Proof of Mirror Theory for any $\xi_{\max}$

Benoît Cogliati[1] and Avijit Dutta[2] and Mridul Nandi[3] and Jacques Patarin[4,5] and Abishanka Saha[3]

[1] CISPA Helmholtz Center for Information Security, Saabrücken, Germany
[2] Institute for Advancing Intelligence, TCG-CREST, Kolkata, India
[3] Indian Statistical Institute, Kolkata, India
[4] Laboratoire de Mathématiques de Versailles, Versailles, France
[5] Thales DIS France SAS, Meudon, 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 $X_1, X_2, \ldots, X_q$ are pairwise distinct is either 0 or greater than the average over all $\lambda_{i,j}$ values in $\{0,1\}^n$. This result is known as "$P_i \oplus P_j$ *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 block cipher-(or even ideal permutation-) based designs. Unfortunately, the proof of the result contains gaps which are non-trivial to fix. In this work, we present the first complete proof of the $P_i \oplus P_j$ for any $\xi_{\max}$ theorem. As an illustration of our result, we also revisit the security proofs of two optimally secure blockcipher-based pseudorandom functions, and provide updated security bounds. Our result is actually more general in nature as we consider equations of the form $X_i \oplus X_j = \lambda_k$ over a commutative group $\mathscr{G}$ under addition, and of exponent 2.

1 Introduction

Pseudorandom Function (PRF) and Pseudorandom Permutation (PRP) are two fundamental cryptographic objects in symmetric key cryptography. An enormous use of pseudorandom functions in designing cryptographic schemes e.g., authentication protocols, encryption schemes, hash functions etc. make it a valuable object from the cryptographic view points. However, practical candidates of PRF are very scarce. On the other hand, PRP or block ciphers are available in plenty in practice. One can consider a block cipher 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 block cipher is n-bits, then one can consider the block cipher to be a secure PRF until the number of queries reaches to $2^{n/2}$. Such a bound is acceptable when n is moderately large, e.g., 128 bits. However, due to the ongoing trend of lightweight cryptography, a number of lightweight block ciphers have been designed with smaller block size e.g., 64

bits. In such a situation, a block cipher 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 that

Can we design a pseudorandom function out of lightweight block ciphers 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 [3,19,21,9,18,43,44,45,35,13,12,22]. Out of several such designs, *xor of two pseudorandom permutations* is the most popular one, where the output of two pseudorandom permutations on the same input is xored together to produce the output. We refer to this construction as **Sum function**.

History of Sum function: In [3], Bellare et al. have first proposed the *sum function* in the name of *Luby-Rackoff backwards*, defined as: $\mathsf{XOR}_2(x) := \mathsf{E}_{k_1}(x) \oplus \mathsf{E}_{k_2}(x)$. [6] However, the authors of [3] did not give the security analysis of XOR_2 and its single-keyed variant $\mathsf{XOR}_1(x) := \mathsf{E}_k(0\|x) \oplus \mathsf{E}_k(1\|x)$. Popularity of these constructions have started gaining attention in the cryptographic community in the last few years due to their use in many important block cipher and tweakable block cipher-based designs that includes constructions like [43,44,45,35,13,12,23,27,20,17,22,34,26]. In an unpublished work [2], Bellare et al. first showed that XOR_1 is a secure PRF up to $2^n/n$ queries. In [28], Lucks proved that XOR_2 achieves $2n/3$ bit PRF security. Afterwards, in a series of papers [40,41,42], Patarin claimed that XOR construction (i.e., both XOR_1 and XOR_2) is secured up to $O(2^n)$ queries. In 2017, Dai et al. [10] have shown that XOR_1 and XOR_2 are optimally secure PRFs using the χ^2-method. In a related work, Cogliati et al. [7] have shown that XOR_k, i.e., xor of k independent permutations, for $k \geq 2$, achieves $kn/(k+1)$-bit PRF security.

