

Building PRFs from TPRPs: Beyond the Block and the Tweak Length Bounds

Wonseok Choi¹, Jooyoung Lee² and Yeongmin Lee²

¹ Purdue University, West Lafayette, IN, USA

wonseok@purdue.edu

² KAIST, Daejeon, Korea

{hicalf,dudals4780}@kaist.ac.kr

Abstract. A secure n -bit tweakable block cipher (TBC) using t -bit tweaks can be modeled as a tweakable uniform random permutation, where each tweak defines an independent random n -bit permutation. When an input to this tweakable permutation is fixed, it can be viewed as a perfectly secure t -bit random function. On the other hand, when a tweak is fixed, it can be viewed as a perfectly secure n -bit random permutation, and it is well known that the sum of two random permutations is pseudorandom up to 2^n queries.

A natural question is whether one can construct a pseudorandom function (PRF) beyond the block and the tweak length bounds using a small number of calls to the underlying tweakable permutations. A straightforward way of constructing a PRF from tweakable permutations is to xor the outputs from two tweakable permutations with c bits of the input to each permutation fixed. Using the multi-user security of the sum of two permutations, one can prove that the $(t + n - c)$ -to- n bit PRF is secure up to 2^{n+c} queries.

In this paper, we propose a family of PRF constructions based on tweakable permutations, dubbed XoTP $_c$, achieving stronger security than the straightforward construction. XoTP $_c$ is parameterized by c , giving a $(t + n - c)$ -to- n bit PRF. When $t < 3n$ and $c = \frac{t}{3}$, XoTP $_{\frac{t}{3}}$ becomes an $(n + \frac{2t}{3})$ -to- n bit pseudorandom function, which is secure up to $2^{n + \frac{2t}{3}}$ queries. It provides security beyond the block and the tweak length bounds, making two calls to the underlying tweakable permutations.

In order to prove the security of XoTP $_c$, we extend Mirror theory to $q \gg 2^n$, where q is the number of equations. From a practical point of view, our construction can be used to construct TBC-based MAC finalization functions and CTR-type encryption modes with stronger provable security compared to existing schemes.

Keywords: Mirror theory · pseudorandom function · tweakable block cipher · sum of permutations

1 Introduction

CONSTRUCTING PRFS FROM PRPS. A block cipher is typically modeled as a pseudorandom permutation (PRP) in a provable security setting: any adversary should not be able to distinguish the block cipher from a truly random permutation by making a certain number of encryption and decryption queries in a black-box manner. However, for some modes of operation, one might want the block cipher to behave like a pseudorandom function (PRF). For example, a counter mode generates a keystream

$$E_K(N \parallel 0), E_K(N \parallel 1), E_K(N \parallel 2), \dots$$

using a block cipher E with a secret key K and a nonce N . In this mode of operation, all the blocks are pairwise distinct, allowing an adversary to distinguish it from a truly random keystream. For this reason, the counter mode is proved to be secure only up to the birthday bound (in the assumption that E is a pseudorandom permutation). This observation motivates the problem of constructing a pseudorandom function from pseudorandom permutations. Sometimes this problem is called “Luby-Rackoff backward” [BKR98]: the Feistel network transforms a set of (not necessarily one-to-one) functions into a permutation, and this problem considers its opposite direction.

A natural way of building a PRF by using PRPs is to xor two independent pseudorandom permutations. Given two n -bit (keyed) PRPs P and P' , their sum, denoted XoP, maps $X \in \{0, 1\}^n$ to

$$\text{XoP}(X) \stackrel{\text{def}}{=} P(X) \oplus P'(X).$$

Alternatively, one can simply truncate outputs from a single permutation. This construction, denoted TRP, maps $X \in \{0, 1\}^n$ to

$$\text{TRP}_m(X) \stackrel{\text{def}}{=} \text{Tr}_m(P(X))$$

where m is a positive integer such that $m < n$, and Tr_m is a truncation function that takes an n -bit string and returns leftmost m bits of the input. There has been a significant amount of research on these constructions [BI99, BKR98, BN18, CLL19, DHT17, GGM18, GM20, HWKS98, Lee17, Pat08a, Pat10a].

TWEAKABLE BLOCK CIPHERS. Tweakable block ciphers (TBC), first introduced in [LRW02], are a generalization of standard block ciphers that accept extra inputs called *tweaks*. The tweak, providing inherent variability to the block cipher, makes it easy to design various higher level cryptographic schemes such as message authentication codes and modes of operation.

Tweakable block ciphers can either be designed from scratch [Cro00, FLS⁺10, SO98], or be built upon off-the-shelf cryptographic primitives such as block ciphers and (public) permutations [CLS15, LST12, Men16, Nai17]. Recently, a unified vision for the tweak and key inputs has been proposed within the TWEAKEY framework [JNP14]. Skinny [BJK⁺16] and Deoxys-BC [JNPS16] follow this framework. Theoretically, a secure TBC is modeled as a tweakable pseudorandom permutation (TPRP); when a key is chosen uniformly at random and kept secret, the keyed TBC should behave like an independent random permutation for each tweak. The ideal counterpart of a TPRP is called a *tweakable uniform random permutation* (TURP).

BUILDING PRFs FROM TPRPs. As tweakable block ciphers are widely used and studied, it is natural to ask how to efficiently construct a PRF on top of a tweakable block cipher. The underlying tweakable block cipher being modeled as an n -bit TURP using t -bit tweaks, denoted \tilde{P} , a straightforward construction is to fix a message input to \tilde{P} , obtaining a t -to- n bit function. Then such a construction is perfectly secure for every possible query; it is secure up to 2^t queries. On the other hand, one can obtain a perfectly random n -bit permutation by fixing a tweak input to \tilde{P} . This construction is secure only up to the birthday bound. By summing two distinct permutations (using different tweaks), one can obtain a pseudorandom function that is secure up to 2^n queries [Pat08a].

