Applications of H-Technique: Revisiting Symmetric Key Security Analysis

Ashwin Jha and Mridul Nandi

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

Abstract. The Coefficients H Technique (also called H-technique), by Patarin, is a tool to obtain upper bound on the distinguishing advantage. The tool is known for providing quite simpler and tight bound proofs as compared to some other well-known tools such as Game-playing technique and Random Systems methodology. In this paper, we aim to provide a brief survey on the H-technique. The survey is in three parts: First, we redevelop the necessary nomenclatures and tools required to study the security of symmetric key designs. Second, we give a full description of the H-technique and show that it can provide optimal bounds on the distinguishing advantage. Third, we give simpler proofs for some popular symmetric key designs, across different paradigms, using the H-technique.

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 [1] and (strong) pseudo random permutations or (S)PRPs [2] have been defined via distinguishing games. Informally, an adversary interacts with either the keyed construction of our interest or with the ideal version such as a uniform random function or permutation. The adversary's goal is to determine 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).

If we closely look at the security proofs for known 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 theoretic indistinguishable from ideal candidates). The next and the final step is to provide security analysis of the hybrid construction. 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 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.

Game-Playing Technique: Arguably the most popular, and certainly the oldest proof technique is the so-called Game-playing technique [3,4]. 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 towards 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 has been used in many early works [5,6]. In later years, Shoup extensively used this technique [7,8,4,9,10,11].

The contemporary version of this tool is due to Bellare and Rogaway's systematized treatment [3], 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 identicality breaks when one of the game sets a flag *bad* to true. Consequently the adversary's advantage in distinguishing the two games is upper bounded by the probability that this flag gets set. Game-playing technique has been used to prove security in almost all type of security notions in symmetric-key cryptography. For example game-playing technique was employed in the following:

1. (Tweakable) Enciphering Schemes such as CMC [12], EME [13], TET [14], HCH [15], HCTR [16], HEH [17,18], XLS [19];
2. PRFs and MACs such as CBC-MAC [20,21], ECBC, FCBC and XCBC [22], PMAC+ [23], sum of ECBC [24] etc.;
3. Online Ciphers such as HCBC1 and HCBC2 [25], TC1, TC2 and TC3 [26], POEx [27] etc.;
4. AE schemes such as OCB [28,29], COPA [30] and POET [31].

Coefficient H-Technique: At SAC '08, Patarin formally introduced the coefficient H-technique [32], although he had already used the technique in some of his earlier works [33,34,35,36,37]. In fact, it was Vaudenay who first reported the H-technique publicly in his decorrelation theory [38]. However, he mentioned that the technique is described in Patarin's PhD thesis [34] written in French. Independently, Bernstein rediscovered a weaker version of the result in [39], as the *interpolation theorem*. This was later strengthened by Nandi [40] as the *strong interpolation theorem*. Later, Chen and Steinberger gave a renewed interpretation of H-technique in their work on key alternating ciphers [41]. They hoped that *"paper will serve as a useful additional tutorial on (or introduction to) Patarins 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.

The H-technique concentrates on the input-output tuple generated by 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 a transcript can be realized by the real oracle to the probability that it can be realized by the ideal oracle. But it might be possible that certain transcripts are bad (may lead to inconsistency or are improbable) in the real world. In those cases, we also have to add the probability of realizing a bad transcript in the ideal world to the distinguishing advantage. It can 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 steady rise in the application of H-technique. Some of the schemes which were analyzed with H-technique include:

- (Online) PRP/SPRPs such as Feistel [37,42,43], MHCBC and MCBC [44], (Tweakable) Even-Mansour [45,41,46,47,48,49], FMix [50], OleF [51], two-round LDT [52] etc.;
- PRFs and MACs such as CBC-MAC [53], EWCDM [54,55], HaT and NaT [56], 1k-PMAC+ [57], EHtM [58], ZMAC+ [59], DWCDM [60] etc.;
- AE schemes such as ELmE [61], COFB [62], OCB3 [63], Beetle [64], GCM-SIV [65] and many more.

Maurer's Random System: At Eurocrypt '02, Maurer introduced the random system methodology (also called Maurer's methodology) for indistinguishability proofs [66]. 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, initialized to 0, if they give rise to same sequence of conditional probabilities until $B = 0$. 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 [66,67,68,69]. Later, Maurer's methodology was also applied to prove the security of PMAC, TMAC and XCBC [70], ENR and its variants [71,72,73], and XTX [74].

The Expectation and χ^2 Methods: The expectation method by Hoang and Tessaro [75] 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 [75] and to get multi-user security in [75,76,77].

The χ^2-method was proposed by Dai, Hoang and Tessaro [78], 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 [78,79], 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 [80] and the indifferentiability of sum of permutations [81]. Recently, beyond birthday security analysis of three-round LDT [82] 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.

Apart from these, Steinberger used the Hellinger distance [83] to study key alternating ciphers.

1.2 The H-Technique vs Other Proof Techniques

While the game-playing technique is simple in its philosophy, its application can be problematic in many cases. First, the proofs are awfully long and complex in some cases. For example, the first proof of PRF security of CBC-MAC [20] was quite complex and was later reduced to a very short and alternate proof by Bernstein [84]. The proofs are long partly due to the need for description of several intermediate games in order to rightly capture the bad events. Second, and a bit more serious issue is the high level description of probability distributions, which are prone to mistakes in actual probability calculations. For example such errors are prominent in [19,25,85,27,86]. To avoid this one has to describe the games in a more finer detail which adds to the proof complexity.

Maurer's methodology partly resolves some issues in game-playing technique. But even here one has to ensure that two oracles behave exactly identical until some bad events hold (similar to the game playing approach). However, in some cases showing this identical behavior is not easy.

In contrast to both game-playing and Maurer's random system methodology, the H-technique (and its variants) allows more flexibility in the sense that it does not require exactly identical behavior until bad. Rather it requires that the ratio of the two joint distributions should be bounded within some small ϵ from 1. This allows for significantly simple proofs. In later section we show that an extended version of H-technique can actually achieve optimality which shows that the tool is flexible yet powerful.

1.3 Our Contribution

In this paper we revisit the security analysis of some of the well known symmetric-key constructions. We first model an interactive algorithm in its functional view, which provides the language of the proof of symmetric key designs. We describe the H-technique and see its application to the following constructions:

1. Composition of non-adaptive PRPs.
2. Hash-based schemes: Hash-then-PRF, Hash-then-TBC [59] and ENR [71,72]. In case of ENR we study a generic scheme, called NR*, which allows for simple proofs for both ENR and LDT [52].
3. Feistel cipher: 3-round Luby-Rackoff [2] and 3-round tweakable block cipher based Luby-Rackoff [87].
4. SPRP enciphering schemes: HCTR [16] and TET [14].

The constructions are chosen based on the relative simplicity of their proofs in H-technique as compared to game-playing technique or Maurer's methodology. We intend to further extend this list in future.

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 we prove the optimality of H-technique and use similar ideas to give an alternate proof for the non-adaptive to adaptive PRP composition. In section 6, 7 and 8, we give alternate proofs for some hash based schemes, Feistel-like schemes and popular SPRP schemes, respectively.

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. 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 $\mathscr{X}$, we write $\mathscr{X}^{(r)}$ for the set of all r tuples $x^r \in \mathscr{X}^r$ 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 $\mathscr{X}$ is N then clearly, $|\mathscr{X}^{(r)}| = (N)_r$.

A function $g(a, b)$ is functionally independent of b if for all 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 $\mathscr{I}$, we denote an indexed family (or a tuple) as $\{x_i\}_{i \in \mathscr{I}}$ or $x^{\mathscr{I}}$. [1] More formally, it can be represented as a function from the index set to some set where x_i values belong.

[1] Note that it is different from the set $\{x_i : i \in \mathscr{I}\}$. 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 $\mathscr{X}$ to $\mathscr{Y}$ is denoted as $\mathsf{Func}(\mathscr{X}, \mathscr{Y})$. Similarly, the set of all permutations over $\mathscr{Y}$ is denoted as $\mathsf{Perm}(\mathscr{Y})$.

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 [88] 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 Ω. We define statistical distance between Pr_0 and Pr_1 as*

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

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 of the probability distributions are disjoint and it is zero if the support of the probability distributions are same.

