Proof of Mirror Theory for a Wide Range of ξmax

Benoît Cogliati, Jacques Patarin, Avijit Dutta, Mridul Nandi, Abishanka Saha

Proof of Mirror Theory for a Wide Range of $\xi_{\max}$

Benoît Cogliati[1], Avijit Dutta[2], Mridul Nandi[2,3], Jacques Patarin[1,4], and Abishanka Saha[3]

[1] Thales DIS France SAS, Meudon, France
[2] Institute for Advancing Intelligence, TCG-CREST, Kolkata, India
[3] Indian Statistical Institute, Kolkata, India
[4] Laboratoire de Mathématiques de Versailles, UVSQ, CNRS, Université Paris-Saclay, Versailles, France
benoit.cogliati@gmail.com, avirocks.dutta13@gmail.com, mridul.nandi@gmail.com, jpatarin@club-internet.fr, sahaa.1993@gmail.com

Abstract. In CRYPTO'03, Patarin conjectured a lower bound on the number of distinct solutions $(P_1, \ldots, P_q) \in (\{0,1\}^n)^q$ satisfying a system of equations of the form $X_i \oplus X_j = \lambda_{i,j}$ such that $P_1, P_2, \ldots, P_q$ are pairwise distinct. This result is known as "$P_i \oplus P_j$ *Theorem for any* $\xi_{\max}$" or alternatively as *Mirror Theory for general* $\xi_{\max}$, which was later proved by Patarin in ICISC'05. Mirror theory for general $\xi_{\max}$ stands as a powerful tool to provide a high-security guarantee for many blockcipher-(or even ideal permutation-) based designs. Unfortunately, the proof of the result contains gaps that are non-trivial to fix. In this work, we present the first complete proof of the $P_i \oplus P_j$ theorem for a wide range of $\xi_{\max}$, typically up to order $O(2^{n/4}/\sqrt{n})$. Furthermore, our proof approach is made simpler by using a new type of equation, dubbed link-deletion equation, that roughly corresponds to half of the so-called orange equations from earlier works. As an illustration of our result, we also revisit the security proofs of two optimally secure blockcipher-based pseudorandom functions, and n-bit security proof for six round Feistel cipher, and provide updated security bounds.

Keywords: Mirror Theory · system of affine equations · PRP · PRF · beyond-birthday-bound security

1 Introduction

Pseudorandom Function (PRF) and Pseudorandom Permutation (PRP) are two fundamental cryptographic objects in symmetric key cryptography. Extensive use of pseudorandom functions in designing cryptographic schemes e.g., authentication protocols, encryption schemes, hash functions, etc. makes it a valuable object from the cryptographic perspective. However, practical candidates for PRF are very scarce. On the other hand, PRP or blockciphers are available in plenty in practice. One can consider a blockcipher to be a pseudorandom function, but due to the PRP-PRF switching lemma, it comes at the cost of birthday-bound security, i.e., if the block size of the blockcipher is n-bits, then one can

consider the blockcipher to be a secure PRF until the number of queries reaches $2^{n/2}$. Such a bound is acceptable when n is moderately large, e.g., 128 bits. However, due to the ongoing trend of lightweight cryptography, several lightweight blockciphers have been designed with smaller block size e.g., 64 bits. In such a situation, a blockcipher is not considered to be a good PRF as birthday-bound security is not adequate with 64 bit block size. Therefore, the natural question arises:

Can we design a pseudorandom function out of lightweight blockciphers that guarantees security beyond the birthday bound?

It turns out that over the past several years researchers have invested a lot of effort in designing such pseudorandom functions [3,20,22,10,19,45,46,47,34,14,13,23]. Out of several such designs, *xor of two pseudorandom permutations*, $\mathsf{XOR}_2(x) := \mathsf{E}_{k_1}(x) \oplus \mathsf{E}_{k_2}(x)$ [5], and its single-keyed variant $\mathsf{XOR}_1(x) := \mathsf{E}_k(0\|x) \oplus \mathsf{E}_k(1\|x)$, are the most popular ones. In a series of papers [39,40,42], Patarin claimed that XOR construction (i.e., both XOR_1 and XOR_2) is secure up to $O(2^n)$ queries. Following Patarin's analysis, XOR_2 construction yields the following system of bivariate affine equations:

$$\mathbb{E}_\lambda = \{P_1 \oplus P_2 = \lambda_1, P_3 \oplus P_4 = \lambda_2, \ldots, P_{2q-1} \oplus P_{2q} = \lambda_q\},$$

where $q \geq 1$ and $\lambda := (\lambda_1, \ldots, \lambda_q)$ is a tuple of n-bit binary strings (similarly the XOR_1 construction yields the same system of equations with the additional requirement that $\lambda_1, \ldots, \lambda_q$ are non-zero n-bit binary strings). The entire security analyses for both the constructions rely on finding a good lower bound on the number of solutions $(P_1, \ldots, P_{2q})$ [6] to $\mathbb{E}_\lambda$ where (i) for XOR_1 construction, we require that $P_i \neq P_j$ for $i \neq j$, while (ii) for XOR_2 construction, we require that $P_i \neq P_j$ for $i \neq j$, such that i, j are either both odd or both even. During the process of finding the solutions to $\mathbb{E}_\lambda$, assigning values to a variable P_i in $\mathbb{E}_\lambda$ fixes the value of exactly two variables (which are P_i and P_{i+1} if i is odd and P_{i-1}, P_i otherwise) in $\mathbb{E}_\lambda$. However, for a generic bivariate system of affine equations, assigning value to a single variable P_i can fix the values of $k \geq 2$ variables in the set of equations. Patarin [40] named this notion as *block maximality* in a system of bivariate affine equations, denoted as $\xi_{\max}$. It is natural to see that the block maximality of the system of equations $\mathbb{E}_\lambda$ is 2 and thus the security analysis of the XOR construction is reduced to establishing the following result.

"For a given system of bivariate affine equations over a finite group with non-equalities among the variables and $\xi_{\max} = 2$, the number of distinct solutions is always greater than the average number of solutions."

Patarin named this result as **Theorem** $P_i \oplus P_j$ **for** $\xi_{\max} = 2$ [37] (and later in [40], named *Mirror theory* the study of sets of linear equations and linear non-equations in finite groups). This result was stated as a conjecture in [35] and an

[5] Here, E_{k_1} and E_{k_2} denote two n-bit independent pseudorandom permutations

[6] Abusing the notation, we use the same symbol to denote the variables and the solution of a given system of equations.

incomplete and at times unverifiable proof is given in [37]. The result has been acknowledged in the community as a potentially strong approach to establish the optimal security of XOR constructions (i.e., XOR_1 and XOR_2). Beside this result, Patarin [37] also claimed that the number of distinct solutions to a system of q bivariate affine equations with $2 < \xi_{\max} \ll 2^{n/2}$ and with non-equality among the variables is always larger than the average number of solutions provided $q \ll 2^n$. Patarin named this result the **Theorem** $P_i \oplus P_j$ **for any** $\xi_{\max}$. This result was stated as a conjecture [35, Conjecture 8.1] in the context of analysing the security of the Feistel cipher. Only a couple of years later, this result was articulated in many follow-up works for analysing the security of the *xor of two permutations*, and it took a few articles [37,39,40,42] for his result and security argument to evolve. Later, in 2017, this work culminated in a book [32] called *Feistel Ciphers: Security Proofs and Cryptanalysis* by Nachef et al. Unfortunately, some important results were either hard to verify, or stated without proof, which has been reported in multiple works [7,11,15,25,29]. While this has led to some innovations such as the development of the aforementioned χ^2 technique, this state of affairs is unsatisfactory as Mirror Theory is an essential tool for provable security in symmetric cryptography.

1.1 Main Result and Our Contribution

In this paper, our goal is to give a complete and easily verifiable proof of the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$. From a high level, this amounts to lower-bounding the number of solutions of a system of equations of the form $P_i \oplus P_j = \lambda_{ij}$, such that the P_i variables are pairwise distinct.

This result has seen several applications in proving the optimal security bound for several blockcipher and tweakable blockcipher-based schemes such as optimally-secure PRFs, XORP [21,22] and 2k-HtmB-p2 [7] [See Sect. 4]. This result is also applied in the optimal security proof of the Feistel scheme [36,32,41]. The significance of the last application is due to the wide-ranged use of this scheme. Feistel scheme has been classically used to design many blockciphers (like DES [1], Lucifer [44] etc.), which has the prime advantage over the alternative, substitution permutation networks, of being invertible even if the round functions are not. The Feistel scheme has also been used in format preserving encryption, an important example being the Thorp shuffle [4], which is but an unbalanced Feistel cipher [43]. Along with giving a verifiable proof of the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$, we also provide updated security bounds for these three constructions using our main result, along with proof sketches, to illustrate the impact of the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$.

Notations. For integers $a \leq b$, the set $\{a, a+1, \cdots, b\}$ is denoted as $[a..b]$ (or simply $[b]$, when $a = 1$). We write $\mathsf{X} \leftarrow\!\!\$\, S$ to mean that X is sampled uniformly from S and independent of all random variables defined so far. Similarly, we write $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow\!\!\$\, S$ to mean that $\mathsf{X}_1, \ldots, \mathsf{X}_s$ are uniformly and independently distributed over S. We write X^q to denote a q-tuple $(X_1, \ldots, X_q)$. For $x \in S$, we write $S \setminus x$ to mean $S \setminus \{x\}$. We use $A \sqcup B$ to denote the disjoint union of A and

B (which implicitly means that A and B are disjoint). We consider the vector space $\{0,1\}^n$ over the field $\{0,1\}$, endowed with the two binary operations, $\oplus$ (i.e., addition modulo 2) and multiplication modulo 2. We denote by $N := 2^n$, the number of elements in $\{0,1\}^n$. For a positive integer $e \leq N$, we write $N^{\underline{e}} := N(N-1)\cdots(N-e+1)$.

A multiset γ is a collection of elements that can repeat. In other words, multiset is an unordered version of a tuple. For $S \in \gamma$, we write γ_{-S} to denote the multiset formed by removing S from γ. We similarly write γ_{+T} to denote the multiset formed by adding an element T to γ. For $S \in \gamma$, we also write γ_{-S+T} to denote the resulting multiset after deleting S and adding T to γ. We say that γ is a **set-system** if it is a multiset of sets. When we want to emphasize an ordering of the elements of γ, we also write the set-system as $\gamma^{[\alpha]} = (\gamma_1, \ldots, \gamma_\alpha)$, which is an enumeration of the sets in γ. In this paper, we consider set-systems γ of non-empty subsets of $\{0,1\}^n$.

System of Difference Equations. Consider a system of difference equations $AX = \Lambda$ over the vector space $\{0,1\}^n$, where $A = (A_{ij})_{i\in[m],j\in[p]}$ is a $m \times p$ matrix with full row rank (and hence consistent), such that each row contains exactly two 1's, and remaining zeros, X is a $p \times 1$ vector of variables and $\Lambda \in (\{0,1\}^n)^m$. As the column sum is zero, we must have $m < p$ [7]. Note that each equation in the above system is of the form $X_j \oplus X_k = \lambda_i$ for some i, j, k with $j \neq k$. A solution $X^p \in (\{0,1\}^n)^p$ of the above system is called a *pairwise distinct solution*, or in short a p.d. solution if $X_j \neq X_k$ for $j \neq k \in [p]$. The number of solutions of the system of equations is exactly N^{p-m} which can quite easily be shown by using elementary linear algebra. However, counting the number of p.d. solutions to this system of equations is quite involved. The main aim of this paper is to provide a good lower bound to the number of p.d. solutions.

Graph Theoretic Representation of the System. With every matrix A as described above in the system of difference equations, we can associate a labeled directed graph $G = (V := [p], E, L)$ where the edge set $E = \{(j,k) \in V^2 \mid \exists i \in [m]$ such that $A_{ij} = A_{ik} = 1\}$ and $L(j,k) = \lambda_i$ if $A_{ij} = A_{ik} = 1$. So, whenever there is an edge between j and k, we have directed edges in both directions. Thus, every connected component is strongly connected (there are edges in both directions between two connected vertices). The full row rank of A also implies that the graph G is acyclic and hence is a forest. If the graph G has q components then we must have $|E| = |V| - q$, or $m = p - q$. Given a directed path P from j to k, the equation $X_j \oplus X_k = \bigoplus_{e\in P} L(e)$ is a dependent equation (i.e., it can be obtained by adding a set of equations from the system). So, one can equivalently represent the system of difference equations $AX = \Lambda$ such that the corresponding graph has only star graphs as components. In other words, the

[7] This is because, the column sum is zero, which implies that the all-1 vector belongs to the kernel of the matrix, implying that it is non-invertible, and since it is already assumed to have full row rank, it cannot possibly have full column rank, hence $m = \mathrm{rank}(A) < p$.

system of equations corresponding to a component is of the form

$$X_{j_1} \oplus X_{j_\xi} = \lambda_{i_1}, \ldots, X_{j_{\xi-1}} \oplus X_{j_\xi} = \lambda_{i_{\xi-1}}.$$

We call such a system of difference equations *standard system of difference equations.*

Definition 1. *A system of difference equations $AX = \Lambda$ is called* p.d.-consistent *if $\lambda'_i \neq 0$ for all $i \in [m]$ and for all $i \neq i'$ in the same component, $\lambda'_i \neq \lambda'_{i'}$, where $A'X = \Lambda' := \lambda'^m$ is a standard form for the system.*

To have a p.d. solution, p.d.-consistency is a necessary condition. The following theorem provides a lower bound on the number of p.d. solutions for any p.d.-consistent system of difference equations.

