A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF

Ashwin Jha and Mridul Nandi

Indian Statistical Institute, Kolkata
{ashwin.jha1991,mridul.nandi}@gmail.com

Abstract. The Coefficients H Technique (also called H-technique), developed by Patarin in circa '91, is a tool to obtain upper bounds on distinguishing advantages. This tool is known to provide relatively simpler and (in some cases) tight bound proofs in comparison to some other well-known tools such as the Game-playing technique and Random Systems methodology. In this systematization of knowledge (SoK) paper, we aim to provide a brief survey on the H-technique. The SoK is in four parts: First, we redevelop the necessary nomenclatures and tools required to study the security of any symmetric key design, especially in the H-technique setting. Second, we give a full description of H-technique and some related tools. Third, we give (simple) H-technique based proofs for some popular symmetric-key designs, across different paradigms. Finally, we show that H-technique can actually provide optimal bounds on distinguishing advantage.

Keywords: provable security · coefficients H technique · Feistel · ENR · LDT · HCTR · TET

1 Introduction

The general goal of any cryptographic scheme is to achieve some kind of indistinguishability (pseudorandom behavior) from an ideal (random) system. In this respect, distinguishing games have a key role in defining cryptographic security definitions. In symmetric key cryptography, pseudorandom functions or PRFs [GGM84] and (strong) pseudorandom permutations or (S)PRPs [LR85] have been defined via distinguishing games. Informally, an adversary interacts with either the keyed construction (real system) of our interest or with the ideal system such as a uniform random function or permutation. The adversary's goal is to reliably tell with whom it interacts. If no adversary can distinguish the real system from the ideal system with non-negligible probability, we say that the construction is *pseudo-ideal* (e.g., PRF or PRP).

On a closer inspection of security proofs for most of the symmetric key designs, we mostly see that the underlying primitives are first replaced by some ideal primitives. This can be justified using the hybrid argument at the cost of the distinguishing advantages of each of the underlying primitives. Once we replace these underlying primitives by ideal candidates, we obtain the so-called *hybrid* or *quasi random* construction (information theoretically indistinguishable from ideal candidates). The next and the final step is to provide security analysis of the hybrid construction. This is done in purely information theoretic setting. So, in a way, the provable security analysis guarantees the security of the construction if the underlying primitives are indistinguishable from their ideal counterparts. In this paper we focus on the security analysis of such quasi random constructions.

1.1   Revisiting Some Popular Proof Techniques

Symmetric-key provable security results can be broadly classified according to the proof techniques used. Different constructions may warrant different proof techniques depending upon the proof complexity, the desired security bound, and in some cases, author's biasness. We briefly discuss some of these techniques.

GAME-PLAYING TECHNIQUE: Arguably the most popular, and certainly the oldest proof technique is the so-called Game-playing technique [BR06, Sho04]. At a high level the proofs based on this technique use a sequence of games, where each game is an interaction between the adversary and an oracle. The proof starts with the game corresponding to the real construction and proceeds toward the game corresponding to the ideal system by making stepwise transitions to some intermediate games. Each transition may gain some advantage to the adversary, and the cumulative advantage of all such transitions gives the security bound. This high-level view of game-playing technique is clearly visible in several early works [GM84, Yao82]. In later years, Shoup extensively used this technique [Sho00b, Sho02, Sho04, CS03b, CS03a, AGKS05].

The contemporary version of this tool is due to Bellare and Rogaway's systematized treatment [BR06], called the *code-based game-playing* technique. In this flavor the games are written in pseudocode language, each having their own internal variables and flags. Two games are said to be identical if they are syntactically identical. Usually the syntactical identity breaks when one of the game sets a boolean flag *bad* to true. Consequently, adversary's distinguishing advantage in any game is upper bounded by the probability that this flag gets set. Game-playing technique has been used to prove security for almost all types of security notion in symmetric-key cryptography. For example game-playing technique was employed in the following:

- (Tweakable) (S)PRPs such as 3 and 4 rounds of Feistel [LR85], CLRW2 [LST12] etc.;

- PRFs and MACs such as CBC-MAC [BKR00, BPR05], ECBC, FCBC and XCBC [BR05], PMAC+ [Yas10], sum of ECBC [Yas11] etc.;

- (Tweakable) Enciphering Schemes such as CMC [HR03], EME [HR04], TET [Hal07], HCH [CS08], HCTR [WFW05], XLS [RR07], HEH [Sar07, Sar09] etc.;

- Online Ciphers such as HCBC1 and HCBC2 [BBKN12], TC1, TC2 and TC3 [RZ11], POEx [FLLW16], XTC [JN18] etc.;

- AE schemes such as SIV [RS06], OCB [RBBK01, Rog04, KR11], COPA [ABL+13], POET [AFF+14] etc.

COEFFICIENTS H-TECHNIQUE: Patarin formally introduced the Coefficient H-technique tool [Pat08a] at SAC 2008, although the technique was already used in some of his earlier works [Pat90, Pat91, Pat97, Pat98, Pat03]. In fact, it was Vaudenay who first reported the H-technique publicly in his decorrelation theory [Vau03]. However, he mentioned that the technique is described in Patarin's PhD thesis [Pat91] written in French. Independently, Bernstein rediscovered a similar variant of the result in [Ber99], as the *interpolation theorem*. This was later strengthened by Nandi [Nan06] as the *strong interpolation theorem*. Later, Chen and Steinberger gave a renewed interpretation of H-technique in their work on key alternating ciphers [CS14]. They hoped that *"paper will serve as a useful additional tutorial on (or introduction to) Patarin's H-coefficient technique, which still seems to suffer from a lack of exposure"*. This modernization indeed popularized the H-technique, as to the best of our knowledge, all the recent applications consider this renewed description of H-technique. We remark that Mennink's uses of H-coefficient technique in [MMH+14, Men15] offer a simpler yet similar exposition over relatively simple constructions.

At a very high level, H-technique concentrates on the input-output tuple generated by a adversary's interaction with the oracle at hand, called the transcript. In the simplest case, the H-technique says that the distinguishing advantage is bounded by one minus a lower bound of the ratio of the probability that an *attainable* transcript can be realized by the real oracle to the probability that it can be realized by the ideal oracle. A transcript is called attainable if the probability that it can be realized by the ideal oracle is non-zero.

For example, suppose an adversary $\mathbf{A}$ wants to distinguish a uniform random function $\boldsymbol{\rho} : \mathscr{D} \to \mathscr{D}$ (the real oracle) from a uniform random permutation $\boldsymbol{\pi} : \mathscr{D} \to \mathscr{D}$ (the ideal oracle) by making q queries to the oracle at hand. A typical attainable transcript for this distinguishing game would look like $\omega = ((x_1, y_1), (x_2, y_2), \ldots, (x_q, y_q))$, where x_i and y_i denote the i-th query and response, respectively. Since, the transcript is attainable, we must have $x_i = x_j \iff y_i = y_j$ for all $i \neq j$. Without loss of generality, we may assume that $x_i \neq x_j$, as $\mathbf{A}$ does not get any benefits by duplicate queries. Let Θ_0 and Θ_1 be the transcript random variable generated by $\mathbf{A}$'s interaction with $\boldsymbol{\pi}$ and $\boldsymbol{\rho}$, respectively. Then, it is easy to see that

$$\Pr[\Theta_0] = \Pr_{\boldsymbol{\pi}}[\boldsymbol{\pi}(x_1) = y_1, \ldots, \boldsymbol{\pi}(x_q) = y_q] = \frac{1}{2^n(2^n - 1) \cdots (2^n - q + 1)},$$

and

$$\Pr[\Theta_1] = \Pr_{\boldsymbol{\rho}}[\boldsymbol{\rho}(x_1) = y_1, \ldots, \boldsymbol{\rho}(x_q) = y_q] = \frac{1}{2^{nq}}.$$

Thus, the ratio of the above two probabilities is lower bounded as

$$\frac{\Pr[\Theta_0]}{\Pr[\Theta_1]} = \frac{2^n(2^n - 1) \cdots (2^n - q + 1)}{2^{nq}} \geq \left(1 - \frac{q(q-1)}{2^{n+1}}\right).$$

Finally, coefficients H technique says that $\mathbf{A}$'s advantage in distinguishing $\boldsymbol{\rho}$ from $\boldsymbol{\pi}$ is upper bounded by $q^2/2^{n+1}$.

The above example is quite simple. However, in many cases, it might be possible that certain transcripts are bad (may lead to inconsistency or are improbable) in the real or ideal world. In those cases, we also have to add the probability of realizing a bad transcript in the ideal world to the distinguishing advantage.

Note that we have consciously ignored some key technical details, such as $\mathbf{A}$'s computational resources and its probabilistic nature, to give a short overview on how the H-technique tool works. In later sections, we will give a formal description of H-technique in full generality. Nevertheless, it can still be observed that H-technique, unlike the game-playing technique, does not make any implicit assumptions on the probability distribution of the oracles and requires explicit probability computation in both the worlds to bound the ratio. In recent years, there has been a steady rise in the application of H-technique. Some of the schemes which have been analyzed with H-technique include:

- (Online) PRP/SPRPs such as Feistel [Pat03, Pat04, Nan10], MHCBC and MCBC [Nan08], (Tweakable) Even-Mansour [LPS12, CS14, CLL+14, CS15b, CLS15, CS15a], FMix [BN15], OleF [BN16], two-round LDT [CLMP17], CLRW2 [Men18] etc.;

- PRFs and MACs such as CBC-MAC [JN16], EWCDM [CS16, MN17], HaT and NaT [CLS17], 1k-PMAC+ [DDN+17], EHtM [DJN17], ZMAC+ [LN17], DWCDM [DDNY18] etc.;

- AE schemes such as ELmE [DN14], COFB [CIMN17], OCB3 [BN17], Beetle [CDNY18], GCM-SIV [BHT18] etc.

MAURER'S RANDOM SYSTEM METHODOLOGY: At Eurocrypt '02, Maurer introduced the random system methodology (also called Maurer's methodology) for indistinguishability proofs [Mau02]. The random system methodology defines a sequence of conditional probabilities associated with a system, i.e the interaction between an adversary and an oracle. Further it defines the notion of a monotone binary condition associated to a system. Two systems are said to be equivalent until a monotone binary condition B, if they give rise to same sequence of conditional probabilities while $B = 0$. This formalizes the identical until bad philosophy of the game-playing technique. Expectedly, the advantage is bounded by the probability that the monotone condition changes to 1. Note that in contrast the H-technique considers the joint probability distribution for the systems. The application of Maurer's methodology were, first shown in some indistinguishability and composition proofs [Mau02, MP03, MP04, MPR07]. Later, Maurer's methodology was also applied to prove the security of PMAC, TMAC and XCBC [MM07], ENR and its variants [Min09, MI11, Min15], and XTX [MI15].

EXPECTATION METHOD: The expectation method by Hoang and Tessaro [HT16] is a generalization of the H-technique, where the expected value of the ratio is used instead of a constant (independent of the transcript) lower bound. The expectation method has been applied to get exact bounds in [HT16] and to get multi-user security in [HT16, HT17, GW18].

COUPLING TECHNIQUE: The coupling technique [Mir02, MRS09, HR10, LPS12] is a very useful tool for upper bounding the distinguishing advantage of iterated structures. For example it has been applied, among others, to the iterated Even-Mansour [LPS12], iterated tweakable Even-Mansour [CLS15], and cascaded LRW2 [LS13] schemes. The high level idea is simple: The coupling lemma is used to bound the statistical distance of r-rounds of some iterated scheme from uniform distribution. This step is non-adaptive in nature. Now, given the non-adaptive bound, a straightforward application of the composition lemma from [MP04] gives adaptive security for $2r$ many rounds of the iterated scheme. The coupling technique is known for notoriously loose bounds. This is because even if the coupling lemma gives a tight bound for the non-adaptive security of r rounds, it does not say anything on the adaptive security of r rounds. It might be possible to get the desired level of adaptive security at r rounds itself, but the technique requires $2r$ many rounds.

χ^2-METHOD AND HELLINGER DISTANCE: The χ^2-method was proposed by Dai, Hoang and Tessaro [DHT17], where the statistical distance is bounded in terms of the expectation of the conditional χ^2-distances. The χ^2-method gave improved bounds in some cases, such as sum of permutations and EDM [DHT17, BN18b], where the H-technique failed. Bhattacharya and Nandi explored the applications of χ^2-method in the PRF security of a sum of permutation variant [BN18c] and the indifferentiability of sum of permutations [BN18a]. Recently, beyond birthday security analysis of three-round LDT [CMN18] has been shown. The χ^2 method is quite useful in certain cases where it is easy to compute the conditional probabilities such as sum of permutation. But there is no clear picture on its utility in cases where the conditional probability is not that easy to compute, such as hash based schemes.

The application of a different distance notion to bound the statistical distance is not new. In fact, much earlier Steinberger used the Hellinger distance [Ste12] to study the key alternating ciphers. But this method is yet to be explored for other constructions.

1.2 Our Contribution

The contributions of this SoK are fourfold. First, we reformulate an interactive algorithm in its functional view, which provides the language of the proof of symmetric key designs. Second, we give a complete description of the H-technique tool along with some related tools. Third, we revisit the security analysis of some of the well known symmetric-key

constructions across different paradigms. Specifically, we give H-technique based proofs for the following constructions:

1. Hash-based schemes: Hash-then-PRF, Hash-then-TBC [LN17] and ENR [Min09, MI11]. In case of ENR we study a generic scheme, called NR*, which allows for simple proofs for both ENR and LDT [CLMP17].

2. Feistel cipher: 3-round Luby-Rackoff [LR85] and 3-round tweakable block cipher based Luby-Rackoff [CDMS10].

3. SPRP enciphering schemes: HCTR [WFW05] and TET [Hal07].

4. Beyond the birthday bound secure PRFs: SoP [HWKS98, BI99, Luc00] and SoEM22 [CLM19].

Finally, we show that the extended version of H-technique can achieve optimal security bounds. As a side result, we give an alternate proof for composition of non-adaptive PRPs [MP04].

The above given constructions are chosen for varied reasons. In some cases, we simplify the existing game-playing or Maurer's methodology based proofs. For example, see the proof of ENR, Fesitel ciphers, and SoP. Yet in some cases, we unify the proofs of various related schemes into one general result. For example see the general proof of NR*. For SPRP enciphering schemes, we provide the first proof in H-technique.

1.2.1 Organization of the paper

We start off with developing the notations and conventions, in section 2, that will be used in the paper. In section 3, we formalize the model for bounded query interactive algorithms. In section 4, we describe the H-technique tool and its variant the expectation method. We also give a brief on how to capture the random system methodology in H-technique. In section 5, 6 and 7, we give alternate proofs for some hash based schemes, Feistel-like schemes and popular SPRP schemes, respectively. Section 8 gives proofs for beyond the birthday bound secure PRFs, namely SoP and SoEM22. In section 9 we prove the optimality of H-technique and use similar ideas to give an alternate proof for the non-adaptive to adaptive PRP composition.

2 Preliminaries

2.1 Notation

We simply write the set $\{1, 2, \ldots, m\}$ as $[m]$. We denote a q-tuple $(x_1, \ldots, x_q)$ as x^q. We sometime use the notation $\{x^q\}$ to denote the set $\{x_i : 1 \leq i \leq q\}$. For a q-tuple $v = v^q$, we sometimes denote v_i as $v|_i$. A binary sequence b^q is called monotone if $b_{i+1} \geq b_i$ for all $i \in [q-1]$. So any binary monotone sequence must be of the form $0^i 1^{q-i}$ for some i.

For a set $\mathcal{X}$, we write $\mathcal{X}^{(r)}$ for the set of all r tuples $x^r \in \mathcal{X}^r$ such that $x_1, \ldots, x_r$ are distinct. We write $N(N-1) \cdots (N-r+1)$ as $(N)_r$. If the size of the set $\mathcal{X}$ is N then clearly, $|\mathcal{X}^{(r)}| = (N)_r$.

A function $g(a, b)$ is functionally independent of b if for all a, b, b', $g(a, b) = g(a, b')$. In this case there exists a function g' such that for all a, b, $g(a, b) = g'(a)$.

Given an index set $\mathcal{I}$, we denote an indexed family (or a tuple) as $\{x_i\}_{i \in \mathcal{I}}$ or $x^{\mathcal{I}}$.[1] More formally, it can be represented as a function from the index set to some set where x_i values belong. Note that x^q is a shorthand notation for $x^{[q]}$ where $[q]$ is the index set.

---

[1]Note that it is different from the set $\{x_i : i \in \mathcal{I}\}$. For some $i \neq j$, x_i and x_j may be same and we ignore repetition in the set representation. Whereas, in the indexed family we allow repetition.

NOTATIONS ON COMPATIBILITY. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted as $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$. Similarly, the set of all permutations over $\mathcal{Y}$ is denoted as $\mathsf{Perm}(\mathcal{Y})$.

1. A pair of tuples (x^q, y^q) is called function compatible if $x_i = x_j \Rightarrow y_i = y_j$. We denote it as $x^q \rightsquigarrow y^q$.

2. A pair of tuples (x^q, y^q) is called permutation compatible if $x_i = x_j \Leftrightarrow y_i = y_j$. We denote it as $x^q \leftrightsquigarrow y^q$.

3. A pair of triples (t^q, x^q, y^q) is called tweakable permutation compatible if $(t_i, x_i) = (t_j, x_j) \Leftrightarrow (t_i, y_i) = (t_j, y_j)$. We denote it as $x^q \overset{t^q}{\leftrightsquigarrow} y^q$ (equivalently, $(t^q, x^q) \leftrightsquigarrow (t^q, y^q)$).

2.2 Statistical Distance

Statistical distance (also known as total variation [GS02] in Statistics community) is a metric on the set of probability functions over a finite set Ω. This is the most common metric in cryptography. As we see later it has a close relationship with the distinguishing advantage.

Definition 2.1 (statistical distance)**.** Let Pr_0 and Pr_1 be two probability functions over a finite set Ω. We define statistical distance between Pr_0 and Pr_1 as

$$\|\mathsf{Pr}_0 - \mathsf{Pr}_1\| := \frac{1}{2} \sum_{x \in \Omega} |\mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)|.$$

When X, Y are two random variables over Ω, we define $\Delta(\mathsf{X} ; \mathsf{Y}) = \|\mathsf{Pr}_\mathsf{X} - \mathsf{Pr}_\mathsf{Y}\|$.

It is easy to verify that the statistical distance satisfies the symmetry and **triangle inequality**. Moreover, it is always lying between zero and one. It is one if and only if the support[2] of the probability distributions are disjoint and it is zero if and only if the distributions are same.

Definition 2.2. Given two probability distributions Pr_0 and Pr_1 over Ω, we associate two sets

$$\Omega_> = \{x \in \Omega : \mathsf{Pr}_0(x) > \mathsf{Pr}_1(x)\}, \text{ and}$$
$$\Omega_\geq = \{x \in \Omega : \mathsf{Pr}_0(x) \geq \mathsf{Pr}_1(x)\}.$$

Lemma 2.1. *For any two probability distributions* Pr_0 *and* Pr_1*, we have*

$$\max_{\mathscr{E}} \left(\mathsf{Pr}_0(\mathscr{E}) - \mathsf{Pr}_1(\mathscr{E})\right) = \sum_{x \in \Omega} \max\{0, \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)\} \;\; = \;\; \|\mathsf{Pr}_0 - \mathsf{Pr}_1\|.$$

The maximum is achieved at $\mathscr{E}$ *if and only if* $\Omega_> \subseteq \mathscr{E} \subseteq \Omega_\geq$*.*

Proof. It is easy to see that the maximum value of $\mathsf{Pr}_0(\mathscr{E}) - \mathsf{Pr}_1(\mathscr{E})$ is achieved at $\mathscr{E}$ if and only if $\Omega_> \subseteq \mathscr{E} \subseteq \Omega_\geq$ (for any $x \notin \Omega_\geq$, the contribution $\mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)$ is negative). Now, we note that

$$\max\{0, \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)\} = \begin{cases} 0 & \text{if } x \notin \Omega_> \\ \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x) & \text{if } x \in \Omega_>. \end{cases}$$

---

[2]The set of all elements of having positive probabilities.