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

$$E_{>} = \{x : \mathsf{Pr}_0(x) > \mathsf{Pr}_1(x)\} \text{ and}$$
$$E_{\geq} = \{x : \mathsf{Pr}_0(x) \geq \mathsf{Pr}_1(x)\}.$$

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

$$\max_E \big(\mathsf{Pr}_0(E) - \mathsf{Pr}_1(E)\big) = \sum_{x \in \Omega} \max\{0, \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)\} \ = \ \|\mathsf{Pr}_0 - \mathsf{Pr}_1\|.$$

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

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

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

So,

$$\begin{aligned} \sum_{x\in\Omega} \max\{0, \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x)\} &= \sum_{x\in E_>} \mathsf{Pr}_0(x) - \mathsf{Pr}_1(x) \\ &= \max_E \big(\mathsf{Pr}_0(E) - \mathsf{Pr}_1(E)\big). \end{aligned}$$

This proves the first equality. Now, we write

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

The first sum can be simplified as

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

Similarly, the second sum can be simplified to

$$\begin{aligned} \sum_{x\notin E_>} \mathsf{Pr}_1(x) - \mathsf{Pr}_0(x) &= \mathsf{Pr}_1(E^c_>) - \mathsf{Pr}_0(E^c_>) \\ &= \mathsf{Pr}_0(E_>) - \mathsf{Pr}_1(E_>) \end{aligned}$$

If we add these two sums, we obtain the second equality. □

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 *(i.e.,* $\mathsf{Pr}[\mathsf{X}_0 = x] > 0$*). Then,*

$$\|\mathsf{Pr}_0 - \mathsf{Pr}_1\| \;=\; \mathsf{Ex}\big(\epsilon_{\mathsf{opt}}(\mathsf{X}_0)\big).$$

3 Models for Interactive Algorithms

3.1 Probabilistic Function

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* $\mathcal{X}$ *and an output space* $\mathcal{Y}$ *is a function* $f : \mathcal{R} \times \mathcal{X} \to \mathcal{Y}$ *for some finite set* $\mathcal{R}$*, called* **random coin space**. *We also simply write (abusing notation)* $f : \mathcal{X} \xrightarrow{*} \mathcal{Y}$ *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 $\mathsf{R} \overset{*}{\leftarrow} \mathscr{R}$ (in most cases uniformly) and then we define an output random variable $f(x) := f(\mathsf{R}, x)$ over $\mathscr{Y}$. So, for all $y \in \mathscr{Y}$,

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

Definition 3.2. *With each probabilistic function $f : \mathscr{X} \overset{*}{\rightarrow} \mathscr{Y}$, 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 p^f **probabilistic system** *associated to a 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 $k \in \mathscr{K}$, $F_k : \mathscr{X} \rightarrow \mathscr{Y}$.

We sample key $\mathsf{K} \leftarrow_{\$} \mathscr{K}$ and treat it as a random coin,

we obtain a probabilistic function (abusing notation) $F : \mathscr{X} \overset{*}{\rightarrow} \mathscr{Y}$, mapping x to $F(\mathsf{K}, x) := F_{\mathsf{K}}(x)$ (also written as $\mathsf{K}(x)$, whenever there is no confusion about the family F).

Notation. Given a probabilistic function $f : \mathscr{X} \overset{*}{\rightarrow} \mathscr{Y}_1 \times \mathscr{Y}_2$ we write $f = (f_1, f_2)$ where $f(r, x) = (f_1(r, x), f_2(r, x))$ and $f_i : \mathscr{X} \overset{*}{\rightarrow} \mathscr{Y}_i$, $i = 1, 2$. The probabilistic functions f_1 and f_2 are basically two components of f and we also call them truncated probabilistic functions.

3.2 Function Models of Interactive Algorithms and Their Interaction

An interactive algorithm is modeled as a (probabilistic) interactive Turing machine [89,1]. In this paper, probabilistic functions are modeled for interactive algorithms. This model is general enough to capture finite and bounded interaction (i.e. the number of interaction between two algorithms is bounded by some fixed positive integer, say q) between two interactive algorithms.

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* $\mathbf{F} : \mathscr{X}^q \overset{*}{\to} \mathscr{Y}^q$ *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* $\mathscr{A} : \mathscr{Y}^q \overset{*}{\to} \mathscr{X}^q$ *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. Joint query functions capture those interactive algorithms which can initiate interactions between two interactive algorithms. A joint response function can interact with a joint query function. 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', transcript is the unique pair (x^q, y^q) such that $\mathscr{A}(r, x^q) = y^q$ and $\mathbf{F}(r', y^q) = x^q$. 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

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

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

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

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

Extended Transcript. 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*

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

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 keeps the information whether the bad happened on each query. Whenever bad flag set true, it continues to be true in 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 a MBO S.

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

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

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

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

The proof of the above equation is straightforward from the definition of the transcript (and the independence of random coins of $\mathscr{A}$ and $\bar{\mathbf{F}}$) and so we skip the proof. For simplicity, we sometimes simply call an extended joint response function as a joint response function (the extension or release of the adjoined random variable should be clear from the context).

3.3 Random System: Probabilistic Model for Interactive Algorithms

The probabilistic systems $\mathsf{p}^{\mathbf{F}}$ and $\mathsf{p}^{\mathscr{A}}$ associated with a joint response function $\mathbf{F}$ and joint query function $\mathscr{A}$ are called **response system** and **query system** respectively. Note that $\mathsf{p}^{\mathbf{F}}$ (and similarly $\mathsf{p}^{\mathscr{A}}$) cannot be any arbitrary family of probability functions. As it is induced from a response function,

$$\sum_{y^{\geq i}} \mathsf{p}^{\mathbf{F}}_{x^q}(y^q) \text{ is functionally independent of } x^{\geq i} \text{ for all } i \in [q].$$

$\sum_{y^{\geq i}} \mathsf{p}^{\mathbf{F}}_{x^q}(y^q)$ actually represents the marginal distribution of the first $(i-1)$ responses which can only depend on the first $(i-1)$ queries. So we simply write the above sum as $\mathsf{p}^{\mathbf{F}}_{x^{i-1}}(y^{i-1})$.

An $\mathscr{Y}^q$-indexed family of probability functions p is called response system if $\sum\limits_{y^{\geq i}} \mathsf{p}_{x^q}(y^q)$ is functionally independent of $x^{\geq i}$ for all $i \in [q]$. Similarly, one can define a query system.

Random system Maurer in [66] introduced random system which is basically equivalent representation of response and query systems as defined above. Instead of joint probabilities, random system collects all conditional probabilities which captures the probabilistic behavior of every response given the previous history of query and responses.

Definition 3.6 (random system). *An $(\mathscr{X}, \mathscr{Y})$ random system is a family*

$$\{p_{x^i, y^{i-1}} \mid i \in [q], x^i \in \mathscr{X}^i, y^{i-1} \in \mathscr{Y}^{i-1}\}$$

of probabilities over $\mathscr{Y}$.

In the above definition one can define all these probabilities freely (i.e. no constraint is imposed). Given a family, one can define a response system $\{\mathsf{p}_{x^q} \mid y^q \in \mathscr{Y}^q\}$ where

$$\mathsf{p}_{x^q}(y^q) = \prod_{i=1}^{q} p_{x^i, y^{i-1}}(y_i).$$

It is straightforward to verify the condition of responses system for the above family. Conversely, given a response system p, we define

$$p_{x^i, y^{i-1}}(y_i) = \mathsf{p}_{x^i}(y^i)/\mathsf{p}_{x^{i-1}}(y^{i-1})$$

whenever $\mathsf{p}_{x^{i-1}}(y^{i-1}) > 0$. One can arbitrarily define $p_{x^i, y^{i-1}}(y_i)$ when $\mathsf{p}_{x^{i-1}}(y^{i-1}) = 0$. It is easy to see that if $\mathbf{F}$ is a joint response function, the families defined as above is a random system. So we conclude that the response system and random system are equivalent. In what follows we treat response system and random system equivalently. However, we mostly use the joint distribution (i.e. response system) rather than conditional probabilities, because it simplifies security analyses. Moreover, joint distribution or the response system is directly associated with the joint response function.

3.4 Examples of Response Function or Random System

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

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

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 3.7. *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*

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

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

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

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

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 3.8 (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),*

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

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

Definition 3.9 (random permutation). *An $\mathcal{Y}$ random permutation is an $(\mathcal{Y},\mathcal{Y})$ joint response function $\boldsymbol{\pi}$ such that for all $x^q, y^q \in \mathcal{Y}^q$ with $x^q \leftrightsquigarrow y^q$ (permutation compatible),*

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

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), $\mathsf{Pr}[\boldsymbol{\pi}^{\pm}(\delta^q, x^q) = y^q] = \frac{1}{(N)_s}$ 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 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 random permutation, the keys 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 $\boldsymbol{\pi}(k, x) = k(x)$. Both are actually same function defined over two different domains.

One can simply verify that the probabilistic system associated to these keyed functions are same as those defined above.