Theorem 1 (Main Result). *Let G be the associated graph of a p.d.-consistent system $A_{m\times p}X = \Lambda$, of equations over $\{0,1\}^n$. Suppose the number of vertices in the largest component of G is $\xi_{\max}$. If $p \leq \sqrt{N}$ or $\sqrt{N} \geq \xi^2_{\max} \log_2 N + \xi_{\max}$, and $1 \leq p \leq N/12\xi^2_{\max}$, then the number of p.d. solutions of the system $AX = \Lambda$ is at least $(N)^{\underline{p}}/N^m$.*

Remark 1. Note that, in most cryptographic applications (where $N \geq 2^{64}$), $\xi_{\max}$ is either a small constant, or can be shown to be smaller than $\log_2 N$ with overwhelming probability. Typically, this is sufficient to prove that the cryptographic scheme is secure as long as the number q of adversarial queries is upper bounded by $N/12\xi^2_{\max}$, as $(\log_2 N)^3 \leq \sqrt{N}$ for $N \geq 2^{30}$.

1.2 Applications of Theorem $P_i \oplus P_j$ for any $\xi_{\max}$

Over the years, the Theorem $P_i \oplus P_j$ for any $\xi_{\max}$ has been proven to be a significant result in the context of analysing security bounds of numerous cryptographic designs. Apart from the stand-alone value of XOR_2 or XOR_1 constructions, they are used as a major component in many important blockcipher and tweakable blockcipher-based designs that includes [45,46,47,34,14,13,24,28,21,18,23,33,27]. However, the security proofs of most of these designs, done by application of the H-Coefficient technique [38], involve fixing the outputs, which in turn determines the inputs, thus getting rid of the adaptive nature of the adversary, and we cannot assume distinctness of these outputs of internal primitives because that would lead to the sub-optimal birthday-bound, rendering the $P_i \oplus P_j$ Theorem for $\xi_{\max} = 2$, useless for these security proofs. Instead, these security proofs require (by application of the H-Coefficient technique [38]) a good lower bound on the number of distinct solutions to a system of bivariate affine equations with a general $\xi_{\max}$ and therein comes the role of the result "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$". It has also been used in proving the beyond-birthday-bound security of many nonce-based MACs including [15,16,18,31,5]. Mennink [30] showed the optimal security bound of EWCDM using this result as the primary underlying tool, and Iwata

et al. [22] also used it to show the optimal security bound of CENC. Despite the debate in the community regarding the correctness of the proof of "Theorem $P_i \oplus P_j$ for any $\xi_{\max}$" [37,40], several authors have used this result to derive an optimal bound for some constructions such as [22,30,48]. This triggers the need for a correct and verifiable proof of these two results, which will eventually help to correctly establish the security proof of the above constructions and improve their security.

1.3 Related Work

Beside the applicability of the Theorem $P_i \oplus P_j$ for general $\xi_{\max}$, the more restricted result of "*Theorem* $P_i \oplus P_j$ *for* $\xi_{\max} = 2$" has already been linked to different cryptographic constructions. In particular, equations of the form $P_{2i-1} \oplus P_{2i} = \lambda_i$, which correspond to a simple variant of the systems we consider in this work, have been considered to prove the security of the XORP[2] construction [37,40,32,17,9]. In [42], [8] and [17], systems of the form $\oplus_{j=1}^{k} P_{i,j} = \lambda_i$, where the values $(P_{i,j})_i$ have to be pairwise distinct for $j = 1, \ldots, k$, have been studied to prove the security of the sum of permutations. Recently, a similar problem in the tweakable setting has been examined in [25], with an application to the security of the CLRW2 construction [8]. Mirror Theory has also been considered for nonce-based MACs that rely on an underlying blockcipher or tweakable blockciphers, such as in [15,16,18,31,26]. In that case, constraints also include inequalities of the form $P_i \oplus P_j \neq \lambda_{i,j}$, which also have to be taken into account. Despite the extensive use of the result, its correctness was subject to debate [11]. In [26], Kim et al. have given a verifiable proof of the mirror theory when the number of equations is below the bound $2^{3n/4}$. Datta et al. [12] have extended this result for a system of bivariate affine equations and non-equations. Recently, Dutta et al. [17] and Cogliati and Patarin [9] have independently given a verifiable proof of the "$P_i \oplus P_j$ theorem" for $\xi_{\max} = 2$.

Organization. In Sect. 2, we prove an equivalent formulation of our main result through a probability of an event involving disjointness of some random sets, modulo a Proposition, proof of which is postponed to Sect. 3. We give an overview of our proof strategy and a brief comparison with previous proofs in Sect. 3.2. The proof of the Proposition requires a recursive inequality lemma, proof of which is deferred in Sect. A.2. Then, Sect. 4 briefly revisits several proofs that rely on the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$, and provides the corresponding updated security bounds. Finally, we outline possible extensions of our work in Sect. 5.

[8] CLRW2 or cascading LRW2 is a tweakable blockcipher, defined as $\mathsf{CLRW2}((k_1, k_2, h_1, h_2), t, m) = \mathsf{LRW2}((k_2, h_2), t, \mathsf{LRW2}((k_1, h_1), t, m))$, with $\mathsf{LRW2}((k, h), t, m) = E(k, m \oplus h(t)) \oplus h(t)$, where E is a block cipher, k is the block cipher key, and h is an XOR universal hash function

2 Probability of Disjointness: An Equivalent Formulation

In order to streamline the proof of Theorem 1, we will operate two distinct changes. First, note that, in order to have solutions, the system has to be p.d. consistent, which corresponds to two distinct conditions: $\lambda'_i \neq 0$ for all $i \in [m]$, and for all $i \neq i'$ in the same component, $\lambda'_i \neq \lambda'_{i'}$. While easy to manipulate, both conditions have to be handled in a different way, which complicates the proof. The simplest fix is to introduce, for every component, an additional λ' value that can be thought to be 0^n. Second, in order to avoid powers of N in our formulas, we prefer switching to a probabilistic formulation where, for every component, we simply sample uniformly at random a value in $\{0,1\}^n$, and consider a disjointness event that is derived from the system of equalities.

More formally, given a set-system $\gamma = \{\gamma_i : i \in [\alpha]\}$, we define the following event:

$$\mathsf{Disj}(\gamma) := \gamma_1 \oplus \mathsf{R}_1, \ldots, \gamma_\alpha \oplus \mathsf{R}_\alpha \text{ are disjoint } [9]$$

along with the following probability:

$$\mathsf{P}(\gamma) = \Pr_{\mathsf{R}^\alpha}(\mathsf{Disj}(\gamma)),$$

where $\mathsf{R}_1, \ldots, \mathsf{R}_\alpha \leftarrow\!\!\$\, \{0,1\}^n$. In words, the event says that a random and independent translation of sets from a collection are disjoint. We write $\|\gamma\| := \sum_{i=1}^{\alpha} |\gamma_i|$ and $\|\gamma\|_{\max} = \max_i |\gamma_i|$. It is easy to see that the probability of disjointness is invariant under any translation of the sets, i.e., $\mathsf{P}(\gamma) = \mathsf{P}(\gamma')$ where $\gamma'_i = \gamma_i \oplus a_i$ for $a_1, \ldots, a_\alpha \in \{0,1\}^n$.

Theorem 1 can be rephrased in the following way.

Theorem 1' (Equivalent Formulation) *Let γ be a set-system of elements of $\{0,1\}^n$ such that $\xi_{\max} = \|\gamma\|_{\max}$. If $\|\gamma\| \leq \sqrt{N}$ or $\sqrt{N} \geq \xi_{\max}^2 \log_2 N + \xi_{\max}$, and $1 \leq \|\gamma\| \leq N/12\xi_{\max}^2$, then*

$$\mathsf{P}(\gamma) \geq \frac{(N)^{\underline{\|\gamma\|}}}{N^{\|\gamma\|}}.$$

The equivalence between both statements is proven in Sect. 2.1. From a high level, the proof of Theorem 1' works in two steps:

1. if γ is small ($\|\gamma\| \leq \sqrt{N}$), then simple calculations show that Theorem 1' holds;
2. otherwise, we prove that, for a well-chosen $a \in T \in \gamma$, one has

$$\mathsf{P}(\gamma) \geq \left(1 - \frac{\|\gamma\| - 1}{N}\right) \mathsf{P}(\gamma'),$$

where γ' is a set system containing exactly the same sets as γ, except that the set T has been replaced with $T \setminus \{a\}$; clearly, applying point 2 repeatedly until $\|\gamma\| \leq \sqrt{N}$ allows us to conclude the proof of Theorem 1'.

[9] For a set $A \subseteq \{0,1\}^n$ and a n-bit number $x \in \{0,1\}^n$, $x \oplus A := \{x \oplus a \mid a \in A\}$

Intuitively, the element that we remove from γ is the one that appears, in the associated system of equations, with maximum multiplicity.

More formally, given $z \in \{0,1\}^n \setminus \{0^n\}$, and a set S, we define $\delta_S(z)$ as the number of 2-subsets $\{a,b\}$ of S with $a \oplus b = z$. For a set-system γ, we define

$$\delta_\gamma(z) := \sum_{S \in \gamma} \delta_S(z), \quad \Delta_\gamma := \max_{z \in \{0,1\}^n} \delta_\gamma(z).$$

Clearly, for any set-system γ, $\Delta_\gamma \geq 1$. The underlying statement behind the second point of our proof strategy is the following one.

Proposition 1. *Let λ be a set-system with $\sqrt{N} \leq \|\lambda\| \leq N/12\xi_{\max}^2$ where $\xi_{\max} = \|\lambda\|_{\max}$ satisfies the bound given in Theorem 1', i.e., $\sqrt{N} \geq \xi_{\max}^2 \log_2 N + \xi_{\max}$. Suppose the maximum Δ_λ is attained for $a \oplus b$ with $\{a,b\} \subseteq T \in \lambda$. Then,*

$$\mathsf{P}(\lambda) \geq \left(1 - \frac{\|\lambda\| - 1}{N}\right) \cdot \mathsf{P}(\lambda_{-a|T})$$

where $\lambda_{-a|T} = \lambda_{-T+T\setminus a}$ (i.e. replacing the element T by $T \setminus a$).

The proof of Proposition 1 is given in Section 3, and we explain how to derive Theorem 1' from Proposition 1 in Section 2.2.

2.1 Proof of Equivalence

Here we prove why Theorem 1' is an equivalent statement of our main theorem. First, we establish a one-to-one relationship between the number of disjoint favorable solutions r^q with the number of p.d. solutions of systems of equations.

Let $AX = \Lambda$ be a system of difference equations in standard form, and G be its associated graph. For every component C, let L_C be the set of all labels. By definition of p.d.-consistency, all elements of L_C are distinct (and hence it is a set of size $\xi_C - 1$, where ξ_C is the number of vertices in C) nonzero elements. Let i_C denote the center of the star component. Thus, for all other $j \in C$, we have an equation of the form $X_j \oplus X_{i_C} = \lambda_k$ for some k. Now we consider a set-system γ containing all sets of the form $S_C := L_C \cup \{0\}$. Thus, $\|\gamma\| = \sum_C |C| = e$ and $|\gamma| = q$. Let $C_1, \ldots, C_q$, denote the components (written in some order) and let $i_j := i_{C_j}$. Now consider a map f, mapping a p.d. solution x^e of the system to r^q, where $r_j = x_{i_j}$ for all $j \in [q]$. It is easy to see that $S_{C_j} \oplus r_j$ are disjoint sets (as these represent all x values). Moreover, f is clearly injective as a solution is uniquely determined by the tuple $(x_{i_1}, \ldots, x_{i_q})$. So, f is an injective function. Conversely, for any r^q with disjoint $S_{C_j} \oplus r_j$'s, we can define x^e consisting of all values from the set $\sqcup_j (S_{C_j} \oplus r_j)$ in an appropriate order (with $x_{i_j} = r_j$). Clearly, this map is f^{-1} and so f is a bijective function. Hence, the number of p.d. solutions for $AX = \Lambda$ is same as the number of solutions of r^q so that $\mathsf{Disj}(\gamma)$ holds. Second, we note that Theorem 1' can be simply restated as the number of solutions $r^{|\gamma|}$ so that $(\gamma_i \oplus r_i)$'s are disjoint for all $i \in [q]$ is at least

$$\frac{(N)^{\underline{\|\gamma\|}}}{N^{\|\gamma\| - |\gamma|}} = \frac{(N)^{\underline{e}}}{N^{e-q}},$$

where $p - q = m$ corresponds to the number of equations in the system $AX = \Lambda$. This proves the equivalence between our main theorem and the equivalent formulation.