Following Patarin's analysis, XOR_2 (resp. XOR_1) 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 (for the XOR_1 construction, we additionally require that $\lambda_1, \ldots, \lambda_q$ are non-zero n-bit binary strings). The entire security analyses for both the constructions stand on finding a good lower bound on the number of solutions $(P_1, \ldots, P_{2q})$ [7] to $\mathbb{E}_\lambda$ such that (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 (a) $P_i \neq P_j$ for $i \neq j$, where i, j both are odd, and (b) $P_x \neq P_y$ for $x \neq y$, where x and y both are 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,

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

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

assigning value to a single variable P_i can fix the values of $k \geq 2$ variables in the set of equations. Patarin [41] 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 establish 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** $\xi_{\max} = 2$ [38] (and later in [41], named *Mirror theory* the study of sets of linear equalities and non-equalities in finite groups). This result was stated as a conjecture in [36] and proved in [38]. The result has been acknowledged in the community as a potential and a strong approach to establish the optimal security of XOR constructions (i.e., XOR_1 and XOR_2) [10]. Informally, the result *Theorem* $P_i \oplus P_j$ for $\xi_{\max} = 2$ states the following: let $q \leq 2^n/134$ and $\lambda_1, \ldots, \lambda_q$ be non-zero n-bit strings. Then, the number of solutions of distinct values to $P_1, \ldots, P_{2q}$ satisfying the bivariate affine equations $\mathbb{E}_\lambda$ is at least $\frac{(2^n)^{\underline{2q}}}{2^{nq}}$, where $a^{\underline{b}} := a(a-1)\cdots(a-b+1)$ for two positive integers $a \geq b$. Patarin [40] also showed that for any choice of n-bit strings $\lambda_1, \lambda_2, \ldots, \lambda_q$, the number of solutions to the system of bivariate affine equations $\mathbb{E}_\lambda$ such that $P_1, P_3, \ldots, P_{2q-1}$ are distinct and $P_2, P_4, \ldots, P_{2q}$ are distinct is at least $(2^n)^{\underline{q}}\big)^2/2^{nq} \times (1 - O(q/2^n))$. Beside these two results, Patarin [38] also claimed the generic result for a general $\xi_{\max} > 2$, that the number of distinct solutions to a system of q bivariate affine equations with $\xi_{\max} > 2$ and with non-equality among the variables is always larger than the average number of solutions provided $q \leq 2^n/67.(\xi_{\max} - 1)$. Patarin named this result the "*Theorem* $P_i \oplus P_j$ *for any* $\xi_{\max}$". This result was stated as a conjecture (Conjecture 8.1 of [36]) 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 [38,40,41,42] 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 recently reported in multiple works [6,10,14,24,29]. 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 application in proving the optimal security bound for Feistel schemes [37,33], and several blockcipher and tweakable blockcipher-based schemes such as XORP [20,21], EDM [9,30], or 2k-HtmB-p2 [6]. 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 the last 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 to 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). Let $\mathscr{G}$ be a commutative group under addition $+$ with 0 as the additive identity. Additionally, we require $\mathscr{G}$ to be of exponent 2. This means that all the elements of $\mathscr{G}$ are their own inverses, and that the operations $+$ and $-$ are equivalent. We chose to differentiate them (instead of replacing them by a common symbol such as $\oplus$) in order to emphasize more clearly why this condition is needed in our proof. We denote $|\mathscr{G}| = N$ and $\lceil \log_2 N \rceil = n$. 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 by removing S from γ. We similarly write γ_{+T} to denote the multiset 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 $\gamma^{[\alpha]}$. In this paper we consider set-system γ of non-empty subsets of $\mathscr{G}$.

1.1.1 System of Difference Equations Consider a system of difference equations $AX = \Lambda$ over the group $\mathscr{G}$, where $A = (A_{ij})_{i\in[m],j\in[e]}$ is a $m \times e$ matrix with full row rank (and hence consistent), such that each row contains exactly one $+1$, one -1 and remaining zeros, X is a $e \times 1$ vector of variables and $\Lambda \in \mathscr{G}^m$. As the column sum is zero, we must have $m < e$. Note that each equation in the above system is of the form $X_i - X_j = \lambda_k$ for some i, j, k with $i \neq j$. A solution $x^e \in \mathscr{G}^e$ of the above system is called a *pairwise distinct solution*, or in short a p.d. solution if $x_i \neq x_j$ for $i \neq j \in [e]$. The number of solutions of the system of equations is exactly N^{e-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. When we consider $\mathscr{G} = \{0,1\}^n$ under bitwise xor operation, this leads to the classical mirror theory widely used in cryptography.