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 3.10 (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 $\mathsf{mcoll}(t^q) = c^r$,*

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

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

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

Intuitively, when we response the i^{th} query (t_i, x_i), we look at all those j for which $t_j = t_i$. Let $\mathscr{S}_i$ be the set of all y_j values for which $t_j = t_i$. The response of the i^{th} query is to select an element randomly from $\mathscr{S}_i^c$ (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 $\mathsf{Func}(\mathscr{T}, \mathsf{Perm}(\mathscr{Y}))$, 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 $\mathscr{Y}$. 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: A Tool to Bound Distinguishing Advantage

4.1 Distinguisher and Its Advantage

Let $\mathbf{F}$ and $\mathbf{G}$ be two $(\mathscr{X}, \mathscr{Y})$ joint response functions and $\mathscr{A}$ be an $(\mathscr{X}, \mathscr{Y})$ joint query system with random coin space $\mathscr{R}$. Let $b : \mathscr{R} \times \mathscr{X}^q \times \mathscr{Y}^q \to \{0, 1\}$ 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

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

Let $\mathscr{E}$ be the set of all tuples (r, x^q, y^q) for which b returns 1. So,

$$\mathsf{Pr}[\mathscr{A}_b^{\mathbf{F}} \to 1] = \mathsf{Pr}[(\mathsf{R}, \tau(\mathscr{A}^{\mathbf{F}})) \in \mathscr{E}]$$
$$\mathsf{Pr}[\mathscr{A}_b^{\mathbf{G}} \to 1] = \mathsf{Pr}[(\mathsf{R}, \tau(\mathscr{A}^{\mathbf{G}})) \in \mathscr{E}]$$

From the equivalent definition of statistical distance (see Lemma**??**) 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.

Conventions. Now we state some conventions depending on different situations which are widely used to simplify the distinguishing advantage and analysis.

1. **Unbounded time query system**: When we consider unbounded time adversary, 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. In those cases, all adversaries in what follows are also assumed to be *deterministic adversaries.*[2] This can be justified as follows: 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,
$$\Delta_{\mathscr{A}}(\mathbf{F}\ ;\ \mathbf{G}) \leq \Delta_{\mathscr{A}[r_0]}(\mathbf{F}\ ;\ \mathbf{G}).$$
Now we can simply write the distinguishing advantage as $\Delta_{\mathscr{A}}(\mathbf{F}\ ;\ \mathbf{G}) = \Delta(\tau(\mathscr{A}^{\mathbf{F}})\ ;\ \tau(\mathscr{A}^{\mathbf{G}}))$. If $\tau(\mathscr{A}^{\mathbf{F}}) = (\mathsf{X}^q, \mathsf{Y}^q)$ then X^q is uniquely determined by Y^q as $\mathscr{A}(\mathsf{Y}^q)$. Similarly for the transcript $\tau(\mathscr{A}^{\mathbf{G}})$.
2. **Deterministic keyed function**: 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 $i < j$). This is redundant because the response of jth query is exactly same as that of ith query. So, without loss of generality, *we assume that all such adversaries are non-redundant, i.e. make distinct queries.*
3. **Deterministic keyed strong permutation**: A similar treatment can be applied for deterministic keyed strong permutation. 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 i^{th} 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 i^{th} query. Similarly, we define redundant queries for tweakable keyed permutation. The i^{th} 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 $\mathbb{A}(\theta_C, \theta_D)$ (and $\mathbb{A}_{\text{na}}(\theta_C, \theta_D)$) denote the set

[2] Here we would like to remark that the deterministic adversaries is not assumed when the responses systems may depend on the adversary. This has been the case for one definition of indifferentiable pseudorandom oracle.

of all adversaries $\mathscr{A}$ using at most θ_C computational complexity and θ_D data complexity in an adaptive ways (and nonadaptive ways respectively).

1. - $\mathbf{Adv}^{\mathrm{prf}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\rho}),$
   - $\mathbf{Adv}^{\mathrm{nprf}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}_{\mathrm{na}}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\rho}),$
2. - $\mathbf{Adv}^{\mathrm{prp}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\pi}),$
   - $\mathbf{Adv}^{\mathrm{sprp}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F}^{\pm} \; ; \; \boldsymbol{\pi}^{\pm}),$
   - $\mathbf{Adv}^{\mathrm{nprp}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}_{\mathrm{na}}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \boldsymbol{\pi}),$
3. - $\mathbf{Adv}^{\mathrm{tprp}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F} \; ; \; \widetilde{\boldsymbol{\pi}}),$
   - $\mathbf{Adv}^{\mathrm{tsprp}}_{\mathbf{F}}(\theta_C, \theta_D) = \max\limits_{\mathscr{A} \in \mathbb{A}(\theta_C, \theta_D)} \Delta_{\mathscr{A}}(\mathbf{F}^{\pm} \; ; \; \widetilde{\boldsymbol{\pi}}^{\pm}),$

If the computational complexity is unbounded (or infinity) in all these definitions, we simply drop the notation θ_C.

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. Suppose there is a set $\mathcal{V}_{\mathsf{bad}} \subseteq \mathcal{X}^q \times \mathcal{Y}^q \times \mathcal{S}$ such that for all $(x^q, y^q, s) \notin \mathcal{V}_{\mathsf{bad}}$,*

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

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

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

A proof of the H-technique is given among others in [34,32,40,41]. 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. From Lemma 2.1, we have

$$\begin{aligned}
\Delta(\bar{\tau}(\mathscr{A}^{\mathbf{F}})\ ;\ \bar{\tau}(\mathscr{A}^{\mathbf{G}})) &= \sum_{\nu\in\mathscr{V}} \max\{0, \mathsf{Pr}_{\bar{\mathbf{G}}}(\nu) - \mathsf{Pr}_{\bar{\mathbf{F}}}(\nu)\} \\
&= \sum_{\nu\in\mathscr{V}_{>}} \mathsf{Pr}_{\bar{\mathbf{G}}}(\nu)\cdot\left(1-\frac{\mathsf{Pr}_{\bar{\mathbf{F}}}(\nu)}{\mathsf{Pr}_{\bar{\mathbf{G}}}(\nu)}\right) \\
&\leq \sum_{\nu\in\mathscr{V}_{>}\cap\mathscr{V}_{\mathsf{bad}}} \mathsf{Pr}_{\bar{\mathbf{G}}}(\nu) + \epsilon \sum_{\nu\in\mathscr{V}_{>}\setminus\mathscr{V}_{\mathsf{bad}}} \mathsf{Pr}_{\bar{\mathbf{G}}}(\nu) \\
&\leq \mathsf{Pr}[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \mathscr{V}_{\mathsf{bad}}] + \epsilon.
\end{aligned}$$

□

A Note on Maurer's Tool. The main tool due to Maurer obtaining upper bound of distinguishing advantage is described as below (see [66] for details).

Lemma 4.2. *Let $\mathscr{V}_{\mathsf{bad}} = \{(x^q, y^q, b^q) : x^q \in \mathscr{X}^q, y^q \in \mathscr{Y}^q, b^q \neq 0^q\}$. Suppose $\bar{\mathbf{F}}$ and $\bar{\mathbf{G}}$ are MBO extensions of $(\mathscr{X}, \mathscr{Y})$ random systems $\mathbf{F}$ and $\mathbf{G}$ respectively. If $\bar{\mathbf{F}}$ and $\bar{\mathbf{G}}$ are identical until $\mathscr{V}_{\mathsf{bad}}$ then for all $\mathscr{A}$ interacting with $\mathbf{F}$ or $\mathbf{G}$*

$$\Delta_{\mathscr{A}}(\mathbf{F}\ ;\ \mathbf{G}) \leq \mathsf{Pr}[\tau(\mathscr{A}^{\bar{\mathbf{F}}}) \in \mathscr{V}_{\mathsf{bad}}] = \mathsf{Pr}[\tau(\mathscr{A}^{\bar{\mathbf{G}}}) \in \mathscr{V}_{\mathsf{bad}}] \tag{8}$$

This tool can be captured through the H-technique as follows. As $\bar{\mathbf{F}}$ and $\bar{\mathbf{G}}$ are identical until $\mathscr{V}_{\mathsf{bad}}$, for all (x^q, y^q),

$$\mathsf{Pr}[\bar{\mathbf{F}}(x^q) = (y^q, 0^q)] = \mathsf{Pr}[\bar{\mathbf{G}}(x^q) = (y^q, 0^q)].$$

So in the extended H-technique, we can take $\epsilon = 0$ and hence

$$\Delta_{\mathscr{A}}(\mathbf{F}\ ;\ \mathbf{G}) \leq \mathsf{Pr}[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \mathscr{V}_{\mathsf{bad}}].$$

$\mathsf{Pr}[\tau(\mathscr{A}^{\bar{\mathbf{F}}}) \in \mathscr{V}_{\mathsf{bad}}] = \mathsf{Pr}[\tau(\mathscr{A}^{\bar{\mathbf{G}}}) \in \mathscr{V}_{\mathsf{bad}}]$ can be verified easily from the observation that for all (x^q, y^q), $\mathsf{Pr}[\bar{\mathbf{F}}(x^q) = (y^q, 0^q)] = \mathsf{Pr}[\bar{\mathbf{G}}(x^q) = (y^q, 0^q)]$.

