# Information-Theoretic Secret-Key Agreement: The Secret-Key Rate as a Function of the Channel Quality Ratio

Daniel Jost[1], Ueli Maurer[1], and João L. Ribeiro[2]*

[1] Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland.
{dajost, maurer}@inf.ethz.ch

[2] Department of Computing, Imperial College London, United Kingdom.
j.lourenco-ribeiro17@imperial.ac.uk

**Abstract.** Information theoretically secure secret-key exchange between two parties, Alice and Bob, is a well-studied problem that is provably impossible without additional assumptions. However, it has shown to be feasible in a model where – in addition to an authenticated communication channel – the parties also have access to some correlated randomness. One particular type of such correlated randomness is the so-called satellite setting, where a source of uniform random bits (e.g. sent by a satellite) is received by the parties and the eavesdropper, Eve, via antennas of different sizes, which is modeled as receiving the bits through independent binary symmetric channels with error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$, respectively, where typically $\epsilon_E \ll \epsilon_A \approx \epsilon_B$. The secret-key rate is then defined as the maximal rate, per random bit, at which Alice and Bob can agree on secret key bits about which Eve has arbitrarily little information.

While in computational cryptography the relevant parameter in a security analysis is a bound on Eve's computing power, the corresponding quantity in the satellite setting is a bound on Eve's antenna size. In this work, we study the optimal secret-key rate in the satellite setting as a function of the ratio $Q$ of Eve's tolerable antenna size and the honest parties' antenna size. Technically, we consider the ratio $Q$ of the capacities of the corresponding binary symmetric channels, which corresponds roughly to the antenna size ratio, and we consider the satellite's sending signal strength as a system design parameter that can be optimized. This setting was first considered by Gander and Maurer (ISIT 1994), who conjectured based on numerical evidence that the secret-key rate of the parity-check protocol decreases like $1/Q^2$.

As a first contribution, we prove that this is actually the case, and also prove that this rate is asymptotically optimal, i.e., no protocol can achieve an asymptotically better rate in a setting where $\epsilon_A \approx \epsilon_B$. As a second contribution, we consider the secret-key rate per second rather than per transmitted bit, which might be of higher practical interest, given that one particular way of adjusting the signal strength is to adjust the bit-rate at which the satellite broadcasts. To this end, we introduce a quantity that approximates the secret-key rate per second, prove that for the parity-check protocol this quantity decreases like $1/Q$, and prove again that this is optimal. The difference between quadratic and linear decrease is quite significant in the satellite setting because it is plausible for Eve's antenna to be orders of magnitude larger than Alice's and Bob's.

[*] Part of the work was performed while at ETH Zurich.

# 1 Introduction

## 1.1 Motivation for Information-theoretic Security

In cryptography, one generally considers two types of security of cryptographic schemes. *Unconditional* or *information-theoretic* security means that not even an adversary with unbounded computing power can cause a violation of the security property, whereas *computational* security means that the violation of the security property is impossible for an adversary with (suitably) bounded computing power, but is usually possible for a computationally unbounded adversary. Information-theoretic security was first defined and considered in Shannon's ground-breaking paper [21].

While for the most part cryptographic research is focused on computational security, actually the state of the art in complexity theory is that no cryptographic scheme has been proven to be computationally secure for a general and realistic model of computation. Instead, the term "provable security" is often used for schemes for which a reduction from a commonly agreed conjectured hard problem (such as factoring large integers) is known: Any adversary breaking the cryptographic scheme could be transformed (by the reduction), with reasonable efficiency loss, into an algorithm solving the hard problem with noticeable probability. Therefore, under the assumption that the problem is indeed hard, the scheme is secure.

In summary, there are two main advantages of information-theoretic security:

- Information-theoretic security is stronger because, compared to computational security, the security holds against a larger class of adversaries.
- The security proof does not require an unproven computational assumption.

## 1.2 Circumventing Impossibility Results

Unfortunately, information-theoretic security is in many settings unachievable, often provably so, at least for practical settings. For instance, Shannon's famous impossibility result [21] states that perfectly secure encryption is impossible unless the secret key has at least as much entropy as the message. This result is often quoted as showing that information-theoretic security is not practical since exchanging a fresh truly random key for every message is generally completely impractical.

The significance of such an impossibility result depends on the generality of the conditions underlying the impossibility proof. For example, Shannon's impossibility result was stated (and proven) only under the restriction that the communication between sender and receiver is one-way. That this result also holds in the more realistic setting with interactive communication between sender and receiver was proved only in 1993 [10]. It is therefore possible that a careful re-examination of impossibility results allows to circumvent them by a slight change of the model, where such a change should be as realistic as possible and should not destroy the practicality of schemes proven secure in the model.

One such attempt, proposed by Maurer [14] and investigated by many researchers in different contexts, is the so-called bounded-storage model. Here one assumes that the adversary's memory resources are bounded, but no assumption about the adversary's computing power is needed. Unfortunately, it seems very hard to argue that schemes proven secure in this model are practical for a reasonable bound on the adversary's memory capacity.

Other notable earlier attempts include the works of Wyner [23] and Csiszár and Körner [4], where all parties are connected by noisy channels (and only one-way communication between the two honest parties is allowed), and the work of Ozarow and Wyner [18], where the adversary is allowed to observe a bounded subset of the message's encoding. In these models, perfectly secure encryption is possible only when the adversary is at a disadvantage compared to the honest parties, which is rarely the case in practice.

A more promising approach in the context of secret-key agreement is the so-called *secret-key agreement by public discussion* model proposed by Maurer [15,10]. In this model, two parties Alice and Bob wish to agree on a secret key by communicating over a public authenticated channel perfectly accessible to the adversary Eve. In this setting, without further assumptions, key agreement is provably impossible. However, by a slight modification of the model, namely by considering a setting where Alice, Bob, and Eve have access to correlated random variables $X$, $Y$, and $Z$, respectively, with joint probability distribution $P_{XYZ}$, secret-key agreement becomes possible, even if $X$ and $Y$ are almost not correlated and even if $Z$ is strongly correlated with both $X$ and $Y$.

Often one considers a setting where the experiment generating $X$, $Y$, and $Z$ is repeated many times (independently), and one then considers the *secret-key rate*, the maximal rate (per realization of the random experiment) at which Alice and Bob can generate secret-key bits. Surprisingly, in this model, secret-key agreement (and thus perfectly secure encryption) is also possible in many cases where Eve starts with an advantage over Alice and Bob.

### 1.3 The Satellite Setting and Contributions of this Paper

A setting of particular interest is the so-called satellite setting: A uniform random bit $R$ is generated (e.g. by a satellite, or by a deep-space radio source) and Alice, Bob, and Eve can receive this bit over independent binary symmetric channels with error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$, respectively. Quite surprisingly, one can show [10,13] that in this model secret-key agreement is possible even if Eve's channel is almost perfect, i.e., if $\epsilon_E$ is arbitrarily close to 0 and if Alice's and Bob's channels have arbitrarily high error probability (i.e., $\epsilon_A$ and $\epsilon_B$ are close to 0.5). In other words, secret-key agreement is possible, with a strictly positive rate, in all cases where it is not obviously impossible, namely if either $\epsilon_A = 0.5$, $\epsilon_B = 0.5$, or $\epsilon_E = 0$.

The central open problem in this topic is the characterization of the secret-key rate. However, in practice a characterization in terms of the error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$ is not very useful. Rather, the relevant parameter should be a bound on Eve's capabilities, which in the satellite setting corresponds to her antenna size. Thus, we consider the secret-key rate as a function of the maximal tolerable ratio $Q$ of Eve's and the honest parties' antenna sizes. Especially, we treat the energy used by the satellite to broadcast one bit as a design parameter for the protocol designer.

In a regime with significant noise power compared to the signal power (i.e., with small signal-to-noise ratio), the channel capacity is essentially proportional to the product of the surface of the receiver's antenna and the energy used to transmit each bit. Therefore, in order to model the sketched scenario of fixed antenna sizes but variable energy per bit, we consider the ratios of the capacity of Eve's channel and the capacity of Alice's and Bob's channels to be the relevant quantity. For simplicity, we assume in the following that Alice's and Bob's channel are of roughly the same quality and only consider their maximal error probability $\epsilon_{AB}$. This allows us to consider only a single ratio $Q$, and thus define the secret-key rate per transmitted bit under a fixed quality constraint $Q$ as the optimization over all tuples $(\epsilon_{AB}, \epsilon_E)$ satisfying the channel capacity ratio $Q$. In Section 4, we show that this secret-key rate is inversely proportional to $Q^2$, which is significantly better than the best proven result of the original paper [10], where the secret-key rate decreases exponentially in $Q$.