Our research is motivated by the following question: how can one construct pseudorandom functions that make a small number of calls to the underlying TPRPs, providing security beyond the block and the tweak length bounds? We note that a TBC-based Feistel cipher provides such a strong security bound with at least 10 rounds, using that many tweakable block cipher calls [SGW20].

We will consider two PRF constructions using only two calls to the underlying TPRPs

$$\tilde{P} : \{0, 1\}^t \times \{0, 1\}^n \rightarrow \{0, 1\}^n,$$

$$\tilde{Q} : \{0, 1\}^t \times \{0, 1\}^n \rightarrow \{0, 1\}^n,$$

where \tilde{P} and \tilde{Q} can be seen as TURPs up to their TPRP-security. Given a (public) constant $C \in \{0, 1\}^c$ for an integer c such that $0 \leq c \leq n$, we might consider the sum of TPRPs, dubbed MXoP_c , is defined as follows.

$$\text{MXoP}_c(X, Y) \stackrel{\text{def}}{=} \tilde{P}(Y, C \parallel X) \oplus \tilde{Q}(Y, C \parallel X)$$

for $X \in \{0, 1\}^{n-c}$ and $Y \in \{0, 1\}^t$ (see Figure 1). One can view MXoP as XoP in the multi-user setting, where the number of users is 2^t and each user is allowed to make at most 2^{n-c} queries. Note that MXoP_c is parameterized by c (instead of C) since its security depends only on the length of the constant.

Since the construction is mathematically identical to the multiple instances of XoP , we can use previous analyses. As far as we know, the best-known result about multi-user security of XoP is by Hoang and Shen [HS20], which gives $(n/\log n)$ -bit security for the standard multi-user assumption, i.e., when an adversary can always freely choose an instance for its next query. They left its n -bit security proof as an open problem. Since security of MXoP_c is easily proved by Mirror theory, we do not claim the contribution of full multi-user security proof of XoP , while there is no literature that explicitly states its optimal security in the multi-user setting, so we will give a complete proof for MXoP_c that the adversarial advantage in breaking the PRF-security of MXoP_c is upper bounded by $O\left(\frac{q}{2^{n+c}}\right)$. In particular, when $t < 2n$, $\text{MXoP}_{\frac{t}{2}}$ is secure up to $2^{n+\frac{t}{2}}$ queries. When $t \geq 2n$, MXoP_n is secure up to 2^t queries.

It is noteworthy that recently there has been a new approach to proving multi-user security by fixing the number of queries made to each instance [BN21, CKLL22, CCL23, CHWZ23], and those works parameterized security bounds by the maximum number of queries per instance. This line of research shows that, with the assumption they used, one may obtain stronger security with respect to the number of instances.¹ On the other hand, in this paper, we focus on a more generalized setting without any limit on the number of queries per instance.

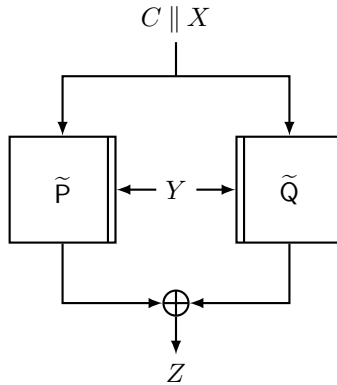


Figure 1: MXoP_c based on \tilde{P} and \tilde{Q} .

1.1 Our Contribution

In this paper, we propose a new construction for a TPRP-based PRF enjoying stronger security than MXoP_c (for a certain range of parameters) and provide a new way of analyzing

¹However, the maximum number of queries per instance is qualitatively different from the number of total queries. For example, if an adversary makes almost all possible queries to a single instance, their bounds [BN21, CKLL22, CCL23, CHWZ23] can be significantly worse.

its security even when message and tweak inputs are correlated (which is not the case for MXoP_c). Our new construction, dubbed XoTP_c , is defined as follows: when $t \geq n - c$,

$$\text{XoTP}_c(X, Y, W) = \tilde{\text{P}}(W \parallel Y, C \parallel X) \oplus \tilde{\text{Q}}(W \parallel X, C \parallel Y)$$

for $X, Y \in \{0, 1\}^{n-c}$ and $W \in \{0, 1\}^{t-n+c}$, and when $t < n - c$,

$$\text{XoTP}_c(X, Y, W) = \tilde{\text{P}}(Y, C \parallel W \parallel X) \oplus \tilde{\text{Q}}(X, C \parallel W \parallel Y)$$

for $X, Y \in \{0, 1\}^t$ and $W \in \{0, 1\}^{n-t-c}$ (see Figure 2). In this way, XoTP_c becomes a $(t + n - c)$ -to- n bit pseudorandom function.

We prove that when $t \geq n - c$ (resp. $t < n - c$), the adversarial advantage in breaking the PRF-security of XoTP_c is upper bounded by $O\left(\min\left\{\frac{q}{2^{n+2c}}, \frac{q^2}{2^{3n}}\right\}\right)$ (resp. $O\left(\max\left\{\frac{q}{2^{n+t+c}}, \frac{q}{2^{n+2c}}\right\}\right)$). In particular, when $c < t$, the adversarial distinguishing advantage is upper bounded by $O\left(\frac{q}{2^{n+2c}}\right)$. Since the input size of XoTP_c is $(t + n - c)$ bits, the threshold number of queries is maximized when $c = \frac{t}{3}$ (assuming $t \leq 3n$). Then $\text{XoTP}_{\frac{t}{3}}$ is secure up to $2^{n+\frac{2t}{3}}$ queries. Figure 3 shows the threshold number of queries q as a function of tweak size t for $\text{MXoP}_{\min\{\frac{t}{2}, n\}}$ and $\text{XoTP}_{\frac{t}{3}}$. We see that $\text{XoTP}_{\frac{t}{3}}$ enjoys security beyond the block and the tweak length bounds when $t < 3n$.