4.4 Expectation Method

Hoang and Tessaro [75] 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 4.3 (Expectation Method). *Suppose $\bar{\mathbf{F}} := (\mathbf{F}, \mathsf{S})$ and $\bar{\mathbf{G}} := (\mathbf{G}, \mathsf{S}')$ are two $\mathscr{S}$-extended $(\mathscr{X}, \mathscr{Y})$ response systems. Suppose there is a set $\mathscr{V}_{\mathsf{bad}} \subseteq \mathscr{X}^q \times \mathscr{Y}^q \times \mathscr{S}$, and a non-negative function $\epsilon : \mathscr{X}^q \times \mathscr{Y}^q \times \mathscr{S} \to [0, \infty)$ such that $\forall \bar{\tau} = (x^q, y^q, s) \notin \mathscr{V}_{\mathsf{bad}}$, 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 $(\mathscr{X}, \mathscr{Y})$ adversary $\mathscr{A}$,

$$\Delta_{\mathscr{A}}(\mathbf{F}\ ;\ \mathbf{G}) \leq \mathsf{Pr}[(\tau(\mathscr{A}^{\mathbf{G}}), \mathsf{S}') \in \mathscr{V}_{\mathsf{bad}}] + \mathbb{E}\left[\epsilon\left(\bar{\tau}(\mathbf{A}^{\mathbf{G}})\right)\right]. \tag{9}$$

One can set $\epsilon(\bar{\tau}) = 1$, for $\bar{\tau} \in \mathscr{V}_{\mathsf{bad}}$ to avoid the separate calculation of bad transcript probability. The extended H-technique is obtained from Eq. 9, 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 $\bar{\tau} \in \mathscr{X}^q \times \mathscr{Y}^q \times \mathscr{S}$, 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. 9, if we apply the expectation method with $\mathscr{V}_{\mathsf{bad}} = \emptyset$.

5 Composition of Two Weak Makes Strong

5.1 Optimality of Extended H-Technique

We have already seen that the expectation method can achieve optimal bounds for distinguishing advantage. 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 $(\mathscr{X}, \mathscr{Y})$ 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

$$\mathscr{E}_{\mathbf{F}\geq\boldsymbol{\alpha}} = \{(x^q,y^q) \mid r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q,y^q) \overset{\text{def}}{=} \frac{\mathsf{Pr}[\mathbf{F}(x^q) = y^q]}{\mathsf{Pr}[\boldsymbol{\alpha}(x^q) = y^q]} \geq 1\}.$$

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

$$\mathsf{Pr}[\mathsf{B} = 0 \mid \boldsymbol{\alpha}(x^q) = y^q] = 1, \quad \forall (x^q,y^q) \in \mathscr{E}_{\mathbf{F}\geq\boldsymbol{\alpha}} \tag{10}$$

and

$$\mathsf{Pr}[\mathsf{B} = 0 \mid \boldsymbol{\alpha}(x^q) = y^q] = r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q,y^q), \quad \forall (x^q,y^q) \in \mathscr{E}_{\mathbf{F}<\boldsymbol{\alpha}}. \tag{11}$$

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

$$\mathsf{Pr}[\mathsf{B} = 1 \mid \boldsymbol{\alpha}(x^q) = y^q] = \max\{0, 1 - r^{\mathbf{F}/\boldsymbol{\alpha}}(x^q,y^q)\} \tag{12}$$

and hence

$$\mathsf{Pr}[\mathsf{B} = 1, \boldsymbol{\alpha}(x^q) = y^q] = \max\{0, \mathsf{Pr}[\boldsymbol{\alpha}(x^q) = y^q] - \mathsf{Pr}[\mathbf{F}(x^q) = y^q]\}. \tag{13}$$

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

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

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 1. 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.

5.2 Nonadaptive PRP to SPRP

"Two weak make one strong" or the composition lemma [68,69] states that, in information-theoretic setting, the composition of two NPRP secure block ciphers gives an SPRP secure block cipher. The initial proofs [68,69] of this result were based on Maurer's random system methodology. Later Cogliati, Patarin and Seurin [90] 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 5.1.

Theorem 5.1. *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 [90], the following result has been proved. Lemma 5.1 gives a simple proof for Theorem 5.1 using standard H-technique.

Lemma 5.1. *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 extended-H technique. We give a similar but alternative proof for Theorem 5.1 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 $\mathsf{Z}^q \xleftarrow{\text{wor}} \mathscr{X}$ 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 $x^q, y^q, z^q \in \mathscr{X}^{(q)}$. 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,

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

We now show that $\mathsf{Pr}[\mathsf{B}_1 = 1] \leq \mathbf{Adv}_{\mathbf{F}}^{\text{nprp}}(q)$. Similarly one can show that $\mathsf{Pr}[\mathsf{B}_2 = 1] \leq \mathbf{Adv}_{\mathbf{G}}^{\text{nprp}}(q)$. Similar to Eq. 13, we have

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

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 $p_i := \mathsf{Pr}[\mathsf{B}_i = 0 \mid \boldsymbol{\pi}(x^q) = y^q, \mathsf{Z}^q = z^q]$. Then we have

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

The result follows from extended H-technique Lemma 4.1.

6 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 $\mathbf{H} : \mathscr{M} \xrightarrow{*} \mathscr{X}$ is a keyed function with key space (or random coin space) $\mathscr{H}$. For the sake of simplicity, we assume that hash key is chosen at random form the hash key space. Given a hash key $h \in \mathscr{H}$, we also simply denote the function $\mathbf{H}(h, M)$ as $h(M)$ whenever the keyed hash function $\mathbf{H}$ is understood from the context.

A hash function $\mathbf{H} : \mathscr{M} \xrightarrow{*} \mathscr{X}$ is called ϵ-*universal* if for all $m \neq m' \in \mathscr{M}$, $\Pr_{\mathsf{H} \leftarrow\!\!\$ \mathscr{H}}[\mathsf{H}(m) = \mathsf{H}(m')] = \Pr_{\mathsf{H} \leftarrow\!\!\$ \mathscr{H}}[\mathbf{H}(\mathsf{H}, m) = \mathbf{H}(\mathsf{H}, m')] \leq \epsilon$.

6.1 Hash-then-PRF

Construction. Let $\mathbf{H} : \mathscr{M} \xrightarrow{*} \mathscr{X}$ be an ϵ-universal hash and $\boldsymbol{\rho} : \mathscr{X} \xrightarrow{*} \mathscr{Y}$ be a random function. The composition function $\boldsymbol{\rho} \circ \mathbf{H} : \mathscr{M} \xrightarrow{*} \mathscr{Y}$ is known as hash-then-PRF construction. This construction has been studied in [91,92]. Many PRF constructions can be viewed as hash-then-PRF. For example, EMAC [93], ECBC and FCBC [22], LightMAC [94] and protected counter sum or PCS [39].

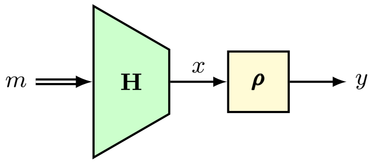

Fig. 6.1: The Hash-then-PRF paradigm. The double equal sign path denotes the possibility of a multi-block message.

Lemma 6.1. $\mathbf{Adv}^{\mathrm{prf}}_{\boldsymbol{\rho}\circ\mathbf{H}}(q) \leq \binom{q}{2}\epsilon$.

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 H-technique.

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 $\tau = (m^q, y^q)$ denote a transcript where $m^q \in \mathscr{M}^{(q)}$. All transcripts are considered to be good, i.e. no bad transcript is required in this proof. Now, given a transcript $\tau = (m^q, y^q)$, $\mathsf{Pr}[\boldsymbol{\rho}'(m^q) = y^q] = N^{-q}$. Now,

$$\begin{aligned} \mathsf{Pr}[\mathbf{F}(m^q) = y^q] &\geq \sum_{x^q \in \mathscr{X}^{(q)}} \mathsf{Pr}[\mathsf{H}(m^q) = x^q, \boldsymbol{\rho}(x^q) = y^q] \\ &= \sum_{x^q \in \mathscr{X}^{(q)}} \mathsf{Pr}[\mathsf{H}(m^q) = x^q] \times \mathsf{Pr}[\boldsymbol{\rho}(x^q) = y^q] \\ &= \mathsf{Pr}[\mathsf{H}(m^q) \in \mathscr{X}^{(q)}] \times N^{-q} \\ &\geq (1 - \binom{q}{2}\epsilon) \times N^{-q} \end{aligned}$$

Here we used the shorthand notation $\mathsf{H}(x) = \mathbf{H}(\mathsf{H}, x)$, i.e. H denotes the hash key. The last inequality follows from the union bound. Note that the complement of the event $\mathsf{H}(m^q) \in \mathscr{X}^{(q)}$ is that there is $i \neq j$, $\mathsf{H}(m_i) = \mathsf{H}(m_j)$. Finally, the ratio

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

Hence, by using H-technique, we have $\mathbf{Adv}^{\mathrm{prf}}_{\mathbf{F}}(q) \leq \binom{q}{2}\epsilon$. □

6.2 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.