2.2 Proof of Theorem 1'

We first prove the statement when $\|\gamma\| \leq \sqrt{N}$. In this case we remove elements from γ one by one until we end up with a single element. We first note that

$$\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-S}) \times \left(1 - \frac{\|\gamma\| - 1}{N}\right) \qquad \textit{if } |S| = 1 \tag{1}$$

$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma_{-S}) \times \left(1 - \frac{|S| \times \|\gamma_{-S}\|}{N}\right) \qquad \textit{if } |S| \geq 2 \tag{2}$$

where $S \in \gamma$. The above relations are easy to verify (by looking at the restriction imposed on R which translates the set S). Indeed, let us assume $S = \gamma_1$. Then, using the independence of the $(\mathsf{R}_i)_{i=1,\ldots,|\gamma|}$ random variables, once $\mathsf{R}_2, \ldots, \mathsf{R}_{|\gamma|}$ are chosen such that the equations from $\mathsf{Disj}(\gamma_{-S})$ are satisfied, $\mathsf{Disj}(\gamma)$ adds the following restrictions on R_1:

$$\mathsf{R}_1 \oplus x \neq \mathsf{R}_i \oplus y \text{ for all } x \in S,\ i \neq 1,\ y \in \gamma_i.$$

Hence, if $|S| = 1$, R_1 has to be different from exactly $\|\gamma\| - 1$ values, while, if $|S| \neq 1$, it has to avoid at most $|S| \times \|\gamma_{-S}\|$ group elements.

Let us write $W_i := (1 - \frac{i}{N})$, so that $\prod_{i=1}^{k-1} W_i = (N)^{\underline{k}}/N^k$. Now we claim that, for $\|\gamma\| \leq \sqrt{N}$,

$$\left(1 - \frac{|S| \times \|\gamma_{-S}\|}{N}\right) \geq \prod_{i=\|\gamma_{-S}\|}^{\|\gamma\|-1} W_i \tag{3}$$

and hence $\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma_{-S}) \times \prod_{i=\|\gamma_{-S}\|}^{\|\gamma\|-1} W_i$. After repeatedly removing an element one by one, we have $\mathsf{P}(\gamma) \geq \prod_{i=1}^{\|\gamma\|-1} W_i$ which proves the theorem. Now we prove Eq. (3). It is sufficient to show that

$$1 - \frac{ar}{N} \geq \left(1 - \frac{a}{N}\right) \cdots \left(1 - \frac{a+r-1}{N}\right)$$

where $a + r \leq \sqrt{N}$. This can be easily shown by induction on r. For $r = 1$, it is obvious. Now by applying induction hypothesis for r, we obtain

$$\begin{aligned}\left(1 - \frac{a}{N}\right) \cdots \left(1 - \frac{a+r-1}{N}\right)\left(1 - \frac{a+r}{N}\right) &\leq \left(1 - \frac{ar}{N}\right)\left(1 - \frac{a+r}{N}\right) \\ &\leq 1 - \frac{ar+a}{N} - \frac{r}{N}\left(1 - \frac{a(a+r)}{N}\right) \leq 1 - \frac{ar+a}{N}.\end{aligned}$$

For the last inequality we use the fact that $a + r + 1 \leq \sqrt{N}$.

For the next case, we assume that $\sqrt{N} \leq \|\gamma\| \leq N/12\xi_{\max}^2$, i.e. $\|\lambda\|$ is within the required bounds for which Proposition 1 holds. We can create a sequence of nested set-systems $\{\gamma^{(i)}\}_{i=0}^{\sigma}$, with

$$\gamma^{(0)} := \gamma, \quad \|\gamma^{(i+1)}\| = \|\gamma^{(i)}\| - 1, \ \forall i \in [\sigma - 1], \quad \|\gamma^{(\sigma)}\| \leq \sqrt{N},$$

in the following manner: Let $\{x_i, y_i\} \subseteq S_i \in \gamma^{(i)}$ such that $x_i \oplus y_i$ attains the highest multiplicity in $\gamma^{(i)}$, $\Delta_{\gamma^{(i)}}$. We choose one arbitrarily if there exists more than one choice. We define $\gamma^{(i+1)} := \gamma^{(i)}_{-x_i|S_i}$. Now for every $i \in [\sigma-1]$, if $|S_i| = 1$ we apply Eq. (1), and if $|S_i| \geq 2$, we apply Proposition 1, to obtain

$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma^{(\sigma)}) \prod_{i=1}^{\sigma} \left(1 - \frac{\|\gamma\| - i}{N}\right).$$

We already have shown the result for $\gamma^{(\sigma)}$ that $\mathsf{P}(\gamma^{(\sigma)}) \geq (N)_{\|\gamma^{(\sigma)}\|}/N^{\|\gamma^{(\sigma)}\|}$, which completes the proof.

3 Proof of Proposition 1

Notations and Conventions. In the Proposition statement, $\{a, b\} \subseteq T \in \lambda$ and $\Delta_\lambda = \sum_{S \in \lambda} \delta_S(a \oplus b)$. Let $\lambda = \{\lambda_i : i \in [q]\}$ and we write $|\lambda_i| = \xi_i, \xi_{\max} = \max_i \xi_i$ and $\sigma := \sum_i \xi_i$. We also write Δ to denote Δ_λ. Throughout the section we follow this notation. Moreover, we use the notation γ to denote a set-system such that $\gamma \subseteq \lambda$ (as a multiset).

3.1 Initial Condition

Note that, after applying Eq. (2) repeatedly (or by applying induction on $|\lambda \setminus \gamma|$) for $\gamma \subseteq \lambda$, we have

$$\frac{\mathsf{P}(\lambda)}{\mathsf{P}(\gamma)} \geq \left(1 - \frac{q\xi_{\max}^2}{N}\right)^{|\lambda \setminus \gamma|}. \tag{4}$$

We call this an initial condition that would be used later to prove Proposition 1.

3.2 Link-deletion Equation and Proof Overview

Link-deletion Equation. Let $x \in S \in \gamma \subseteq \lambda$. Let us write

$$\gamma = \{\gamma_1, \ldots, \gamma_\alpha\}$$

using an arbitrary ordering of the multiset γ, and let us assume $S = \gamma_1$ and $x = \gamma_{1,1}$. Then, the event $\mathsf{Disj}(\gamma)$ corresponds to the fact that all the $\mathsf{R}_i \oplus \gamma_{i,j}$ values are pairwise distinct, and the event $\mathsf{Disj}(\gamma_{-x|S})$ corresponds to the same

event, where the conditions involving $\mathsf{R}_1 \oplus \gamma_{1,1}$ are ignored. Hence, one has $\mathsf{Disj}(\gamma) \Rightarrow \mathsf{Disj}(\gamma_{-x|S})$. Suppose $\mathsf{Disj}(\gamma_{-x|S}) \wedge \neg\mathsf{Disj}(\gamma)$ holds. Then, there must exist $y \in S' \in \gamma_{-\gamma_1}$ such that $S' = \gamma_i$ for some integer $i \neq 1$, and $y \oplus \mathsf{R}_i = x \oplus \mathsf{R}_1$. As $(S \setminus x) \oplus \mathsf{R}_1$ is disjoint from $S' \oplus \mathsf{R}_i$ (same as $S' \oplus (x \oplus y \oplus \mathsf{R}_1)$), $S \setminus x$ should be disjoint from $S' \oplus x \oplus y$. Let

$$I := \{(x \oplus y, S') : y \in S' \in \gamma_{-S}, \quad S' \oplus (x \oplus y) \text{ is disjoint with } S \setminus x\}.$$

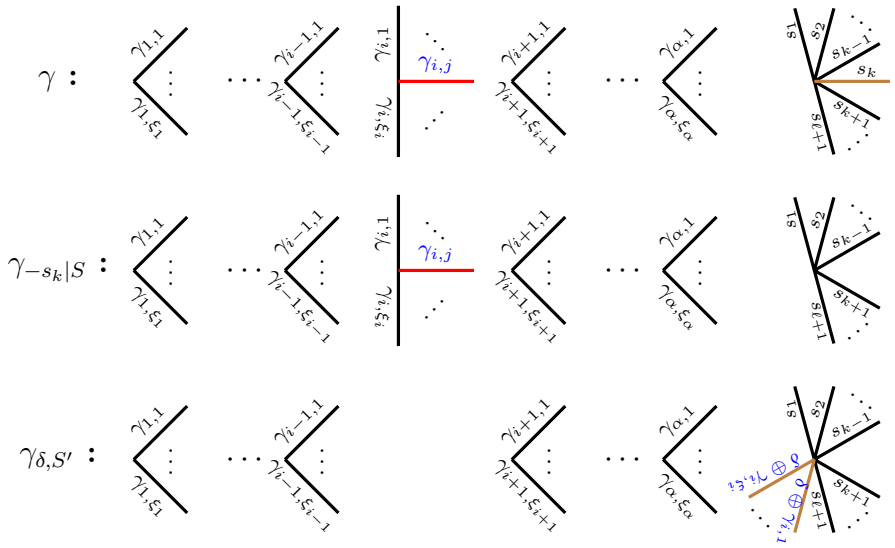

Fig. 3.1: Graphical depiction of the link-deletion operation. Here, we have represented graphs corresponding to the three types of terms appearing in the link-deletion equation, with $x = s_k$, $y = \gamma_{i,j}$, $\delta = s_k \oplus \gamma_{i,j}$, $S = \{s_1, \ldots, s_{\ell+1}\}$, and $S' = \gamma_i$. Central vertices correspond to the $\mathsf{R}_1, \ldots, \mathsf{R}_\alpha, \mathsf{R}$ random variables.

Note that simultaneously $\mathsf{R}_1 \oplus x = \mathsf{R}_i \oplus y = \mathsf{R}_j \oplus y'$ for some $y' \in \gamma_j \in \gamma_{-S}$ cannot hold. Since otherwise, the disjointness of $\gamma_{-x|S}$ cannot hold. Thus, we have established a useful relation, called **link-deletion equation**.

$$\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-x|S}) - \frac{1}{N} \sum_{(\delta,S') \in I} \mathsf{P}(\gamma_{\delta,S'}) \tag{5}$$

where $\gamma_{\delta,S'} = \gamma_{-S-S'+S_1}$ and $S_1 = (\delta \oplus S') \sqcup (S \setminus x)$. This is because, the probability $P(\gamma_{-x|S})$ can be divided in two disjoint events:

– either adding x as a link to the set S does not create any collision (this happens with probability $\mathsf{P}(\gamma)$), or

– a collision is created; all those collision events are disjoint, and correspond to a unique element from the set I. For every $(\delta, S') \in I$, the probability that such a collision occurs (while keeping all the other disjointness conditions), is exactly $\mathsf{P}(\gamma_{\delta,S'})/N$, as this event corresponds to the event, $\mathsf{Disj}(\gamma_{\delta,S'}) \wedge (R_1 = R_i \oplus \delta)$, where the sub-event $R_1 = R_i \oplus \delta$ occurs with probability $1/N$ independently of $\mathsf{Disj}(\gamma_{\delta,S'})$ (because $\gamma_{\delta,S'}$ does not involve S' and hence R_i).

Proof Strategy. In order to prove Proposition 1, we will prove that $|\mathsf{P}(\gamma_{\delta,S'}) - \mathsf{P}(\gamma_{-x|S})|$ is small enough in front of $\mathsf{P}(\gamma_{-x|S})$, for all $(\delta, S') \in I$. This will be done in the following steps.

1. Upper bound the size of the set I (in Section 3.3).
2. Establish a recursive inequality between the maximum difference between terms of the form $\mathsf{P}(\gamma'_{-x|S})$, and terms of the form $\mathsf{P}(\gamma'_{\delta,S'})$, with $\gamma'_{-S} \subset \lambda$, and S an arbitrary set of some fixed size (in Section A.2). This will be done by applying the link-deletion equation to the two probabilities that maximize the difference term, thus introducing new difference terms and an error term.
3. After applying this inequality a logarithmic number of times along with simple bounds on the probability ratios, prove that remaining terms become sufficiently small thanks to the geometric reduction offered by the recursive inequality (Sections 3.5 and A.2).

Comparison with Previous Proofs. The main difference with previous proof strategies is centered around the link-deletion equation. Indeed, previous works started with the introduction of the so-called orange equation, which can be seen as two consecutive applications of the link-deletion equations. Hence, instead of always merging a single set $S' \in \gamma$ with the final set S, this could be seen as merging two distinct sets $S', S'' \in \gamma$, which leads to a more complicated analysis.

3.3 Size Lemma

We also write the above set I as $I_{x|S}$ to emphasize that I depends on x, S. Clearly, for all $x \in S \in \gamma$, $|I| \leq \|\gamma\|$. However, we establish an improved upper bound for the size of $I_{a|T}$ where a and T are described in the statement of the Proposition.

