $P_{Y_{1:M_D}|X}$ of binary channels, we achieve the boundary points of $\mathcal{R}_1$ and $\mathcal{R}_2$ when $\widetilde{X}^n = X^n$ by using channels $P_{X|U}$ that are BSCs. It turns out that this claim is valid for mixtures $P_{Y_{1:M_D}|X}$ of BSCs, but not necessarily otherwise. The reason is that one cannot necessarily achieve equality in [12, (25) and (26)]. This is illustrated in Appendix A.5 for a binary asymmetric channel.

4.4. Model Comparisons

4.4.1. Hidden Source Model

We study the GS model with a hidden binary symmetric source (BSS) such that $P_X(0)=P_X(1)=0.5$. Suppose $P_{\widetilde{X}|X}$ is a BSC with crossover probability p_{E} and $P_{Y_{1:M_D}|X}$ consists of M_D independent BSCs each with crossover probability p_{D}. The inverse channel $P_{X|\widetilde{X}}$ is also a BSC with crossover probability p_{E} because of source symmetry. Due to the independence assumption for M_D BSCs, the probabilities of sequences $y_{1:M_D}$ with the same Hamming weight are equal. Therefore, the decoder-output entropy is

$$H(Y_{1:M_D}) = \sum_{k=0}^{M_D} \left(\Pr\left[\sum_{m=1}^{M_D} Y_m = k\right] \times \log_2 \left(\binom{M_D}{k} \Big/ \Pr\left[\sum_{m=1}^{M_D} Y_m = k\right] \right) \right) \tag{4.29}$$

where

$$\Pr\left[\sum_{m=1}^{M_D} Y_m = k\right] = \binom{M_D}{k} \left(\frac{\bar{p}_D^{M_D-k} p_{\mathrm{D}}^{k} + \bar{p}_D^{k} p_{\mathrm{D}}^{M_D-k}}{2} \right). \tag{4.30}$$

By Theorem 4.5, the crossover probability $\tilde{x}$, as in (4.28), of the BSC $P_{\widetilde{X}|U}$ is the only parameter required to characterize $\mathcal{R}_1$ for the considered source and channels. Thus, using Theorem 4.5, the conditional entropy $H(Y_{1:M_D}|U)$ can be calculated similarly as in (4.29) by using the weighted sum in (4.30) with the weights $\tilde{p} = \tilde{p}_1 = \tilde{p}_2$ and $1 - \tilde{p}$, defined in Section 4.3, instead of $\frac{1}{2}$.

4.4.2. Mismatched Code Design

The encoder, e.g., a hardware manufacturer (for PUFs) or a trusted entity (for biometrics), models the source as visible or hidden, and a code is then constructed for the assumed model. Therefore, the assumed model determines the performance of the actual system. In the literature, the physical and biometric identifiers are modeled by the VSM; see, e.g., [54–57]. We first illustrate that treating the HSM as if it were a VSM might give pessimistic privacy-leakage rate results for $M_D \geq 1$, and over-optimistic secret-key and storage rate results for $M_D > 1$, which results in unnoticed secrecy leakage and reduced reliability.

Consider the crossover probabilities $p_{\mathrm{E}} \in \{0.03, 0.10\}$, which are realistic values for biometric [56] and physical identifiers [7]. We fix the crossover probability of $P_{Y_i|X}$ for $i = 1, 2, \ldots, M_D$ to $p_{\mathrm{D}} = 0.10$. For the supposed VSM, $\widetilde{X}^n$ is mistakenly considered to be a noise-free source, i.e., $p_{\mathrm{E}}^{VSM} = 0$, and the corresponding decoder-output channel $P^{VSM}_{Y_{1:M_D}|\widetilde{X}}$ consists of M_D independent BSCs each with crossover probability $p_{\mathrm{E}} * p_{\mathrm{D}}$ because $P_{Y|\widetilde{X}}$ is estimated from identifier measurements. However, the HSM considers an encoder measurement through a BSC with crossover probability p_{E} and M_D independent decoder measurements through BSCs, each with crossover probability p_D. Therefore, the HSM results in a conditional probability distribution $P_{Y_{1:M_D}|\widetilde{X}}$ that is different from the supposed VSM distribution $P^{VSM}_{Y_{1:M_D}|\widetilde{X}}$ for $M_D > 1$ and in a key-leakage-storage region $\mathcal{R}_1$ that is different from the supposed VSM region $\mathcal{R}_1^{VSM}$ for $M_D \geq 1$. We next illustrate the rate regions for different numbers of encoder and decoder measurements with p_{E} and p_{D} values given above.

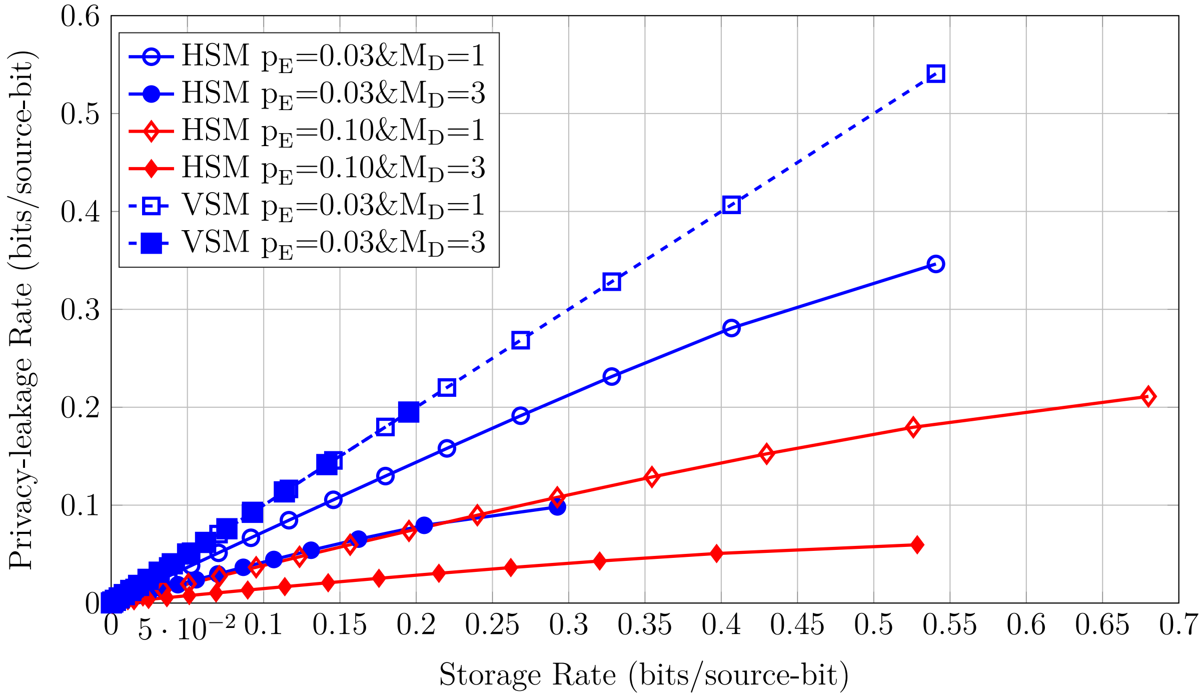

Figure 4.4.: Storage-leakage projection of the boundary triples for the GS model example with $p_{\mathrm{D}}=0.10$.

4.4.3. Single Encoder and Multiple Decoder Measurements

The projections of the boundary triples (R_s, R_ℓ, R_w) for the HSM and VSM onto the (R_w, R_ℓ)-plane and onto the (R_w, R_s)-plane are depicted in Figures 4.4 and 4.5, respectively, for different crossover probabilities at the encoder and different numbers of measurements at the decoder. Every marker on each curve corresponds to the evaluation of the rate-region boundaries for a fixed crossover probability $\tilde{x}$ given in (4.28), so Figures. 4.4 and 4.5 should be considered jointly for analysis. Recall from (4.7a) that any smaller R_s and greater R_ℓ and R_w than the boundary triples are achievable.

At the highest storage-leakage points (R_w^*, R_ℓ^*) in Figure 4.4, one achieves the maximum secret-key rates R_s^*, which corresponds to the highest points in Figure 4.5. Moreover, Figure 4.4 shows that if $M_D=1$, for the supposed VSM the privacy-leakage and storage rates are equal, and are also equal to the storage rate for the HSM, and the supposed VSM gives pessimistic privacy-leakage rate results. Figure 4.5 shows that increasing the number of decoder measurements increases the maximum secret-key rate R_s^* for the HSM and supposed VSM. The R_s^* of the HSM and supposed VSM are equal if $M_D=1$, but the supposed VSM gives over-optimistic secret-key and storage rate results for $M_D > 1$. These comparisons show that designing a code for the supposed VSM can lead to substantial secrecy leakage, which violates (4.3), and reliability reduction, which violates (4.2).

Consider, for instance, the parameters $\big(p_{\mathrm{E}}=0.03,\ p_{\mathrm{D}}=0.10,\ M_D=35\big)$. For the GS and

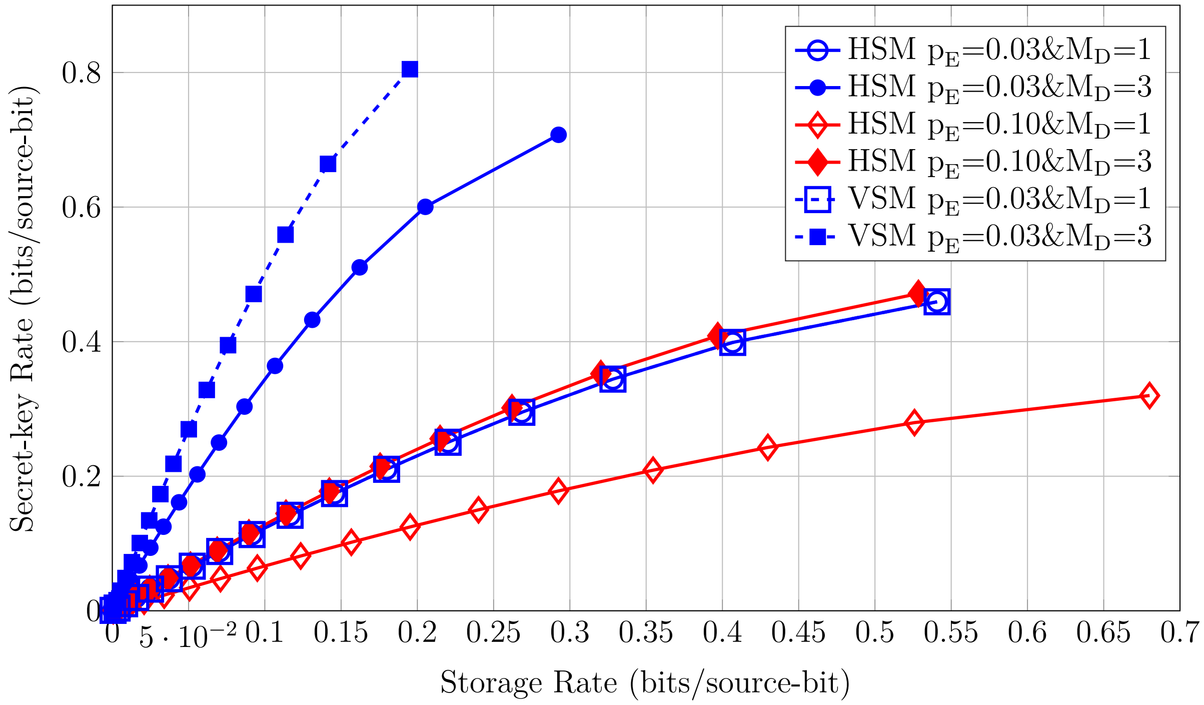

Figure 4.5.: Storage-key projection of the boundary triples for the GS model example with $p_\mathrm{D}=0.10$.

CS models with the HSM, R_ℓ^* is then approximately 3×10^{-9} bits/source-bit. The privacy-leakage rate can thus be made small for both models with multiple decoder measurements. R_w^* is approximately 0.194 bits/source-bit for the GS model, which is smaller than the 0.541 bits/source-bit obtained for $M_D=1$. We remark that less storage decreases the hardware cost. It is not possible for the CS model to give such a small storage rate with multiple decoder measurements since the key is independent of the hidden source. Independence of the key results in an additional storage rate, equal to R_s^* that is non-decreasing with respect to M_D, to reliably reconstruct the secret key at the decoder.

One may build intuition about the gains achieved by having multiple decoder measurements as follows. Since the decoder sees M_D noisy versions $Y_{1:M_D}$ of the same hidden source symbol X, it can "combine" the measurements to form a less noisy equivalent channel. This is entirely similar to using maximal ratio combining to obtain a sufficient statistic about a symbol that is transmitted several times over an AWGN channel. The resulting gain may thus be interpreted as a diversity gain.

Figures. 4.4 and 4.5 further show that increasing p_E decreases R_s^* and R_ℓ^*, and increases R_w^* for the HSM. For instance, consider the HSM, and fix $M_D = 1$ and the secret-key rate to its maximum $R_s^* = 0.320$ bits/source-bit achieved for $p_\mathrm{E} = 0.10$. The storage rate for $p_\mathrm{E} = 0.03$ is approximately 56.2% less than the storage rate for $p_\mathrm{E} = 0.10$ and their privacy-leakage rates are equal. Therefore, more reliable encoder-output channels $P_{\widetilde{X}|X}$, i.e., channels with smaller p_E values, achieve better storage rates. Similarly, we can show

Table 4.1.: Key-leakage-storage (R_s^*, R_ℓ^*, R_w^*) rate points for the GS model with the HSM for $p_{\mathrm{E}}=0.03$ and $p_{\mathrm{D}}=0.10$.

(M_E, M_D)	(R_s^*, R_ℓ^*, R_w^*) bits/source-bit
$(1,1)$	$(0.459, 0.346, 0.541)$
$(1,3)$	$(0.707, 0.098, 0.293)$
$(3,1)$	$(0.525, 0.458, 1.041)$
$(3,3)$	$(0.849, 0.134, 0.717)$

that more reliable decoder-output channels $P_{Y_{1:M_D}|X}$, i.e., channels with smaller p_{D} values, improve the rate triples (see also [12, Figure 5]) due to the independence assumption for encoder and decoder measurements.

Remark 4.4. One can alternatively consider encoder and decoder measurements through a broadcast channel. An unreliable channel at the encoder might be desirable for this case if the decoder-output channel is unreliable, since such correlations might allow less storage and privacy-leakage, and greater secret-key rates.

4.4.4. Multiple Encoder and Decoder Measurements

Consider the general case with $M_E \geq 1$ measurements $\widetilde{X}^n_{1:M_E} = [\widetilde{X}_1\widetilde{X}_2 \dots \widetilde{X}_{M_E}]^n$ of the hidden source X^n at the encoder for the GS model with the HSM. Suppose each encoder-output channel $P_{\widetilde{X}_i|X}$ for $i=1,2,\dots,M_E$ is an independent BSC with crossover probability p_{E}. The maximum secret-key rate R_s^* is achieved by choosing $U=\widetilde{X}_{1:M_E}$ for $\mathcal{R}_1$. We list the (R_s^*, R_ℓ^*, R_w^*) points in Table 4.1 for different numbers of encoder and decoder measurements with $p_{\mathrm{E}}=0.03$ and $p_{\mathrm{D}}=0.10$. Table 4.1 shows that the storage rates for multiple encoder measurements can be greater than 1 bit/source-bit, which cannot be the case for a single encoder measurement. Increasing the number M_E of encoder measurements to increase the secret-key rate, as listed in Table 4.1, can therefore come at a large cost of storage and can increase the privacy-leakage rate.

5

Optimal Code Constructions

Consider the two-terminal key agreement problem defined in Chapter 4 when the identifier outputs during enrollment are noiseless (visible). In this chapter, we propose two optimal linear code constructions based on Wyner-Ziv (WZ) coding. The first construction uses random linear codes and achieves all points of the key-leakage-storage regions of the GS and CS models. The second construction uses nested polar codes for vector quantization during enrollment and error correction during reconstruction. Simulations show that the nested polar codes achieve privacy-leakage and storage rates that improve on existing code designs. One proposed code achieves a rate tuple that cannot be achieved by existing methods. We also show how to extend these results to the hidden source model defined in Chapter 4. The results of this chapter are submitted for publication in [14], where the polar code design tools of Onurcan İşcan were used.

5.1. Motivation

Several practical code constructions for key agreement with identifiers have been proposed in the literature. For instance, the COFE and the FCS both require an error-correction code to satisfy the constraints of, respectively, the key generation (GS model) and key embedding (CS model) problems. Similarly, a polar code construction is proposed in [97] for the GS model. We show that these constructions are suboptimal in terms of the privacy-leakage and storage rates.

The binary Golay code is used in [56] as a vector quantizer (VQ) in combination with Slepian-Wolf (SW) codes [98] to illustrate that the key vs. storage (or key vs. leakage) rate ratio can be increased via quantization. This observation motivates the use of a VQ to improve the performance of previous constructions. In this work, we apply VQ by using WZ coding [99] to decrease storage rates, as suggested in [100, Remark 4.5].

The WZ-coding construction turns out to be optimal, which is not coincidental. For instance, the bounds on the storage rate of the GS model and on the WZ rate (storage rate) have the same mutual information terms optimized over the same conditional probability distribution. This similarity suggests an *equivalence* that is closely related to *formula duality* defined, e.g., in [101]. In fact, the optimal random code construction, encoding, and decoding operations are identical for both problems. We therefore call the GS model and WZ problem *functionally equivalent*. Such a strong connection suggests that there might exist constructive methods that are optimal for both problems for all measurement channels, which is closely related to *operational duality*; see [101].

5.1.1. Summary of Contributions

We propose code constructions for the key agreement model defined in Chapter 4 and illustrate that they are asymptotically optimal and improve on all existing methods. A summary of the main contributions is as follows.

- ▷ The GS and WZ problems are shown to be functionally equivalent, in the sense that the constraints of both problems are satisfied simultaneously by using the same random code construction.

- ▷ We describe two WZ-coding constructions for BSSs and binary symmetric channels (BSCs). Such sources and channels are often used for physical identifiers such as RO PUFs [7] and SRAM PUFs [50]. The first WZ-coding construction is based on [102] and achieves all points of the key-leakage-storage regions of the GS and CS models. The second construction uses nested polar codes.

- ▷ We design and simulate our polar codes for standard parameters for SRAM PUFs under ideal environmental conditions, and for RO PUFS under varying environmental conditions. The target block error probability is $P_B = 10^{-6}$ and the target secret-key size is 128 bits. One of the codes achieves key-leakage-storage rates that cannot be achieved by existing methods.

- ▷ In Appendix B.1, we prove that there are random binning and random coding based approaches that achieve all points of the key-leakage-storage regions of the GS and CS models and that result in strong secrecy.

- ▷ In Appendix B.2, we consider a hidden identifier source whose noisy measurements via BSCs are observed at the encoder and decoder. The first WZ-coding construction is shown to be optimal also for such identifiers.

5.1.2. Organization

This chapter is organized as follows. In Sections 5.2.1 and 5.2.2, we briefly review the GS and CS models, describe the WZ problem, and give their rate regions. In Section 5.2.3, we show that there is a random code construction that satisfies the constraints of the WZ problem and the GS model simultaneously to motivate using a WZ-coding construction for key generation and embedding. We show that existing methods are suboptimal even after applying improvements described in Section 5.3. Section 5.4 describes a random linear code construction based on WZ-coding. Section 5.5 describes a nested polar code design for the GS model and illustrates that it improves on existing code designs.

5.2. Problem Formulations

5.2.1. Generated-secret (GS) and Chosen-secret (CS) Models

Consider again the GS model in Figure 4.1, where a secret key is generated from a biometric or physical source. During enrollment, the encoder observes an i.i.d. noiseless sequence $\widetilde{X}^n = X^n$, generated by the visible source according to some P_X, and computes a secret key S and public helper data W as $(S,W) = \mathsf{Enc}(X^n)$. During reconstruction, the decoder observes a noisy source measurement Y^n of the visible source X^n through a memoryless channel $P_{Y|X}$ together with the helper data W. The decoder estimates the secret key as $\widehat{S} = \mathsf{Dec}(Y^n, W)$. Similarly, Figure 4.2 shows the CS model, where a secret key S that is independent of (X^n, Y^n) is embedded into the helper data as $W = \mathsf{Enc}(X^n, S)$. The decoder for the CS model estimates the secret key as $\widehat{S} = \mathsf{Dec}(Y^n, W)$. The source, measurement, secret key, and storage alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{S}$, and $\mathcal{W}$ are finite sets.

Definition 5.1. A key-leakage-storage tuple (R_s, R_ℓ, R_w) is *achievable* for GS and CS models with a visible source if, given any $\epsilon > 0$, there is some $n \geq 1$, an encoder, and a decoder such that $R_s = \frac{\log|\mathcal{S}|}{n}$ and (4.2)-(4.6) are satisfied. The *key-leakage-storage* regions $\mathcal{R}_1'$ and $\mathcal{R}_2'$ for, respectively, the GS and CS models with a visible source are the closures of the sets of achievable tuples for the corresponding models.

Theorem 5.1. The key-leakage-storage regions for the GS and CS models with a visible source, respectively, are

$$\begin{aligned}\mathcal{R}_1' = \bigcup_{P_{U|X}} \Big\{ & (R_s, R_\ell, R_w) : \\ & 0 \leq R_s \leq I(U;Y), \\ & R_\ell \geq I(U;X) - I(U;Y), \\ & R_w \geq I(U;X) - I(U;Y) \;\text{ for} \\ & P_{UXY} = P_{U|X} P_X P_{Y|X} \Big\},\end{aligned} \tag{5.1}$$

$$\begin{aligned}\mathcal{R}_2' = \bigcup_{P_{U|X}} \Big\{ & (R_s, R_\ell, R_w) : \\ & 0 \le R_s \le I(U;Y), \\ & R_\ell \ge I(U;X) - I(U;Y), \\ & R_w \ge I(U;X) \ \text{for} \\ & P_{UXY} = P_{U|X} P_X P_{Y|X} \Big\}. \end{aligned} \tag{5.2}$$

These regions are convex sets. The alphabet $\mathcal{U}$ of the auxiliary random variable U can be limited to have size $|\mathcal{U}| \le |\mathcal{X}| + 1$ for both regions $\mathcal{R}_1'$ and $\mathcal{R}_2'$.

Remark 5.1. The proof of Theorem 5.1 follows from the regions $\mathcal{R}_1$ and $\mathcal{R}_2$ given, respectively, in Theorems 4.1 and 4.2 by choosing $\widetilde{X} = X$; see Appendix B.1 for alternative proofs.

5.2.2. Wyner-Ziv (WZ) Problem

Consider two dependent random variables X and Y with joint distribution P_{XY}. Figure 5.1 depicts the WZ problem. The source, side information, and message alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{W}$ are finite sets. An encoder that observes X^n generates the message $W \in [1, 2^{nR_w}]$. The decoder observes Y^n and W and puts out a quantized version $\widehat{X}^n$ of X^n. Define the average distortion between X^n and the reconstructed sequence $\widehat{X}^n$ as

$$\frac{1}{n}\sum_{i=1}^{n} E[d(X_i, \widehat{X}_i(Y^n, W))] \tag{5.3}$$

where $d(x, \hat{x})$ is a distortion function and $\widehat{X}_i(y^n, w)$ is a reconstruction function. For simplicity, assume that $d(x, \hat{x})$ is bounded.

Definition 5.2. A WZ rate-distortion pair (R_w, D) is *achievable* for a distortion measure $d(x, \hat{x})$ if, given any $\epsilon > 0$, there is some $n \ge 1$, an encoder, and a decoder that satisfy the inequalities (4.6) and

$$\frac{1}{n}\sum_{i=1}^{n} E[d(X_i, \widehat{X}_i(Y^n, W))] \le D + \epsilon. \tag{5.4}$$

The WZ rate-distortion region $\mathcal{R}_{\mathrm{WZ}}$ is the closure of the set of achievable rate-distortion pairs. ◊

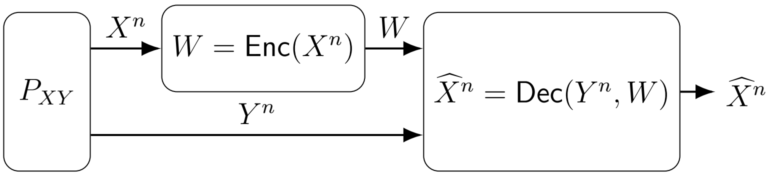

Figure 5.1.: The WZ problem.

Theorem 5.2 ([99])**.** The WZ rate-distortion region is

$$\begin{aligned}\mathcal{R}_{\text{WZ}} = \bigcup_{P_{U|X}} \bigcup_{\widehat{X}(Y,U)} \Big\{ &(R_w, D) : \\ &R_w \geq I(U;X) - I(U;Y), \\ &D \geq E[d(X, \widehat{X}(Y,U))] \;\text{ for} \\ &P_{UXY} = P_{U|X}P_{XY} \Big\}\end{aligned} \tag{5.5}$$

where $\widehat{X}(Y,U)$ is a reconstruction function used at the decoder. One can limit the alphabet $\mathcal{U}$ of the auxiliary random variable U to have size $|\mathcal{U}| \leq |\mathcal{X}| + 1$. The region $\mathcal{R}_{\text{WZ}}$ is convex.

5.2.3. Functional Equivalence

The duality of two problems is sometimes useful because it can help to find optimal code constructions for otherwise difficult-looking problems. Similar to duality, we call the problems given in Definitions 5.1 and 5.2 *functionally equivalent* because the optimal random code constructions for the GS model and WZ problem are the same. More precisely, we say that the problems are functionally equivalent for some specified (R_s, R_ℓ, R_w, D) if there is a random code construction that satisfies (4.2)-(4.6) and (5.4) simultaneously. Functional duality is closely related to functional equivalence, but we do not exchange the encoders and decoders for the latter, unlike for the functional duality.

Theorem 5.3. The GS model with the probability distributions P_X and $P_{Y|X}$, and the WZ problem with the joint probability distribution $P_{XY} = P_X P_{Y|X}$ and a distortion function $d(x, \hat{x})$ are functionally equivalent.

Proof Sketch. Fix a $P_{U|X}$ and $\widehat{X}(y,u)$ such that $E[d(X, \hat{X}(Y,U))] \leq D + \epsilon$ for some distortion $D > 0$ and $\epsilon > 0$. Randomly and independently generate codewords $u^n(w,s)$, $w = 1, 2, \ldots, 2^{nR_w}$, $s = 1, 2, \ldots, 2^{nR_s}$ according to $\prod_{i=1}^n P_U(u_i)$, where
$P_U(u_i) = \sum_{x \in \mathcal{X}} P_{U|X}(u|x)P_X(x)$. These codewords define the random codebook

$$\mathcal{C} = \{U^n(w,s)\}_{(w,s)=(1,1)}^{(2^{nR_w}, 2^{nR_s})}. \tag{5.6}$$

Let $0 < \epsilon' < \epsilon$.

Encoding: Given x^n, the encoder looks for a codeword that is jointly typical with x^n, i.e., $(u^n(w,s),x^n)\in\mathcal{T}_{\epsilon'}^n(P_{UX})$. If there is one or more such codeword, the encoder chooses one of them and puts out (w,s). If there is no such codeword, set $w=s=1$. The encoder publicly stores w.

Decoding: The decoder puts out $\hat{s}$ if there is a unique key label $\hat{s}$ that satisfies the typicality check $(u^n(w,\hat{s}),y^n)\in\mathcal{T}_{\epsilon}^n(P_{UY})$; otherwise, it sets $\hat{s}=1$. The decoder then puts out $\widehat{X}(y_i,u_i(w,\hat{s}))=\hat{x}_i$ for all $i=1,2,\dots,n$.

Using covering and packing lemmas [103, Lemmas 3.3 and 3.1], there is a code that satisfies (4.2)-(4.6) and (5.4) if we consider large n and approximately $2^{n(I(U;X)-I(U;Y))}$ storage labels w and $2^{nI(U;Y)}$ key labels s. This code asymptotically achieves the key-leakage-storage tuple $(R_s,R_\ell,R_w)=(I(U;Y),I(U;X)-I(U;Y),I(U;X)-I(U;Y))$. Using the typical average lemma [103, Section 2.4], the rate-distortion (R_w,D) pair can be achieved as well. □

Note that by using the coding scheme defined in the proof of Theorem 5.3 and by taking the union of the achieved rate tuples over all $P_{U|X}$, one can achieve the key-leakage-storage region $\mathcal{R}_1'$. Achieving the region $\mathcal{R}_2'$ follows by adding a one-time pad step to the proof of the GS model [56]; see Appendix A.1.2 for similar steps. Similarly, by using the same coding scheme and by taking the union of the achieved tuples over all $P_{U|X}$ and all reconstruction functions $\widehat{X}(\cdot)$, one can achieve the rate-distortion region $\mathcal{R}_{\text{WZ}}$.

Motivated by Theorem 5.3, we show in Section 5.4 that a linear WZ-coding construction achieves all boundary points of the key-leakage-storage regions of the GS and CS models for uniform binary sources measured through a BSC.

5.3. Prior Art and Comparisons

There are several existing code constructions proposed for the GS and CS models. We here consider the three best methods: FCS for the CS model, and COFE and the polar code construction in [97] for the GS model.

During enrollment with the FCS, an encoder takes a uniformly distributed secret key S as input to generate a codeword C^n. The codeword and the binary source output X^n are summed modulo-2, and the sum is stored as the helper data W. During reconstruction, W and another binary sequence Y^n, correlated with X^n through, e.g., a BSC(p_A), are summed modulo-2 and this sum is used by a decoder to estimate S. Similar steps are applied in the COFE, except that the secret key is a hashed version of X^n. The FCS achieves the single optimal point in the key-leakage region with the maximum secret-key rate $R_s^*=I(X;Y)$; the privacy-leakage rate is $R_\ell^*=H(X|Y)$ [58]. Similarly, the COFE achieves the same boundary point in the key-leakage region. This is, however, the only boundary point of the key-leakage regions that these methods can achieve.

We can improve both methods by adding a VQ step: instead of X^n we use its quantized version X_q^n during enrollment. This asymptotically corresponds to summing the original helper data and an independent random variable $J^n\sim\text{Bern}^n(q)$ such that $W=X^n\oplus$

$C^n \oplus J^n$ is the new helper data so that we create a virtual channel $P_{Y|X\oplus J}$ and apply the FCS or COFE to this virtual channel. The modified FCS and COFE can achieve all points of the key-leakage region if we take a union of all rate pairs achieved over all $q \in [0, 0.5]$. However, the helper data has n bits for both methods, and the resulting storage rate of 1 bit/source-bit is not necessarily optimal.