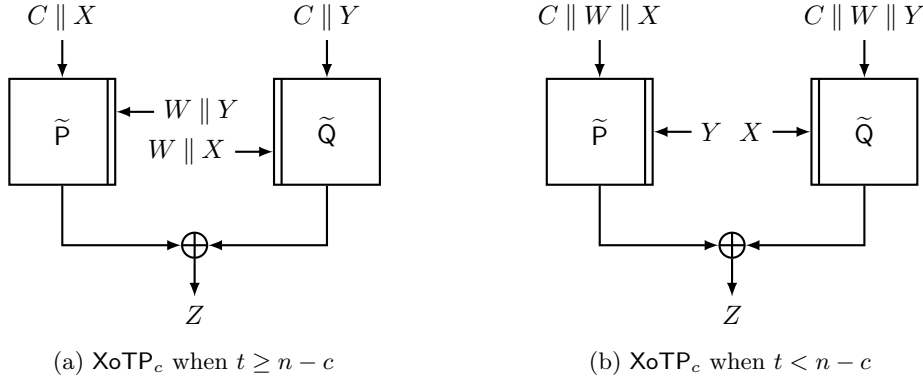


Figure 2: XoTP_c based on $\tilde{\text{P}}$ and $\tilde{\text{Q}}$.

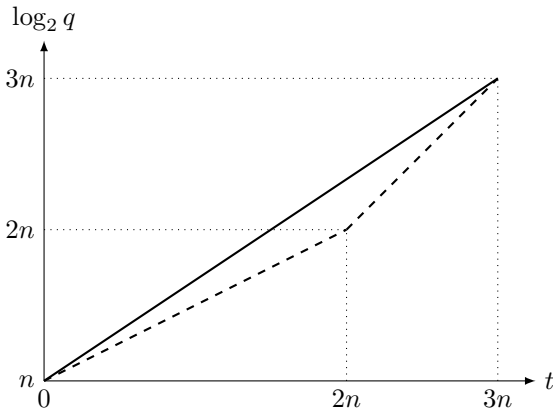


Figure 3: The threshold number of queries q as a function of tweak size t . The dashed line is the bound for $\text{MXoP}_{\min\{\frac{t}{2}, n\}}$, and the solid line is the bound for $\text{XoTP}_{\frac{t}{3}}$.

APPLICATION. First, We note that high provable security allows us to use a small input size of the primitive in the trade-off of tweak size while maintaining the same security level. We notice that a longer tweak size t performs better than a larger input size n when $n + t$ is the same, e.g., SKINNY TBC families.

Many deterministic MAC schemes can be viewed as an instance of the Hash-then-PRF paradigm; a variable-length message is first mapped onto a fixed-length value through a universal hash function, and then a PRF is applied to the hashed message, obtaining a tag. When it comes to TBC-based constructions using two TBC calls at the finalization step, most of such schemes provide at most n -bit security; PMAC-TBC1k [Nai15] provides n -bit security and ZMAC [IMPS17] provides $\min\{n, \frac{n+t}{2}\}$ -bit security.

If XoTP_c is combined with any birthday bound-secure $(t + n - c)$ -bit hash function that has collision-resistant property (though constructing such a nice hash function is an independent open question), then one might expect $\min\{\frac{t+n-c}{2}, \max\{n + 2c, \frac{3n}{2}\}\}$ -bit security for the resulting MAC scheme when XoTP_c is instantiated as a PRF. When $n < t < 6n$, it will provide $\frac{2t+3n}{5}$ -bit security with $c = \frac{t-n}{5}$, which is stronger than existing TBC-based MAC schemes such as [CLS17] (providing n -bit security) or using a trivial t -to- n bit PRF with a single TBC call. Note that if one uses t -to- n bit PRF as a finalization function of the given hash, the security is upper bounded by $\min\{n, \frac{t}{2}\}$.

If a TBC is used to construct a CTR-type encryption mode of rate 1 with a nonce as a tweak input and a block counter as a block cipher input, then the adversarial distinguishing advantage against this mode will be tightly upper bounded by

$$\frac{\sigma l}{2^n}$$

where l is the maximum message length and σ is the total number of message blocks. This security bound might not be sufficient, in particular when n is small.

In order to achieve stronger security (at the cost of worse efficiency), one might use an $(n + t - c)$ -to- n bit PRF XoTP_c to construct a CTR-type encryption mode of rate $\frac{1}{2}$. When $c = \frac{t}{3}$, $n + \frac{2t}{3}$ bits are available for nonces and counters, while the adversarial distinguishing advantage against this mode is upper bounded by

$$O\left(\frac{\sigma}{2^{n+\frac{2t}{3}}}\right).$$

As a numerical example, consider the SKINNY-64-192 tweakable block cipher operating on 64-bit blocks using 192-bit tweakeys. If 128 bits are used as a key, then one can use 64-bit tweaks. In this case, one can use 107 input bits to XoTP_{21} as nonces and counters (say, 67-bit nonces and 40-bit counters), and the resulting encryption mode will be secure as long as the total number of message blocks is small in front of 2^{106} . If $n + \frac{2t}{3}$ bits are not sufficient for nonces and counters, one can simply take a small constant c so that the input size of the resulting PRF is almost $n + t$ bits. For the encryption mode using this PRF, the adversarial distinguishing advantage is still upper bounded by

$$O\left(\frac{\sigma^2}{2^{3n}}\right).$$

PROOF TECHNIQUE. Our proof is based on the standard H-coefficient technique, where Patarin's Mirror theory [Pat10b] is used for the counting arguments. Mirror theory allows one to sharply lower bound the number of solutions to a certain type of system of equations and non-equations. In our security proof, we will consider the following system of equations; for two sets of unknowns $\mathcal{V}_P = \{P_1, \dots, P_q\}$ and $\mathcal{V}_Q = \{Q_1, \dots, Q_q\}$, and for constants