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 $G = (V := [e], E, L)$ where the edge set $E = \{(j,k) \in V^2 \mid \exists i \in (m] \ni |A_{ij}| = |A_{ik}| = 1\}$ and $L(j,k) = \lambda_i$ if $A_{jk} = 1$, or $L(j,k) = -\lambda_i$ if $A_{jk} = -1$. So, whenever there is an edge between j and k, we have directed edges in the 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 $m = e - q$. Given a directed path P from j to k, the equation $X_j - X_k = \sum_{e \in P} L(e)$ 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 system of equations corresponding to a component is of the form

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

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

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 block cipher and tweakable

block cipher-based designs that includes [43,44,45,35,13,12]. However, the security proofs of most of these designs require a degeneration of the final outputs to get rid of the adaptive nature of the adversary. Hence the proof cannot use the fact that the sum function is a PRF. Instead, these security proofs require (by application of the H-Coefficient technique [39]) 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 [14,15,17,31,4]. Mennink [30] showed the optimal security bound of EWCDM using this result as the primary underlying tool, and Iwata et al. [21] 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 $\xi_{\max}$" [38,41], several authors have used this precarious result to derive an optimal bound for some constructions such as [21,30,46]. 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

Besides the applicability of the Theorem $P_i \oplus P_j$ for general $\xi_{\max}$ in cryptographic paradigms, the result of "*Theorem* $P_i \oplus P_j$ *for* $\xi_{\max} = 2$" have 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 [38,41,33,16,8]. In [42], [7] and [16], 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 [24], with an application to the security of the CLRW construction. Mirror Theory has also been considered for nonce-based MACs that rely on an underlying blockcipher or tweakable blockciphers, such as in [14,15,17,31,25]. 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 of the enormous use of the result, its correctness was a subject to debate [10]. In [25], Kim et al. have given a verifiable proof of the mirror theory until the number of equations falls below the bound $2^{3n/4}$. Datta et al. [11] have extended this result for a system of bivariate affine equations and non-equations. Recently, Dutta et al. [16] and Cogliati and Patarin [8] have independently given a verifiable proof of the mirror theory for $\xi_{\max} = 2$.

Organization. In Sect.2, we have proved 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 Section 3.1. The proof of the Proposition requires a recursive inequality

lemma, proof of which is deferred in Sect.A.2. Then, Section 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 Section 5.

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:

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

along with the following probability:

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

where $\mathsf{R}_1, \ldots, \mathsf{R}_\alpha \leftarrow\!\!\$\, \mathscr{G}$. 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 $\gamma'_i = \gamma_i + a_i$ for $a_1, \ldots, a_\alpha \in \{0,1\}^n$.

Theorem 1 can be rephrased in the following way.

Theorem 1' (Equivalent Formulation) *Let $\mathscr{G}$ be a commutative group under addition of order $|\mathscr{G}| = N$, and of exponent 2. Let γ be a set-system of elements of $\mathscr{G}$ such that $\xi_{\max} = \|\lambda\|_{\max}$. 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 Section 2.1. From a high level, the proof of Theorem 1' works in two steps:

1. if λ is small ($\|\lambda\| \leq \sqrt{N}$), then simple calculations show that Theorem 1' holds;

2. otherwise, we prove that, for a well-chosen $a \in T \in \lambda$, one has

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

where λ' corresponds to λ, where the set T has been replaced with $T \setminus \{a\}$; clearly, applying point 2 repeatedly until $\|\lambda\| \leq \sqrt{N}$ allows us to conclude the proof of Theorem 1'.

Intuitively, the element that we remove from λ is the one that corresponds, in the associated system of equations, to the λ'_i that appears with maximum multiplicity.