So,

$$\sum_{x \in \Omega} \max\{0, \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)\} = \sum_{x \in \Omega_>} \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)$$
$$= \max_{\mathscr{E}} \big(\mathsf{Pr}_0(\mathscr{E}) - \mathsf{Pr}_1(\mathscr{E})\big).$$

This proves the first equality. Now, we write

$$2\|\mathsf{Pr}_0 - \mathsf{Pr}_1\| = \sum_{x \in \Omega_>} |\mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)| + \sum_{x \notin \Omega_>} |\mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)|.$$

The first sum can be simplified as

$$\sum_{x \in \Omega_>} \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x) = \mathsf{Pr}_0(\Omega_>) - \mathsf{Pr}_1(\Omega_>).$$

Similarly, the second sum can be simplified to

$$\sum_{x \notin \Omega_>} \mathsf{Pr}_1(x) - \mathsf{Pr}_0(x) = \mathsf{Pr}_1(\Omega_>^c) - \mathsf{Pr}_0(\Omega_>^c)$$
$$= \mathsf{Pr}_0(\Omega_>) - \mathsf{Pr}_1(\Omega_>)$$

If we add these two sums, we obtain the second equality. $\qquad\square$

Corollary 1. *Let* $\mathsf{X}_0 \sim \mathsf{Pr}_0$ *and* $\mathsf{X}_1 \sim \mathsf{Pr}_1$. *Let* $\epsilon_{opt}(x) = \max\{0, 1 - \frac{\mathsf{Pr}_1(x)}{\mathsf{Pr}_0(x)}\}$ *for all* x *in the support of* X_0. *Then,*
$$\|\mathsf{Pr}_0 - \mathsf{Pr}_1\| \;=\; \mathsf{Ex}\big[\epsilon_{opt}(\mathsf{X}_0)\big].$$

3   Models for Interactive Algorithms

3.1   Probabilistic Function

A probabilistic function (defined below) is a mathematical model for the black-box behavior of a probabilistic algorithm. We also use the same object to model probabilistic interactive algorithms.

Definition 3.1 (probabilistic function)**.** A *probabilistic function* with an input space $\mathscr{X}$ and an output space $\mathscr{Y}$ is a function $f : \mathscr{R} \times \mathscr{X} \to \mathscr{Y}$ for some finite set $\mathscr{R}$, called **random coin space**. We also simply write (abusing notation) $f : \mathscr{X} \xrightarrow{*} \mathscr{Y}$ suppressing the notation for random coin space.

If the random coin space is singleton (i.e. degenerated) we simply ignore the random coin space. In this case, the probabilistic function is reduced to a function. Given an input $x \in \mathscr{X}$, we first sample $\mathsf{R} \xleftarrow{*} \mathscr{R}$ (in most cases uniformly) and then we define an output random variable $f(x) := f(\mathsf{R}, x)$ over $\mathscr{Y}$. So, for all $y \in \mathscr{Y}$,

$$\mathsf{p}_x^f(y) := \mathsf{Pr}[f(x) = y] = \sum_{\substack{r \\ f(r,x)=y}} \mathsf{Pr}[\mathsf{R} = r] \qquad (1)$$

Definition 3.2. With each probabilistic function $f : \mathscr{X} \xrightarrow{*} \mathscr{Y}$, we associate a family of probability functions over $\mathscr{Y}$ (indexed by the input space $\mathscr{X}$)

$$\mathsf{p}^f := \{\mathsf{p}_x^f \mid x \in \mathscr{X}\}$$

where $\mathsf{p}_x^f(y) := \mathsf{Pr}[f(x) = y]$. We call the p^f **probabilistic system** associated with the probabilistic function f.

We would like to note that the probabilistic function and probabilistic system are analogous with random variable and its probability distribution.

Example 1 (Keyed Functions). This is an important example for cryptography. Many cryptographic designs are viewed as keyed functions. Let F be a keyed function family $\{F_k \mid k \in \mathscr{K}\}$ such that for all key $k \in \mathscr{K}$, $F_k : \mathscr{X} \to \mathscr{Y}$.

We sample key $\mathsf{K} \leftarrow_\$ \mathscr{K}$ and treat it as a random coin, we obtain a probabilistic function (abusing notation) $F : \mathscr{X} \xrightarrow{*} \mathscr{Y}$, mapping x to $F(\mathsf{K}, x) := F_\mathsf{K}(x)$ (also written as $\mathsf{K}(x)$, whenever K actually represents the function F).

Notation. Given a probabilistic function $f : \mathscr{X} \xrightarrow{*} \mathscr{Y}_1 \times \mathscr{Y}_2$ we write $f = (f_1, f_2)$ where $f(r, x) = (f_1(r, x), f_2(r, x))$ and $f_i : \mathscr{X} \xrightarrow{*} \mathscr{Y}_i$, $i = 1, 2$. The probabilistic functions f_1 and f_2 are basically two components of f and we also call them truncated probabilistic functions. This can be similarly extended for the Cartesian product of more than two sets.

3.2   Function Models of Interactive Algorithms and Their Interaction

An interactive algorithm is modeled as a (probabilistic) interactive Turing machine [GMR85, GGM84]. In this paper, probabilistic functions are modeled for interactive algorithms. This model is general enough to capture finite and bounded interaction between two interactive algorithms (i.e. the number of interaction between two algorithms is bounded by some fixed positive integer, say q).

Definition 3.3 (function models of interactive algorithms). Let q be a positive integer.
1. <u>Joint Response Function</u>:- A *q-joint* $(\mathscr{X}, \mathscr{Y})$ *response function* is a probabilistic function $\mathbf{F} : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}^q$ such that for all random coin r, the mapping $x^q \mapsto \mathbf{F}(r, x^q)|_i$ is *functionally independent* of $x_{i+1}, \ldots, x_q$.

2. <u>Joint Query Function</u>:- A probabilistic function $\mathscr{A} : \mathscr{Y}^q \xrightarrow{*} \mathscr{X}^q$ is called *q-joint* $(\mathscr{X}, \mathscr{Y})$ *query function* if for all random coin r, the mapping $y^q \mapsto \mathscr{A}(r, y^q)|_i$ is *functionally independent* of $y_i, \ldots, y_q$. Moreover, it is called

- **nonadaptive** if $\mathscr{A}(r, y^q)$ is functionally independent of y^q and

- **deterministic** if the random coin space is singleton (we simply drop the random coin space notation and write it as a function $\mathscr{A} : \mathscr{Y}^q \to \mathscr{X}^q$).

We also simply call q-joint $(\mathscr{X}, \mathscr{Y})$ query function and q-joint $(\mathscr{X}, \mathscr{Y})$ response function by $(\mathscr{X}, \mathscr{Y})$ joint query function and $(\mathscr{X}, \mathscr{Y})$ joint response function respectively.

The joint query and response function together capture the interaction. A joint query function captures the functional view of an interactive algorithm that initiates the interaction and a joint response function captures the functional view of the corresponding oracle algorithm. When a joint query function $\mathscr{A}$ interacts with a joint response function $\mathbf{F}$, x_1 only depends on the random coin of $\mathscr{A}$, whereas y_1 depends on x_1 and the random coin of $\mathbf{F}$. Similarly, x_2 depends on y_1 and its random coin, and y_2 depends on x_1, x_2 and its random coin. In this way, we can define x^q and y^q based on random coins of $\mathscr{A}$ and $\mathbf{F}$. The pair (x^q, y^q) is called transcript (which is a function of the pairs of random coins of $\mathscr{A}$ and $\mathbf{F}$).

We now formally define the transcript random variable. From the given conditions of the definitions of the joint response and query functions, there exist functions $\mathscr{A}_i$ and $\mathbf{F}_i$, $i \in [q]$, such that for all y^q, $\mathscr{A}(r, y^q)|_i = \mathscr{A}_i(r, y^{i-1})$ and for all x^q, $\mathbf{F}(r', x^q)|_i = \mathbf{F}_i(r', x^i)$.

Definition 3.4 (transcript). Let $\mathscr{A}$ and $\mathbf{F}$ be $(\mathscr{X}, \mathscr{Y})$ joint query function and joint response function respectively. Let $\mathscr{A}_i$ and $\mathbf{F}_i$ be defined as above. We define the *transcript* random variable as $\tau(\mathscr{A}^{\mathbf{F}}) = (\mathsf{X}^q, \mathsf{Y}^q)$ where X_i's and Y_i's are defined recursively as follows:

$$\mathsf{X}_i = \mathscr{A}_i(\mathsf{R}, \mathsf{Y}^{i-1}), \quad \mathsf{Y}_i = \mathbf{F}_i(\mathsf{R}', \mathsf{X}^i), \quad 1 \le i \le q$$

and R and R' are random coins of $\mathscr{A}$ and $\mathbf{F}$ respectively.

From the above definition, it is clear that for any fixed random coins r and r', the transcript is the unique pair (x^q, y^q) such that $\mathscr{A}(r, y^q) = x^q$ and $\mathbf{F}(r', x^q) = y^q$. So for any $(x^q, y^q) \in \mathscr{X}^q \times \mathscr{Y}^q$, using the independence of random coins of $\mathscr{A}$ and $\mathbf{F}$, we have

$$\Pr[\tau(\mathscr{A}^{\mathbf{F}}) = (x^q, y^q)] = \Pr[\mathscr{A}(y^q) = x^q] \times \Pr[\mathbf{F}(x^q) = y^q]. \tag{2}$$

In terms of the probabilistic systems $\mathsf{p}^{\mathscr{A}}$ and $\mathsf{p}^{\mathbf{F}}$ associated with $\mathscr{A}$ and $\mathbf{F}$ respectively (see Definition 3.2), we can write the probability realizing a transcript $\tau = (x^q, y^q)$ as

$$\Pr[\tau(\mathscr{A}^{\mathbf{F}}) = (x^q, y^q)] = \mathsf{p}^{\mathscr{A}}_{y^q}(x^q) \times \mathsf{p}^{\mathbf{F}}_{x^q}(y^q)$$

So, the transcript probability is determined by the probabilistic systems $\mathsf{p}^{\mathscr{A}}$ and $\mathsf{p}^{\mathbf{F}}$.

EXTENDED TRANSCRIPT. The transcript is an information obtained by the joint query function through an interaction. Sometimes we release an extra information, say S, in addition to the transcript to the adversary. This is given only after all interaction is done. In other words, the queries x^q can not functionally depend on S, whereas S can depend on queries. To formalize this, let us define an extended response function.

Definition 3.5 (extended transcript). An $\mathscr{S}$-*extended* $(\mathscr{X}, \mathscr{Y})$ *joint response function* is a probabilistic function $\bar{\mathbf{F}} = (\mathbf{F}, \mathsf{S}) : \mathscr{X}^q \xrightarrow{*} \mathscr{Y}^q \times \mathscr{S}$. For any $(\mathscr{X}, \mathscr{Y})$ joint query function $\mathscr{A}$, we define the *(extended) transcript of* $\mathscr{A}^{\bar{\mathbf{F}}}$ as

$$\bar{\tau}(\mathscr{A}^{\mathbf{F}}) = \tau(\mathscr{A}^{\bar{\mathbf{F}}}) = (\tau(\mathscr{A}^{\mathbf{F}}) , \mathsf{S}(\mathsf{X}^q)) := (\tau(\mathscr{A}^{\mathbf{F}(\mathsf{R}, \cdot)}) , \mathsf{S}(\mathsf{R}, \mathsf{X}^q))$$

where R denotes the random coin of $\bar{\mathbf{F}}$ and $\tau(\mathscr{A}^{\mathbf{F}}) = (\mathsf{X}^q, \mathsf{Y}^q)$. We call S *adjoined random variable* to $\mathbf{F}$.

MBO EXTENSION. Now we describe a popular joint extended response function. A MBO (monotone binary output) extension $\bar{\mathbf{F}}$ is an $\{0, 1\}^q$-extension of a joint response function $\mathbf{F}$ such that the support of the adjoined random variable S is the set of all monotone binary sequences. We call the extended transcript $\tau(\mathscr{A}^{\bar{\mathbf{F}}})$ good if $\mathsf{S} = 0^q$, otherwise we call it bad. Informally, S denotes whether some bad event occurred on some query or not. This is done by setting the bit corresponding to the query index to 1. Since S is monotone in nature, whenever the bad flag sets to 1, it continues to be 1 for the rest of the queries. This justifies the support of S is $\{0^i 1^{q-i} : 0 \le i \le q\}$.

Later we will see that a simpler and equally powerful extension would be to release a binary variable B to denote whether bad happened or not in the whole transcript. So $\mathsf{B} = 0$ if $\mathsf{S} = 0^q$, otherwise, $\mathsf{B} = 1$. We adjoin the random variable B only instead of an MBO S.

For an extended system $\bar{\mathbf{F}} = (\mathbf{F}, \mathsf{S})$, we can similarly associate a probabilistic system defined as

$$\mathsf{p}^{\bar{\mathbf{F}}}_{x^q}(y^q, s) = \Pr[\mathbf{F}(x^q) = y^q, \mathsf{S} = s] \tag{3}$$

For any $(x^q, y^q, s) \in \mathscr{X}^q \times \mathscr{Y}^q \times \mathscr{S}$ we have

$$\Pr[\tau(\mathscr{A}^{\bar{\mathbf{F}}}) = (x^q, y^q, s)] = \Pr[\mathscr{A}(y^q) = x^q] \times \Pr[\mathbf{F}(x^q) = y^q, \mathsf{S} = s].$$

3.3 Examples of Response Function

Keyed Function. Let F be a keyed function family $\{F_k \mid k \in \mathscr{K}\}$ such that for all key $k \in \mathscr{K}$, $F_k : \mathscr{X} \to \mathscr{Y}$. We also view F as a function $F : \mathscr{K} \times \mathscr{X} \to \mathscr{Y}$ where $F(k, x) = F_k(x)$. If we choose key $\mathsf{K} \leftarrow_{\$} \mathscr{K}$ and treat it as a random coin, we obtain a joint response function (we call it (deterministic) keyed function) as

$$\mathbf{F}(k, x^q) = (F(k, x_1), \dots, F(k, x_q)), \quad x^q \in \mathscr{X}^q.$$

Keyed Strong Permutation. When $F(k, \cdot)$ is a permutation on $\mathscr{Y}$ for all key $k \in \mathscr{K}$, one can consider an interaction in which a joint query function makes queries to the inverse function also. To capture this, we associate a new keyed function

$$F_k^{\pm} : \{1, -1\} \times \mathscr{Y} \to \mathscr{Y}$$

mapping $(1, x)$ to $F_k(x)$ and mapping $(-1, x)$ to $F_k^{-1}(x)$. We also write $F_k(\delta, x) := F_k^{\delta}(x)$. The joint response function associated to the keyed function $F^{\pm}$ is denoted as $\mathbf{F}^{\pm}$ and we call it keyed strong permutation.

Definition 3.6. Given a triple of tuples $(\delta^q, x^q, y^q) \in \{1, -1\}^q \times \mathscr{Y}^{2q}$ we associate a **forward only representation** (δ^q, a^q, b^q) as

$$(a_i, b_i) = \begin{cases} (x_i, y_i) & \text{if } \delta_i = 1 \\ (y_i, x_i) & \text{otherwise.} \end{cases}$$

The forward only representation is an equivalent representation of the original triple as we can uniquely reconstruct the original triple from it.

Suppose (δ^q, a^q, b^q) is a *forward only representation* of (δ^q, x^q, y^q). Then, $F_k(a_i) = b_i$ for all i if and only if $F_k^{\delta_i}(x_i) = y_i$ for all i. So for every (δ^q, x^q, y^q), we have

$$\Pr[\mathbf{F}^{\pm}(\delta^q, x^q) = y^q] = \Pr[\mathbf{F}(a^q) = b^q].$$

So, *the probabilistic system associated to $\mathbf{F}^{\pm}$ is completely determined by the probabilistic system associated with $\mathbf{F}$.*

3.3.1 Some Ideal Random Systems

We describe some popular ideal random systems. Let $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{T}$ be finite sets such that $N = |\mathscr{Y}|$.

Definition 3.7 (random function)**.** An $(\mathscr{X}, \mathscr{Y})$ random function is an $(\mathscr{X}, \mathscr{Y})$ joint response function $\boldsymbol{\rho}$ such that for all $x^q \in \mathscr{X}^q$ and $y^q \in \mathscr{Y}^q$ with $x^q \rightsquigarrow y^q$ (function compatible),

$$\Pr[\boldsymbol{\rho}(x^q) = y^q] = N^{-s}$$

where s is the number of distinct x values present in x^q. In all other cases the probability is zero.

Definition 3.8 (random permutation)**.** An $\mathscr{Y}$ random permutation is an $(\mathscr{Y}, \mathscr{Y})$ joint response function $\boldsymbol{\pi}$ such that for all $x^q, y^q \in \mathscr{Y}^q$ with $x^q \leftrightsquigarrow y^q$ (permutation compatible),

$$\Pr[\boldsymbol{\pi}(x^q) = y^q] = \frac{1}{(N)_s}$$

where s is the number of distinct x_i values present in x^q. In all other cases the probability is zero.

As described before, we can also similarly define a strong random permutation $\boldsymbol{\pi}^{\pm}$ which provides the access of inverse. More precisely, for any (δ^q, x^q, y^q), $\Pr[\boldsymbol{\pi}^{\pm}(\delta^q, x^q) = y^q] = \frac{1}{(N)_s}$ provided $a^q \leftrightsquigarrow b^q$ where (δ^q, a^q, b^q) is the forward only transcript of (δ^q, x^q, y^q) and s is the number of distinct a_i values present in a^q (which is same as the number of distinct values present in b^q).

We have defined the above ideal systems through their probabilistic systems. One can define these through deterministic keyed functions. For a random function, the key space is $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$, the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$. For any $k \in \mathsf{Func}(\mathcal{X}, \mathcal{Y})$, and $x \in \mathcal{X}$, we define $\boldsymbol{\rho}(k, x) = k(x)$. For a random permutation, the key space is $\mathsf{Perm}(\mathcal{Y})$, the set of all permutations over $\mathcal{Y}$. For any $k \in \mathsf{Perm}(\mathcal{Y})$, and $x \in \mathcal{Y}$, we define $\boldsymbol{\pi}(k, x) = k(x)$.

One can easily verify that the probabilistic systems view is same as the deterministic keyed function view. The two views are actually same functions defined over two different domains.

TWEAKABLE RANDOM PERMUTATION. Given a tweakable permutation compatible tuple (t^q, x^q, y^q), we associate a tuple of positive numbers $(c_1, \ldots, c_r)$ as follows: Let $t'_1, \ldots, t'_r$ denote the distinct tweaks present in t^q. We write $\mathsf{mcoll}(t^q) = c^r$ where $c_i = |\{x_j : t_j = t'_i\}|$. Clearly, $\sum_i c_i = q$ when (t^q, x^q, y^q) is tweakable permutation compatible tuple. Basically, $\sum_i c_i$ represents the number of distinct (t_i, x_i) pairs present in (t^q, x^q).

Definition 3.9 (tweakable random permutation). An $(\mathcal{T}, \mathcal{Y})$ tweakable random permutation is an $(\mathcal{T} \times \mathcal{Y}, \mathcal{Y})$ joint response function $\widetilde{\boldsymbol{\pi}}$ such that for all tweakable permutation compatible tuple (t^q, x^q, y^q) with $\mathsf{mcoll}(t^q) = c^r$,

$$\Pr[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] = \prod_{i=1}^{r} \frac{1}{(N)_{c_i}}. \tag{4}$$

The probability is zero for all other tuples (t^q, x^q, y^q).

We can write the above probability into another equivalent form. For each i, we define s_i as the number of $j < i$, such that $t_j = t_i$. Then, we have

$$\Pr[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] = \prod_{i=1}^{q} \frac{1}{N - s_i}. \tag{5}$$

Intuitively, when we response the ith query (t_i, x_i), we look at all those j for which $t_j = t_i$. Let $\mathcal{S}_i$ be the set of all y_j values for which $t_j = t_i$. The response of the ith query is to select an element randomly from $\mathcal{S}_i^c$ (in other words, without replacement sample for the same tweak values).