$Z_i, i = 1, \dots, q,$

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \quad \quad \quad \vdots \\ P_q \oplus Q_q = Z_q. \end{cases}$$

This system of equations can be represented by a simple graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \mathcal{V}_P \sqcup \mathcal{V}_Q$ and P_i and Q_i are connected by a Z_i -weighted edge for $i = 1, \dots, q$. This graph consists of q isolated edges, so the size of the largest component in this graph, denoted ξ_{\max} , is two. The system of equations with $\xi_{\max} = 2$ appears in the security proof of the sum of two independent random permutations, where all the unknowns in \mathcal{V}_P (resp. \mathcal{V}_Q) should be distinct since they are supposed to be outputs from a fixed permutation. These additional constraints can be viewed as non-equations between the unknowns. The resulting system of equations and non-equations has been studied in [Pat10b], and later revisited with more complete and detailed arguments [CP20, DNS22].

When it comes to a *tweakable* permutation, all the outputs are not necessarily distinct, in particular, when they are defined with distinct tweaks. With this observation, we relax the constraints of non-equations by defining partitions of \mathcal{V}_P and \mathcal{V}_Q ; if P_i and P_j (resp. Q_i and Q_j) are contained in the same block, then $P_i \neq P_j$ (resp. $Q_i \neq Q_j$), which implies evaluations of a tweakable permutation of i -th and j -th query share the same tweak input. In this way, we generalize Mirror theory for $\xi_{\max} = 2$, and it leads to the security proof of XoTP. Most notable related works are probably Mirror theory for proving an ideal tweakable permutation model [MN17, JN20]. This type of Mirror theory aims to provide a more rigorous analysis of the number of solutions considering duplications among Z_i -values when Z_i -values serve as a tweak value in their ideal world. On the other hand, our Mirror theory uses tweakable permutations in the real world to construct an ideal random function. Mirror theory for ideal tweakable permutation model [MN17, JN20] studies more deeply the relation between the number of solutions and the distribution of Z_i -values. It is an interesting theoretical question to merge their idea with our relaxation on the output restriction; however, then it uses tweakable permutations to build a tweakable permutation, making it hard to find practical implications.

HISTORY. Tweakable permutation-related Mirror theory was also studied by Mennink et al. [MN17], while they use permutations to construct an ideal tweakable permutation. It was based on the original Mirror theory [Pat10b], which has been controversial due to some mistakes and gaps in the paper. Nandi [Nan20] also pointed out a flaw in [MN17]. Many researchers have revisited Mirror theory in more verifiable ways, while newly established Mirror theory takes more limited conditions for q and ξ_{\max} . Datta et al. [DDNY18] studied Mirror theory for $q = O\left(2^{\frac{2n}{3}}\right)$ and $\xi_{\max} = 3$ to prove the security of the DWCDM nonce-based MAC scheme. Dutta et al. [DNT19] extended it to q and ξ_{\max} such that $q = O\left(2^{\frac{2n}{3}}\right)$ and $q \cdot \xi_{\max} \leq 2^{n-2}$, and proved the security of the CWC+ AEAD mode. Jha and Nandi [JN20] further extended it to q and ξ_{\max} such that $q = O\left(2^{\frac{3n}{4}}\right)$ and $q \cdot \xi_{\max} \leq 2^{n-1}$ to tightly prove the security of CLRW2. Kim et al. [KLL20] studied Mirror theory for $q = O\left(2^{\frac{3n}{4}}\right)$ assuming that the number of components of size ≥ 3 is smaller than $2^{\frac{n}{2}}$, and it was sufficient to tightly prove the security of DbHtS MAC schemes. Recently, Dutta et al. [DNS22] and Cogliati and Patarin [CP20] independently revisited Mirror theory for $q = O(2^n)$, giving clearer and verifiable proofs, while both assume $\xi_{\max} = 2$. Recently, Cogliati et al. [CDN⁺23] improved the result by relaxing the restriction of ξ_{\max} with an assumption $q \cdot \xi_{\max}^2 \ll 2^n$. In this line of research, we firstly establish Mirror theory for $q \gg 2^n$.

OPEN PROBLEMS. First of all, the exact security of the MXoP and XoTP constructions still remains open. Secondly, one can consider an alternative approach to constructing PRFs using a single call to the underlying primitive: to truncate outputs from a tweakable permutation. Fix two positive integers c and m such that $c, m \leq n$ as well as a constant $C \in \{0, 1\}^c$, and let

$$\text{TTRP}_{c,m}(X \parallel Y) \stackrel{\text{def}}{=} \text{Tr}_m \left(\tilde{\text{P}}(Y, C \parallel X) \right)$$

for $X \in \{0, 1\}^{n-c}$ and $Y \in \{0, 1\}^t$. Since TRP_m permits an attack using $2^{n-\frac{m}{2}}$ queries, we need to fix a part of the input, so that an adversary is not able to make that many queries for a single tweak. We leave the (exact) security of $\text{TTRP}_{c,m}$ as an open problem.

When it comes to Mirror theory, relaxing the constraint $\xi_{\max} = 2$ seems to be an important open question from both theoretical and practical point of view. If one can improve Mirror theory in this direction, many practical constructions based on a tweakable block cipher could be proposed. For example, one would be able to construct CENC-like encryption modes [Iwa06] of stronger provable security.