The polar code construction in [97] requires less storage rate than the FCS and COFE. However, this approach improves only the storage rate and cannot achieve all points of the key-leakage-storage region. Furthermore, in [97] some code designs assume that there is a "private" key shared only between the encoder and decoder, which is not realistic since a private key requires hardware protection against invasive attacks. If such a protection is possible, then there is no need to use an on-demand key reconstruction method like a PUF.

The existing methods cannot, therefore, achieve all points of the key-leakage-storage region for a BSC, unlike the WZ-coding constructions we describe in Sections 5.4 and 5.5.

In previous works such as [60], only the secret-key rates of the proposed codes are compared because the sum of the secret-key and storage (or privacy-leakage) rates is one. This constraint means that increasing the key vs. storage (or key vs. leakage) rate ratio is equivalent to increasing the key rate. Instead, our code constructions are more flexible than the existing methods in terms of achievable rate tuples. We will use the key vs. storage rate ratio as a metric to control the storage and privacy leakage in our code designs.

5.4. First WZ-coding Construction

Consider the lossy source coding construction proposed in [102] that achieves the boundary points of the WZ rate-distortion region by using linear codes. We use this code construction to achieve the boundary points of $\mathcal{R}'_1$ and $\mathcal{R}'_2$ for a binary uniform identifier source P_X and a BSC $P_{Y|X}$ with crossover probability p_A (see Chapter 3 and [91] for algorithms to obtain approximately such outputs from correlated and biased identifier outputs). Figure 5.2 plots the proposed code construction for the GS model.

Code Construction: Choose uniformly at random full-rank parity-check matrices $\mathbf{H}_1$, $\mathbf{H}_2$, and $\mathbf{H}$ as

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{bmatrix} \tag{5.7}$$

where $\mathbf{H}_1$ with dimensions $m_1 \times n$ defines a binary $(n, n-m_1)$ linear code $\mathcal{C}_1$ and $\mathbf{H}_2$ with dimensions $m_2 \times n$ defines another binary $(n, n-m_2)$ linear code $\mathcal{C}_2$. The $(n, n-m_1-m_2)$ code $\mathcal{C}$ defined by $\mathbf{H}$ in (5.7) is thus a subcode of $\mathcal{C}_1$ such that $\mathcal{C}_1$ is partitioned into 2^{m_2}

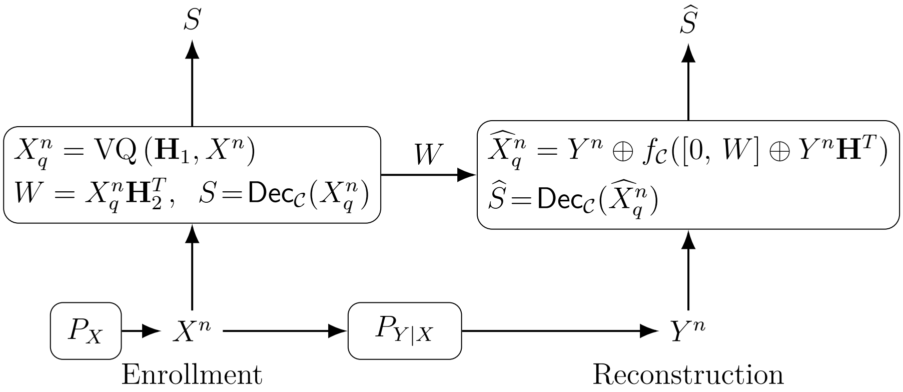
S
$\widehat{S}$
$X_q^n = \mathrm{VQ}(\mathbf{H}_1, X^n)$
$W = X_q^n\mathbf{H}_2^T, \ S = \mathsf{Dec}_{\mathcal{C}}(X_q^n)$
W
$\widehat{X}_q^n = Y^n \oplus f_{\mathcal{C}}([0, W] \oplus Y^n\mathbf{H}^T)$
$\widehat{S} = \mathsf{Dec}_{\mathcal{C}}(\widehat{X}_q^n)$
P_X
X^n
$P_{Y|X}$
Y^n
Enrollment
Reconstruction

Figure 5.2.: First WZ-coding construction for the GS model, where VQ$(\cdot)$ represents the vector quantization and $\mathsf{Dec}_{\mathcal{C}}(\cdot)$ represents the mapping between a codeword of the code $\mathcal{C}_1$ and a corresponding information sequence decoded by the code $\mathcal{C}$.

cosets of $\mathcal{C}$. For some distortion $q \in [0, 0.5]$ and $\delta > 0$, impose the conditions

$$\frac{m_1}{n} = H_b(q) - \delta \tag{5.8}$$

$$\frac{m_1 + m_2}{n} = H_b(q * p_A) + \delta. \tag{5.9}$$

Enrollment: The vector quantizer (VQ) in Figure 5.2 quantizes the source output X^n into the closest codeword X_q^n in $\mathcal{C}_1$ in Hamming metric. If there are two or more codewords with the minimum Hamming distance, the VQ chooses one of them uniformly at random. Define the error sequence

$$E_q^n = X^n \oplus X_q^n \tag{5.10}$$

which resembles an i.i.d. sequence $\sim \mathrm{Bern}^n(q)$ when $n \to \infty$ due to uniformity of X^n and the linearity of $\mathcal{C}_1$ [102].

In the GS model, we publicly store the side information

$$W = X_q^n\mathbf{H}_2^T \tag{5.11}$$

which corresponds to a coset of $\mathcal{C}$. We sum modulo-2 the bit sequence that is in the coset W and that has the minimum Hamming weight with X_q^n to obtain a codeword X_c^n of $\mathcal{C}$. Then, we assign the information sequence that is encoded to the codeword X_c^n as the secret key S such that $X_c^n = S\mathbf{G}$, where $\mathbf{G}$ is the generator matrix of $\mathcal{C}$. The secret key has length $n - m_1 - m_2$ bits. We denote this operation as $\mathsf{Dec}_{\mathcal{C}}(\cdot)$.

Consider the secrecy leakage for the GS model:

$$\begin{aligned}
&\lim_{n\to\infty}\frac{1}{n}I(S;W)=\lim_{n\to\infty}\frac{1}{n}\Big(H(S)+H(W)-H(W,S)\Big)\\
&\overset{(a)}{\le}\lim_{n\to\infty}\frac{1}{n}\Big(\log|\mathcal{S}|+\log|\mathcal{W}|-H(W,S,X_q^n)\Big)\\
&\le\lim_{n\to\infty}\frac{1}{n}\Big((n-m_1-m_2)+m_2-H(X_q^n)\Big)\\
&\overset{(b)}{\le}\lim_{n\to\infty}\frac{1}{n}\Big(n-m_1-(n-m_1-n\delta_n)\Big)=0
\end{aligned}\tag{5.12}$$

where (a) follows because (W,S) determines X_q^n and (b) follows with high probability for some δ_n such that $\lim_{n\to\infty}\delta_n=0$ due to the translation invariance of the linear code $\mathcal{C}_1$ and the uniformity of X^n (see also the discussions in [104, Section I]).

For the CS model, we have access to an embedded (chosen) secret key $S\in\mathcal{S}$ that is independent of (X^n,Y^n). Assume that a secret key $S'\in\mathcal{S}$ and helper data W' are generated by using the GS model. For the CS model, we store the helper data $W=[W',\,S'\oplus S]$. The secrecy leakage for the CS model is

$$\begin{aligned}
&\lim_{n\to\infty}\frac{1}{n}I(S;W)=\lim_{n\to\infty}\frac{1}{n}I(S;W',S'\oplus S)\\
&\overset{(a)}{=}\lim_{n\to\infty}\frac{1}{n}\Big(H(S)+H(W',S'\oplus S)-H(W',S')-H(S)\Big)\\
&\le\lim_{n\to\infty}\frac{1}{n}\Big(H(W')+H(S'\oplus S)-H(W',S')\Big)\\
&\overset{(b)}{\le}\lim_{n\to\infty}\frac{1}{n}\Big(\log|\mathcal{W}|+\log|\mathcal{S}|-H(W',S',X_q^n)\Big)\\
&\overset{(c)}{\le}\lim_{n\to\infty}\frac{1}{n}\Big(m_2+(n-m_1-m_2)-(n-m_1-n\delta_n)\Big)=0
\end{aligned}\tag{5.13}$$

where (a) follows because S is independent of (W',S'), (b) follows because $S'\in\mathcal{S}$ and (W',S') determines X_q^n, and (c) follows with high probability for some δ_n such that $\lim_{n\to\infty}\delta_n=0$ due to the translation invariance of the linear code $\mathcal{C}_1$ and uniformity of X^n.

Remark 5.2. We can improve the weak-secrecy results in (5.12) and (5.13) to strong-secrecy results, i.e., we replace (4.3) with

$$I(S;W)\le\epsilon \qquad\qquad \text{(strong secrecy)}\tag{5.14}$$

by applying information reconciliation and privacy amplification steps to multiple blocks of identifier outputs as described in [105], e.g., by using multiple PUFs for key agreement.

Remark 5.3. We prove in Appendix B.1 that there are code constructions that provide strong secrecy for general probability distributions P_{XY} without additional information reconciliation and privacy amplification steps.

Reconstruction: The noisy identifier output observed during reconstruction is $Y^n = X^n \oplus Z^n$, where Z^n is independent of X^n and $Z^n \sim \text{Bern}^n(p_A)$. The error sequence E_q^n and the noise sequence Z^n are independent. Furthermore, E_q^n asymptotically resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ when $n \to \infty$, as discussed above. Therefore, when $n \to \infty$, the sequence $E_q^n \oplus Z^n$, which corresponds to the noise sequence of the equivalent channel $P_{Y^n|X_q^n}$, is distributed according to $\text{Bern}^n(q * p_A)$ since the equivalent channel is a concatenation of two BSCs. One can thus reconstruct X_q^n with high probability when $n \to \infty$ by using the syndrome decoder $f_{\mathcal{C}}(\cdot)$ of the code $\mathcal{C}$ as follows

$$\begin{aligned}
\widehat{X_q^n} &= Y^n \oplus f_{\mathcal{C}}([0,\, W] \oplus Y^n\mathbf{H}^T)\\
&\overset{(a)}{=} Y^n \oplus f_{\mathcal{C}}(X_q^n\mathbf{H}^T \oplus Y^n\mathbf{H}^T)\\
&\overset{(b)}{=} (X_q^n \oplus E_q^n \oplus Z^n) \oplus f_{\mathcal{C}}((E_q^n \oplus Z^n)\mathbf{H}^T)\\
&\overset{(c)}{=} (X_q^n \oplus E_q^n \oplus Z^n) \oplus (E_q^n \oplus Z^n)\\
&= X_q^n
\end{aligned} \tag{5.15}$$

where (a) follows by (5.11) and because X_q^n is a codeword of $\mathcal{C}_1$, (b) follows by (5.10), and (c) follows with high probability because, asymptotically, $E_q^n \oplus Z^n \sim \text{Bern}^n(q*p_A)$ so that the syndrome decoder $f_{\mathcal{C}}(\cdot)$ determines the noise sequence $E_q^n \oplus Z^n$. This is because the constraint in (5.9) indicates that the code rate of $\mathcal{C}$ is below the capacity of the BSC$(q*p_A)$.

The secret-key is reconstructed in the GS model as

$$\widehat{S} = \mathsf{Dec}_{\mathcal{C}}(\widehat{X_q^n}) \tag{5.16}$$

and in the CS model as

$$\widehat{S} = \widehat{S'} \oplus (S' \oplus S) \tag{5.17}$$

both of which result in the same error probability.

5.4.1. Optimality of the Proposed Construction for the GS Model

Recall that $X^n \sim \text{Bern}^n(\frac{1}{2})$ and that the channel $P_{Y|X}$ is a BSC(p_A), where $p_A \in [0, 0.5]$. Using Mrs. Gerber's lemma, the key-leakage-storage region of the GS model is

$$\begin{aligned}
\mathcal{R}'_{1,\text{bin}} = \bigcup_{q\in[0,0.5]} \Big\{ &(R_s, R_\ell, R_w)\colon\\
&0 \le R_s \le 1 - H_b(q * p_A),\\
&R_\ell \ge H_b(q * p_A) - H_b(q),\\
&R_w \ge H_b(q * p_A) - H_b(q)\Big\}.
\end{aligned} \tag{5.18}$$

Theorem 5.4. The key-leakage-storage region $\mathcal{R}'_{1,\text{bin}}$ for the GS model is achieved by using the WZ-coding construction proposed above.

Proof. By (5.8) and (5.9), we have

$$\frac{\log|\mathcal{W}|}{n} = \frac{m_2}{n} = H_b(q * p_A) - H_b(q) + 2\delta \leq R_w + 2\delta \tag{5.19}$$

if $R_w \geq H_b(q * p_A) - H_b(q)$.

The secret key satisfies

$$\begin{aligned}\frac{H(S)}{n} &\geq \frac{n - m_1 - m_2}{n} - \delta = 1 - H_b(q * p_A) - 2\delta \\ &\geq R_s - 2\delta\end{aligned} \tag{5.20}$$

if $R_S \leq 1 - H_b(q * p_A)$. Furthermore, we have

$$\begin{aligned}\frac{I(X^n; W)}{n} &\overset{(a)}{=} \frac{H(W)}{n} \leq \frac{\log|\mathcal{W}|}{n} = \frac{m_2}{n} \\ &= H_b(q * p_A) - H_b(q) + 2\delta \leq R_\ell + 2\delta\end{aligned} \tag{5.21}$$

if $R_\ell \geq H_b(q * p_A) - H_b(q)$, where (a) follows because X^n determines W. □

5.4.2. Optimality of the Proposed Construction for the CS Model

The key-leakage-storage region of the CS model for a uniform binary source measured through a BSC(p_A) is

$$\begin{aligned}\mathcal{R}'_{2,\text{bin}} = \bigcup_{q\in[0,0.5]} \Big\{ &(R_s, R_\ell, R_w) : \\ &0 \leq R_s \leq 1 - H_b(q * p_A), \\ &R_\ell \geq H_b(q * p_A) - H_b(q), \\ &R_w \geq 1 - H_b(q) \Big\}.\end{aligned} \tag{5.22}$$

Theorem 5.5. The key-leakage-storage region $\mathcal{R}'_{2,\text{bin}}$ for the CS model is achieved by using the WZ-coding construction proposed above.

Proof. The storage rate for the CS model is the sum of the storage and secret-key rates of the GS model. By choosing achievable storage and key rates for the GS model, we can achieve for the CS model a storage rate of

$$R_w \geq 1 - H_b(q). \tag{5.23}$$

Since $H(S) = \log|\mathcal{S}|$, $S' \in \mathcal{S}$, and S is independent of (X^n, Y^n), the secret-key and privacy-leakage rates are the same as in the GS model, i.e., we have

$$R_s \leq 1 - H_b(q * p_A) \tag{5.24}$$

$$R_\ell \geq H_b(q * p_A) - H_b(q). \tag{5.25}$$

□

Remark 5.4. We show in Appendix B.2 that the above WZ-coding construction is optimal also for hidden sources, i.e., the encoder observes a noisy measurement of the source rather than the source itself.

5.5. Second WZ-coding Construction

Polar codes [106] have a low encoding/decoding complexity, asymptotic optimality for various problems, and good finite length performance if a list decoder is used. Furthermore, they have a structure that allows simple nested code design and they can be used for WZ coding [107].

Polar codes rely on the *channel polarization* phenomenon, where a channel is converted into polarized bit channels by a polar transform. This transform converts an input sequence U^n with frozen and unfrozen bits to a codeword of the same length n. A polar decoder processes a noisy observation of the codeword together with the frozen bits to estimate U^n.

Let $\mathcal{C}(n, \mathcal{F}, G^{|\mathcal{F}|})$ denote a polar code of length n, where $\mathcal{F}$ is the set of indices of the frozen bits and $G^{|\mathcal{F}|}$ is the sequence of frozen bits. In the following, we use the nested polar code construction proposed in [107].

5.5.1. Polar Code Construction for the GS Model

We use two polar codes $\mathcal{C}_1(n, \mathcal{F}_1, V)$ and $\mathcal{C}(n, \mathcal{F}, \overline{V})$ with $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_w$ and $\overline{V} = [V, W]$, where V has length m_1 and W has length m_2 such that m_1 and m_2 satisfy (5.8) and (5.9). The indices in $\mathcal{F}_1$ represent frozen channels with assigned values V for both codes and $\mathcal{C}$ has additional frozen channels with assigned values W denoted by $\mathcal{F}_w$, i.e., the codes are nested.

The code $\mathcal{C}_1$ serves as a VQ with a desired distortion q and the code $\mathcal{C}$ serves as the error-correction code for a BSC$(q * p_A)$. The idea is to obtain W during enrollment and store it as public helper data. For reconstruction, W is used by the decoder to estimate the secret key S of length $n - m_1 - m_2$. Figure 5.3 shows the block diagram of the proposed construction. In the following, suppose V is the all-zero vector so that no additional storage is necessary. This choice has no effect on the average distortion $E[q]$ between X^n and X_q^n defined below; see [107, Lemma 10].

Enrollment: The uniform binary sequence X^n generated by a PUF during enrollment is treated as the noisy observation of a BSC(q). X^n is quantized by a polar decoder of $\mathcal{C}_1$.

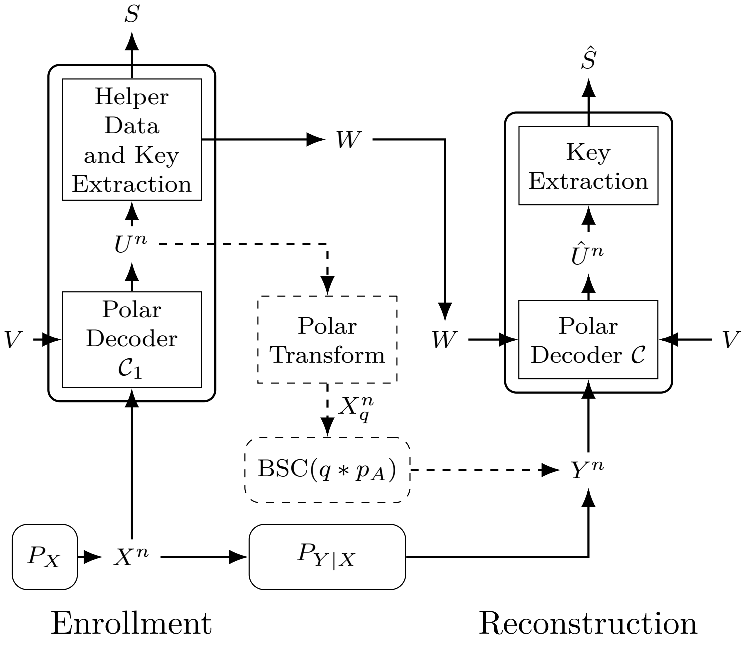

Figure 5.3.: Second WZ-coding construction for the GS model.

We extract from the decoder output U^n the bits at indices $\mathcal{F}_w$ and store them as the helper data W. The bits at the indices $i \in \{1, 2, \ldots, n\} \setminus \mathcal{F}$ are used as the secret key. Note that applying a polar transform to U^n generates X_q^n, which is a distorted version of X^n. The distortion between X^n and X_q^n is modeled as a BSC(q) because the error sequence $E_q^n = X^n \oplus X_q^n$ resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ when $n \to \infty$ [107, Lemma 11].

Reconstruction: During reconstruction, the polar decoder of $\mathcal{C}$ observes the binary sequence Y^n, which is a noisy measurement of X^n through a BSC(p_A). The frozen bits $\overline{V} = [V, W]$ at indices $\mathcal{F}$ are input to the polar decoder. The output $\widehat{U}^n$ of the polar decoder is the estimate of U^n and contains the estimate $\widehat{S}$ of the secret key at the unfrozen indices of $\mathcal{C}$, i.e., $i \in \{1, 2, \ldots, n\} \setminus \mathcal{F}$.

We next give a method to design practical nested polar codes for the GS model.

Construction of $\mathcal{C}$ and $\mathcal{C}_1$: Since $\mathcal{C} \subseteq \mathcal{C}_1$ are nested codes, they must be constructed jointly. $\mathcal{F}$ and $\mathcal{F}_1$ should be selected such that the reliability and security constraints are satisfied. For a given secret key size $n - m_1 - m_2$, block length n, crossover probability p_A, and target block-error probability $P_B = \Pr[S \neq \widehat{S}]$, we propose the following procedure.

1. Construct a polar code of rate $(n - m_1 - m_2)/n$ and use it as the code $\mathcal{C}$, i.e., define the set of frozen indices $\mathcal{F}$.

2. Evaluate the error correction performance of $\mathcal{C}$ with a decoder for a BSC over a range of crossover probabilities to obtain the crossover probability p_c, resulting in a target block-error probability of P_B. Using $p_c = E[q] * p_A$, we obtain the target distortion $E[q]$ averaged over a large number of realizations of X^n.

3. Find an $\mathcal{F}_1 \subset \mathcal{F}$ that results in an average distortion of $E[q]$ with a minimum possible amount of helper data. Use $\mathcal{F}_1$ as the frozen set of $\mathcal{C}_1$.

Step 1 is a conventional polar code design task and step 2 is applied by Monte-Carlo simulations. For step 3, we start with $\mathcal{F}_1^{'} = \mathcal{F}$ and compute the resulting average distortion $E[q']$ via Monte-Carlo simulations. If $E[q']$ is not less than $E[q]$, we remove elements from $\mathcal{F}_1^{'}$ according to the reliabilities of the polarized bit channels and repeat the procedure until we obtain the desired average distortion $E[q]$.

We remark that the distortion level introduced by the VQ is an additional degree of freedom in choosing the code design parameters. For instance, different values of P_B can be targeted with the same code by changing the distortion level. Alternatively, devices with different p_A values can be supported by using the same code. This additional degree of freedom makes the proposed code design suitable for a wide range of applications.

5.5.2. Proposed Codes for the GS Model

Consider, for instance, the GS model where S is used in the advanced encryption standard (AES) with length 128, i.e., $\log|\mathcal{S}| = n - m_1 - m_2 = 128$ bits. If we use PUFs in a field-programmable gate array (FPGA) as the randomness source, we must satisfy a block-error probability P_B of at most 10^{-6} [108]. Consider a BSC $P_{Y|X}$ with crossover probability $p_A = 0.15$, which is a common value for SRAM PUFs under ideal environmental conditions [50] and for RO PUFs under varying environmental conditions [8]. We design nested polar codes for these parameters to illustrate that we can achieve better key-leakage-storage rate tuples than previously proposed codes.

Code 1: Consider $n = 1024$ and recall that $n - m_1 - m_2 = 128$, $P_B = 10^{-6}$, and $p_A = 0.15$. Polar successive cancellation list (SCL) decoders with list size 8 are used as the VQ and channel decoder. We first design the code $\mathcal{C}$ of rate 128/1024 and evaluate its performance with the SCL decoder for a BSC with a range of crossover probabilities, as shown in Figure 5.4. We observe a block-error probability of 10^{-6} at a crossover probability of $p_c = 0.1819$. Since $p_A = 0.15$, this corresponds to an average distortion of $E[q] = 0.0456$, i.e., $E[q] * p_A = 0.1819$.

Figure 5.5 shows the average distortion $E[q]$ with respect to $n - m_1 = n - |\mathcal{F}_1|$, obtained by Monte-Carlo simulations. We observe from Figure 5.5 that the target average distortion is obtained at $n - m_1 = 778$ bits. Thus, $m_2 = 650$ bits of helper data suffice to obtain a block-error probability of $P_B = 10^{-6}$ to reconstruct an $n - m_1 - m_2 = 128$-bit secret key.

We observe that the parameter p_c is less than $p_A = 0.15$ when we apply the procedure in Section 5.5.1 to $n = 512$ with the same P_B. Therefore, it is not possible to construct a code with our procedure for $n \leq 512$ since $q * p_A$ is an increasing function of q for any $q \in [0, 0.5]$. Such a code construction for $n = 512$ might be possible if one improves the code design and the decoder.

Code 2: Consider the same parameters as in code 1, except $n = 2048$. We apply the same steps as above and plot the performance of an SCL decoder for a BSC with a range of crossover probabilities in Figure 5.4. A crossover probability of $p_c = 0.2682$ is required to

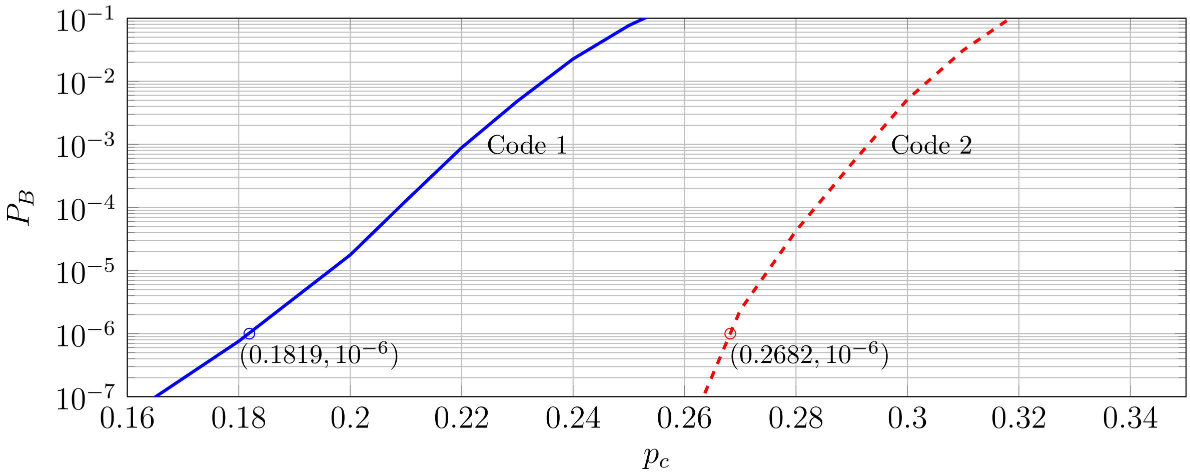

Figure 5.4.: Block error probability of $\mathcal{C}$ over a BSC(p_c) with an SCL decoder (list size 8) for codes 1 (blue) and 2 (red) of length 1024 and 2048, respectively.

obtain a block-error probability of 10^{-6}, which gives an average distortion of $E[q] = 0.1689$. As depicted in Figure 5.5, we achieve the target average distortion with $n - m_1 = 739$ bits so that helper data of length 611 bits is required to satisfy $P_B = 10^{-6}$ for a secret key of length 128 bits.

Remark 5.5. Our assumptions on the channel statistics are not necessarily satisfied for the model depicted in Figure 5.3 for finite n since, e.g., the channel $P_{X^n|X_q^n}$ is not $\sim \text{Bern}^n(q)$. However, our code designs and analysis are based on simulations made over a large number of possible inputs at fixed lengths, which allows us to give reliability guarantees to a set of input realizations. The results of such guarantees are given below.

The error probability P_B is calculated as an average over a large number of PUF realizations, i.e., over a large number of PUF devices with the same circuit design. To satisfy the block-error probability requirement for each PUF realization, one could consider using the maximum distortion instead of $E[q]$ as a metric in step 3 in Section 5.5.1. This would increase the amount of helper data. We can guarantee a block-error probability of at most 10^{-6} for 99.99% of all realizations x^n of X^n by adding 32 bits to the helper data for code 1 and 33 bits for code 2. The numbers of extra helper data bits required are small since the variance of the distortion q over all PUF realizations is small for the blocklengths considered. For comparisons, we use the helper data sizes required to guarantee $P_B = 10^{-6}$ for 99.99% of all PUF realizations.

5.5.3. Code Comparisons and Discussions

We show in Figure 5.6 the storage-key (R_w, R_s) projection of the boundary points of the region $\mathcal{R}'_{1,\text{bin}}$ for $p_A = 0.15$. Furthermore, we show the point with the maximum secret-key rate R_s^* and the minimum storage rate R_w^* to achieve R_s^*. For the FCS and COFE, we

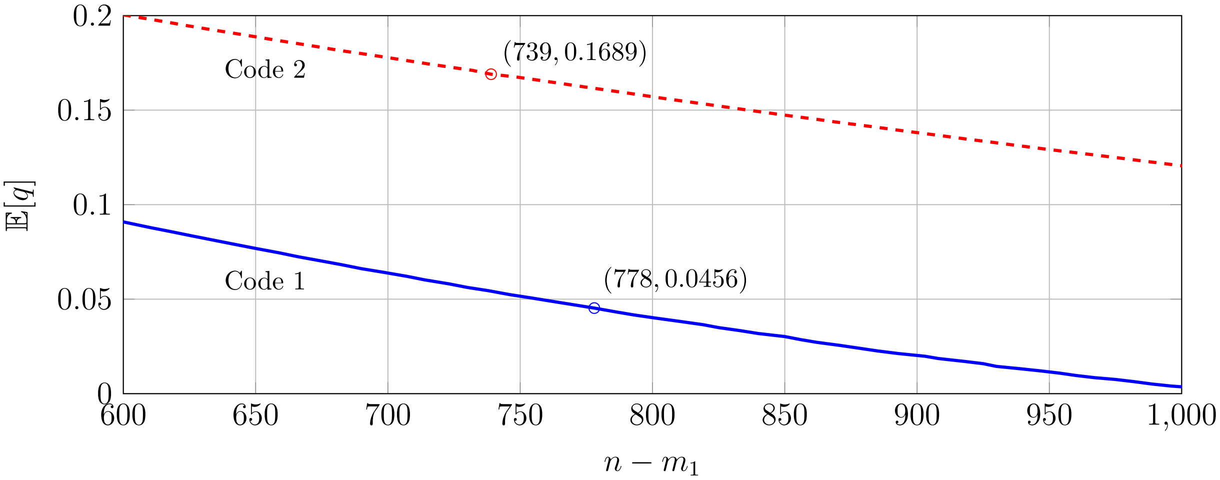

Figure 5.5.: Average distortion $E[q]$ with respect to $n - m_1$ with an SCL decoder (list size 8) for codes 1 (blue) and 2 (red) of length 1024 and 2048, respectively.

use the random coding union bound [80, Thm. 16] to confirm that the plotted rate pairs are achievable for a secret-key length of 128 bits, an error probability of $P_B = 10^{-6}$, and blocklengths of $n = 1024$ and $n = 2048$. These rate pairs are shown in Figure 5.6 to the right of the dashed line representing $R_w + R_s = 1$. Similarly, the rate pairs achieved by the previous polar code design, and codes 1 and 2 are shown in Figure 5.6.

The storage rates of the FCS and COFE are 1 bit/source-bit, which is suboptimal as discussed in Section 5.3. The previous polar code construction in [97] achieves a rate point with $R_s + R_w = 1$ bit/source-bit, which is expected since this is a SW-coding construction. The polar code construction improves on the rate pairs achieved by the FCS and COFE in terms of the key vs. storage ratio.