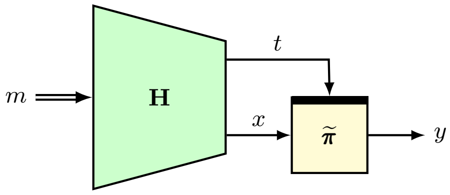

Fig. 6.2: The Hash-then-TPRP paradigm. The double equal sign path denotes the possibility of a multi-block message.

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 [56]. Later, the analysis of the above construction has been done [59]. 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 $\mathscr{X}$ (this is similar to the well know result of PRP-PRF switching lemma [3]). 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 the tweak space $\mathscr{T}$ as T. Let $\boldsymbol{\rho}$ be an ideal candidate, i.e. a random function from $\mathscr{M}$ to $\mathscr{X}$.

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 [59] 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 6.2. *Let Hash-then-TBC be defined as above. Then we have*

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

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 $\mathscr{H}$ be the key space of the hash function. We define a subset $\mathscr{H}_{\mathsf{good}} \subseteq \mathscr{H}$ as the set of all $h \in \mathscr{H}$ 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 $\mathsf{Pr}[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] \geq N^{-q}$. In the following, for any h, we denote $h(m^q) = (t^q, x^q)$.

$$\begin{aligned}
\mathsf{Pr}[\mathbf{F}(m^q) = y^q] &\geq \sum_{h \in \mathscr{H}_{\mathsf{good}}} \mathsf{Pr}[\mathsf{H} = h, \ \widetilde{\boldsymbol{\pi}}(\mathsf{H}(m^q)) = y^q] \\
&= \sum_{h \in \mathscr{H}_{\mathsf{good}}} \mathsf{Pr}[\mathsf{H} = h, \ \widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] \\
&= \sum_{h \in \mathscr{H}_{\mathsf{good}}} \mathsf{Pr}[\mathsf{H} = h] \times \mathsf{Pr}[\widetilde{\boldsymbol{\pi}}(t^q, x^q) = y^q] \\
&\geq \sum_{h \in \mathscr{H}_{\mathsf{good}}} \mathsf{Pr}[\mathsf{H} = h] \times N^{-q} \\
&= (1 - \mathsf{Pr}[\mathsf{H} \notin \mathscr{H}_{\mathsf{good}}]) \times N^{-q} \\
&\geq \left(1 - \binom{q}{2} \cdot \epsilon - C \cdot \epsilon_1\right) \times N^{-q} \qquad (14)
\end{aligned}$$

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

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

To obtain a bound, we have to get a good upper bound for $C(y^q)$ for all y^q. Now we have following two options to bound this.

(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

$$\mathsf{Pr}[\tau(\mathscr{A}^{\boldsymbol{\rho}}) \in \mathscr{V}_{\mathsf{bad}}] = \mathsf{Pr}[\mathsf{C} \geq \alpha] \leq \mathbb{E}[\mathsf{C}]/\alpha = \binom{q}{2} \cdot \frac{1}{\alpha N} \tag{15}$$

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. 14, we get

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

Finally, using the bad transcript probability of Eq. 15 and the standard H-technique, we get

$$\mathbf{Adv}^{\mathrm{prf}}_{\widetilde{\boldsymbol{\pi}} \circ \mathbf{H}} \leq \binom{q}{2} \cdot \frac{1}{\alpha N} + \binom{q}{2} \cdot \epsilon + \alpha \cdot \epsilon_1. \tag{16}$$

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

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

(2) Expectation Method: For small messages, there are universal hash function with $\epsilon \approx \frac{1}{NT}$ and $\epsilon_1 \approx \frac{1}{T}$. In this case, the prf advantage is $O(q^2/NT) + O(q/\sqrt{NT})$ So, the dominating term of the above result 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. 14). Thus we can use Lemma 4.3 to get

$$\mathbf{Adv}^{\text{prf}}_{\widetilde{\boldsymbol{\pi}}\circ\mathbf{H}}(q) \leq \mathbb{E}[\epsilon(\tau)] = \binom{q}{2}\epsilon + \binom{q}{2}\frac{\epsilon_1}{N}. \quad \square \tag{17}$$

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,

$$\mathbf{Adv}^{\mathrm{prf}}_{\widetilde{\boldsymbol{\pi}}\circ\mathbf{H}}(q) \leq \binom{q}{2} \cdot (\epsilon + \epsilon_1/N). \qquad \square \tag{18}$$

Remark 2. The XTX [74] and HaT [56] constructions are quite similar to Ht-TBC [59]. Consequently we get similar results for these constructions.

6.3 An extension of Naor-Reingold

The basic version of ENR is a $2n$-bit permutation based on an (n, n)-TBC and an n-bit AXU hash function, essentially adapting the Naor-Reingold [95] 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[52] in which the hash function is not present (can also be viewed as an identity function).

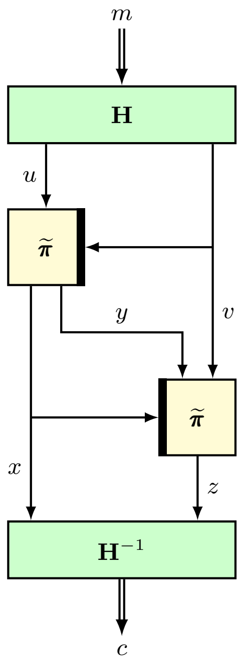
m
$\mathbf{H}$
u
$\widetilde{\boldsymbol{\pi}}$
y
v
$\widetilde{\boldsymbol{\pi}}$
x
z
$\mathbf{H}^{-1}$
c

Fig. 6.3: 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 $\boldsymbol{\Pi}$ 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 6.3.

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

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

Extended Systems. Suppose (δ^q, m^q, c^q) is the forward only transcript (before we extend). Now, we define $(\mathscr{H} \times \mathbb{F}^q_{2^{n-t}})$-extended random system. In the ideal system $\boldsymbol{\Pi}$, 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 $\boldsymbol{\Pi}$. Let $\bar{\boldsymbol{\Pi}}^{\pm} = (\boldsymbol{\Pi}^{\pm}, \mathsf{H}, \mathsf{Y}^q)$ 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. 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). Now we calculate the probability that a transcript $\tau(\mathscr{A}^{\bar{\boldsymbol{\Pi}}^{\pm}})$ 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 $\mathsf{Pr}[\mathsf{Y}_i = \mathsf{Y}_j] = 2^{t-n}$. Moreover, Y_i's are chosen independent of $(\boldsymbol{\Pi}, \mathsf{H})$ and hence independent of X and V values. So, it is sufficient to bound $\mathsf{Pr}[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j]$ for some $i < j$.

Claim. $\mathsf{Pr}[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j] \leq \frac{\epsilon}{T}$.

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 $\mathbf{H}_1(h, m_i) = \mathbf{H}_1(h, m_j)$ holds as $\mathscr{H}'$. So,

$$\begin{aligned}\mathsf{Pr}[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j \mid \mathsf{E}] &= \mathsf{Pr}[\mathbf{H}_1(\mathsf{H}, m_i) = \mathbf{H}_1(\mathsf{H}, m_j),\ \mathbf{H}_1(\mathsf{H}, c_i) = \mathbf{H}_1(\mathsf{H}, \mathsf{C}_j) \mid \mathsf{E}] \\ &= \sum_{h \in \mathscr{H}'} \mathsf{Pr}[\mathsf{H} = h,\ \mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}] \\ &= \sum_{h \in \mathscr{H}'} \mathsf{Pr}[\mathsf{H} = h] \times \mathsf{Pr}[\mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}] \\ &\leq \sum_{h \in \mathscr{H}'} \mathsf{Pr}[\mathsf{H} = h] \times \frac{1}{T}\end{aligned}$$

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 $NT - (j-1)$. Now, $\mathbf{H}_1(h, \mathsf{C}_j)$ realizes a value leads to $\mathbf{H}(h, \mathsf{C}_j)$ belong to a set of size N. Hence, $\mathsf{Pr}[\mathbf{H}_1(h, c_i) = \mathbf{H}_1(h, \mathsf{C}_j) \mid \mathsf{E}] \leq \frac{N}{NT-(j-1)} \leq \frac{1}{T}$. This proves that $\mathsf{Pr}[\mathsf{X}_i = \mathsf{X}_j, \mathsf{V}_i = \mathsf{V}_j \mid \mathsf{E}] \leq \frac{\epsilon}{T}$ which holds for any conditional event E and hence it is true for unconditional event also. This completes the proof of the claim.