Lemma 1 (size lemma). *For a given $a \in T \in \lambda$ as described in the Proposition statement, we have $|I_{a|T}| \leq \|\lambda\| - \Delta - |T|/2$.*

Proof. Take any $S \in \lambda_{-T}$. Note that there are $\delta_S(a \oplus b)$ many 2-sets $\{w_1, w_2\} \subseteq S$ such that $w_1 \oplus w_2 = a \oplus b$ and hence $b = w_2 \oplus (a \oplus w_1) \in S \oplus (a \oplus w_1)$. So, $(a \oplus w_1, S) \notin I_{a|T}$. So,

$$|I_{a|T}| \leq \sum_{S \in \lambda \setminus T} (|S| - \delta_S(a \oplus b)) = (\|\lambda\| - |T|) - \Delta_\lambda + \delta_T(a \oplus b) \leq \|\lambda\| - \Delta_\lambda - |T|/2,$$

as $\delta_T(a \oplus b) \leq |T|/2$. Indeed, for every element, $x \in T$, there exists at most one element y in T such that $x \oplus y = a \oplus b$. In the case where it exists, then neither x nor y can be part of a different 2-set. □

3.4 Recursive Inequality of D-Terms

In this section, we introduce D-terms, which correspond to the maximum difference between the two types of terms that can appear in the link-deletion equation. Formally, one has the following definition.

Definition 2. *$\tau = \gamma_{+U}$ with $\gamma \subseteq \lambda$ where $|\gamma| = \alpha$ and $|U| = \ell + 1$. For any $S \in \gamma$ disjoint with U, let $\tau' := \gamma_{-S+(S \sqcup U)}$ (same as $\tau_{-S-U+S \sqcup U}$, i.e., we merge two disjoint elements of τ). We define*

$$D(\alpha, \ell) = \max_{\gamma, U, S} \left| \mathsf{P}(\tau) - \mathsf{P}(\tau') \right|, \tag{6}$$

where the maximum is taken over all choices of $\gamma \subseteq \lambda$ of size α, $S \in \gamma$ and a set U of size $\ell + 1$ disjoint with S. For all $\ell < 0$, we define $D(\alpha, \ell) = 0$.

Now we state and prove the Recursive Inequality for D-terms:

Lemma 2 (Recursive Inequality of D-Terms). *Let $\alpha \leq q \leq \frac{N}{12\xi_{\max}^2}$, $\ell \geq 0$. We write $\beta := \xi_{\max}/N$. Then,*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \frac{\xi_{\max}}{N} \sum_{i=1}^{q} D(\alpha - 1, \ell + \xi_i - 1) + \frac{2\Delta\xi_{\max} \cdot \mathsf{P}(\lambda)}{N\left(1 - q\xi_{\max}^2/N\right)^{q-\alpha}}. \tag{7}$$

Note, for $q \leq \|\lambda\| \leq N/12\xi_{\max}^2$, $\frac{\xi_{\max}}{N(1-q\xi_{\max}^2/N)} \leq (4\xi eq)^{-1}$. Denoting $\beta := \xi_{\max}/N$, and $a_{d,\ell} = \frac{\beta^d}{2\mathsf{P}(\lambda)} D(q-d, \ell)$ we have,

$$a_{d,\ell} \leq a_{d,\ell-1} + \sum_{i=1}^{q} a_{d+1,\ell+\ell_i} + \beta\Delta \left(4e\xi_{\max} q\right)^{-d},$$

where $\ell_i = \xi_i - 1$.

The proof of this Lemma is postponed to Appendix A.1.

Remark 2. Note that the r.h.s. of the inequality contains three types of terms:

- $D(\alpha, \ell - 1)$ which will disappear after $\ell - 1$ applications of the recursive inequality,
- terms of the form $D(\alpha - 1, \ell + \xi_i - 1)$ which involve a smaller set-system, but a larger U set; however, those terms are multiplied by $\frac{\xi_{\max}}{N}$, which will ensure their geometric reduction,
- a parasite term that, as we will see, is small enough not to cause an issue after a logarithmic number of iterations.

Besides, in addition to the above recursive inequality, we also have the following bound, which follows from Eq. (4):

$$D(\alpha, \ell) = |\mathsf{P}(\tau) - \mathsf{P}(\tau')| \leq \frac{2\mathsf{P}(\lambda)}{(1 - q \cdot \|\lambda\|_{\max}^2/N)^{|\lambda \setminus \gamma|}}$$

and so

$$a_{d,\ell} = \frac{\beta^d}{2\mathsf{P}(\lambda)} D(q-d, \ell) \leq \left(\frac{\xi_{\max}}{N\,(1 - q\xi_{\max}^2/N)} \right)^d \leq 1/(4e\xi_{\max} q)^d$$

3.5 Final Wrap up of Proof

We can conclude the proof of Proposition 1 using Lemmas 1, 2, along with the following result that will be proven in Appendix A.2.

Lemma 3 (Recursive Inequality Lemma). *Suppose $a_{d,\ell} \geq 0$ such that: (i) $a_{d,k} := 0$ for all $k < 0$, and (ii) for all $0 \leq d \leq \xi n$ and $0 \leq \ell_i \leq \xi - 1$ for $i \in [q]$, we have*

$$a_{d,\ell} \leq (4\xi eq)^{-d} \qquad \text{(initial bound)} \tag{8}$$

$$a_{d,\ell} \leq a_{d,\ell-1} + \sum_{i=1}^{q} a_{d+1,\ell+\ell_i} + C \cdot (4\xi eq)^{-d} \qquad \text{(recursive inequality)} \tag{9}$$

for some $C > 0$. Then, for every $\ell \in [\xi - 2]$,

$$a_{0,\ell} \leq \frac{4}{N} + 4C\xi.$$

Let a, b, T, λ be as in the statement of Proposition 1, and let $\lambda_0 = \lambda_{-T}$. Note that one has $\xi_{\max}^2 n \leq \sqrt{N} - \xi_{\max} \leq \|\lambda_0\| \leq N/12\xi_{\max}^2$. Moreover, let $q = |\lambda_0|$. Similarly, one has $\xi_{\max} q \geq \|\lambda_0\| \geq \xi_{\max}^2 n$, which means that $q \geq \xi_{\max} n$. We are going to apply Lemma 3 to λ_0 as follows.

Let us take, $\xi = \xi_{\max}$, $C = \beta\Delta = \Delta_\lambda \xi_{\max}/N$ in the statement of the above Lemma 3. From the definition of $a_{d,\ell} = \frac{\beta^d}{2\mathsf{P}(\lambda_0)} D(q-d, \ell)$, we must ensure that $q \geq d$ in order to apply Lemma 3. This can easily be seen to be true as $q \geq \xi n$ and $d \leq \xi n$. Then, for $(\delta, S) \in I_{a|T}$, we have

$$|\mathsf{P}(\lambda_{\delta,S}) - \mathsf{P}(\lambda_{-a|T})| \leq D(q, |T| - 2) \leq 2\mathsf{P}(\lambda_0) a_{0,|T|-2} \leq \frac{8\mathsf{P}(\lambda_0)}{N}(\Delta\xi_{\max}^2 + 1).$$

Note that one has

$$\mathsf{P}(\lambda_{-a|T}) \geq \mathsf{P}(\lambda_0)\left(1 - \frac{\|\lambda_0\|\xi_{\max}}{N}\right) \geq \mathsf{P}(\lambda_0)\left(1 - \frac{1}{12\xi_{\max}}\right) \geq \mathsf{P}(\lambda_0)\frac{23}{24}.$$

Thus, one has

$$\mathsf{P}(\lambda_{\delta,S}) \le \frac{8\mathsf{P}(\lambda_0)}{N}(\Delta\xi_{\max}^2+1) + \mathsf{P}(\lambda_{-a|T}) \le \left(\frac{8\mathsf{P}(\lambda_0)(\Delta\xi_{\max}^2+1)}{N\cdot\mathsf{P}(\lambda_{-a|T})}+1\right)\mathsf{P}(\lambda_{-a|T})$$
$$\le \left(\frac{24\cdot 8}{23\cdot N}(\Delta\xi_{\max}^2+1)+1\right)\mathsf{P}(\lambda_{-a|T}) \le \left(\frac{C'\Delta}{N}+1\right)\mathsf{P}(\lambda_{-a|T}),$$

where $C' = 9(\xi_{\max}^2+1)$, as $\Delta \ge 1$. Using this bound in the appropriate link deletion equation we have:

$$\begin{aligned}
\mathsf{P}(\lambda) &= \mathsf{P}(\lambda_{-a|T}) - \frac{1}{N}\sum_{(\delta,S)\in I_{a|T}} \mathsf{P}(\lambda_{\delta,S}) \quad \text{(From Eq. (5))}\\
&\ge \mathsf{P}(\lambda_{-a|T}) - \frac{1}{N}\sum_{(\delta,S)\in I_{a|T}} \mathsf{P}(\lambda_{-a|T})(1+C'\Delta/N)\\
&\ge \mathsf{P}(\lambda_{-a|T})\left(1-\frac{\|\lambda\|-\Delta-|T|/2}{N}\left(1+\frac{C'\Delta}{N}\right)\right) \quad \text{(From Lemma 1)}\\
&\ge \mathsf{P}(\lambda_{-a|T})\left(1-\frac{\|\lambda\|-1}{N}+\frac{\Delta}{N}\left(1-\frac{C'(\|\lambda\|-\Delta-1)}{N}\right)\right)\\
&\ge \mathsf{P}(\lambda_{-a|T})\left(1-\frac{\|\lambda\|-1}{N}\right).
\end{aligned}$$

The last inequality follows as $C'\|\lambda\| \le N$, for $\|\lambda\| \le N/12\xi_{\max}^2$, which concludes our proof of Proposition 1. □

Remark 3. Note that the initial bound ensures only that $a_{0,\ell} \le 1$. However, the presence of recursive inequality forces the value of $a_{0,\ell}$ to be very small.

4 Cryptographic Applications

In order to give an overview of how Mirror Theory can be used, and to illustrate the importance of the "$P_i \oplus P_j$ theorem" for any $\xi_{\max}$, we provide security proofs for a diverse set of constructions. Note that we focus on the parts of the proof that involve system of bivariate equations and omit the other parts, for which we cite the relevant results in the literature. We felt the need to add this section mainly to motivate the readers on the importance of the proof of this result.

4.1 The H coefficients technique

In this section, we consider one of the main applications of Theorem 1, which is proving the security of a pseudorandom function (PRF) F, or a pseudorandom permutation, P, based on a secret random primitve. Formally, for any information-theoretical adversary $\mathbf{A}$ that is allowed at most q oracle queries, we

define its advantage in distinguishing F from a truly uniformly random oracle, denoted \$, as follows:

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathbf{A}) := \left|\mathsf{Pr}\left(\mathbf{A}^F = 1\right) - \mathsf{Pr}\left(\mathbf{A}^{\$} = 1\right)\right|.$$

Whereas, for any information-theoretical adversary $\mathbf{A}$ that is allowed at most q forward and backward oracle queries, we define its advantage in distinguishing P from a truly uniformly random permutation oracle, denoted \$\$, as follows:

$$\mathbf{Adv}_P^{\mathrm{sprp}}(\mathbf{A}) := \left|\mathsf{Pr}\left(\mathbf{A}^P = 1\right) - \mathsf{Pr}\left(\mathbf{A}^{\$\$} = 1\right)\right|.$$

One way of upper-bounding the prf-advantage of $\mathbf{A}$ is to use the H coefficients technique, which is tightly linked to Mirror Theory. To use this method, we summarize the interaction of $\mathbf{A}$ with its oracle in what we refer to as a transcript

$$\tau = \{(X_1, Y_1), \ldots, (X_q, Y_q)\},$$

where, for each pair (x_i, y_i), $\mathbf{A}$ made a query x_i and received y_i as an answer (or made a query y_i and received x_i as an answer, in case of backward queries). We also introduce two random variables $\mathrm{T}_{\mathrm{real}}$ and $\mathrm{T}_{\mathrm{ideal}}$ which correspond to the value of τ when $\mathbf{A}$ interacts respectively with the real world (the construction F or P) and the ideal world (resp., \$ or \$\$). We say that a transcript τ is *attainable* if it satisfies $\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right) > 0$. The set of all attainable transcripts is written $\mathscr{T}$. One has the following result.

Lemma 4 ([38]). *Let $\mathscr{T}_{\mathsf{good}} \subset \mathscr{T}$ be a subset of the set of all attainable transcripts. Assume that, for every $\tau \in \mathscr{T}_{\mathsf{good}}$, one has*

$$\frac{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{real}} = \tau\right)}{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right)} \geq 1 - \varepsilon.$$

Then, one has

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathbf{A}) \leq \mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} \in \mathscr{T} \setminus \mathscr{T}_{\mathsf{good}}\right) + \varepsilon.$$

Mirror Theory is generally used when computing the lower bound of the ratio $\mathsf{Pr}\left(\mathrm{T}_{\mathrm{real}} = \tau\right) / \mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right)$ by providing a lower bound for the number of intermediate values for the underlying random primtive. We now illustrate this technique by revisiting existing security proofs using Theorem 1.