We achieve the key-leakage-storage rates of approximately $(0.125, 0.666, 0.666)$ bits/source-bit by code 1 and $(0.063, 0.315, 0.315)$ bits/source-bit by code 2, projections of which are depicted in Figure 5.6. These rates are significantly better than the best rate tuple $(0.125, 0.875, 0.875)$ bits/source-bit in the literature, i.e., the previous polar code construction in [97], for the same parameters and without any private key assumption. We increase the key vs. storage rate ratio R_s/R_w from approximately 0.188 for code 1 to 0.199 for code 2, which suggests to increase the blocklength to obtain better ratios. Furthermore, code 2 achieves privacy-leakage and storage rates that cannot be achieved by existing methods without applying *time sharing* (see, e.g., [103, Section 4.4]). This is because code 2 achieves privacy-leakage and storage rates of 0.315 bits/source-bit that are significantly less than the minimum privacy-leakage and storage rates $R_w^* = R_\ell^* = H_b(p_A) \approxeq 0.610$ bits/source-bit that can be asymptotically achieved by existing methods at the maximum secret-key rate $R_s^* \approxeq 0.390$ bits/source-bit.

We use the sphere packing bound [109, Eq. (5.8.19)] to upper bound the key vs. storage rate ratio that can be achieved by SW-coding constructions for the maximum secret-key rate point. Consider $p_A = 0.15$, $n = 1024$, and $P_B = 10^{-6}$, for which the sphere packing

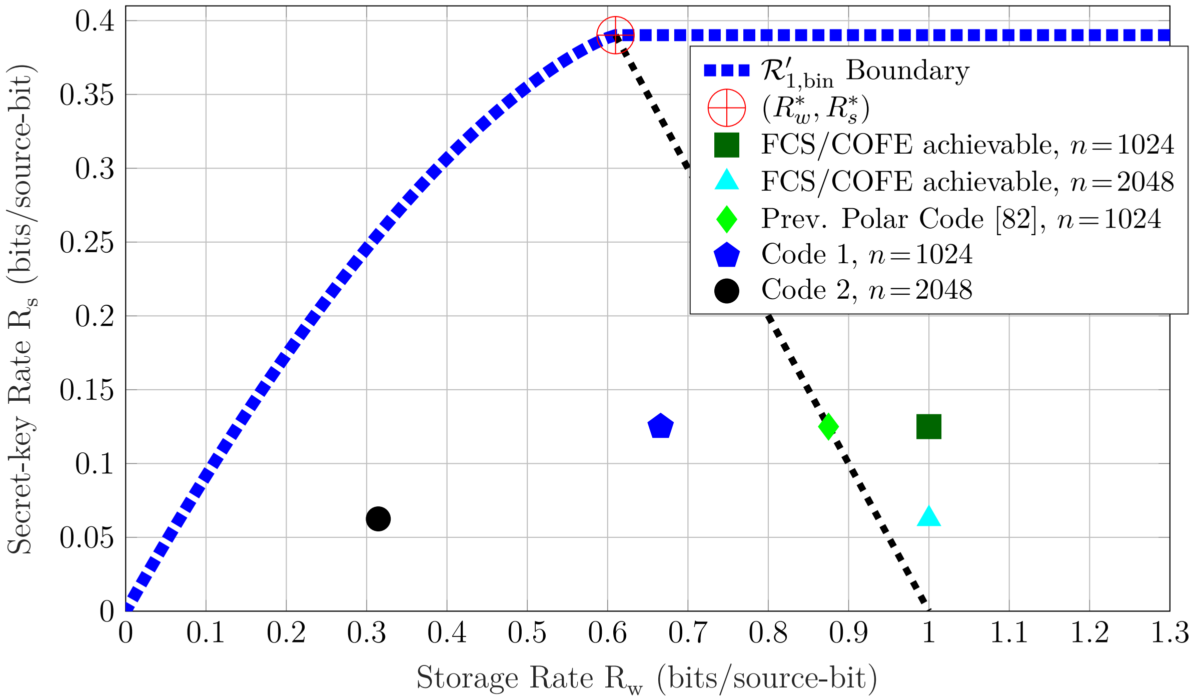

Figure 5.6.: Storage-key rates for the GS model with $p_A = 0.15$. The (R_w^*, R_s^*) point is the best possible point achieved by SW-coding constructions, which lies on the dashed line representing $R_w + R_s = H(X)$. The block error probability satisfies $P_B \leq 10^{-6}$ and the key length is 128 bits for all code points.

bound requires that the rate of the code $\mathcal{C}$ satisfies $R_\mathcal{C} \leq 0.273$. If we assume that the key rate is given by its maximal value $R_s = R_\mathcal{C}$ and the storage rate is given by its minimal value $R_w = 1 - R_\mathcal{C}$, then we arrive at $R_s/R_w \leq 0.375$. A similar calculation for $n = 2048$ yields $R_s/R_w \leq 0.437$. These results indicate that there are still gaps between the maximum key vs. storage rate ratios achieved by WZ-coding constructions, which might achieve higher ratios than SW-coding constructions, and the ratios achieved by codes 1 and 2. The gaps can be reduced by using, e.g., larger list sizes at the decoder, which is not desired for IoT applications where hardware complexity is constrained.

6

Controllable Measurements for Private Authentication

We consider here another extension of the key agreement problem. Suppose the key agreed by using an identifier is used for authentication under a privacy constraint on the source sequence. Furthermore, we allow the identifier measurements during authentication (or reconstruction) to be controllable via a cost-constrained "action" sequence. We characterize the optimal trade-off among the secret-key rate, privacy-leakage rate, storage rate, and action cost for two problems, where noisy (hidden) measurements of the source are enrolled to generate (the GS model) or embed (the CS model) secret keys. The results are relevant for several user-authentication scenarios, including physical and biometric authentication with multiple measurements as discussed in Chapter 4. Our results include as special cases results for secret-key generation and embedding with action-dependent side information without any privacy constraint on the enrolled source sequence. The results of this chapter were published in [15].

6.1. Motivation

There is a fundamental trade-off between privacy and security of an authentication system. An information theoretic formulation provides a framework to capture such a trade-off [56], [57]. Moreover, the identifier measurements can be controlled or tuned with an additional cost. In this chapter, we study the optimal trade-offs among the key, privacy-leakage and storage rates, and expected action cost for discrete memoryless sources and measurement channels. The availability of post-processing methods in Chapter 3 to obtain memoryless channels and sources from biometric or physical identifiers allows us to avoid considering channels with memory and correlated sources; see [110] and [111].

The use of authentication for access control is an effective method to ensure information security. Unlike concealing the data to be transmitted as in a wiretap channel [40], authentication of a user by using a secret requires correlated random variables in order to agree on a sequence [62, 63]. Most important physical identifiers used for device authentication are PUFs. Similarly, body traits like irises and fingerprints are used as biometric randomness sources for authentication. There are code constructions in the biometric secrecy literature proposed for authentication, e.g., the fuzzy vault scheme [112], FCS, and COFE. We show in Chapter 5 that the FCS and COFE are suboptimal for a simplified version of the private authentication problem we consider in this chapter. Accordingly, we are interested in understanding the fundamental limits of private authentication by studying optimal code constructions and their rate regions.

The use of biometric or physical identifiers that involve different *forms of measurements*, e.g., the use of multiple measurements or variations in the quality of the measurement process [90], [113], motivates us to consider a new private authentication model. In this model, the measurement process is represented by a cost-constrained action-dependent (adaptive) side information acquisition, where an action sequence determines the measurement channel. A high action cost can, for instance, represent the use of a high quality measurement device.

Similar to the previous chapters, we first consider the GS model, where the key is generated from the identifier outputs. The secret key reconstructed at the decoder is generally stored in a trusted database. It can be practical to embed a uniformly-distributed and independently chosen key into the encoder rather than generating it from identifier outputs. We therefore also consider this practical model, defined in the previous chapters as the CS model, with additional cost-constrained actions and show how much more storage it requires as compared to the GS model.

Biometric and physical identifier outputs are noisy by nature. For instance, a cut in the palm corresponds to noise on the palmprint. Similar to multiple-antenna systems, multiple identifier measurements at the decoder can significantly improve the rate regions as compared to a single measurement. Suppose we have multiple measurements also at the encoder, as in Chapter 4 where the source is hidden. It is shown in Chapter 4 that if a noiseless (visible) source is mistakenly assumed for system design, there can be unnoticed secrecy leakage and the reliability at the decoder can decrease. Motivated by these results, we study hidden identifiers with cost-constrained actions for the GS and CS models.

6.1.1. Summary of Contributions and Organization

Chapter 4 illustrated that rate regions can grow by using multiple noisy measurements of a hidden source. An attacker, this time with access to a correlated identifier measurement, tries to deceive the authentication in [114]. We combine and extend the models in Chapter 4 and [114], and consider a cost-constrained action sequence that controls the source measurements during authentication to reconstruct the secret key. Multiple identifier measurements both at the encoder and decoder are allowed by considering a hidden identifier.

The main contributions of this chapter are as follows.

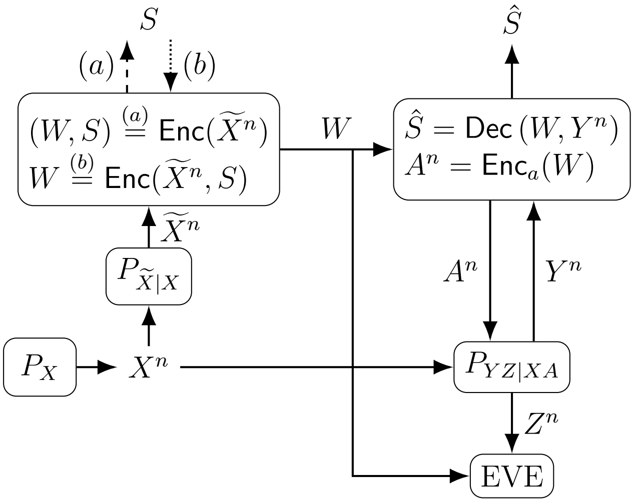
S
(a)
(b)
$\hat{S}$
$(W,S) \overset{(a)}{=} \mathsf{Enc}(\widetilde{X}^n)$
$W \overset{(b)}{=} \mathsf{Enc}(\widetilde{X}^n, S)$
W
$\hat{S} = \mathsf{Dec}\,(W, Y^n)$
$A^n = \mathsf{Enc}_a(W)$
$\widetilde{X}^n$
$P_{\widetilde{X}|X}$
A^n
Y^n
P_X
X^n
$P_{YZ|XA}$
Z^n
EVE

Figure 6.1.: A hidden source: (a) represents the GS model and (b) represents the CS model. The decoder and EVE measurements can be performed after observing the action sequence.

- ▷ The key-leakage-storage-cost region for secret-key generation from an identifier with a cost-constrained action at the decoder and a noisy (hidden) output at the encoder is given. This rate region recovers several results in the literature including the key-leakage rate regions for a visible source in [56] and [57].

- ▷ We extend the region for key generation to a chosen secret-key embedding scenario (CS model), where the source output is used to conceal the chosen key.

- ▷ As an example, we use realistic channel and source model parameters to generate secret keys from PUFs and illustrate the key-leakage-storage-cost trade-off for a binary physical identifier with cost-constrained actions during authentication.

This chapter is organized as follows. In Section 6.2, we describe the models considered in this chapter. We develop the key-leakage-storage-cost regions for the two problems. An achievable key-leakage-storage-cost region for a binary source with cost-constrained measurements during authentication is illustrated in Section 6.4.

6.2. Problem Formulations

6.2.1. Hidden Source, GS Model

Consider the system model in Figure 6.1(a), where a key is generated from a hidden source. The decoder observes cost-constrained controllable source measurements Y^n during authentication, whereas the encoder observes uncontrollable noisy measurements $\widetilde{X}^n$ of the hidden source outputs X^n through a memoryless channel $P_{\widetilde{X}|X}$. The source alphabet $\mathcal{X}$, the measurement alphabets $\widetilde{\mathcal{X}}, \mathcal{Y}, \mathcal{Z}$, and the action alphabet $\mathcal{A}$ are finite sets.

Definition 6.1. A $\big(|\mathcal{W}|, |\mathcal{S}|, n\big)$-code $\mathcal{C}_n$ for private authentication with a key generated from noisy measurements of a hidden source, controllable decoder measurements, and noisy encoder measurements consists of

- an encoder $\mathsf{Enc}(\cdot) : \widetilde{\mathcal{X}}^n \to \mathcal{W} \times \mathcal{S}$,
- an action encoder $\mathsf{Enc}_a(\cdot) : \mathcal{W} \to \mathcal{A}^n$,
- a decoder $\mathsf{Dec}(\cdot) : \mathcal{W} \times \mathcal{Y}^n \to \mathcal{S}$. ◊

Definition 6.2. A key-leakage-storage-cost tuple (R_s, R_ℓ, R_w, C) is said to be *achievable* for a hidden source with the GS model if, for any $\delta > 0$, there is some $n \geq 1$ and a $\big(|\mathcal{W}|, |\mathcal{S}|, n\big)$-code for which $R_s = \dfrac{\log|\mathcal{S}|}{n}$ such that

$$\Pr[\hat{S} \neq S] \leq \delta, \qquad (reliability) \qquad (6.1)$$

$$\frac{1}{n} I(S; W, Z^n) \leq \delta \qquad (weak\ secrecy) \qquad (6.2)$$

$$\frac{1}{n} H(S) \geq R_s - \delta \qquad (uniformity) \qquad (6.3)$$

$$\frac{1}{n} I(X^n; W, Z^n) \leq R_\ell + \delta \qquad (privacy) \qquad (6.4)$$

$$\frac{1}{n} \log\big|\mathcal{W}\big| \leq R_w + \delta \qquad (storage) \qquad (6.5)$$

$$\mathbb{E}[\Gamma(A^n)] \leq C + \delta \qquad (cost) \qquad (6.6)$$

where we have $(W, S) = \mathsf{Enc}(\widetilde{X}^n)$, $A^n = \mathsf{Enc}_a(W)$, $\hat{S} = \mathsf{Dec}(W, Y^n)$, and $\Gamma(A^n) = \frac{1}{n}\sum_{i=1}^n \Gamma(A_i)$ for some cost function $\Gamma(\cdot)$. The *key-leakage-storage-cost* region $\mathcal{R}_{hgs}$ is the closure of all achievable tuples. ◊

6.2.2. Hidden Source, CS Model

Consider the problem of binding a chosen secret key to a hidden biometric or physical identifier, as shown in Figure 6.1(*b*). The decoder observes cost-constrained controllable source measurements during authentication, whereas the encoder observes uncontrollable noisy source outputs.

Definition 6.3. A $\big(|\mathcal{W}|, |\mathcal{S}|, n\big)$-code $\mathcal{C}_n$ for private authentication with an embedded secret key concealed by noisy measurements of a hidden source, controllable decoder measurements, and noisy encoder measurements consists of

- an encoder $\mathsf{Enc}(\cdot) : \widetilde{\mathcal{X}}^n \times \mathcal{S} \to \mathcal{W}$,

- an action encoder $\mathsf{Enc}_a(\cdot) : \mathcal{W} \to \mathcal{A}^n$,
- a decoder $\mathsf{Dec}(\cdot) : \mathcal{W} \times \mathcal{Y}^n \to \mathcal{S}$. ◊

Definition 6.4. A key-leakage-storage-cost tuple (R_s, R_ℓ, R_w, C) is said to be *achievable* for a hidden source with the CS model if, for any $\delta > 0$, there is some $n \geq 1$ and a $\Big(|\mathcal{W}|, |\mathcal{S}|, n\Big)$-code for which $R_s = \dfrac{\log |\mathcal{S}|}{n}$ such that (6.1)-(6.6) are satisfied, where we have $W = \mathsf{Enc}(\widetilde{X}^n, S)$, $A^n = \mathsf{Enc}_a(W)$, $\hat{S} = \mathsf{Dec}(W, Y^n)$, and $\Gamma(A^n) = \frac{1}{n}\sum_{i=1}^n \Gamma(A_i)$ for some cost function $\Gamma(\cdot)$. The *key-leakage-storage-cost* region $\mathcal{R}_{hcs}$ is the closure of all achievable tuples. ◊

Remark 6.1. The encoder- and decoder-measurement channels in Figure 6.1 are modeled as two separate channels, i.e., $\widetilde{X} - (A, X) - (Y, Z)$ forms a Markov chain. This is the case if, e.g., there is a considerable amount of time between the encoder and decoder measurements of a palmprint so that any cuts on it during enrollment and authentication are independent.

6.3. Key-leakage-storage-cost Regions

We are interested in characterizing the optimal trade-off among the secret-key rate, privacy-leakage rate, storage rate, and expected action cost. We next give the rate regions.

Theorem 6.1 (*Hidden Source, GS*)**.** For given P_X, $P_{\widetilde{X}|X}$, and $P_{YZ|XA}$, the key-leakage-storage-cost region $\mathcal{R}_{hgs}$ is given as the set of all tuples (R_s, R_ℓ, R_w, C) satisfying

$$R_s \leq I(V;Y|A,U) - I(V;Z|A,U) \tag{6.7}$$
$$R_\ell \geq I(X;A,V,Y) + I(X;Z|A,U) - I(X;Y|A,U) \tag{6.8}$$
$$R_w \geq I(\widetilde{X};A) + I(V;\widetilde{X}|A,Y) \tag{6.9}$$

for some $P_X P_{\widetilde{X}|X} P_{A|\widetilde{X}} P_{YZ|XA} P_{V|\widetilde{X}A} P_{U|V}$ such that $\mathbb{E}[\Gamma(A)] \leq C$ with $|\mathcal{U}| \leq |\widetilde{\mathcal{X}}||\mathcal{A}| + 3$ and $|\mathcal{V}| \leq (|\widetilde{\mathcal{X}}||\mathcal{A}| + 3)(|\widetilde{\mathcal{X}}||\mathcal{A}| + 2)$.

Proof. Achievability is based on a random coding scheme that consists of superposition of a rate-distortion code for communicating the action sequence and a two-layered binning for secret-key generation. The converse is based on standard properties of entropy functions. The proof is given in Appendices C.4.1-C.4.2. □

Remark 6.2. We can write the bounds in (6.7) and (6.8), respectively, as

$$R_s \leq I(V;Y|A) - I(V;Z|A) - (I(U;Y|A) - I(U;Z|A)) \tag{6.10}$$
$$R_\ell \geq I(X;A,V,Y) + I(X;Z|A) - I(X;Y|A) + (I(U;Y|A) - I(U;Z|A)). \tag{6.11}$$

To maximize the secret-key rate and minimize the privacy-leakage rate simultaneously, we should minimize the term $I(U;Y|A)-I(U;Z|A)$. This term is minimized by choosing an auxiliary random variable $U=U^*$ such that $I(U;Y|A)-I(U;Z|A)\leq 0$ and if we choose U as a constant, we have $I(U;Y|A)-I(U;Z|A)=0$; see [115]. This suggests that the eavesdropper can decode the codeword U^n in the first layer given Z^n and A. Therefore, we can view the two-layer binning approach used in the achievability proofs as having a *public* codeword U^n and a *private* codeword V^n; see [85, Remark 1] for a similar conclusion.

Theorem 6.2 (*Hidden Source, CS*)**.** For given P_X, $P_{\widetilde{X}|X}$, and $P_{YZ|XA}$, the key-leakage-storage-cost region $\mathcal{R}_{hcs}$ is given as the set of all tuples (R_s,R_ℓ,R_w,C) satisfying

$$R_s\leq I(V;Y|A,U)-I(V;Z|A,U) \tag{6.12}$$

$$R_\ell\geq I(X;A,V,Y)+I(X;Z|A,U)-I(X;Y|A,U) \tag{6.13}$$

$$R_w\geq I(\widetilde{X};A,V)-I(U;Y|A)-I(V;Z|A,U) \tag{6.14}$$

for some $P_XP_{\widetilde{X}|X}P_{A|\widetilde{X}}P_{YZ|XA}P_{V|\widetilde{X}A}P_{U|V}$ such that $\mathbb{E}[\Gamma(A)]\leq C$ with $|\mathcal{U}|\leq|\widetilde{\mathcal{X}}||\mathcal{A}|+3$ and $|\mathcal{V}|\leq(|\widetilde{\mathcal{X}}||\mathcal{A}|+3)(|\widetilde{\mathcal{X}}||\mathcal{A}|+2)$.

Proof. We use the proof of achievability for Theorem 6.1 and add a one-time padding step. The secret-key and privacy-leakage rate bounds have the same expressions, and the new storage rate bound is the sum of the secret-key and storage rate bounds of the GS model for a hidden source. The proof details are given in Appendices C.5.1-C.5.2. □

Remark 6.3. Theorems 6.1 and 6.2 can be seen as extensions of the results in Chapter 4 with the addition of cost-constrained action-dependent measurements at the decoder and correlated side information at the eavesdropper.

Remark 6.4. If $\widetilde{X}^n=X^n$ in Figure 6.1, we recover the noiseless (visible) source models. By choosing $\widetilde{X}=X$ in Theorems 6.1 and 6.2, we have the rate regions $\mathcal{R}_{gs}$ and $\mathcal{R}_{cs}$, respectively, for the GS and CS models for a visible source; see Appendices C.2.1-C.3.2 for proofs. This means that Theorems 6.1 and 6.2 also include, as special cases, results for one-round secret-key generation and embedding, respectively, that extend the results in [62], where there is no privacy constraint on the source sequence. Moreover, Theorem 6.1 can also be seen as an extension of the result in [114] because we additionally capture cost-constrained action-dependent decoder measurements.

6.3.1. Rate Region Comparisons and Discussions

Consider the key-leakage-storage region given in [114, Theorem 2] for the GS model and a visible source, which is a simplified version of the model we consider. We compare this region with the rate region $\mathcal{R}_{gs}$ to illustrate the effects of the cost-constrained action sequence. In particular, we observe that the action A appears in $\mathcal{R}_{gs}$ as a conditioning random variable in each mutual information term in [114, Theorem 2], the new storage and privacy-leakage rate limits are increased by the rate-distortion coding amount of $I(X;A)$

and the probability distribution of A is restricted due to an expected cost constraint. Therefore, the cost-constrained action sequence A^n brings the possibility of enlarging the rate region, which recovers the rate region in [114, Theorem 2] by choosing a constant action with fixed cost. The action sequence A^n has similar effects on other rate regions.

The rate region $\mathcal{R}_{gs}$ differs from the rate region $\mathcal{R}_{cs}$ only in the bound for the storage rate. The bound in (6.14) with $\widetilde{X} = X$ can be written as $I(X;A) + I(X;V|A,Y) + I(V;Y|A,U) - I(V;Z|A,U)$ (cf. (6.9) with $\widetilde{X} = X$), revealing an additional rate that is $I(V;Y|A,U) - I(V;Z|A,U)$ (cf. (6.12)) needed to convey the chosen secret to the decoder. Suppose $(R_s, R_\ell, R_w, C) \in \mathcal{R}_{cs}$ for given P_X and $P_{YZ|XA}$. Therefore, there exist A, U, and V such that $U - V - (X,A) - (Y,Z)$ forms a Markov chain. It is straightforward to show that $(R_s, R_\ell, R_w - R_s, C) \in \mathcal{R}_{gs}$ for the same P_X and $P_{YZ|XA}$. Similar conclusions follow also for a hidden source.

The bounds for the secret-key and privacy-leakage rates of visible and hidden sources have the same expressions, i.e., for the GS model in $\mathcal{R}_{gs}$ and $\mathcal{R}_{hgs}$, and for the CS model in $\mathcal{R}_{cs}$ and $\mathcal{R}_{hcs}$, respectively. However, the storage-rate limits of different source models are different. Moreover, the Markov chain constraints and the cardinality bounds on the auxiliary random variables are different for the visible and hidden source models. The rate regions therefore differ significantly, which can result in unnoticed secrecy leakages and reliability reductions if the wrong source model is used for the system design; see Chapter 4.

6.4. Example

We want to illustrate an achievable rate region for cost-constrained action-dependent secret-key generation from a visible source. We first define the scenario where a PUF in an IoT device is used for key generation so that only a mobile device with access to the key can control the IoT device. We then derive an achievable rate region for this scenario by proving specific convexity results. These convexity results significantly simplify the encoder design by decreasing the cardinality of the auxiliary random variable.

Suppose X is binary and uniformly distributed, the channel $P_{A|X}$ is a BSC with crossover probability α, and the channels $P_{Y|AX}(.|a,.)$ are BSCs with crossover probabilities p_a for $a=0,1$. Suppose the eavesdropper has degraded side information and the channel $P_{Z|Y}$ is a BSC with crossover probability p. In practice, quantized fine variations of RO outputs follow these source and channel models. The effects of voltage and temperature variations can also be suppressed by a legitimate user by applying additional post-processing steps to the RO outputs [8]. Classic crossover probabilities for the BSCs $P_{Y|AX}(\cdot|a,\cdot)$ under ideal environmental conditions are $p_a = 0.03$ and 0.05 for $a = 0,1$, where, e.g., $a = 0$ corresponds to the case that X^n is sent through the $P_{Y|AX}(\cdot|0,\cdot)$ channel.

Suppose the attacker has access to a noisy version Z^n of the RO outputs X^n disturbed by environmental variations in addition to noise. A classic crossover probability for one of the BSCs $P_{Z|AX}(\cdot|a,\cdot)$ is $p' = 0.15$ [8]. We thus choose $p_0 = 0.03$, $p_1 = 0.05$, $p = 0.1277$ so that $p * p_0 = 0.15 = p'$ and $p * p_1 = 0.1649$. We also consider the cost of $\Gamma(0) = 0.5$ units for

$a=0$ and $\Gamma(1)=0.3$ units for $a=1$ since obtaining a more reliable channel requires more post-processing steps, which results in higher cost.

Suppose the crossover probability α of the BSC $P_{A|X}$ is 0.2. It is therefore more likely that the input $X=1$ is sent through a channel that is stochastically degraded with respect to the channel through which the input $X=0$ is sent because $p_1>p_0$. This is the case if, e.g., a one-bit quantizer is applied to RO outputs, where the bit 0 is extracted if the output value is less than the mean over all ROs and the bit 1 otherwise. RO output values decrease with increasing temperature. Therefore, the error probability of the channel through which the input bit 0 is sent is smaller than the bit 1 is sent if the ambient temperature is greater than the temperature assumed for the system design.

We now illustrate an achievable rate region for the RO PUF problem defined above by proving convexity of a function used for entropy calculations. Choose the auxiliary random variable V as (A,X) for simplicity so that the rate region of interest for the GS model with a visible source is

$$\begin{aligned}
&R_s \leq I(X;Y|A,U) - I(X;Z|A,U)\\
&R_\ell \geq H(X) - (I(X;Y|A,U) - I(X;Z|A,U))\\
&R_w \geq I(X;A) + H(X|A,Y)
\end{aligned}\tag{6.15}$$

such that $U-(A,X)-(Y,Z)$ forms a Markov chain and $C\geq \mathbb{E}[\Gamma(A)]$. The optimization problem of achieving boundary points in (6.15) is equivalent to

$$\min_{P_{AX|U}} H(Z|A,U) \text{ for a fixed } H(Y|A,U)=\eta \tag{6.16}$$

for all $0\leq\eta\leq 1$, which is a similar problem to MGL. Denote the conditional probabilities $P_{AX|U}(a,x|i)=\hat{x}_{i,ax}$ and the probabilities $P_U(i)=u_i$ for $i=1,2,\dots,|\mathcal{U}|$. To preserve P_{AX}, we obtain the constraints

$$\sum_{i=1}^{|\mathcal{U}|} u_i\hat{x}_{i,01} = \sum_{i=1}^{|\mathcal{U}|} u_i\hat{x}_{i,10} = \frac{\alpha}{2}, \tag{6.17}$$

$$\sum_{i=1}^{|\mathcal{U}|} u_i\hat{x}_{i,00} = \sum_{i=1}^{|\mathcal{U}|} u_i\hat{x}_{i,11} = \frac{1-\alpha}{2}. \tag{6.18}$$

To fix $H(Y|A,U)$, it therefore suffices for all $i=1,2,\dots,|\mathcal{U}|$ to consider

$$\hat{x}_{i,01} = \frac{1}{2}-\hat{x}_{i,00}, \qquad \hat{x}_{i,10} = \frac{1}{2}-\hat{x}_{i,11}. \tag{6.19}$$

Define the functions

$$f(\hat{x}_{i,00},\hat{x}_{i,11}) = \left[H_b\left(p_0 * \frac{2\hat{x}_{i,00}}{1-2(\hat{x}_{i,11}-\hat{x}_{i,00})}\right) + H_b\left(p_1 * \frac{2\hat{x}_{i,11}}{1-2(\hat{x}_{i,00}-\hat{x}_{i,11})}\right)\right], \tag{6.20}$$

$$g(\hat{x}_{i,00},\hat{x}_{i,11})=\left[H_b\left(p*p_0*\frac{2\hat{x}_{i,00}}{1-2(\hat{x}_{i,11}-\hat{x}_{i,00})}\right)+H_b\left(p*p_1*\frac{2\hat{x}_{i,11}}{1-2(\hat{x}_{i,00}-\hat{x}_{i,11})}\right)\right]. \quad (6.21)$$

Using (6.19), (6.20), and (6.21), we obtain

$$H(Y|A,U)=\sum_{i=1}^{|\mathcal{U}|}u_i\,\frac{1}{2}\,f(\hat{x}_{i,00},\hat{x}_{i,11}), \quad (6.22)$$

$$H(Z|A,U)=\sum_{i=1}^{|\mathcal{U}|}u_i\,\frac{1}{2}\,g(\hat{x}_{i,00},\hat{x}_{i,11}). \quad (6.23)$$

Define an inverse function $f^{-1}(\nu)=(\bar{x},\bar{x})$ for all $\nu\in[H_b(p_0)+H_b(p_1),\ 2]$ and $\bar{x}\in[0,\ 0.5]$ so that it suffices to replace $f(\hat{x}_{i,00},\hat{x}_{i,11})$ with

$$\bar{f}(\bar{x})=f\left(\frac{\bar{x}}{2},\frac{\bar{x}}{2}\right) \quad (6.24)$$

to obtain any value in (6.22). Similarly, it suffices to replace $g(\hat{x}_{i,00},\hat{x}_{i,11})$ with

$$\bar{g}(\bar{x})=g\left(\frac{\bar{x}}{2},\frac{\bar{x}}{2}\right) \quad (6.25)$$

to obtain any value in (6.23).

Note that this choice of functions is not necessarily optimal to achieve the boundary points of the rate region in (6.15), which is discussed below.

Lemma 6.3. There is a unique $\bar{x}$ in the interval [0, 0.5] for which $H(Y|A,U)=\frac{1}{2}\bar{f}(\bar{x})$.