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

$$\mathsf{Pr}[\tau(\mathscr{A}^{\bar{\boldsymbol{\Pi}}^{\pm}}) \text{ is bad}] \leq \frac{q(q-1)\epsilon}{2N}. \tag{19}$$

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,

$$\begin{aligned}\mathsf{Pr}[\mathbf{F}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}'^q = y^q] &= \mathsf{Pr}[\widetilde{\boldsymbol{\pi}}_1(v^q, u^q) = x^q \| y^q] \times \mathsf{Pr}[\widetilde{\boldsymbol{\pi}}_2(x^q, y^q \| v^q) = z^q] \times \mathsf{Pr}[\mathsf{H} = h] \\ &\geq \frac{1}{|\mathscr{H}|} \times \frac{1}{N^{2q}}.\end{aligned}$$

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

$$\begin{aligned}\mathsf{Pr}[\boldsymbol{\Pi}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}^q = y^q] &= \frac{1}{|\mathscr{H}|} \times \frac{1}{(NT)_q} \times \frac{T^q}{N^q} \\ &\leq \frac{1}{|\mathscr{H}|} \times \frac{1}{(NT)^q \cdot (1 - \frac{q(q-1)}{2NT})} \times \frac{T^q}{N^q}.\end{aligned}$$

So, the ratio

$$\frac{\mathsf{Pr}[\mathbf{F}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}'^q = y^q]}{\mathsf{Pr}[\boldsymbol{\Pi}(m^q) = c^q, \mathsf{H} = h, \mathsf{Y}^q = y^q]} \geq 1 - \frac{\binom{q}{2}}{NT}. \tag{20}$$

Combining Eq. 19 and Eq. 20 with Lemma 4.1 we get,

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathsf{NR}^*}(q) \leq \frac{\binom{q}{2}}{N}(\epsilon + \frac{1}{T}). \quad \square$$

Based on the security analysis of this generic design we can have simple proofs for ENR [71,72] and LDT [52].

A simple proof for ENR: The basic version of ENR [71] 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 $\mathsf{SmallBlock}$ [72] 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*

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

A simple proof for LDT[52]: The LDT 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.

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

7 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.

7.1 3-round Luby-Rackoff

Construction. Suppose $\boldsymbol{\psi}$ is a random functions over a set $\{0,1\}^n$ 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 [2] scheme, denoted $\mathsf{LR3}$, is defined as $\Psi_3 \circ \Psi_2 \circ \Psi_1$.

$\mathsf{LR3}$ is a well-studied birthday bound pseudorandom permutation. The original proof by Luby and Rackoff [2] is one of the foundational results in symmetric-key provable security. We now show how a fairly modern tool in symmetric-key

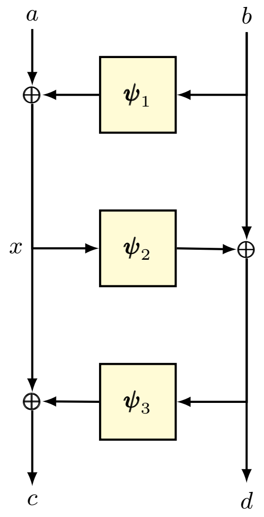

Fig. 7.1: The 3-round Luby-Rackoff or $\mathsf{LR3}$ construction.

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 [96]. Here we provide the proof of $\mathsf{LR3}$ in our language.

Lemma 7.1. *For $t \leq n$ we have*

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

Proof. We apply the basic 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 $\mathsf{LR3}$ and $\boldsymbol{\Pi}$ 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,

$$\mathsf{Pr}[\tau(\mathscr{A}^{\boldsymbol{\Pi}}) \text{ is bad }] \leq \frac{q(q-1)(N-1)}{2(N^2-1)} \leq \frac{q^2}{2N}. \tag{21}$$

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 $q^2/2N$.

Let $\mathsf{Func}_{\mathsf{good}} = \mathsf{Func} \setminus \mathsf{Func}_{\mathsf{bad}}$. So we have,

$$\begin{aligned}\Pr[\mathbf{F}(a^q, b^q) = (c^q, d^q)] &\geq \Pr[\boldsymbol{\psi}_1 \in \mathsf{Func}_{\mathsf{good}}] \times \Pr[\boldsymbol{\psi}_2(x^q) = b^q \oplus d^q, \boldsymbol{\psi}_3(d^q) = x^q \oplus c^q \mid \boldsymbol{\psi}_1] \\ &\geq (1 - \frac{q^2}{2N}) \times \frac{1}{N^{2q}} \\ &\geq (1 - \frac{q^2}{2N} - \frac{q^2}{N^2}) \times \frac{1}{(N^2)_q}\end{aligned}$$

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

$$\frac{\Pr[\mathbf{F}(a^q, b^q) = (c^q, d^q)]}{\Pr[\boldsymbol{\Pi}(a^q, b^q) = (c^q, d^q)]} \geq (1 - \frac{q^2}{2N} - \frac{q^2}{N^2}). \tag{22}$$

The result follows from Eq. 21 and Eq. 22 using standard H-technique. □

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 $q^2/2N$. For a good transcript the ratio can be similarly shown to be at least $1 - q^2/N^2$ 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 $\boldsymbol{\psi}_3$.

7.2 3-round TBC-based Luby-Rackoff

In [87], Coron et al. gave an alternative for 3-round Luby-Rackoff using tweakable block cipher, called $\mathsf{TLR3}$, 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 $\mathsf{TLR3}$ 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 $\mathsf{TLR3}$.

Proposition 7.1. *For $N = 2^n$ and $q < N/2$ we have*

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

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 7.2. Let $\mathbf{F}$ be the response system corresponding to $\mathsf{TLR3}$ and $\boldsymbol{\Pi}$ 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 $\mathsf{TLR3}$.

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

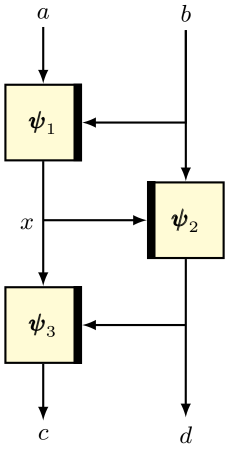

Fig. 7.2: The 3-round TPRP-based Luby-Rackoff or $\mathsf{TLR3}$ construction.

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 $\boldsymbol{\Pi}$, 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

$$\begin{aligned}\mathsf{Pr}[\bar{\tau}(\boldsymbol{\Pi}) \in \mathscr{V}_{\mathsf{bad}}] &= \sum_{i \in [q]} \left(\sum_{i < j \in [q]_e} \mathsf{Pr}[\mathsf{X}_i = \mathsf{X}_j, \mathsf{D}_i = \mathsf{D}_j] + \sum_{i < j \in [q]_d} \mathsf{Pr}[\mathsf{B}_i = \mathsf{B}_j, \mathsf{X}_i = \mathsf{X}_j] \right) \\ &\leq q(q-1) \times \frac{2^n - 1}{2^{2n} - j + 1} \times \frac{1}{2^n - q} \\ &\leq \frac{q(q-1)}{N(N-q)}. \qquad (23)\end{aligned}$$

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,

$$\begin{aligned}\mathsf{Pr}[\bar{\tau}(\mathbf{F})] &= \mathsf{Pr}[\boldsymbol{\psi}_1(b^q, a^q) = x^q] \times \mathsf{Pr}[\boldsymbol{\psi}_2(x^q, b^q) = d^q] \times \mathsf{Pr}[\boldsymbol{\psi}_3(d^q, x^q) = c^q] \\ &= \frac{1}{\prod_{i=1}^{u} (N)_{\alpha_i}} \times \frac{1}{\prod_{j=1}^{v} (N)_{\beta_j}} \times \frac{1}{\prod_{k=1}^{w} (N)_{\gamma_k}}.\end{aligned}$$

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

$$\begin{aligned}
\mathsf{Pr}[\bar{\tau}(\boldsymbol{\mathit{\Pi}})] &= \frac{1}{(N^2)_q} \times \frac{1}{\prod_{i' \in [q]_e}(N - r_{i'})} \times \frac{1}{\prod_{k' \in [q]_d}(N - s_{k'})} \\
&\leq \frac{1}{(1 - \frac{q^2}{N^2}) \times N^{2q}} \times \frac{1}{\prod_{i' \in [q]_e}(N - r_{i'})} \times \frac{1}{\prod_{k' \in [q]_d}(N - s_{k'})}.
\end{aligned}$$

Thus the ratio is

$$\frac{\mathsf{Pr}[\bar{\tau}(\mathbf{F})]}{\mathsf{Pr}[\bar{\tau}(\boldsymbol{\mathit{\Pi}})]} \geq \left(1 - \frac{q^2}{N^2}\right) \times \frac{N^{2q} \times \prod_{i' \in [q]_e}(N - r_{i'}) \times \prod_{k' \in [q]_d}(N - s_{k'})}{\prod_{i=1}^{u}(N)_{\alpha_i} \times \prod_{j=1}^{v}(N)_{\beta_j} \times \prod_{k=1}^{w}(N)_{\gamma_k}}. \tag{24}$$