2 Preliminaries

NOTATION. Throughout this work, we fix positive integers n , t , and q . We denote 0^n (i.e., n -bit string of all zeros) by $\mathbf{0}$. For integers a and b such that $0 \leq a < b$, we write $[a, b] \stackrel{\text{def}}{=} \{a, \dots, b\}$ and $[b] \stackrel{\text{def}}{=} \{1, \dots, b\}$. Given a non-empty set \mathcal{X} , $x \leftarrow_{\S} \mathcal{X}$ denotes that x is chosen uniformly at random from \mathcal{X} . The set of all functions from \mathcal{X} to \mathcal{Y} is denoted $\text{Func}(\mathcal{X}, \mathcal{Y})$. We use an indicator function, denoted $\mathbb{1}$, such that for a statement E , $\mathbb{1}(E) = 1$ if a statement E is true, and $\mathbb{1}(E) = 0$ otherwise. When two sets \mathcal{X} and \mathcal{Y} are disjoint, their (disjoint) union is denoted $\mathcal{X} \sqcup \mathcal{Y}$.

TWEAKABLE BLOCK CIPHER. A *tweakable block cipher* (TBC) is a keyed function $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \rightarrow \mathcal{X}$, where \mathcal{K} is the key space, $\mathcal{T} = \{0, 1\}^t$ is the tweak space, and $\mathcal{X} = \{0, 1\}^n$ is the message space, such that for any $(K, T) \in \mathcal{K} \times \mathcal{T}$, $\tilde{E}(K, T, \cdot)$ is a permutation over \mathcal{X} .

A *tweakable permutation* is the mapping $\tilde{\text{P}} : \mathcal{T} \times \mathcal{X} \rightarrow \mathcal{X}$ such that $\tilde{\text{P}}(T, \cdot)$ is a permutation of \mathcal{X} for any tweak $T \in \mathcal{T}$. When a tweakable permutation is chosen uniformly at random from the set of all possible tweakable permutations, such an ideal object is called a *tweakable uniform random permutation* (TURP). A secure tweakable block cipher should behave like a tweakable uniform random permutation with the same message and tweak spaces (when the key is chosen uniformly at random from the key space and kept secret), and hence it is viewed as a *tweakable pseudorandom permutation* (TPRP).

PSEUDORANDOM FUNCTION. Let $\text{C} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ be a keyed function with key space \mathcal{K} , domain \mathcal{X} , and range \mathcal{Y} . We will consider an information theoretic distinguisher \mathcal{D} that makes oracle queries to C , and returns a single bit. The advantage of \mathcal{D} in breaking the PRF-security of C , i.e., in distinguishing C from a uniformly chosen function $\text{F} \leftarrow_{\S} \text{Func}(\mathcal{X}, \mathcal{Y})$, is defined as

$$\text{Adv}_{\text{C}}^{\text{prf}}(\mathcal{D}) = \left| \Pr \left[K \leftarrow_{\S} \mathcal{K} : \mathcal{D}^{\text{C}(K, \cdot)} = 1 \right] - \Pr \left[\text{F} \leftarrow_{\S} \text{Func}(\mathcal{X}, \mathcal{Y}) : \mathcal{D}^{\text{F}(\cdot)} = 1 \right] \right|.$$

We define $\text{Adv}_{\text{C}}^{\text{prf}}(q)$ as the maximum of $\text{Adv}_{\text{C}}^{\text{prf}}(\mathcal{D})$ over all the distinguishers against C making at most q queries.

H-COEFFICIENT TECHNIQUE [PAT08B]. Consider a PRF construction $\text{C}[\tilde{\text{P}}, \tilde{\text{Q}}] : \mathcal{X} \rightarrow \mathcal{Y}$ based on two TURPs $\tilde{\text{P}}$ and $\tilde{\text{Q}}$. In this case, $\tilde{\text{P}}$ and $\tilde{\text{Q}}$ can be viewed as keys. Suppose that an information-theoretic distinguisher \mathcal{D} adaptively makes q queries to the construction

oracle, which is either $C[\tilde{P}, \tilde{Q}]$ (in the real world) or a truly random function F (in the ideal world), recording all the queries $(X_i, Y_i)_{1 \leq i \leq q}$. So according to the instantiation, it would imply either $C[\tilde{P}, \tilde{Q}](X_i) = Y_i$ or $F(X_i) = Y_i$. We will call

$$\tau = ((X_1, Y_1), \dots, (X_q, Y_q))$$

the *transcript* of the attack; it contains all the information that \mathcal{D} has obtained at the end of the attack. When we consider an information theoretic distinguisher, we can assume that the distinguisher is deterministic without making any redundant query.

Fix a transcript $\tau = (X_i, Y_i)_{1 \leq i \leq q}$. If there exists a function $F \in \text{Func}(\mathcal{X}, \mathcal{Y})$ such that $F(X_i) = Y_i$ for every $i = 1, \dots, q$, then we will call the transcript τ *attainable*. We denote Γ the set of attainable transcripts. We also denote T_{re} (resp. T_{id}) the probability distribution of the transcript τ induced by the real world (resp. the ideal world). By extension, we use the same notation to denote a random variable distributed according to each distribution. Without considering “bad events”, the coefficient-H technique is summarized as follows.

Lemma 1. *Let $\varepsilon > 0$. Suppose that*

$$\frac{\Pr[\mathsf{T}_{\text{re}} = \tau]}{\Pr[\mathsf{T}_{\text{id}} = \tau]} \geq 1 - \varepsilon$$

for any $\tau \in \Gamma$. Then one has

$$\text{Adv}_{\mathsf{C}}^{\text{prf}}(q) \leq \varepsilon.$$

USEFUL LEMMA. Dutta et al. [DNS22] proved the following combinatorial lemma. This lemma will also be used in our Mirror theory.