While a characterization of the secret-key rate per transmitted bit is interesting on its own, the more compelling quantity to look at is the secret-key rate per second. Especially, adjusting the energy used to transmit one bit, in practice, would probably be done by adjusting the bit-rate, as this allows to keep a fixed signal power. This highlights a very interesting trade-off: A smaller transmission time allows Alice and Bob to receive more bits per second, but yields larger error probabilities for all parties, rendering the optimal bit-rate a priori unclear. In order to investigate this question, we introduce a quantity that approximates the secret-key rate per second by dividing the secret-key rate per transmitted bit by the capacity of Alice's channel. This approximation is again motivated by the fact that the capacity is roughly inversely proportional to the bit-rate and since this approximation mainly holds in a regime with small signal-to-noise ratio, it is natural to choose Alice's and not Eve's channel capacity. In Section 5 we then show that this quantity decreases inversely proportional to $Q$, rather than $Q^2$. Note that this is a significant difference, since Eve's antenna must be assumed to be orders of magnitudes larger than those of Alice and Bob (who might for instance use a mobile phone). In summary, the fact that the secret-key rate per second only decreases linearly in $Q$ is a highly surprising result, which brings secret-key exchange in the satellite model within the reach of practicality.

### 1.4 Related Work

There have been considerable efforts to find good approximations for the secret-key rate, both in the satellite setting and for more general probability distributions, and also for setting with more than three parties.

The first bounds on the secret-key rate were proved by Maurer [10,12], and by Ahlswede and Csiszár [1], who studied the secret-key rate when only one-way communication from Alice to Bob is allowed. Later, Maurer and Wolf [11] and Renner, Skripsky, and Wolf [19] introduced improved upper bounds for general distributions, called the *intrinsic mutual information* and the *reduced intrinsic mutual information*, respectively.

For the satellite setting, there exist better lower bounds on the secret-key rate due to the study of several *advantage distillation protocols*. The first such protocol, called the *repeater-code protocol*, was introduced and studied by Maurer [15,10]. An improved version of this protocol, called the *parity-check protocol*, was studied by Gander and Maurer [15,6]. Later, Liu, Van Tilborg, and Van Dijk [9] proposed a more complex protocol that outperforms the parity-check protocol, but from which it appears to be difficult to compute better lower bounds.

Csiszár and Narayan [5] extended the study of the secret-key rate to settings with more than three parties, and exhibited connections between information-theoretic secret-key agreement and the problem of *communication for omniscience*. Then, Gohari and Anantharam [7] showcased new lower and upper bounds on the secret-key rate for an arbitrary number of parties, which in particular are strict improvements over the previously known bounds for our setting.

Naito et al. [17] considered a scenario where Alice, Bob, and Eve receive the random bits in the satellite setting through Gaussian channels, instead of binary symmetric channels, and so are able to make use of soft-decoding. They show that Alice and Bob can extract more secret-key rate in the Gaussian scenario.

There has been some recent interest in the secret-key rate in the finite blocklength setting, where the number of available realizations $(X, Y, Z)$ is bounded. Tyagi and Watanabe [22] showcase a connection between the secret-key rate in this setting and binary hypothesis testing, and use it to obtain an upper bound on the secret-key rate for a bounded number of realizations. Later, Hayashi, Tyagi, and Watanabe [8] used this connection to better understand how the gap between the secret-key rate in the finite blocklength and asymptotic settings decreases as the number of available realizations increases, for certain probability distributions.

## 2 Preliminaries

### 2.1 Notation

We denote random variables by uppercase letters such as $X$, $Y$, and $Z$. We may denote sequences of random variables $X_1, X_2, \ldots, X_N$ as $X^N$. We say that $X_1, X_2, \ldots, X_N$ are i.i.d. if all the $X_i$ are independent random variables and they all have the same distribution. Most sets are denoted by uppercase calligraphic letters such as $\mathcal{S}$. The set of real numbers is denoted by $\mathbb{R}$ and for a natural number $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \ldots, n\}$. Given a set $\mathcal{S}$, the size of $\mathcal{S}$ is denoted by $|\mathcal{S}|$. For a string $x \in \{0,1\}^*$, $|x|$ denotes the length of $x$. The (Hamming) weight of a string $x \in \{0,1\}^*$ is defined as $w(x) \coloneqq |\{i : x_i = 1\}|$, where $x_i$ is the $i$-th entry of $x$. We denote the logarithm to the base 2 by log and the natural logarithm by ln. The closed interval in $\mathbb{R}$ between two real numbers $a$ and $b$ is denoted by $[a, b]$.

Given an event $A$, we denote the probability that $A$ happens by $\Pr[A]$, which is the sum of the probabilities of all outcomes in event $A$. Given two events $A$ and $B$, the probability that $A$ and $B$ happen simultaneously is denoted by $\Pr[A, B]$. The conditional probability of $A$ given $B$, provided $\Pr[B] > 0$, is $\Pr[A|B] \coloneqq \frac{\Pr[A,B]}{\Pr[B]}$.

The probability distribution of a finite random variable $X$ is denoted by $P_X$, and so $P_X(x)$ denotes the probability that $X$ takes the value $x$. Given an event $A$, $P_{X|A}$ denotes the conditional probability distribution of $X$ conditioned on $A$. For two finite random variables $X$ and $Y$, $P_{X|Y}(\cdot, y)$ denotes the probability distribution of $X$ conditioned on the event $Y = y$.

### 2.2 Information Theory

Throughout this paper we will make use of some fundamental concepts from information theory. We briefly define the required notions in this section; a more detailed exposition of this field can be found in [3].

Fix a finite random variable $X$ with range $\mathcal{X}$. The *entropy of* $X$, denoted by $H(X)$, is defined as

$$H(X) \coloneqq -\sum_{x \in \mathcal{X}} P_X(x) \log P_X(x).$$

Intuitively, the entropy measures the uncertainty about a given random variable. In fact, a finite random variable $X$ with range $\mathcal{X}$ satisfies $0 \leq H(X) \leq \log|\mathcal{X}|$ with equality in the lower bound if and only if $P_X(x) = 1$ for some $x \in \mathcal{X}$, and with equality in the upper bound if and only if $X$ is uniform over $\mathcal{X}$. We call

$$h(p) \coloneqq -p\log(p) - (1-p)\log(1-p)$$

the *binary entropy function* and note that for a binary random variable $X$ with $P_X(1) = p$ we have that $H(X) = h(p)$.

Given two finite random variables $X$ and $Y$ with ranges $\mathcal{X}$ and $\mathcal{Y}$, respectively, we define the *conditional entropy of $X$ given $Y$*, denoted by $H(X|Y)$, as

$$H(X|Y) := \sum_{y\in\mathcal{Y}} P_Y(y)H(X|Y=y).$$

Given an event $A$, $H(X|Y,A)$ is defined as

$$H(X|Y,A) := \sum_{y\in\mathcal{Y}} P_{Y|A}(y)H(X|Y=y,A).$$

We define the *mutual information between $X$ and $Y$*, denoted by $I(X;Y)$, as

$$I(X;Y) := H(X) - H(X|Y).$$

Intuitively, the mutual information measures how independent two random variables are, and we have $I(X;Y)=0$ if and only if $X$ and $Y$ are independent. Given an event $A$, $I(X;Y|A)$ is defined as

$$I(X;Y|A) := H(X|A) - H(X|Y,A).$$

Finally, if additionally $Z$ is a finite random variable with range $\mathcal{Z}$, the *conditional mutual information between $X$ and $Y$ given $Z$*, denoted by $I(X;Y|Z)$, is defined as

$$I(X;Y|Z) := \sum_{z\in\mathcal{Z}} P_Z(z)I(X;Y|Z=z).$$

We will be dealing with a simple instance of a *discrete memoryless channel.* A discrete memoryless channel with input $X$ and output $W$ is characterized by a conditional probability distribution $P_{W|X}$. The term *memoryless* stems from the fact that the channel's output depends only on the current input, and so is independent of previous channel utilizations. The *binary symmetric channel with error probability $\epsilon$* is the discrete memoryless channel with input $X \in \{0,1\}$ and conditional probability distribution such that $P_{W|X}(b,b) = 1-\epsilon$ and $P_{W|X}(1-b,b) = \epsilon$ for $b \in \{0,1\}$. Intuitively, the binary symmetric channel receives a bit as input and flips it with a certain error probability.