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

$$\delta_\gamma(z) := \sum_{S \in \gamma} \delta_S(z), \quad \Delta_\gamma := \max_{z \in \mathscr{G}} \delta_\gamma(z).$$

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 $\sqrt{N} \leq \|\lambda\| \leq N/12\xi^2_{\max}$ where $\xi_{\max} = \|\lambda\|_{\max}$. Suppose the maximum Δ_λ is attained for $a - b$ with $\{a, b\} \subseteq T \in \lambda$. Then,*

$$\mathsf{P}(\lambda) \geq \left(1 - \frac{\|\lambda\| - 1}{2^n}\right) \cdot \mathsf{P}(\lambda_{-a|T})$$

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 disjointness 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 $X_j - X_{i_C} = \lambda_k$ 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 set of all 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 $S_{C_j} + r_j$ 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 $S_{C_j} + r_j$'s, we can define x^e consisting of all values from the set $\sqcup_j (S_{C_j} + r_j)$ 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 $(\gamma_i + r_i)$'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 $e - q = m$ 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

$$\mathsf{P}(\gamma) = \mathsf{P}(\gamma_{-S}) \times \left(1 - \frac{\|\gamma\| - 1}{2^n}\right) \qquad \text{if } |S| = 1 \tag{1}$$

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

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.

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

$$\frac{\mathsf{P}(\lambda)}{\mathsf{P}(\gamma)} \geq \left(1 - \frac{q\xi_{\max}^2}{N}\right)^{|\lambda \setminus \gamma|}. \tag{3}$$

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

Let us write $W_i := (1 - \frac{i}{N})$. Now we claim that

$$\left(1 - \frac{|S| \times \|\gamma_{-S}\|}{2^n}\right) \geq \prod_{i=\|\gamma_{-S}\|}^{\|\gamma\|-1} W_i \tag{4}$$

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 the Eq. 4. It is sufficient to show that

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

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

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

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

Now we assume that $\sqrt{N} \leq \|\lambda\| \leq N/12\xi_{\max}^2$. 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 $\{x_i, y_i\} \subseteq T_i \in \gamma^{(i)}$ such that $x_i - y_i$ attains the highest multiplicity in $\gamma^{(i)}$, $\Delta_{\gamma^{(i)}}$. We choose one arbitrarily if there exists more than one choice. We define $\gamma^{(i+1)} := \gamma^{(i)}_{-x_i|S_i}$. We now apply Proposition 1 for every $i \in [\sigma - 1]$ and obtain

$$\mathsf{P}(\gamma) \geq \mathsf{P}(\gamma^{(\sigma)}) \prod_{i=1}^{\sigma} \left(1 - \frac{\|\gamma\| - i}{2^n}\right).$$

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

3 Proof of Proposition 1

Notations and Conventions. In the Proposition statement, $\{a, b\} \subseteq T \in \lambda$ and $\Delta_\lambda = \sum_{S \in \lambda} \delta_S(a - b)$. 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 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 $y + \mathsf{R}_i = x + \mathsf{R}_1$. As $(S \setminus x) + \mathsf{R}_1$ is disjoint from $S' + \mathsf{R}_i$ (same as $S' + (x - y + \mathsf{R}_1)$), $S \setminus x$ should be disjoint from $S' + x - y$. Let

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

Note that simultaneously $\mathsf{R}_1 + x = \mathsf{R}_i + y = \mathsf{R}_j + y'$ 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 $S_1 = (\delta + S') \sqcup (S \setminus x)$. The factor $1/N$ appears as $\mathsf{R}_1 = \mathsf{R}_i + \delta$ needs to hold which is independent of disjointness of $\gamma_{-S-S'+S_1}$ (which does not involve S' and hence R_i). Note that, in previous proof strategies, the first recursive equation to be introduced was the so-called orange equation. Roughly speaking, this corresponds to 2 applications of our link-deletion equation, which is why we can also refer to Equation (5) as the *half-orange equation*.

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 3.2).
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 is 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 3.4 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 lead to a more complicated analysis.