To realize this probabilistic system, we define a keyed function corresponding to it. Let the key space be $\mathsf{Func}(\mathcal{T}, \mathsf{Perm}(\mathcal{Y}))$, the set of all functions from the tweak space to the set of all permutations. So, if k is a key and t is a tweak, $k(t)$ is a permutation over $\mathcal{Y}$. We write $k(t)(x)$ as $k(t, x)$ or $\widetilde{\boldsymbol{\pi}}(k, (t, x))$. One can again check that the probabilistic system associated with this joint response function is same as the tweakable random permutation as defined above.

4 H-Technique Tools

4.1 Distinguisher and Its Advantage

Let $\mathbf{F}$ and $\mathbf{G}$ be two $(\mathcal{X}, \mathcal{Y})$ joint response functions and $\mathscr{A}$ be an $(\mathcal{X}, \mathcal{Y})$ joint query system with random coin space $\mathscr{R}$. Let $b : \mathscr{R} \times \mathcal{X}^q \times \mathcal{Y}^q \to \{0, 1\}$ be a binary function (also called decision function). We call the pair $(\mathscr{A}, b)$, denoted as $\mathscr{A}_b$, a **distinguisher**.

1. The algorithm $\mathscr{A}$ obtains a transcript $\tau = (x^q, y^q)$.

2. The function b finally makes a decision based on the transcript and the random coin initially sampled by $\mathscr{A}$.

More formally, the output of $\mathscr{A}_b^{\mathbf{F}}$ is $b(\mathsf{R}, \tau(\mathscr{A}^{\mathbf{F}}))$ where R is the random coin of $\mathscr{A}$ which is used to generate the transcript $\tau(\mathscr{A}^{\mathbf{F}})$. We now define

$$\boxed{\Delta_{\mathscr{A}_b}(\mathbf{F} \; ; \; \mathbf{G}) := \left| \mathsf{Pr}[\mathscr{A}_b^{\mathbf{F}} \to 1] - \mathsf{Pr}[\mathscr{A}_b^{\mathbf{G}} \to 1] \right|.}$$

Let $\mathscr{E}$ be the set of all tuples (r, x^q, y^q) for which b returns 1. From the equivalent definition of statistical distance (see Lemma 2.1) we have

$$\Delta_{\mathscr{A}_b}(\mathbf{F} \; ; \; \mathbf{G}) \leq \Delta((\mathsf{R}, \tau(\mathscr{A}^{\mathbf{F}})) \; ; \; (\mathsf{R}, \tau(\mathscr{A}^{\mathbf{G}}))). \tag{6}$$

Moreover, equality is achieved if we define the decision function, called optimal decision function and denoted b_{opt}, as follows:

$$b_{opt}(r, x^q, y^q) = 1 \Leftrightarrow \mathsf{Pr}[\mathsf{R} = r, \tau(\mathscr{A}^{\mathbf{F}}) = (x^q, y^q)] \geq \mathsf{Pr}[\mathsf{R} = r, \tau(\mathscr{A}^{\mathbf{G}}) = (x^q, y^q)].$$

COMPLEXITY. Note that the computation of b_{opt} may not be efficient. In general, we consider two types of complexities for an adversary (both for the query system and the decision function) to measure the efficiency of an algorithm. One type considers all computational complexities which includes e.g. time, memory etc. The other type considers the data complexities which includes the number of queries (which is q in our case), total number of bits in all queries, the size of the largest queries etc. As we are interested in information theoretic analysis, we only keep complexity related to oracle calls and we consider only **unbounded time adversaries** only. We always assume the decision making function b is optimum and hence $\Delta_{\mathscr{A}_b}(\mathbf{F} \; ; \; \mathbf{G}) = \Delta((\mathsf{R}, \tau(\mathscr{A}^{\mathbf{F}})) \; ; \; (\mathsf{R}, \tau(\mathscr{A}^{\mathbf{G}})))$. So we simply write a distinguisher as $\mathscr{A}$ (by its joint query function) ignoring the notation b.

4.1.1   Conventions

Now we state some conventions which can be assumed without loss of generality in this paper. This would simplify the distinguishing advantage analysis.

1. **Distinguishers are deterministic**: Given any query function $\mathscr{A}$, and for a fixed random coin r, let $\mathscr{A}[r] := \mathscr{A}(r, \cdot)$ denote the deterministic query function which basically runs $\mathscr{A}$ with the random coin r. It is easy to verify that $\Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \mathbf{G}) = \mathsf{Ex}_{\mathsf{R}}(\Delta_{\mathscr{A}[\mathsf{R}]}(\mathbf{F} \; ; \; \mathbf{G}))$ and hence there exists r_0 for which $\mathsf{Ex}_{\mathsf{R}}(\Delta_{\mathscr{A}[\mathsf{R}]}(\mathbf{F} \; ; \; \mathbf{G})) \leq \Delta_{\mathscr{A}[r_0]}(\mathbf{F} \; ; \; \mathbf{G})$. Hence,

$$\Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \mathbf{G}) \leq \Delta_{\mathscr{A}[r_0]}(\mathbf{F} \; ; \; \mathbf{G}).$$

2. **No redundant queries**: In this paper we only consider deterministic keyed functions. An adversary $\mathscr{A}$ interacting with a deterministic keyed function is called redundant if $\mathscr{A}$ makes two identical queries (i.e. $x_i = x_j$ for some $i < j$). An adversary $\mathscr{A}$ interacting with a deterministic keyed strong permutation $\mathbf{F}^{\pm}$ is called redundant if for some $i < j$, $(\delta_j, x_j) = (\delta_i, x_i)$ or $(\delta_j, x_j) = (-\delta_i, y_i)$ where y_i is the response of the ith query. Note that, in this case, $(a_j, b_j) = (a_i, b_i)$ where (δ^q, a^q, b^q) denotes the forward only transcript. The response of jth query is uniquely determined from the ith query. Similarly, we define redundant queries for tweakable keyed permutation. The ith query (δ_i, t_i, x_i) is called redundant if there is $j < i$ with $t_j = t_i$, either $(\delta_j, x_j) = (\delta_i, x_i)$ or $(\delta_j, y_j) = (-\delta_i, x_i)$.

   Note that for all redundant queries the response is uniquely determined from the previous query-responses and hence without loss of generality we may ignore those queries. So, *we assume that all such adversaries are non-redundant.*

4.2 Security Definitions

Here we define PRF, PRP, SPRP and their tweakable versions against adaptive and nonadaptive adversaries. Let $\mathbb{A}(\theta_D)$ (and $\mathbb{A}_{\mathrm{na}}(\theta_D)$) denote the set of all adversaries $\mathscr{A}$ using at most θ_D data complexity in adaptive ways (and nonadaptive ways respectively). If the computational complexity is unbounded (or infinity) in all these definitions, we simply drop the notation θ_C.

1. • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{prf}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\rho})$,

    • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{nprf}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}_{\mathrm{na}}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\rho})$,

2. • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{prp}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\pi})$,

    • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{sprp}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F}^{\pm} \; ; \; \boldsymbol{\pi}^{\pm})$,

    • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{nprp}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}_{\mathrm{na}}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\pi})$,

3. • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{tprp}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \widetilde{\boldsymbol{\pi}})$,

    • $\mathbf{Adv}_{\mathbf{F}}^{\mathrm{tsprp}}(\theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_D)} \Delta_{\mathscr{A}}(\mathbf{F}^{\pm} \; ; \; \widetilde{\boldsymbol{\pi}}^{\pm})$.

4.3 H-Technique

We describe the extended version of H-technique. The basic or standard version, also called coefficients H technique, is a simple instantiation of the extended version (viewing the adjoined random variable as a degenerated or fixed constant).

Lemma 4.1 (Extended H-technique). *Suppose $\bar{\mathbf{F}} := (\mathbf{F}, \mathsf{S})$ and $\bar{\mathbf{G}} := (\mathbf{G}, \mathsf{S}')$ are two $\mathcal{S}$-extended $(\mathcal{X}, \mathcal{Y})$ response systems. Let Ω denote the set of all attainable transcripts, i.e. the support of $\Pr_{\bar{\mathbf{G}}}$. Suppose there is a set $\Omega_{\mathsf{bad}} \subseteq \Omega$ such that for all $(x^q, y^q, s) \notin \Omega_{\mathsf{bad}}$,*

$$\frac{\Pr[\mathbf{F}(x^q) = y^q, \mathsf{S} = s]}{\Pr[\mathbf{G}(x^q) = y^q, \mathsf{S}' = s]} \geq (1 - \epsilon)$$

for some $\epsilon \geq 0$. Then, for any $(\mathcal{X}, \mathcal{Y})$ adversary $\mathscr{A}$,

$$\Delta_{\mathscr{A}}(\mathbf{F}; \mathbf{G}) \leq \Delta(\bar{\tau}(\mathscr{A}^{\mathbf{F}}); \bar{\tau}(\mathscr{A}^{\mathbf{G}})) \leq \Pr[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \Omega_{\mathsf{bad}}] + \epsilon. \tag{7}$$

A proof of the H-technique is given among others in [Pat91, Pat08a, Nan06, CS14]. Here we give a short proof for the sake of completeness.

Proof. For any adversary $\mathscr{A}$, it is easy to see that $\Delta_{\mathscr{A}}(\mathbf{F}; \mathbf{G}) \leq \Delta(\bar{\tau}(\mathscr{A}^{\mathbf{F}}); \bar{\tau}(\mathscr{A}^{\mathbf{G}}))$. This holds as the decision making function is free to discard the additional information. Let $\Pr_0 = \Pr_{\bar{\mathbf{G}}}$ and $\Pr_1 = \Pr_{\bar{\mathbf{F}}}$. Then $\Omega_{>}$ is well-defined (see Definition 2.2). From Lemma 2.1, we have

$$\Delta(\bar{\tau}(\mathscr{A}^{\mathbf{F}}); \bar{\tau}(\mathscr{A}^{\mathbf{G}})) = \sum_{\omega \in \Omega} \max\{0, \Pr_{\bar{\mathbf{G}}}(\omega) - \Pr_{\bar{\mathbf{F}}}(\omega)\}$$

$$= \sum_{\omega \in \Omega_{>}} \Pr_{\bar{\mathbf{G}}}(\omega) \cdot \left(1 - \frac{\Pr_{\bar{\mathbf{F}}}(\omega)}{\Pr_{\bar{\mathbf{G}}}(\omega)}\right)$$

$$\leq \sum_{\omega \in \Omega_{>} \cap \Omega_{\mathsf{bad}}} \Pr_{\bar{\mathbf{G}}}(\omega) + \epsilon \sum_{\omega \in \Omega_{>} \setminus \Omega_{\mathsf{bad}}} \Pr_{\bar{\mathbf{G}}}(\omega)$$

$$\leq \Pr[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \Omega_{\mathsf{bad}}] + \epsilon.$$

$\square$

4.4   Expectation Method

Hoang and Tessaro [HT16] introduced a somewhat generalized version of the H-technique, termed as the *expectation method*. We describe it in a slightly different way just to suit our notational conformity.

Lemma 4.2 (Expectation Method). *Suppose* $\bar{\mathbf{F}} := (\mathbf{F}, \mathsf{S})$ *and* $\bar{\mathbf{G}} := (\mathbf{G}, \mathsf{S}')$ *are two* $\mathcal{S}$-*extended* $(\mathcal{X}, \mathcal{Y})$ *response systems. Let* Ω *be the support of* $\mathsf{Pr}_{\bar{\mathbf{G}}}$ *and suppose there is a set* $\Omega_{\mathsf{bad}} \subseteq \Omega$, *and a non-negative function* $\epsilon : \mathcal{X}^q \times \mathcal{Y}^q \times \mathcal{S} \to [0, \infty)$ *such that* $\forall \bar{\tau} = (x^q, y^q, s) \notin \Omega_{\mathsf{bad}}$, *we have*

$$\frac{\mathsf{Pr}[\mathbf{F}(x^q) = y^q, \mathsf{S} = s]}{\mathsf{Pr}[\mathbf{G}(x^q) = y^q, \mathsf{S}' = s]} \geq 1 - \epsilon(\bar{\tau}).$$

Then, for any $(\mathcal{X}, \mathcal{Y})$ *adversary* $\mathscr{A}$,

$$\Delta_{\mathscr{A}}(\mathbf{F} \ ; \ \mathbf{G}) \leq \mathsf{Pr}[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \Omega_{\mathsf{bad}}] + \mathsf{Ex}\left[\epsilon\left(\bar{\tau}(\mathbf{A}^{\mathbf{G}})\right)\right]. \tag{8}$$

One can set $\epsilon(\bar{\tau}) = 1$, for $\bar{\tau} \in \Omega_{\mathsf{bad}}$ to avoid the separate calculation of bad transcript probability. The extended H-technique is obtained from Eq. 8, when ϵ is a constant function. From CS's view of the H-technique, the expectation method is like partitioning the set of transcripts into singletons. So one could argue that the expectation method should achieve optimality. This is possible if one could identify a suitable definition of the ϵ function and give a tight estimation for the expectation value. Specifically, for $\bar{\tau} \in \mathcal{X}^q \times \mathcal{Y}^q \times \mathcal{S}$, we define $\epsilon(\bar{\tau})$ as

$$\epsilon(\bar{\tau}) = \begin{cases} 1 - \frac{\mathsf{Pr}_{\bar{\mathbf{F}}}(x^q, y^q, s)}{\mathsf{Pr}_{\bar{\mathbf{G}}}(x^q, y^q, s)} & \text{when } \mathsf{Pr}_{\bar{\mathbf{G}}}(x^q, y^q, s) > \mathsf{Pr}_{\bar{\mathbf{F}}}(x^q, y^q, s), \\ 0 & \text{otherwise.} \end{cases}$$

Now equality holds in Eq. 8, if we apply the expectation method with $\Omega_{\mathsf{bad}} = \emptyset$.

5   Hash-based Constructions

Now we briefly describe the power of (extended) H-technique by proving the security of some hash based constructions. A hash function $\mathbf{H} : \mathcal{M} \xrightarrow{*} \mathcal{X}$ is called ϵ-*universal* if for all $m \neq m' \in \mathcal{M}$, $\mathsf{Pr}_{\mathsf{H} \leftarrow \$ \mathscr{K}}[\mathsf{H}(m) = \mathsf{H}(m')] = \leq \epsilon$.

5.1   Hash-then-PRF

CONSTRUCTION. Let $\mathbf{H} : \mathcal{M} \xrightarrow{*} \mathcal{X}$ be an ϵ-universal hash and $\boldsymbol{\rho} : \mathcal{X} \xrightarrow{*} \mathcal{Y}$ be a random function. The composition function $\boldsymbol{\rho} \circ \mathbf{H} : \mathcal{M} \xrightarrow{*} \mathcal{Y}$ is known as hash-then-PRF construction. This construction has been studied in [WC79, Sho00a]. Many PRF constructions can be viewed as hash-then-PRF. For example, EMAC [BdBB$^+$95], ECBC and FCBC [BR05], LightMAC [LPTY16] and protected counter sum or PCS [Ber99].

Lemma 5.1. *Let Hash-then-PRF be defined as above. Then, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\boldsymbol{\rho} \circ \mathbf{H}}(q) \leq \binom{q}{2}\epsilon.$$
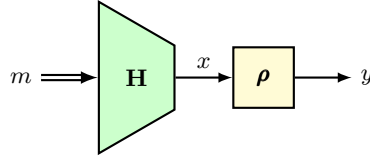
Figure 5.1: The Hash-then-PRF paradigm. The double equal sign path denotes the possibility of large message size.

Proof. We recall that all adversaries considered in this paper are deterministic and make no redundant queries (in this case all queries are distinct). The basic idea of the proof is that as long as there is no collision among the hash outputs, the $\boldsymbol{\rho}$ returns random values and hence the composition function behaves like a random function defined over larger input space $\mathscr{M}$. We capture this to prove the lemma formally by using extended H-technique.

EXTENDED SYSTEMS. We denote the composition system $\mathbf{F} = \boldsymbol{\rho} \circ \mathbf{H}$. Let $\boldsymbol{\rho}'$ be a random function from the message space $\mathscr{M}$ to $\mathscr{Y}$. We denote the size of the set $\mathscr{Y}$ as N. Let $\mathscr{H}$ be the key space of the hash function. We define $\mathscr{H}$-extended random system. In the ideal system $\boldsymbol{\rho}'$, we simply adjoin a hash key $\mathsf{H} \leftarrow_\$ \mathscr{H}$ chosen independent of $\boldsymbol{\rho}$. Let $\bar{\boldsymbol{\rho}}' = (\boldsymbol{\rho}, \mathsf{H})$ be the extended system. In case of $\mathbf{F}$, we simply release the hash key H'. We denote the extended system $\breve{\mathbf{F}} = (\mathbf{F}, \mathsf{H})$.

BAD TRANSCRIPTS AND ITS ANALYSIS. Let $\tau = (m^q, y^q, h)$ denote a transcript where $m^q \in \mathscr{M}^{(q)}$, $y^q \in \mathscr{Y}^q$, and $h \in \mathscr{H}$. We define $x^q = h(m^q) := \mathbf{H}(h, m^q)$ (i.e. h is the key of $\mathbf{H}$). As mentioned above, we say that a transcript is bad if

there exists distinct $i, j \in [q]$, such that $x_i = x_j$.

We bound the probability of this event by $\binom{q}{2}\epsilon$, as the hash function is ϵ-universal and there are at most $\binom{q}{2}$ (i, j) pairs. All other transcripts are considered to be good.

GOOD TRANSCRIPT ANALYSIS. Fix a good transcript $\tau = (m^q, y^q, h)$. In the ideal world, we have

$$\Pr[\boldsymbol{\rho}'(m^q) = y^q, \mathsf{H}' = h] = \frac{1}{|\mathscr{H}|} \times \frac{1}{N^q}.$$

In the real world, we have

$$\Pr[\mathbf{F}(m^q) = y^q, \mathbf{H} = h] = \frac{1}{|\mathscr{H}|} \times \Pr[\mathbf{F}(m^q) = y^q \mid \mathbf{H} = h]$$

$$= \frac{1}{|\mathscr{H}|} \times \Pr[\boldsymbol{\rho}(x^q) = y^q]$$

$$= \frac{1}{|\mathscr{H}|} \times \frac{1}{N^q}$$

$$= \Pr[\boldsymbol{\rho}'(m^q) = y^q, \mathsf{H} = h].$$

The result follows by using extended H-technique. $\qquad\square$

5.2 Hash-then-TBC

CONSTRUCTION. Let $\mathbf{H} := (\mathbf{H}_1, \mathbf{H}_2) : \mathscr{M} \xrightarrow{*} \mathscr{T} \times \mathscr{X}$ be an ϵ-universal hash such that $\mathbf{H}_1$ is ϵ_1-universal hash. Let $\widetilde{\boldsymbol{\pi}}$ be a tweakable random permutation on $\mathscr{X}$ with tweak space $\mathscr{T}$. We define the composition function $\mathbf{F} = \widetilde{\boldsymbol{\pi}} \circ \mathbf{H}$ as Hash-then-TBC.

A special instantiation (in which $\mathbf{H}_1$ and $\mathbf{H}_2$ are assumed to be independent) of the above construction is first considered in [CLS17]. Later, the analysis of the above
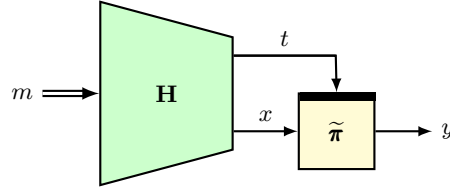
Figure 5.2: The Hash-then-TPRP paradigm. The double equal sign path denotes the possibility of large message size.

construction has been done [LN17]. In the same paper, the composition is used to define a MAC, called ZMAC+. Note that a tweakable random permutation is a PRF with maximum advantage about $q^2/2N$ where N is the size of the set $\mathcal{X}$ (this is similar to the well know result of PRP-PRF switching lemma [BR06]). So, one can apply the previous result for this construction. However, the construction can be shown to have better PRF advantage. Let us denote the size of $\mathcal{T}$ and $\mathcal{X}$ by T and N, respectively. Let $\boldsymbol{\rho}$ be an ideal candidate, i.e. a random function from $\mathcal{M}$ to $\mathcal{X}$.