The *capacity* is a fundamental quantity associated to every channel. Informally, the capacity of a channel is the optimal rate at which one can communicate through the channel while ensuring that the decoding error probability goes to zero as the number of channel uses increases. Shannon [20] proved that the capacity of a channel $P_{W|X}$ is given by $\max_{P_X} I(X;W)$. In particular, it is easily shown that the capacity of the binary symmetric channel with error probability $\epsilon$ is $1-h(\epsilon)$, where $h$ is the binary entropy function.

## 3 Secret-Key Agreement by Public Discussion

### 3.1 The Source Model and the Secret-Key Rate

We study information-theoretic secret-key agreement, in which Alice and Bob want to agree on a shared secret-key, about which Eve has (almost) no information. To circumvent the trivial impossibility results, we consider the model introduced by Maurer [15,10], called *secret-key agreement by public discussion from common information.* In this model, we assume that in addition to a bidirectional authenticated noiseless channel, which Eve can listen in to but not tamper with, the parties also share some form of correlated randomness. More specifically, we will look at the setting where the correlated randomness of Alice, Bob, and Eve consists of several independent and identically distributed realizations of discrete random variables $X$, $Y$, and $Z$, respectively, distributed according to some joint probability distribution $P_{XYZ}$.

In this setting, the main quantity of interest is the maximal rate (per number of realizations of $X$, $Y$, and $Z$ received) at which Alice and Bob can generate secret-key bits, about which Eve has almost no information, as a function of the probability distribution $P_{XYZ}$. We first define what we mean by a secret-key agreement protocol.

**Definition 1.** *Given a finite probability distribution $P_{XYZ}$, an $(N, R, \epsilon)$-*secret-key agreement protocol for *$P_{XYZ}$ is an interactive protocol for Alice and Bob, which receive $X^N = (X_1, \ldots, X_N)$ and $Y^N = (Y_1, \ldots, Y_N)$, respectively, as input. Then they generate a communication transcript $C^M = (C_1, \ldots, C_M)$ (where $M$ is also a random variable) by sending messages over authenticated channels in an alternating manner. After the interaction is finished, Alice and Bob produce outputs $S_A$ and $S_B$ over the finite range $\mathcal{S}$, respectively.*

*We require that if for $i \in [N]$, the random variables $(X_i, Y_i, Z_i)$ are i.i.d. according to $P_{XYZ}$, then the following properties must hold:*

1. $H(S_A) \geq N(R - \epsilon)$;
2. $H(S_A) \geq \log|\mathcal{S}| - \epsilon$;
3. $\Pr[S_A = S_B] \geq 1 - \epsilon$;
4. $I(S_A; Z^N C^M) \leq \epsilon$.

Intuitively, property 1 in Definition 1 states that, on average, Alice and Bob extract at least $R - \epsilon$ secret bits per realization of $(X, Y, Z)$, i.e., the rate is at least $R - \epsilon$. Property 2 enforces that $S_A$ is almost uniform over $\mathcal{S}$, property 3 implies that $S_A$ and $S_B$ should coincide with high probability, and property 4 means that Eve's information, which consists of $Z^N$ and the transcript $C^M$, gives almost no information about the secret keys $S_A$ and $S_B$. We are now ready to define the secret-key rate.

**Definition 2.** *Given a finite probability distribution $P_{XYZ}$, the* secret-key rate*, denoted by $S(X; Y \| Z)$, is the supremum of all real numbers $R$ such that for all $\epsilon > 0$ and large enough $N$ there exists an $(N, R, \epsilon)$-secret-key agreement protocol for $P_{XYZ}$.*

The secret-key rate was first studied by Maurer [15,10], while Csiszár and Körner [1] studied the *one-way* secret-key rate, where only one-way communication from Alice to Bob is allowed.

The following theorem states basic bounds for the secret-key rate. The lower bound was proved by Maurer [10,12] and Csiszár and Körner [1], while the upper bound was proved by Maurer [10].

**Lemma 1 ([10, Theorem 2] and [12, Theorem 4]).** *For all finite probability distributions $P_{XYZ}$, we have*

$$I(X; Y) - \min(I(X; Z), I(Y; Z)) \leq S(X; Y \| Z) \leq \min(I(X; Y), I(X; Y|Z)).$$

Note that our definition of the secret-key rate corresponds to the so-called strong secret-key rate, which Maurer and Wolf [16] have proven to be equivalent to the weak one initially considered in the lower bounds.

### 3.2 A Special Case: The Satellite Setting

Our focus will lie on the secret-key rate of a conceptually simple, but realistic and interesting, class of distributions $P_{XYZ}$, named the *satellite setting.*

Fix real numbers $\epsilon_A, \epsilon_B, \epsilon_E \in [0, 1/2]$ and consider the following experiment:

1. Sample a bit $R \in \{0, 1\}$ uniformly at random;
2. Send $R$ to Alice, Bob, and Eve through independent binary symmetric channels with error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$, respectively. The random variables $X$, $Y$, and $Z$ are the output of these three channels.

This class of distributions was introduced by Maurer [15,10]. The satellite setting earned its name because a realistic implementation of such a scenario would consist of having a satellite orbiting the Earth which broadcasts random bits. On the ground, Alice, Bob, and Eve would be in possession of their own antennas, which they can use to listen to the satellite broadcasts. The quality of a party's antenna would then dictate how reliably they receive the random bits from the satellite. For instance, a better antenna leads to a smaller error probability.

An additional surprising benefit of this model is that secret-key agreement is possible whenever it is not trivially impossible, as stated in the following theorem of Maurer and Wolf [10,13].

**Theorem 1 ([13, Theorem 2, adapted]).** *We have* $S(X; Y \| Z) > 0$ *if and only if* $\epsilon_E > 0$ *and* $\epsilon_A, \epsilon_B < 1/2$*.*

This stands in stark contrast to the well-known fact that secret-key agreement with one-way communication from Alice to Bob (in the sense of [1]) is impossible whenever Eve's antenna is better than both Alice's and Bob's antennas, i.e. whenever $\epsilon_E < \epsilon_A$ and $\epsilon_E < \epsilon_B$.

While Theorem 1 assures that the secret-key rate is positive in all non-trivial settings, computing (or even approximating) it has proven to be a surprisingly difficult problem for most parameters $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$.

### 3.3 Advantage Distillation Protocols

The strategy used in [10,13] to prove Theorem 1 is based on the construction of an *advantage distillation protocol* in the satellite setting. In such a protocol, Alice and Bob, starting with random variables $X^N$ and $Y^N$ for $N$ large enough, interact over several rounds of communication to obtain new random variables $\hat{X}$ and $\hat{Y}$ satisfying

$$I(\hat{X}; \hat{Y}) - I(\hat{X}; \hat{Z}) > 0,$$

where $\hat{Z}$ denotes Eve's total information at the end of the protocol. Intuitively, Bob ends up with more information about Alice than Eve does, and so the protocol "distills" an advantage for Alice and Bob over Eve. The existence of such a protocol implies that $S(X; Y \| Z) > 0$. In fact,

$$S(X; Y \| Z) \geq \frac{S(\hat{X}; \hat{Y} \| \hat{Z})}{N} \geq \frac{I(\hat{X}; \hat{Y}) - I(\hat{X}; \hat{Z})}{N} > 0,$$

where the second inequality follows from Lemma 1.

The first advantage distillation protocol was the *repeater-code protocol* [15,10]. Suppose, without loss of generality, that $\epsilon_A \geq \epsilon_B$. Then, the repeater-code protocol works as follows:

1. Alice samples $C \in \{0,1\}$ uniformly at random and sends $C \oplus X^N = (C \oplus X_1, \dots, C \oplus X_N)$ to Bob over the authenticated channel;
2. Bob computes $C \oplus X^N \oplus Y^N = (C \oplus X_1 \oplus Y_1, \dots, C \oplus X_N \oplus Y_N)$ and sets $A = 1$ if $C \oplus X^N \oplus Y^N = 0^N$ or $C \oplus X^N \oplus Y^N = 1^N$. Otherwise, Bob sets $A = 0$. Then, Bob sends $A$ to Alice through the authenticated channel;
3. If $A = 1$, then Alice sets $\hat{X} = C$ and Bob sets $\hat{Y} = C \oplus X_1 \oplus Y_1$. Otherwise, if $A = 0$, then Alice and Bob set $\hat{X} = \hat{Y} = \perp$.