Proof. The function $\bar{f}(\bar{x})$ is strictly increasing from $H_b(p_0)+H_b(p_1)$ to 2 in the interval $[0,0.5)$ and we have $H_b(p_0)+H_b(p_1)\leq 2H(Y|A,U)\leq 2H(Y)\leq 2$. □

Lemma 6.4. Define $\tilde{p}'=\min\{p',1-p'\}$ for some $0\leq p'\leq 1$. If $\tilde{p}*\tilde{p}_0\geq\tilde{p}_1$ and $\tilde{p}*\tilde{p}_1\geq\tilde{p}_0$, the function $\bar{g}(f^{-1}(\nu))$ is convex in ν for $\nu\in[H_b(p_0)+H_b(p_1),\ 2]$.

Proof. The functions $\bar{f}(\bar{x})$ and $\bar{g}(\bar{x})$ are symmetric with respect to $p_0=\frac{1}{2}$, $p_1=\frac{1}{2}$, and $p=\frac{1}{2}$. It thus suffices to prove the convexity for $0\leq\tilde{p}_0,\tilde{p}_1,\tilde{p}\leq 0.5$. $\bar{g}(f^{-1}(\nu))$ is convex in ν if

$$\frac{\partial^2}{\partial\nu^2}\left(\bar{g}(f^{-1}(\nu))\right)=\frac{1}{\bar{f}'(\bar{x})}\frac{\partial}{\partial\bar{x}}\left(\frac{\bar{g}'(\bar{x})}{\bar{f}'(\bar{x})}\right)\geq 0 \quad (6.26)$$

for all $\bar{x}\in[0,0.5]$, as proved in Appendix A.4. Note that $H_b(\cdot)$ is an increasing function for $\bar{x}\in[0,0.5]$, so $\bar{f}'(\bar{x})\geq 0$ for all $\bar{x}\in[0,0.5]$. It thus suffices to show that $\frac{\partial}{\partial\bar{x}}\left(\frac{\bar{g}'(\bar{x})}{\bar{f}'(\bar{x})}\right)\geq 0$, i.e.,

$$\bar{g}''(\bar{x})\bar{f}'(\bar{x})-\bar{f}''(\bar{x})\bar{g}'(\bar{x})\geq 0. \quad (6.27)$$

The functions $\bar{f}(\bar{x})$ and $\bar{g}(\bar{x})$ consist of two parts as $H_b(\tilde{p}_a * \bar{x})$ and $H_b(\tilde{p} * \tilde{p}_a * \bar{x})$, respectively, for $a=0,1$. It is shown in [79] that $H_b(\tilde{p} * H_b^{-1}(\nu))$ is convex in $0 \leq \nu \leq 1$ for any $\tilde{p} \in [0,\ 0.5]$, so the terms in (6.27) that consist of the multiplications of the parts with the same $\tilde{p}_a$ are positive valued. It thus suffices to find a set of $\tilde{p}_0$ and $\tilde{p}_1$ values that satisfies

$$\frac{1-2(\tilde{p}*\tilde{p}_a)}{(\tilde{p}*\tilde{p}_a*\bar{x})(1-\tilde{p}*\tilde{p}_a*\bar{x})\log\left(\frac{1-\tilde{p}*\tilde{p}_a*\bar{x}}{\tilde{p}*\tilde{p}_a*\bar{x}}\right)} \leq \frac{1-2\tilde{p}_b}{(\tilde{p}_b*\bar{x})(1-\tilde{p}_b*\bar{x})\log\left(\frac{1-\tilde{p}_b*\bar{x}}{\tilde{p}_b*\bar{x}}\right)} \tag{6.28}$$

where $b=1-a$ for $a=0,1$. Define the function

$$l(\hat{p}) = \frac{1-2\hat{p}}{(\hat{p}*\bar{x})(1-\hat{p}*\bar{x})\log\left(\frac{1-\hat{p}*\bar{x}}{\hat{p}*\bar{x}}\right)} \tag{6.29}$$

for $0 \leq \hat{p}, \bar{x} \leq 0.5$. It is straightforward to prove that $l(\hat{p})$ is a decreasing function by showing that $l(\hat{p})$ is convex and $l'(0.5)=0$. The inequality in (6.28) is thus satisfied if $\tilde{p}*\tilde{p}_a \geq \tilde{p}_b$ for $a=0,1$. This proves the convexity. □

We use the convexity property for channels satisfying the assumptions in Lemma 6.4 to give an achievable lower bound for $H(Z|A,U)$ when $H(Y|A,U)$ is fixed.

Lemma 6.5. Suppose $\bar{g}(f^{-1}(\nu))$ is convex in ν. With the assumptions given above, we have

$$H(Z|A,U) \geq \frac{1}{2}\,\bar{g}(f^{-1}(2H(Y|A,U))). \tag{6.30}$$

Proof. Using Jensen's inequality, we have

$$H(Z|A,U) = \sum_{i=1}^{|\mathcal{U}|} u_i\,\frac{1}{2}\,\bar{g}(f^{-1}(\bar{f}(\bar{x}_i))) \geq \frac{1}{2}\,\bar{g}\Big(f^{-1}\Big(\sum_{i=1}^{|\mathcal{U}|} u_i \bar{f}(\bar{x}_i)\Big)\Big) = \frac{1}{2}\,\bar{g}\Big(f^{-1}(2H(Y|A,U))\Big). \square$$

Lemma 6.6. Consider the problem setup defined above and the region in (6.15). The BSCs $P_{AX|U}(a,\cdot|\cdot)$ with the same crossover probability $\bar{x} \in [0,\ 0.5]$ when $P_{A|U}(\cdot|\cdot) = \frac{1}{2}$ achieve the region that satisfies equality in (6.30) if $\tilde{p} * \tilde{p}_0 \geq \tilde{p}_1$ and $\tilde{p} * \tilde{p}_1 \geq \tilde{p}_0$ are satisfied.

Proof. Consider the bounds in (6.15) that depend on U. Using Lemma 6.5, we obtain

$$R_s \leq H(Y|A,U) - H(Y|A,X) - \frac{1}{2}\,\bar{g}\Big(f^{-1}(2H(Y|A,U))\Big) + H(Z|A,X), \tag{6.31}$$

$$R_\ell \geq H(X) - H(Y|A,U) + H(Y|A,X) + \frac{1}{2}\,\bar{g}\Big(f^{-1}(2H(Y|A,U))\Big) - H(Z|A,X) \tag{6.32}$$

where we use Lemma 6.4 for the convexity requirement and Lemma 6.3 to show that the inverse function $f^{-1}(\cdot)$ is a bijective mapping. Equalities in (6.31) and (6.32) are achieved by BSCs $P_{AX|U}(a,\cdot|\cdot)$ with the same crossover probability $0\leq\bar{x}\leq 0.5$, defined in Lemma 6.3, for $a=0,1$ when $P_{AX|U}(\cdot,0|\cdot)+P_{AX|U}(\cdot,1|\cdot)=P_{A|U}(\cdot|\cdot)=\frac{1}{2}$, which follows by (6.19). □

Remark 6.5. One can show that the lower bound in (6.30) can be improved for $H(Z|A,U)$ given in (6.23) that is a function of a general $g(\hat{x}_{i,00},\hat{x}_{i,11})$, although this lower bound is tight for the function $\bar{g}(\bar{x})$.

For the RO PUF problem with the source and channel parameters given above, we obtain that $R_w\geq 0.4731$ bits/source-bit and $C\geq 0.4$ units since P_{AXYZ} is fixed. The boundary points for R_s and R_ℓ sum up to $H(X)=1$ bits, which determines the trade-off between the secret-key and privacy-leakage rates for this example. The maximum R_s achievable by using Lemma 6.6 is $R_s^*=0.3876$ bits/source-bit, achieved with $R_\ell\geq 0.6124$ bits/source-bit.

7 Other Contributions

This chapter briefly summarizes two of our other contributions. The first contribution considers multiple enrollments of the same PUF. The second contribution considers conditions for the secret-key rate to be positive when multiple rounds of communication between legitimate parties are allowed. We have more contributions that are in progress and not summarized in the thesis, e.g., key agreement with broadcast channel measurements of hidden biometric or physical identifiers, and the operational equivalence of the WZ problem and the GS model. The results of this chapter were published in [16], where the proof of the general two-enrollment case is from Frans Willems and Lieneke Kusters, and in [17], where the majority of the work was done by Amin Gohari. The extension of [17] will be submitted for publication in [18].

7.1. Key Agreement with Multiple PUF Enrollments

In the key agreement literature, usually only a single enrollment is performed for each PUF. We are interested in cases where multiple enrollments are used to generate multiple keys. This may happen in practice when the used key is replaced with a new key.

Suppose multiple keys and helper messages are generated from different measurements of the same PUF. For example, Figure 7.1 shows an enrollment model, where during each enrollment $j \in \{1,2\}$, a key S_j and corresponding helper message W_j are generated from a noisy observation $\widetilde{X}_j$ of the hidden PUF source X^n. The helper message W_j should have enough information so that a decoder can reconstruct the secret S_j when another noisy observation Y_j^n of the hidden source X^n is available. An eavesdropper, given all helper messages (W_1, W_2); however, should learn only a negligible amount of information about any of the secrets. We assume that the same encoding $\mathsf{Enc}(\cdot)$ and decoding $\mathsf{Dec}(\cdot)$ algorithms are used for each enrollment.

Definition 7.1. A secret-key rate tuple $(R_1, R_2, \dots, R_{|\mathcal{J}|})$ is said to be *achievable* for a

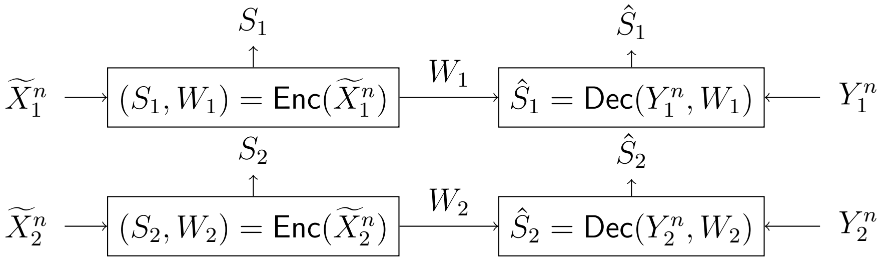
S_1
$\hat{S}_1$
$\widetilde{X}_1^n$
$(S_1, W_1) = \mathsf{Enc}(\widetilde{X}_1^n)$
W_1
$\hat{S}_1 = \mathsf{Dec}(Y_1^n, W_1)$
Y_1^n
S_2
$\hat{S}_2$
$\widetilde{X}_2^n$
$(S_2, W_2) = \mathsf{Enc}(\widetilde{X}_2^n)$
W_2
$\hat{S}_2 = \mathsf{Dec}(Y_2^n, W_2)$
Y_2^n

Figure 7.1.: Two-enrollment model.

multiple-enrollment model if, given any $\delta > 0$, there is some $n \geq 1$, an encoder, and a decoder such that for $\forall j \in \mathcal{J}$, we have $R_j = \dfrac{\log|\mathcal{S}_j|}{n}$ and

$$\Pr[\hat{S}_j \neq S_j] \leq \delta \qquad (\textit{reliability}) \tag{7.1}$$

$$\frac{1}{n} I(S_j; \{W_j : j \in \mathcal{J}\}) \leq \delta \qquad (\textit{weak secrecy}) \tag{7.2}$$

$$\frac{1}{n} H(S_j) \geq R_j - \delta \qquad (\textit{uniformity}) \tag{7.3}$$

where we have $(W_j, S_j) = \mathsf{Enc}(\widetilde{X}_j^n)$ and $\hat{S}_j = \mathsf{Dec}(W_j, Y_j^n)$. The secret-key rate region $\mathcal{R}$ is the closure of all achievable secret-key rate tuples. ◊

7.1.1. Two-Enrollment Model with the Same Measurement Channels

We first assume that every noisy measurement of the hidden source is made through the same memoryless channel for the two-enrollment model, i.e., we assume

$$P_{\widetilde{X}_1|X}(z|x) = P_{\widetilde{X}_2|X}(z|x) = P_{Y_1|X}(z|x) = P_{Y_2|X}(z|x) \qquad \forall z \in \widetilde{\mathcal{X}_1} = \widetilde{\mathcal{X}_2} = \mathcal{Y}_1 = \mathcal{Y}_2. \tag{7.4}$$

We have $\widetilde{X} \overset{d}{=} \widetilde{X}_1 \overset{d}{=} \widetilde{X}_2$ and $Y \overset{d}{=} Y_1 \overset{d}{=} Y_2$, where $\overset{d}{=}$ denotes the equality in probability distribution, since they have the same statistical properties. For the two-enrollment model shown in Figure 7.1 with the assumption of the condition in (7.4), we have the following result; see [16] for the proof.

Theorem 7.1. The secret-key region $\mathcal{R}$ for a two-enrollment model that satisfies (7.4) is

$$\mathcal{R} = \{(R_1, R_2) : 0 \leq R_1 \leq I(\widetilde{X}; Y), \quad 0 \leq R_2 \leq I(\widetilde{X}; Y)\}. \tag{7.5}$$

This result shows that for two enrollments of a PUF where all measurement channels have the same statistics, we can achieve the maximum secret-key rates for each enrollment simultaneously. Therefore, having two enrollments does not necessarily reduce the individual secret-key rates achieved.

7.1.2. Zero Secrecy Leakage for Symmetric PUFs

In this section, we illustrate cases where zero secrecy leakage occurs for any number $|\mathcal{J}|$ of enrollments, when a linear code is used in the FCS, and the PUF source has a certain type of symmetry. We use the following theorem.

Theorem 7.2 ([116])**.** Consider $|\mathcal{J}|$ PUF enrollments when the symmetry condition

$$\Pr[\widetilde{X}_1=\tilde{x}_1,\widetilde{X}_2=\tilde{x}_2,\dots,\widetilde{X}_{|\mathcal{J}|}=\tilde{x}_{|\mathcal{J}|}]=\Pr[\widetilde{X}_1=\overline{\tilde{x}_1},\widetilde{X}_2=\overline{\tilde{x}_2},\dots,\widetilde{X}_{|\mathcal{J}|}=\overline{\tilde{x}_{|\mathcal{J}|}}] \tag{7.6}$$

where $\bar{x}$ is the one's complement of the bit x, is satisfied for all $\tilde{x}_1,\tilde{x}_2,\dots,\tilde{x}_{|\mathcal{J}|}\in\widetilde{\mathcal{X}}$. Then, for any secret-key rate tuple $(R_1,R_2,\dots,R_{|\mathcal{J}|})$ such that $R_j\le I(\widetilde{X}_j;Y_j)$ for all $j\in\{1,2,\dots,|\mathcal{J}|\}$, we have zero secrecy leakage about each secret key, i.e., we obtain

$$I(S_j;W_1,W_2,\dots,W_{|\mathcal{J}|})=0 \tag{7.7}$$

for all $j\in\{1,2,\dots,|\mathcal{J}|\}$ if we use the FCS discussed in Chapter 3.

We give two cases that satisfy the constraint in Theorem 7.2.

SRAM-PUF Model Under Varying Ambient Temperature

An SRAM has binary outputs and each SRAM cell has two hidden model variables to define the probability $\Pr[\widetilde{X}=1]$ at an ambient temperature T. The hidden variable M defines the bias of the cell and D defines the effect of temperature, when M and D are independent. For an SRAM cell with given realizations m and d, the j^{th} observation at temperature $T^{(j)}$ is modeled as [117]

$$\tilde{x}^{(j)}(T^{(j)})=\begin{cases}0 & \text{if } m+n^{(j)}+d\cdot T^{(j)}\le\tau,\\ 1 & \text{if } m+n^{(j)}+d\cdot T^{(j)}>\tau\end{cases} \tag{7.8}$$

where n represents the noise in each measurement distributed according to $\mathcal{N}(0,1)$. The probability that $\widetilde{X}=1$ is observed at temperature T for this cell is given by $Q(-m-d\cdot T+\tau)$, where $Q(\cdot)$ is the Q-function. The realizations m and d are assumed to be unknown and they are modeled as the realizations of the random variables, respectively, $M\sim\mathcal{N}(\mu_M,\sigma_M)$ and $D\sim\mathcal{N}(0,\sigma_D)$ for each SRAM cell. Therefore, at the j-th measurement we have

$$\Pr[\widetilde{X}^{(j)}=1]=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}Q(-m-d\cdot T^{(j)}+\tau)p_M(m)p_D(d)\,\mathrm{d}m\,\mathrm{d}d. \tag{7.9}$$

Suppose that the SRAM cells are unbiased, i.e., $\mu_M=\tau$. For $|\mathcal{J}|$ observations of an SRAM cell at various *given* temperatures $T^{|\mathcal{J}|}=(T^{(1)},T^{(2)},\dots,T^{(|\mathcal{J}|)})$, we show that

$$\Pr(\widetilde{X}^{|\mathcal{J}|}=\tilde{x}^{|\mathcal{J}|})=\Pr(\widetilde{X}^{|\mathcal{J}|}=\overline{\tilde{x}^{|\mathcal{J}|}}) \tag{7.10}$$

by using the symmetry properties $p_M(m) = p_M(-m)$ and $p_D(d) = p_D(-d)$. Since the hidden model variables are i.i.d. over all SRAM cells, we have for n SRAM cells

$$\begin{aligned}
&\Pr\left[\widetilde{X}_1^{|\mathcal{J}|} = \tilde{x}_1^{|\mathcal{J}|}, \widetilde{X}_2^{|\mathcal{J}|} = \tilde{x}_2^{|\mathcal{J}|}, \ldots, \widetilde{X}_n^{|\mathcal{J}|} = \tilde{x}_n^{|\mathcal{J}|}\right] = \prod_{i=1}^{n} \Pr[\widetilde{X}_i^{|\mathcal{J}|} = \tilde{x}_i^{|\mathcal{J}|}] \\
&\overset{(a)}{=} \prod_{i=1}^{n} \Pr[\widetilde{X}_i^{|\mathcal{J}|} = \overline{\tilde{x}_i^{|\mathcal{J}|}}] \\
&= \Pr\left[\widetilde{X}_1^{|\mathcal{J}|} = \overline{\tilde{x}_1^{|\mathcal{J}|}}, \widetilde{X}_2^{|\mathcal{J}|} = \overline{\tilde{x}_2^{|\mathcal{J}|}}, \ldots, \widetilde{X}_n^{|\mathcal{J}|} = \overline{\tilde{x}_n^{|\mathcal{J}|}}\right] \qquad (7.11)
\end{aligned}$$

where (a) follows by (7.10). This shows that the model given in (7.8) meets the symmetry condition in (7.6). By Theorem 7.2, the temperature dependent SRAM-PUF model (7.8) results in zero secrecy leakage about each embedded key, as in (7.7), if the FCS is used for secret-key agreement.

Other PUF Models with the Symmetry Property

Any binary-input symmetric memoryless measurement channel, as discussed in Chapter 4, satisfies the symmetry constraint (7.6) if the hidden source is symmetric.

We give an example source-channel model pair where both the source and channel are asymmetric but the outputs are symmetric to further illustrate that the symmetry property in (7.6) is not limited to a small set of source-channel models. Consider a measurement channel with probability transition matrix

$$T_u = \begin{bmatrix} 1 & 0 & 0 & 0 \\ \frac{9}{64} & \frac{25}{64} & \frac{15}{64} & \frac{15}{64} \end{bmatrix} \qquad (7.12)$$

and a binary hidden source X with $\Pr[X = 1] = 0.8$. This setup corresponds to the measurement of a binary hidden source through two independent Z-channels, both with parameter $z = 0.375$. The first two outputs in (7.12) have the same probability 5/16 and the last two outputs in (7.12) have probability 3/16. This shows that (7.6) is satisfied, which is a sufficient condition for zero secrecy leakage for multiple enrollments with the FCS. Also note that for this source-channel model, the secret-key capacity for each key is approximately $R_s = 0.0456$ bits/source-bit, which illustrates that key agreement is possible with linear codes used in the FCS.

7.2. Coding for Positive Rate in the Key Agreement Problem

We now consider a general key agreement problem where the legitimate parties are allowed to talk over a public and authenticated channel in both directions and multiple times, unlike our previous models. Furthermore, we allow the eavesdropper to observe a sequence that is correlated with the observations of the legitimate parties. Such a scenario can be observed in key agreement via a wireless channel, i.e., physical-layer security, and in key agreement with two legitimate parties that observe different noisy measurements of the same biometric source.

Suppose Alice, Bob, and eavesdropper (Eve), respectively, observe n i.i.d. realizations of X, Y, and Z that are distributed according to the pmf $p_{XYZ}(x,y,z)$ for $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$, where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite sets. Alice and Bob want to agree on a key hidden from Eve as follows: Alice first creates a public message F_1 using some $p_{F_1|X^n}(f_1|x^n)$ and sends it to Bob. Bob generates a public message F_2 using some $p_{F_2|Y^nF_1}(f_2|y^n, f_1)$ and sends it to Alice, then Alice generates F_3 according to some $p_{F_3|X^nF_{1:2}}(f_3|x^n, f_{1:2})$, etc. After k rounds of communications, Alice creates a key K_A according to some $p_{K_A|X^nF_{1:k}}(k_A|x^n, f_{1:k})$ and Bob creates a key K_B according to some $p_{K_B|Y^nF_{1:k}}(k_B|y^n, f_{1:k})$.

A key rate R_s is achievable if, given any $\delta > 0$, there is some $n \geq 1$, an encoder, and a decoder for which $R_s = \frac{1}{n}\log|\mathcal{K}_A|$ and

$$\begin{aligned}
&\Pr[K_A \neq K_B] \leq \delta && \text{(reliability)}\\
&\frac{1}{n}H(K_A) \geq R_s - \delta && \text{(uniformity)}\\
&\frac{1}{n}I(K_A; Z^n, F_{1:k}) \leq \delta && \text{(weak secrecy).}
\end{aligned} \tag{7.13}$$

The supremum of all achievable key rates is called the source model secret-key (SK) capacity and denoted by $S(X;Y\|Z)$.

Definition 7.2. (X,Y,Z) is an erasure source with parameter ϵ if $p_{Z|XY}$ is an erasure channel, i.e., $Z = XY$ with probability $1-\epsilon$ and $Z = \mathsf{e}$ with probability ϵ, where e is the erasure symbol. The alphabet of Z is $\mathcal{Z} = \{\mathsf{e}\} \cup (\mathcal{X} \times \mathcal{Y})$.

We here restrict the pmfs to the erasure sources; see our results in [18] for extensions to general pmfs.

Definition 7.3. (X,Y) is a doubly symmetric binary source (DSBS) with parameter p, i.e., DSBS(p), for $X, Y \in \{0,1\}$, if $p_{XY}(0,0) = p_{XY}(1,1) = p/2$ and $p_{XY}(0,1) = p_{XY}(1,0) = (1-p)/2$.

Definition 7.4. (X,Y,Z) is a doubly symmetric binary-erasure (DSBE) source with parameters (p,ϵ) if (X,Y,Z) is an erasure source with parameter ϵ and (X,Y) is a DSBS(p). The alphabet of Z is $\mathcal{Z} = \{\mathsf{e},(0,0),(1,1),(0,1),(1,0)\}$.

Consider an erasure source with parameter ϵ. When $\epsilon = 0$, we have $Z = XY$ and $S(X;Y\|Z) = 0$. When $\epsilon = 1$, $Z = \mathsf{e}$ is constant and $S(X;Y\|Z) = I(X;Y)$. We are interested in the values of $\epsilon \in [0,1]$ such that $S(X;Y\|Z) > 0$. Our approach provides a sufficient condition on ϵ such that $S(X;Y\|Z) > 0$. We also prove the necessity of this condition when X or Y is binary.

7.2.1. Literature Review

We now list the most important bounds on the SK capacity.

SK Capacity Lower Bounds

The SK capacity when messages are transmitted only in one direction over the public channel is given in [62]. The one-way SK capacity from X to Y, denoted by $S_{\text{ow}}(X;Y\|Z)$, is

$$S_{\text{ow}}(X;Y\|Z)=\max_{U-V-X-YZ} I(V;Y|U)-I(V;Z|U) \tag{7.14}$$

which is a lower bound on the SK capacity $S(X;Y\|Z)$.

The best known lower bound on the SK capacity $S(X;Y\|Z)$ for general sources (using interactive communication) was as follows [118]. Given random variables $U_1,U_2,\cdots,U_k$ satisfying the Markov chain conditions

$$U_i - XU_{1:i-1} - YZ \text{ for odd } i, \tag{7.15}$$

$$U_i - YU_{1:i-1} - XZ \text{ for even } i \tag{7.16}$$

and for any integer ζ such that $1\leq\zeta\leq k$, we have $S(X;Y\|Z)\geq L(X;Y\|Z)$ where

$$\begin{aligned} L(X;Y\|Z)=&\sum_{\substack{i\geq\zeta\\ \text{odd } i}} I(U_i;Y|U_{1:i-1})-I(U_i;Z|U_{1:i-1})\\ &+\sum_{\substack{i\geq\zeta\\ \text{even } i}} I(U_i;X|U_{1:i-1})-I(U_i;Z|U_{1:i-1}). \end{aligned} \tag{7.17}$$

Denote the best possible lower bound obtained from (7.17) by $\bar{L}(X;Y\|Z)$.

SK Capacity Upper Bound

The *intrinsic mutual information* upper bound [62, pp. 1126, Remark 2], [119] is

$$S(X;Y\|Z)\leq B_0(X;Y\|Z)\triangleq \min_{P_{J|Z}(j|z)} I(X;Y|J). \tag{7.18}$$

We next list three results below; see [18] for proofs.

7.2.2. Main Results

Our first main result follows by relating the parameter ϵ with the strong data processing constant [120]; see also [119].

Theorem 7.3. Let (X,Y,Z) be a DSBE source with parameters (p,ϵ). Then $\bar{L}(X;Y\|Z)=0$ if and only if the one-way SK capacity $S_{\text{ow}}(X;Y\|Z)$ from Alice to Bob (or Bob to Alice) vanishes, which is the case if and only if

$$\epsilon \leq 4p(1-p). \tag{7.19}$$

We define a path before giving our second main result.

Definition 7.5. A sequence $(x_1, y_1, x_2, y_2, \cdots, x_k, y_k)$ forms a path if all x_i's with $x_i \in \mathcal{X}$ are distinct and also all y_i's with $y_i \in \mathcal{Y}$ are distinct. We say the length of the path is $2k$ and we assign the following value to the path

$$\left(\frac{\prod_{i=1}^{k} p_{XY}(x_i, y_i)}{p_{XY}(x_1, y_k) \prod_{i=2}^{k} p_{XY}(x_i, y_{i-1})} \right)^{1/k}. \tag{7.20}$$

Let ϵ_1 be the minimum assigned value of all possible paths and ϵ_2 be the minimum assigned value of all possible paths of length at most four.

We now give lower and upper bounds on the maximum erasure probability for which the SK capacity is zero for an erasure source.

Theorem 7.4. For any erasure source (X, Y, Z) with erasure probability ϵ, we have $S(X; Y \| Z) = 0$ if $\epsilon \leq \epsilon_1$, and $S(X; Y \| Z) > 0$ if $\epsilon > \epsilon_2$, where ϵ_1 and ϵ_2 are as in Definition 7.5.

Remark 7.1. If X or Y is binary, we have $\epsilon_1 = \epsilon_2$ so that this theorem gives a tight bound on the maximum erasure probability for which the SK capacity is zero.

The proof of the converse for Theorem 7.4 follows from the intrinsic mutual information upper bound $B_0(X; Y \| Z)$ by constructing a random variable J such that $p_{XYZJ} = p_{XYZ} p_{J|Z}$ and $I(X; Y|J) = 0$.

For achievability, suppose that ϵ_2 is obtained at the minimizer path (x_1, y_1, x_2, y_2). Define $p_{ij} = p_{XY}(x_i, y_j)$ for $i = 1, 2$ and $j = 1, 2$. Therefore, ϵ_2 is equal to the value of this path, i.e., we have

$$\epsilon_2 = \left(\frac{p_{11} p_{22}}{p_{12} p_{21}} \right)^{1/2}. \tag{7.21}$$

The achievability proof of Theorem 7.4 follows by converting the source $P_{X^n Y^n Z^n}$ into a DSBE source with parameters $(\tilde{p}, \epsilon^n)$; see [18] for the coding scheme, where

$$\tilde{p} = \frac{p_{11}^{n/2} p_{22}^{n/2}}{p_{11}^{n/2} p_{22}^{n/2} + p_{12}^{n/2} p_{21}^{n/2}}. \tag{7.22}$$

It therefore follows from Theorem 7.3 that, we can find a fixed and sufficiently large n such that $S(X;Y||Z) > 0$ if

$$\epsilon > \frac{\min\{\sqrt{p_{11}p_{22}},\ \sqrt{p_{21}p_{12}}\}}{\max\{\sqrt{p_{11}p_{22}},\ \sqrt{p_{21}p_{12}}\}} \tag{7.23}$$

whose right-hand side is less than or equal to ϵ_2 given in (7.21). This proves that SK capacity is positive if $\epsilon > \epsilon_2$.

Our third main result is the observation that $S(X;Y\|Z) \neq \bar{L}(X;Y\|Z)$ for a DSBE(p,ϵ) source if

$$\frac{\min\{p, 1-p\}}{\max\{p, 1-p\}} < \epsilon \leq 4p(1-p) \tag{7.24}$$

where the left hand side is equal to ϵ_2. This result follows directly from Theorems 7.3 and 7.4, which illustrates that the lower bound $\bar{L}(X;Y\|Z)$ is loose.

8

Conclusion

In this thesis, we studied the source model key agreement problem with PUFs and biometrics. Our main focus was on:

- Algorithm designs with a small hardware area to eliminate PUF (or biometric) output correlations, bias, and noise;
- Gains from multiple measurements of a noisy (hidden) PUF source as compared to a noiseless (visible) source;
- Information-theoretically optimal, future-proof, and practical code constructions based on binning;
- Improvements from action-dependent (adaptive) decoder measurements during reconstruction.

In the following, we summarize the main results of the thesis.

Chapter 3 The reliability, uniqueness, security, computational-complexity, and key-length performance of various transforms were compared to select the best transforms for reliable secret-key binding for RO PUFs by using the FCS. The DWHT and DHT were shown to perform the best in terms of computational-complexity, maximum key length, and reliability. All transforms gave close to optimal uniqueness and good security results. A reference hardware design with the DWHT showed that the hardware area required by the transform-coding approach is small and less than the area required by existing RO PUF designs. Low-complexity concatenated codes with high secret-key and small privacy-leakage rates are proposed for a block-error probability of 10^{-9}. The codes improve on previous designs. Furthermore, we designed quantizers with reliability guarantees. These quantizers convert the block-error probability constraint $P_B \leq 10^{-9}$ into a constraint on the number of transform coefficients allowed to be in error. We proposed a BCH code with a higher code rate than our previously proposed codes. Comparisons with the region of all achievable (secret-key, privacy-leakage) rate pairs for the FCS showed that there is still a gap between the optimal rate pairs and the proposed code. This gap can be closed by using other channel codes and decoders at the cost of higher hardware area or by designing codes for other code constructions, as illustrated in Chapter 5.