In the previous construction we avoid the collision among hash outputs since the hash outputs are fed to random function. In this case, the hash output is fed to tweakable random permutation (as an input as well as a tweak). Hence, we need to avoid simultaneous collisions on the tweak and output as well as the tweak and input of $\widetilde{\boldsymbol{\pi}}$. The following lemma was proved in [LN17] using H-technique. We first tackle this problem without extending the random system which would require a bit more effort and then show how the extended H-technique as well as expectation method can help to bound the advantage very easily.

Lemma 5.2. *Let Hash-then-TBC be defined as above. Then we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\widetilde{\boldsymbol{\pi}} \circ \mathbf{H}}(q) \leq \binom{q}{2}\epsilon + \binom{q}{2}\frac{\epsilon_1}{N}.$$

5.2.1 A. Proof without releasing the internal values

Let $\tau = (m^q, y^q)$ be the transcript at hand. Let $C := C(y^q)$ be the number of colliding pairs in the output tuple y^q. More formally,

$$C = |\{(i,j) \; : \; i < j, y_i = y_j\}|.$$

When $\mathsf{Y}_1, \ldots, \mathsf{Y}_q \leftarrow_\$ \mathcal{X}^q$, we write the random variable $C(\mathsf{Y}^q)$ as C.

GOOD HASH KEY. Let $\mathcal{H}$ be the key space of the hash function. We define a subset $\mathcal{H}_{\mathsf{good}} \subseteq \mathcal{H}$ as the set of all $h \in \mathcal{H}$ so that there is

1. no collision among $(t_1, x_1), \ldots, (t_q, x_q)$ and

2. no collision among $(t_1, y_1), \ldots, (t_q, y_q)$.

where $h(m^q) = (t^q, x^q)$.

Clearly, for a good hash key h, (t^q, x^q, y^q) is tweakable permutation compatible and

$\Pr[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] \geq N^{-q}$. In the following, for any h, we denote $h(m^q) = (t^q, x^q)$.

$$\Pr[\mathbf{F}(m^q) = y^q] \geq \sum_{h \in \mathscr{H}_{\mathsf{good}}} \Pr[\mathsf{H} = h,\ \widetilde{\boldsymbol{\pi}}(\mathsf{H}(m^q)) = y^q]$$

$$= \sum_{h \in \mathscr{H}_{\mathsf{good}}} \Pr[\mathsf{H} = h,\ \widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q]$$

$$= \sum_{h \in \mathscr{H}_{\mathsf{good}}} \Pr[\mathsf{H} = h] \times \Pr[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q]$$

$$\geq \sum_{h \in \mathscr{H}_{\mathsf{good}}} \Pr[\mathsf{H} = h] \times N^{-q}$$

$$= (1 - \Pr[\mathsf{H} \notin \mathscr{H}_{\mathsf{good}}]) \times N^{-q}$$

$$\geq \left(1 - \binom{q}{2} \cdot \epsilon - C \cdot \epsilon_1\right) \times N^{-q} \tag{9}$$

The last inequality follows from the union bound. A bad hash key can arise due to either collision on tweak-input pairs (which happens with probability at most $\binom{q}{2} \cdot \epsilon$) or collision on tweak-output pairs. As there are C pairs at which y_i values collide, we must have collision of tweak values among these C pairs. Hence the probability of having a tweak-output collision is at most $C \cdot \epsilon_1$. This justifies the last inequality. Now, the ratio

$$\frac{\Pr[\mathbf{F}(M^q) = y^q]}{\Pr[\boldsymbol{\rho}'(M^q) = y^q]} \geq 1 - \binom{q}{2} \cdot \epsilon - C \cdot \epsilon_1.$$

To obtain a bound, we have to get a good upper bound for $C(y^q)$ for all y^q. At this point, we have two options to bound the value of $C(y^q)$.

(1) Standard H-Technique: In this case we can use Markov's inequality to bound $\mathsf{C} = C(\mathsf{Y}^q)$ to a moderate value where Y^q is a q-tuple independent uniform random variable (responses of $\boldsymbol{\rho}$). We can write $\mathsf{C} = \sum_{i < j} \mathsf{I}_{i,j}$ where $\mathsf{I}_{i,j}$ is the binary random variable which takes value 1 if $\mathsf{Y}_i \neq \mathsf{Y}_j$. So,

$$\mathsf{Ex}(\mathsf{C}) = \frac{q(q-1)}{2N}.$$

BAD TRANSCRIPTS AND ITS ANALYSIS. Let α be a threshold parameter (which would be determined soon). We call a transcript (m^q, y^q) *bad* if the number of collision pairs of y_i values is more than α. Using Markov's inequality we get

$$\Pr[\tau(\mathscr{A}^{\boldsymbol{\rho}}) \in \Omega_{\mathsf{bad}}] = \Pr[\mathsf{C} \geq \alpha] \leq \mathbb{E}[\mathsf{C}]/\alpha = \binom{q}{2} \cdot \frac{1}{\alpha N} \tag{10}$$

for any adversary $\mathscr{A}$.

ANALYSIS OF GOOD TRANSCRIPTS. Now, fix any good transcript $\tau = (m^q, y^q)$. Using α as an upper bound for $C(y^q)$ in Eq. 9, we get

$$\frac{\Pr[\mathbf{F}(M^q) = y^q]}{\Pr[\boldsymbol{\rho}'(M^q) = y^q]} \geq 1 - \binom{q}{2} \cdot \epsilon - \alpha \cdot \epsilon_1.$$

Finally, using the bad transcript probability of Eq. 10 and the standard H-technique, we get

$$\mathbf{Adv}^{\mathrm{prf}}_{\widetilde{\boldsymbol{\pi}} \circ \mathbf{H}} \leq \binom{q}{2} \cdot \frac{1}{\alpha N} + \binom{q}{2} \cdot \epsilon + \alpha \cdot \epsilon_1. \tag{11}$$

By equating the two terms $\binom{q}{2} \cdot \frac{1}{\alpha N}$ and $\alpha \cdot \epsilon_1$, we set $\alpha = \frac{q}{\sqrt{N\epsilon_1}}$. With this choice of α, the PRF advantage is bounded as

$$\mathbf{Adv}^{\mathrm{prf}}_{\boldsymbol{\pi} \circ \mathbf{H}} \leq \binom{q}{2} \cdot \epsilon + 2q\sqrt{\epsilon_1/N}.$$

(2) Expectation Method: For small messages, there are universal hash function with $\epsilon \approx 1/NT$ and $\epsilon_1 \approx 1/T$. In this case, the standard H-technique bounds the prf advantage to $O(q^2/NT) + O(q/\sqrt{NT})$. Clearly, the dominating term is $O(q/\sqrt{NT})$. Instead of a crude estimation of C, if we apply the expectation method (which needs to work with expected value of C instead of an upper bound), we can get rid of the dominating term $O(q/\sqrt{NT})$.

We define $\epsilon : \mathscr{M}^q \times \mathscr{X}^q \to [0, \infty)$ by the mapping

$$\epsilon(\tau) = \binom{q}{2}\epsilon + \mathsf{C} \cdot \epsilon_1.$$

Clearly ϵ is non-negative and the ratio of real to ideal interpolation probabilities is at least $1 - \epsilon(\tau)$ (using Eq. 9). Thus we can use Lemma 4.2 to get

$$\mathbf{Adv}^{\mathrm{prf}}_{\boldsymbol{\pi} \circ \mathbf{H}}(q) \leq \mathsf{Ex}[\epsilon(\tau)] = \binom{q}{2}\epsilon + \binom{q}{2}\frac{\epsilon_1}{N}. \tag{12}$$

5.2.2   B. Proof by releasing the internal values

Now we show that extended H-technique can also help to bound this construction very easily.

EXTENDED SYSTEMS. Let $\mathscr{H}$ be the key space of the hash function. We define $\mathscr{H}$-extended random system. In the ideal system $\boldsymbol{\rho}$, we simply adjoin a hash key $\mathsf{H} \leftarrow_\$ \mathscr{H}$ chosen independent of $\boldsymbol{\rho}$. Let $\bar{\boldsymbol{\rho}} = (\boldsymbol{\rho}, \mathsf{H})$ be the extended system. In case of $\mathbf{F}$ based on the hash key H' and tweakable random permutation $\widetilde{\boldsymbol{\pi}}$, we release the hash key H'. We denote the extended system $\bar{\mathbf{F}} = (\mathbf{F}, \mathsf{H}')$.

BAD TRANSCRIPTS AND ITS ANALYSIS. Given any hash key h, we define $h(m^q) = (t^q, x^q)$. We say that an extended transcript (m^q, y^q, h) is bad if either

1. there is a collision among (t^q, x^q) or

2. there is a collision among (t^q, y^q).

In the extended ideal world, an adversary can realize a bad transcript with probability at most $\binom{q}{2} \cdot (\epsilon + \epsilon_1/N)$. The probability that there is a collision among (t^q, x^q) is at most $\binom{q}{2} \cdot \epsilon$. The probability that there is a collision among (t^q, y^q) is at most $\binom{q}{2}\frac{\epsilon_1}{N}$ (a pair of y values will collide with probability $1/N$ whereas a pair of t values will collide with probability at most ϵ_1 and these events are independent).

ANALYSIS OF A GOOD TRANSCRIPT. Now we fix a good transcript $\tau = (m^q, y^q, h)$. For the ideal system we have,

$$\mathsf{Pr}[\bar{\boldsymbol{\rho}}(m^q) = (y^q, h)] = \frac{1}{|\mathscr{H}|} \times \frac{1}{N^q},$$

and for the real system we have,

$$\mathsf{Pr}[\bar{\mathbf{F}}(m^q) = (y^q, h)] = \mathsf{Pr}[\mathsf{H} = h] \times \mathsf{Pr}[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] \geq \frac{1}{|\mathscr{H}|} \times \frac{1}{N^q}.$$

Note that we have applied Eq. 4 for the real system as the transcript is tweakable permutation consistent and it is non-redundant. Hence the extended H-technique of Lemma 4.1 gives,

$$\mathbf{Adv}^{\mathrm{prf}}_{\widetilde{\boldsymbol{\pi}} \circ \mathbf{H}}(q) \leq \binom{q}{2} \cdot (\epsilon + \epsilon_1 / N).$$

(13)

Remark 1. The XTX [MI15] and HaT [CLS17] constructions are quite similar to HtTBC [LN17]. Consequently we get similar proofs for these constructions.

5.3   An extension of Naor-Reingold

The basic version of ENR [Min09] is a $2n$-bit permutation based on an (n, n)-TBC and an n-bit AXU hash function, essentially adapting the Naor-Reingold [NR97] simplification of 4-round Feistel structure. Here, we describe a version which generalizes ENR based on (t, n)-TBC (for $t \leq n$) as well as LDT[CLMP17] in which the hash function is not present (can also be viewed as an identity function).
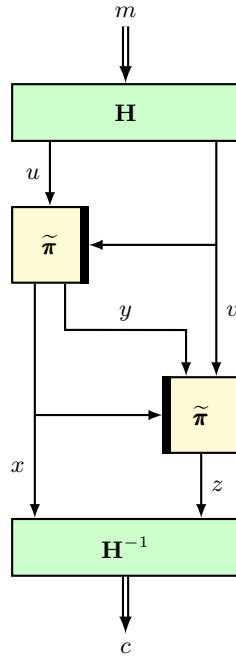
Figure 5.3: The NR* paradigm. The double equal sign path denotes $(n + t)$-bit message and ciphertext.

CONSTRUCTION. Let $\mathscr{M} = \mathbb{F}_{2^t} \times \mathbb{F}_{2^n}$. Suppose $\mathbf{H} := (\mathbf{H}_1, \mathbf{H}_2) : \mathscr{M} \xrightarrow{*} \mathbb{F}_{2^t} \times \mathbb{F}_{2^n}$ is an invertible keyed function such that $\mathbf{H}_1$ is an ϵ-universal hash function. Suppose $\widetilde{\boldsymbol{\pi}}_1$ and $\widetilde{\boldsymbol{\pi}}_2$ are two independently sampled tweakable random permutations on $\mathbb{F}_{2^n}$ with tweak space $\mathbb{F}_{2^t}$. We define $\mathsf{NR*} : \mathbb{F}_{2^n} \times \mathbb{F}_{2^t} \xrightarrow{*} \mathbb{F}_{2^n} \times \mathbb{F}_{2^t}$ as follows:

– Input: $m \in \mathscr{M}$.

1. $(v, u) = \mathbf{H}(h, m)$.
2. $x \| y = \widetilde{\boldsymbol{\pi}}_1(v, u)$, where $x \in \mathbb{F}_{2^t}$ and $y \in \mathbb{F}_{2^{n-t}}$.
3. $z = \widetilde{\boldsymbol{\pi}}_2(x, y \| v)$.
4. $c = \mathbf{H}^{-1}(h, x \| z)$.

     5. return $c := \mathsf{NR}^*(m)$.

Let $\mathbf{F}$ be the response system corresponding to NR^* and $\mathbf{\Pi}$ be the system corresponding to a random permutation over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^t}$. It is easy to see that $\mathbf{F}$ is an invertible response system.

Lemma 5.3.

$$\mathbf{Adv}_{\mathsf{NR}^*}^{\mathrm{sprp}}(q) \leq \frac{\binom{q}{2}}{2^n}\left(\epsilon + \frac{1}{2^t}\right).$$

Proof. We apply extended H-technique and so we define the additional random variables released after the interaction.

EXTENDED SYSTEMS. Suppose (δ^q, m^q, c^q) is the forward only transcript (before we extend). Now, we define $(\mathscr{H} \times \mathbb{F}_{2^{n-t}}^q)$-extended random system. In the ideal system $\mathbf{\Pi}$, we simply adjoin a hash key $\mathsf{H} \leftarrow_{\$} \mathscr{H}$ and $\mathsf{Y}_1, \ldots, \mathsf{Y}_q \leftarrow_{\$} \mathbb{F}_{2^{n-t}}$, chosen independent of $\mathbf{\Pi}$. Let $\bar{\mathbf{\Pi}}^{\pm} = (\mathbf{\Pi}^{\pm}, \mathsf{H}, \mathsf{Y}^q)$ be the extended ideal system.

    In case of $\mathbf{F}^{\pm}$ based on the hash key H and tweakable random permutation $\widetilde{\boldsymbol{\pi}}_1, \widetilde{\boldsymbol{\pi}}_2$, we release the hash key H and all q internal values $\mathsf{Y}_1, \ldots, \mathsf{Y}_q$ where Y_i is the value of y in step-2 while computing $\mathbf{F}(m_i)$. We denote the extended system $\bar{\mathbf{F}}^{\pm} = (\mathbf{F}^{\pm}, \mathsf{H}, \mathsf{Y}^q)$.

ANALYSIS OF BAD TRANSCRIPTS. Let $\tau = (\delta^q, m^q, c^q, h, y^q)$ be a transcript. We define $h(m^q) = (v^q, u^q)$ and $h(c^q) = (x^q, z^q)$. We say that an extended transcript τ is bad if there is a collision among $v_1\|x_1\|y_1, v_2\|x_2\|y_2, \ldots, v_q\|y_q\|x_q$ values.[3] Now we calculate the probability that the extended transcript $\bar{\tau}(\mathscr{A}^{\bar{\mathbf{\Pi}}^{\pm}})$ is bad for any adversary $\mathscr{A}$ making q queries. Let $[q]_e$ and $[q]_d$ denote the set of all forward and backward query indices. Let us denote the random variables corresponding to m, c, x, y and v values in the ideal world as $\mathsf{M}, \mathsf{C}, \mathsf{X}, \mathsf{Y}$ and V respectively.

    Now, the bad event means that there is $i < j$ such that $\mathsf{X}_i = \mathsf{X}_j, \mathsf{Y}_i = \mathsf{Y}_j, \mathsf{V}_i = \mathsf{V}_j$. We have $\Pr[\mathsf{Y}_i = \mathsf{Y}_j] = 2^{t-n}$. Moreover, Y_i's are chosen independent of $(\mathbf{\Pi}, \mathsf{H})$ and hence independent of X and V values. So, it is sufficient to bound $\Pr[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j]$ for some $i < j$.

Claim.

$$\Pr[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j] \leq \frac{\epsilon}{2^t}.$$

We prove the claim when $j \in [q]_e$. A similar proof is applied for $j \in [q]_d$. As $j \in [q]_e$, V_j depends on C_j and the hash key H of $\mathbf{H}$. We first condition on all query responses $\mathsf{M}^{j-1} = m^{j-1}, \mathsf{C}^{j-1} = c^{j-1}$ up to $j - 1$ queries. Note that up to $j - 1$ queries, the queries can be both encryption or decryption. So, $\mathsf{M}^{j-1}, \mathsf{C}^{j-1}$ is simply the forward only reordering of the query and responses. Once we condition on it and $j \in [q]_e$, the value of M_j is fixed (say m_j) and $\mathsf{C}_j \leftarrow_{\$} \mathscr{M} \setminus \{c_1, \ldots, c_{j-1}\}$. Let us write the conditional event $\mathsf{M}^{j-1} = m^{j-1}, \mathsf{C}^{j-1} = c^{j-1}$ as E and the set of all h for which $\mathbf{H}_1(h, m_i) = \mathbf{H}_1(h, m_j)$

---

    [3]Observe that the bad event is quite similar to the one arising in Hash-then-TBC analysis. In fact in most of the TBC based constructions the sole bad event is of this particular type (avoiding tweak-input and tweak-output collisions).

holds as $\mathscr{H}'$. So,

$$\Pr[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j \mid \mathsf{E}] = \Pr[\mathbf{H}_1(\mathsf{H}, m_i) = \mathbf{H}_1(\mathsf{H}, m_j), \ \mathbf{H}_1(\mathsf{H}, c_i) = \mathbf{H}_1(\mathsf{H}, \mathsf{C}_j) \mid \mathsf{E}]$$

$$= \sum_{h \in \mathscr{H}'} \Pr[\mathsf{H} = h, \ \mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}]$$

$$= \sum_{h \in \mathscr{H}'} \Pr[\mathsf{H} = h] \times \Pr[\mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}]$$

$$\leq \sum_{h \in \mathscr{H}'} \Pr[\mathsf{H} = h] \times \frac{1}{2^t}$$

To justify the last inequality, we first note that $\mathbf{H}(h, \cdot)$ is an invertible function and so the conditional distribution of $\mathbf{H}(h, \mathsf{C}_j)$ is uniformly distributed over a set of size $2^{n+t} - (j-1)$. Hence, $\Pr[\mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}] \leq \frac{2^n}{2^{n+t} - (j-1)} \leq \frac{1}{2^t}$. To complete the proof of the claim we sum over all such event E (i.e. varying m^{j-1} and c^{j-1}) after multiplying the probability of E.