4.2 The XORP Construction

In [21], Iwata introduced CENC, a beyond-birthday-bound secure mode of operation which uses an underlying permutation-based PRF dubbed XORP which is defined as follows:

$$\begin{aligned} \mathsf{XORP}[w] : \{0,1\}^{n-s} &\longrightarrow \{0,1\}^{wn} \\ x &\longmapsto \|_{i=1}^{w} \pi\left(\langle 0\rangle_s \| x\right) \oplus \pi\left(\langle i\rangle_s \| x\right), \end{aligned}$$

where $s = \lceil \log_2(w+1) \rceil$, and π is a uniformly random secret n-bit permutation. Later, Iwata, Mennink, and Vizár [22] made the link between XORP and Mirror Theory explicit, and proved optimal security for the construction, using [40, Theorem 6]. We revisit their proof by applying Theorem 1 in order to demonstrate the following result[10].

Theorem 2. *Let* $\mathbf{A}$ *be an adversary against the prf-security of* $\mathsf{XORP}[w]$*, which is allowed at most* q *queries. If* $q \leq 2^n/12(w+1)^2$*, one has*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[w]}(\mathbf{A}) \leq \frac{wq}{2^n} + \frac{w^2 q}{2^{n+1}}.$$

Proof. We are going to rely on the H coefficients technique. Let us fix an adversary $\mathbf{A}$ against the prf-security of $\mathsf{XORP}[w]$, which is allowed at most q queries. We assume without loss of generality that $\mathbf{A}$ is deterministic (as it is time-unbounded), never repeats queries, and always makes exactly q queries. The transcript τ of the interaction of $\mathbf{A}$ with its oracle can be written as

$$\tau = \{(X_1, Y_{1,1} \| \dots \| Y_{1,w}), \dots, (X_q, Y_{q,1} \| \dots \| Y_{q,w})\},$$

where, for $i = 1, \dots, q$ and $j = 1, \dots, w$, one has $|Y_{i,j}| = n$. We say that an attainable transcript τ is bad if at least one of those conditions is satisfied:

- there exists $(i,j) \in (q] \times (w]$ such that $Y_{i,j} = 0^n$;
- there exists $(i,j,j') \in (q] \times (w] \times (w]$ such that $j \neq j'$ and $Y_{i,j} = Y_{i,j'}$.

The set $\mathscr{T}_{\mathsf{good}}$ consists in all attainable transcripts which are not bad. Since the $Y_{i,j}$ values are uniformly random and independent in the ideal world, it is easy to see that one has

$$\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} \in \mathscr{T} \setminus \mathscr{T}_{\mathsf{good}}\right) \leq \frac{wq}{2^n} + \frac{w^2 q}{2^{n+1}}. \tag{10}$$

Let us fix any good transcript τ. By taking $X'_{i,j} = \pi\left(\langle j \rangle_s \| X_i\right)$, the event $\mathrm{T}_{\mathrm{real}} = \tau$ can easily be turned into the following system of bivariate affine equations:

$$\begin{array}{ccc} X'_{1,0} \oplus X'_{1,1} = Y_{1,1} & & X'_{1,0} \oplus X'_{q,1} = Y_{q,1} \\ \vdots & \dots & \vdots \\ X'_{1,0} \oplus X'_{1,w} = Y_{1,w} & & X'_{1,0} \oplus X'_{q,w} = Y_{q,w} \end{array}$$

Since τ is a good transcript, the corresponding graph clearly has q components, of size $w+1$, and the sum of labels of edges of any path in the graph is not 0^n. Let us denote N the number of pairwise distinct solutions of this system. Then the probability that $X'_{i,j} = \pi\left(\langle j \rangle_s \| X_i\right)$ for all pairs (i,j) is exactly $1/(2^n)^{\underline{(w+1)q}}$. Hence, one has

$$\frac{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{real}} = \tau\right)}{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right)} \geq N \frac{(2^n)^{wq}}{(2^n)^{\underline{(w+1)q}}} \geq 1, \tag{11}$$

where the last inequality results from the application of Theorem 1. Combining Lemma 4 with Eqs (10) and (11) ends the proof of Theorem 2.

[10] We do not claim novelty for this Theorem, but we present its proof for illustration purpose.

4.3 Optimally Secure Variable-Input-Length PRFs

In [7], Cogliati, Jha and Nandi propose several constructions to build optimally secure variable-input-length (VIL) PRFs from secret random permutations. Those schemes combine a diblock almost collision-free universal hash function with a finalization function based on the Benes construction [2]. The most efficient variant, whose representation can be found in Figure 4.1, relies on two independent permutations, and its security proof [7, Theorem 7.3] involves the use of Mirror Theory for a single permutation.

First, let us recall the necessary definition for keyed hash function. A $(\mathscr{K}, \mathscr{X}, \mathscr{Y})$-keyed function H is said to be ϵ-*almost universal (AU) hash function* if for any distinct $X, X' \in \mathscr{X}$, we have

$$\mathsf{Pr}_{\mathsf{K} \xleftarrow{\$} \mathscr{K}} \left(H_{\mathsf{K}}(X) = H_{\mathsf{K}}(X')\right) \leq \epsilon. \tag{12}$$

Let us fix a non-empty set $\mathscr{X} \subset \{0,1\}^*$, and let H be a $(\mathscr{K}, \mathscr{X}, \mathscr{Y})$-keyed function that processes its inputs in n-bit blocks. H is said to be (q, σ, ϵ)-*Almost θ-Collision-free Universal* (or ACU_θ) if, for every $X^q \in (\mathscr{X})_q$ such that X^q contains at most σ blocks, one has $\mathsf{Pr}[C \geq \theta] \leq \epsilon$, where

$$C := |\{(i,j) \,:\, 1 \leq i < j \leq q,\, H_K(X_i) = H_K(X_j)\}|.$$

Finally, we say that a pair $H = (H_1, H_2)$ of two $(\mathscr{K}, \mathscr{X}, \mathscr{Y})$-keyed hash functions H_1, H_2 is $(q, \sigma, \epsilon_2, \epsilon_1)$-*Diblock ACU_q* (or DbACU_q) if H is (q, σ, ϵ_2)-AU and H_1, H_2 are (q, σ, ϵ_1)-ACU_q.

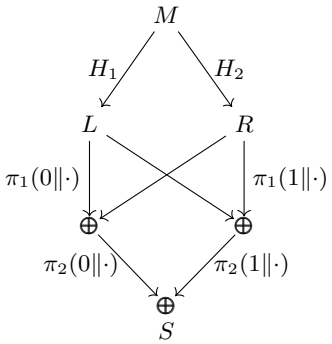

Fig. 4.1: Representation of the 2k-HtmB-p2$[H]$ based on two uniformly random and independent n-bit permutations π_1, π_2. An edge (u, v) with label g denotes the mapping $v = g(u)$. Unlabelled edges are identity mapping. The inputs to the functions $\pi_i(j\|\cdot)$ are first truncated before the application of π_i.

Having defined the required security notion for the underlying hash function, the following result holds.

Theorem 3. *For $\epsilon_1, \epsilon_2, \sigma \geq 0$, $q \leq 2^n/12n^2$, and $(q, \sigma, \epsilon_2, \epsilon_1)$-DbACU$_q$ hash function H instantiated with key $K \leftarrow_{\$} \mathscr{K}$, the prf-advantage of any distinguisher $\mathbf{A}$ that makes at most q queries against* 2k-HtmB-p2$[H]$ *is given by*

$$\mathbf{Adv}^{\mathrm{prf}}_{\text{2k-HtmB-p2}[H]}(\mathbf{A}) \leq \frac{128q^2}{2^{3n}} + \frac{136q^2}{2^{2n}} + \frac{8q}{2^n} + \epsilon_2 + 2\epsilon_1.$$

The complete proof of this result is exactly the same as the one of [7, Theorem 7.3] where [40, Theorem 6] is replaced with Theorem 1.

Proof Sketch. Let us denote with M_i, for $i = 1, \ldots, q$, the inputs from $\mathbf{A}$. We introduce several random variables: $L_i = H_1(M_i)$, $R_i = H_2(M_i)$, $X_i = \mathsf{trunc}_{n-1}(\pi_1(0\|L_i) \oplus R_i)$ and $Y_i = \mathsf{trunc}_{n-1}(\pi_1(1\|R_i) \oplus L_i)$, so that

$$S_i = \pi_2(0\|X_i) \oplus \pi_2(1\|Y_i).$$

Additionally, at the end of the interaction of $\mathbf{A}$ with its oracle, we release the values of the L_is, R_is,X_is, and Y_is. In the real world, we release the actual values, while in the ideal world we simply draw uniformly random keys for H_1 and H_2, along with a lazily sampled uniformly random π_1. Note that this can only increase the advantage of an adversary, so this can be done without loss of generality.

In order to apply Theorem 1, we need to make sure that the system (S) consisting of the q equations

$$S_i = \pi_2(0\|X_i) \oplus \pi_2(1\|Y_i)$$

satisfies the initial conditions. We recall that an alternating trail of length k is a sequence $(i_1, \ldots, i_{k+1})$ such that either $X_{i_j} = X_{i_j+1}$ or $Y_{i_j} = Y_{i_j+1}$ for $j = 1, \ldots, k$, and consecutive equalities do not involve the same family of variables (i.e. an equality in X should be followed with an equality in Y). Moreover, an alternating cycle is a special type of alternating trail of even length, such that $i_{k+1} = i_1$. We say that a transcript τ is bad if at least one of the following conditions hold:

- τ contains an alternating cycle;
- τ contains an alternating trail $(i_1, \ldots, i_{k+1})$ such that $\oplus_{j=1}^{k+1} S_{i_j} = 0$;
- the largest block of equalities contains at least $n + 1$ variables.[11]

In [7], the authors prove that

$$\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} \in \mathscr{T} \setminus \mathscr{T}_{\mathsf{good}}\right) \leq \frac{128q^2}{2^{3n}} + \frac{136q^2}{2^{2n}} + \frac{8q}{2^n} + \epsilon_2 + 2\epsilon_1. \tag{13}$$

Moreover, for any good transcript τ, one has

$$\frac{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{real}} = \tau\right)}{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right)} = \frac{s2^{nq}}{(2^n)^{\underline{q_X + q_Y}}} \geq 1, \tag{14}$$

[11] We say that two variables are in the same block of equalities if there exists an alternating trail involving both variables.

where s denotes the number of p.d. solutions to the system (S) of equations, and q_X (resp. q_Y) the number of pairwise distinct X_i (resp. Y_i) values, and the last inequality results from the application of Theorem 1. Combining Lemma 4 with Equations (13) and (14) ends the proof of Theorem 3.

4.4 Feistel schemes

In [41], Patarin introduced the study of beyond-birthday-bound security of balanced and unbalanced Feistel schemes using Mirror Theory. Since our work has improved upon the bounds of the '$P_i \oplus P_j$ Theorem for any $\xi_{\max}$' used by Patarin, we present here the proof sketch of security analysis of six-round balanced Feistel scheme with our new improved bounds.

Defintion of ψ^k. Suppose Func_n is the collection of all n-bit functions from $\{0,1\}^n$ to itself, and Perm_{2n} be the collection of all permutations on $\{0,1\}^{2n}$. Then for $f \in \mathsf{Func}_n$ and $L, R \in \{0,1\}^n$, $\psi(f) \in \mathsf{Perm}_{2n}$ is defined as follows:

$$\psi(f)[L,R] := [R, L \oplus f(R)]$$

In general, for $f_1, \cdots, f_k \in \mathsf{Func}_n$, $\psi^k(f_1, \cdots, f_k) \in \mathsf{Perm}_{2n}$ is defined as,

$$\psi^k(f_1, \cdots, f_k) := \psi(f_k) \circ \cdots \circ \psi(f_1).$$

The permutation $\psi^k(f_1, \cdots, f_k)$ is called a *balanced Feistel scheme with k rounds*. When $f_1, \cdots, f_k$ are randomly and independently chosen in Func_n, $\psi^k(f_1, \cdots, f_k)$ is called a *random Feistel scheme with k rounds*.

To analyse the PRP security of k-round Feistel scheme via the H-coefficient technique, given a transcript containing q query-response pairs

$$\tau := \{([L_i, R_i], [S_i, T_i]) : L_i, R_i, S_i, T_i \in \{0,1\}^n, i \in [q]\},$$

we would like to find out the probability of realizing this transcript in the real world,

$$\Pr(T_{\text{real}} = \tau) = \Pr_{\substack{(f_1, \cdots, f_k) \\ \xleftarrow{\$} \mathsf{Func}_n^k}} \left(\psi^k(f_1, \cdots, f_k)[L_i, R_i] = [S_i, T_i] \ \forall i \in [q]\right) = \frac{H_k(\tau)}{|\mathsf{Func}_n|^k}$$

where,

$$H_k(\tau) := \left|\{(f_1, \cdots, f_k) \in \mathsf{Func}_n^k : \psi^k(f_1, \cdots, f_k)[L_i, R_i] = [S_i, T_i] \ \forall i \in [q]\}\right|$$

Note that, here, irrespective of whether the transcript was realized in the real or the ideal world, we will have that $[L_i, R_i], i \in [q]$ are pairwise distinct, and $[S_i, T_i], i \in [q]$ are pairwise ditinct. There are no bad trancripts in the following analysis.