In the above expression, we claim the following:

$$\begin{aligned}
\prod_{i=1}^{u}(N)_{\alpha_i} &= \prod_{i' \in [q]_e}(N - r_{i'}) \times \prod_{\hat{i} \in [q]_d}(N - \gamma_{\hat{i}}), \text{ and} \\
\prod_{k=1}^{w}(N)_{\gamma_k} &= \prod_{k' \in [q]_d}(N - s_{k'}) \times \prod_{\hat{k} \in [q]_e}(N - \gamma_{\hat{k}}),
\end{aligned}$$

where for all $\hat{i}$ and $\hat{j}$, $\gamma_{\hat{i}}, \gamma_{\hat{j}} \geq 0$. 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 $\phi(i') \rightarrow (i, p)$ 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. 24 we have

$$\begin{aligned}
\frac{\mathsf{Pr}[\bar{\tau}(\mathbf{F})]}{\mathsf{Pr}[\bar{\tau}(\boldsymbol{\mathit{\Pi}})]} &\geq \left(1 - \frac{q^2}{N^2}\right) \times \frac{N^{2q}}{\prod_{\hat{i} \in [q]_d}(N - \gamma_{\hat{i}}) \times \prod_{j=1}^{v}(N)_{\beta_j} \times \prod_{\hat{k} \in [q]_e}(N - \gamma_{\hat{k}})} \\
&\geq \left(1 - \frac{q^2}{N^2}\right) \times \frac{N^{2q}}{\prod_{\hat{i} \in [q]_d}(N - \gamma_{\hat{i}}) \times \prod_{\hat{k} \in [q]_e}(N - \gamma_{\hat{k}})} \\
&\geq \left(1 - \frac{q^2}{N^2}\right) \qquad (25)
\end{aligned}$$

The result follows from extended H-technique using Eq. 23 and Eq. 25.

8 SPRP Designs

More notations: For $\ell \geq 1$, $p \in \mathscr{M}^{\ell}$, $p[i]$ denotes the i-th $\mathscr{M}$-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 $\mathscr{M}$-substring of p consisting of consecutive $\mathscr{M}$-blocks $p[i], p[i+1], \ldots, p[j]$, for $1 \leq i < j \leq \ell$.