So for any $i < j$, $\Pr[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j, \mathsf{Y}_i = \mathsf{Y}_j] \leq \frac{\epsilon}{2^n}$. This proves that

$$\Pr[\bar{\tau}(\mathscr{A}^{\boldsymbol{\Pi}^{\pm}}) \text{ is bad}] \leq \frac{q(q-1)\epsilon}{2^{n+1}}. \tag{14}$$

ANALYSIS OF A GOOD TRANSCRIPT. We fix a good transcript $\tau = (\delta^q, m^q, c^q, h, y^q)$ and let $h(m^q) = (v^q, u^q)$ and $h(c^q) = (x^q, z^q)$. By definition of good transcript, $(v^q, u^q, x^q \| y^q)$ and $(x^q, y^q \| v^q, z^q)$ is tweakable permutation compatible which is also non-redundant. So,

$$\Pr[\mathbf{F}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}'^q = y^q] = \Pr[\widetilde{\pi}_1(v^q, u^q) = x^q \| y^q] \times \Pr[\widetilde{\pi}_2(x^q, y^q \| v^q) = z^q] \times \Pr[\mathsf{H} = h]$$

$$\geq \frac{1}{|\mathscr{H}|} \times \frac{1}{2^{2nq}}.$$

On the other hand, realizing the transcript by the extended ideal system is

$$\Pr[\boldsymbol{\Pi}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}^q = y^q] = \frac{1}{|\mathscr{H}|} \times \frac{1}{(2^{n+t})_q} \times \frac{1}{2^{(n-t)q}}$$

$$\leq \frac{1}{|\mathscr{H}|} \times \frac{1}{2^{(n+t)q} \cdot \left(1 - \frac{q(q-1)}{2^{n+t+1}}\right)} \times \frac{1}{2^{(n-t)q}}.$$

So, the ratio

$$\frac{\Pr[\mathbf{F}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}'^q = y^q]}{\Pr[\boldsymbol{\Pi}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}^q = y^q]} \geq 1 - \frac{\binom{q}{2}}{2^{n+t}}. \tag{15}$$

Combining Eq. 14 and Eq. 15 with Lemma 4.1 we get,

$$\mathbf{Adv}_{\mathsf{NR}^\star}^{\mathrm{sprp}}(q) \leq \frac{\binom{q}{2}}{2^n}\left(\epsilon + \frac{1}{2^t}\right). \qquad \qquad \square$$

Based on the security analysis of this generic design we can have simple proofs for ENR [Min09, MI11] and LDT [CLMP17].

5.3.1 A simple proof for ENR

The basic version of ENR [Min09] can be viewed as a specific instantiation of NR* where the hash function is defined as $(a, b) \mapsto (a, (a \odot \mathsf{K} \oplus b))$ for $\mathsf{K} \leftarrow_\$ \mathbb{F}_{2^n}$. Later Minematsu and Iwata gave a simpler definition for ENR for $t < n$, called SmallBlock [MI11] that just redefines the hash to be $(a, (a \odot \mathsf{K} \oplus b))_{|t}$. Now, we have the following corollary.

Corollary 2. *For $t \leq n$ we have*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{ENR}}(q) \leq \frac{q^2}{2^{n+t}}.$$

5.3.2   A simple proof for LDT

The two rounds LDT construction by Chen et al. [CLMP17] can also be viewed as a specific instantiation of NR* where the hash function is defined to be the identity function. This immediately gives the following corollary on the SPRP advantage of LDT.

Corollary 3.

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{LDT}}(q) \leq \frac{q^2}{2^n}.$$

# 6   Feistel structure based schemes

A (keyed) bijective function Ψ based on internal primitive $\boldsymbol{\psi}$ is said to be *inverse-free* if and only if the computation of Ψ^{-1} does not require the execution of $\boldsymbol{\psi}^{-1}$. Feistel structure has this property.

6.1   3-round Luby-Rackoff

CONSTRUCTION. Suppose $\boldsymbol{\psi}$ is a random function over $\{0,1\}^n$ and Ψ is round function defined by the mapping

$$(a,b) \overset{\Psi}{\mapsto} (b, a \oplus \boldsymbol{\psi}(b)).$$

Suppose Ψ_i denotes the round function based on random function $\boldsymbol{\psi}_i$. The well-known 3-round Luby-Rackoff [LR85] scheme, denoted LR3, is defined as $\Psi_3 \circ \Psi_2 \circ \Psi_1$.
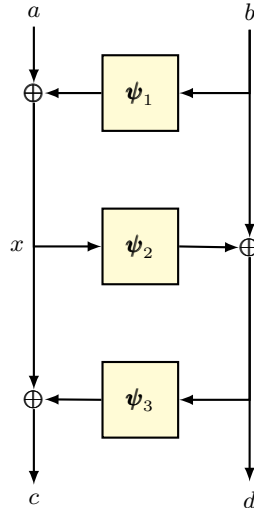
Figure 6.1: The 3-round Luby-Rackoff or LR3 construction.

LR3 is a well-studied birthday bound pseudorandom permutation. The original proof by Luby and Rackoff [LR85] is one of the foundational results in symmetric-key provable security. We now show how a fairly modern tool in symmetric-key provable security can simplify the security analysis as compared to the original proof. We note that a simpler

proof based on H-technique is already available from Nachef, Patarin and Volte [NPV17]. Here we provide the proof of LR3 in our language.

Lemma 6.1. *For $t \leq n$ we have*

$$\mathbf{Adv}_{3\mathsf{LR}}^{\mathrm{prp}}(q) \leq \frac{q^2}{2^n} + \frac{q^2}{2^{2n}}.$$

Proof. We apply the standard H-technique (i.e. no need to extend the system).

ANALYSIS OF BAD TRANSCRIPTS. For input (a, b) and output (c, d), let the 1-round and 2-round outputs be (x, b) and (x, d). Let $\mathbf{F}$ be the response system corresponding to LR3 and $\mathbf{\Pi}$ be the system corresponding to a random permutation. The transcript random variable τ is defined as the tuple $(\mathsf{A}^q, \mathsf{B}^q, \mathsf{C}^q, \mathsf{D}^q)$. We say that a transcript (a^q, b^q, c^q, d^q) is bad if d^q has a colliding pair, i.e for two distinct queries i and j, $d_i = d_j$. So we have,

$$\Pr[\tau(\mathscr{A}^{\mathbf{\Pi}}) \text{ is bad }] \leq \frac{q(q-1)(2^n-1)}{2(2^{2n}-1)} \leq \frac{q^2}{2^{n+1}}. \tag{16}$$

ANALYSIS OF GOOD TRANSCRIPTS. Fix a good transcript (a^q, b^q, c^q, d^q). We say that a function $f \in \mathsf{Func}$ is bad, denoted $f \in \mathsf{Func}_{\mathsf{bad}}$ if for some distinct $i, j \in [q]$, $f(b_i) \oplus a_i = f(b_j) \oplus a_j$, otherwise we say it is good. Clearly for a uniform random f the probability of f being bad is bounded to at most $q^2/2^{n+1}$. Let $\mathsf{Func}_{\mathsf{good}} = \mathsf{Func} \setminus \mathsf{Func}_{\mathsf{bad}}$. So we have,

$$\Pr[\mathbf{F}(a^q, b^q) = (c^q, d^q)] \geq \Pr[\boldsymbol{\psi}_1 \in \mathsf{Func}_{\mathsf{good}}] \times \Pr[\boldsymbol{\psi}_2(x^q) = b^q \oplus d^q, \boldsymbol{\psi}_3(d^q) = x^q \oplus c^q \mid \boldsymbol{\psi}_1]$$

$$\geq \left(1 - \frac{q^2}{2^{n+1}}\right) \times \frac{1}{2^{2nq}}$$

$$\geq \left(1 - \frac{q^2}{2^{n+1}} - \frac{q^2}{2^{2n}}\right) \times \frac{1}{(2^{2n})_q}$$

As $\Pr[\mathbf{\Pi}(a^q, b^q) = (c^q, d^q)] = \frac{1}{(2^{2n})_q}$, we have

$$\frac{\Pr[\mathbf{F}(a^q, b^q) = (c^q, d^q)]}{\Pr[\mathbf{\Pi}(a^q, b^q) = (c^q, d^q)]} \geq \left(1 - \frac{q^2}{2^n} - \frac{q^2}{2^{2n}}\right). \tag{17}$$

The result follows from Eq. 16 and Eq. 17 using standard H-technique. $\qquad\square$

Remark 2. Note that the above proof can be easily converted into a proof with extended transcript. In particular, we release X^q values. In case of ideal oracle oracle, it is computed as follows: $\mathsf{X}_i = \boldsymbol{\psi}_1(b_i) \oplus a_i$ for all i. We add one more bad event which is a presence of collision among X^q values. The probability of this new bad event can be easily shown to be at most $q^2/2^{n+1}$. For a good transcript the ratio can be similarly shown to be at least $1 - q^2/2^{2n}$ and hence we get exactly the same bound for the PRP advantage.

One can have an SPRP proof for four-round LR using the extended transcript. The proof is more or less similar with some bad events avoiding all possible collisions among inputs of $\boldsymbol{\psi}_2$ and $\boldsymbol{\psi}_3$.

6.2   3-round TBC-based Luby-Rackoff

In [CDMS10], Coron et al. gave an alternative for 3-round Luby-Rackoff using tweakable block cipher, called TLR3, and showed $O(q/2^n)$-query security. In this case $\boldsymbol{\psi}$ is a tweakable random permutation and Ψ function is defined by the mapping $(a, b) \overset{\Psi}{\mapsto} (b, \boldsymbol{\psi}(b, a))$. The original work by Coron et al. is mainly focused on the indifferentiability of TLR3 with respect to an ideal cipher. However, their result also implies $\Omega(2^n)$-query SPRP security. We present a relatively simple proof for the SPRP security of TLR3.
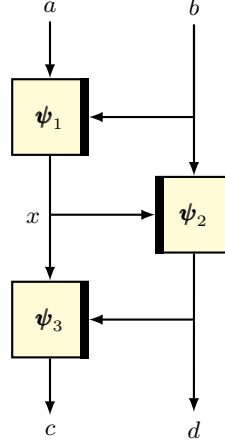
Figure 6.2: The 3-round TPRP-based Luby-Rackoff or TLR3 construction.

Proposition 6.1. *For $q < 2^{n-1}$ we have*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{TLR3}}(q) \leq \frac{q^2}{2^{2n-1}}.$$

Proof. We will use the extended H-technique to prove the claimed security.

EXTENDED SYSTEMS. The variables arising in the following analysis are analogous to the ones given in Figure 6.2. Let $\mathbf{F}$ be the response system corresponding to TLR3 and $\mathbf{\Pi}$ be the system corresponding to a random permutation. The transcript τ is defined as the tuple $(\mathsf{A}^q, \mathsf{B}^q, \mathsf{C}^q, \mathsf{D}^q)$. We define $\mathbb{F}^q_{2^n}$-extended response systems by adjoining the internal value X^q. In case of $\mathbf{F}$ this is well-defined from the definition of TLR3.

In the ideal system $\mathbf{\Pi}$, we sample X^q as follows:

1. for all $i \in [q]_e$,

$$\mathsf{X}_i \leftarrow_\$ \{0,1\}^n \setminus \{x \in \{0,1\}^n : \exists j < i, \mathsf{X}_j = x \wedge \mathsf{B}_i = \mathsf{B}_j\};$$

2. for all $i \in [q]_d$,

$$\mathsf{X}_i \leftarrow_\$ \{0,1\}^n \setminus \{x \in \{0,1\}^n : \exists j < i, \mathsf{X}_j = x \wedge \mathsf{D}_i = \mathsf{D}_j\};$$

BAD TRANSCRIPT AND ITS ANALYSIS. We say that an extended transcript $(a^q, b^q, x^q, c^q, d^q)$ is bad if and only if (b^q, a^q, x^q), (x^q, b^q, d^q) and (d^q, x^q, c^q) are not tweakable permutation consistent. Due to the way we sample X^q in $\mathbf{\Pi}$, the necessary and sufficient condition for the inconsistency of $(\mathsf{B}^q, \mathsf{A}^q, \mathsf{X}^q)$, $(\mathsf{X}^q, \mathsf{B}^q, \mathsf{D}^q)$, and $(\mathsf{D}^q, \mathsf{X}^q, \mathsf{C}^q)$ is: $i < j \in [q]$ and (1) $j \in [q]_e$ and $(\mathsf{X}_j, \mathsf{D}_j) = (\mathsf{X}_i, \mathsf{D}_i)$; or (2) $j \in [q]_d$ and $(\mathsf{B}_j, \mathsf{X}_j) = (\mathsf{B}_i, \mathsf{X}_i)$. Formally we have

$$\Pr[\bar{\tau}(\mathbf{\Pi}) \in \mathscr{V}_{\mathsf{bad}}] = \sum_{i \in [q]} \left(\sum_{i < j \in [q]_e} \Pr[\mathsf{X}_i = \mathsf{X}_j, \mathsf{D}_i = \mathsf{D}_j] + \sum_{i < j \in [q]_d} \Pr[\mathsf{B}_i = \mathsf{B}_j, \mathsf{X}_i = \mathsf{X}_j] \right)$$

$$\leq \binom{q}{2} \times \frac{2^n - 1}{2^{2n} - j + 1} \times \frac{1}{2^n - q}$$

$$\leq \frac{q(q-1)}{2^{n+1}(2^n - q)}. \tag{18}$$

ANALYSIS OF GOOD TRANSCRIPTS. For a good transcript $(a^q, b^q, x^q, c^q, d^q)$, we know that (b^q, a^q, x^q), (x^q, b^q, d^q), and (d^q, x^q, c^q) are tweakable permutation consistent. Let

$\alpha^u = \mathsf{mcoll}(b^q)$, $\beta^v = \mathsf{mcoll}(x^q)$, and $\gamma^w = \mathsf{mcoll}(d^q)$. Given a good transcript, for real system we have,

$$\Pr[\bar{\tau}(\mathbf{F})] = \Pr[\boldsymbol{\psi}_1(b^q, a^q) = x^q] \times \Pr[\boldsymbol{\psi}_2(x^q, b^q) = d^q] \times \Pr[\boldsymbol{\psi}_3(d^q, x^q) = c^q]$$

$$= \frac{1}{\prod_{i=1}^{u}(2^n)_{\alpha_i}} \times \frac{1}{\prod_{j=1}^{v}(2^n)_{\beta_j}} \times \frac{1}{\prod_{k=1}^{w}(2^n)_{\gamma_k}}.$$

For $i \in [q]$, let r_i and s_i denote the number of previous queries j and j' such that $b_i = b_j$ and $d_i = d_{j'}$, respectively. Then for the ideal system we have,

$$\Pr[\bar{\tau}(\mathbf{\Pi})] = \frac{1}{(2^{2n})_q} \times \frac{1}{\prod_{i' \in [q]_e}(2^n - r_{i'})} \times \frac{1}{\prod_{k' \in [q]_d}(2^n - s_{k'})}$$

$$\leq \frac{1}{\left(1 - \frac{q^2}{2^{2n}}\right) \times 2^{2nq}} \times \frac{1}{\prod_{i' \in [q]_e}(2^n - r_{i'})} \times \frac{1}{\prod_{k' \in [q]_d}(2^n - s_{k'})}.$$

Thus the ratio is

$$\frac{\Pr[\bar{\tau}(\mathbf{F})]}{\Pr[\bar{\tau}(\mathbf{\Pi})]} \geq \left(1 - \frac{q^2}{2^{2n}}\right) \times \frac{2^{2nq} \times \prod_{i' \in [q]_e}(2^n - r_{i'}) \times \prod_{k' \in [q]_d}(2^n - s_{k'})}{\prod_{i=1}^{u}(2^n)_{\alpha_i} \times \prod_{j=1}^{v}(2^n)_{\beta_j} \times \prod_{k=1}^{w}(2^n)_{\gamma_k}}. \quad (19)$$

In the above expression, we claim the following:

$$\prod_{i=1}^{u}(2^n)_{\alpha_i} = \prod_{i' \in [q]_e}(2^n - r_{i'}) \times \prod_{\hat{i} \in [q]_d}(2^n - \hat{\gamma}_{\hat{i}}), \text{ and}$$

$$\prod_{k=1}^{w}(2^n)_{\gamma_k} = \prod_{k' \in [q]_d}(2^n - s_{k'}) \times \prod_{\hat{k} \in [q]_e}(2^n - \hat{\gamma}_{\hat{k}}),$$

where for all $\hat{i}$ and $\hat{k}$, $\hat{\gamma}_{\hat{i}}, \hat{\gamma}_{\hat{k}} \geq 0$. We argue the first one and the second can be argued similarly. The set $[u]$ can be viewed as an indexing over the set of distinct tweak values. Now consider the first term on the right hand side (the one indexed by i'). For all $i' \in [q]_e$, we define $\phi(i') \to (i, p)$ such that i is the index of the tweak of the i'-th query, i.e $i \leq u$, and p is the number of previous queries with same tweak, i.e $p = r_{i'} \leq \alpha_i$. The mapping is well-defined. Further it is injective: for distinct $i'_1, i'_2 \in [q]_e$, either the tweaks are different, i.e. $i_1 \neq i_2$, or if the tweaks are same then $p_1 = r_{i'_1} \neq r_{i'_2} = p_2$. Observe that ϕ also maps each of the $(N - r_{i'})$ term on the right hand side to a unique $(N - p)$ term (taken from $(N)_{\alpha_i}$ expansion) on the left exhausting all the terms corresponding to encryption queries. Thus we are left with only the terms corresponding to all the decryption queries. Using the above relations in Eq. 19 we have

$$\frac{\Pr[\bar{\tau}(\mathbf{F})]}{\Pr[\bar{\tau}(\mathbf{\Pi})]} \geq \left(1 - \frac{q^2}{N^2}\right) \times \frac{N^{2q}}{\prod_{\hat{i} \in [q]_d}(N - \hat{\gamma}_{\hat{i}}) \times \prod_{j=1}^{v}(N)_{\beta_j} \times \prod_{\hat{k} \in [q]_e}(N - \hat{\gamma}_{\hat{k}})}$$

$$\geq \left(1 - \frac{q^2}{N^2}\right) \quad (20)$$

The result follows from extended H-technique using Eq. 18 and Eq. 20.

7 Strong Pseudo Random Permutation Designs

MORE NOTATIONS: For $\ell \geq 1$, $p \in \mathcal{M}^\ell$, $p[i]$ denotes the i-th $\mathcal{M}$-block of p, for all $i \in [\ell]$. In this case, we also write p, alternatively, as $p[1..\ell]$. By extending the notation, $p[i..j]$ denotes the $\mathcal{M}$-substring of p consisting of consecutive $\mathcal{M}$-blocks $p[i], p[i+1], \ldots, p[j]$, for $1 \leq i < j \leq \ell$.

7.1 HCTR

CONSTRUCTION. HCTR is an encryption scheme by Wang, Feng and Fu [WFW05], based on the Hash-CTR-Hash paradigm, that uses a sandwich of CTR mode in between two AXU hash functions. Suppose $\mathbf{H}_1$ and $\mathbf{H}_2$ are two independently keyed ϵ-AXU hash functions. Suppose $\boldsymbol{\pi}$ is a random permutation sampled independently off the two hashes. Then the HCTR scheme is defined as

1. For $\ell \in [L]$, for all $p = p[1..\ell] \in (\mathbb{F}_{2^n})^\ell$:

a. $x := p[1] \oplus \mathbf{H}_1(p[2..\ell])$.

b. $y := \boldsymbol{\pi}(x)$.

c. $z := x \oplus y$.

d. $c[2..\ell] := \mathsf{CTR}_{\boldsymbol{\pi}}(z) \oplus p[2..\ell]$.

e. $c[1] := y \oplus \mathbf{H}_2(c[2..\ell])$.

f. Return $\mathsf{HCTR}(p) := c = c[1..\ell]$.

where $\mathsf{CTR}_{\boldsymbol{\pi}}$ denotes the standard encryption schemes using IV-based counter mode [Dwo01]. The original HCTR was defined to be a tweakable encryption scheme with a
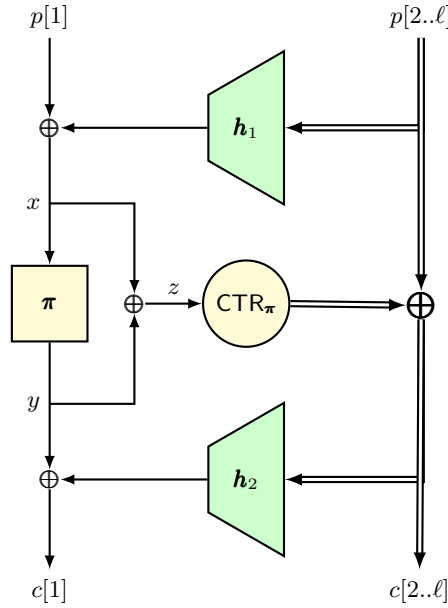
Figure 7.1: A simplified view of the HCTR enciphering scheme. The double equal style paths denote a compressed view of $(\ell - 1)$ many parallel paths.

single hash key. We use the above definition just for the sake of simplicity. The original scheme can be very easily accommodated within our proof.