Lemma 2. *Let m be a positive integer, and let $(D_{\alpha, \beta})_{\alpha, \beta}$ be a two-dimensional sequence of non-negative numbers, where $1 \leq \alpha \leq m$ and $\beta \leq \alpha - 1$. Suppose that $D_{\alpha, \beta} = 0$ if $\beta \leq 0$, and if $2 \leq \alpha \leq m$ and $\beta \leq \alpha - 3$, then the following recurrence relation holds.*

$$D_{\alpha, \beta} \leq D_{\alpha-1, \beta-1} + 2A \cdot D_{\alpha-1, \beta} + A^2 \cdot D_{\alpha-1, \beta+1} + \frac{C}{(2^n - 2A)^{m-\alpha+\beta}}$$

for some positive constants A and C such that $A < 2^{n-1}$. Then, for any integer r such that $1 \leq r \leq \frac{\alpha}{2} - 1$, one has

$$D_{\alpha, 1} \leq \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r, 1-r+i} + \sum_{j=0}^{r-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}. \quad (1)$$

Lemma 2 is proved by mathematical induction on r .

3 Proof of Lemma 2

We will use induction on r . One can easily see that (1) holds when $r = 1$. Suppose that (1) holds for r such that $r \leq \frac{\alpha}{2} - 2$. By the recurrence relation, we have

$$\begin{aligned} \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r, 1-r+i} &\leq \sum_{i=r}^{2r} \binom{2r}{i} A^i \left(D_{\alpha-r-1, i-r} + 2A \cdot D_{\alpha-r-1, 1-r+i} \right. \\ &\quad \left. + A^2 \cdot D_{\alpha-r-1, 2-r+i} + \frac{C}{(2^n - 2A)^{m-\alpha+1+i}} \right) \end{aligned}$$

$$= \sum_{i=r}^{2r+1} B_i D_{\alpha-r-1, 1-r+i} + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}},$$

for some B_i , where

$$\begin{aligned} B_i &= \binom{2r}{i+1} A^{i+1} + \binom{2r}{i} A^i \cdot 2A + \binom{2r}{i-1} A^{i-1} \cdot A^2 \\ &= \left(\binom{2r}{i+1} + 2\binom{2r}{i} + \binom{2r}{i-1} \right) A^{i+1} \\ &= \left(\binom{2r+1}{i+1} + \binom{2r+1}{i} \right) A^{i+1} \\ &= \binom{2r+2}{i+1} A^{i+1} \end{aligned}$$

when $r+1 \leq i \leq 2r-1$. Even for $i \in \{r, 2r, 2r+1\}$, one easily sees that $B_i \leq \binom{2r+2}{i+1} A^{i+1}$. Therefore, we have

$$\begin{aligned} \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r, 1-r+i} &\leq \sum_{i=r+1}^{2r+2} \binom{2r+2}{i} A^i D_{\alpha-r-1, i-r} \\ &\quad + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}. \end{aligned}$$

Combined with the induction hypothesis, we have

$$\begin{aligned} D_{\alpha,1} &\leq \sum_{i=r}^{2r} \binom{2r}{i} A^i D_{\alpha-r, 1-r+i} + \sum_{j=0}^{r-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}} \\ &\leq \sum_{i=r+1}^{2r+2} \binom{2r+2}{i} A^i D_{\alpha-r-1, i-r} + \sum_{i=r}^{2r} \binom{2r}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}} \\ &\quad + \sum_{j=0}^{r-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}} \\ &\leq \sum_{i=r+1}^{2r+2} \binom{2r+2}{i} A^i D_{\alpha-r-1, i-r} + \sum_{j=0}^r \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+1+i}}, \end{aligned}$$

which completes the proof.

4 Mirror Theory for $\xi_{max} = 2$ with Relaxed Constraints

For a fixed positive integer q , let

$$\begin{aligned} \mathcal{V}_P &\stackrel{\text{def}}{=} \{P_1, \dots, P_q\}, \\ \mathcal{V}_Q &\stackrel{\text{def}}{=} \{Q_1, \dots, Q_q\} \end{aligned}$$

be sets of *unknowns* such that $P_i, Q_i \in \{0, 1\}^n$ for $i \in [q]$. For a sequence of constants $(Z_1, \dots, Z_q) \in (\{0, 1\}^n)^q$, consider a system of equations

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \vdots \\ P_q \oplus Q_q = Z_q. \end{cases}$$

The original Mirror theory estimates the number of solutions with pairwise distinct P variables and pairwise distinct Q variables. However, when each variable is derived from a tweakable block cipher, only variables from the same tweak input should be distinct. Consequently, we introduce a new theory to estimate the number of solutions such that only variables from a common tweak are distinct.

We will fix two partitions of $[q]$, namely,

$$\begin{aligned}\mathbb{P} &= \left\{ \mathcal{P}^{(1)}, \dots, \mathcal{P}^{(a)} \right\}, \\ \mathbb{Q} &= \left\{ \mathcal{Q}^{(1)}, \dots, \mathcal{Q}^{(b)} \right\}\end{aligned}$$

for some positive integers a and b , where

$$[q] = \mathcal{P}^{(1)} \sqcup \dots \sqcup \mathcal{P}^{(a)} = \mathcal{Q}^{(1)} \sqcup \dots \sqcup \mathcal{Q}^{(b)}.$$

Let

$$A \stackrel{\text{def}}{=} \max_{i \in [a], j \in [b]} \left\{ \left| \mathcal{P}^{(i)} \right|, \left| \mathcal{Q}^{(j)} \right| \right\}$$

denote the size of the largest block in the two partitions. Throughout this section, we will assume

$$A \leq \frac{2^n}{13}.$$

We will write $i \stackrel{P}{\sim} j$ (resp. $i \stackrel{Q}{\sim} j$) if there exists k such that $i, j \in \mathcal{P}^{(k)}$ (resp. $i, j \in \mathcal{Q}^{(k)}$). With respect to these relations, we will put additional constraints on Γ as follows.