8.1 HCTR

Construction. HCTR is an encryption scheme by Wang, Feng and Fu [16], 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 $\mathsf{HCTR}(p) := c = c[1..\ell]$.
```

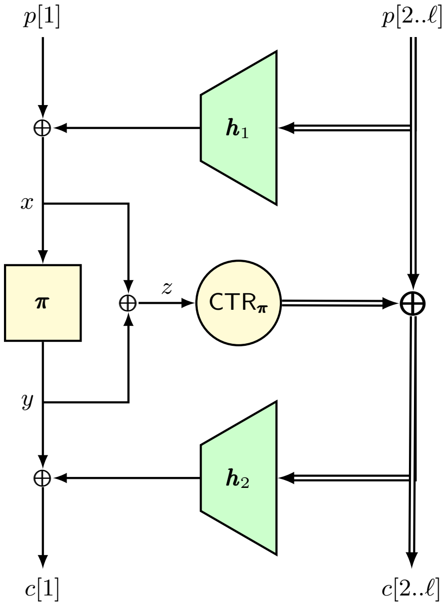

Fig. 8.1: A simplified view of the HCTR enciphering scheme. The double equal style paths denote a compressed view of $(\ell - 1)$ many parallel paths.

The original HCTR was defined to be a tweakable encryption scheme with a 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 8.1.

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

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:

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

Bound on Pr[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[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

$$\begin{aligned}\mathsf{Pr}[\mathbf{F}(p^q) = c^q, \mathsf{H}_1 = h_1, \mathsf{H}_2 = h_2] &= \frac{1}{|\mathscr{H}^2|} \times \frac{1}{(N)_\sigma} \\ &\geq \frac{1}{|\mathscr{H}^2|} \times \prod_{\ell=1}^{L} \frac{1}{(N^\ell)_{q_\ell}} \\ &\geq \Pr[\boldsymbol{\Pi}(p^q) = c^q, \mathsf{H}_1 = h_1, \mathsf{H}_2 = h_2]\end{aligned}$$

The result follows from extended H-technique. □

8.2 TET

Construction. TET is an encryption scheme by Halevi [14], based on the Hash-Encrypt-Hash paradigm [14,17,18], that uses a sandwich of ECB mode in between two blockwise universal and invertible hash functions.

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

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 independently off the two hashes. Then the composition $\mathbf{H}_2^{-1} \circ \mathsf{ECB}_{\boldsymbol{\pi}} \circ \mathbf{H}_1$ is called the TET construction.

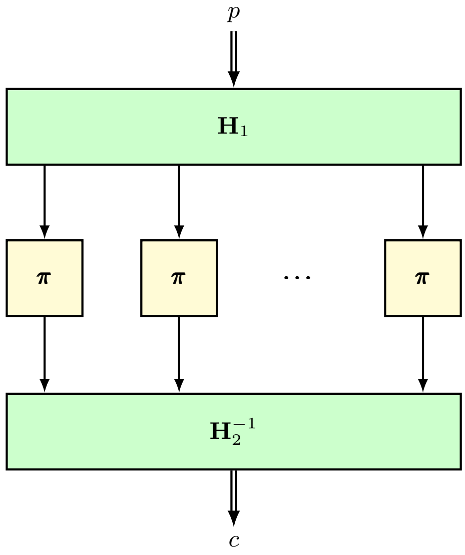

Fig. 8.2: A simplified view of the TET enciphering scheme.

Lemma 8.2.

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

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,

$$\begin{aligned}
\Pr[\mathbf{F}(p^q) = c^q] &\geq \sum_{x^q, y^q \in \mathbb{F}_{2^n}^{(\sigma)}} \Pr[\mathsf{H}_1(p^q) = x^q, \boldsymbol{\pi}(x^q) = y^q, \mathsf{H}_2^{-1}(y^q) = c^q] \\
&= \sum_{x^q, y^q \in \mathbb{F}_{2^n}^{(\sigma)}} \Pr[\mathsf{H}_1(p^q) = x^q, \mathsf{H}_2(c^q) = y^q] \times \Pr[\boldsymbol{\pi}(x^q) = y^q] \\
&= \Pr[\mathsf{H}_1(p^q) \in \mathbb{F}_{2^n}^{(\sigma)}, \mathsf{H}_2(c^q) \in \mathbb{F}_{2^n}^{(\sigma)}] \times \frac{1}{(N)_\sigma} \\
&\geq \left(1 - \binom{\sigma}{2}\epsilon - \binom{\sigma}{2}\epsilon\right) \times \Pr[\boldsymbol{\Pi}(p^q) = c^q] \qquad (26)
\end{aligned}$$

The result follows from substituting Eq. 26 in standard H-technique. □

References

1. Goldreich, O., Goldwasser, S., Micali, S.: 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. (1984) 464–479
2. Luby, M., Rackoff, C.: 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. (1985) 447
3. Bellare, M., Rogaway, P.: 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. (2006) 409–426
4. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive **2004** (2004) 332
5. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2) (1984) 270–299
6. Yao, A.C.: Theory and applications of trapdoor functions (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982. (1982) 80–91
7. Shoup, V.: 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. (2000) 275–288

8. Shoup, V.: OAEP reconsidered. J. Cryptology **15**(4) (2002) 223–249
9. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. **33**(1) (2003) 167–226
10. Camenisch, J., Shoup, V.: 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. (2003) 126–144
11. Abe, M., Gennaro, R., Kurosawa, K., Shoup, V.: 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. (2005) 128–146
12. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. (2003) 482–499
13. Halevi, S., Rogaway, P.: 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. (2004) 292–304
14. Halevi, S.: 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. (2007) 412–429
15. Chakraborty, D., Sarkar, P.: HCH: A new tweakable enciphering scheme using the hash-counter-hash approach. IEEE Trans. Information Theory **54**(4) (2008) 1683–1699
16. Wang, P., Feng, D., Wu, W.: HCTR: A variable-input-length enciphering mode. In: Information Security and Cryptology: First SKLOIS Conference, CISC 2005, Proceedings. (2005) 175–188
17. Sarkar, P.: Improving upon the TET mode of operation. In: Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings. (2007) 180–192
18. Sarkar, P.: Efficient tweakable enciphering schemes from (block-wise) universal hash functions. IEEE Trans. Information Theory **55**(10) (2009) 4749–4760
19. Ristenpart, T., Rogaway, P.: 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. (2007) 101–118
20. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. **61**(3) (2000) 362–399
21. Bellare, M., Pietrzak, K., Rogaway, P.: Improved Security Analyses for CBC MACs. In: Proc. CRYPTO 2005. (2005) 527–545
22. Black, J., Rogaway, P.: CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. J. Cryptol. **18** (2005) 111–131
23. Yasuda, K.: 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. (2010) 366–381
24. Yasuda, K.: 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. (2011) 596–609
25. Bellare, M., Boldyreva, A., Knudsen, L.R., Namprempre, C.: On-line ciphers and the hash-cbc constructions. J. Cryptology **25**(4) (2012) 640–679

26. Rogaway, P., Zhang, H.: 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. (2011) 237–249
27. Forler, C., List, E., Lucks, S., Wenzel, J.: 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.
28. Rogaway, P., Bellare, M., Black, J., Krovetz, T.: OCB: a block-cipher mode of operation for efficient authenticated encryption. In: CCS 2001, Proceedings. (2001) 196–205
29. Krovetz, T., Rogaway, P.: 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. (2011) 306–327
30. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I. (2013) 424–443
31. Abed, F., Fluhrer, S.R., Forler, C., List, E., Lucks, S., McGrew, D.A., Wenzel, J.: Pipelineable on-line encryption. In: Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers. (2014) 205–223
32. Patarin, J.: The "coefficients H“ technique. In: Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers. (2008) 328–345
33. Patarin, J.: Pseudorandom permutations based on the DES scheme. In: EUROCODE '90, International Symposium on Coding Theory and Applications, Udine, Italy, November 5-9, 1990, Proceedings. (1990) 193–204
34. Patarin, J.: Etude des Générateurs de Permutations Pseudo-aléatoires Basés sur le Schéma du DES. PhD thesis, Université de Paris (1991)
35. Patarin, J.: Improved security bounds for pseudorandom permutations. In: CCS '97, Proceedings of the 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 1-4, 1997. (1997) 142–150
36. Patarin, J.: About feistel schemes with six (or more) rounds. In: Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings. (1998) 103–121
37. Patarin, J.: Luby-rackoff: 7 rounds are enough for $2^{\mathrm{n(1\text{-}epsilon)}}$security. In: Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. (2003) 513–529
38. Vaudenay, S.: Decorrelation: A theory for block cipher security. J. Cryptology **16**(4) (2003) 249–286
39. Bernstein, D.J.: How to Stretch Random Functions: The Security of Protected Counter Sums. J. Cryptol. **12** (1999) 185–192
40. Nandi, M.: 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. (2006) 317–334
41. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Confer-

ence on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. (2014) 327–350

42. Patarin, J.: Security of random feistel schemes with 5 or more rounds. In: Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. (2004) 106–122
43. Nandi, M.: 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. (2010) 82–97
44. Nandi, M.: 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. (2008) 350–362
45. Lampe, R., Patarin, J., Seurin, Y.: 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. (2012) 278–295
46. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: 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. (2014) 39–56
47. Cogliati, B., Seurin, Y.: 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. (2015) 584–613
48. Cogliati, B., Lampe, R., Seurin, Y.: 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. (2015) 189–208
49. Cogliati, B., Seurin, Y.: 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. (2015) 134–158
50. Bhaumik, R., Nandi, M.: 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. (2015) 159–180
51. Bhaumik, R., Nandi, M.: Olef: an inverse-free online cipher. an online SPRP with an optimal inverse-free construction. IACR Trans. Symmetric Cryptol. **2016**(2) (2016) 30–51
52. Chen, Y.L., Luykx, A., Mennink, B., Preneel, B.: Efficient length doubling from tweakable block ciphers. IACR Trans. Symmetric Cryptol. **2017**(3) (2017) 253–270
53. Jha, A., Nandi, M.: Revisiting Structure Graphs: Applications to CBC-MAC and EMAC. J. Mathematical Cryptology **10**(3–4) (2016) 157–180
54. Cogliati, B., Seurin, Y.: 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. (2016) 121–149

55. Mennink, B., Neves, S.: 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. (2017) 556–583
56. Cogliati, B., Lee, J., Seurin, Y.: New constructions of macs from (tweakable) block ciphers. IACR Trans. Symmetric Cryptol. **2017**(2) (2017) 27–58
57. Datta, N., Dutta, A., Nandi, M., Paul, G., Zhang, L.: Single key variant of pmac_plus. IACR Trans. Symmetric Cryptol. **2017**(4) (2017) 268–305
58. Dutta, A., Jha, A., Nandi, M.: Tight security analysis of ehtm MAC. IACR Trans. Symmetric Cryptol. **2017**(3) (2017) 130–150
59. List, E., Nandi, M.: ZMAC+ - an efficient variable-output-length variant of ZMAC. IACR Trans. Symmetric Cryptol. **2017**(4) (2017) 306–325
60. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. IACR Cryptology ePrint Archive **2018** (2018) 500
61. Datta, N., Nandi, M.: 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. (2014) 306–321
62. Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M.: 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. (2017) 277–298
63. Bhaumik, R., Nandi, M.: 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. (2017) 638–666
64. Chakraborti, A., Datta, N., Nandi, M., Yasuda, K.: Beetle family of lightweight and secure authenticated encryption ciphers. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2018**(2) (2018) 218–241
65. Bose, P., Hoang, V.T., Tessaro, S.: 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. (2018) 468–499
66. Maurer, U.M.: 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. (2002) 110–132
67. Maurer, U.M., Pietrzak, K.: The security of many-round luby-rackoff pseudorandom permutations. In: Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings. (2003) 544–561
68. Maurer, U.M., Pietrzak, K.: 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. (2004) 410–427
69. Maurer, U.M., Pietrzak, K., Renner, R.: Indistinguishability amplification. In: Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings. (2007) 130–149

70. Minematsu, K., Matsushima, T.: New Bounds for PMAC, TMAC, and XCBC. In: Proc. Fast Software Encryption - FSE 2007. (2007) 434–451
71. Minematsu, K.: 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. (2009) 308–326
72. Minematsu, K., Iwata, T.: 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. (2011) 391–412
73. Minematsu, K.: Building blockcipher from small-block tweakable blockcipher. Des. Codes Cryptography **74**(3) (2015) 645–663
74. Minematsu, K., Iwata, T.: Tweak-length extension for tweakable blockciphers. In: Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings. (2015) 77–93
75. Hoang, V.T., Tessaro, S.: 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. (2016) 3–32
76. Hoang, V.T., Tessaro, S.: 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. (2017) 381–411
77. Guo, C., Wang, L.: Revisiting key-alternating feistel ciphers for shorter keys and multi-user security. IACR Cryptology ePrint Archive **2018** (2018) 816
78. Dai, W., Hoang, V.T., Tessaro, S.: 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. (2017) 497–523
79. Bhattacharya, S., Nandi, M.: A note on the chi-square method: A tool for proving cryptographic security. Cryptography and Communications **10**(5) (2018) 935–957
80. Bhattacharya, S., Nandi, M.: Revisiting variable output length XOR pseudorandom function. IACR Trans. Symmetric Cryptol. **2018**(1) (2018) 314–335
81. Bhattacharya, S., Nandi, M.: Full indifferentiable security of the xor of two or more random permutations using the \chi ˆ2 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. (2018) 387–412
82. Chen, Y.L., Mennink, B., Nandi, M.: Short variable length domain extenders with beyond birthday bound security. IACR Cryptology ePrint Archive **2018** (2018) 783
83. Steinberger, J.P.: Improved security bounds for key-alternating ciphers via hellinger distance. IACR Cryptology ePrint Archive **2012** (2012) 481
84. Bernstein, D.J.: A Short Proof of the Unpredictability of Cipher Block Chaining (2005)
85. Landecker, W., Shrimpton, T., Terashima, R.S.: 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. (2012) 14–30
86. Andreeva, E., Barwell, G., Bhaumik, R., Nandi, M., Page, D., Stam, M.: Turning online ciphers off. IACR Transactions on Symmetric Cryptology **2017**(2) (2017)

87. Coron, J., Dodis, Y., Mandal, A., Seurin, Y.: 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. (2010) 273–289
88. Gibbs, A.L., Su, F.E.: On choosing and bounding probability metrics. International Statistical Review **70**(3) (2002) 419–435
89. Goldwasser, S., Micali, S., Rackoff, C.: 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. (1985) 291–304
90. Cogliati, B., Patarin, J., Seurin, Y.: 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. (2014) 129–146
91. Wegman, M.N., Carter, L.: New classes and applications of hash functions. In: 20th Annual Symposium on Foundations of Computer Science, San Juan, Puerto Rico, 29-31 October 1979. (1979) 175–182
92. Shoup, V.: 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. (2000) 445–452
93. Berendschot, A., den Boer, B., Boly, J., Bosselaers, A., Brandt, J., Chaum, D., Damgård, I., Dichtl, M., Fumy, W., van der Ham, M., Jansen, C., Landrock, P., Preneel, B., Roelofsen, G., de Rooij, P., Vandewalle, J.: Final Report of Race Integrity Primitives. Volume 1007 of Lecture Notes in Computer Science, Springer-Verlag, 1995. Springer-Verlag (1995)
94. Luykx, A., Preneel, B., Tischhauser, E., Yasuda, K.: A MAC mode for lightweight block ciphers. In: Proc. Fast Software Encryption - FSE 2016. (2016) 43–59
95. Naor, M., Reingold, O.: 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. (1997) 189–199
96. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017)