Lemma 7.1.
$$\mathbf{Adv}_{\mathsf{HCTR}}^{\mathrm{sprp}}(q, \sigma) \leq \sigma^2 \epsilon.$$

Proof. The basic idea of the proof is quite simple. We have to bound two types of collisions, namely the input and output collisions on the underlying random permutation.

EXTENDED SYSTEM. Let $\mathbf{F}$ be the response system corresponding to HCTR and $\boldsymbol{\Pi}$ be the system corresponding to a random permutation. The transcript random variable $\boldsymbol{\tau}$ is defined as the tuple $(\mathsf{P}^q, \mathsf{C}^q)$ where for all $i \in [q]$, P_i and C_i are of length ℓ_i and $\sum_{i \in [q]} \ell_i = \sigma$. We define $\mathscr{H}^2$-extended random system. In the real world we simply release the hash key $(\mathsf{H}_1, \mathsf{H}_2)$. Let $\bar{\mathbf{F}}^\pm = (\mathbf{F}^\pm, \mathsf{H}_1, \mathsf{H}_2)$ be the extended real system. In the ideal system we adjoin a dummy hash key $(\mathsf{H}_1, \mathsf{H}_2) \leftarrow_\$ \mathscr{H}^2$, chosen independently of $\boldsymbol{\Pi}$. Note that this also fixes the internal variables $\mathsf{X}[1]$ and $\mathsf{Y}[1]$, and Z. Let $\bar{\boldsymbol{\Pi}}^\pm = (\boldsymbol{\Pi}^\pm, \mathsf{H}_1, \mathsf{H}_2)$ be the extended ideal system.

ANALYSIS OF BAD TRANSCRIPTS. For all $i \in [q]$, $j \in [2..\ell]$, let $x_i[j] = z_i \oplus \langle j \rangle_n$, $y_i[j] = c_i[j] \oplus p_i[j]$, where $\langle j \rangle_n$ denotes the n-bit binary representation of j. We say that a transcript is bad if one of the following conditions is met:

- $\texttt{xcoll}$: $\exists i, i' \in [q]$, $(j, j') \in [\ell_i] \times [\ell_{i'}]$, $(i, j) \neq (i', j')$, such that $x_i[j] = x_{i'}[j']$.

- $\texttt{ycoll}$: $\exists i, i' \in [q]$, $(j, j') \in [\ell_i] \times [\ell_{i'}]$, $(i, j) \neq (i', j')$, such that $y_i[j] = y_{i'}[j']$.

Bound on $\Pr[\texttt{xcoll}]$: Let us fix some $(i, j) \neq (i', j')$. Then $\ell_i, \ell_{i'} \geq 2$. Suppose $j, j' \neq 1$. Then $\mathsf{X}_i[j] = \mathsf{X}_{i'}[j']$ is same as

$$\mathsf{H}_1(\mathsf{P}_i[2..\ell_i]) \oplus \mathsf{H}_1(\mathsf{P}_{i'}[2..\ell_{i'}]) \oplus \mathsf{H}_2(\mathsf{C}_i[2..\ell_i]) \oplus \mathsf{H}_2(\mathsf{C}_{i'}[2..\ell_{i'}]) = \delta,$$

where $\delta := \langle j \rangle_n \oplus \langle j' \rangle_n \oplus \mathsf{P}_i[1] \oplus \mathsf{P}_{i'}[1] \oplus \mathsf{C}_i[1] \oplus \mathsf{C}_{i'}[1]$. This equation holds with at most ϵ probability as $(\mathsf{H}_1, \mathsf{H}_2)$ is uniformly chosen from $\mathscr{H}^2$. The case where at least one of j or j' is 1, can be bounded in a similar fashion. Finally we have at most $\binom{\sigma}{2}$ (i, j), (i', j') pairs, which gives a bound of at most $\sigma^2 \epsilon / 2$ for $\Pr[\texttt{xcoll}]$.

Bound on $\Pr[\texttt{ycoll}]$: Again we fix some $(i, j) \neq (i', j')$. Suppose $j, j' \neq 1$. Then $\mathsf{X}_i[j] = \mathsf{X}_{i'}[j']$ is same as $\mathsf{P}_i[j] \oplus \mathsf{P}'_i[j'] = \mathsf{C}_i[j] \oplus \mathsf{C}'_i[j']$. Without loss of generality we assume that $i' \geq i$ and it is an encryption query. Then by conditioning on the values of $\mathsf{P}_i[j]$, $\mathsf{P}_{i'}[j']$, and $\mathsf{C}_i[j]$ we bound the probability of $\mathsf{C}'_i[j'] = \mathsf{P}_i[j] \oplus \mathsf{P}'_i[j'] \oplus \mathsf{C}_i[j]$ to at most $1/N$. The case where at least one of j or j' is 1, can be bounded to at most ϵ, using the ϵ-XOR universality of $\mathbf{H}_2$. We have at most $\binom{\sigma}{2}$ (i, j), (i', j') pairs, and it is known that $\epsilon \geq 1/N$, which gives a bound of at most $\sigma^2 \epsilon / 2$ for $\Pr[\texttt{ycoll}]$.

Thus the probability of getting a bad transcript is easily bounded by $\sigma^2 \epsilon$ for the ideal system.

ANALYSIS OF GOOD TRANSCRIPTS. Fix a good transcript (p^q, c^q, h_1, h_2). Let q_ℓ denote the number of queries of length ℓ for all $\ell \in [L]$. Since for a good transcript there is no input/output collisions for $\boldsymbol{\pi}$. So we have

$$\Pr[\mathbf{F}(p^q) = c^q, \mathsf{H}_1 = h_1, \mathsf{H}_2 = h_2] = \frac{1}{|\mathscr{H}^2|} \times \frac{1}{(N)_\sigma}$$

$$\geq \frac{1}{|\mathscr{H}^2|} \times \prod_{\ell=1}^{L} \frac{1}{(N^\ell)_{q_\ell}}$$

$$\geq \Pr[\boldsymbol{\Pi}(p^q) = c^q, \mathsf{H}_1 = h_1, \mathsf{H}_2 = h_2]$$

The result follows from extended H-technique. $\square$

7.2   TET

CONSTRUCTION.   TET is an encryption scheme by Halevi [Hal07], based on the Hash-Encrypt-Hash paradigm [Hal07, Sar07, Sar09], that uses a sandwich of ECB mode in between two blockwise universal and invertible hash functions.

A hash function $\mathbf{H} : \mathcal{M}^{\leq L} \xrightarrow{*} \mathcal{M}^{\leq L}$ is called ϵ-*blockwise universal* if for all $\ell, \ell' \in [L]$, $m \in \mathcal{M}^{\ell}$, $m' \in \mathcal{M}^{\ell'}$, $i \in [\ell]$, and $i' \in [\ell']$, $\Pr_{\mathsf{H} \leftarrow\$ \mathcal{K}}[\mathsf{H}(m)[i] = \mathsf{H}(m')[i']] = \Pr_{\mathsf{H} \leftarrow\$ \mathcal{K}}[\mathbf{H}(\mathsf{H}, m)[i] = \mathbf{H}(\mathsf{H}, m')[i]] \leq \epsilon$.

Suppose $\mathbf{H}_1$ and $\mathbf{H}_2$ are two independently sampled ϵ-blockwise universal and invertible hash functions over $\mathbb{F}_{2^n}^{\leq L}$. Suppose $\boldsymbol{\pi}$ is a random permutation over $\mathbb{F}_{2^n}$ sampled independent off the two hash keys. Then the composition $\mathbf{H}_2^{-1} \circ \mathsf{ECB}_{\boldsymbol{\pi}} \circ \mathbf{H}_1$ is called the TET construction.
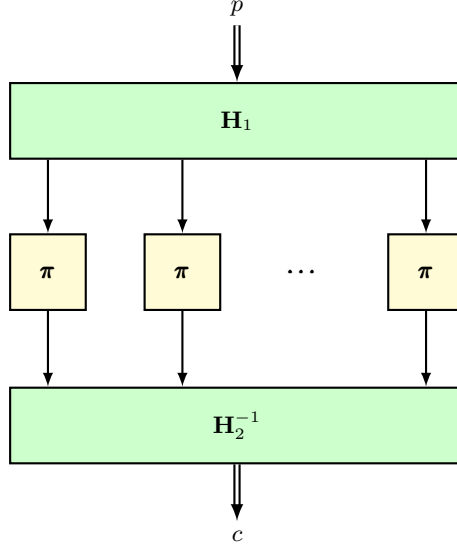
Figure 7.2: A simplified view of the TET enciphering scheme.

Lemma 7.2.

$$\mathbf{Adv}_{\mathsf{TET}}^{\mathrm{sprp}}(q, \sigma) \leq \sigma^2 \epsilon.$$

Proof. We will again use the same idea of avoiding collisions among the input/output of the internal random permutation $\boldsymbol{\pi}$. Let $\mathbf{F}$ be the response system corresponding to TET and $\boldsymbol{\Pi}$ be the system corresponding to a random permutation. The transcript τ is defined as the tuple $(\mathsf{P}^q, \mathsf{C}^q)$ where for all $i \in q$, P_i and C_i are of length ℓ_i and $\sum_{i \in [q]} \ell_i = \sigma$.

ANALYSIS OF GOOD TRANSCRIPTS. This proof will be similar to that of hash-then-prf. For any transcript (p^q, c^q) we have,

$$\Pr[\mathbf{F}(p^q) = c^q] \geq \sum_{x^q, y^q \in \mathbb{F}_{2^n}^{(\sigma)}} \Pr[\mathsf{H}_1(p^q) = x^q, \boldsymbol{\pi}(x^q) = y^q, \mathsf{H}_2^{-1}(y^q) = c^q]$$

$$= \sum_{x^q, y^q \in \mathbb{F}_{2^n}^{(\sigma)}} \Pr[\mathsf{H}_1(p^q) = x^q, \mathsf{H}_2(c^q) = y^q] \times \Pr[\boldsymbol{\pi}(x^q) = y^q]$$

$$= \Pr[\mathsf{H}_1(p^q) \in \mathbb{F}_{2^n}^{(\sigma)}, \mathsf{H}_2(c^q) \in \mathbb{F}_{2^n}^{(\sigma)}] \times \frac{1}{(N)_\sigma}$$

$$\geq \left(1 - \binom{\sigma}{2}\epsilon - \binom{\sigma}{2}\epsilon\right) \times \Pr[\boldsymbol{\Pi}(p^q) = c^q] \tag{21}$$

The result follows from substituting Eq. 21 in standard H-technique. $\qquad\square$

8 Beyond the Birthday Bound Secure Schemes

In this section, we revisit some beyond the birthday bound secure schemes. All these schemes are inherently based on one of the most celebrated problems in symmetric-key cryptography, called the sum of permutations problem [HWKS98, BI99, Men18, CLM19].

8.1 Pseudorandom Functions

There are many beyond the birthday bound PRF constructions from PRP [HWKS98, CS16]. The sum of permutations [HWKS98, BI99, Luc00] is one such construction which constructs a PRF from two independently keyed random permutations.

We first state and prove a simple proposition that lower bounds the probability distribution of sum of permutations conditioned on the event that the underlying random permutations are already sampled on some fixed number of points. We remark that a similar result is already available in [DDN$^+$17, Theorem 2], albeit for the single permutation setting.

Proposition 8.1. *Let $s_1, s_2, q \geq 0$ and $s_1 + s_2 + 2q \leq 2^{n-1}$. Let $\boldsymbol{\pi}_1$ and $\boldsymbol{\pi}_2$ be two independent and uniform random permutations over $\{0,1\}^n$. For all $a^{s_1}, b^{s_1} \in (\{0,1\}^n)^{(s_1)}$, $c^{s_2}, d^{s_2} \in (\{0,1\}^n)^{(s_2)}$, $x^q \in (\{0,1\}^n)^{(q)} \setminus (\{a^{s_1}\})^{(q)}$, $y^q \in (\{0,1\}^n)^{(q)} \setminus (\{b^{s_2}\})^{(q)}$, and $z^q \in (\{0,1\}^n)^q$ we have*

$$\Pr[\boldsymbol{\pi}_1(x^q) \oplus \boldsymbol{\pi}_2(y^q) = z^q \mid \mathsf{F}] \geq \left(1 - \frac{2s_1 s_2 q}{2^{2n}} - \frac{(s_1 + s_2)q^2}{2^{2n}} - \frac{q^3}{2^{2n}}\right) \times \frac{1}{2^{nq}},$$

where F denotes the event $\boldsymbol{\pi}_1(a^{s_1}) = b^{s_1} \wedge \boldsymbol{\pi}_2(c^{s_2}) = d^{s_2}$.

Proof. We compute a lower bound on the probability by following the chain rule of conditional probabilities, i.e. we compute the conditional probability of $\boldsymbol{\pi}_1(x_i) \oplus \boldsymbol{\pi}_2(y_i) = z_i$ for some $i \in [q]$, given F, and $\boldsymbol{\pi}_1(x_j) \oplus \boldsymbol{\pi}_2(y_j) = z_j$ for all $j < i$.

Let $\mathsf{P}_i = \boldsymbol{\pi}_1(x_i)$, $\mathsf{Q}_i = \boldsymbol{\pi}_2(y_i)$, and E_i denote the event that the i-th equation $\mathsf{P}_i \oplus \mathsf{Q}_i = z_i$ holds, for all $i \in [q]$.

For all $1 \leq i \leq q$, consider the i-th equation $\mathsf{P}_i \oplus \mathsf{Q}_i = z_i$. We have at least $2^n - s_1 - s_2 - 2(i-1)$ possibilities for P_i. This can be argued by removing b^{s_1}, $d^{s_2} \oplus z_i$, P_j and $\mathsf{Q}_j \oplus z_i$ values for all $j < i$. Once we fix P_i, Q_i fixes to $\mathsf{P}_i \oplus z_i$. Further, for each such value, E_i occurs with $1/(2^n - s_1 - i + 1)(2^n - s_2 - i + 1)$ probability given that F occurs, and E_j occurs for all $j < i$. Let $k = i - 1$. Then, we have

$$\Pr[\mathsf{E}_i \mid \mathsf{F} \wedge \mathsf{E}_1 \wedge \cdots \wedge \mathsf{E}_k] \geq \frac{2^n - s_1 - s_2 - 2k}{(2^n - s_1 - k)(2^n - s_2 - k)}$$

$$\geq \frac{2^{2n} - (s_1 + s_2 + 2k)2^n}{2^{2n} - (s_1 + s_2 + 2k)2^n + s_1 s_2 + (s_1 + s_2)k + k^2} \times \frac{1}{2^n}$$

$$= \left(1 - \frac{s_1 s_2 + (s_1 + s_2)k + k^2}{2^{2n} - (s_1 + s_2 + 2k)2^n + s_1 s_2 + (s_1 + s_2)k + k^2}\right) \times \frac{1}{2^n}$$

$$\geq \left(1 - \frac{2(s_1 s_2 + (s_1 + s_2)k + k^2)}{2^{2n}}\right) \times \frac{1}{2^n},$$

where the last inequality follows from the assumptions that $(s_1 + s_2 + 2k)2^n < (s_1 + s_2 +$

$2q)2^n < 2^{2n-1}$ and $s_1 s_2 + (s_1 + s_2)k + k^2 \geq 0$. Finally, we have

$$\Pr[\boldsymbol{\pi}_1(x^q) \oplus \boldsymbol{\pi}_2(y^q) = z^q \mid \mathsf{F}] = \Pr[\mathsf{E}_1 \mid \mathsf{F}] \times \Pr[\mathsf{E}_2 \mid \mathsf{F} \wedge \mathsf{E}_1] \times \cdots \times \Pr[\mathsf{E}_q \mid \mathsf{F} \wedge \mathsf{E}_1 \wedge \cdots \wedge \mathsf{E}_{q-1}]$$

$$\geq \prod_{k=0}^{q-1} \left(1 - \frac{2(s_1 s_2 + (s_1 + s_2)k + k^2)}{2^{2n}}\right) \times \frac{1}{2^{nq}}$$

$$\geq \left(1 - 2\sum_{k=0}^{q-1} \frac{s_1 s_2 + (s_1 + s_2)k + k^2}{2^{2n}}\right) \times \frac{1}{2^{nq}}$$

$$\geq \left(1 - \frac{2s_1 s_2 q}{2^{2n}} - \frac{(s_1 + s_2)q^2}{2^{2n}} - \frac{q^3}{2^{2n}}\right) \times \frac{1}{2^{nq}}.$$

$\square$

Note that, Proposition 8.1 is useful in both conditional and unconditional (i.e. $s_1 = s_2 = 0$) case. Now, we discuss two straightforward applications of the above given proposition.

8.1.1   Sum of Permutations [HWKS98, BI99, Luc00]

CONSTRUCTION: Suppose $\boldsymbol{\pi}_1$ and $\boldsymbol{\pi}_2$ are two independent uniform random permutations over $\{0,1\}^n$. The sum of permutation (or SoP) construction (illustrated in Figure 8.1) is a length-preserving function over $\{0,1\}^n$ defined by the mapping,

$$x \xmapsto{\mathsf{SoP}} \boldsymbol{\pi}_1(x) \oplus \boldsymbol{\pi}_2(x).$$

It is well-known [Pat08b, Pat10, DHT17] that SoP is indistinguishable from a uniform random function up to $o(2^n)$ queries. The H-technique based proofs in [Pat08b, Pat10], though tight, contain some non-trivial gaps, whereas the proof in [DHT17] uses the recently introduced χ^2-technique.
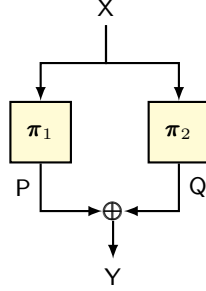
Figure 8.1: The Sum of Permutations construction.

In one of the early works on this problem, Lucks [Luc00] gave a suboptimal bound of $2^{2n/3}$ query using game-playing technique. Here we give a very simple and short proof for $2^{2n/3}$ query bound using standard H-technique.

Lemma 8.1. *For $q \leq 2^{2n/3}$,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{SoP}_{\boldsymbol{\pi}_1, \boldsymbol{\pi}_2}}(q) \leq \frac{q^3}{2^{2n}}.$$

Proof. We write $\mathbf{F} = \mathsf{SoP}_{\boldsymbol{\pi}_1, \boldsymbol{\pi}_2}$. Let $\boldsymbol{\rho}$ be a uniform random function over $\{0,1\}^n$. Let $\tau = (x^q, y^q)$ denote a transcript where $x^q \in (\{0,1\}^n)^{(q)}$. All transcripts are considered to be good.

ANALYSIS OF GOOD TRANSCRIPTS. Given a transcript $\tau = (x^q, y^q)$, it is easy to see that

$$\Pr[\boldsymbol{\rho}(x^q) = y^q] = \frac{1}{2^{nq}}, \tag{22}$$

as $x^q \leadsto y^q$. For the lower bound on $\Pr[\mathbf{F}(x^q) = y^q]$, we summon Proposition 8.1, with $s_1 = 0$ and $s_2 = 0$, i.e. the random permutations are not sampled at any points as of now. Accordingly, we have

$$\Pr[\mathbf{F}(x^q) = y^q] = \left(1 - \frac{q^3}{2^{2n}}\right) \times \frac{1}{2^{nq}}$$

$$\geq \left(1 - \frac{q^3}{2^{2n}}\right) \times \Pr[\boldsymbol{\rho}(x^q) = y^q]$$

$$\frac{\Pr[\mathbf{F}(x^q) = y^q]}{\Pr[\boldsymbol{\rho}(x^q) = y^q]} \geq \left(1 - \frac{q^3}{2^{2n}}\right).$$

The result follows from standard H-technique. $\qquad\square$

8.1.2   Sum of Even-Mansour [CLM19]

In a recent paper [CLM19], Chen et al. presented various beyond the birthday bound secure PRF constructions based on public[4] random permutations. Here we consider SoEM22, or the Sum of Even-Mansour with two independent random permutations and two independent keys.