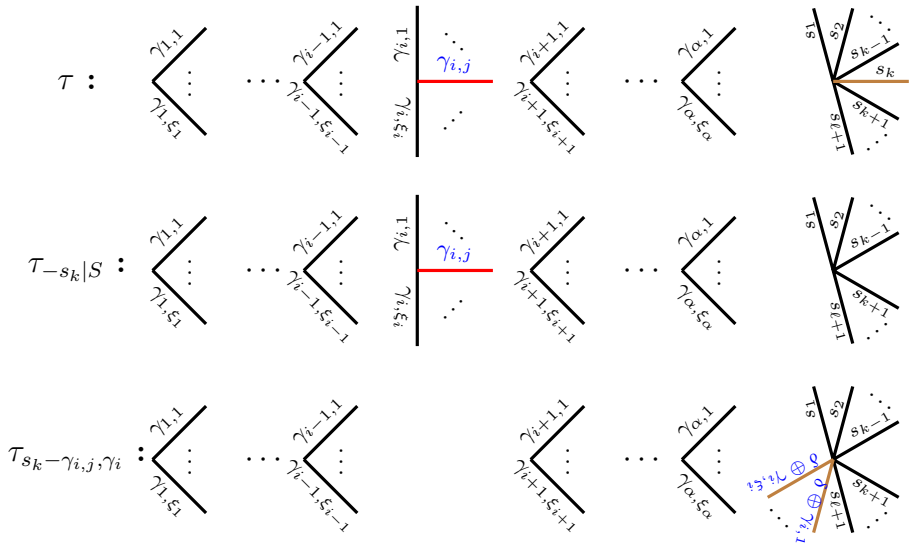

Fig. 3.1: Graphical depiction of the link-deletion operation. Here, we have represented graphs corresponding to the three types of terms appearing in the link-deletion equation, with $x = s_k$, $y = \gamma_{i,j}$, $\delta = s_k - \gamma_{i,j}$, $S = \{s_1, \ldots, s_{\ell+1}\}$, and $S' = \gamma_{i,j}$.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

3.2 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 $\delta_S(a-b)$ many 2-sets $\{w_1, w_2\} \subseteq S$ such that $w_1 - w_2 = a - b$ and hence $b = w_2 + (a - w_1) \in S + (a - w_1)$. So, $(a - w_1, S) \notin I_{a|T}$. So,

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

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

Remark 2. Note that this is where we use the hypothesis that $\mathscr{G}$ is of exponent 2. We exhibit a simple counter-example when this is not the case. Take for example

$\mathscr{G} = \mathbb{Z}/6\mathbb{Z}$, and $T = \{0, 2, 4\}$. Then one has $\delta_T(2) = 3 = |T|$. Note that, as we will see in Section 3.4, the condition $\delta_T(a-b) \leq |T| - 1$ is required to conclude the proof of Proposition 1. This hints that either the case where the exponent of $\mathscr{G}$ is greater than 3 is fundamentally different from our case, or that our current proof strategy can still be tightened.

3.3 Recursive Inequality of D-Terms

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

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

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

where the maximum is taken over all choices of $\gamma \subseteq \lambda$ of size α, $S \in \gamma$ and a set $\mathcal{S}$ 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 3. 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 $\mathcal{S}$ 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 initial bound:

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

and so

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

3.4 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 $a_{d,k} := 0$ for all $k < 0$ and for all $0 \leq d \leq \xi n$ and $0 \leq \ell_i \leq \xi - 1$ for $i \in [q]$, we have*

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

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

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 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 3.4. 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 3.4. 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

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

Thus, one has

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

where $C' = 9(\xi_{\max}^2 + 1)$, as $\Delta \geq 1$. Hence $\mathsf{P}(\lambda_{\delta,S}) \leq (1 + C'\Delta/N)\,\mathsf{P}(\lambda_{-a|T})$. Using this bound in the appropriate link deletion equation we have:

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

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

Remark 4. Note that the initial bound ensures only that $a_{0,\ell} \leq 1$. However, the presence of recursive inequality forces the value of $a_{0,\ell}$ to be very small.

4 Cryptographic Applications

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, based on a secret random permutation π. 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:

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

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. 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 F and \$. 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 ([39]). *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 permutation π. We now illustrate this technique by revisiting existing security proofs using Theorem 1.

4.2 The XORP Construction

In [20], 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 [21] made the link between XORPand Mirror Theory explicit, and proved optimal security for the construction, using [41, Theorem 6]. We revisit their proof by applying Theorem 1 in order to demonstrate the following result[8].

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*

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

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

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

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

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

– 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:

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

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.

Remark 5. Note that there exists another proof of optimal security for the XORP construction [5], that does not rely on Mirror Theory. Instead, it uses the so-called χ^2 technique [10].

4.3 Optimally Secure Variable-Input-Length PRFs

In [6], 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 [1]. The most efficient variant, whose representation can be found in Figure 4.1, relies on two independent permutations, and its security proof [6, 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

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

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.