Eve's total information $\hat{Z}$ consists of $\hat{Z} = (Z^N, C \oplus X^N, A)$. Define $\beta := \Pr[X \neq Y] = \epsilon_A(1-\epsilon_B) + (1-\epsilon_A)\epsilon_B$ and $\alpha_{rs} := \Pr[X \oplus Y = r, X \oplus Z = s]$ for $r, s \in \{0,1\}$. It can be shown [10] that, for a fixed $N$,

$$\frac{I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z})}{N} = \frac{p_{a,N}}{N} \left( \sum_{w=0}^{N} \binom{N}{w} \frac{p_w}{p_{a,N}} \cdot h\left( \frac{p_w}{p_w + p_{N-w}} \right) - h(\beta_N) \right), \qquad (1)$$

where $h$ is the binary entropy function and:

- $p_{a,N} := \Pr[A = 1] = \beta^N + (1-\beta)^N$;
- $\beta_N := \Pr[\hat{X} \neq \hat{Y} | A = 1] = \frac{\beta^N}{\beta^N + (1-\beta)^N}$;
- $p_w := \alpha_{00}^{N-w}\alpha_{01}^{w} + \alpha_{10}^{N-w}\alpha_{11}^{w}$ is the probability that Bob accepts and $X^N \oplus Z^N$ is a specific codeword of Hamming weight $w$.

Maurer and Wolf [13] proved that, for all triples $(\epsilon_A, \epsilon_B, \epsilon_E)$ such that $\epsilon_A < 1/2$, $\epsilon_B < 1/2$, and $\epsilon_E > 0$, we have

$$I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z}) > 0$$

provided $N$ is large enough.

While the repeater-code protocol is good enough to prove that secret-key agreement is possible in the satellite setting, it guarantees only a very small lower bound on the secret-key rate, especially when $\epsilon_A$ and $\epsilon_B$ are much larger than $\epsilon_E$. This issue motivated the search for better advantage distillation protocols in the satellite setting.

Gander and Maurer [15,6] studied an improved protocol, called the *parity-check protocol*. Again, we assume, without loss of generality, that $\epsilon_A \geq \epsilon_B$. The parity-check protocol with $\ell$ rounds works as follows:

1. Alice and Bob start with initially empty strings $U_A$ and $U_B$, respectively;
2. Alice and Bob divide $X^N$ and $Y^N$ into pairs $(X_{2i}, X_{2i+1})$ and $(Y_{2i}, Y_{2i+1})$, respectively, for $i = 0, \dots, \lfloor N/2 \rfloor$;
3. For each $i$, Alice sends $X_{2i} \oplus X_{2i+1}$ to Bob via the authenticated channel;
4. Bob sets $A_i = 1$ if $X_{2i} \oplus X_{2i+1} = Y_{2i} \oplus Y_{2i+1}$. Otherwise, Bob sets $A_i = 0$. Then, he sends $A_i$ to Alice;
5. If $A_i = 1$, Alice adds $X_{2i}$ to her string $U_A$, and Bob adds $Y_{2i}$ to his string $U_B$, and they discard the remaining bits. If $A_i = 0$, Alice and Bob discard all the bits;
6. If $\ell = 1$, then Alice and Bob stop the protocol. Alice sets $\hat{X} = U_A$ and Bob sets $\hat{Y} = U_B$;
7. If $\ell > 1$ and $|U_A| \geq 2^{\ell-1}$, Alice and Bob run the parity-check protocol with $\ell - 1$ rounds on the strings $U_A$ and $U_B$. Otherwise, if $|U_A| < 2^{\ell-1}$, then Alice and Bob set $\hat{X} = \perp$ and $\hat{Y} = \perp$, respectively.

If $\hat{X}$ and $\hat{Y}$ are the outputs of the parity-check protocol with $\ell$ rounds, then each pair of bits $(\hat{X}_i, \hat{Y}_i)$ behaves like the output of a successful run of the repeater-code protocol with $N = L := 2^\ell$. Furthermore, all pairs $(\hat{X}_i, \hat{Y}_i)$ are independent of each other. It can then be shown that the parity-check protocol with $\ell$ rounds yields the lower bound

$$S(X;Y\|Z) \geq R_\ell \left( \sum_{w=0}^{L} \binom{L}{w} \frac{p_w}{p_{a,L}} \cdot h\left( \frac{p_w}{p_w + p_{L-w}} \right) - h(\beta_L) \right),$$

where

$$R_\ell \coloneqq \lim_{N\to\infty} \frac{\mathrm{E}[|\hat{X}|]}{N} = 2^{-\ell} \prod_{i=0}^{\ell-1} (\beta_{2^i}^2 + (1-\beta_{2^i})^2), \tag{2}$$

and $\beta_{2^i} = \frac{\beta^{2^i}}{\beta^{2^i}+(1-\beta)^{2^i}}$ is the error probability between Alice's and Bob's bits after $i$ rounds of the parity-check protocol.

The intuition behind Equation (2) is the following: Suppose there are $N_i$ bits left after $i$ rounds of the parity-check protocol. These $N_i$ bits are partitioned into $\lfloor N_i/2 \rfloor$ pairs (if $N_i$ is even, Alice and Bob discard a bit), and, in round $i+1$, Alice and Bob keep a bit from a given pair with probability $\beta_{2^i}^2 + (1-\beta_{2^i})^2$. Therefore, we have

$$\mathrm{E}[N_{i+1} \mid N_i \text{ bits after } i \text{ rounds}] \approx \frac{\beta_{2^i}^2 + (1-\beta_{2^i})^2}{2} \cdot N_i,$$

where $N_{i+1}$ is the random variable denoting the number of bits after $i+1$ rounds of the parity-check protocol.

The lower bound obtained through the parity-check protocol is, for most choices of error probabilities in the satellite setting, much better than the lower bound given by the repeater-code protocol.

Note that the parity-check protocol consists of the iterative application of the repeater-code protocol with length 2 to pairs of bits of $X^N$ and $Y^N$. This protocol can be further improved in a natural way for some interesting choices of error probabilities in the satellite setting by modifying the length of the repeater-code protocol that is applied iteratively, and reutilizing discarded bits from failed runs of the repeater-code protocol which are "almost" successful. We do not expand on this, since the original parity-check protocol suffices for our needs.

### 3.4 The Secret-Key Rate under a fixed Channel Quality Ratio

In this section, we formally define the two main quantities of this work: The secret-key rate per transmitted bit and the secret-key rate per second. Rather than defining them as functions of the error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$, we define them as functions of a channel quality ratio between Eve's channel and those of Alice and Bob, which are assumed to be roughly equivalent. This is motivated by the following observation: In practice, the satellite setting would, for example, be implemented by having a satellite broadcast random bits and the three parties use antennas to receive them. Moreover, we want to assume that the antennas are of a fixed size (typically Eve's antenna is large, while Alice's and Bob's antennas are small, e.g. mobile phone antennas), but the energy which the satellite uses to transmit each random bit is a parameter the protocol designer is free to choose.

If we can choose the signal strength, this clearly affects the error probabilities $\epsilon_A$, $\epsilon_B$, and $\epsilon_E$, which therefore do not directly reflect the fixed parameters. However, in a regime with significant noise power compared to the signal power (i.e., with small signal-to-noise ratio), the channel capacity is essentially proportional to the product of the surface of the receiver's antenna and the energy used to transmit the bits.