Chapter 4 We derived the key-leakage-storage regions for a HSM for biometric and physical identifiers. For a BSS, we used MGL to evaluate the key-leakage-storage regions for decoder-output channels that can be decomposed into a mixture of BSCs and quantified the rate improvements with multiple measurements at the decoder as compared to a single measurement. By taking a large number of measurements of the hidden source at the decoder, the privacy-leakage rate is made small for the GS and CS models, and the storage rate is significantly decreased for the GS model, which is not possible for the CS model. We showed that if one mistakenly uses the VSM when the source is hidden, then the privacy-leakage rate might be pessimistic, whereas the secret-key and storage rates might be over-optimistic, which leads to unnoticed secrecy leakage and reliability reductions. The rate points at the maximum secret-key rates in the key-leakage-storage regions for multiple encoder measurements showed that the gain in the secret-key rate from multiple encoder measurements results in greater privacy-leakage and significantly greater storage rates. The examples illustrate that higher reliability in the encoder measurements improves the storage rate, which also applies to decoder measurements because the encoder and decoder measurements are obtained through separate channels.

In **Chapter 5**, we showed that there are random codes that asymptotically achieve all points of the rate regions of the WZ problem and GS model simultaneously, i.e., these problems are functionally equivalent. Extending the functional equivalence, we argued that the first WZ-coding construction based on random linear codes is asymptotically optimal for the GS and CS models with uniform binary sources with decoder measurements through a BSC. These source and channel models are the standard models for RO PUFs and SRAM PUFs. We implemented the second WZ-coding construction with nested polar codes that achieve better rate tuples than existing methods, and one of our codes achieves a rate tuple that cannot be achieved by existing methods without time sharing. Gaps to the maximum key vs. storage rate ratios were illustrated. Other code constructions to achieve strong secrecy results, and extensions to HSMs, were also given.

Chapter 6 We derived the key-leakage-storage-cost regions for a hidden source with the GS and CS models when a cost-constrained action sequence controls the source measurements during authentication. Correlated side information at the eavesdropper is also considered as a realistic assumption, especially for biometric identifiers. The achievability proof of the GS model involves layered random binning. We illustrate achievable key-leakage-storage-cost regions with an example motivated by realistic authentication scenarios.

Chapter 7 We studied security of the key agreement scheme with multiple PUF enrollments. We proved that there exist codes for certain PUF measurement channels such that the secret key remains secure when the same PUF is enrolled for the second time. Furthermore, we show that the FCS remains secure for any number of enrollments when the PUF outputs meet a symmetry condition. We argued that there is a large set of source-channel models that satisfies this symmetry condition. For instance, the temperature-dependent output model for SRAM-PUFs is shown to meet this condition.

We also consider an erasure source and provide a sufficient condition to obtain a positive SK capacity when two legitimate parties are allowed to communicate in multiple rounds. We prove the necessity of this condition when at least one of the legitimate parties' source is binary. Furthermore, we show, for the first time in the literature, that the best existing lower bound for general sources is loose. Extensions to non-erasure sources are also mentioned.

We discussed that our algorithm and code designs can be further improved at the cost of higher complexity. A brief list of ongoing and future works is as follows:

- ▷ Derive water-filling techniques for the transform-coding algorithm to improve the reliability and security performance;
- ▷ Consider key-leakage-storage regions for encoder and decoder measurements through a broadcast channel to show that reduced reliability in the measurements might enlarge the rate regions;
- ▷ Show whether the WZ problem and GS model are operationally equivalent to motivate the usage of WZ-coding constructions for the GS model with general sources;
- ▷ Consider key-leakage-storage-cost regions for adaptive decoder measurements with causal actions that depend on the helper data and previous decoder measurements, which might improve the rate regions as compared to noncausal actions considered in Chapter 6;
- ▷ Apply our methods to private search problems, which are closely related to private information retrieval problems.

A

Appendices for Chapter 4

A.1. Achievability Proofs

A.1.1. Achievability Proof for Theorem 4.1

Overview

We choose the conditional probabilities $P_{U|\widetilde{X}}(u|\tilde{x})$ for all $u\in\mathcal{U}$ and $\tilde{x}\in\widetilde{\mathcal{X}}$. We randomly and independently generate $2^{n(R_w+R_s)}\approx 2^{nI(U;\widetilde{X})}$ sequences $u^n(w,s)$ for $w=1,\dots,2^{nR_w}$ and $s=1,\dots,2^{nR_s}$. Consider $2^{nR_w}\approx 2^{n(I(U;\widetilde{X})-I(U;Y))}$ storage labels w and $2^{nR_s}\approx 2^{nI(U;Y)}$ key labels s, which can be considered as bins. The encoder finds a $u^n(w,s)$ sequence that is jointly typical with the observed measurement $\tilde{x}^n$ of the source x^n. It then publicly sends the storage label w to the decoder. The decoder sees another measurement y^n of the source and it determines the unique $u^n(w,\hat{s})$ that is jointly typical with y^n. Using standard arguments, one can show that the error probability $\Pr[S\neq\hat{S}]\to 0$ as $n\to\infty$. The secrecy-leakage rate is negligible if there is no error. The privacy-leakage rate is approximately $I(U;X)-I(U;Y)$, which requires a different analysis than in [56].

Proof

Fix $P_{U|\widetilde{X}}$. Randomly and independently generate codewords $u^n(w,s)$, $w=1,\dots,2^{nR_w}$, $s=1,\dots,2^{nR_s}$ according to $\prod_{i=1}^n P_U(u_i)$, where

$$P_U(u_i)=\sum_{(\tilde{x},x)\in\widetilde{\mathcal{X}}\times\mathcal{X}} P_{U|\widetilde{X}}(u_i|\tilde{x})P_{\widetilde{X}|X}(\tilde{x}|x)Q_X(x). \tag{A.1}$$

These codewords define the codebook

$$\mathcal{C} = \{u^n(w,s), w = 1,\dots,2^{nR_w}, s = 1,\dots,2^{nR_s}\}$$

and we denote the random codebook by

$$\tilde{\mathcal{C}} = \{U^n(w,s)\}_{(w,s)=(1,1)}^{(2^{nR_w},2^{nR_s})}. \tag{A.2}$$

Let $0<\epsilon'<\epsilon$.

Encoding: Given $\tilde{x}^n$, the encoder looks for a codeword that is jointly typical with $\tilde{x}^n$, i.e., $(u^n(w,s),\tilde{x}^n) \in \mathcal{T}_{\epsilon'}^n(P_{U\widetilde{X}})$. If there is one or more such codeword, then the encoder chooses one of them and puts out (w,s). If there is no such codeword, set $w=s=1$. The encoder publicly stores the label w.

Decoding: The decoder puts out $\hat{s}$ if there is a unique key label $\hat{s}$ that satisfies the typicality check $(u^n(w,\hat{s}),y^n)\in\mathcal{T}_{\epsilon}^n(P_{UY})$; otherwise, it sets $\hat{s}=1$.

Error Probability: Define the error events

$$E_1 = \Big\{(U^n(w,s),\widetilde{X}^n) \notin \mathcal{T}_{\epsilon'}^n(P_{U\widetilde{X}}) \text{ for all } (w,s)\in[1:2^{nR_w}]\times[1:2^{nR_s}]\Big\}$$
$$E_2 = \Big\{(U^n(W,s),\widetilde{X}^n,Y^n) \notin \mathcal{T}_{\epsilon}^n(P_{U\widetilde{X}Y}) \text{ for all } s\in[1:2^{nR_s}]\Big\}$$
$$E_3 = \Big\{(U^n(W,s'),Y^n) \in \mathcal{T}_{\epsilon}^n(P_{UY}) \text{ for some } s'\neq S\Big\}.$$

and the overall error event $E=\cup_{i=1}^3 E_i$. Using the union bound, we have

$$\Pr[E]\le\Pr[E_1]+\Pr[E_1^c\cap E_2]+\Pr[E_3]. \tag{A.3}$$

$\Pr[E_1]$ is small with large n and small ϵ' if

$$R_w+R_s>I(U;\widetilde{X})+\delta(\epsilon') \tag{A.4}$$

where $\delta(\epsilon')$ is small with small ϵ' (see the covering lemma [103, Lemma 3.3]).

Note that the event $\{\widetilde{X}^n=\tilde{x}^n, U^n=u^n\}$ implies $Y^n\sim\prod_{i=1}^n P_{Y|\widetilde{X}}(y_i|\tilde{x}_i)$. By the conditional typicality lemma [103, Section 2.5], we obtain that $\Pr[E_1^c\cap E_2]$ is small with large n.

Due to symmetry in the code generation, we can set $W=1$ and have

$$\Pr[E_3]=\Pr[(U^n(1,s'),Y^n)\in\mathcal{T}_{\epsilon}^n(P_{UY}) \text{ for some } s'\neq S].$$

Using the packing lemma [103, Lemma 3.1], we find that $\Pr[E_3]$ is small with large n and small ϵ if

$$R_s<I(U;Y)-\delta(\epsilon) \tag{A.5}$$

where $\delta(\epsilon)$ is small with small ϵ.

We therefore define some δ_1 and δ_2, where $\delta_2>\delta(\epsilon)$ and $\delta_1>\delta(\epsilon')+\delta_2$, that are small with small ϵ and some δ' that is small with large n and small ϵ such that

$$\Pr[E] \leq \delta' \tag{A.6}$$

$$R_w = I(U;\widetilde{X}) - I(U;Y) + \delta_1 \tag{A.7}$$

$$R_s = I(U;Y) - \delta_2. \tag{A.8}$$

We first establish bounds on the secrecy-leakage, secret-key, privacy-leakage, and storage rates averaged over the random codebook $\tilde{\mathcal{C}}$ and then we show that there exists a codebook satisfying (4.2)-(4.6). In the following, U^n represents $U^n(W,S)$.

Secrecy-leakage Rate: Observe that

$$\begin{aligned}
&H(W,S|\tilde{\mathcal{C}}) \overset{(a)}{=} H(U^n,W,S|\tilde{\mathcal{C}})\\
&\geq H(U^n|\tilde{\mathcal{C}})\\
&= H(U^n,\widetilde{X}^n|\tilde{\mathcal{C}}) - H(\widetilde{X}^n|U^n,\tilde{\mathcal{C}})\\
&\overset{(b)}{\geq} nH(\widetilde{X}) - H(\widetilde{X}^n|U^n,\tilde{\mathcal{C}})\\
&\overset{(c)}{\geq} nH(\widetilde{X}) - n(H(\widetilde{X}|U) + \delta_\epsilon)\\
&= n(I(U;\widetilde{X}) - \delta_\epsilon)\\
&\overset{(d)}{=} n(R_w + R_s - \delta_1 + \delta_2 - \delta_\epsilon)
\end{aligned} \tag{A.9}$$

where
(a) follows because, given the codebook, (W,S) determines U^n,
(b) follows because $\widetilde{X}^n$ is independent of the codebook,
(c) follows by using Lemma C.2 for δ_ϵ that is small with small ϵ,
(d) follows by (A.7) and (A.8).

Using (A.9), we obtain

$$\begin{aligned}
&\frac{1}{n}I(S;W|\tilde{\mathcal{C}}) = \frac{1}{n}(H(S|\tilde{\mathcal{C}}) + H(W|\tilde{\mathcal{C}}) - H(W,S|\tilde{\mathcal{C}}))\\
&\leq \frac{1}{n}(nR_s + nR_w - H(W,S|\tilde{\mathcal{C}}))\\
&\leq \delta_1 - \delta_2 + \delta_\epsilon
\end{aligned} \tag{A.10}$$

which is small with small ϵ.

Key Uniformity: We have

$$\begin{aligned}
&\frac{1}{n}H(S|\tilde{\mathcal{C}}) \geq \frac{1}{n}(H(W,S|\tilde{\mathcal{C}}) - H(W|\tilde{\mathcal{C}}))\\
&\overset{(a)}{\geq} R_s - \delta_1 + \delta_2 - \delta_\epsilon.
\end{aligned} \tag{A.11}$$

where (a) follows by (A.9).

Privacy-leakage Rate: First, consider

$$\begin{aligned}
&H(W|X^n\tilde{\mathcal{C}}) = H(W,\widetilde{X}^n|X^n,\tilde{\mathcal{C}})-H(\widetilde{X}^n|W,X^n,\tilde{\mathcal{C}})\\
&\overset{(a)}{\geq}H(\widetilde{X}^n|X^n)-H(\widetilde{X}^n|W,X^n,\tilde{\mathcal{C}})\\
&\overset{(b)}{=}H(\widetilde{X}^n|X^n)-H(\widetilde{X}^n,S|W,X^n,\tilde{\mathcal{C}})\\
&\overset{(c)}{\geq}nH(\widetilde{X}|X)-H(S|W,X^n,\tilde{\mathcal{C}})-H(\widetilde{X}^n|X^n,U^n,\tilde{\mathcal{C}})\\
&\overset{(d)}{=}nH(\widetilde{X}|X)-H(S|W,X^n,Y^n,\hat{S},\tilde{\mathcal{C}})-H(\widetilde{X}^n|X^n,U^n,\tilde{\mathcal{C}})\\
&\overset{(e)}{\geq}nH(\widetilde{X}|X)-\Pr[E]\log|\mathcal{S}|-H_b(\Pr[E])-H(\widetilde{X}^n|X^n,U^n,\tilde{\mathcal{C}})\\
&\overset{(f)}{=}nH(\widetilde{X}|X)-n\delta''-H(\widetilde{X}^n|X^n,U^n,\tilde{\mathcal{C}})\\
&\overset{(g)}{\geq}nH(\widetilde{X}|X)-n\delta''-n(H(\widetilde{X}|X,U)+\delta'_\epsilon)\\
&=n(I(U;\widetilde{X}|X)-(\delta''+\delta'_\epsilon))
\end{aligned}\tag{A.12}$$

where
(a) follows because $\tilde{\mathcal{C}}$ is independent of $(\widetilde{X}^n,X^n)$,
(b) follows because, given the codebook, $\widetilde{X}^n$ determines S,
(c) follows since, given the codebook, (W,S) determines U^n,
(d) follows by the Markov chain $(S,W,U^n)-\widetilde{X}^n-X^n-Y^n$,
(e) follows from Fano's inequality,
(f) follows by using $|\mathcal{S}|\leq|\widetilde{\mathcal{X}}|^n$ and defining a parameter δ'' that is small with large n and small ϵ due to (A.6),
(g) follows by using Lemma C.2 for δ_ϵ that is small with small ϵ.

Using (A.12), we have

$$\begin{aligned}
&\frac{1}{n}I(X^n;W|\tilde{\mathcal{C}})=\frac{1}{n}(H(W|\tilde{\mathcal{C}})-H(W|X^n,\tilde{\mathcal{C}}))\\
&\leq R_w-(I(U;\widetilde{X}|X)-(\delta''+\delta'_\epsilon))\\
&\overset{(a)}{=}R_w-(H(U|X)-H(U|\widetilde{X})-(\delta''+\delta'_\epsilon))\\
&\overset{(b)}{=}I(U;X)-I(U;Y)+\delta''+\delta'_\epsilon+\delta_1
\end{aligned}\tag{A.13}$$

where (a) follows by the Markov chain $U-\widetilde{X}-X$ and (b) follows by (A.7).

Storage Rate: Using (A.7), we have

$$\frac{1}{n}\log|\mathcal{W}| = R_w = I(U;\widetilde{X}) - I(U;Y) + \delta_1. \tag{A.14}$$

Applying the selection lemma [100, Lemma 2.2] to these results, there exists a codebook for the GS model that approaches the key-leakage-storage triple

$$(R_s, R_\ell, R_w) = \Big(I(U;Y), I(U;X)-I(U;Y), I(U;\widetilde{X})-I(U;Y)\Big).$$

A.1.2. Achievability Proof for Theorem 4.2

Overview

We use the achievability proof of the GS model in combination with a one-time pad to conceal the embedded secret key S by the key S' generated by the GS model. The embedded key S is uniformly distributed and independent of other random variables. The secret-key and privacy-leakage rates do not change, but the storage rate $I(U;\widetilde{X})$ is approximately the sum of the storage and secret-key rates of the GS model.

Proof

Suppose S has the same cardinality as S', i.e., $|\mathcal{S}|=|\mathcal{S}'|$. We use the codebook, encoder, and decoder of the GS model and add the masking layer (one-time pad) approach of [56] and [62] for the CS model as follows:

$$W = \mathsf{Enc}(\widetilde{X}^n, S) \ = [S'+S, W'] \tag{A.15}$$

$$\hat{S} = \mathsf{Dec}(Y^n, W) = S'+S-\hat{S}' \tag{A.16}$$

where W' is the helper data of the GS model, and the addition and subtraction operations are modulo-$|\mathcal{S}|$.

Error Probability: We have

$$\Pr[S \neq \hat{S}] = \Pr[S' \neq \hat{S}'] \tag{A.17}$$

which is small by (A.6).

Secrecy-leakage Rate: The helper data W of the CS model consists of $S'+S$ and the helper data W' of the GS model. Using (A.10), (A.11), and since S is independent of $(S', W', \tilde{\mathcal{C}})$ and uniformly distributed, we obtain

$$\frac{1}{n} I(S; W', S'+S|\tilde{\mathcal{C}}) \leq 2(\delta_1 - \delta_2 + \delta_\epsilon). \tag{A.18}$$

We thus have a secrecy-leakage rate that is small with small ϵ.

Privacy-leakage Rate: Using (A.13), we have

$$\frac{1}{n} I(X^n; W', S'+S|\tilde{\mathcal{C}}) \leq I(U;X)-I(U;Y)+\delta''+\delta'_\epsilon+\delta_1 \tag{A.19}$$

since $S'+S$ is independent of $(W', X^n, \tilde{\mathcal{C}})$.

Storage Rate: We obtain

$$\begin{aligned}
&\frac{1}{n}H(W',S'{+}S|\tilde{\mathcal{C}}) \overset{(a)}{\leq} R_w + \frac{1}{n}H(S'{+}S)\\
&\overset{(b)}{=} I(U;\widetilde{X}){-}I(U;Y){+}\delta_1 + I(U;Y){-}\delta_2 = I(U;\widetilde{X}) + \delta_1{-}\delta_2 \qquad \text{(A.20)}
\end{aligned}$$

where (a) follows because $S'{+}S$ is independent of $(W',\tilde{\mathcal{C}})$, and (b) follows by (A.7) and (A.8).

Using the selection lemma [100, Lemma 2.2], there exists a codebook for the CS model that approaches the key-leakage-storage triple

$$(R_s,R_\ell,R_w) = \Big(I(U;Y), I(U;X){-}I(U;Y), I(U;\widetilde{X})\Big).$$

A.2. Converses

The converses for Theorems 4.1 and 4.2 follow similar steps. Therefore, we give the proofs of both theorems with different bounds for the storage rates.

Suppose that for some $\delta > 0$ and n there is an encoder and a decoder such that (4.2)-(4.6) are satisfied for the GS or CS model by the key-leakage-storage triple (R_s, R_ℓ, R_w). Fano's inequality for S and $\hat{S}$ gives

$$n\epsilon_n \geq H(S|\hat{S}) \overset{(a)}{\geq} H(S|W,Y^n) \qquad \text{(A.21)}$$

where $\epsilon_n = \delta R_s + H_b(\delta)/n$ and (a) permits randomized decoding. Note that $\epsilon_n \to 0$ if $\delta \to 0$. We use (A.21) to bound the key, leakage, and storage rates.

Secret-key rate: Using (4.3), (4.5), (A.21), and because $Y^{i-1} - (W,S,X^{i-1}) - Y_i$ forms a Markov chain, we obtain

$$\begin{aligned}
n(R_s{-}\delta) &\leq H(S) = I(S;W) + I(S;Y^n|W) + H(S|W,Y^n)\\
&\leq nH(Y) - \sum_{i=1}^{n} H(Y_i|W,S,X^{i-1}) + n(\delta{+}\epsilon_n). \qquad \text{(A.22)}
\end{aligned}$$

Identify $U_i \triangleq (W,S,X^{i-1})$ in (A.22), so $U_i - \widetilde{X}_i - X_i - Y_i$ forms a Markov chain, which follows since $P_{Y|X}$ and $P_{\widetilde{X}|X}$ are memoryless channels. Introduce a time-sharing random variable $Q \sim \text{Unif}[1:n]$ independent of other random variables. Define $X = X_Q$, $\widetilde{X} = \widetilde{X}_Q$, $Y = Y_Q$, and $U = (U_Q,Q)$, so $U - \widetilde{X} - X - Y$ forms a Markov chain. Using (A.22), we obtain

$$\begin{aligned}
R_s &\leq H(Y) - \frac{1}{n}\sum_{i=1}^{n} H(Y_i|U_i) + 2\delta + \epsilon_n\\
&= H(Y) - H(Y_Q|U_Q,Q) + 2\delta + \epsilon_n = I(U;Y) + 2\delta + \epsilon_n. \qquad \text{(A.23)}
\end{aligned}$$

Storage rate: For the GS model, we have

$$\begin{aligned}
&n(R_w+\delta) \overset{(a)}{\geq} H(W) \geq H(W|Y^n)\\
&\overset{(b)}{\geq} H(W,S,Y^n)-H(Y^n)-H(S|W,Y^n) - H(W,S|\widetilde{X}^n)\\
&\overset{(c)}{\geq} \Big[\sum_{i=1}^{n} I(W,S,\widetilde{X}^{i-1};\widetilde{X}_i)-I(W,S,Y^{i-1};Y_i)\Big]-n\epsilon_n\\
&\overset{(d)}{\geq} \Big[\sum_{i=1}^{n} I(W,S,X^{i-1};\widetilde{X}_i)-I(W,S,X^{i-1};Y_i)\Big]-n\epsilon_n\\
&= \Big[\sum_{i=1}^{n} I(U_i;\widetilde{X}_i) - I(U_i;Y_i)\Big]-n\epsilon_n
\end{aligned} \tag{A.24}$$

where (a) follows by (4.6), (b) follows from the encoding step, (c) follows by (A.21) and because $\widetilde{X}^n$ and Y^n are i.i.d., and (d) follows by the Markov chains

$$Y^{i-1}-(W,S,X^{i-1})-Y_i \tag{A.25a}$$

$$X^{i-1}-(W,S,\widetilde{X}^{i-1})-\widetilde{X}_i. \tag{A.25b}$$

Using the definition of U above, we obtain for the GS model

$$R_w \geq I(U;\widetilde{X}) - I(U;Y) - (\delta+\epsilon_n). \tag{A.26}$$

For the CS model, we have

$$\begin{aligned}
&n(R_w+\delta) \overset{(a)}{\geq} H(W)\\
&= I(W,S;\widetilde{X}^n)-H(S|W)+H(W,S|\widetilde{X}^n)\\
&\overset{(b)}{\geq} I(W,S;\widetilde{X}^n)+I(S;W)\\
&\geq \sum_{i=1}^{n} I(W,S,\widetilde{X}^{i-1};\widetilde{X}_i)\\
&\overset{(c)}{\geq} \sum_{i=1}^{n} I(W,S,X^{i-1};\widetilde{X}_i)\\
&= \sum_{i=1}^{n} I(U_i;\widetilde{X}_i)
\end{aligned} \tag{A.27}$$

where (a) follows by (4.6), (b) follows because S is independent of $\widetilde{X}^n$ and from the encoding step, and (c) follows by applying (A.25b). Using the definition of U above, we have for the CS model

$$R_w \geq I(U;\widetilde{X}) - \delta. \tag{A.28}$$

Privacy-leakage rate: Observe that

$$\begin{aligned}
n(R_\ell{+}\delta) &\overset{(a)}{\geq} I(X^n;W) \geq H(W|Y^n) - H(W|X^n)\\
&= H(W,S,Y^n){-}H(S|W,Y^n){-}H(Y^n){-}H(W|X^n)\\
&\geq I(W,S;X^n){-}I(W,S;Y^n){-}H(S|W,Y^n)\\
&\overset{(b)}{\geq} \Big[\sum_{i=1}^{n} I(W,S,X^{i-1};X_i){-}I(W,S,Y^{i-1};Y_i)\Big]{-}n\epsilon_n\\
&\overset{(c)}{\geq} \Big[\sum_{i=1}^{n} I(W,S,X^{i-1};X_i){-}I(W,S,X^{i-1};Y_i)\Big]{-}n\epsilon_n\\
&= \Big[\sum_{i=1}^{n} I(U_i;X_i) - I(U_i;Y_i)\Big] - n\epsilon_n
\end{aligned} \tag{A.29}$$

where (a) follows by (4.4), (b) follows by (A.21), and (c) follows from the Markov chain in (A.25a). Using the definition of U above, we have

$$R_\ell \geq I(U;X) - I(U;Y) - (\delta{+}\epsilon_n). \tag{A.30}$$

The converse for Theorem 4.1 follows by (A.23), (A.26), and (A.30), and by letting $\delta \to 0$. The converse for Theorem 4.2 follows by (A.23), (A.28), and (A.30), and by letting $\delta \to 0$.

A.3. Cardinality Bound

Consider $\widetilde{\mathcal{X}} = \{\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{|\widetilde{\mathcal{X}}|}\}$ and the following $|\widetilde{\mathcal{X}}|{+}2$ real-valued continuous functions on the connected compact subset $\mathcal{P}$ of all probability distributions on $\widetilde{\mathcal{X}}$:

$$f_j(P_{\widetilde{X}}) = \begin{cases} P_{\widetilde{X}}(\tilde{x}_j) \text{ for } j = 1,2,\ldots,|\widetilde{\mathcal{X}}|{-}1\\ H(X) \text{ for } j = |\widetilde{\mathcal{X}}|\\ H(\widetilde{X}) \text{ for } j = |\widetilde{\mathcal{X}}| + 1\\ H(Y) \text{ for } j = |\widetilde{\mathcal{X}}| + 2. \end{cases} \tag{A.31}$$

By using the support lemma [83, Lemma 15.4], we find that there is a random variable U' taking at most $|\widetilde{\mathcal{X}}|{+}2$ values such that $P_{\widetilde{X}}$, $H(\widetilde{X})$, $H(X|U)$, $H(\widetilde{X}|U)$, and $H(Y|U)$ are preserved if we replace U with U'. We preserve the joint distribution $P_{\widetilde{X}XY}(\tilde{x},x,y) = P_{\widetilde{X}}(\tilde{x})P_{X|\widetilde{X}}(x|\tilde{x})P_{Y|X}(y|x)$ by preserving $P_{\widetilde{X}}(\tilde{x})$, so the entropies $H(X)$ and $H(Y)$ are also preserved. Hence, the expressions in Theorems 4.1 and 4.2

$$\begin{aligned}
&I(U;Y) {=} H(Y){-}H(Y|U)\\
&I(U;X) - I(U;Y) {=} H(X){-}H(X|U){-}H(Y){+}H(Y|U)
\end{aligned}$$

$$I(U;\widetilde{X})-I(U;Y)=H(\widetilde{X})-H(\widetilde{X}|U)-H(Y)+H(Y|U)$$
$$I(U;\widetilde{X})=H(\widetilde{X})-H(\widetilde{X}|U)$$

are preserved by some U' that satisfies the Markov condition $U'-\widetilde{X}-X-Y$ with $|\mathcal{U}'| \leq |\widetilde{\mathcal{X}}|+2$.

A.4. Alternative Convexity Proof for Independent BSCs

We first give a sufficient condition for the convexity of the function $g(f^{-1}(\nu))$ in ν for $\nu \in [0,1]$ and some general functions $f(\cdot)$, which is different from the function in (4.9), and $g(\cdot)$. Define $f^{'}(x)=\frac{d}{dx}f(x)$, $f^{''}(x)=\frac{d^2}{dx^2}f(x)$ and note that

$$\frac{d}{dx}f^{-1}(x) = \frac{1}{f'(f^{-1}(x))}. \tag{A.32}$$

Let $\nu = f(x)$, where $f(\cdot)$ is invertible. The second partial derivative of $g(f^{-1}(\nu))$ with respect to ν is

$$\begin{aligned}
&\frac{\partial^2}{\partial\nu^2}\Big(g(f^{-1}(\nu))\Big) = \frac{\partial}{\partial\nu}\left(\frac{g^{'}(f^{-1}(\nu))}{f'(f^{-1}(\nu))}\right)\\
&= \frac{g^{''}(f^{-1}(\nu))f^{'}(f^{-1}(\nu)) - g^{'}(f^{-1}(\nu))f^{''}(f^{-1}(\nu))}{f'(f^{-1}(\nu))^3}\\
&= \frac{g^{''}(x)f^{'}(x) - g^{'}(x)f^{''}(x)}{f'(x)^3}\\
&= \frac{1}{f'(x)}\frac{\partial}{\partial x}\left(\frac{g^{'}(x)}{f'(x)}\right).
\end{aligned} \tag{A.33}$$

Observe that (A.33) is non-negative, and thus $g(f^{-1}(\nu))$ is convex in ν, as long as the ratio $g^{'}(x)/f^{'}(x)$ is non-decreasing and $f(x)$ is strictly increasing. There are other possibilities to satisfy convexity, e.g., a strictly decreasing $f(x)$ and a non-increasing derivative ratio. We next show that independent BSCs satisfy the former sufficient condition.