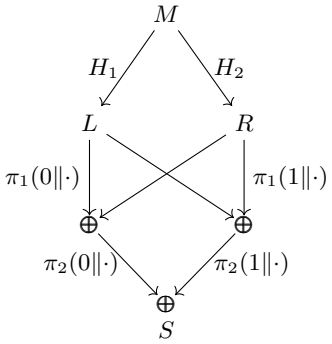

Fig. 4.1: Representation of the 2k-HtmB-p2$[H]$ based on two uniformly random and independent n-bit permutations π_1, π_2. An edge (u, v) with label g denotes the mapping $v = g(u)$. Unlabelled edges are identity mapping. The inputs to the functions $\pi_i(j\|\cdot)$ are first truncated before the application 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 [6, Theorem 7.3] where [41, 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.[9]

In [6], 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

$$\frac{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{real}} = \tau\right)}{\mathsf{Pr}\left(\mathrm{T}_{\mathrm{ideal}} = \tau\right)} = \frac{N2^{nq}}{(2^n)^{\underline{q_X+q_Y}}} \geq 1, \tag{14}$$

where N 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.

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 $\xi_{\max}$. As an application, we give proofs of n-bit security for the XORP and 2k-HtmB-p2 constructions, thus confirming the results from [21] and [6]. Theorem 1 could also be used to revisit the security proofs of balanced Feistel schemes [33] and prove the optimal security of six rounds Feistel

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

scheme [33]. However, the H coefficients technique can be used to transform cryptographic security proofs into Mirror Theory problems that can be more general than the one we target in this work. As a consequence, studying generalizations of Theorem 1 would help to improve security bounds for current and future cryptographic constructions. Moreover, using our result, one can also show an asymptotically optimal security bound for DWCDM [14,15] construction albeit the analysis of some more complicated bad events like bounding an alternating path of length more than ξ or a valid cycle of length more than ξ etc., where ξ is a predefined threshold.

Acknowledgements

This work was carried out in the framework of the French-German-Center for Cybersecurity, a collaboration of CISPA and LORIA.

References

1. William Aiello and Ramarathnam Venkatesan. Foiling birthday attacks in length-doubling transformations - benes: A non-reversible alternative to feistel. In *Advances in Cryptology - EUROCRYPT '96. Proceeding*, pages 307–320, 1996.
2. Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. *IACR Cryptology ePrint Archive*, 1999:24, 1999.
3. Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, pages 266–280, 1998.
4. Arghya Bhattacharjee, Avijit Dutta, Eik List, and Mridul Nandi. Cencpp* - beyond-birthday-secure encryption from public permutations. Cryptology ePrint Archive, Report 2020/602, 2020.
5. Srimanta Bhattacharya and Mridul Nandi. Revisiting variable output length xor pseudorandom function. *IACR Transactions on Symmetric Cryptology*, 2018(1):314–335, Mar. 2018.
6. Benoît Cogliati, Ashwin Jha, and Mridul Nandi. How to build optimally secure prfs using block ciphers. In Shiho Moriai and Huaxiong Wang, editors, *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*, volume 12491 of *Lecture Notes in Computer Science*, pages 754–784. Springer, 2020.
7. Benoit Cogliati, Rodolphe Lampe, and Jacques Patarin. 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*, pages 285–302, 2014.
8. Benoît Cogliati and Jacques Patarin. Mirror theory: A simple proof of the pi+pj theorem with xi_max=2. *IACR Cryptol. ePrint Arch.*, 2020:734, 2020.