CONSTRUCTION: Suppose $\boldsymbol{\pi}_1$ and $\boldsymbol{\pi}_2$ are two independent uniform random permutations over $\{0,1\}^n$ and $(\mathsf{K}_1, \mathsf{K}_2) \leftarrow_\$ \{0,1\}^{2n}$. The SoEM22 construction (illustrated in Figure 8.2) is a length-preserving function over $\{0,1\}^n$ defined by the mapping,

$$x \xmapsto{\;\mathsf{SoEM22}\;} \boldsymbol{\pi}_1(x \oplus \mathsf{K}_1) \oplus \mathsf{K}_1 \oplus \boldsymbol{\pi}_2(x \oplus \mathsf{K}_2) \oplus \mathsf{K}_2.$$

In [CLM19], SoEM22 has been shown to be a secure PRF up to $o(2^{2n/3})$ queries to both the underlying permutations as well as the construction itself. Further, it has been shown that the bound is tight. We show a similar security bound using Proposition 8.1.
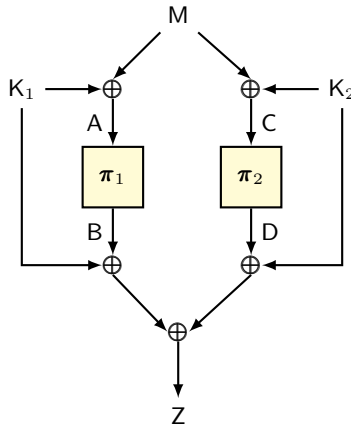
Figure 8.2: The Sum of Even-Mansour construction.

---

[4]The adversary has oracle access to the underlying random permutations.

Lemma 8.2. *Let q and p denote the total number of construction and primitive queries, respectively. Then, for $q, p \leq 2^{2n/3}$, we have*

$$\mathbf{Adv}_{\mathsf{SoEM22}}^{\mathrm{prf}}(q, p) \leq \frac{2p^2 q}{2^{2n}} + \frac{9pq^2}{2^{2n}} + \frac{5q^3}{2^{2n}}.$$

Proof. We write $\mathbf{F} = \mathsf{SoEM22}_{\boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \mathsf{K}_1, \mathsf{K}_2}$. Let $\boldsymbol{\rho}$ be a uniform random function over $\{0,1\}^n$. Let $\tau_C = (m^q, z^q)$ denote the transcript corresponding to $\mathbf{F}$, where $x^q \in (\{0,1\}^n)^{(q)}$. Without loss of generality we assume that the adversary makes same number of queries to the underlying random permutations. Let $\tau_P = (u^p, v^p)$ and (x^p, y^p) denote the forward only transcript corresponding to direct access of $\boldsymbol{\pi}_1^{\pm}$ and $\boldsymbol{\pi}_2^{\pm}$, respectively.

We define $\{0,1\}^{2n}$-extended response systems by adjoining the masking keys $\mathsf{K}_1, \mathsf{K}_2$. In case of $\mathbf{F}$ this is well-defined from the definition of $\mathsf{SoEM22}$. In the ideal system we sample $(\mathsf{K}_1, \mathsf{K}_2) \leftarrow_{\$} \{0,1\}^{2n}$. Note that, once K_1 and K_2 are released, one can easily obtain A^q, C^q, B^q, and D^q.

BAD TRANSCRIPT AND ITS ANALYSIS. A transcript is called bad precisely when it leads to permutation incompatibility for any one of the underlying permutations. One way to avoid such inconsistencies is to avoid input/output collision constraints over the two permutations simultaneously. More formally, we say that a transcript is bad if one of the following events occur for some $(\mathsf{M}_i, \mathsf{Z}_i) \in \tau_c, (\mathsf{U}_j, \mathsf{V}_j) \in \tau_1, (\mathsf{X}_{j'}, \mathsf{Y}_{j'}) \in \tau_2$,

1. B1: $\mathsf{A}_i = \mathsf{U}_j$ and $\mathsf{C}_i = \mathsf{X}_{j'}$.

2. B2: $\mathsf{A}_i = \mathsf{U}_j$ and $\mathsf{B}_i \oplus \mathsf{Z}_i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2 = \mathsf{Y}_{j'}$.

3. B3: $\mathsf{C}_i = \mathsf{X}_{j'}$ and $\mathsf{D}_i \oplus \mathsf{Z}_i \oplus \mathsf{K}_1 \oplus \mathsf{K}_2 = \mathsf{V}_j$.

Here, B1 corresponds to collision on the input of the two underlying permutation; B2 corresponds to input collision on $\boldsymbol{\pi}_1$ and output collision on $\boldsymbol{\pi}_2$; and, B3 corresponds to input collision on $\boldsymbol{\pi}_2$ and output collision on $\boldsymbol{\pi}_1$. Note that we only consider collisions between construction and primitive queries. This is because of the fact that construction to construction and primitive to primitive collisions are forbidden by design. Now, we have

$$\Pr[\bar{\tau}(\mathbf{A}^{\boldsymbol{\rho}, \boldsymbol{\pi}_1^{\pm}, \boldsymbol{\pi}_2^{\pm}}) \in \Omega_{\mathsf{bad}}] \leq \sum_{i,j,j'} \Pr[\mathsf{B1}] + \Pr[\mathsf{B2}] + \Pr[\mathsf{B3}] \leq \frac{3qp^2}{2^{2n}},$$

where the last inequality can be argued by the fact that there are at most qp^2 many (i, j, j') triples, and for each such triple, $\Pr[\mathsf{Bi}] = 1/2^{2n}$ for all $\mathsf{i} \in [3]$. This is because each bad event reduces to a system of two linear equations in two independent and uniform random variables K_1 and K_2, whence a solution occurs with $1/2^{2n}$ probability.

ANALYSIS OF GOOD TRANSCRIPTS. Given a transcript $\tau = (x^q, y^q)$, it is easy to see that

$$\Pr[\boldsymbol{\rho}(x^q) = y^q, \boldsymbol{\pi}_1(u^p) = v^p, \boldsymbol{\pi}_2(x^p) = y^p, \mathsf{K}_1, \mathsf{K}_2] = \frac{1}{2^{nq}} \times \frac{1}{(2^n)_p} \times \frac{1}{(2^n)_p} \times \frac{1}{2^{2n}}, \quad (23)$$

as $m^q \rightsquigarrow z^q$, $u^p \leftrightsquigarrow v^p$, and $x^p \leftrightsquigarrow y^p$ and $(\mathsf{K}_1, \mathsf{K}_2)$ are chosen uniformly from $\{0,1\}^{2n}$. In real world, for primitive queries we know that $u^p \leftrightsquigarrow v^p$, and $x^p \leftrightsquigarrow y^p$. In construction queries, the i-th query could be one of the three types: (1) $a_i = u_j$ and $c_i \neq x_{j'}$ for all $j' \in [p]$; (2) $a_i \neq u_j$ for all $j \in [p]$ and $c_i = x_{j'}$; (3) $a_i \neq u_j$ and $c_i \neq x_{j'}$ for all $j, j' \in [p]$. It is easy to see that both a and c cannot collide simultaneously as the transcript is good. Let τ_C^1, τ_C^2, and τ_C^3 denote the type 1, type 2, and type 3, respectively, construction transcripts,

and q_1, q_2, and q_3, respectively, denote the number of such queries. Finally, we have

$$
\begin{aligned}
\Pr[\mathbf{F}(x^q) = y^q, \boldsymbol{\pi}_1(u^p) = v^p, \boldsymbol{\pi}_2(x^p) = y^p, \mathsf{K}_1, \mathsf{K}_2] &= \Pr[\tau_C, \tau_P, \mathsf{K}_1, \mathsf{K}_2] \\
&= \Pr[\tau_P] \times \Pr[\tau_C^1 \mid \tau_P] \times \Pr[\tau_C^2 \mid \tau_P \wedge \tau_C^1] \\
&\quad \times \Pr[\tau_C^3 \mid \tau_P \wedge \tau_C^1 \wedge \tau_C^2] \times \frac{1}{2^{2n}} \\
&= \frac{1}{2^{2n}} \times \frac{1}{(2^n)_p (2^n)_p} \times \frac{1}{(2^n - p)_{q_1}} \\
&\quad \times \frac{1}{(2^n - p)_{q_2}} \times \Pr[\tau_C^3 \mid \tau_P \wedge \tau_C^1 \wedge \tau_C^2]
\end{aligned}
$$

Observe that we can apply Proposition 8.1 to bound the conditional probability of τ_C^3 given τ_P, τ_C^1, and τ_C^2. So by using $s_1 = p + q_1$, $s_2 = p + q_2$, and the relation $q_1, q_2, q_3 < q$, we have

$$
\begin{aligned}
\Pr[\mathbf{F}(x^q) = y^q, \boldsymbol{\pi}_1(u^p) = v^p, \boldsymbol{\pi}_2(x^p) = y^p, \mathsf{K}_1, \mathsf{K}_2] &\geq \left(1 - \frac{2p^2 q}{2^{2n}} - \frac{6pq^2}{2^{2n}} - \frac{5q^3}{2^{2n}}\right) \times \frac{1}{2^{nq_3}} \\
&\quad \times \frac{1}{(2^n)_p (2^n)_p} \times \frac{1}{(2^n - p)_{q_1}} \\
&\quad \times \frac{1}{(2^n - p)_{q_2}} \times \frac{1}{2^{2n}}.
\end{aligned}
\tag{24}
$$

The result follows by dividing Eq. (24) by Eq. (23). □

9 Optimality of the Extended H-technique

We have already seen that the expectation method can achieve optimal bounds for distinguishing advantage. The extended H-technique is also a potential tool to obtain tight bound for distinguishing advantage. Now we describe why it is so. Suppose $\mathbf{F}$ and $\boldsymbol{\alpha}$ are two $(\mathcal{X}, \mathcal{Y})$ random systems. We usually choose $\boldsymbol{\alpha}$ to be an ideal random system (such as a random permutation or a random function) and $\mathbf{F}$ is the construction of our interest. Let

$$
\mathscr{E}_{\mathbf{F} \geq \boldsymbol{\alpha}} = \left\{ (x^q, y^q) \;\middle|\; r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q, y^q) := \frac{\Pr[\mathbf{F}(x^q) = y^q]}{\Pr[\boldsymbol{\alpha}(x^q) = y^q]} \geq 1 \right\}.
$$

The complement of the above set is denoted as $\mathscr{E}_{\mathbf{F} < \boldsymbol{\alpha}}$. We also define a binary random variable B adjoined with $\boldsymbol{\alpha}$ as follows. Let

$$
\Pr[\mathsf{B} = 0 \mid \boldsymbol{\alpha}(x^q) = y^q] = 1, \quad \forall (x^q, y^q) \in \mathscr{E}_{\mathbf{F} \geq \boldsymbol{\alpha}}
\tag{25}
$$

and

$$
\Pr[\mathsf{B} = 0 \mid \boldsymbol{\alpha}(x^q) = y^q] = r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q, y^q), \quad \forall (x^q, y^q) \in \mathscr{E}_{\mathbf{F} < \boldsymbol{\alpha}}.
\tag{26}
$$

We can combine these two equations and write the following for all (x^q, y^q):

$$
\Pr[\mathsf{B} = 1 \mid \boldsymbol{\alpha}(x^q) = y^q] = \max\{0, 1 - r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q, y^q)\}
\tag{27}
$$

and hence

$$
\Pr[\mathsf{B} = 1, \boldsymbol{\alpha}(x^q) = y^q] = \max\{0, \Pr[\boldsymbol{\alpha}(x^q) = y^q] - \Pr[\mathbf{F}(x^q) = y^q]\}.
\tag{28}
$$

We say that a transcript (x^q, y^q, b) is bad if $b = 1$. Fix any deterministic adversary $\mathscr{A}$. The probability that the extended transcript random variable $\bar{\tau}(\mathscr{A}^{\boldsymbol{\alpha}})$ is bad is

$$
\begin{aligned}
\Pr[\mathsf{B} = 1] &= \sum_{\mathscr{A}(y^q) = x^q} \max\{0, \Pr[\boldsymbol{\alpha}(x^q) = y^q] - \Pr[\mathbf{F}(x^q) = y^q]\} \\
&= \Delta(\tau(\mathscr{A}^{\mathbf{F}}) \; ; \; \tau(\mathscr{A}^{\boldsymbol{\alpha}})).
\end{aligned}
$$

Now we define B' adjoined with $\mathbf{F}$. The random variable B' is degenerated and takes value zero with probability one. In other words, $\Pr[\mathbf{F}(x^q) = y^q, \mathsf{B}' = 0] = \Pr[\mathbf{F}(x^q) = y^q]$. It is easy to see that for all (x^q, y^q),

$$\Pr[\mathbf{F}(x^q) = y^q, \mathsf{B}' = 0] \geq \Pr[\boldsymbol{\alpha}(x^q) = y^q, \mathsf{B} = 0].$$

So if we apply H-technique we actually obtain equality in Eq. 7.

Remark 3. Here we like to remark that although the extended H-technique and the expectation method can achieve optimal distinguishing bounds, this might require a very involved analysis. For the expectation method, identifying the optimal ϵ function and then giving a tight estimation for the expectation of this function could be quite hard. Similarly for the extended H-technique identifying the optimal bad event could be very hard. One thing is clear, however, that both these tools can achieve optimality whenever it is possible through game-playing or random systems methodology.

9.1   Nonadaptive PRP to SPRP

"Two weak make one strong" or the composition lemma [MP04, MPR07] states that, in information-theoretic setting, the composition of two NPRP secure block ciphers gives an SPRP secure block cipher. The initial proofs [MP04, MPR07] of this result were based on Maurer's random system methodology. Later Cogliati, Patarin and Seurin [CPS14] gave a much simpler proof using the standard H-technique.

CONSTRUCTION. Let $\mathbf{F}$ and $\mathbf{G}$ be two NPRP secure quasi-random permutations over $\mathcal{X}$. Then we are interested in the SPRP security of the composition $\mathbf{G}^{-1} \circ \mathbf{F}$. Formally the composition result is stated in Theorem 9.1.

Theorem 9.1. *Suppose $\mathbf{F}$ and $\mathbf{G}$ are two random systems over $\mathcal{X}$ then,*

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathbf{G}^{-1} \circ \mathbf{F}}(q) \leq \mathbf{Adv}^{\mathrm{nprp}}_{\mathbf{F}}(q) + \mathbf{Adv}^{\mathrm{nprp}}_{\mathbf{G}}(q).$$

In [CPS14], the following result has been proved. Lemma 9.1 gives a simple proof for Theorem 9.1 using standard H-technique.

Lemma 9.1. *For all $x^q, y^q \in \mathcal{X}^{(q)}$, we have*

$$\frac{\Pr[\mathbf{G}^{-1} \circ \mathbf{F}(x^q) = y^q]}{\Pr[\boldsymbol{\pi}(x^q) = y^q]} \geq 1 - \mathbf{Adv}^{\mathrm{nprp}}_{\mathbf{F}}(q) - \mathbf{Adv}^{\mathrm{nprp}}_{\mathbf{G}}(q).$$

Alternate proof using the extended-H technique. We give a similar but alternative proof for Theorem 9.1 using the idea of optimality of extended H-technique. Since we will employ extended H-technique, we start off with a description of the extended systems.

EXTENDED SYSTEMS. We consider $(\mathcal{X}^q \times \{0,1\}^2)$-extended random systems. We first define a triple of random variables $(\mathsf{Z}^q, \mathsf{B}_1, \mathsf{B}_2) \leftarrow \mathcal{X}^q \times \{0,1\} \times \{0,1\}$ adjoined with $\boldsymbol{\pi}^{\pm}$. Let $\tau(\mathscr{A}^{\boldsymbol{\pi}^{\pm}}) := (\delta^q, \mathsf{X}^q, \mathsf{Y}^q)$ be the forward only transcript. We sample $\mathsf{Z}^q \stackrel{\mathrm{wor}}{\longleftarrow} \mathcal{X}$ independent of $\boldsymbol{\pi}$ (and hence independent of the transcript τ as well). Now, we define the conditional distribution of $\mathsf{B}_1, \mathsf{B}_2$ given $(\delta^q, \mathsf{X}^q, \mathsf{Y}^q, \mathsf{Z}^q)$.

Fix three tuples $x^q, y^q, z^q \in \mathcal{X}^{(q)}$. We define the distributions of $\mathsf{B}_1, \mathsf{B}_2$ given that $\mathsf{X}^q = x^q, \mathsf{Y}^q = y^q$ and $\mathsf{Z}^q = z^q$. Note that the sampling of Z^q can be viewed as $\boldsymbol{\pi}'(\mathsf{X}^q)$ for a random permutation $\boldsymbol{\pi}'$ independent of $\boldsymbol{\pi}$. If $(x^q, z^q) \in \mathscr{E}_{\mathbf{F} \geq \boldsymbol{\pi}'}$ then $\mathsf{B}_1 = 0$ with probability one. Otherwise, B_1 follows Bernoulli distribution $\mathsf{ber}(1 - r^{\mathbf{F}/\boldsymbol{\pi}'}(x^q, z^q))$. Similarly, if $(y^q, z^q) \in \mathscr{E}_{\mathbf{G} \geq \boldsymbol{\pi}'}$ then $\mathsf{B}_2 = 0$ with probability one. Otherwise, B_2 follows Bernoulli distribution $\mathsf{ber}(1 - r^{\mathbf{G}/\boldsymbol{\pi}'}(y^q, z^q))$.