For a channel $P_{Y_{1:L}|X}$ that consists of L independent BSCs with crossover probability p we have (see (4.12))

$$g(x)=-\left(\sum_{k=0}^{L}\binom{L}{k}\Big(x\bar{p}^{L-k}p^{k}+\bar{x}\bar{p}^{k}p^{L-k}\Big)\times\log_2\Big(x\bar{p}^{L-k}p^{k}+\bar{x}\bar{p}^{k}p^{L-k}\Big)\right). \tag{A.34}$$

Observe from (4.10) and (A.34) that we have

$$f(x) = H_b(x) = H_b(\bar{x}),\ \ g(x) = g(\bar{x}),\ \ g_p(x) = g_{\bar{p}}(x) \tag{A.35}$$

so it suffices to prove convexity for $0 \le x \le 0.5$ and $0 \le p \le 0.5$. We compute $H_b^{'}(x) = \ln(\bar{x}/x)$, which is positive for $0 \le x < 0.5$. In addition, we define

$$h_{L,k}(p,x) = \Big(b(k,p) - b(k,\bar{p})\Big) \times \ln \frac{xb(k,\bar{p}) + \bar{x}b(k,p)}{xb(k,p) + \bar{x}b(k,\bar{p})} \tag{A.36}$$

where $b(k,p) = \binom{L}{k} p^k \bar{p}^{L-k}$. Hence, we have

$$g^{'}(x) = \sum_{k=0}^{\lfloor \frac{L-1}{2} \rfloor} h_{L,k}(p,x) \tag{A.37}$$

where we exploit the symmetry in the summation terms. $g^{'}(x)$ is non-negative when $0 \le x < 0.5$ and $0 \le p \le 0.5$. Define

$$q_{L,k}(p,x) = \frac{h_{L,k}(p,x)}{\ln\left(\frac{\bar{x}}{x}\right)} \tag{A.38}$$

so that the ratio $g^{'}(x)/H_b^{'}(x)$ becomes

$$F(x) = \sum_{k=0}^{\left\lfloor \frac{L-1}{2} \right\rfloor} q_{L,k}(p,x). \tag{A.39}$$

$F(x) = g^{'}(x)/f^{'}(x)$ should be then non-decreasing in x to satisfy the convexity property. We show that each summation term in (A.39) increases in x. Define $u = \bar{x}/x$ and $c = b(k,\bar{p})/b(k,p)$. The new constraints are $u > 1$ and $0 \le c \le 1$ since we restrict ourselves to $0 \le x < 0.5$ and $0 \le p \le 0.5$ when $k \in \{0, 1, \dots, \lfloor \frac{L-1}{2} \rfloor\}$. The term $(b(k,p) - b(k,\bar{p}))$ is non-negative for all k and it is zero if $p = 0.5$. Hence, by $dx = (-1/(u+1)^2)du$, it suffices to show that

$$\frac{\partial}{\partial u}\left(\frac{\ln\left(\frac{c+u}{cu+1}\right)}{\ln u}\right) \leqslant 0 \tag{A.40}$$

which is equivalent to

$$\ln u \leqslant \ln\left(\frac{c+u}{cu+1}\right) \cdot \frac{(c+u)(cu+1)}{(1-c)(c+1)u}. \tag{A.41}$$

The inequality in (A.41) is valid when $c = 0$ for every u. It therefore suffices to prove that the right hand side is increasing with respect to c for every u so that

$$\frac{\partial}{\partial c}\left(\ln\left(\frac{c+u}{cu+1}\right)\cdot\frac{(c+u)(cu+1)}{(1-c)(c+1)u}\right)\geqslant 0 \tag{A.42}$$

which has to satisfy the same conditions with the following inequality for all $u>1$ and $0\leq c\leq 1$:

$$\ln\left(\frac{c+u}{cu+1}\right)\geqslant\frac{(1-c^2)\left(u^2-1\right)}{c^2\left(u^2+1\right)+4cu+u^2+1}. \tag{A.43}$$

Using the inequality $\frac{2\theta}{2+\theta}\leqslant\ln(1+\theta)$ that is valid for $\theta\geq 0$ [121], it suffices to show that

$$\frac{2\left(\frac{c+u}{cu+1}-1\right)}{2+\frac{c+u}{cu+1}-1}-\frac{(1-c^2)\left(u^2-1\right)}{c^2\left(u^2+1\right)+4cu+u^2+1}\geqslant 0 \tag{A.44}$$

which is equivalent to

$$\frac{(1-c)^3(u-1)^3}{(c+1)(u+1)\left(c^2\left(u^2+1\right)+4cu+u^2+1\right)}\geqslant 0. \tag{A.45}$$

The last inequality is satisfied by all u and c with $u>1$ and $0\leq c\leq 1$. For $x=0.5$ the functions are constants, so convexity also follows for this case. Hence, convexity of $g(H_b^{-1}(\nu))$ in ν is established for independent BSCs.

A.5. On A Lower Bound for Binary Asymmetric Channels

Consider the Markov chain $U-X-Y_1$, a binary random variable X with the probability distribution Q_X, and a binary channel $P_{Y_1|X}$ with probability transition matrix

$$T=\begin{bmatrix} a & 1-a\\ b & 1-b\end{bmatrix} \tag{A.46}$$

which is asymmetric if $a{+}b\neq 1$. One can restrict attention to the cases $a{+}b\leq 1$ and $a\geq b$ by swapping the outputs and inputs, respectively, if necessary [95]. The conditional entropies $H(X|U)$ and $H(Y_1|U)$ are as defined in (4.10) and (4.11), respectively. Since the convexity property is satisfied for all binary channels $P_{Y_1|X}$ (see Section 4.3), we have the following lower bound due to Lemma 4.3:

$$H(Y_1|U)\geq H_b\Big(aH_b^{-1}(H(X|U))+b\Big(1-H_b^{-1}(H(X|U))\Big)\Big). \tag{A.47}$$

Note that if $a=b$, then (A.47) does not depend on $H(X|U)$, since the channel would then have zero capacity.

Consider the achievability of the bound in (A.47) for the model considered in [12, Theorem 1], where a ternary U suffices to evaluate the key-leakage-storage region. For a channel $P_{X|U}$ with probability transition matrix

$$T_u = \begin{bmatrix} a_u & 1-a_u \\ b_u & 1-b_u \\ c_u & 1-c_u \end{bmatrix} \tag{A.48}$$

we obtain

$$H(X|U) = P_U(u_0)H_b(a_u)+P_U(u_1)H_b(b_u)+P_U(u_2)H_b(c_u) \tag{A.49}$$

and

$$\begin{aligned} H(Y_1|U) = {} & P_U(u_0)H_b(aa_u+b(1-a_u)) \\ & + P_U(u_1)H_b(ab_u+b(1-b_u)) + P_U(u_2)H_b(ac_u+b(1-c_u)) \end{aligned} \tag{A.50}$$

where $P_U(u_2)=1-P_U(u_0)-P_U(u_1)$ and

$$P_U(u_1)=\frac{P_X(0)-c_u-P_U(u_0)(a_u-c_u)}{b_u-c_u}. \tag{A.51}$$

Figure A.1 shows the possible $(H(X|U),\ H(Y_1|U))$ pairs by assigning an appropriate set of values to the first column of T_u and to $P_U(u_0)$ for a uniform X and an asymmetric binary channel $P_{Y_1|X}$ with parameters $a=0.4$ and $b=0.2$. The convexity lower bound in Figure A.1 is thus not tight for such an asymmetric binary channel. Our simulations suggest that this is the case for all asymmetric channels, except for special cases like $a=b$.

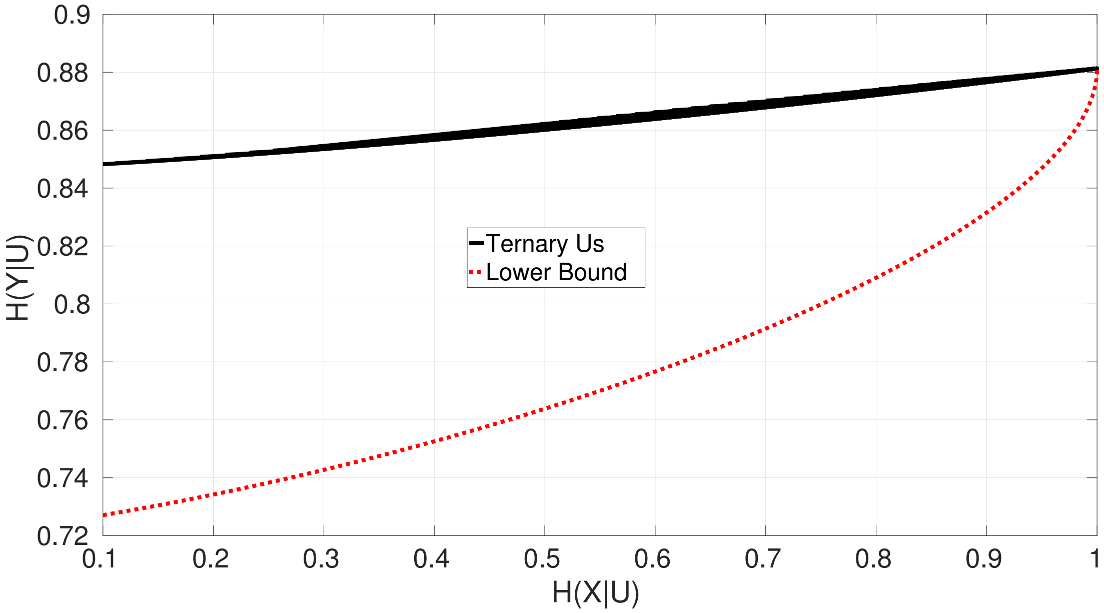

Figure A.1.: Comparison of the lower bound and possible choices of U for a uniform input and a binary channel $P_{Y_1|X}$ with parameters $a=0.4$ and $b=0.2$ in (A.46).

B

Appendices for Chapter 5

B.1. Strong Secrecy

Theorem B.1. For the GS model (or CS model), given any $\epsilon > 0$, there exist some $n \geq 1$, an encoder, and a decoder that achieve the key-leakage-storage region $\mathcal{R}_1'$ (or $\mathcal{R}_2'$) and that satisfy the strong-secrecy constraint (5.14).

We prove Theorem B.1 for the GS model by using two approaches; the first proof uses output statistics of random binning (OSRB) [122] and the second uses resolvability [123] and a likelihood encoder [124]. The proofs for the CS model follow by applying a one-time pad step, as in Section 5.2.3.

Proof Sketch 1. We first give a random binning based proof by following the steps in [122]. Fix a $P_{U|X}$ and let (U^n, X^n, Y^n) be i.i.d. according to $P_{U|X}P_XP_{Y|X}$. For each u^n, assign three random bin indices $S \in [1 : 2^{nR_s}]$, $W \in [1 : 2^{nR_w}]$, and $C \in [1 : 2^{nR_c}]$, which represent, respectively, the secret key, helper data, and randomness shared by the encoder, decoder, and eavesdropper (similar to W).

We use a SW decoder to estimate $\widehat{U}^n$ from (C, W, Y^n), which satisfies (4.2) if (see [122, Lemma 1])

$$R_w + R_c > H(U|Y). \tag{B.1}$$

We further have that (S, W, C) are almost mutually independent and uniform so that (4.5) and (5.14) are satisfied if we have (see [122, Theorem 1])

$$R_s + R_w + R_c < H(U). \tag{B.2}$$

Similarly, the shared randomness C is almost independent of X^n, suggesting that it is almost independent of Y^n also, if

$$R_c < H(U|X). \tag{B.3}$$

Applying Fourier-Motzkin elimination [125, Section 12.2] to (B.1)-(B.3) and following a similar privacy-leakage rate analysis as in Theorem 5.3, there exists a binning with a fixed value of C and that achieves all rate tuples (R_s, R_ℓ, R_w) in the key-leakage-storage region $\mathcal{R}'_1$ with strong secrecy. □

Proof Sketch 2. We next give a random coding based proof by following the steps in [124] and [126, Section 1.6.2]. Consider the allied channel coding problem where $S \in [1:2^{nR_s}]$ and $W \in [1:2^{nR_w}]$ are uniform and independent inputs of an encoder $\mathsf{Enc}(\cdot)$ with the output codeword U^n that passes through a channel $P_{X|U}$ to obtain X^n, which further passes through the channel $P_{Y|X}$ to obtain Y^n. Applying the resolvability result from [123, Theorem 1], one can simulate $X^n \sim \prod_{i=1}^n P_X(x_i)$ if

$$R_s + R_w > I(U;X). \tag{B.4}$$

Furthermore, one can reliably estimate $\widehat{U}^n$ from (W, Y^n) if

$$R_s < I(U;Y). \tag{B.5}$$

Note that this channel coding problem defines a joint probability distribution

$$\begin{aligned}&\widetilde{P}_{SWX^nY^n}(s,w,x^n,y^n)\\ &= \text{Unif}\,[1\!:\!|\mathcal{S}|](s)\text{Unif}\,[1\!:\!|\mathcal{W}|](w)\mathbb{1}\{x^n\!=\!\mathsf{Enc}(w,s)\}\prod_{i=1}^n P_{Y|X}(y_i|x_i)\end{aligned} \tag{B.6}$$

where Unif$\,[1:|\mathcal{S}|]$ and Unif$\,[1:|\mathcal{W}|]$ are uniform probability distributions over the sets, respectively, $\mathcal{S} = [1:2^{nR_s}]$ and $\mathcal{W} = [1:2^{nR_w}]$, and $\mathbb{1}\{\cdot\}$ is the indicator function.

However, for the original problem, we should invert the random coding and use a stochastic encoder according to the conditional probability distribution $\widetilde{P}_{SW|X^n}$ obtained from (B.6), which is induces a joint distribution

$$P_{SWX^nY^n}(s,w,x^n,y^n) = \widetilde{P}_{SW|X^n}(s,w|x^n)\prod_{i=i}^n P_X(x_i)P_{Y|X}(y_i|x_i). \tag{B.7}$$

It follows from the above channel coding problem that (4.2), (4.5), (4.6), and (5.14) are satisfied. Following similar privacy-leakage rate analysis as in Theorem 5.3, there exist some $n \geq 1$, an encoder, and a decoder that achieve all rate tuples (R_s, R_ℓ, R_w) in the key-leakage-storage region $\mathcal{R}'_1$ with strong secrecy. □

Remark B.1. Since resolvability can be achieved by a random linear code (RLC) construction [127] for binary input channels $P_{X|U}$, one can use the decoder for such an RLC during enrollment to obtain the bins (S, W) with strong secrecy. Note that a binary U is optimal for the rate regions $\mathcal{R}_1'$ and $\mathcal{R}_2'$ if, e.g., $P_{Y|X}$ can be decomposed into a mixture of BSCs; see Section 4.3.

Remark B.2. In [128, Theorem 10], a polar code construction based on OSRB is shown to be optimal for the GS model with strong secrecy. This construction requires chains of identifier-outputs, each of which has size n, and a secret seed shared between the encoder and decoder. Furthermore, the constructions used in Proofs 1 and 2 of Theorem B.1 are stochastic and such code constructions do not seem to be practical.

B.2. Extensions to Hidden Sources with Multiple Decoder Measurements

In Chapter 4, the encoder measures a noisy version $\widetilde{X}^n$ of a hidden, or remote, identifier source X^n rather than the source itself. This is a more general model than the visible source model assumed in Chapter 5. The key-leakage-storage regions $\mathcal{R}_1$ and $\mathcal{R}_2$ that satisfy (4.2)-(4.6) for the GS and CS models with a hidden source are given, respectively, in Theorems 4.1 and 4.2.

Suppose next the encoder measures a binary hidden source X^n through a channel $P_{\widetilde{X}|X}$ such that the inverse channel $P_{X|\widetilde{X}}$ is a BSC, and the decoder measures the source through a channel $P_{Y|X}$ that is a BSC. Using Theorem 4.5, we next argue the optimality of the first WZ-coding construction given in Section 5.4 for the GS and CS models with the hidden source model considered.

Theorem B.2. The WZ-coding construction given in Section 5.4 achieves the regions $\mathcal{R}_1$ and $\mathcal{R}_2$ for a uniform source X^n, an inverse channel $P_{X|\widetilde{X}}$ that is a BSC, and a decoder-measurement channel $P_{Y|X}$ that is also a BSC.

Proof. We first modify the WZ-coding construction in Section 5.4 by defining the new error sequence

$$\widetilde{E}_q^n = \widetilde{X}^n \oplus \widetilde{X}_q^n \tag{B.8}$$

which resembles an i.i.d. sequence $\sim \text{Bern}^n(q)$ for some $q \in [0, 0.5]$ when $\widetilde{X}_q^n$ is the closest codeword of $\mathcal{C}_1$ to $\widetilde{X}^n$ in Hamming distance and $n \to \infty$. The new error sequence represents the BSCs $P_{\widetilde{X}|U}$ since the new common randomness $\widetilde{X}_q^n$ asymptotically represents the auxiliary random variable U^n. Therefore, we asymptotically obtain i.i.d. channels $P_{\widetilde{X}|U} \sim \text{BSC}(q)$. It follows from Theorem 4.5 that applying the code construction and taking a union of the rate tuples achieved over all $q \in [0, 0.5]$, we can achieve the boundary points of $\mathcal{R}_1$ and $\mathcal{R}_2$. □

Remark B.3. Applying additional information reconciliation and privacy amplification steps to multiple blocks of identifier outputs, as in Remark 5.2, can improve the weak-secrecy results to strong-secrecy results also for hidden sources. Alternatively, random binning and random coding based approaches can be applied, as in Theorem B.1, to show that there exist code constructions that provide strong secrecy for the GS and CS models with a hidden source.

C

Appendices for Chapter 6

C.1. Proofs of Rate Regions

Based on the condition that all sequences are jointly typical with high probability, we bound some conditional entropy terms of interest with single letter expressions using the following two lemmas.

Lemma C.1 ([113])**.** Let (X^n, A^n) be jointly typical with high probability and Z^n i.i.d. $\sim P_{Z|XA}$, we have $H(Z^n|X^n, A^n) \geq n(H(Z|X, A) - \delta_\epsilon)$, where $\delta_\epsilon \to 0$ as $\epsilon \to 0$ and $\epsilon \to 0$ as $n \to \infty$.

Lemma C.2 ([113])**.** Let (A^n, U^n, Z^n) be jointly typical with high probability and $\mathcal{C}_n$ represent a random codebook generated according to $\prod_{i=1}^n P_{U|A}(u_i|a_i)$. Then, $H(Z^n|A^n, U^n, \mathcal{C}_n) \leq n(H(Z|A, U) + \delta_\epsilon)$, where $\delta_\epsilon \to 0$ as $\epsilon \to 0$ and $\epsilon \to 0$ as $n \to \infty$.

C.2. Proof for $\mathcal{R}_{gs}$

C.2.1. Proof of Achievability

The proof follows from standard random coding arguments where we show the existence of a code that satisfies the key, privacy-leakage, and storage rate, and expected cost constraints; see also [19].

Codebook generation: Fix $P_{A|X} P_{V|XA} P_{U|V}$ such that $\mathbb{E}[\Gamma(A)] \leq C + \epsilon$.

- Randomly and independently generate $2^{n(I(X;A)+\delta_\epsilon)}$ codewords $a^n(w_a)$ according to $\prod_{i=1}^n P_A(a_i(w_a))$ for $w_a \in [1 : 2^{n(I(X;A)+\delta_\epsilon)}]$.

- For each w_a, randomly and conditionally independently generate $2^{n(I(U;X|A)+\delta_\epsilon)}$ codewords $u^n(w_a, m)$ each according to $\prod_{i=1}^n P_{U|A}(u_i|a_i(w_a))$ for $m \in [1 : 2^{n(I(U;X|A)+\delta_\epsilon)}]$, and distribute them uniformly at random into $2^{n(I(U;X|A)-I(U;Y|A)+2\delta_\epsilon)}$ bins $b_U(w_u)$ for $w_u \in [1 : 2^{n(I(U;X|A)-I(U;Y|A)+2\delta_\epsilon)}]$. Without loss of generality, we can identify the index $m = (w_u, m')$ for some $m' \in [1 : 2^{n(I(U;Y|A)-\delta_\epsilon)}]$.

- ▷ For each (w_a, m) pair, randomly and conditionally independently generate $2^{n(I(V;X|A,U)+\delta_\epsilon)}$ codewords $v^n(w_a, m, l)$ each according to $\prod_{i=1}^n P_{V|UA}(v_i|u_i(w_a, m), a_i(w_a))$ for $l \in [1 : 2^{n(I(V;X|A,U)+\delta_\epsilon)}]$, and distribute them uniformly at random into $2^{n(I(V;X|A,U)-I(V;Y|A,U)+3\delta_\epsilon)}$ bins $b_V(m, w_v)$ for $w_v \in [1 : 2^{n(I(V;X|A,U)-I(V;Y|A,U)+3\delta_\epsilon)}]$. Furthermore, for each bin, we divide codewords v^n into $2^{n(I(V;Y|A,U)-I(V;Z|A,U)-\delta_\epsilon)}$ equal-sized subbins, each denoted by a subbin index w_s. Without loss of generality, we can identify the index $l = (w_v, w_s, l')$ for some $l' \in [1 : 2^{n(I(V;Z|A,U)-\delta_\epsilon)}]$.

The codebook is revealed to all parties.

Encoding:

- ▷ For a given source sequence x^n, the encoder looks for a $a^n(w_a)$ which is jointly typical with x^n. Since there are more than $2^{nI(X;A)}$ codewords a^n, by the covering lemma [103], there exists such an a^n with high probability. If there are more than one, we choose one uniformly at random and send the corresponding index w_a to the decoder.
- ▷ The encoder then looks for a $u^n(w_a, m)$ that is jointly typical with (x^n, a^n). Since there are more than $2^{nI(U;X|A)}$ codewords u^n, by the covering lemma, there exists such a u^n with high probability. If there are more than one, we choose one uniformly at random and send the corresponding bin index w_u to the decoder.
- ▷ Again, the encoder looks for a $v^n(w_a, m, l)$ which is jointly typical with (x^n, a^n, u^n). Since there are more than $2^{nI(V;X|A,U)}$ codewords v^n, by the covering lemma, there exists such a v^n with high probability. If there are more than one, we choose one uniformly at random and send the corresponding bin index w_v to the decoder. The secret key s is chosen to be the subbin index w_s of the chosen codeword v^n.

This gives the total storage rate of

$$\begin{aligned} &I(X;A) + [I(U;X|A) - I(U;Y|A)] + [I(V;X|A,U) - I(V;Y|A,U)] + 6\delta_\epsilon \\ &\qquad = I(X;A) + I(V;X|A,Y) + 6\delta_\epsilon. \end{aligned} \tag{C.1}$$

Once the action sequence is chosen, action-dependent side information (y^n, z^n) is generated as the output of the memoryless channel $P_{YZ|XA}$.

Decoding:

- ▷ Upon receiving the indices (w_a, w_u, w_v) and side information y^n, the decoder looks for the unique u^n which is jointly typical with (y^n, a^n). Since there are less than $2^{nI(U;Y|A)}$ sequences in the bin $b_U(w_u)$, by the packing lemma [103], it will find the unique and correct u^n with high probability.

- ▷ Then, the decoder looks for the unique v^n which is jointly typical with (y^n, a^n, u^n). Since there are less than $2^{nI(V;Y|A,U)}$ sequences in the bin $b_V(m, w_v)$, by the packing lemma, it will find the unique and correct v^n with high probability. The decoder puts out $\hat{s}$ as the subbin index $\hat{w}_s$ of the decoded codeword v^n which will be the correct one with high probability.

Action Cost: Since each action sequence a^n is in the typical set with high probability, by the typical average lemma [103], the expected cost constraint is satisfied.

Privacy-leakage Rate: The information leakage averaged over the random codebook $\mathcal{C}_n$ can be bounded as

$$\begin{aligned}
&I(X^n; W_a, W_u, W_v, Z^n|\mathcal{C}_n)\\
&\leq I(X^n; W_a, M, W_v, Z^n|\mathcal{C}_n)\\
&= H(X^n|\mathcal{C}_n) - H(X^n, W_a, M, W_v, Z^n|\mathcal{C}_n) + H(W_a, M, W_v|\mathcal{C}_n) + H(Z^n|W_a, M, W_v, \mathcal{C}_n)\\
&= -H(Z^n|X^n, \mathcal{C}_n) - H(W_a, M, W_v|X^n, Z^n, \mathcal{C}_n) + H(W_a, M, W_v|\mathcal{C}_n) + H(Z^n|W_a, M, W_v, \mathcal{C}_n)\\
&\overset{(a)}{\leq} -H(Z^n|X^n, A^n) + H(W_a, M, W_v|\mathcal{C}_n) + H(Z^n|W_a, M, W_v, \mathcal{C}_n)\\
&\overset{(b)}{\leq} -H(Z^n|X^n, A^n) + H(W_a|\mathcal{C}_n) + H(M|\mathcal{C}_n) + H(W_v|\mathcal{C}_n) + H(Z^n|A^n, U^n, \mathcal{C}_n)\\
&\overset{(c)}{\leq} n[-H(Z|X, A) + I(X; A) + I(U; X|A) + 5\delta_\epsilon\\
&\quad + (I(V; X|A, U) - I(V; Y|A, U)) + H(Z|A, U)]\\
&\overset{(d)}{=} n[I(X; A, V, Y) - I(X; Y|A, U) + I(X; Z|A, U) + \delta'_\epsilon]\\
&\leq n[R_\ell + \delta'_\epsilon] \qquad\qquad \text{(C.2)}
\end{aligned}$$

if $R_\ell \geq I(X; A, V, Y) - (I(X; Y|A, U) - I(X; Z|A, U))$, where (a) follows because conditioning cannot increase entropy, and because $Z^n - (X^n, A^n) - \mathcal{C}_n$ forms a Markov chain, (b) follows because given the codebook, (A^n, U^n) are functions of (W_a, M), (c) follows from the codebook generation, from the memoryless properties of the source and the side information channel, from Lemma C.1 with which we bound the term $H(Z^n|X^n, A^n)$, and from Lemma C.2 with which we bound the term $H(Z^n|A^n, U^n, \mathcal{C}_n)$, and (d) follows from the Markov chain $(Y, Z) - (X, A) - V - U$.

Secrecy-leakage Rate: The secrecy-leakage rate averaged over the random codebook $\mathcal{C}_n$ can be bounded as

$$\begin{aligned}
&I(W_s; W_a, W_u, W_v, Z^n|\mathcal{C}_n)\\
&\leq H(W_s|\mathcal{C}_n) - H(W_s|W_a, M, W_v, Z^n, \mathcal{C}_n)\\
&= H(W_s|\mathcal{C}_n) - H(W_a, M, L, Z^n|\mathcal{C}_n) + H(L'|W_a, M, W_v, W_s, Z^n, \mathcal{C}_n) + H(W_a, M, W_v, Z^n|\mathcal{C}_n)\\
&\overset{(a)}{\leq} H(W_s|\mathcal{C}_n) - H(A^n, U^n, V^n, Z^n|\mathcal{C}_n) + n\epsilon_n + H(W_a|\mathcal{C}_n) + H(M|\mathcal{C}_n) + H(W_v|\mathcal{C}_n)\\
&\qquad + H(Z^n|A^n, U^n, \mathcal{C}_n)
\end{aligned}$$

$$\begin{aligned}
&\overset{(b)}{\leq} H(W_s|\mathcal{C}_n) - H(A^n, U^n, V^n, Z^n|\mathcal{C}_n) + n\epsilon_n + n(I(X;A) + I(U;X|A)\\
&\qquad + I(V;X|A,U,Y) + H(Z|A,U) + \delta'_\epsilon)\\
&\overset{(c)}{\leq} n\delta_\epsilon^{(2)} \qquad\qquad \text{(C.3)}
\end{aligned}$$

where (a) follows because, given the codebook, (A^n, U^n) are functions of (W_a, M) and V^n of (W_a, M, L), and from Fano's inequality where, given (W_a, M, W_v, W_s, Z^n), the codeword V^n and thus L' can be decoded correctly with high probability since there are less than $2^{nI(V;Z|A,U)}$ remaining V^n, (b) follows from the codebook generation and Lemma C.2, and (c) follows from the codebook generation, from the bound on $H(A^n, U^n, V^n, Z^n|\mathcal{C}_n)$ which is shown below, and from the Markov chain $U - V - (X, A) - (Y, Z)$. We have

$$\begin{aligned}
&H(A^n, U^n, V^n, Z^n|\mathcal{C}_n)\\
&\overset{(a)}{=} H(A^n, U^n, V^n, X^n|\mathcal{C}_n) + H(Z^n|X^n, A^n) - H(X^n|A^n, U^n, V^n, Z^n, \mathcal{C}_n)\\
&\geq H(X^n) + H(Z^n|X^n, A^n) - H(X^n|A^n, U^n, V^n, Z^n, \mathcal{C}_n)\\
&\overset{(b)}{\geq} n(H(X) + H(Z|X,A) - H(X|A,U,V,Z) - \delta'_\epsilon)
\end{aligned}$$

where (a) follows from the Markov chain $Z^n - (X^n, A^n) - (U^n, V^n, \mathcal{C}_n)$ and (b) follows from Lemma C.1 and from a bound on $H(X^n|A^n, U^n, V^n, Z^n, \mathcal{C}_n)$ which can be derived similarly as in Lemma C.2.

Secret-key Rate: The key rate averaged over the random codebook $\mathcal{C}_n$ can be bounded as follows:

$$\begin{aligned}
&H(W_s|\mathcal{C}_n) \geq H(W_s|W_a, M, W_v, L', \mathcal{C}_n)\\
&\overset{(a)}{\geq} H(A^n, U^n, V^n|\mathcal{C}_n) - H(W_a|\mathcal{C}_n) - H(M|\mathcal{C}_n) - H(W_v|\mathcal{C}_n) - H(L'|\mathcal{C}_n)\\
&\overset{(b)}{\geq} n(I(X;A,U,V) - I(X;A) - I(U;X|A) - I(V;X|A,U,Y) - I(V;Z|A,U) - \delta'_\epsilon)\\
&= n(I(V;Y|A,U) - I(V;Z|A,U) - \delta'_\epsilon) \geq n(R_s - \delta'_\epsilon) \qquad\qquad \text{(C.4)}
\end{aligned}$$

if $R_s \leq I(V;Y|A,U) - I(V;Z|A,U)$, where (a) follows from the fact that given the codebook (A^n, U^n, V^n) are functions of (W_a, M, L), (b) follows from the codebook generation, from the bound $P_{A^nU^nV^n}(a^n, u^n, v^n) = \sum_{x^n \in \mathcal{T}_\epsilon(X|a^n,u^n,v^n)} P_{X^n}(x^n) \leq 2^{-n(I(X;A,U,V)-\delta_\epsilon)}$, and from the Markov chain $V - (X, A, U) - Y$.

Using the selection lemma [100, Lemma 2.2], we have that a tuple (R_s, R_ℓ, R_w, C) that satisfies (6.7)-(6.9) with $\widetilde{X} = X$ for some $P_{A|X}$, $P_{V|XA}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)] \leq C$ is achievable.

C.2.2. Proof of Converse

Let $U_i \triangleq (W, A^{n\setminus i}, Y_{i+1}^n, Z^{i-1})$ and $V_i \triangleq (W, S, A^{n\setminus i}, Y_{i+1}^n, Z^{i-1})$, which satisfy the Markov chain $U_i - V_i - (A_i, X_i) - (Y_i, Z_i)$ for all $i = 1, 2, \ldots, n$. For any achievable tuple (R_s, R_ℓ, R_w, C), we have the following.