Therefore, having a fixed ratio between the antenna sizes but variable energy used to transmit a bit corresponds to having a fixed ratio of the channel capacities. As a consequence, this ratio is the relevant parameter to describe the secret-key rate as a function of. For simplicity, we assume in the following that both Alice and Bob have a channel with equal error probability $\alpha := \epsilon_A = \epsilon_B$, and we set $\gamma := \epsilon_E$ as Eve's error probability. Note that all of our lower bounds would remain true if $\epsilon_A \neq \epsilon_B$ and $\alpha := \max\{\epsilon_A, \epsilon_B\}$ instead. However, the upper bounds would no longer be valid, if $\epsilon_A$ and $\epsilon_B$ differ significantly. Let $Q$ denote the fixed size-ratio between the antennas of the honest parties (which have the same size) and Eve's antenna. Adjusting the energy per bit then corresponds to choosing $\alpha$ and $\gamma$ under the following constraint:

$$\frac{1-h(\gamma)}{1-h(\alpha)} = Q.$$

This leads us directly to our definition of the secret-key rate per transmitted bit.

**Definition 3.** *The* secret-key rate per transmitted bit under a channel quality ratio constraint *$Q$, denoted by $S(Q)$, is defined as*

$$S(Q) := \sup_{\alpha,\gamma: \frac{1-h(\gamma)}{1-h(\alpha)}=Q} S(\alpha;\gamma),$$

*where $S(\alpha;\gamma)$ is the secret-key rate of the satellite setting when $\epsilon_A = \epsilon_B = \alpha$ and $\epsilon_E = \gamma$.*

Secondly, we also define the secret-key rate per second, which is motivated by the observation that adjusting the energy used to transmit a bit can be achieved by modifying the bit-rate (the number of bits transmitted per second) while retaining a fixed power consumption. In this case, a higher bit-rate corresponds to a larger quantity of lower quality bits transmitted per second, since less energy is spent in the transmission of each bit. Since the bit-rate can be chosen at will, it is sensible to measure the secret-key rate per second instead of per bit transmitted. In order to approximate the bit-rate as a function of $\alpha$ and $\gamma$, by which we then have to multiply the secret-key rate per bit in order to obtain the secret-key rate per second, we note that the capacity is roughly inversely proportional to the bit-rate. Since this approximation is better in a regime with small signal-to-noise ratio, it is natural to choose Alice's capacity instead of Eve's. Although this is only an approximation, it should be without a significant loss of exactness in our results, since we are solely interested in the asymptotic behavior of the secret-key rate, and not the exact rate. This leads us to the following definition of the secret-key rate per second.

**Definition 4.** *The* secret-key rate per second under a channel quality ratio constraint *$Q$, denoted by $S^*(Q)$, is defined as*

$$S^*(Q) := \sup_{\alpha,\gamma: \frac{1-h(\gamma)}{1-h(\alpha)}=Q} \frac{S(\alpha;\gamma)}{1-h(\alpha)},$$

*where $S(\alpha;\gamma)$ is the secret-key rate of the satellite setting when $\epsilon_A = \epsilon_B = \alpha$ and $\epsilon_E = \gamma$.*

The main question we seek to answer in the remainder of this work is the following: How do $S(Q)$ and $S^*(Q)$ behave as $Q$ increases?

## 4 Asymptotic Behavior of the Secret-Key Rate per Random Bit and a Conjecture of Gander and Maurer

In this section, we prove that $S(Q)$ is inversely proportional to $Q^2$. Moreover, we show that the parity-check protocol is optimal in an asymptotic manner, i.e., the rate of the parity-check protocol is also inversely proportional to $Q^2$, which was first conjectured to be true by Gander and Maurer [6], based on numerical evidence.

Let $R(\ell, \alpha, \gamma)$ denote the rate per random bit generated by the parity-check protocol when $\epsilon_A = \epsilon_B = \alpha$ and $\epsilon_E = \gamma$. Furthermore, define

$$R(Q) \coloneqq \sup_{\ell,\alpha,\gamma:\, \frac{1-h(\gamma)}{1-h(\alpha)}=Q} R(\ell, \alpha, \gamma).$$

Then, we have the following result.

**Theorem 2.** *There exist constants $c_1, c_2 > 0$ such that*

$$\frac{c_1}{Q^2} \leq R(Q) \leq S(Q) \leq \frac{c_2}{Q^2}$$

*for all $Q \geq 1$.*

Here the second inequality simply represents the fact that the secret-key rate $R(Q)$ generated by the parity-check protocol is a lower bound on the general secret-key rate in the satellite setting. In the following two subsections, we prove the first and the third inequalities from Theorem 2.

### 4.1 Upper bound on $S(Q)$

In this subsection, we prove the following proposition.

**Proposition 1.** *We have*

$$S(Q) \leq \frac{4\ln(2)^2}{Q^2} < \frac{2}{Q^2}$$

*for all $Q \geq 1$.*

Before we prove Proposition 1, we need the following auxiliary result.

**Lemma 2 ([2, Theorem 2.2]).** *If $p = 1/2 - \epsilon$, we have*

$$\frac{2\epsilon^2}{\ln(2)} \leq 1 - h(p) \leq 4\epsilon^2.$$

We now proceed to the actual proof, which we split into two lemmas that we will reuse later.

**Lemma 3.** *Let $Q \geq 1$, $\alpha, \gamma \in [0, 1/2]$ such that $\frac{1-h(\gamma)}{1-h(\alpha)} = Q$, and $\delta \coloneqq 1/2 - \alpha$. We then have*

$$S(\alpha; \gamma) \leq 16\delta^4.$$

*Proof.* Note that

$$S(\alpha; \gamma) \leq I(X; Y) = 1 - h(\beta),$$

where $X$ and $Y$ are Alice's and Bob's random variables in the satellite setting with $\epsilon_A = \epsilon_B = \alpha$, and $\beta \coloneqq \Pr[X \neq Y] = 2\alpha(1-\alpha)$. Since $\beta = 2\alpha(1-\alpha) = 1/2 - 2\delta^2$, using $\epsilon \coloneqq 2\delta^2$, it follows by Lemma 2 that

$$1 - h(\beta) \leq 16\delta^4,$$

concluding the proof. □

It remains to bound $\delta^4$ by a function of $Q$.

**Lemma 4.** *Let $Q \geq 1$, $\alpha, \gamma \in [0, 1/2]$ such that $\frac{1-h(\gamma)}{1-h(\alpha)} = Q$, and $\delta := 1/2 - \alpha$. We then have*

$$2\delta^2 \leq \frac{\ln(2)}{Q}.$$

*Proof.* Using Lemma 2 we obtain

$$\frac{2\delta^2}{\ln(2)} \leq 1 - h(\alpha) = \frac{1-h(\gamma)}{Q} \leq \frac{1}{Q}.$$

□

Combining Lemmas 3 and 4 yields

$$S(Q) = \sup_{\alpha,\gamma\colon \frac{1-h(\gamma)}{1-h(\alpha)}=Q} S(\alpha;\gamma) \leq 16\delta^4 \leq \frac{4\ln(2)^2}{Q^2} < \frac{2}{Q^2}$$

for all $Q \geq 1$, concluding the overall proof of Proposition 1.

### 4.2 Lower bound on $S(Q)$

In this subsection, we prove the following proposition.

**Proposition 2.** *There exists a constant $c > 0$ such that*

$$R(Q) \geq \frac{c}{Q^2}$$

*for all $Q \geq 1$.*

Recall that the secret-key rate $R(Q)$ of the parity-check protocol under the channel quality constraint $Q$ is defined as

$$R(Q) := \sup_{\ell,\alpha,\gamma\colon \frac{1-h(\gamma)}{1-h(\alpha)}=Q} R(\ell,\alpha,\gamma).$$

In order to lower bound this supremum, we carefully choose a sequence of triples $(\ell_k, \alpha_k, \gamma_k)$ such that $R\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right)$ does not decrease too quickly when compared to $\frac{1-h(\gamma_k)}{1-h(\alpha_k)}$. In the first step, we will show that

$$R\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) \geq \frac{c_1}{k^4}$$

for some constant $c_1 > 0$, and then in a second step use that $\frac{1-h(\gamma_k)}{1-h(\alpha_k)}$ increase like $k^2$, in order to derive the desired result.