In Fig. 4.2 we have denoted the outputs of the successive rounds as follows:

$$[L_i, R_i] \xrightarrow{\psi(f_1)} [R_i, X_i] \xrightarrow{\psi(f_2)} [X_i, Y_i] \xrightarrow{\psi(f_3)} [Y_i, Z_i] \xrightarrow{\psi(f_4)} [Z_i, A_i] \xrightarrow{\psi(f_5)} [A_i, S_i] \xrightarrow{\psi(f_6)} [S_i, T_i]$$

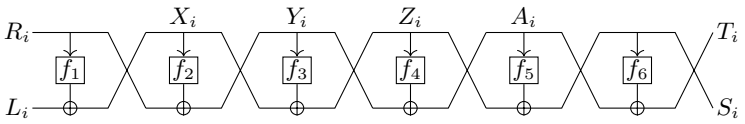

Fig. 4.2: Balanced Feistel scheme with 6 rounds

Viewing 6-round Feistel as $\psi^6(f_1, \cdots, f_6) = \psi(f_1) \circ \psi^4(f_2, \cdots, f_5) \circ \psi(f_6)$, we can write

$$H_6(\tau) = \sum_{f_1, f_6 \in \mathsf{Func}_n} H_4(\tau') \tag{15}$$

where

$$\tau' = \{([R_i, X_i], [A_i, S_i]) : X_i := L_i \oplus f_1(R_i), A_i := T_i \oplus f_6(S_i), i \in [q]\}$$

Frameworks for ψ^4. To calculate $H_4(\tau')$ we define a 'framework' as collection of equations of the form $Y_i = Y_j$ or $Z_i = Z_j$. We will say that two frameworks are equal if they imply exactly the same set of equalities in Y and Z. Let $\mathscr{F}$ be a framework. We will denote by $\mathsf{weight}(\mathscr{F})$ the number of $(Y_i, Z_i) \in (\{0,1\}^n)^2, i \in [q]$ that satisfy $\mathscr{F}$. If we denote $y_{\mathscr{F}}$ (resp., $z_{\mathscr{F}}$) the number of independent equalities of the form $Y_i = Y_j$ (resp., of the form $Z_i = Z_j$) in $\mathscr{F}$, then obviously we have $\mathsf{weight}(\mathscr{F}) = (N)^{\underline{q-y_{\mathscr{F}}}} \cdot (N)^{\underline{q-z_{\mathscr{F}}}}$

Note that, for a given framework $\mathscr{F}$, $Y_i = Y_j \in \mathscr{F} \implies f_3(Y_i) = f_3(Y_j)$, which is equivalent to saying $X_i \oplus Z_i = X_j \oplus Z_j$. Similarly, $Z_i = Z_j \in \mathscr{F} \implies Y_i \oplus A_i = Y_j \oplus A_j$. Moreover, $X_i = X_j \implies f_2(X_i) = f_2(X_j)$ which is equivalent to saying $R_i \oplus Y_i = R_j \oplus Y_j$. Similarly, $A_i = A_j \implies Z_i \oplus S_i = Z_j \oplus S_j$.

Let x be the number of independent equalities of the form $X_i = X_j, i \neq j$ and a be the number of independent equalities of the form $A_i = A_j, i \neq j$. Then by simple alegbraic manipulation we have the following result.

Lemma 5 (exact formula for $H_4(\tau')$).

$$H_4(\tau') = |\mathsf{Func}_n|^4 \sum_{\mathscr{F}} \frac{[\#Y^q \textit{ satisfying } (C1)] \cdot [\#Z^q \textit{ satisfying } (C2)]}{N^{4q-x-y_{\mathscr{F}}-z_{\mathscr{F}}-a}} \tag{16}$$

where

$$(C1): \begin{cases} X_i = X_j \implies Y_i \oplus Y_j = R_i \oplus R_j \\ Z_i = Z_j \in \mathscr{F} \implies Y_i \oplus Y_j = A_i \oplus A_j \\ \textit{The only equations } Y_i = Y_j, i < j, \textit{ are exactly those implied by } \mathscr{F} \end{cases}$$

$$(C2): \begin{cases} A_i = A_j \implies Z_i \oplus Z_j = S_i \oplus S_j \\ Y_i = Y_j \in \mathscr{F} \implies Z_i \oplus Z_j = X_i \oplus X_j \\ \textit{The only equations } Z_i = Z_j, i < j, \textit{ are exactly those implied by } \mathscr{F} \end{cases}$$

The summation on the r.h.s. of Eq. (16) *is taken over all possible frameworks $\mathscr{F}$.*

A we can see (C_1) yeilds a system of difference equations in the variables Y^q, and $(C2)$ a system of difference equations in Z^q. To find the number of solutions to these systems of equations using Theorem 1, we have to ensure: (1) the systems are p.d.-consistent, (2) the conditions specified in the theorem, like the bound on the maximum component size, and that on the number of variables, is satisfied by the concerned systems.

Now the systems will be p.d. consistent if there is no cycle of non-zero label sum. To be on the safe side, we eliminate the possibility of any cycle whatsoever. Note that, there will be a cycle in the graph representing the system of difference equations in $(C1)$ (resp., $(C2)$) only if there is a 'circle in $X, Z_{\mathscr{F}}$' (resp., 'circle in $A, Y_{\mathscr{F}}$'), by which we mean that, for some $k \geq 3$, there is a cyclic tuple of indices $(i_1, \cdots, i_k)$, with $i_1, \cdots, i_{k-1}$ pairwise distinct and $i_k = i_1$, such that for all $j \in [k-1]$, either we have $X_{i_j} = X_{i_{j+1}}$ or we have $Z_{i_j} = Z_{i_{j+1}} \in \mathscr{F}$. We define a circle in $A, Y_{\mathscr{F}}$ similarly.

Following the same arguments there will be component of size ξ in the graph representing the system of difference equations in $(C1)$ (resp., $(C2)$) only if there is a 'line in $X, Z_{\mathscr{F}}$' (resp., 'line in $A, Y_{\mathscr{F}}$') of length ξ, by which we mean that, there are $\xi + 1$ distinct indices $i_1, \cdots, i_{\xi+1}$ such that for all $j \in [\xi]$, either $X_{i_j} = X_{i_{j+1}}$ or $Z_{i_j} = Z_{i_j} \in \mathscr{F}$. We define a line in $A, Y_{\mathscr{F}}$ similarly.

Good Framework. We call a framework for ψ^4, $\mathscr{F}$, a *good framework*, if it does not result in any of the following:

1. a circle in $X, Z_{\mathscr{F}}$
2. a circle in $A, Y_{\mathscr{F}}$
3. a line in $X, Z_{\mathscr{F}}$ of length $\geq n$
4. a line in $A, Y_{\mathscr{F}}$ of length $\geq n$

From elaborate probability calculations done in Appendix C of [41] we have the following result:

Lemma 6 ([41]). *For a realizable trancript $\tau = \{([L_i, R_i], [S_i, T_i]) : i \in [q]\}$, when $f_1, f_6 \leftarrow\!\!\$\ \mathsf{Func}_n$ and $\mathscr{F}$ is randomly chosen (i.e., with probability proportional to $\mathsf{weight}(\mathscr{F})$), then*

$$\Pr[\mathscr{F} \textit{ is a good framework}] \geq 1 - \frac{8q}{N}.$$

If a good framework $\mathscr{F}$ is chosen, then the systems of difference equations in $(C1)$ and $(C2)$ are p.d.-consistent and satisfy the conditions of Theorem 1 with $\xi_{\max} \leq n$. Now the system of difference equations in $(C1)$ (resp., $C2$) has $x + z_{\mathscr{F}}$ equations in $q - y_{\mathscr{F}}$ variables (resp., $a + y_{\mathscr{F}}$ equations in $q - z_{\mathscr{F}}$ variables) and hence by Theorem 1 has at least $(N)^{\underline{q-y_{\mathscr{F}}}}/N^{x+z_{\mathscr{F}}}$ solutions (resp., $(N)^{\underline{q-z_{\mathscr{F}}}}/N^{a+y_{\mathscr{F}}}$ solutions) if $q \leq N/12(\log_2 N)^2$. Then from Eq. (15) and Eq. (16) we get that

$$H_6(\tau) \geq \frac{|\mathsf{Func}_n|^4}{N^{4q}} \sum_{f_1, f_6 \in \mathsf{Func}_n} \sum_{\text{good } \mathscr{F}} \underbrace{(N)^{\underline{q-y_{\mathscr{F}}}} \cdot (N)^{\underline{q-z_{\mathscr{F}}}}}_{\mathsf{weight}(\mathscr{F})} \overset{(\star)}{\geq} \frac{|\mathsf{Func}_n|^6}{N^{2q}} \left(1 - \frac{8q}{N}\right)$$

where $(\star)$ follows from Lemma 6 and the fact that $\sum_{\mathscr{F}} \mathsf{weight}(\mathscr{F}) = N^{2q}$. Thus, we have a for a realizable transcipt τ

$$\frac{\Pr[T_{\text{real}} = \tau]}{\Pr[T_{\text{ideal}} = \tau]} = \frac{\frac{1}{N^{2q}}\left(1 - \frac{8q}{N}\right)}{1/(N^2)^{\underline{q}}} \geq 1 - \frac{8q}{N} - \frac{q^2}{N^2}.$$

Summarizing we have the following result.

Theorem 4. *If $q \leq \frac{2^n}{12n^2}$, then for every CPCA-2 adversary* [12] $\mathbf{A}$ *with q adaptive chosen plaintext or chosen ciphertext queries, we have*

$$\mathbf{Adv}^{\text{sprp}}_{\psi^6(f_1,\cdots,f_6)}(\mathbf{A}) \leq \frac{8q}{2^n} + \frac{q^2}{2^{2n}}.$$

where $f_1, \cdots, f_6 \leftarrow\!\!\$\ \mathsf{Func}_n$.

4.5 A comparative study of the security bounds

First we consider the security bounds attainable for the above constructions without using Mirror Theory.

1. There exists another proof of optimal n-bit security for the $\mathsf{XORP}[w]$ construction [6], that does not rely on Mirror Theory. Instead, it uses the so-called χ^2 technique [11].
2. In [7] Cogliati et al proposes several VIL PRF constructions from secret random permutations using the Hash-then-modified-Benes method. To obtain optimal security without using Mirror Theory they proposed the candidate $\mathsf{2k\text{-}HtmB\text{-}p1}[H]$, which requires 6 secret random permutations. In comparision $\mathsf{2k\text{-}HtmB\text{-}p2}[H]$ only needs 4 secret random permutations (obtained from domain separating two random permutations) to attain n-bit security. However, the only existing security proof of the latter depends crucially on Mirror Theory.
3. Six-round Feistel construction can only be shown to be birthday-bound secure without using Mirror Theory, no better security proof is known.

Also, the optimal n-bit security bounds for the above three constructions, are obtained in [22], [7] and [41], respectively, by using the following conjectured version of Mirror Theory [40, Theorem 6], whose proof is incomplete:

"Theorem $P_i \oplus P_j$" for any $\xi_{\max}$. *Let (A) be a set of a equation $P_i \oplus P_j = \lambda_k$ with α variables such that:*

1. *We have no circle in P in the equations (A).*
2. *We have no more than $\xi_{\max}$ indices in the same block.*
3. *By linearity from (A) we cannot generate an equation $P_i = P_j$ with $i \neq j$.*

[12] CPCA-2 adversary here means an adversary that adaptively queries Chosen Plaintexts and Chosen Ciphertexts.

Then: if $\xi_{\max}^2\alpha \ll 2^n$*, we have* $H_\alpha \geq J_\alpha$*. More precisely the fuzzy condition* $\xi_{\max}^2\alpha \ll 2^n$ *can be written with the explicit bound:* $(\xi_{\max}-1)^2\alpha \leq 2^n/67$*.*

In the above theorem conditions 1 and 3 correspond to the p.d.-consistency condition of this paper, and condition 2 correspond to the condition that the maximum component size of the corresponding graph is $\xi_{\max}$. α in the above theorem is replaced by p in Theorem 1 of this paper. Also using the notation of [40], $H_\alpha \geq J_\alpha$ translates to: the number of p.d. solutions of the system of equations (A) is $\geq (2^n)^{\underline{\alpha}}/2^{nm} = (N)^{\underline{\alpha}}/N^m$, which is exactly the bound obtained in this paper. However we notice the following important differences:

1. The above theorem is for any $\xi_{\max}$, while Theorem 1 of this paper works for $\xi_{\max}$ of the order $O(N^{1/4})$.
2. The bound on α or p in the above theorem is $N/67(\xi_{\max}-1)^2$, while the one attained in Theorem 1 of this paper is $N/12\xi_{\max}^2$, which is slightly better.