1. If $i \stackrel{P}{\sim} j$, then $P_i \neq P_j$.
2. If $i \stackrel{Q}{\sim} j$, then $Q_i \neq Q_j$.

Those two relations are closely related to the model of our applications: the tweakable permutation model. By identifying \mathcal{V}_P (and \mathcal{V}_Q) with outputs of a tweakable permutation, each partition of \mathbb{P} (and \mathbb{Q}) is matched with outputs of a tweakable permutation of the same tweak, which should be distinct to each other. On the other hand, it is possible to have the same value for two distinct random variables P_i and P_j if $i \stackrel{P}{\sim} j$. The relation implies that P_i and P_j are distinct outputs from two distinct inputs of a tweakable permutation. Apart from the previous Mirror theories, we do not identify P_i and P_j as random variables since they are from distinct outputs, and that is the reason why we call our Mirror theory $\xi_{\max} = 2$ even if it is possible to have $P_i = P_j$.

The goal of our Mirror theory is to sharply lower bound the number of solutions to Γ , denoted $h(\Gamma, \stackrel{P}{\sim}, \stackrel{Q}{\sim})$, subject to the above constraints. In order to state the main result of our Mirror theory, we need to define sets

$$\mathcal{P}_i \stackrel{\text{def}}{=} \left\{ j \in [i-1] \mid j \stackrel{P}{\sim} i \right\}, \quad \mathcal{Q}_i \stackrel{\text{def}}{=} \left\{ j \in [i-1] \mid j \stackrel{Q}{\sim} i \right\}. \quad (2)$$

for $i \in [q]$. We note that \mathcal{P}_i (resp. \mathcal{Q}_i) is a subset of the block containing i in partition \mathbb{P} (resp. \mathbb{Q}). If i is the smallest element in the block, then \mathcal{P}_i or \mathcal{Q}_i is an empty set.

Theorem 1. *One has*

$$\begin{aligned}h(\Gamma, \stackrel{P}{\sim}, \stackrel{Q}{\sim}) &\geq \left(1 - \sum_{i=1}^q \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}} \right) - \frac{6(n+1)^3}{2^{2n}} \right) \\ &\quad \times \prod_{i=1}^q \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n} \right).\end{aligned}$$

The proof of Theorem 1 will be given in the next section. Let

$$B \stackrel{\text{def}}{=} \max_{i \in [a], j \in [b]} \left\{ |\mathcal{P}^{(i)} \cap \mathcal{Q}^{(j)}| \right\}.$$

Then we have the following lemma.

Lemma 3. *One has*

$$\sum_{i=1}^q |\mathcal{P}_i| |\mathcal{Q}_i| \leq \min \{A^2 q, Bq^2\}.$$

Proof. Since \mathcal{P}_i (resp. \mathcal{Q}_i) is a subset of a single block in \mathbb{P} (resp. \mathbb{Q}), we have

$$\sum_{i=1}^q |\mathcal{P}_i| |\mathcal{Q}_i| \leq \sum_{i=1}^q A^2 = A^2 q. \quad (3)$$

For $k \in [a]$, let $U_k = |\mathcal{P}^{(k)} \cap [q-1]|$, and for $l \in [b]$, let $V_l = |\mathcal{Q}^{(l)} \cap [q-1]|$. Then, we see that

$$\sum_{k \in [a]} U_k = \sum_{l \in [b]} V_l = q - 1.$$

For $i \in [q]$, there exists a unique pair (k, l) such that $i \in \mathcal{P}^{(k)} \cap \mathcal{Q}^{(l)}$, in which case $|\mathcal{P}_i| \leq U_k$ and $|\mathcal{Q}_i| \leq V_l$. On the other hand, for $(k, l) \in [a] \times [b]$, there are at most B indices i such that $i \in \mathcal{P}^{(k)} \cap \mathcal{Q}^{(l)}$. Therefore, we have

$$\sum_{i=1}^q |\mathcal{P}_i| |\mathcal{Q}_i| \leq \sum_{(k,l) \in [a] \times [b]} (BU_k V_l) = B \sum_{k \in [a]} U_k \sum_{l \in [b]} V_l = B(q-1)^2. \quad (4)$$

By (3) and (4), the proof is complete. \square

By Lemma 3 and since $|\mathcal{P}_i \cap \mathcal{Q}_i| \leq B - 1$ for every $i \in [q]$, Theorem 1 is simplified as follows.

Corollary 1. *One has*

$$\begin{aligned} h(\Gamma, \mathcal{P}, \mathcal{Q}) &\geq \left(1 - \frac{2(B-1)q + 6(n+1)^3}{2^{2n}} - \frac{20 \min \{A^2 q, Bq^2\}}{2^{3n}} \right) \\ &\quad \times \prod_{i=1}^q \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n} \right). \end{aligned}$$

4.1 Proof of Theorem 1

GRAPH REPRESENTATION, DEFINITIONS AND NOTATIONS. Let $\alpha \in [q]$. For a set of α indices $\mathcal{I} = \{i_1, \dots, i_\alpha\} \subset [q]$, we define

$$\begin{aligned} \mathcal{V}[\mathcal{I}] &\stackrel{\text{def}}{=} \{P_{i_1}, Q_{i_1}, \dots, P_{i_\alpha}, Q_{i_\alpha}\}, \\ \mathcal{E}[\mathcal{I}] &\stackrel{\text{def}}{=} \{(P_{i_1}, Q_{i_1}, Z_{i_1}), \dots, (P_{i_\alpha}, Q_{i_\alpha}, Z_{i_\alpha})\}, \\ \mathcal{G}[\mathcal{I}] &\stackrel{\text{def}}{=} (\mathcal{V}[\mathcal{I}], \mathcal{E}[\mathcal{I}]), \end{aligned}$$

where $(P, Q, Z) \in \mathcal{E}[\mathcal{I}]$ represents an edge connecting P and Q with weight Z . When $\mathcal{I} = [\alpha]$, we will simply write \mathcal{G}_α to denote $\mathcal{G}[\mathcal{I}]$. By definition, $\mathcal{G}_0 = \emptyset$. We will identify $\mathcal{G}[\mathcal{I}]$ with a system of equations $P_i \oplus Q_i = Z_i$ for $i \in \mathcal{I}$. So \mathcal{G}_q becomes Γ .