ANALYSIS OF BAD TRANSCRIPTS. We say that a transcript $(x^q, y^q, z^q, b_1, b_2)$ is bad if $b_1 = 1 \vee b_2 = 1$. For the random transcript variable $(\mathsf{X}^q, \mathsf{Y}^q, \mathsf{Z}^q, \mathsf{B}_1, \mathsf{B}_2)$, we denote this event by bad. By union bound,

$$\Pr[\mathsf{bad}] \le \Pr[\mathsf{B}_1 = 1] + \Pr[\mathsf{B}_2 = 1].$$

We now show that $\Pr[\mathsf{B}_1 = 1] \le \mathbf{Adv}_{\mathbf{F}}^{\mathrm{nprp}}(q)$. Similarly one can show that $\Pr[\mathsf{B}_2 = 1] \le \mathbf{Adv}_{\mathbf{G}}^{\mathrm{nprp}}(q)$. Similar to Eq. 28, we have

$$
\begin{aligned}
\Pr[\mathsf{B}_1 = 1] &= \sum_{\substack{(x^q, y^q) \in \mathscr{A} \\ z^q \in \mathscr{X}^{(q)}}} \Pr[\mathsf{B}_1 = 1, \mathsf{Z}^q = z^q, \mathsf{X}^q = x^q, \mathsf{Y}^q = y^q] \\
&= \sum_{\substack{(x^q, y^q) \in \mathscr{A} \\ z^q \in \mathscr{X}^{(q)}}} \Pr[\mathsf{B}_1 = 1, \boldsymbol{\pi}'(x^q) = z^q, \boldsymbol{\pi}(x^q) = y^q] \\
&= \sum_{(x^q, y^q) \in \mathscr{A}} \Pr[\boldsymbol{\pi}(x^q) = y^q] \sum_{z^q \in \mathscr{X}^{(q)}} \Pr[\boldsymbol{\pi}'(x^q) = z^q] \times \max\{0, 1 - r^{\mathbf{F}/\boldsymbol{\pi}'}(x^q, z^q)\} \\
&= \sum_{(x^q, y^q) \in \mathscr{A}} \Pr[\boldsymbol{\pi}(x^q) = y^q] \sum_{z^q \in \mathscr{X}^{(q)}} \max\{0, \Pr[\boldsymbol{\pi}'(x^q) = z^q] - \Pr[\mathbf{F}(x^q) - z^q]\} \\
&= \sum_{(x^q, y^q) \in \mathscr{A}} \Pr[\boldsymbol{\pi}(x^q) = y^q] \times \|\Pr_{\boldsymbol{\pi}'(x^q)} - \Pr_{\mathbf{F}(x^q)}\| \\
&\le \max_{a^q \in \mathscr{X}^{(q)}} \|\Pr_{\boldsymbol{\pi}'(a^q)} - \Pr_{\mathbf{F}(a^q)}\| \sum_{(x^q, y^q) \in \mathscr{A}} \Pr[\boldsymbol{\pi}(x^q) = y^q] \\
&\le \mathbf{Adv}_{\mathbf{F}}^{\mathrm{nprp}}(q).
\end{aligned}
$$

ANALYSIS OF GOOD TRANSCRIPTS. We define B_1' and B_2' adjoined with $\mathbf{F}$ in a similar fashion as in the case of optimality result. Both B_1' and B_2' are degenerated and take value zero with probability one. For $x^q, y^q, z^q \in \mathscr{X}^{(q)}$ and $i \in \{1, 2\}$, let $\mathsf{p}_i := \Pr[\mathsf{B}_i = 0 \mid \boldsymbol{\pi}(x^q) = y^q, \mathsf{Z}^q = z^q]$. Then we have

$$
\begin{aligned}
\Pr[\boldsymbol{\pi}(x^q) = y^q, \mathsf{Z}^q = z^q, \mathsf{B}_1 = 0, \mathsf{B}_2 = 0] &= \Pr[\boldsymbol{\pi}(x^q) = y^q] \times \Pr[\mathsf{Z}^q = z^q] \times \mathsf{p}_1 \times \mathsf{p}_2 \\
&= \Pr[\boldsymbol{\pi}(x^q) = y^q] \times \Pr[\mathsf{Z}^q = z^q] \times \mathsf{p}_1 \times \mathsf{p}_2 \\
&\le \Pr[\mathbf{F}(x^q) = z^q] \times \Pr[\mathbf{G}(y^q) = z^q] \\
&= \Pr[\mathbf{F}(x^q) = z^q, \mathbf{G}(y^q) = z^q, \mathsf{B}_1' = 0, \mathsf{B}_2' = 0] \\
&= \Pr[\mathbf{G}^{-1} \circ \mathbf{F}(x^q) = y^q, \mathsf{B}_1' = 0, \mathsf{B}_2' = 0]
\end{aligned}
$$

The result follows from extended H-technique Lemma 4.1.

10 Conclusion

In this systematization of knowledge, our main goal was to revisit a popular tool in symmetric-key provable security, called the (coefficients) H-technique [Pat91, Pat08a]. We re-formalized the notations and conventions necessary to study the security of any symmetric-key design. We then described the H-technique tool and showed that it can achieve optimal security bounds. To illustrate the effectiveness of this tool we gave simple security proofs for some popular symmetric key designs, across different paradigms.

Although our main goal is to promote the application of H-technique, we emphasize that it is not a universal solution. In particular there are many problems where a straightforward

application of H-technique may not give tight bound. A prime example is the sum of permutations or SoP problem [HWKS98, BI99]. While there are some tight bound proofs [Pat08b, Pat10] for SoP problem using H-technique, the veracity of these proofs is not yet established. In contrast, a recent tool by Dai et al., called the χ^2-method [DHT17], gives a much simple and asymptotically tight bound proof for SoP. The preceding example is just one such instance where one tool is somewhat superior to another. There could be many more. For instance, it is still not clear how one can apply the χ^2-method, with same ease as the H-technique, to the analysis of schemes based on low entropy primitives (such as universal hash functions).

To conclude, a thorough study on the various available tools is the need of the hour. This will help in choosing the right tools for a given set of problems, which in turn may give tight and/or simple proofs. We believe that this work is a step in that direction. It would be interesting to see similar work on some other popular tools like coupling technique [Mir02, MRS09, HR10] and χ^2-method [DHT17, BN18b]. At the same time, we must also look at some other avenues in probability theory to get new tools. For example Morris, Rogaway and Stegers explored the applications of Markov chains [MRS09], and Steinberger explored the Hellinger distance [Ste12].

References

[ABL+13]   Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tis-chhauser, and Kan Yasuda. Parallelizable and authenticated online ciphers. In *Advances in Cryptology - ASIACRYPT 2013 - 19th International Confer-ence on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, pages 424–443, 2013.

[AFF+14]   Farzaneh Abed, Scott R. Fluhrer, Christian Forler, Eik List, Stefan Lucks, David A. McGrew, and Jakob Wenzel. Pipelineable on-line encryption. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 205–223, 2014.

[AGKS05]   Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-kem/dem: A new framework for hybrid encryption and A new analysis of kurosawa-desmedt KEM. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 128–146, 2005.

[BBKN12]   Mihir Bellare, Alexandra Boldyreva, Lars R. Knudsen, and Chanathip Nam-prempre. On-line ciphers and the hash-cbc constructions. *J. Cryptology*, 25(4):640–679, 2012.

[BdBB+95]   A. Berendschot, B. den Boer, J. Boly, A. Bosselaers, J. Brandt, D. Chaum, I. Damgård, M. Dichtl, W. Fumy, M. van der Ham, C. Jansen, P. Landrock, B. Preneel, G. Roelofsen, P. de Rooij, and J Vandewalle. *Final Report of Race Integrity Primitives*, volume 1007 of *Lecture Notes in Computer Science, Springer-Verlag, 1995*. Springer-Verlag, 1995.

[Ber99]   Daniel J. Bernstein. How to Stretch Random Functions: The Security of Protected Counter Sums. *J. Cryptol.*, 12:185–192, 1999.

[BHT18]   Priyanka Bose, Viet Tung Hoang, and Stefano Tessaro. Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In *Advances*

in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I, pages 468–499, 2018.

[BI99] Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. *IACR Cryptology ePrint Archive*, 1999:24, 1999.

[BKR00] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.

[BN15] Ritam Bhaumik and Mridul Nandi. An inverse-free single-keyed tweakable enciphering scheme. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 159–180, 2015.

[BN16] Ritam Bhaumik and Mridul Nandi. Olef: an inverse-free online cipher. an on-line SPRP with an optimal inverse-free construction. *IACR Trans. Symmetric Cryptol.*, 2016(2):30–51, 2016.

[BN17] Ritam Bhaumik and Mridul Nandi. Improved security for OCB3. In *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, pages 638–666, 2017.

[BN18a] Srimanta Bhattacharya and Mridul Nandi. Full indifferentiable security of the xor of two or more random permutations using the \chi ^2 method. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 387–412, 2018.

[BN18b] Srimanta Bhattacharya and Mridul Nandi. A note on the chi-square method: A tool for proving cryptographic security. *Cryptography and Communications*, 10(5):935–957, 2018.

[BN18c] Srimanta Bhattacharya and Mridul Nandi. Revisiting variable output length XOR pseudorandom function. *IACR Trans. Symmetric Cryptol.*, 2018(1):314–335, 2018.

[BPR05] Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved Security Analyses for CBC MACs. In *Proc. CRYPTO 2005*, pages 527–545, 2005.

[BR05] John Black and Phillip Rogaway. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. *J. Cryptol.*, 18:111–131, 2005.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 409–426, 2006.

[CDMS10] Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, pages 273–289, 2010.

[CDNY18]   Avik Chakraborti, Nilanjan Datta, Mridul Nandi, and Kan Yasuda. Beetle family of lightweight and secure authenticated encryption ciphers. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):218–241, 2018.

[CIMN17]   Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi. Blockcipher-based authenticated encryption: How small can we go? In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 277–298, 2017.

[CLL+14]   Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the two-round even-mansour cipher. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 39–56, 2014.

[CLM19]   Yu Long Chen, Eran Lambooij, and Bart Mennink. How to build pseudorandom functions from public random permutations. *IACR Cryptology ePrint Archive*, 2019:554, 2019.

[CLMP17]   Yu Long Chen, Atul Luykx, Bart Mennink, and Bart Preneel. Efficient length doubling from tweakable block ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(3):253–270, 2017.

[CLS15]   Benoit Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking even-mansour ciphers. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 189–208, 2015.

[CLS17]   Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New constructions of macs from (tweakable) block ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(2):27–58, 2017.

[CMN18]   Yu Long Chen, Bart Mennink, and Mridul Nandi. Short variable length domain extenders with beyond birthday bound security. *IACR Cryptology ePrint Archive*, 2018:783, 2018.

[CPS14]   Benoit Cogliati, Jacques Patarin, and Yannick Seurin. Security amplification for the composition of block ciphers: Simpler proofs and new results. In *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, pages 129–146, 2014.

[CS03a]   Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 126–144, 2003.

[CS03b]   Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. Comput.*, 33(1):167–226, 2003.

[CS08]   Debrup Chakraborty and Palash Sarkar. HCH: A new tweakable enciphering scheme using the hash-counter-hash approach. *IEEE Trans. Information Theory*, 54(4):1683–1699, 2008.

[CS14]   Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 327–350, 2014.

[CS15a]   Benoît Cogliati and Yannick Seurin. Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 134–158, 2015.

[CS15b]   Benoit Cogliati and Yannick Seurin. On the provable security of the iterated even-mansour cipher against related-key and chosen-key attacks. In *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, pages 584–613, 2015.

[CS16]   Benoît Cogliati and Yannick Seurin. EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 121–149, 2016.

[DDN+17]   Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of pmac_plus. *IACR Trans. Symmetric Cryptol.*, 2017(4):268–305, 2017.

[DDNY18]   Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. *IACR Cryptology ePrint Archive*, 2018:500, 2018.

[DHT17]   Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, pages 497–523, 2017.

[DJN17]   Avijit Dutta, Ashwin Jha, and Mridul Nandi. Tight security analysis of ehtm MAC. *IACR Trans. Symmetric Cryptol.*, 2017(3):130–150, 2017.

[DN14]   Nilanjan Datta and Mridul Nandi. Elme: A misuse resistant parallel authenticated encryption. In *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, pages 306–321, 2014.

[Dwo01]   M Dworkin. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38a, NIST, U. S. Department of Commerce, 2001.

[FLLW16]   Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. POEx: A beyond-birthday-bound-secure on-line cipher. ArcticCrypt 2016, 2016. https://www.researchgate.net/publication/299565944_POEx_A_Beyond-Birthday-Bound-Secure_On-Line_Cipher.

[GGM84]   Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). In *25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984*, pages 464–479, 1984.

[GM84]   Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[GMR85]   Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 291–304, 1985.

[GS02]   Alison L. Gibbs and Francis Edward Su. On choosing and bounding probability metrics. *International Statistical Review*, 70(3):419–435, 2002.

[GW18]   Chun Guo and Lei Wang. Revisiting key-alternating feistel ciphers for shorter keys and multi-user security. *IACR Cryptology ePrint Archive*, 2018:816, 2018.

[Hal07]   Shai Halevi. Invertible universal hashing and the TET encryption mode. In *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, pages 412–429, 2007.

[HR03]   Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 482–499, 2003.

[HR04]   Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, pages 292–304, 2004.

[HR10]   Viet Tung Hoang and Phillip Rogaway. On generalized feistel networks. In *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, pages 613–630, 2010.

[HT16]   Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, pages 3–32, 2016.

[HT17]   Viet Tung Hoang and Stefano Tessaro. The multi-user security of double encryption. In *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, pages 381–411, 2017.

[HWKS98]   Chris Hall, David A. Wagner, John Kelsey, and Bruce Schneier. Building prfs from prps. In *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, pages 370–389, 1998.

[JN16]   Ashwin Jha and Mridul Nandi. Revisiting Structure Graphs: Applications to CBC-MAC and EMAC. *J. Mathematical Cryptology*, 10(3–4):157–180, 2016.

[JN18]   Ashwin Jha and Mridul Nandi. On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers. *Cryptography and Communications*, 10(5):731–753, 2018.

[KR11]   Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, pages 306–327, 2011.

[LN17]   Eik List and Mridul Nandi. ZMAC+ - an efficient variable-output-length variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.

[LPS12]   Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An asymptotically tight security analysis of the iterated even-mansour cipher. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 278–295, 2012.

[LPTY16]   Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A MAC mode for lightweight block ciphers. In *Proc. Fast Software Encryption - FSE 2016*, pages 43–59, 2016.

[LR85]   Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions (abstract). In *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, page 447, 1985.

[LS13]   Rodolphe Lampe and Yannick Seurin. Tweakable blockciphers with asymptotically optimal security. In *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, pages 133–151, 2013.

[LST12]   Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, pages 14–30, 2012.

[Luc00]   Stefan Lucks. The sum of prps is a secure PRF. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 470–484, 2000.

[Mau02]   Ueli M. Maurer. Indistinguishability of random systems. In *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, pages 110–132, 2002.

[Men15]   Bart Mennink. Optimally secure tweakable blockciphers. In *Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, pages 428–448, 2015.

[Men18]   Bart Mennink. Towards tight security of cascaded LRW2. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, pages 192–222, 2018.

[MI11]   Kazuhiko Minematsu and Tetsu Iwata. Building blockcipher from tweakable blockcipher: Extending FSE 2009 proposal. In *Cryptography and Coding - 13th IMA International Conference, IMACC 2011, Oxford, UK, December 12-15, 2011. Proceedings*, pages 391–412, 2011.

[MI15]   Kazuhiko Minematsu and Tetsu Iwata. Tweak-length extension for tweakable blockciphers. In *Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings*, pages 77–93, 2015.

[Min09]   Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, pages 308–326, 2009.

[Min15]   Kazuhiko Minematsu. Building blockcipher from small-block tweakable blockcipher. *Des. Codes Cryptography*, 74(3):645–663, 2015.

[Mir02]   Ilya Mironov. (not so) random shuffles of RC4. In *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, pages 304–319, 2002.

[MM07]   Kazuhiko Minematsu and Toshiyasu Matsushima. New Bounds for PMAC, TMAC, and XCBC. In *Proc. Fast Software Encryption - FSE 2007*, pages 434–451, 2007.

[MMH+14]   Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, pages 306–323, 2014.

[MN17]   Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, pages 556–583, 2017.

[MP03]   Ueli M. Maurer and Krzysztof Pietrzak. The security of many-round luby-rackoff pseudo-random permutations. In *Advances in Cryptology - EURO-CRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, pages 544–561, 2003.

[MP04]   Ueli M. Maurer and Krzysztof Pietrzak. Composition of random systems: When two weak make one strong. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, pages 410–427, 2004.

[MPR07]   Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, pages 130–149, 2007.

[MRS09]   Ben Morris, Phillip Rogaway, and Till Stegers. How to encipher messages on
           a small domain. In *Advances in Cryptology - CRYPTO 2009, 29th Annual
           International Cryptology Conference, Santa Barbara, CA, USA, August 16-20,
           2009. Proceedings*, pages 286–302, 2009.

[Nan06]   Mridul Nandi. A simple and unified method of proving indistinguishability.
           In *Progress in Cryptology - INDOCRYPT 2006, 7th International Conference
           on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings*,
           pages 317–334, 2006.

[Nan08]   Mridul Nandi. Two new efficient cca-secure online ciphers: MHCBC and
           MCBC. In *Progress in Cryptology - INDOCRYPT 2008, 9th International
           Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008.
           Proceedings*, pages 350–362, 2008.

[Nan10]   Mridul Nandi. The characterization of luby-rackoff and its optimum single-key
           variants. In *Progress in Cryptology - INDOCRYPT 2010 - 11th International
           Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010.
           Proceedings*, pages 82–97, 2010.

[NPV17]   Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers -
           Security Proofs and Cryptanalysis*. Springer, 2017.

[NR97]   Moni Naor and Omer Reingold. On the construction of pseudo-random
           permutations: Luby-rackoff revisited (extended abstract). In *Proceedings of
           the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El
           Paso, Texas, USA, May 4-6, 1997*, pages 189–199, 1997.

[Pat90]   Jacques Patarin. Pseudorandom permutations based on the DES scheme.
           In *EUROCODE '90, International Symposium on Coding Theory and Ap-
           plications, Udine, Italy, November 5-9, 1990, Proceedings*, pages 193–204,
           1990.

[Pat91]   Jacques Patarin. *Etude des Générateurs de Permutations Pseudo-aléatoires
           Basés sur le Schéma du DES*. PhD thesis, Université de Paris, 1991.

[Pat97]   Jacques Patarin. Improved security bounds for pseudorandom permutations.
           In *CCS '97, Proceedings of the 4th ACM Conference on Computer and Com-
           munications Security, Zurich, Switzerland, April 1-4, 1997.*, pages 142–150,
           1997.

[Pat98]   Jacques Patarin. About feistel schemes with six (or more) rounds. In *Fast
           Software Encryption, 5th International Workshop, FSE '98, Paris, France,
           March 23-25, 1998, Proceedings*, pages 103–121, 1998.

[Pat03]   Jacques Patarin. Luby-rackoff: 7 rounds are enough for $2^{n(1\text{-epsilon})}$ security.
           In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryp-
           tology Conference, Santa Barbara, California, USA, August 17-21, 2003,
           Proceedings*, pages 513–529, 2003.

[Pat04]   Jacques Patarin. Security of random feistel schemes with 5 or more rounds.
           In *Advances in Cryptology - CRYPTO 2004, 24th Annual International Cryp-
           tologyConference, Santa Barbara, California, USA, August 15-19, 2004, Pro-
           ceedings*, pages 106–122, 2004.

[Pat08a]   Jacques Patarin. The "coefficients H" technique. In *Selected Areas in Cryp-
           tography, 15th International Workshop, SAC 2008, Sackville, New Brunswick,
           Canada, August 14-15, Revised Selected Papers*, pages 328–345, 2008.

[Pat08b]   Jacques Patarin. A proof of security in o(2n) for the xor of two random permutations. In *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*, pages 232–248, 2008.

[Pat10]   Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.

[RBBK01]   Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In *CCS 2001, Proceedings*, pages 196–205, 2001.

[Rog04]   Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, pages 16–31, 2004.

[RR07]   Thomas Ristenpart and Phillip Rogaway. How to enrich the message space of a cipher. In *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, pages 101–118, 2007.

[RS06]   Phillip Rogaway and Thomas Shrimpton. A provable-security treatment of the key-wrap problem. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, pages 373–390, 2006.

[RZ11]   Phillip Rogaway and Haibin Zhang. Online ciphers from tweakable blockciphers. In *Topics in Cryptology - CT-RSA 2011 - The Cryptographers' Track at the RSA Conference 2011, San Francisco, CA, USA, February 14-18, 2011. Proceedings*, pages 237–249, 2011.

[Sar07]   Palash Sarkar. Improving upon the TET mode of operation. In *Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings*, pages 180–192, 2007.

[Sar09]   Palash Sarkar. Efficient tweakable enciphering schemes from (block-wise) universal hash functions. *IEEE Trans. Information Theory*, 55(10):4749–4760, 2009.

[Sho00a]   Victor Shoup. A composition theorem for universal one-way hash functions. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 445–452, 2000.

[Sho00b]   Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 275–288, 2000.

[Sho02]   Victor Shoup. OAEP reconsidered. *J. Cryptology*, 15(4):223–249, 2002.

[Sho04]   Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive*, 2004:332, 2004.

[Ste12] John P. Steinberger. Improved security bounds for key-alternating ciphers via hellinger distance. *IACR Cryptology ePrint Archive*, 2012:481, 2012.

[Vau03] Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptology*, 16(4):249–286, 2003.

[WC79] Mark N. Wegman and Larry Carter. New classes and applications of hash functions. In *20th Annual Symposium on Foundations of Computer Science, San Juan, Puerto Rico, 29-31 October 1979*, pages 175–182, 1979.

[WFW05] Peng Wang, Dengguo Feng, and Wenling Wu. HCTR: A variable-input-length enciphering mode. In *Information Security and Cryptology: First SKLOIS Conference, CISC 2005, Proceedings*, pages 175–188, 2005.

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 80–91, 1982.

[Yas10] Kan Yasuda. The sum of CBC macs is a secure PRF. In *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, pages 366–381, 2010.

[Yas11] Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, pages 596–609, 2011.