5 Conclusion and Future Work

In this work, we present the first complete and verifiable proof of the $P_i \oplus P_j$ Theorem with any $\xi_{\max}$. Our proof builds on the previous works on this subject by reusing the overall strategy. However, our core novelty is the use of the link-deletion equation, which allows a better proof by induction that introduces a much smaller number of terms. This improvement leads to a shorter proof and a slightly better bound, as long as $\xi_{\max}$ is of the order $O(N^{1/4})$. As an application, we give proofs of n-bit security for the XORP and 2k-HtmB-p2 constructions, thus confirming the results from [22] and [7]. Theorem 1 is also used to revisit the security proofs of balanced Feistel schemes [41,32] and prove the optimal security of six rounds Feistel scheme [41,32]. Moreover, using our result, one can also show an asymptotically optimal security bound for DWCDM [15,16] construction. In fact, the H coefficients technique can be used to transform many cryptographic security proofs into Mirror Theory problems. However, these problems may sometimes be more general than the one we target in this work. For example, in this work we deal with pairwise distinctness of the solution to a system of equations, which is same as finding solutions to the given system of equations, along with a system of non-equations of the form $X_j \oplus X_k \neq 0^n$ for all $j \neq k$. However, when dealing with constructions like the Feistel cipher where the round functions are permutations, we find that in addition to the conditions of the form $(C1)$ obtained in Lemma 5, we also get that $X_i \neq X_j \implies Y_i \oplus Y_j \neq R_i \oplus R_j$, i.e. non-equations with non-zero labels. This indicates to the following more general problem, that is yet to be solved:

Open Problem 1. Find the lower bound to the number of solutions to a system of equations and a *possibly non-homogeneous system of non-equations.*

Studying variants of Theorem 1, as the one mentioned above, would help to improve security bounds for current and future cryptographic constructions:

Open Problem 2. Generalize Theorem 1 for *groups of exponent* $\neq 2$. Then it can be used for security proof of Feistel network whose operator is modular addition, and not $\oplus$ (which is important for Format-Preserving Encryption).

Open Problem 3. Generalize Theorem 1 for $\xi_{\max} > O(2^{n/4}/\sqrt{n})$. This might be used for optimal security proof of nonce misuse resistant MAC scheme nEHtM. Note that the bound does not always hold when $\xi_{\max}$ gets close to $2^{n/2}$. A counterexample can be found in [32, page 225].

Open Problem 4. Generalize Theorem 1 for the case when *the solutions are chosen from a proper subset of* $\{0,1\}^n$. This is applicable for ideal-permutation-based keyed constructions. As an adversary can make direct queries to the ideal permutation P, some inputs and outputs are fixed beforehand.

Open Problem 5. Generalize for *systems of equations having more than just two variables*, for example, say, $X_1 \oplus X_2 \oplus X_3 \oplus X_4 = 0$. This will prove optimal security for constructions like the ones mentioned in [8].

Also, there are two other conjectured Mirror-Theory-like results [32, Conjecture 14.1 & 14.2] about the number of permutations g and h such that $g * h$ is equal to a given function f, for any commutative group law $*$.

Acknowledgements

Part of this work was carried out in the framework of the French-German-Center for Cybersecurity, a collaboration of CISPA and LORIA, while Benoît Cogliati was employed at the CISPA Helmholtz Center for Information Security.

A Postponed Proofs

A.1 Proof of Lemma 2

We fix $S \in \gamma \subseteq \lambda$ where $|\gamma| = \alpha$ and a set U with $|U| = \ell + 1$ disjoint with S. Let $\tau := \gamma_{+U}$ and $\tau' := \gamma_{-S+(S \sqcup U)}$. In words, γ is a set-system that is included in λ, U is any subset of $\mathscr{G}$ of size $\ell + 1$, and S is an element of γ. Then, τ corresponds to the $\gamma \cup \{U\}$, while τ' corresponds to τ after S and U have been merged. Looking back at Fig. 3.1, τ and τ' would correspond respectively to the second and third graphs. We assume that γ, U, S are chosen in such a manner that $|\mathsf{P}(\tau) - \mathsf{P}(\tau')| = D(\alpha, \ell)$. Now we prove the inequality in two cases.

Case $|U| = 1$. In this case, let $U = \{x\}$. Then $\mathsf{P}(\tau) = \mathsf{P}(\gamma) \cdot (1 - \|\gamma\|/2^n)$ from Eq. (1). Also $\tau'_{-x|S \sqcup U} = \gamma$. Hence from link deletion equation, Eq. (5),

$$\mathsf{P}(\tau') = \mathsf{P}(\gamma) - N^{-1} \sum_{(\delta, S') \in I} \mathsf{P}(\tau'_{\delta, S'})$$

where $I := I_{x,S} = \{(\delta, S') : x \oplus \delta \in S' \in \gamma_{-S}, S' \oplus \delta \text{ is disjoint with } S\}$. For $z' \in S' \in \gamma_{-S}$, $(x \oplus z, S') \notin I$ if and only if there exists $y \in S$ and $w \in S'$

such that $x \oplus y = z \oplus w$. Thus $|I| \geq \sum_{S' \in \gamma_{-S}} \left(|S'| - \sum_{y \in S} 2\delta_{S'}(x \oplus y) \right) = \|\gamma\| - |S| - \sum_{y \in S} 2\delta_{\gamma_{-S}}(x \oplus y) \geq \|\gamma\| - \|\gamma\|_{\max} \cdot 2\delta_\gamma$. Hence

$$\begin{aligned} D(\alpha, 0) = |\mathsf{P}(\tau) - \mathsf{P}(\tau')| &= \left| \frac{\|\gamma\|}{N} \mathsf{P}(\gamma) - N^{-1} \sum_{(\delta, S') \in I} \mathsf{P}(\tau'_{\delta, S'}) \right| \\ &\overset{(\star)}{\leq} N^{-1} \sum_{(\delta, S') \in I} |\mathsf{P}(\gamma) - \mathsf{P}(\tau'_{\delta, S'})| + \frac{2\Delta_\gamma \|\gamma\|_{\max} \cdot \mathsf{P}(\lambda)}{N \left(1 - \frac{\|\lambda \setminus \gamma\|_{\max} \times \|\gamma\|}{N}\right)^{|\lambda \setminus \gamma|}} \\ &\leq \frac{\|\gamma_{-S}\|_{\max}}{N} \sum_{S' \in \gamma \setminus S} D(\alpha - 1, |S'| - 1) + \frac{2\Delta_\gamma \|\gamma\|_{\max} \cdot \mathsf{P}(\lambda)}{N \left(1 - \frac{\|\lambda \setminus \gamma\|_{\max} \times \|\gamma\|}{N}\right)^{|\lambda \setminus \gamma|}}, \end{aligned}$$

where the last term in $(\star)$ is obtained from the initial condition Eq. (4).

Case $|U| \geq 2$. Fix $x \in U$. By link-deletion equation, we have

$$\begin{aligned} \mathsf{P}(\tau) &= \mathsf{P}(\tau_{-x|U}) - \frac{1}{N} \sum_{(\delta, S') \in I} \mathsf{P}(\tau_{\delta, S'}) \\ \mathsf{P}(\tau') &= \mathsf{P}(\tau'_{-x|S \sqcup U}) - \frac{1}{N} \sum_{(\delta, S') \in I'} \mathsf{P}(\tau'_{\delta, S'}), \end{aligned}$$

where

$$\begin{aligned} I &:= I_{x|U} = \{(\delta, S') : x \oplus \delta \in S' \in \gamma, \quad S' \oplus \delta \text{ is disjoint with } U \setminus x\}, \\ I' &:= I_{x|S \sqcup U} = \{(\delta, S') : x \oplus \delta \in S' \in \gamma_{-S}, \quad S' \oplus \delta \text{ is disjoint with } S \sqcup U \setminus x\}. \end{aligned}$$

It is easy to see that $I' \subseteq I$. If $(\delta, S') \in I \setminus I'$, then,

- either $S' = S$ and $\delta = x \oplus y$ for some $y \in S$, such that $S \oplus (x \oplus y)$ is disjoint with $U \setminus x$ or
- $S' \in \gamma \setminus S$ and $\delta = x \oplus z$ for some $z \in S'$, such that $S' \oplus (x \oplus z)$ is disjoint with $U \setminus x$ but not disjoint with $S \sqcup (U \setminus x)$.

The first case can contribute at most $|S|$. The second case will happen if for some $z, w \in S'$, and $y \in S$, $z \oplus w = x \oplus y$. Thus

$$|I \setminus I'| \leq |S| + \sum_{y \in S} \delta_{\gamma_{-S}}(x \oplus y) \leq \|\gamma\|_{\max} \cdot 2\Delta_\gamma.$$

Hence, we have the following:

$$
\begin{aligned}
&D(\alpha,\ell) = |\mathsf{P}(\tau) - \mathsf{P}(\tau')| \\
&\le \left|\mathsf{P}(\tau_{-x}) - \mathsf{P}(\tau'_{-x})\right| + N^{-1} \sum_{(\delta,S')\in I'} \left|\mathsf{P}(\tau_{\delta,S'}) - \mathsf{P}(\tau'_{\delta,S'})\right| + \sum_{(\delta,S')\in I\setminus I'} \mathsf{P}(\tau_{\delta,S'})/N \\
&\le D(\alpha,\ell-1) + \frac{\|\gamma_{-S}\|_{\max}}{N} \sum_{S'\in\gamma_{-S}} D(\alpha-1,\ell+|S'|-1) + \frac{2\Delta_\gamma \|\gamma\|_{\max}\cdot \mathsf{P}(\lambda)}{N\left(1-\frac{\|\lambda\setminus\gamma\|_{\max}\times\|\gamma\|}{N}\right)^{|\lambda\setminus\gamma|}}.
\end{aligned} \tag{17}
$$

The last inequality follows from the observation that $\tau_{\delta,S'}$ and $\tau'_{\delta,S'}$ are considered when we take maximum to compute $D(\alpha-1,\ell+|S'|-1)$. Moreover, from our initial condition Eq. (4),

$$
\mathsf{P}(\tau_{\delta,S'}) \le \mathsf{P}(\gamma) \le \mathsf{P}(\lambda)/\left(1-\frac{\|\lambda\setminus\gamma\|_{\max}\times\|\gamma\|}{N}\right)^{|\lambda\setminus\gamma|}
$$

Now, taking upper bounds of the total size terms, and adding some positive terms in the middle sum, and noting that $\Delta_\gamma \le \Delta_\lambda$ [13], the inequality, Eq. (17) can be easily modified to the theorem statement, Eq. (7).

A.2 Proof of Recursive Inequality Lemma

Let us denote by an ordered tuple of integers from $[q]$, as $i^k := (i_1,\cdots,i_k) \in [q]^k$. Note that, for all positive integer j, $e^j \ge \frac{j^j}{j!}$ and so $1/j! \le (e/j)^j$, and we have

$$
\binom{m}{j} \le \frac{m^j}{j!} \le (em/j)^j. \tag{18}
$$

This inequality will be frequently used for the proof of this lemma. We also use the following fact extensively: for $r<1$, $\sum_{j\ge i} r^j \le \frac{r^i}{1-r}$.

We state the following claim, which follows from iterated applications of the recursive inequality.

Claim 1. *For any $0 \le d \le \xi n$, and $0 \le \ell < \xi - 1$ we have*

$$
a_{0,\ell} \le \sum_{k=\lceil\frac{d-\ell}{\xi}\rceil}^{d} \binom{d}{k} \sum_{i^k\in[q]^k} a_{k,k+\sum_{j=1}^k \ell_{i_j}-d} + C\sum_{i=0}^{d-1}\sum_{j=\lceil\frac{i-\ell}{\xi}\rceil}^{i} \binom{i}{j}(4\xi e)^{-j}. \tag{19}
$$

[13] Since $\gamma\subseteq\lambda$, we have $\sum_{S\in\gamma}\delta_S(z) \le \sum_{S'\in\lambda}\delta_{S'}(z)$ for every $z\in\{0,1\}^n$, since every $S\in\gamma$ is subset of some $S'\in\lambda$. So taking maximum over all $z\in\{0,1\}^n$, on both sides would give us $\Delta_\gamma \le \Delta_\lambda$.