**Lower bounding the SKR of the parity-check protocol with concrete parameters.** In this section we show that for $\ell_k = 2\log(k)$ rounds, in the satellite setting with $\epsilon_A = \epsilon_B = \alpha_k = 1/2 - 1/k$, and $\epsilon_E = \gamma_k = 2/5$, the secret-key rate of the parity-check protocol $R(\ell_k, \alpha_k, \gamma_k)$ decreases inversely proportional to $k^4$. For simplicity, we drop the subscript $k$ in most terms from now on. Recall that

$$R(\ell, \alpha, \gamma) = 2^{-\ell} \Phi(L, \alpha, \gamma) \prod_{i=0}^{\ell-1} \left(\beta_{2^i}^2 + (1-\beta_{2^i})^2\right),$$

where

$$\Phi(L, \alpha, \gamma) \coloneqq \sum_{w=0}^{L} \binom{L}{w} \frac{p_w}{\beta^L + (1-\beta)^L} h\left(\frac{p_w}{p_w + p_{L-w}}\right) - h(\beta_L)$$

and $L \coloneqq 2^l$, $\beta$, and $p_w$ are defined as in Section 3.3.

Before lower bounding $R(\ell, \alpha, \gamma)$ we need a few auxiliary definitions and results. First, note that

$$p_w = \alpha_{00}^{L-w}\alpha_{01}^{w} + \alpha_{10}^{L-w}\alpha_{11}^{w} = \alpha_{00}^{L-w}\alpha_{01}^{w} + (2\alpha(1-\alpha))^L,$$

where $\alpha_{rs} = \Pr[X \oplus Y = r, X \oplus Z = s]$, since $\epsilon_A = \epsilon_B = \alpha$. Let

$$p'_w \coloneqq \alpha_{00}^{L-w}\alpha_{01}^{w}.$$

Then $p'_w$ is the probability that $X^L \oplus Z^L$ is a particular codeword of weight $w$ and $X^L = Y^L$. Furthermore,

$$p_w = p'_w + (2\alpha(1-\alpha))^L > p'_w.$$

for all $w$. We have the following lemmas.

**Lemma 5.** *We have*

$$h\left(\frac{p_w}{p_w + p_{L-w}}\right) \geq h\left(\frac{p'_w}{p'_w + p'_{L-w}}\right)$$

*for all $L$ and $w$.*

*Proof.* This lemma is a consequence of the fact that, for $a, b, x > 0$,

$$\frac{a+x}{a+b+2x} \leq \frac{a}{a+b}$$

if and only if $a \geq b$.

Fix $w \leq L/2$. Then

$$\frac{p_w}{p_w + p_{L-w}} \geq \frac{1}{2}$$

since $p_w \geq p_{L-w}$. Furthermore, it holds that

$$\frac{p'_w}{p'_w + p'_{L-w}} \geq \frac{(\alpha(1-\alpha))^L + p'_w}{2(\alpha(1-\alpha))^L + p'_w + p'_{L-w}} = \frac{p_w}{p_w + p_{L-w}} \geq \frac{1}{2}.$$

On the other hand, if $w > L/2$, then $p_w < p_{L-w}$ holds, and so

$$\frac{p'_w}{p'_w + p'_{L-w}} \leq \frac{p_w}{p_w + p_{L-w}} < 1/2.$$

This implies the desired result. □

**Lemma 6.** *Suppose $w = L(1/2 - \delta)$ for some $\delta > 0$. Then*

$$\frac{p'_{L-w}}{p'_w} = \left(\frac{\alpha_{01}}{\alpha_{00}}\right)^{2\delta L}.$$

*Proof.* It suffices to note that

$$\frac{p'_{L-w}}{p'_w} = \frac{\alpha_{00}^w \alpha_{01}^{L-w}}{\alpha_{00}^{L-w} \alpha_{01}^w} = \left(\frac{\alpha_{01}}{\alpha_{00}}\right)^{L-2w},$$

and that $L - 2w = L - 2L(1/2 - \delta) = 2\delta L$. □

Next, we lower bound $R(\ell, \alpha, \gamma)$.

**Lemma 7.** *For all $k \in \{2^j : j \in \mathbb{N}\}$, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$. We then have*

$$R(\ell_k, \alpha_k, \gamma_k) \geq \frac{1}{k^4} \Phi(k^2, \alpha_k, \gamma_k).$$

*Proof.* First, note that $L = 2^\ell = 2^{2\log(k)} = k^2$. Second, we have

$$\prod_{i=0}^{\ell-1} [\beta_{2^i}^2 + (1 - \beta_{2^i})^2] \geq \prod_{i=0}^{\ell-1} \frac{1}{2} = 2^{-\ell} = \frac{1}{k^2},$$

since $p^2 + (1-p)^2 \geq 1/2$ for all $p \in [0, 1]$. □

**Lemma 8.** *For $k \in \{2^j : j \in \mathbb{N}\}$, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$. Then there exists a positive constant $c > 0$ such that*

$$\Phi(k^2, \alpha_k, \gamma_k) \geq c$$

*for large enough $k \in \{2^j : j \in \mathbb{N}\}$.*

*Proof.* It holds that

$$\lim_{k\to\infty} h(\beta_{k^2}) = h\left(\lim_{k\to\infty} \frac{1}{1 + (1 + 8/k^2)^{k^2}}\right) = h\left(\frac{1}{1 + e^8}\right) < 5 \cdot 10^{-3}. \qquad (3)$$

Furthermore, we have

$$\begin{aligned}
&\sum_{w=0}^{k^2} \binom{k^2}{w} \frac{p_w}{\beta^{k^2} + (1-\beta)^{k^2}} \cdot h\left(\frac{p_w}{p_w + p_{k^2-w}}\right) \geq \\
&\quad \geq \sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p_w}{\beta^{k^2} + (1-\beta)^{k^2}} \cdot h\left(\frac{p_w}{p_w + p_{k^2-w}}\right) \geq \\
&\quad \geq \frac{1}{2} \sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p_w}{(1-\beta)^{k^2}} \cdot h\left(\frac{p_w}{p_w + p_{k^2-w}}\right) \geq \\
&\quad \geq \frac{1}{2} \sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p'_w}{(1-\beta)^{k^2}} \cdot h\left(\frac{p_w}{p_w + p_{k^2-w}}\right) \geq \\
&\quad \geq \frac{1}{2} \sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p'_w}{(1-\beta)^{k^2}} \cdot h\left(\frac{p'_w}{p'_w + p'_{k^2-w}}\right) \geq \\
&\quad \geq \frac{1}{2} \sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p'_w}{(1-\beta)^{k^2}} \cdot h\left(\frac{1}{1+\left(\frac{\alpha_{01}}{\alpha_{00}}\right)^{4k}}\right) \qquad (4)
\end{aligned}$$

for large enough $k$, where the first inequality holds for $k \geq 5$ since all terms in the sum are positive, the second inequality holds because

$$\beta^{k^2} + (1-\beta)^{k^2} \leq 2(1-\beta)^{k^2},$$

the third inequality follows because $p_w > p'_w$, the fourth inequality follows from Lemma 5, and the fifth inequality follows from Lemma 6 with $L = k^2$ and $\delta = 2/k$, and from the fact that

$$h\left(\frac{p'_w}{p'_w + p'_{L-w}}\right) \leq h\left(\frac{p'_{w+1}}{p'_{w+1} + p'_{L-w-1}}\right)$$

for all $w < L/2$.

In order to lower bound the binary entropy term in (4), observe that we have

$$\lim_{k\to\infty} h\left(\frac{1}{1+\left(\frac{\alpha_{01}}{\alpha_{00}}\right)^{4k}}\right) = h\left(\frac{1}{1+e^{-32/5}}\right) > 1.7 \cdot 10^{-2}, \qquad (5)$$

since

$$\lim_{k\to\infty} \left(\frac{\alpha_{01}}{\alpha_{00}}\right)^{4k} = \lim_{k\to\infty} \left(1 - \frac{8}{5k}\right)^{4k} = e^{-32/5}.$$

Next, let $W \coloneqq (w(X^{k^2} \oplus Z^{k^2}) \mid X^{k^2} = Y^{k^2})$, where $w(u)$ denotes the weight of a string $u$. Then

$$\sum_{w=k^2(1/2-2/k)}^{k^2(1/2+2/k)} \binom{k^2}{w} \frac{p'_w}{(1-\beta)^{k^2}} = \Pr[|W - k^2/2| \leq 2k]. \qquad (6)$$

It suffices now to find a suitable lower bound for $\Pr[|W - k^2/2| \leq 2k]$. In order to do that, we will apply Chebyshev's inequality. First, note that

$$\mathrm{E}[W] = k^2 \cdot \frac{\alpha_{01}}{\alpha_{00} + \alpha_{01}} = k^2 \cdot \frac{\alpha^2(1-\gamma) + (1-\alpha)^2\gamma}{\alpha^2 + (1-\alpha)^2} \leq \frac{k^2}{2}.$$