9. Benoît Cogliati and Yannick Seurin. EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In *CRYPTO 2016, Proceedings, Part I*, pages 121–149, 2016.
10. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 497–523, 2017.
11. Nilanjan Datta, Avijit Dutta, and Kushankur Dutta. Improved security bound of (E/D)WCDM. *IACR Trans. Symmetric Cryptol.*, 2021(4):138–176, 2021.
12. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: A paradigm for constructing bbb secure prf. *IACR Trans. Symmetric Cryptol.*, 2018(3):36–92, 2018.
13. Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of pmac_plus. *IACR Trans. Symmetric Cryptol.*, 2017(4):268–305, 2017.
14. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-key beyond birthday secure nonce-based MAC. In *Advances in Cryptology - CRYPTO 2018. Proceedings, Part I*, pages 631–661, 2018.
15. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. sfdwcdm+: A BBB secure nonce based MAC. *Adv. in Math. of Comm.*, 13(4):705–732, 2019.
16. Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of mirror theory for $\xi_{\max} = 2$. Cryptology ePrint Archive, Report 2020/669, 2020.
17. Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure MAC in faulty nonce model. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 437–466, 2019.
18. Chun Guo, Yaobin Shen, Lei Wang, and Dawu Gu. Beyond-birthday secure domain-preserving prfs from a single permutation. *Des. Codes Cryptogr.*, 87(6):1297–1322, 2019.
19. Chris Hall, David A. Wagner, John Kelsey, and Bruce Schneier. Building prfs from prps. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 370–389. Springer, 1998.
20. Tetsu Iwata. 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*, pages 310–327, 2006.
21. Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is optimally secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.
22. Tetsu Iwata and Kazuhiko Minematsu. Stronger security variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2016(1):134–157, 2016.
23. Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 34–65, 2017.
24. Ashwin Jha and Mridul Nandi. Tight security of cascaded lrw2. Cryptology ePrint Archive, Report 2019/1495, 2019. `https://eprint.iacr.org/2019/1495`.
25. Seongkwang Kim, ByeongHak Lee, and Jooyoung Lee. Tight security bounds for double-block hash-then-sum macs. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May*

10-14, 2020, Proceedings, Part I, volume 12105 of *Lecture Notes in Computer Science*, pages 435–465. Springer, 2020.
26. Eik List and Mridul Nandi. 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*, pages 258–274, 2017.
27. Eik List and Mridul Nandi. ZMAC+ - an efficient variable-output-length variant of ZMAC. *IACR Trans. Symmetric Cryptol.*, 2017(4):306–325, 2017.
28. Stefan Lucks. The sum of prps is a secure PRF. In *EUROCRYPT 2000*, pages 470–484, 2000.
29. Bart Mennink. Towards tight security of cascaded LRW2. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 192–222. Springer, 2018.
30. Bart Mennink and Samuel Neves. Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In *Advances in Cryptology - CRYPTO 2017. Proceedings, Part III*, pages 556–583, 2017.
31. Alexander Moch and Eik List. 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*, pages 131–151, 2019.
32. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.
33. Valérie Nachef, Jacques Patarin, and Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017.
34. Yusuke Naito. 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*, pages 167–182, 2015.
35. Yusuke Naito. 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*, pages 446–470, 2017.
36. Jacques Patarin. 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*, pages 513–529, 2003.
37. Jacques Patarin. Security of random feistel schemes with 5 or more rounds. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.
38. Jacques Patarin. 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*, pages 299–321, 2005.
39. Jacques Patarin. The "coefficients H" technique. In *Selected Areas in Cryptography - SAC 2008. Revised Selected Papers*, pages 328–345, 2008.

40. Jacques Patarin. A proof of security in o(2n) for the xor of two random permutations. In *Information Theoretic Security, Third International Conference, ICITS 2008, Calgary, Canada, August 10-13, 2008, Proceedings*, pages 232–248, 2008.
41. Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.
42. Jacques Patarin. Security in o(2^{n}) for the xor of two random permutations \\ - proof with the standard H technique -. *IACR Cryptology ePrint Archive*, 2013:368, 2013.
43. Kan Yasuda. The sum of CBC macs is a secure PRF. In *CT-RSA 2010*, pages 366–381, 2010.
44. Kan Yasuda. A new variant of PMAC: beyond the birthday bound. In *Advances in Cryptology - CRYPTO 2011. Proceedings*, pages 596–609, 2011.
45. Liting Zhang, Wenling Wu, Han Sui, and Peng Wang. 3kf9: Enhancing 3gpp-mac beyond the birthday bound. In *ASIACRYPT 2012*, pages 296–312, 2012.
46. Ping Zhang, Honggang Hu, and Qian Yuan. Close to optimally secure variants of GCM. *Security and Communication Networks*, 2018:9715947:1–9715947:12, 2018.