Proof of the Claim. We prove the claim by induction on d. The result holds trivially for $d = 1$ (by applying $d = \ell = 0$ in Eqn. (9)). Now we prove the statement for $d_0 + 1$, assuming it true for d_0. Therefore, we have

$$\begin{aligned}
a_{0,\ell} &\leq \sum_{k=\lceil \frac{d_0-\ell}{\xi} \rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - d_0} + C \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j} \\
&\leq \sum_{k=\lceil \frac{d_0-\ell}{\xi} \rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} \left(\sum_{i_{k+1} \in [q]} a_{k+1,k+1+\sum_{j=1}^{k+1} \ell_{i_j} - (d_0+1)} + C \cdot (4\xi eq)^{-k} \right) \\
&\quad + \sum_{k=\lceil \frac{d_0-\ell}{\xi} \rceil}^{d_0} \binom{d_0}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - (d_0+1)} + C \sum_{i=0}^{d_0-1} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j} \\
&\leq \sum_{k=\lceil \frac{d_0+1-\ell}{\xi} \rceil}^{d_0+1} \binom{d_0}{k-1} \sum_{i^{k-1} \in [q]^{k-1}} \sum_{i_k \in [q]} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - (d_0+1)} \\
&\quad + \sum_{k=\lceil \frac{d_0+1-\ell}{\xi} \rceil}^{d_0+1} \binom{d_0}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - (d_0+1)} + C \sum_{i=0}^{d_0} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j}.
\end{aligned}$$

The range of the first and second summations has deliberately been taken to start from $\lceil (d_0 + 1 - \ell)/\xi \rceil \leq \lceil (d_0 - \ell)/\xi \rceil + 1$, because if $k < \lceil (d_0 + 1 - \ell)/\xi \rceil$, then $k + \sum_{j=1}^{k} \ell_{i_j} - (d_0 + 1) \leq k\xi - (d_0 + 1) < 0$ and hence $a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - (d_0+1)} = 0$. Now we can see that the coefficient of $\sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - (d_0+1)}$ in the above summation is bounded by $\binom{d_0}{k-1} + \binom{d_0}{k} = \binom{d_0+1}{k}$. This concludes the proof of the claim. □

Proof of Lemma 3. Let us take $d = \xi n$. In that case, Claim 1 becomes

$$a_{0,\ell} \leq \sum_{k=\lceil \frac{\xi n-\ell}{\xi} \rceil}^{\xi n} \binom{\xi n}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - \xi n} + C \sum_{i=0}^{\xi n-1} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j}.$$

We are going to upper bound both terms of the sum in subsequent turns. For the first term, note that one has $k \geq n - \frac{\ell}{\xi} > n - 1$ since $\ell < \xi - 1$ by definition. This implies that

$$\binom{\xi n}{k} \leq \left(\frac{e\xi n}{k} \right)^k \leq \left(\frac{e\xi n}{n-1} \right)^k \leq (2e\xi)^k.$$

Hence, using the initial bound, one has

$$\sum_{k=\lceil \frac{\xi n-\ell}{\xi} \rceil}^{\xi n} \binom{\xi n}{k} \sum_{i^k \in [q]^k} a_{k,k+\sum_{j=1}^{k} \ell_{i_j} - \xi n} \leq \sum_{k=\lceil \frac{\xi n-\ell}{\xi} \rceil}^{\xi n} (2e\xi)^k q^k (4\xi eq)^{-k} \leq \frac{4}{2^n} \leq \frac{4}{N}$$

As for the second term, we make the following observation: For $\xi k < i \le \xi(k+1)$, $k \in (n-1]$, $j \ge \lceil \frac{i-\ell}{\xi} \rceil \ge k$, and hence

$$\binom{i}{j} \le \left(\frac{ei}{j}\right)^j \le \left(\frac{e\xi(k+1)}{k}\right)^j \le (2e\xi)^j.$$

For $0 \le i \le \xi$ and $j \ge 1$, $\binom{i}{j} \le \left(\frac{ei}{j}\right)^j \le (e\xi)^j$. Thus, we are going to break the sum into two parts:

$$\begin{aligned}
\sum_{i=0}^{\xi n-1} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j} &= \sum_{i=0}^{\xi} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j} + \sum_{i=\xi+1}^{\xi n-1} \sum_{j=\lceil \frac{i-\ell}{\xi} \rceil}^{i} \binom{i}{j} (4\xi e)^{-j} \\
&\le \xi + 1 + \sum_{i=0}^{\xi} \sum_{j=1}^{i} (e\xi)^j (4e\xi)^{-j} + \sum_{i=\xi+1}^{\xi n-1} \sum_{j=\lceil i/\xi \rceil - 1}^{i} (2e\xi)^j (4e\xi)^{-j} \\
&\le \xi + 1 + \frac{\xi+1}{3} + 4 \sum_{i=\xi+1}^{\xi n-1} \frac{1}{2^{\lceil i/\xi \rceil}} \\
&\overset{(1)}{\le} \frac{4}{3}(\xi+1) + 2\xi \overset{(2)}{\le} 4\xi,
\end{aligned}$$

where the last inequality follows from the fact that $\xi \ge 2$.

References

1. Data encryption standard. Federal Information Processing Standards Publication **112** (1999)
2. Aiello, W., Venkatesan, R.: Foiling birthday attacks in length-doubling transformations - benes: A non-reversible alternative to feistel. In: Advances in Cryptology - EUROCRYPT '96. Proceeding. pp. 307–320 (1996). https://doi.org/10.1007/3-540-68339-9_27
3. Bellare, M., Krovetz, T., Rogaway, P.: Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In: Advances in Cryptology - EUROCRYPT '98, Proceeding. pp. 266–280 (1998). https://doi.org/10.1007/BFb0054132
4. Ben Morris, Phillip Rogaway, T.S.: How to encipher messages on a small domain. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009. pp. 286–302. Springer Berlin Heidelberg, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_17
5. Bhattacharjee, A., Dutta, A., List, E., Nandi, M.: Cencpp* - beyond-birthday-secure encryption from public permutations (2020)
6. Bhattacharya, S., Nandi, M.: Revisiting variable output length xor pseudorandom function. IACR Transactions on Symmetric Cryptology **2018**(1), 314–335 (Mar 2018). https://doi.org/10.13154/tosc.v2018.i1.314-335

7. Cogliati, B., Jha, A., Nandi, M.: How to build optimally secure prfs using block ciphers. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 754–784. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_25
8. Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of k permutations. In: Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers. pp. 285–302 (2014). https://doi.org/10.1007/978-3-662-46706-0_15
9. Cogliati, B., Patarin, J.: Mirror theory: A simple proof of the pi+pj theorem with xi_max=2. Cryptology ePrint Archive, Report 2020/734 (2020), https://eprint.iacr.org/2020/734
10. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: CRYPTO 2016, Proceedings, Part I. pp. 121–149 (2016). https://doi.org/10.1007/978-3-662-53018-4_5
11. Dai, W., Hoang, V.T., Tessaro, S.: Information-theoretic indistinguishability via the chi-squared method. In: Advances in Cryptology - CRYPTO 2017. Proceedings, Part III. pp. 497–523 (2017). https://doi.org/10.1007/978-3-319-63697-9_17
12. Datta, N., Dutta, A., Dutta, K.: Improved security bound of (E/D)WCDM. IACR Trans. Symmetric Cryptol. **2021**(4), 138–176 (2021). https://doi.org/10.46586/tosc.v2021.i4.138-176
13. Datta, N., Dutta, A., Nandi, M., Paul, G.: Double-block hash-then-sum: A paradigm for constructing bbb secure prf. IACR Trans. Symmetric Cryptol. **2018**(3), 36–92 (2018). https://doi.org/10.13154/tosc.v2018.i3.36-92
14. Datta, N., Dutta, A., Nandi, M., Paul, G., Zhang, L.: Single key variant of pmac_plus. IACR Trans. Symmetric Cryptol. **2017**(4), 268–305 (2017). https://doi.org/10.13154/tosc.v2017.i4.268-305
15. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In: Advances in Cryptology - CRYPTO 2018. Proceedings, Part I. pp. 631–661 (2018). https://doi.org/10.1007/978-3-319-96884-1_21
16. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: sfdwcdm+: A BBB secure nonce based MAC. Adv. in Math. of Comm. **13**(4), 705–732 (2019). https://doi.org/10.3943/amc.2019042
17. Dutta, A., Nandi, M., Saha, A.: Proof of mirror theory for $\xi_{\max} = 2$. IEEE Transactions on Information Theory **68**(9), 6218–6232 (2022). https://doi.org/10.1109/TIT.2022.3171178
18. Dutta, A., Nandi, M., Talnikar, S.: Beyond birthday bound secure MAC in faulty nonce model. In: Advances in Cryptology - EUROCRYPT 2019, Proceedings, Part I. pp. 437–466 (2019). https://doi.org/10.1007/978-3-030-17653-2_15
19. Guo, C., Shen, Y., Wang, L., Gu, D.: Beyond-birthday secure domain-preserving prfs from a single permutation. Des. Codes Cryptogr. **87**(6), 1297–1322 (2019). https://doi.org/10.1007/s10623-018-0528-8
20. Hall, C., Wagner, D.A., Kelsey, J., Schneier, B.: Building prfs from prps. In: Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 370–389. Springer (1998). https://doi.org/10.1007/BFb0055742

21. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers. pp. 310–327 (2006). https://doi.org/10.1007/11799313_20
22. Iwata, T., Mennink, B., Vizár, D.: CENC is optimally secure. Cryptology ePrint Archive, Report 2016/1087 (2016), https://eprint.iacr.org/2016/1087
23. Iwata, T., Minematsu, K.: Stronger security variants of GCM-SIV. IACR Trans. Symmetric Cryptol. **2016**(1), 134–157 (2016). https://doi.org/10.13154/tosc.v2016.i1.134-157
24. Iwata, T., Minematsu, K., Peyrin, T., Seurin, Y.: ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In: Advances in Cryptology - CRYPTO 2017. Proceedings, Part III. pp. 34–65 (2017). https://doi.org/10.1007/978-3-319-63697-9_2
25. Jha, A., Nandi, M.: Tight security of cascaded lrw2 (2019), https://eprint.iacr.org/2019/1495
26. Kim, S., Lee, B., Lee, J.: Tight security bounds for double-block hash-then-sum macs. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12105, pp. 435–465. Springer (2020). https://doi.org/10.1007/978-3-030-45721-1_16
27. List, E., Nandi, M.: Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption. In: Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings. pp. 258–274 (2017). https://doi.org/10.1007/978-3-319-52153-4_15
28. List, E., Nandi, M.: ZMAC+ - an efficient variable-output-length variant of ZMAC. IACR Trans. Symmetric Cryptol. **2017**(4), 306–325 (2017). https://doi.org/10.13154/tosc.v2017.i4.306-325
29. Mennink, B.: Towards tight security of cascaded LRW2. In: Beimel, A., Dziembowski, S. (eds.) Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11240, pp. 192–222. Springer (2018). https://doi.org/10.1007/978-3-030-03810-6_8
30. Mennink, B., Neves, S.: Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In: Advances in Cryptology - CRYPTO 2017. Proceedings, Part III. pp. 556–583 (2017). https://doi.org/10.1007/978-3-319-63697-9_19
31. Moch, A., List, E.: Parallelizable macs based on the sum of prps with security beyond the birthday bound. In: Applied Cryptography and Network Security - 17th International Conference, ACNS 2019, Bogota, Colombia, June 5-7, 2019, Proceedings. pp. 131–151 (2019). https://doi.org/10.1007/978-3-030-21568-2_7
32. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017). https://doi.org/10.1007/978-3-319-49530-9
33. Naito, Y.: Full prf-secure message authentication code based on tweakable block cipher. In: Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings. pp. 167–182 (2015). https://doi.org/10.1007/978-3-319-26059-4_9
34. Naito, Y.: Blockcipher-based macs: Beyond the birthday bound without message length. 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 III. pp. 446–470 (2017). https://doi.org/10.1007/978-3-319-70700-6_16

35. Patarin, J.: Luby-rackoff: 7 rounds are enough for $2^{n(1\text{-epsilon})}$security. In: Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. pp. 513–529 (2003). https://doi.org/10.1.1.732.242
36. Patarin, J.: Security of random feistel schemes with 5 or more rounds. In: Franklin, M.K. (ed.) Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. Lecture Notes in Computer Science, vol. 3152, pp. 106–122. Springer (2004). https://doi.org/10.1007/978-3-540-28628-8_7
37. Patarin, J.: On linear systems of equations with distinct variables and small block size. In: Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers. pp. 299–321 (2005). https://doi.org/10.1007/11734727_25
38. Patarin, J.: The "coefficients H" technique. In: Selected Areas in Cryptography - SAC 2008. Revised Selected Papers. pp. 328–345 (2008). https://doi.org/10.1007/978-3-642-04159-4_21
39. Patarin, J.: A proof of security in o(2n) for the xor of two random permutations. In: Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings. pp. 232–248 (2008). https://doi.org/10.1007/978-3-540-85093-9_22
40. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. Cryptology ePrint Archive, Report 2010/287 (2010), https://eprint.iacr.org/2010/287
41. Patarin, J.: Security of balanced and unbalanced feistel schemes with linear non equalities. Cryptology ePrint Archive, Paper 2010/293 (2010), https://eprint.iacr.org/2010/293
42. Patarin, J.: Security in $o(2^n)$ for the xor of two random permutations - proof with the standard H technique. Cryptology ePrint Archive, Report 2013/368 (2013), https://eprint.iacr.org/2013/368
43. Schneier, B., Kelsey, J.: Unbalanced feistel networks and block cipher design. In: FSE. vol. 96, pp. 121–144 (1996)
44. Sorkin, A.: Lucifer, a cryptographic algorithm. Cryptologia **8**(1), 22–42 (1984). https://doi.org/10.1080/0161-118491858746
45. Yasuda, K.: The sum of CBC macs is a secure PRF. In: CT-RSA 2010. pp. 366–381 (2010). https://doi.org/10.1007/978-3-642-11925-5_25
46. Yasuda, K.: A new variant of PMAC: beyond the birthday bound. In: Advances in Cryptology - CRYPTO 2011. Proceedings. pp. 596–609 (2011). https://doi.org/10.1007/978-3-642-22792-9_34
47. Zhang, L., Wu, W., Sui, H., Wang, P.: 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In: ASIACRYPT 2012. pp. 296–312 (2012). https://doi.org/10.1007/978-3-642-34961-4_19
48. Zhang, P., Hu, H., Yuan, Q.: Close to optimally secure variants of GCM. Security and Communication Networks **2018**, 9715947:1–9715947:12 (2018). https://doi.org/10.1155/2018/9715947