Storage Rate: We obtain

$$\begin{aligned}
&n(R_w+\delta_n) \geq \log|\mathcal{W}| \geq H(W)\\
&\overset{(a)}{=} H(W) + H(A^n|W) = H(A^n) + H(W|A^n)\\
&\geq [H(A^n) - H(A^n|X^n,Z^n)] + [H(W|A^n,Y^n) - H(W|A^n,X^n,Y^n,Z^n)]\\
&= H(X^n,Z^n) - H(X^n,Z^n|A^n) + H(X^n,Z^n|A^n,Y^n) - H(X^n,Z^n|A^n,Y^n,W)\\
&= H(X^n) + H(Z^n|X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) - H(Z^n|X^n,A^n)\\
&\qquad - H(X^n,Z^n|A^n,Y^n,W,S) - I(X^n,Z^n;S|A^n,Y^n,W)\\
&\geq H(X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) - H(X^n,Z^n|A^n,Y^n,W,S) - H(S|A^n,Y^n,W)\\
&\overset{(b)}{\geq} \sum_{i=1}^n H(X_i) - H(Y_i|A_i) + H(Y_i,Z_i|X_i,A_i) - H(X_i,Z_i|A^n,Y^n,W,S,X^{i-1},Z^{i-1}) - n\epsilon_n\\
&\overset{(c)}{\geq} \sum_{i=1}^n H(X_i) - H(Y_i|A_i) + H(Y_i|X_i,A_i,Z_i) + H(Z_i|X_i,A_i) - H(X_i,Z_i|A_i,Y_i,V_i) - n\epsilon_n\\
&\geq \sum_{i=1}^n I(X_i;A_i) + I(V_i;X_i|A_i,Y_i) - n\epsilon_n
\end{aligned} \tag{C.5}$$

where (a) follows from the deterministic action encoder, (b) follows from Fano's inequality, and (c) follows from the definition of V_i.

Privacy-leakage Rate: We have

$$\begin{aligned}
&n(R_\ell+\delta_n) \geq I(X^n;W,Z^n)\\
&= I(X^n;W) + I(X^n;Z^n|W)\\
&\overset{(a)}{=} I(X^n;W,A^n) + I(X^n;Z^n|W,A^n)\\
&= H(X^n) - H(X^n|W,S,A^n,Y^n) - I(X^n;S|W,A^n,Y^n) - I(X^n;Y^n|W,A^n) + I(X^n;Z^n|W,A^n)\\
&\overset{(b)}{\geq} \sum_{i=1}^n H(X_i) - H(X_i|W,S,A^n,Y^n,X^{i-1}) - H(Y_i|W,A^n,Y_{i+1}^n) + H(Y_i|X_i,A_i)\\
&\qquad + H(Z_i|W,A^n,Z^{i-1}) - H(Z_i|X_i,A_i) - n\epsilon_n\\
&\overset{(c)}{=} \sum_{i=1}^n H(X_i) - H(X_i|W,S,A^n,Y^n,X^{i-1},Z^{i-1}) - I(X_i;Y_i|A_i) + H(Y_i|A_i) + I(X_i;Z_i|A_i)\\
&\qquad - H(Z_i|A_i) - H(Y_i|W,A^n,Y_{i+1}^n) + H(Z_i|W,A^n,Z^{i-1}) - n\epsilon_n\\
&\overset{(d)}{\geq} \sum_{i=1}^n H(X_i) - H(X_i|V_i,A_i,Y_i) - I(X_i;Y_i|A_i) + H(Y_i|A_i) + I(X_i;Z_i|A_i) - H(Z_i|A_i)\\
&\qquad - H(Y_i|W,A^n,Y_{i+1}^n) + H(Z_i|W,A^n,Z^{i-1}) - n\epsilon_n
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} \underbrace{I(X_i;A_i,V_i,Y_i) - I(X_i;Y_i|A_i) + I(X_i;Z_i|A_i)}_{\triangleq P_i} + I(W,Y_{i+1}^n,A^{n\backslash i};Y_i|A_i)\\
&\quad - I(W,Z^{i-1},A^{n\backslash i};Z_i|A_i) - n\epsilon_n
\end{aligned}
$$

where (a) follows from the deterministic action encoder, (b) follows from Fano's inequality and the Markov chain $(W,S,A^{n\backslash i},X^{n\backslash i},Y_{i+1}^n,Z^{i-1}) - (A_i,X_i) - (Y_i,Z_i)$, (c) follows from the Markov chain $(X_i,W,S,A_i^n,Y_i^n) - (A^{i-1},X^{i-1}) - (Z^{i-1},Y^{i-1})$, and (d) follows from the definition of V_i and the deterministic action encoder.

By adding Csiszár sum identity [129, 130], i.e.,

$$
\sum_{i=1}^{n} I(Y_i;Z^{i-1}|A^n,W,Y_{i+1}^n) - I(Z_i;Y_{i+1}^n|A^n,W,Z^{i-1}) = 0
$$

to the right hand side, we get

$$
\begin{aligned}
n(R_\ell+\delta_n) &\geq \sum_{i=1}^{n} P_i + I(W,Y_{i+1}^n,Z^{i-1},A^{n\backslash i};Y_i|A_i) - I(W,Y_{i+1}^n,Z^{i-1},A^{n\backslash i};Z_i|A_i) - n\epsilon_n\\
&\overset{(a)}{=} \sum_{i=1}^{n} I(X_i;A_i,V_i,Y_i) - I(X_i;Y_i|A_i) + I(X_i;Z_i|A_i) + I(U_i;Y_i|A_i) - I(U_i;Z_i|A_i) - n\epsilon_n\\
&\overset{(b)}{=} \sum_{i=1}^{n} I(X_i;A_i,V_i,Y_i) - I(X_i;Y_i|U_i,A_i) + I(X_i;Z_i|U_i,A_i) - n\epsilon_n, \qquad \text{(C.6)}
\end{aligned}
$$

where (a) follows from the definitions of P_i and U_i and (b) from the Markov chain $U_i - (A_i,X_i) - (Y_i,Z_i)$.

Secret-key Rate: We obtain

$$
\begin{aligned}
&n(R_s-\delta_n) \leq H(S) \overset{(a)}{\leq} H(S|W,Z^n) + n\delta_n\\
&\overset{(b)}{=} H(S|W,A^n,Z^n) + n\delta_n\\
&\overset{(c)}{\leq} H(S|W,A^n,Z^n) - H(S|W,A^n,Y^n) + 2n\delta_n\\
&= \sum_{i=1}^{n} I(S;Y_i|W,A^n,Y_{i+1}^n) - I(S;Z_i|W,A^n,Z^{i-1}) + 2n\delta_n\\
&\overset{(d)}{=} \sum_{i=1}^{n} I(S;Y_i|W,A^n,Y_{i+1}^n,Z^{i-1}) - I(S;Z_i|W,A^n,Y_{i+1}^n,Z^{i-1}) + 2n\delta_n\\
&\overset{(e)}{=} \sum_{i=1}^{n} I(V_i;Y_i|A_i,U_i) - I(V_i;Z_i|A_i,U_i) + 2n\delta_n \qquad \text{(C.7)}
\end{aligned}
$$

where (a) follows by (6.2), (b) follows from the deterministic action encoder, (c) follows from Fano's inequality, (d) follows from Csiszár's sum identity, and (e) follows from the definitions of U_i and V_i.

Action Cost: We have

$$C+\delta_n \geq \mathbb{E}\Big[\Gamma(A^n)\Big] = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[\Gamma(A_i)\Big]. \tag{C.8}$$

Finally, we complete the proof by the standard time-sharing argument and letting $\delta_n \to 0$.

Cardinality Bounds: It can be shown by using the support lemma [83] that $\mathcal{U}$ should have $|\mathcal{X}||\mathcal{A}|-1$ elements to preserve P_{XA} and three more to preserve $H(X|U,V,A,Y)$, $I(X;Z|A,U)-I(X;Y|A,U)$, and $I(V;Y|A,U)-I(V;Z|A,U)$. Similarly, the cardinality $|\mathcal{V}|$ can be limited to at most $(|\mathcal{X}||\mathcal{A}|+2)(|\mathcal{X}||\mathcal{A}|+1)$.

C.3. Proof for $\mathcal{R}_{cs}$

C.3.1. Proof of Achievability

Fix $P_{A|X}$, $P_{V|XA}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)]\leq C+\epsilon$. We use the achievability proof of the GS model. Suppose the key $S'=W_{s'}$, generated as in the GS model, has the same cardinality as the chosen key $S=W_s$, i.e., $|\mathcal{S}'|=|\mathcal{S}|$. Consider an encoder $\mathsf{Enc}(\cdot)$ with inputs (X^n,S) and outputs $W=(S'+S,W')$, where W' is the helper data for the GS model, and a decoder $\mathsf{Dec}(\cdot)$ with inputs (Y^n,W) and output $\hat{S}=S'+S-\hat{S}'$, where the addition and subtraction operations are modulo-$|\mathcal{S}|$. The decoder of the GS model is used at the decoder to obtain $\hat{S}'$. Furthermore, the action encoder $\mathsf{Enc}_a(\cdot)$ takes W' as its input.

Error Probability: We have

$$\Pr[S\neq\hat{S}]=\Pr[S'\neq\hat{S}'] \tag{C.9}$$

which is small due to the proof of achievability for the GS model.

Action Cost: Similar to the GS model, one can show that the expected cost constraint is satisfied with high probability by using the typical average lemma.

Privacy-leakage Rate: We obtain

$$\begin{aligned}
&I(X^n;W_{a'},W_{u'},W_{v'},W_s+W_{s'},Z^n|\mathcal{C}_n)\\
&=I(X^n;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+I(X^n;W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\leq I(X^n;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+H(W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\qquad -H(W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,X^n,W_{s'},\mathcal{C}_n)\\
&\overset{(a)}{\leq} I(X^n;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+\log|\mathcal{S}|-H(W_s)\\
&\overset{(b)}{\leq} n[I(X;A,V,Y)-(I(X;Y|A,U)-I(X;Z|A,U))+\delta'_\epsilon]\\
&\leq n[R_\ell+\delta'_\epsilon]
\end{aligned} \tag{C.10}$$

if $R_\ell \geq I(X;A,V,Y)-(I(X;Y|A,U)-I(X;Z|A,U))$, where (a) follows because the chosen key $S=W_s$ is independent of $(W_{a'},W_{u'},W_{v'},Z^n,X^n,W_{s'},\mathcal{C}_n)$ and (b) follows from uniformity of W_s and (C.2).

Secrecy-leakage Rate: Observe that

$$\begin{aligned}
&I(W_s;W_{a'},W_{u'},W_{v'},W_s+W_{s'},Z^n|\mathcal{C}_n)\\
&=I(W_s;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+I(W_s;W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\overset{(a)}{=}H(W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)-H(W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\leq\log|\mathcal{S}|-H(W_{s'})+I(W_{s'};W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)\\
&\overset{(b)}{\leq}n(\delta_n+\delta_\epsilon^{(2)})
\end{aligned}\tag{C.11}$$

where (a) follows because $S=W_s$ is independent of $(W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)$ and (b) follows by (C.3) and (C.4).

Secret-key Rate: We have

$$\begin{aligned}
&H(W_s|\mathcal{C}_n)=\log|\mathcal{S}|\geq H(W_{s'}|\mathcal{C}_n)\\
&\overset{(a)}{\geq}n(I(V;Y|A,U)-I(V;Z|A,U)-\delta_\epsilon')\geq n(R_s-\delta_\epsilon')
\end{aligned}\tag{C.12}$$

if $R_s\leq I(V;Y|A,U)-I(V;Z|A,U)$, where (a) follows by (C.4).

Storage Rate: The storage rate is the sum of the storage $R_{w'}$ for the GS model and for $S'+S$. We obtain

$$\begin{aligned}
&R_w\leq R_{w'}+\frac{1}{n}\log|\mathcal{S}|\\
&\overset{(a)}{=}I(X,A)+I(V;X|A,Y)+6\delta_\epsilon+R_s\\
&\overset{(b)}{\leq}I(X,A)+I(V;X|A,Y)+6\delta_\epsilon+I(V;Y|A,U)-I(V;Z|A,U)\\
&\overset{(c)}{=}I(X;A,V)-I(U;Y|A)-I(V;Z|A,U)+6\delta_\epsilon
\end{aligned}\tag{C.13}$$

where (a) follows from the storage rate of the GS model, (b) follows by (C.12), and (c) follows from the Markov chain $U-V-(X,A)-(Y,Z)$.

Using the selection lemma, we have that a tuple (R_s,R_ℓ,R_w,C) that satisfies (6.12)-(6.14) with $\widetilde{X}=X$ for some $P_{A|X}$, $P_{V|XA}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)]\leq C$ is achievable.

C.3.2. Proof of Converse

Use the definitions of U_i and V_i given in Appendix C.2.2 so that $U_i-V_i-(A_i,X_i)-(Y_i,Z_i)$ forms a Markov chain for all $i=1,2,\dots,n$. The main step is the proof of converse for the storage rate.

Secret-key Rate: Use similar steps as in (C.7) to obtain

$$R_s \le \frac{1}{n}\Big[\sum_{i=1}^{n} I(V_i;Y_i|A_i,U_i) - I(V_i;Z_i|A_i,U_i) + 3n\delta_n\Big]. \tag{C.14}$$

Action Cost: Similar to Appendix C.2.2, we obtain (C.8) for the expected cost constraint.

Privacy-leakage Rate: We apply similar steps as in Appendix C.2.2 and obtain

$$R_\ell \ge \frac{1}{n}\Big[\sum_{i=1}^{n} I(X_i;V_i,A_i,Y_i) - I(X_i;Y_i|U_i,A_i) + I(X_i;Z_i|U_i,A_i) - n\epsilon_n - n\delta_n\Big]. \tag{C.15}$$

Storage Rate: We have

$$\begin{aligned}
&n(R_w+\delta_n) \ge \log|\mathcal{W}| \ge H(W)\\
&\overset{(a)}{=} H(W) + H(A^n|W) = H(A^n) + H(W|A^n)\\
&\overset{(b)}{\ge} H(A^n) - H(A^n|X^n,Z^n) + H(A^n|X^n,Z^n) + H(W|A^n,Y^n) - H(W|A^n,X^n,Y^n,Z^n)\\
&\qquad + H(W|A^n,X^n)\\
&= H(X^n,Z^n) - H(X^n,Z^n|A^n) + H(A^n|X^n,Z^n) + H(X^n,Z^n|A^n,Y^n)\\
&\qquad - H(X^n,Z^n|A^n,Y^n,W) + H(W|A^n,X^n)\\
&= H(X^n) + H(Z^n|X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) - H(Z^n|X^n,A^n)\\
&\qquad + H(A^n|X^n,Z^n) - H(X^n,Z^n|A^n,Y^n,W,S) - I(X^n,Z^n;S|A^n,Y^n,W) + H(W|A^n,X^n)\\
&= H(X^n) + I(Z^n;A^n|X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) + H(A^n|X^n,Z^n)\\
&\quad - H(X^n,Z^n|A^n,Y^n,W,S) - H(S|A^n,Y^n,W) + H(S|A^n,Y^n,W,X^n,Z^n) + H(W|A^n,X^n)\\
&\overset{(c)}{=} H(X^n) + H(W,A^n,S|X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n)\\
&\qquad - H(X^n,Z^n|A^n,Y^n,W,S) - H(S|A^n,Y^n,W)\\
&\overset{(d)}{\ge} H(X^n) + H(S) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) - H(X^n,Z^n|A^n,Y^n,W,S) - H(S|A^n,Y^n,W)\\
&\ge H(X^n) - H(Y^n|A^n) + H(Y^n,Z^n|X^n,A^n) - H(X^n,Z^n|A^n,Y^n,W,S) + H(S|A^n,Z^n,W)\\
&\qquad - H(S|A^n,Y^n,W)\\
&\ge \sum_{i=1}^{n} H(X_i) - H(Y_i|A_i) + H(Y_i,Z_i|X_i,A_i) - H(X_i,Z_i|A^n,Y^n,W,S,X^{i-1},Z^{i-1})\\
&\qquad + I(S;Y_i|W,A^n,Y_{i+1}^n) - I(S;Z_i|W,A^n,Z^{i-1})\\
&\overset{(e)}{=} \sum_{i=1}^{n} H(X_i) - H(Y_i|A_i) + H(Y_i,Z_i|X_i,A_i) - H(X_i,Z_i|A^n,Y^n,W,S,X^{i-1},Z^{i-1})\\
&\qquad + I(S;Y_i|W,A^n,Y_{i+1}^n,Z^{i-1}) - I(S;Z_i|W,A^n,Y_{i+1}^n,Z^{i-1})
\end{aligned}$$

$$
\begin{aligned}
&\overset{(f)}{\geq} \sum_{i=1}^{n} H(X_i) - H(Y_i|A_i) + H(Y_i|X_i, A_i, Z_i) + H(Z_i|X_i, A_i) - H(X_i, Z_i|A_i, Y_i, V_i)\\
&\qquad + I(V_i; Y_i|A_i, U_i) - I(V_i; Z_i|A_i, U_i)\\
&\geq \sum_{i=1}^{n} I(X_i; A_i) + I(V_i; X_i|Y_i, A_i) + I(V_i; Y_i|A_i, U_i) - I(V_i; Z_i|A_i, U_i)\\
&\overset{(g)}{=} \sum_{i=1}^{n} I(X_i; A_i, V_i) - I(U_i; Y_i|A_i) - I(V_i; Z_i|A_i, U_i)
\end{aligned}
$$

where (a) follows from the deterministic action encoder, (b) follows from the Markov chain $W - (A^n, X^n) - (Y^n, Z^n)$, (c) follows from the Markov chain $(S, W) - (A^n, X^n) - (Y^n, Z^n)$, (d) follows because the chosen key S is independent of X^n, and (e) follows from Csiszár's sum identity. We use the definitions of U_i and V_i in (f), and (g) follows because $U_i - V_i - (A_i, X_i) - (Y_i, Z_i)$ forms a Markov chain for all $i = 1, 2, \dots, n$.

The converse follows by applying the standard time-sharing argument and letting $\delta_n \to 0$.

Cardinality Bounds: We use the support lemma and should satisfy the Markov condition $U - V - (A, X) - (Y, Z)$. We therefore preserve P_{XA} by using $|\mathcal{X}||\mathcal{A}| - 1$ elements. The bound in (6.14) with $\widetilde{X} = X$ for the storage rate can be written as

$$
\begin{aligned}
&I(X; A, V) - I(U; Y|A) - I(V; Z|A, U)\\
&= I(X; A) + I(V; X|A, Y) + I(V; Y|A, U) - I(V; Z|A, U).
\end{aligned}
$$

We thus have to preserve three more expressions, i.e., $I(V; Y|A, U) - I(V; Z|A, U)$, $H(X|U, V, A, Y)$, and $I(X; Z|A, U) - I(X; Y|A, U)$. One can therefore preserve all expressions in $\mathcal{R}_{cs}$ by using an auxiliary random variable U with $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{A}| + 2$ and, similarly, V with $|\mathcal{V}| \leq (|\mathcal{X}||\mathcal{A}| + 2)(|\mathcal{X}||\mathcal{A}| + 1)$.

C.4. Proof of Theorem 6.1

C.4.1. Proof of Achievability

Consider the codebook generation, encoding, and decoding steps of the GS model with a visible source. Fix $P_{A|\widetilde{X}}$, $P_{V|\widetilde{X}A}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)] \leq C + \epsilon$.

We apply the steps in Appendix C.2.1 after replacing every X with $\widetilde{X}$ and every realization x^n with $\tilde{x}^n$. These replacements guarantee that $(\widetilde{X}^n, A^n, U^n, V^n, Y^n)$ are jointly typical with high probability due to standard arguments used in Appendix C.2.1 for error analysis. The Markov lemma [103] then ensures that $(X^n, \widetilde{X}^n, A^n, U^n, V^n, Y^n)$ are also jointly typical with high probability.

Action Cost: The typical average lemma shows that the expected cost constraint is satisfied with high probability.

Storage Rate: After replacing X with $\widetilde{X}$ in Appendix C.2.1, the total storage rate in this case is $R_w = I(\widetilde{X}, A) + I(V;\widetilde{X}|A,Y) + 6\delta_\epsilon$ because $U - V - (A,\widetilde{X}) - (A,X) - (Y,Z)$ forms a Markov chain.

Privacy-leakage Rate: Consider the leakage about the hidden source averaged over the random codebook $\mathcal{C}_n$:

$$
\begin{aligned}
&I(X^n;W_a,W_u,W_v,Z^n|\mathcal{C}_n) \leq I(X^n;W_a,W_u,M',W_v,Z^n|\mathcal{C}_n)\\
&= I(X^n;W_a,M,W_v,Z^n|\mathcal{C}_n)\\
&= H(X^n|\mathcal{C}_n) - H(X^n,W_a,M,W_v,Z^n|\mathcal{C}_n) + H(W_a,M,W_v|\mathcal{C}_n) + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&\overset{(a)}{=} -H(Z^n|X^n,\mathcal{C}_n) - H(W_a,A^n,M,W_v|X^n,Z^n,\mathcal{C}_n) + H(W_a,M,W_v|\mathcal{C}_n) + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&= -H(Z^n|X^n,A^n,\mathcal{C}_n) - I(A^n;Z^n|X^n,\mathcal{C}_n) - H(A^n|X^n,Z^n,\mathcal{C}_n) - H(W_a,M,W_v|X^n,Z^n,A^n,\mathcal{C}_n)\\
&\quad + H(W_a,M,W_v|\mathcal{C}_n) + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&\overset{(b)}{=} -H(Z^n|X^n,A^n) - H(A^n|X^n,\mathcal{C}_n) - H(W_a,M,W_v,W|X^n,Z^n,A^n,\mathcal{C}_n)\\
&\quad + H(W_a,M,W_v|\mathcal{C}_n) + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&= -H(Z^n|X^n,A^n) - H(A^n|X^n,\mathcal{C}_n) - H(W_a,M,W_v,W,V^n|X^n,Z^n,A^n,\mathcal{C}_n)\\
&\quad + H(V^n|X^n,Z^n,A^n,W_a,M,W_v,W,\mathcal{C}_n) + H(W_a,M,W_v|\mathcal{C}_n) + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&\overset{(c)}{\leq} -H(Z^n|X^n,A^n) - H(A^n|X^n,\mathcal{C}_n) - H(V^n|X^n,Z^n,A^n,\mathcal{C}_n) + n\epsilon_n + H(W_a,M,W_v|\mathcal{C}_n)\\
&\quad + H(Z^n|W_a,M,W_v,\mathcal{C}_n)\\
&\overset{(d)}{\leq} -H(Z^n|X^n,A^n) - H(V^n,A^n|X^n,\mathcal{C}_n) + H(W_a|\mathcal{C}_n)\\
&\quad + H(M|\mathcal{C}_n) + H(W_v|\mathcal{C}_n) + H(Z^n|A^n,U^n,\mathcal{C}_n) + n\epsilon_n\\
&\overset{(e)}{\leq} -H(Z^n|X^n,A^n) - n[H(V,A|X) - H(V,A|\widetilde{X}) - 2\delta_\epsilon] + H(W_a|\mathcal{C}_n) + H(M|\mathcal{C}_n) + H(W_v|\mathcal{C}_n)\\
&\quad + H(Z^n|A^n,U^n,\mathcal{C}_n) + n\epsilon_n\\
&\overset{(f)}{\leq} -n[H(Z|X,A) - H(V,A|X) + H(V,A|\widetilde{X}) + 7\delta_\epsilon + I(\widetilde{X};A) + I(\widetilde{X};U|A) + I(V;\widetilde{X}|A,U)\\
&\quad - I(V;Y|A,U) + H(Z|A,U) + \epsilon_n]\\
&\overset{(g)}{=} n[I(\widetilde{X};V,A) - H(V,A|X) + H(V,A|\widetilde{X}) - I(V;Y|A,U) + I(X;Z|A,U) + \delta_\epsilon^{(3)}]\\
&= n[I(X;V,A) - I(V;Y|A,U) + I(X;Z|A,U) + \delta_\epsilon^{(3)}]\\
&\overset{(h)}{=} n[I(X;A,V,Y) - (I(X;Y|A,U) - I(X;Z|A,U)) + \delta_\epsilon^{(3)}]\\
&\leq n[R_\ell + \delta_\epsilon^{(3)}] \qquad \text{(C.16)}
\end{aligned}
$$

if $R_\ell \geq I(X;A,V,Y) - (I(X;Y|A,U) - I(X;Z|A,U))$, where (a) follows since given $\mathcal{C}_n$, W_a determines A^n,
(b) follows since $Z^n - (X^n,A^n) - \mathcal{C}_n$ forms a Markov chain and (W_a,W_u,W_v) determine the helper data W,
(c) follows from the Markov chain $V^n - (X^n,A^n,W,\mathcal{C}_n) - Y^n$ and Fano's inequality applied

as

$$\begin{aligned}&H(V^n|X^n,Z^n,A^n,W_a,M,W_v,W,\mathcal{C}_n)\\&\leq H(V^n|X^n,A^n,W,\mathcal{C}_n)\leq H(V^n|Y^n,A^n,W,\mathcal{C}_n)\leq n\epsilon_n,\end{aligned}$$

(d) follows from the Markov chain $V^n-(X^n,A^n,\mathcal{C}_n)-Z^n$ and because, given the codebook, W_a determines A^n and (W_a,M) determine U^n,
(e) follows from the following inequality

$$\begin{aligned}&H(V^n,A^n|X^n,\mathcal{C}_n)\\&=H(A^n|X^n,\mathcal{C}_n)+H(V^n|X^n,A^n,\widetilde{X}^n,\mathcal{C}_n)+I(V^n;\widetilde{X}^n|X^n,A^n,\mathcal{C}_n)\\&\geq H(\widetilde{X}^n,A^n|X^n,\mathcal{C}_n)-H(\widetilde{X}^n|X^n,A^n,V^n,\mathcal{C}_n)\\&\overset{(a)}{\geq} H(\widetilde{X}^n|X^n)-H(\widetilde{X}^n|X^n,A^n,V^n,\mathcal{C}_n)\\&\overset{(b)}{\geq} n[H(\widetilde{X}|X)-H(\widetilde{X}|X,A,V)-2\delta_\epsilon]\\&\overset{(c)}{=} n[H(V,A|X)-H(V,A|\widetilde{X})-2\delta_\epsilon]\end{aligned}$$

where (a) follows since $\widetilde{X}^n-X^n-\mathcal{C}_n$ forms a Markov chain, (b) follows by applying Lemma C.2 to bound the term $H(\widetilde{X}^n|X^n,A^n,V^n,\mathcal{C}_n)$, and (c) follows due to the Markov chain $(V,A)-\widetilde{X}-X$,
(f) follows from the codebook generation, from the memoryless property of the source and side information channels, from Lemma C.1 applied to $H(Z^n|X^n,A^n)$, and from Lemma C.2 applied to $H(Z^n|A^n,U^n,\mathcal{C}_n)$,
(g) follows from the Markov chains $U-(V,A)-\widetilde{X}$ and $U-(A,X)-Z$,
(h) follows from the Markov chain $U-V-(A,X)-Y$.

Secrecy-leakage Rate: The secrecy-leakage rate analysis follows by replacing every X^n in Appendix C.2.1 with $\widetilde{X}^n$ when bounding the term $H(A^n,U^n,V^n,Z^n|\mathcal{C}_n)$ since, this time, $(U^n,V^n,\mathcal{C}_n)-(A^n,\widetilde{X}^n)-Z^n$ and $U-V-(A,\widetilde{X})-(Y,Z)$ form Markov chains. Use

$$\begin{aligned}&H(Z^n|\widetilde{X}^n,A^n,\mathcal{C}_n)\\&=H(Z^n|\widetilde{X}^n,A^n,X^n,\mathcal{C}_n)+I(Z^n;X^n|\widetilde{X}^n,A^n,\mathcal{C}_n)\\&\overset{(a)}{=}H(Z^n|A^n,X^n)+H(X^n|\widetilde{X}^n)-H(X^n|\widetilde{X}^n,A^n,Z^n,\mathcal{C}_n)\\&\overset{(b)}{\geq}n(H(Z|A,X)+H(X|\widetilde{X})-2\delta_\epsilon)-H(X^n|\widetilde{X}^n,A^n,Z^n,\mathcal{C}_n)\\&\overset{(c)}{\geq}n(H(Z|A,X)+H(X|\widetilde{X},A)-H(X|\widetilde{X},A,Z)-3\delta_\epsilon)\\&\overset{(d)}{=}n(H(Z|\widetilde{X},A)-3\delta_\epsilon)\end{aligned}$$

where (a) follows because $Z^n-(A^n,X^n)-(\widetilde{X}^n,\mathcal{C}_n)$ and $X^n-\widetilde{X}^n-(A^n,\mathcal{C}_n)$ form Markov chains, (b) follows by applying Lemma C.1 to bound the term $H(Z^n|A^n,X^n)$ because

Z^n is i.i.d. $\sim P_{Z|XA}$, (c) follows from the Markov chain $X - \widetilde{X} - A$ and by applying Lemma C.2 to bound the term $H(X^n|\widetilde{X}^n, A^n, Z^n, \mathcal{C}_n)$, and (d) follows from the Markov chain $Z - (A, X) - \widetilde{X}$. We thus obtain

$$I(W_s; W_a, W_u, W_v, Z^n|\mathcal{C}_n) \leq n\delta_\epsilon^{(4)}. \tag{C.17}$$

Secret-key Rate: Using the codebook generation in Appendix C.2.1 and the Markov chain $V - (A, \widetilde{X}, U) - Y$, it is straightforward to show that

$$\begin{aligned} H(W_s|\mathcal{C}_n) &\geq n[I(V; Y|A, U) - I(Y; Z|A, U) - \delta_\epsilon^{(3)}] \\ &\geq n(R_s - \delta_\epsilon^{(3)}) \end{aligned} \tag{C.18}$$

if $R_s \leq I(V; Y|A, U) - I(V; Z|A, U)$.

Using the selection lemma, we have that a tuple (R_s, R_ℓ, R_w, C) that satisfies (6.7)-(6.9) for some $P_{A|\widetilde{X}}$, $P_{V|\widetilde{X}A}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)] \leq C$ is achievable.

C.4.2. Proof of Converse

Use the definitions of U_i and V_i given in Appendix C.2.2 so that $U_i - V_i - (A_i, \widetilde{X}_i) - (A_i, X_i) - (Y_i, Z_i)$ forms a Markov chain for all $i = 1, 2, \dots, n$.