Second, algebraic manipulation yields

$$\frac{k^2/2 - \mathrm{E}[W]}{k} = \frac{1}{5/2 + 10/k^2} \leq \frac{2}{5},$$

which implies that

$$k^2/2 - 2k/5 \leq \mathrm{E}[W] \leq k^2/2$$

for all $k$. Thus, we have

$$k^2(1/2 - 2/k) = k^2/2 - 2k \leq \mathrm{E}[W] - k,$$

and

$$k^2(1/2 + 2/k) = k^2/2 + 2k \geq \mathrm{E}[W] + k.$$

Therefore,

$$\Pr[|W - k^2/2| \leq 2k] \geq \Pr[|W - \mathrm{E}[W]| \leq k] \geq 1 - \frac{\mathrm{Var}[W]}{k^2} \geq \frac{3}{4}, \qquad (7)$$

where the second inequality follows from Chebyshev's inequality, and the third inequality follows from the fact that

$$\mathrm{Var}[W] = k^2 \cdot \Pr[X \neq Z | X = Y](1 - \Pr[X \neq Z | X = Y]) \leq \frac{k^2}{4}.$$

Combining (4), (5), (6), and (7) yields

$$\sum_{w=0}^{k^2} \binom{k^2}{w} \frac{p_w}{\beta^{k^2} + (1-\beta)^{k^2}} \cdot h\left(\frac{p_w}{p_w + p_{k^2-w}}\right) > \frac{1}{2} \cdot \frac{3}{4} \cdot 1.7 \cdot 10^{-2} > 5 \cdot 10^{-3} > h(\beta_{k^2})$$

for large enough $k \in \{2^j : j \in \mathbb{N}\}$. □

Combining the previous two lemmas yields the main result of this section.

**Lemma 9.** *For all $k \in \{2^j : j \in \mathbb{N}\}$, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$. Then there exists a constant $c > 0$ such that we have*

$$R(\ell_k, \alpha_k, \gamma_k) \geq \frac{c}{k^4}$$

*for large enough $k \in \{2^j : j \in \mathbb{N}\}$.*

*Proof.* This follows directly by combining Lemmas 7 and 8.

**Deriving a lower bound in $Q$.** It now remains to show that Lemma 9 actually implies the desired lower bound in $Q$. We proceed by first showing that $\frac{1-h(\gamma_k)}{1-h(\alpha_k)}$ increases like $k^2$, and then substitute this term by $Q$.

**Lemma 10.** *For all $k \in \mathbb{N}$, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$. We then have*

$$\frac{1-h(\gamma_k)}{1-h(\alpha_k)} \geq \frac{k^2}{200}.$$

*Proof.* Note that $1 - h(\gamma_k) = 1 - h(0.4) > 1/50$ for all $k$. Moreover, Lemma 2 yields

$$1 - h(\alpha_k) \leq \frac{4}{k^2}$$

and thus,

$$\frac{1-h(\gamma_k)}{1-h(\alpha_k)} \geq \frac{(1-h(\gamma_k))k^2}{4} > \frac{k^2}{200}$$

for all $k$. □

**Lemma 11.** *For all $k \in \{2^j : j \in \mathbb{N}\}$, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$. We then have*

$$R\left(\frac{k^2}{200}\right) \geq R(\ell_k, \alpha_k, \gamma_k).$$

*Proof.* First, observe that $R(Q)$ is a decreasing function of $Q$. Indeed, fix $Q < Q'$. For each choice $(\alpha', \gamma')$ for $R(Q')$, we can obtain a choice $(\alpha, \gamma)$ for $R(Q)$ by setting $\alpha = \alpha'$ and $\gamma > \gamma'$. It follows immediately that running the parity-check protocol with the same parameters for the new choice $(\alpha, \gamma)$ yields a larger secret-key rate, and thus $R(Q) \geq R(Q')$. Combining this with Lemma 10 immediately yields

$$R\left(\frac{k^2}{200}\right) \geq R\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right).$$

Finally, observe that by definition we have

$$R\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) = \sup_{\ell,\alpha,\gamma: \frac{1-h(\gamma)}{1-h(\alpha)} = \frac{1-h(\gamma_k)}{1-h(\alpha_k)}} R(\ell, \alpha, \gamma) \geq R(\ell_k, \alpha_k, \gamma_k),$$

concluding the proof. □

We are now ready to actually prove Proposition 2 by substituting $k^2/200$ with $Q$.

*Proof (Proposition 2).* Combining Lemmas 9 and 11 we know that there exists a constant $c_1 > 0$ such that

$$R\left(\frac{k^2}{200}\right) \geq \frac{c_1}{k^4}$$

for large enough $k \in \{2^j : j \in \mathbb{N}\}$. Substituting $Q \coloneqq k^2/200$ and $c_2 \coloneqq c_1/200^2 > 0$ we obtain

$$R(Q) \geq \frac{c_2}{Q^2},$$

for large enough $Q \in \{4^j/200 \mid j \in \mathbb{N}\}$. This inequality can be extended to all large enough values of $Q$ by noting that, for every $Q \geq 1$, there is an integer $j$ such that

$$Q \leq \frac{4^j}{200} \leq 6Q.$$

In fact, if $j$ is such that $Q \leq 4^j \leq 4Q$, which we know exists, then

$$Q \leq \frac{4^{j+4}}{200} = \frac{256 \cdot 4^j}{200} \leq 6Q.$$

Using that $R(\cdot)$ is a decreasing function, we thus obtain, if $j$ is large enough,

$$R(Q) \geq R\left(\frac{4^{j+4}}{200}\right) \geq \frac{c_2}{(6Q)^2} = \frac{c_3}{Q^2},$$

where $c_3 = c_2/6^2 > 0$ is a positive constant independent of $Q$.

The inequality can finally be extended to all $Q \geq 1$ as follows. Let $Q_0$ be such that $R(Q_0) \geq c_3/Q_0^2$. Then, set $c_4 = c_3/Q_0^2 \leq c_3$. For all $1 \leq Q < Q_0$ we have

$$R(Q) \geq R(Q_0) \geq c_4 \geq \frac{c_4}{Q^2},$$

which implies the desired result with $c = c_4$. □

*Remark 1.* The proof of Proposition 2 also goes through if we choose $\ell_k$, $\alpha_k$ and $\gamma_k$ in a way that the channel quality ratio $Q$ increases linearly with $k$, e.g. by choosing $\ell_k = \log(k)$, $\alpha_k = 1/2 - 1/\sqrt{k}$ and $\gamma_k = 2/5$. We opted for the current settings because the derivation is slightly easier to follow.

## 5 Asymptotic Behavior of the Secret-Key Rate per Second

In this section, we establish the exact asymptotic behavior of $S^*(Q)$ as a function of $Q$, up to a multiplicative constant. Recall that $R(\ell, \alpha, \gamma)$ denotes the rate generated by the parity-check protocol in the satellite setting when $\epsilon_A = \epsilon_B = \alpha$ and $\epsilon_E = \gamma$. Define

$$R^*(Q) \coloneqq \sup_{\ell,\alpha,\gamma:\frac{1-h(\gamma)}{1-h(\alpha)}=Q} \frac{R(\ell,\alpha,\gamma)}{1-h(\alpha)}.$$

We have the following result.

**Theorem 3.** *There exist constants $c_1, c_2 > 0$ such that*

$$\frac{c_1}{Q} \leq R^*(Q) \leq S^*(Q) \leq \frac{c_2}{Q}$$

*for all $Q \geq 1$.*

*Proof.* The overall proof is very similar to the one of Theorem 2 and reuses most of its lemmas. Again, the second inequality represents the trivial fact that the secret-key rate $R^*(Q)$ generated by the parity-check protocol is a lower bound on the general secret-key rate in the satellite setting.