A Postponed Proofs

A.1 Proof of Lemma 2

We fix $S \in \gamma \subseteq \lambda$ where $|\gamma| = \alpha$ and a set $\mathcal{S}$ with $|\mathcal{S}| = \ell + 1$ disjoint with S. Let $\tau := \gamma_{+\mathcal{S}}$ and $\tau' := \gamma_{-S+(S \sqcup \mathcal{S})}$. In words, γ is a set-system that is included in λ, $\mathcal{S}$ is any subset of $\mathcal{G}$ of size $\ell + 1$, and S is an element of γ. Then, τ corresponds to the $\gamma \cup \{\mathcal{S}\}$, while τ' corresponds to τ after S and $\mathcal{S}$ have been merged. Looking back at Fig. 3.1, τ and τ' would correspond respectively to the second and third graphs. We assume that $\gamma, \mathcal{S}, S$ 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 $|\mathcal{S}| = 1$. In this case, let $\mathcal{S} = \{x\}$. Then $\mathsf{P}(\tau) = \mathsf{P}(\gamma) \cdot (1 - \|\gamma\|/2^n)$ from Eq. (1). Also $\tau'_{-x|S \sqcup \mathcal{S}} = \gamma$. 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 $I := I_{x,S} = \{(\delta, S') : x - \delta \in S' \in \gamma_{-S}, S' + \delta \text{ is disjoint with } S\}$. For $z' \in S' \in \gamma_{-S}$, $(x - z, S') \notin I$ if and only if there exists $y \in S$ and $w \in S'$ such that $x - y = z - w$. Thus $|I| \geq \sum_{S' \in \gamma_{-S}} \left(|S'| - \sum_{y \in S} 2\delta_{S'}(x - y) \right) =$

$\|\gamma\| - |S| - \sum_{y\in S} 2\delta_{\gamma-S}(x-y) \geq \|\gamma\| - \|\gamma\|_{\max} \cdot 2\delta_\gamma$. Hence

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

where the last term in $(\star)$ is obtained from Eq. (3).

Case $|\mathcal{S}| \geq 2$. Fix $x \in \mathcal{S}$. By link-deletion equation, we have

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

where

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

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

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

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

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

Hence, we have the following:

$$
\begin{aligned}
D(\alpha,\ell) &= |\mathsf{P}(\tau) - \mathsf{P}(\tau')| \\
&\le \left|\mathsf{P}(\tau_{-x}) - \mathsf{P}(\tau'_{-x})\right| + N^{-1} \sum_{(\delta,S')\in I'} \left|\mathsf{P}(\tau_{\delta,S'}) - \mathsf{P}(\tau'_{\delta,S'})\right| \\
&\qquad + \sum_{(\delta,S')\in I\setminus I'} \mathsf{P}(\tau_{\delta,S'})/N \\
&\le D(\alpha,\ell-1) + \frac{\|\gamma\setminus S\|_{\max}}{N} \sum_{S'\in\gamma\setminus S} D(\alpha-1,\ell+|S'|-1) \\
&\qquad + \frac{2\Delta_\gamma \|\gamma\|_{\max}\cdot \mathsf{P}(\lambda)}{N\left(1-\frac{\|\lambda\setminus\gamma\|_{\max}\times\|\gamma\|}{N}\right)^{|\lambda\setminus\gamma|}}. \qquad (15)
\end{aligned}
$$

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 bound,

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

Now, taking upper bounds of the total size terms, and adding some positive terms, the inequality, Eq. (15) 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

$$
\binom{m}{j} \le \frac{m^j}{j!} \le (em/j)^j. \qquad (16)
$$

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

We state the following claim, which follows from iterated applications of the recursive inequality. A proof of the claim is deferred to the end of this section.

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

$$
a_{0,\ell} \le \sum_{k=\lceil\frac{d-\ell}{\xi}\rceil}^{d} \binom{d}{k} \sum_{i^k\in[q]^k} a_{k,k+\sum_{j=1}^k \ell_{i_j}-d} + C\sum_{i=0}^{d-1}\sum_{j=\lceil\frac{i-\ell}{\xi}\rceil}^{i} \binom{i}{j}(4\xi e)^{-j}. \qquad (17)
$$

Proof of Lemma 3.4: 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 $\xi k < i \leq \xi(k+1)$, $k \in (n-1]$, $j \geq \lceil \frac{i-\ell}{\xi} \rceil \geq k$, and hence

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

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

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

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

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

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

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