Storage Rate: Replace every X^n with $\widetilde{X}^n$ and every X_i with $\widetilde{X}_i$ for all $i = 1, 2, \dots, n$ in Appendix C.2.2 and apply similar steps to obtain

$$R_w \geq \frac{1}{n}\Big[\sum_{i=1}^n I(\widetilde{X}_i; A_i) + I(V_i; \widetilde{X}_i|A_i, Y_i) - n\epsilon_n - n\delta_n\Big]. \tag{C.19}$$

Privacy-leakage Rate: We apply similar steps as in Appendix C.2.2. It is also straightforward to show that $(W, S, A^{n\backslash i}, X^{n\backslash i}, Y_{i+1}^n, Z^{i-1}) - (A_i, X_i) - (Y_i, Z_i)$, $(X_i, W, S, A_i^n, Y_i^n) - (A^{i-1}, X^{i-1}) - (Z^{i-1}, Y^{i-1})$, and $U_i - (A_i, X_i) - (Y_i, Z_i)$ form Markov chains for all $i = 1, 2, \dots, n$ also for a hidden source. We thus obtain

$$R_\ell \geq \frac{1}{n}\Big[\sum_{i=1}^n I(X_i; A_i, V_i, Y_i) - I(X_i; Y_i|A_i, U_i) + I(X_i; Z_i|A_i, U_i) - n\epsilon_n - n\delta_n\Big]. \tag{C.20}$$

Secret-key Rate: The converse is similar to the converse for a visible source with the GS model. By applying similar steps as in Appendix C.2.2, we obtain

$$R_s \leq \frac{1}{n}\Big[\sum_{i=1}^n I(V_i; Y_i|A_i, U_i) - I(V_i; Z_i|A_i, U_i) + 3n\delta_n\Big]. \tag{C.21}$$

Action Cost: We obtain (C.8) for the expected cost constraint.

The converse follows by applying the standard time-sharing argument and letting $\delta_n \to 0$.

Cardinality Bounds: We use the support lemma and should satisfy the Markov condition

$U-V-(A,\widetilde{X})-(A,X)-(Y,Z)$, so we preserve $P_{\widetilde{X}A}$ by using $|\widetilde{\mathcal{X}}||\mathcal{A}|-1$ real-valued continuous functions. We have to preserve four more expressions, i.e., $I(V;Y|A,U)-I(V;Z|A,U)$, $H(\widetilde{X}|U,V,A,Y)$, $H(X|U,V,A,Y)$, and $I(X;Z|A,U)-I(X;Y|A,U)$. One can therefore preserve all expressions in Theorem 6.1 by using an auxiliary random variable U with $|\mathcal{U}|\leq|\widetilde{\mathcal{X}}||\mathcal{A}|+3$ and, similarly, V with $|\mathcal{V}|\leq(|\widetilde{\mathcal{X}}||\mathcal{A}|+3)(|\widetilde{\mathcal{X}}||\mathcal{A}|+2)$.

C.5. Proof of Theorem 6.2

C.5.1. Proof of Achievability

Fix $P_{A|\widetilde{X}}$, $P_{V|\widetilde{X}A}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)]\leq C+\epsilon$. We use the achievability proof of Theorem 6.1. Suppose the key $S'=W_{s'}$ generated as in the GS model for a hidden source has the same cardinality as the chosen key $S=W_s$, i.e., $|\mathcal{S}'|=|\mathcal{S}|$. Consider an encoder $\mathsf{Enc}(\cdot)$ with inputs $(\widetilde{X}^n,S)$ and outputs $W=(S'+S,W')$, where W' is the helper data in the GS model for a hidden source. Similarly, consider a decoder $\mathsf{Dec}(\cdot)$ with inputs (Y^n,W) and output $\hat{S}=S'+S-\hat{S}'$, where the addition and subtraction operations are modulo-$|\mathcal{S}|$. Note that the decoder of the GS model for a hidden source is used at the decoder to obtain $\hat{S}'$. Furthermore, the action encoder $\mathsf{Enc}_a(\cdot)$ takes W' as its input.

Error Probability: We obtain (C.9), which is small due to the proof of achievability for Theorem 6.1.

Action Cost: Similar to Appendix C.4.1, one can show that the expected cost constraint is satisfied with high probability by using the typical average lemma.

Privacy-leakage Rate: We have

$$\begin{aligned}
&I(X^n;W_{a'},W_{u'},W_{v'},W_s+W_{s'},Z^n|\mathcal{C}_n)\\
&\leq I(X^n;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+\log|\mathcal{S}|-H(W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,X^n,W_{s'},\mathcal{C}_n)\\
&\overset{(a)}{\leq} n[I(X;A,V,Y)-(I(X;Y|A,U)-I(X;Z|A,U))+\delta_\epsilon^{(3)}]\\
&\leq n[R_\ell+\delta_\epsilon^{(3)}] \qquad\qquad (C.22)
\end{aligned}$$

if $R_\ell\geq I(X;A,V,Y)-(I(X;Y|A,U)-I(X;Z|A,U))$, where (a) follows because $S=W_s$ is independent of $(W_{a'},W_{u'},W_{v'},Z^n,X^n,W_{s'},\mathcal{C}_n)$, and from uniformity of W_s and (C.16).

Secrecy-leakage Rate: We obtain

$$\begin{aligned}
&I(W_s;W_{a'},W_{u'},W_{v'},W_s+W_{s'},Z^n|\mathcal{C}_n)\\
&=I(W_s;W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)+I(W_s;W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\overset{(a)}{=} H(W_s+W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)-H(W_{s'}|W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)\\
&\leq\log|\mathcal{S}|-H(W_{s'})+I(W_{s'};W_{a'},W_{u'},W_{v'},Z^n|\mathcal{C}_n)\\
&\overset{(b)}{\leq} n(\delta_n+\delta_\epsilon^{(4)}) \qquad\qquad (C.23)
\end{aligned}$$

where (a) follows because $S=W_s$ is independent of $(W_{a'},W_{u'},W_{v'},Z^n,\mathcal{C}_n)$ and (b) follows by (C.17) and (C.18).

Secret-key Rate: Observe that

$$\begin{aligned}
&H(W_s|\mathcal{C}_n) = \log|\mathcal{S}| \geq H(W_{s'}|\mathcal{C}_n)\\
&\overset{(a)}{\geq} n(I(Y;V|A,U) - I(Z;V|A,U) - \delta_\epsilon^{(3)})\\
&\geq n(R_s - \delta_\epsilon^{(3)})
\end{aligned} \tag{C.24}$$

if $R_s \leq I(V;Y|A,U) - I(V;Z|A,U)$, where (a) follows by (C.18).

Storage Rate: The storage rate is the sum of the storage $R_{w'}$ for a hidden source with the GS model and for $S' + S$. We obtain

$$\begin{aligned}
&R_w \leq R_{w'} + \frac{1}{n}\log|\mathcal{S}|\\
&\overset{(a)}{=} I(\widetilde{X}, A) + I(V;\widetilde{X}|A,Y) + 6\delta_\epsilon + R_s\\
&\overset{(b)}{\leq} I(\widetilde{X}, A) + I(V;\widetilde{X}|A,Y) + 6\delta_\epsilon + I(V;Y|A,U) - I(V;Z|A,U)\\
&\overset{(c)}{=} I(\widetilde{X};A,V) - I(U;Y|A) - I(V;Z|A,U) + 6\delta_\epsilon
\end{aligned} \tag{C.25}$$

where (a) follows from the storage rate for a hidden source with the GS model, (b) follows by (C.24), and (c) follows from the Markov chain $U - V - (A,\widetilde{X}) - (Y,Z)$.

Using the selection lemma, we have that a tuple (R_s, R_ℓ, R_w, C) that satisfies (6.12)-(6.14) for some $P_{A|\widetilde{X}}$, $P_{V|\widetilde{X}A}$, and $P_{U|V}$ such that $\mathbb{E}[\Gamma(A)]\leq C$ is achievable.

C.5.2. Proof of Converse

Use the definitions of U_i and V_i given in Appendix C.2.2 so that $U_i - V_i - (A_i,\widetilde{X}_i) - (A_i,X_i) - (Y_i,Z_i)$ forms a Markov chain for all $i = 1,2,\dots,n$.

Secret-key Rate: The converse for the secret-key rate is similar to the converse for a hidden source with the GS model. We obtain

$$R_s \leq \frac{1}{n}\Big[\sum_{i=1}^{n} I(V_i;Y_i|A_i,U_i) - I(V_i;Z_i|A_i,U_i) + 3n\delta_n\Big]. \tag{C.26}$$

Action Cost: Similar to Appendix C.4.2, we obtain (C.8) for the expected cost constraint.

Privacy-leakage Rate: We apply similar steps to Appendix C.4.2. It is straightforward to show that $(W,S,A^{n\setminus i},X^{n\setminus i},Y_{i+1}^n,Z^{i-1}) - (A_i,X_i) - (Y_i,Z_i)$, $(X_i,W,S,A_i^n,Y_i^n) - (A^{i-1},X^{i-1}) - (Z^{i-1},Y^{i-1})$, and $U_i - (A_i,X_i) - (Y_i,Z_i)$ form Markov chains for all $i = 1,2,\dots,n$ also for a hidden source and an chosen secret key S. We thus obtain

$$R_\ell \geq \frac{1}{n}\Big[\sum_{i=1}^{n} I(X_i;A_i,V_i,Y_i) - I(X_i;Y_i|A_i,U_i) + I(X_i;Z_i|A_i,U_i) - n\epsilon_n - n\delta_n\Big]. \tag{C.27}$$

Storage Rate: This time, we apply similar steps as in Appendix C.3.2. Replace every sequence X^n with $\widetilde{X}^n$ and every X_i with $\widetilde{X}_i$ for all $i = 1, 2, \ldots, n$. Using similar steps as in Appendix C.3.2, and the facts that $U_i - V_i - (A_i, \widetilde{X}_i) - (Y_i, Z_i)$ for all $i = 1, 2, \ldots, n$ and $(S, W) - (A^n, \widetilde{X}^n) - (Y^n, Z^n)$ form Markov chains, we obtain

$$R_w \geq \frac{1}{n}\Big[\sum_{i=1}^{n} I(\widetilde{X}_i; A_i, V_i) - I(U_i; Y_i|A_i) - I(V_i; Z_i|A_i, U_i) - n\delta_n\Big]. \tag{C.28}$$

The converse follows by applying the standard time-sharing argument and letting $\delta_n \to 0$.

Cardinality Bounds: We use the support lemma. One also has to satisfy the Markov condition $U - V - (A, \widetilde{X}) - (A, X) - (Y, Z)$. We preserve $P_{\widetilde{X}A}$ by using $|\widetilde{\mathcal{X}}||\mathcal{A}| - 1$ real-valued continuous functions. The bound in (6.14) can be written as

$$\begin{aligned}&I(\widetilde{X}; A, V) - I(U; Y|A) - I(V; Z|A, U)\\ &= I(\widetilde{X}; A) + I(\widetilde{X}; V|A, Y) + I(V; Y|A, U) - I(V; Z|A, U).\end{aligned}$$

We therefore have to preserve four more expressions, i.e., $I(V; Y|A, U) - I(V; Z|A, U)$, $H(\widetilde{X}|U, V, A, Y)$, $H(X|U, V, A, Y)$, and $I(X; Z|A, U) - I(X; Y|A, U)$. One can therefore preserve all expressions in Theorem 6.2 by using an auxiliary random variable U with $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{A}| + 3$ and, similarly, V with $|\mathcal{V}| \leq (|\mathcal{X}||\mathcal{A}| + 3)(|\mathcal{X}||\mathcal{A}| + 2)$.

D

Abbreviations

AES	Advanced Encryption Standard
AICc	corrected Akaike information criterion
AWGN	additive white Gaussian noise
BCH	Bose-Chaudhuri-Hocquenghem
BIC	Bayesian information criterion
BMDD	bounded minimum distance decoder
BPSK	binary phase shift keying
BSC	binary symmetric channel
BSS	binary symmetric source
CAN	controller area network
CMOS	complementary metal–oxide–semiconductor
COFE	code-offset fuzzy extractor
CS	chosen-secret
DCT	discrete cosine transform
DHT	discrete Haar transform
DWHT	discrete Walsh-Hadamard transform
EVE	eavesdropper
FCS	fuzzy commitment scheme

FPGA	field-programmable gate array
FSM	finite-state machine
GCC	generalized concatenated code
GS	generated-secret
HSM	hidden source model
i.i.d.	independent and identically distributed
IC	integrated circuit
IoT	Internet-of-things
IP	intellectual property
KLT	Karhunen-Loève transform
LDPC	low density parity check
LUTs	lookup tables
MGL	Mrs. Gerber's lemma
MLD	maximum likelihood decoder
MUX	multiplexer
NIST	National Institute of Standards and Technology
NVM	non-volatile memory
POWFs	physical one-way functions
PUF	physical unclonable function
RAM	random access memory
RFID	radio frequency identification
RM	Reed-Muller
RO	ring oscillator
ROM	read-only memory
RS	Reed-Solomon
SK	secret-key
SNR	signal-to-noise ratio
SoC	system-on-chip
SRAM	static random access memory
SW	Slepian-Wolf
VSM	visible source model
WZ	Wyner-Ziv

Bibliography

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] D. Kahn, *The Codebreakers: The Story of Secret Writing.* New York, NY: Macmillan Publishers, 1967.

[3] B. Schneier, *Applied cryptography: Protocols, algorithms, and source code in C*, 2nd ed. John Wiley & Sons, Jan. 1996.

[4] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice.* New York: Springer-Verlag, 2012.

[5] O. Günlü, “Design and analysis of discrete cosine transform based ring oscillator physical unclonable functions,” Master’s thesis, Techn. Univ. Munich, Munich, Germany, Oct. 2013.

[6] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, “Silicon physical random functions,” in *ACM Conf. Computer Commun. Security*, Washington, DC, USA, Nov. 2002, pp. 148–160.

[7] O. Günlü and O. İşcan, “DCT based ring oscillator physical unclonable functions,” in *IEEE Int. Conf. Acoustics Speech Sign. Process.*, Florence, Italy, May 2014, pp. 8198–8201.

[8] O. Günlü, O. İşcan, and G. Kramer, “Reliable secret key generation from physical unclonable functions under varying environmental conditions,” in *IEEE Int. Workshop Inf. Forensics Security*, Rome, Italy, Nov. 2015, pp. 1–6.

[9] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, “Reliable secret-key binding for physical unclonable functions with transform coding,” in *IEEE Global Conf. Sign. Inf. Process.*, Greater Washington, DC, USA, Dec. 2016, pp. 986–991.

[10] O. Günlü, A. Belkacem, and B. C. Geiger, “Secret-key binding to physical identifiers with reliability guarantees,” in *IEEE Int. Conf. Commun.*, Paris, France, May 2017, pp. 1–6.

[11] O. Günlü, T. Kernetzky, O. İşcan, V. Sidorenko, G. Kramer, and R. F. Schaefer, “Secure and reliable key agreement with physical unclonable functions,” *Entropy*, vol. 20, no. 5, May 2018.

[12] O. Günlü, G. Kramer, and M. Skórski, "Privacy and secrecy with multiple measurements of physical and biometric identifiers," in *IEEE Conf. Commun. Network Security*, Florence, Italy, Sep. 2015, pp. 89–94.

[13] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[14] O. Günlü, O. İşcan, V. Sidorenko, and G. Kramer, "Code constructions for physical unclonable functions and biometric secrecy systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.

[15] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[16] L. Kusters, O. Günlü, and F. M. Willems, "Zero secrecy leakage for multiple enrollments of physical unclonable functions," in *Symp. Inf. Theory Sign. Process. the Benelux*, Enschede, the Netherlands, May 2018.

[17] A. Gohari, O. Günlü, and G. Kramer, "On achieving a positive rate in the source model key agreement problem," in *IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, June 2018, pp. 2659–2663.

[18] ——, "Coding for positive rate in the source model key agreement problem," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6303–6323, Oct. 2020.

[19] K. Kittichokechai, O. Günlü, R. F. Schaefer, and G. Caire, "Private authentication with controllable measurement," in *Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2016, pp. 1680–1684.

[20] O. Günlü, *Key Agreement with Physical Unclonable Functions and Biometric Identifiers.* Munich, Germany: Dr. Hut Verlag, Feb. 2019.

[21] O. Günlü and G. Kramer, "Research directions: Physical and biometric identifiers for key agreement," in *ITG Angewandte Informationstheorie Workshop*, Berlin, Germany, May 2018, pp. 158–164.

[22] O. Günlü, "Transform coding for physical unclonable functions (PUFs)," in *ITG Angewandte Informationstheorie Workshop*, Hamburg, Germany, Apr. 2015.

[23] O. Günlü, O. Iscan, V. Sidorenko, and G. Kramer, "Key agreement with multiple noisy measurements of physical unclonable functions," in *ITG Angewandte Informationstheorie Workshop*, Ulm, Germany, Mar. 2019, pp. 109–121.

[24] O. Günlü and R. F. Schaefer, "An optimality summary: Secret key agreement with physical unclonable functions," *Entropy*, vol. 23, no. 1, Jan. 2021.

[25] O. Günlü, “Multi-entity and multi-enrollment key agreement with correlated noise,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1190–1202, 2021.

[26] O. Günlü and R. F. Schaefer, “Controllable key agreement with correlated noise,” *IEEE J. Selected Areas Inf. Theory*, 2021.

[27] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, “An overview of information-theoretic security and privacy: Metrics, limits, and applications,” *IEEE J. Selected Areas Inf. Theory*, 2021.

[28] O. Günlü, R. F. Schaefer, and G. Kramer, “Private authentication with physical identifiers through broadcast channel measurements,” in *IEEE Inf. Theory Workshop*, Visby, Sweden, Aug. 2019, pp. 1–5.

[29] O. Günlü and R. F. Schaefer, “Low-complexity and reliable transforms for physical unclonable functions,” in *IEEE Int. Conf. Acoustics, Speech Signal Process.*, Barcelona, Spain, May 2020, pp. 2807–2811.

[30] T. Jerkovits, O. Günlü, V. Sidorenko, and G. Kramer, “Nested tailbiting convolutional codes for secrecy, privacy, and storage,” in *ACM Workshop Inf. Hiding Multimedia Security*, Denver, CO, June 2020, pp. 79–89.

[31] O. Günlü, R. F. Schaefer, and H. V. Poor, “Biometric and physical identifiers with correlated noise for controllable private authentication,” in *IEEE Int. Symp. Inf. Theory*, Los Angeles, CA, June 2020, pp. 874–878.

[32] O. Günlü, P. Trifonov, M. Kim, R. F. Schaefer, and V. Sidorenko, “Randomized nested polar subcode constructions for privacy, secrecy, and storage,” in *IEEE Int. Symp. Inf. Theory Appl.*, Kapolei, HI, Oct. 2020, pp. 475–479.

[33] O. Günlü and R. F. Schaefer, “Controllable key agreement with correlated noise,” *IEEE J. Sel. Areas in Inf. Theory*, vol. 2, no. 1, pp. 82–94, 2021.

[34] O. Günlü, M. Bloch, and R. F. Schaefer, “Secure multi-function computation with private remote sources,” in *IEEE Int. Symp. Inf. Theory*, 2021, pp. 1403–1408.

[35] J. L. Massey, *Applied Digital Information Theory.* Zurich, Switzerland: ETH Zurich, 1980–1998.

[36] A. Orlitsky and J. R. Roche, “Coding for computing,” *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[37] R. Maes, *Physically Unclonable Functions.* Berlin-Heidelberg, Germany: Springer-Verlag, 2013.

[38] O. Goldreich, *Modern cryptography, probabilistic proofs and pseudorandomness.* Berlin Heidelberg, Germany: Springer-Verlag, 1998, vol. 17.

[39] R. Pappu, "Physical one-way functions," Ph.D. dissertation, M.I.T., Cambridge, MA, USA, Oct. 2001.

[40] A. D. Wyner, "The wire-tap channel," *The Bell Sys. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[41] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Int. Conf. Detection Intrusions Malware Vulnerability Assessment*, Bonn, Germany, July 2017, pp. 185–206.

[42] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on physical unclonable function (PUF)," in *Int. Wireless Commun. Mobile Comput. Conf.*, Sardinia, Italy, July 2013, pp. 1314–1318.

[43] E. Simpson and P. Schaumont, "Offline hardware/software authentication for reconfigurable platforms," in *Int. Workshop Cryp. Hardware Embedded Sys.*, Yokohama, Japan, Oct. 2006, pp. 311–323.

[44] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *IEEE Int. Conf. RFID*, Las Vegas, NV, USA, Apr. 2008, pp. 58–64.

[45] B. Škorić, "Quantum readout of physical unclonable functions," *Int. J. Quantum Inf.*, vol. 10, no. 1, Feb. 2012.

[46] W.-C. Wang, Y. Yona, S. N. Diggavi, and P. Gupta, "Design and analysis of stability-guaranteed PUFs," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 24, pp. 978–992, Apr. 2018.

[47] B. Gassend, "Physical random functions," Master's thesis, M.I.T., Cambridge, MA, USA, Jan. 2003.

[48] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integration Sys.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[49] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Int. Workshop Cryp. Hardware Embedded Syst.*, Vienna, Austria, Sep. 2007, pp. 63–80.

[50] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs," in *IEEE Int. Symp. Inf. Theory*, Seoul, Korea, June-July 2009, pp. 2101–2105.

[51] M. K. Mandal and B. C. Sarkar, "Ring oscillators: Characteristics and applications," *Indian J. Pure Appl. Physics*, vol. 48, no. 2, pp. 136–145, Feb. 2010.

[52] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *ACM Des. Automation Conf.*, San Diego, CA, USA, June 2007, pp. 9–14.

[53] C.-E. Yin and G. Qu, "Improving PUF security with regression-based distiller," in *ACM Ann. Des. Automation Conf.*, Austin, TX, USA, June 2013, pp. 184:1–184:6.

[54] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Jan. 2008.

[55] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM Conf. Comp. Commun. Security*, New York City, NY, USA, Nov. 1999, pp. 28–36.

[56] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[57] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security trade-offs in biometric security systems - Part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[58] T. Ignatenko and F. M. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 2337–348, June 2010.

[59] ——, "Privacy-leakage codes for biometric authentication systems," in *IEEE Int. Conf. Acoustics Speech Sign. Process.*, Florence, Italy, May 2014, pp. 1601–1605.

[60] R. Maes, A. V. Herrewege, and I. Verbauwhede, "PUFKY: A fully functional PUF-based cryptographic key generator," in *Int. Workshop Cryp. Hardware Embedded Sys.*, Leuven, Belgium, Sep. 2012, pp. 302–319.

[61] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptology*, vol. 24, no. 2, pp. 375–397, Apr. 2011.

[62] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[63] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[64] S. Eiroa and I. Baturone, "An analysis of ring oscillator PUF behaviour in FPGAs," in *IEEE Int. Conf. Field-Programm. Techn.*, New Delhi, India, Dec. 2011, pp. 1–4.

[65] A. Maiti *et al.*, "A large scale characterization of RO-PUF," in *IEEE Int. Symp. Hardware-Orient. Security Trust*, Anaheim, CA, USA, June 2010, pp. 94–99.

[66] N. Sugiura, “Further analysis of the data by Akaike’s information criterion and the finite corrections,” *Commun. Stat.-Theory Methods*, vol. 7, no. 1, pp. 13–26, Jan. 1978.

[67] G. Schwarz, “Estimating the dimension of a model,” *Annals Stat.*, vol. 6, no. 2, pp. 461–464, 1978.

[68] R. Wang, *Introduction to orthogonal transforms: With applications in data processing and analysis.* Cambridge, U.K.: Cambridge Univ. Press, 2012.

[69] C. M. Bishop, *Pattern Recognition and Machine Learning.* New York, NY, USA: Springer-Verlag, 2006, vol. 1.

[70] J.-R. Ohm, *Multimedia Signal Coding and Transmission.* Berlin Heidelberg, Germany: Springer-Verlag, 2015.

[71] S. Puchinger *et al.*, “On error correction for physical unclonable functions,” in *VDE Int. ITG Conf. Sys. Commun. Coding*, Hamburg, Germany, Feb. 2015, pp. 1–6.

[72] K. Komatsu and K. Sezaki, “Lossless 2D discrete Walsh-Hadamard transform,” in *IEEE Int. Conf. Acoustics Speech Sign. Process.*, vol. 3, Salt Lake City, UT, USA, May 2001, pp. 1917–1920.

[73] “EAMBA AXI and ACE Protocol Specification AXI3, AXI4, AXI5, ACE and ACE5,” Tech. Rep., 2017. [Online]. Available: developer.arm.com/docs/ihi0022/latest/amba-axi-and-ace-protocol-specification-axi3-axi4-axi5-ace-and-ace5

[74] “AMBA AXI4-Stream Protocol Specification v1.0,” Tech. Rep., 2010. [Online]. Available: https://developer.arm.com/docs/ihi0051/latest/amba-axi4-stream-protocol-specification-v10

[75] A. Rukhin *et al.*, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” National Inst. Stand. Techno., Tech. Rep., 2001, Rev. in 2010.

[76] S. Lin and D. J. Costello, *Error control coding.* Englewood Cliffs, NJ, USA: Prentice-Hall, May 2004.

[77] W.-H. Chen and W. Pratt, “Scene adaptive coder,” *IEEE Trans. Commun.*, vol. 32, no. 3, pp. 225–232, Mar. 1984.

[78] Y. Hong, “On computing the distribution function for the sum of independent and nonidentical random indicators,” Dep. Stat., Virginia Tech., Blacksburg, VA, USA, Tech. Rep., Apr. 2011.

[79] A. D. Wyner and J. Ziv, “A theorem on the entropy of certain binary sequences and applications: Part I,” *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 769–772, Nov. 1973.

[80] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[81] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[82] M. Koide and H. Yamamoto, "Coding theorems for biometric systems," in *IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, June 2010, pp. 2647–2651.

[83] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[84] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression.* Englewood Cliffs, NJ, USA: Prentice-Hall, 1971.

[85] K. Kittichokechai and G. Caire, "Secret key-based identification and authentication with a privacy constraint," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6189–6203, Nov. 2016.

[86] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6747–6765, Nov. 2012.

[87] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret-key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.

[88] A. Khisti, S. N. Diggavi, and G. W. Wornell, "Secret-key generation using correlated sources and channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 652–670, Feb. 2012.

[89] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A theoretical analysis of authentication, privacy, and reusability across secure biometric systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1825–1840, July 2012.

[90] H. Permuter and T. Weissman, "Source coding with a side information "Vending Machine"," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4530–4544, July 2011.

[91] J. Wayman, A. Jain, D. Maltoni, and D. M. (Eds), *Biometric Systems: Technology, Design and Performance Evaluation.* London, U.K.: Springer-Verlag, 2005.

[92] N. Chayat and S. Shamai, "Extension of an entropy property for binary input memoryless symmetric channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 5, pp. 1077–1079, Sep. 1989.

[93] I. Land, S. Huettinger, P. A. Hoeher, and J. B. Huber, "Bounds on information combining," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 612–619, Feb. 2005.

[94] G. Kramer, *Lecture Notes in Information Theory.* Munich, Germany: TU Munich, Oct. 2017.

[95] H. S. Witsenhausen, "Entropy inequalities for discrete channels," *IEEE Trans. Inf. Theory*, vol. 20, no. 5, pp. 610–616, Sep. 1974.

[96] R. Ahlswede and J. Körner, "On the connection between the entropies of input and output distributions of discrete memoryless channels," in *Conf. Prob. Theory*, Braşov, Romania, Sep. 1974, pp. 13–22.

[97] B. Chen, T. Ignatenko, F. M. Willems, R. Maes, E. van der Sluis, and G. Selimis, "A robust SRAM-PUF key generation scheme based on polar codes," in *IEEE Global Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

[98] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[99] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[100] M. Bloch and J. Barros, *Physical-layer Security.* Cambridge, U.K.: Cambridge Univ. Press, 2011.

[101] A. Gupta and S. Verdú, "Operational duality between Gelfand-Pinsker and Wyner-Ziv coding," in *IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, June 2010, pp. 530–534.

[102] S. Shamai, S. Verdú, and R. Zamir, "Systematic lossy source/channel coding," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 564–579, Mar. 1998.

[103] A. E. Gamal and Y.-H. Kim, *Network Information Theory.* Cambridge, U.K.: Cambridge Univ. Press, 2011.

[104] V. Guruswami, J. Hastad, and S. Kopparty, "On the list-decodability of random linear codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 718–725, Feb. 2011.

[105] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Int. Conf. Theory Appl. Cryptographic Techn.*, Bruges, Belgium, May 2000, pp. 351–368.

[106] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[107] S. B. Korada and R. L. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1751–1768, Apr. 2010.

[108] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on FPGAs," in *Int. Workshop Cryp. Hardware Embedded Sys.*, Washington, DC, USA, Aug. 2008, pp. 181–197.

[109] R. G. Gallager, *Low-Density Parity-Check Codes.* Cambridge, MA, USA: M.I.T. Press, 1963.

[110] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in *Int. Conf. Theory Appl. Cryptology Inf. Security*, Chennai, India, Dec. 2005, pp. 199–216.

[111] H. Tyagi and S. Watanabe, "Converses for secret key agreement and secure computing," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4809–4827, Sept. 2015.

[112] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des. Codes Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006.

[113] K. Kittichokechai, T. J. Oechtering, M. Skoglund, and Y. K. Chia, "Secure source coding with action-dependent side information," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6444–6464, Dec. 2015.

[114] K. Kittichokechai and G. Caire, "Secret key-based authentication with a privacy constraint," in *IEEE Int. Symp. Inf. Theory*, Hong Kong, June 2015, pp. 1791–1795.

[115] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, June 2013.

[116] L. Kusters, T. Ignatenko, F. M. J. Willems, R. Maes, E. van der Sluis, and G. Selimis, "Security of helper data schemes for SRAM-PUF in multiple enrollment scenarios," in *IEEE Int. Symp. Inf. Theory*, Aachen, Germany, June 2017, pp. 1803–1807.

[117] R. Maes, "An accurate probabilistic reliability model for silicon PUFs," in *Int. Workshop Cryp. Hardware Embedded Sys.*, Santa Barbara, CA, USA, Aug. 2013, pp. 73–89.

[118] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[119] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[120] R. Ahlswede and P. Gács, "Spreading of sets in product spaces and hypercontraction of the Markov operator," *Annals Probability*, vol. 4, no. 6, pp. 925–939, Dec. 1976.

[121] F. Topsøe, "Some bounds for the logarithmic function," *Ineq. Theory Appl.*, vol. 4, 2004.

[122] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[123] J. Hou and G. Kramer, "Informational divergence approximations to product distributions," in *Canadian Workshop Inf. Theory*, Toronto, ON, Canada, June 2013, pp. 76–81.

[124] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy compression," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1836–1849, Apr. 2016.

[125] A. Schrijver, *Theory of Linear and Integer Programming.* Chichester, West Sussex, England: John Wiley & Sons Ltd, 1998.

[126] M. Bloch, *Lecture Notes in Information-Theoretic Security.* Atlanta, GA, USA: Georgia Inst. Technol., July 2018.

[127] R. A. Amjad and G. Kramer, "Channel resolvability codes based on concatenation and sparse linear encoding," in *IEEE Int. Symp. Inf. Theory*, Hong Kong, China, June 2015, pp. 2111–2115.

[128] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[129] I. C. I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[130] J. Körner and K. Marton, "Images of a set via two channels and their role in multiuser communication," *IEEE Trans. Inf. Theory*, vol. 23, no. 6, pp. 751–761, Nov 1977.