We first prove the upper bound on $S^*(Q)$. Fix $Q \geq 1$ and $\alpha, \gamma \in [0, 1/2]$ satisfying $\frac{1-h(\gamma)}{1-h(\alpha)} = Q$, and let $\delta \coloneqq 1/2 - \alpha$. Then, by Lemma 2, we have

$$1 - h(\alpha) \geq \frac{2\delta^2}{\ln(2)}.$$

Combining this with Lemmas 3 and 4 yields

$$\frac{S(\alpha;\gamma)}{1-h(\alpha)} \leq 8\ln(2)\delta^2 \leq \frac{4\ln(2)^2}{Q}.$$

Since the choice of $\alpha$ and $\gamma$ was arbitrary, we have

$$S^*(Q) = \sup_{\alpha,\gamma:\frac{1-h(\gamma)}{1-h(\alpha)}=Q} \frac{S(\alpha;\gamma)}{1-h(\alpha)} \leq \frac{4\ln(2)^2}{Q} < \frac{2}{Q}$$

for all $Q \geq 1$. This concludes the proof on the upper bound on $S^*(Q)$.

It now remains to prove the lower bound on $R^*(Q)$. To this end, let $\ell_k = 2\log(k)$, $\alpha_k = 1/2 - 1/k$, and $\gamma_k = 2/5$ for all $k \in \{2^j : j \in \mathbb{N}\}$. First, observe that by definition we have

$$R^*\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) = \sup_{\ell,\alpha,\gamma:\frac{1-h(\gamma)}{1-h(\alpha)}=\frac{1-h(\gamma_k)}{1-h(\alpha_k)}} \frac{R(\ell,\alpha,\gamma)}{1-h(\alpha)} \geq \frac{R(\ell_k,\alpha_k,\gamma_k)}{1-h(\alpha_k)}.$$

Using Lemma 9 we know that there exists a constant $c > 0$ such that

$$R^*\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) \geq \frac{c}{k^4(1-h(\alpha_k))}$$

for large enough $k \in \{2^j : j \in \mathbb{N}\}$. Moreover, Lemma 2 yields

$$1 - h(\alpha_k) \leq \frac{4}{k^2},$$

and thus we obtain

$$R^*\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) \geq \frac{c}{4k^2}$$

for large enough $k \in \{2^j : j \in \mathbb{N}\}$. Next, observe that analogously to $R(Q)$, $R^*(Q)$ is a decreasing function of $Q$. Combining this with Lemma 10 immediately yields

$$R^*\left(\frac{k^2}{200}\right) \geq R^*\left(\frac{1-h(\gamma_k)}{1-h(\alpha_k)}\right) \geq \frac{c}{4k^2}$$

for large enough $k \in \{2^j : j \in \mathbb{N}\}$. Substituting $Q := k^2/200$ and $c' := c/800 > 0$ we obtain

$$R^*(Q) \geq \frac{c'}{Q},$$

for large enough $Q \in \{4^j/200 \mid j \in \mathbb{N}\}$. This inequality can be extended to all values of $Q \geq 1$ using the same technique as in the proof of Proposition 2 on Page 18. □

## 6 Conclusions and Open Problems

In this paper we investigated the secret-key rate in the satellite model, where we assume an upper bound $Q$ on quality ratio between the honest parties' and Eve's receiving equipment, which we modeled as a constraint on the capacity ratio between the binary symmetric channels. As a first contribution, we have shown that the secret-key rate per transmitted bit asymptotically behaves like $1/Q^2$, and moreover proved that the parity-check protocol achieves this asymptotic rate, yielding a positive answer to a conjecture by Gander and Maurer [6]. As a second contribution, we investigated the secret-key rate per second – a quantity of much higher practical interest – and proved that this rate asymptotically decreases only like $1/Q$. Since in realistic scenarios $Q$ has to be assumed very large, this is a significant improvement over the known bounds, highlighting that secret-key exchange in the satellite model could be practical.

While those results exactly characterize the asymptotic secret-key rate in the satellite setting, the gap between the constants in the upper and lower bounds of Theorem 2 is quite large. In fact, the constant in the upper bound is $4\ln(2)^2$, which is approximately 1.92, while the constant in the lower bound is on the order of $10^{-5}$. This observation raises a natural question: How can we significantly narrow this gap? In order to make the constant in the upper bound smaller, one can attempt to replace the mutual information in the proof of Proposition 1 by a better upper bound on the secret-key rate, such as the intrinsic mutual information [11], the reduced intrinsic mutual information [19], or the upper bound found in [7]. On the other hand, we believe that tightening the lower bound significantly would require substantially different techniques than the one used in the proof of Proposition 2.

## References

1. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography. i. secret sharing. IEEE Transactions on Information Theory 39(4), 1121–1132 (1993)
2. Calabro, C.: The Exponential Complexity of Satisfiability Problems. Ph.D. thesis, University of California, San Diego (2009)
3. Cover, T., Thomas, J.: Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing). Wiley-Interscience (2006)
4. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. IEEE Transactions on Information Theory 24(3), 339–348 (1978)
5. Csiszár, I., Narayan, P.: Secrecy capacities for multiple terminals. IEEE Transactions on Information Theory 50(12), 3047–3061 (2004)
6. Gander, M.J., Maurer, U.M.: On the secret-key rate of binary random variables. In: Proceedings of the 1994 IEEE International Symposium on Information Theory (ISIT 1994). p. 351. IEEE (1994)
7. Gohari, A.A., Anantharam, V.: Information-theoretic key agreement of multiple terminals: Part i. IEEE Transactions on Information Theory 56(8), 3973–3996 (2010)
8. Hayashi, M., Tyagi, H., Watanabe, S.: Secret key agreement: General capacity and second-order asymptotics. IEEE Transactions on Information Theory 62(7), 3796–3810 (2016)
9. Liu, S., Van Tilborg, H.C.A., Van Dijk, M.: A practical protocol for advantage distillation and information reconciliation. Designs, Codes and Cryptography 30(1), 39–62 (2003), https://doi.org/10.1023/A:1024755209150
10. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory 39(3), 733–742 (1993)
11. Maurer, U.M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Transactions on Information Theory 45(2), 499–514 (1999)
12. Maurer, U.: The strong secret key rate of discrete random triples. In: Blahut, R.E., Costello, D.J., Maurer, U., Mittelholzer, T. (eds.) Communications and Cryptography. The Springer International Series in Engineering and Computer Science (Communications and Information Theory), vol. 276, pp. 271–285. Springer, Boston, MA (1994)
13. Maurer, U., Wolf, S.: Towards characterizing when information-theoretic secret key agreement is possible. In: Kim, K., Matsumoto, T. (eds.) Advances in Cryptology – ASIACRYPT 1996. Lecture Notes in Computer Science, vol. 1163, pp. 196–209. Springer, Berlin, Heidelberg (1996)
14. Maurer, U.M.: Conditionally-perfect secrecy and a provably-secure randomized cipher. Journal of Cryptology 5(1), 53–66 (1992), https://doi.org/10.1007/BF00191321
15. Maurer, U.M.: Protocols for secret key agreement by public discussion based on common information. In: Brickell, E.F. (ed.) Advances in Cryptology – CRYPTO 1992. Lecture Notes in Computer Science, vol. 740, pp. 461–470. Springer, Berlin, Heidelberg (1992)

16. Maurer, U.M., Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free. In: Preneel, B. (ed.) Advances in Cryptology — EUROCRYPT 2000. Lecture Notes in Computer Science, vol. 1807, pp. 351–368. Springer, Berlin, Heidelberg (2000)
17. Naito, M., Watanabe, S., Matsumoto, R., Uyematsu, T.: Secret key agreement by reliability information of signals in gaussian maurer's model. In: Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT 2008). pp. 727–731. IEEE (2008)
18. Ozarow, L.H., Wyner, A.D.: Wire-tap channel ii. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) Advances in Cryptology – EUROCRYPT 1984. Lecture Notes in Computer Science, vol. 209, pp. 33–50. Springer, Berlin, Heidelberg (1984)
19. Renner, R., Skripsky, J., Wolf, S.: A new measure for conditional mutual information and its properties. In: Proceedings of the 2003 IEEE International Symposium on Information Theory (ISIT 2003). p. 259. IEEE (2003)
20. Shannon, C.: A mathematical theory of communication. Bell System Technical Journal 27(3), 379–423 (1948)
21. Shannon, C.: Communication theory of secrecy systems. Bell System Technical Journal 28(4), 656–715 (1949)
22. Tyagi, H., Watanabe, S.: A bound for multiparty secret key agreement and implications for a problem of secure computing. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 369–386. Springer, Berlin, Heidelberg (2014)
23. Wyner, A.D.: The wire-tap channel. Bell System Technical Journal 54(8), 1355–1387 (1975)