For a set of edges \mathcal{F} such that every edge of \mathcal{F} connects vertices of $\mathcal{G}[\mathcal{I}]$, we will write $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ to denote $(\mathcal{V}[\mathcal{I}], \mathcal{E}[\mathcal{I}] \cup \mathcal{F})$. The number of solutions to $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ subject to relations $\overset{\mathcal{P}}{\sim}$ and $\overset{\mathcal{Q}}{\sim}$ will be denoted $h(\mathcal{G}[\mathcal{I}] \cup \mathcal{F})$. By definition, $h(\mathcal{G}_0) = 1$. When $h(\mathcal{G}[\mathcal{I}] \cup \mathcal{F}) > 0$, we say that $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ is *valid*. Note that \mathcal{G}_q (with $\mathcal{I} = [q]$ and $\mathcal{F} = \emptyset$) is valid if $A \leq 2^{n-1}$.

Let l be a positive integer. For a trail of length l connecting two vertices V_0 and V_l , say

$$T(V_0, V_l) : ((V_0, V_1, E_1), \dots, (V_{l-1}, V_l, E_l))$$

in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, the *weight* of $T(V_0, V_l)$ is defined as

$$w(T(V_0, V_l)) \stackrel{\text{def}}{=} E_1 \oplus E_2 \oplus \dots \oplus E_l.$$

In order for $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$ to be valid, the following conditions should be satisfied.

1. For any distinct i and j such that $i \overset{\mathcal{P}}{\sim} j$, and for any trail $T(P_i, P_j)$ in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, $w(T(P_i, P_j)) \neq \mathbf{0}$.
2. For any distinct i and j such that $i \overset{\mathcal{Q}}{\sim} j$, and for any trail $T(Q_i, Q_j)$ in $\mathcal{G}[\mathcal{I}] \cup \mathcal{F}$, $w(T(Q_i, Q_j)) \neq \mathbf{0}$.

For $\alpha \in [2, q]$, let $\mathcal{I} \subset [q]$ be an index set such that $|\mathcal{I}| = \alpha$. For $\beta \in [\alpha - 1]$, let

$$\mathcal{J} = (j_1, \dots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$$

be a sequence of *distinct* indices in \mathcal{I} , and let

$$\mathcal{L} = (L_1, \dots, L_\beta) \in (\{0, 1\}^n)^\beta$$

be a sequence of n -bit weights. Then we define an edge set

$$\mathcal{F}[\mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \{(P_{j_1}, Q_{j_2}, L_1), \dots, (P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\}$$

and a weighted graph

$$\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}] \stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I}] \cup \mathcal{F}[\mathcal{J}, \mathcal{L}].$$

We also define subgraphs of $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ as follows.

$$\begin{aligned} \mathcal{G}^+[\mathcal{I}, \mathcal{J}, \mathcal{L}] &\stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \{(P_{j_1}, Q_{j_2}, L_1)\}), \\ \mathcal{G}^-[\mathcal{I}, \mathcal{J}, \mathcal{L}] &\stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I} \setminus \{j_{\beta+1}\}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \{(P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\}), \\ \mathcal{G}^{--}[\mathcal{I}, \mathcal{J}, \mathcal{L}] &\stackrel{\text{def}}{=} \mathcal{G}[\mathcal{I} \setminus \{j_{\beta+1}\}] \cup (\mathcal{F}[\mathcal{J}, \mathcal{L}] \setminus \{(P_{j_1}, Q_{j_2}, L_1), (P_{j_\beta}, Q_{j_{\beta+1}}, L_\beta)\}). \end{aligned}$$

When \mathcal{I} , \mathcal{J} and \mathcal{L} are clear from the context, we will simply write

$$\mathcal{G}^{++} = \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{+-} = \mathcal{G}^+[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{+--} = \mathcal{G}^{--}[\mathcal{I}, \mathcal{J}, \mathcal{L}], \quad \mathcal{G}^{--} = \mathcal{G}^-[\mathcal{I}, \mathcal{J}, \mathcal{L}].$$

Note that \mathcal{G}^{+-} is obtained from \mathcal{G}^{++} by removing one edge, namely (P_{j_1}, Q_{j_2}, L_1) , while \mathcal{G}^{+--} is obtained from \mathcal{G}^{++} by removing two edges that are incident with $Q_{j_{\beta+1}}$. See Figure 4 for an example of \mathcal{G}^{++} , \mathcal{G}^+ , \mathcal{G}^{+-} and \mathcal{G}^{--} . When $\beta = 0$, we have $\mathcal{L} = \emptyset$ and $\mathcal{F}[\mathcal{J}, \mathcal{L}] = \emptyset$ by definition, in which case, $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}] = \mathcal{G}[\mathcal{I}]$. We note that if \mathcal{G}^{++} is valid for given \mathcal{I} , \mathcal{J} , and \mathcal{L} , then \mathcal{G}^+ , \mathcal{G}^{+-} and \mathcal{G}^{--} are also valid.

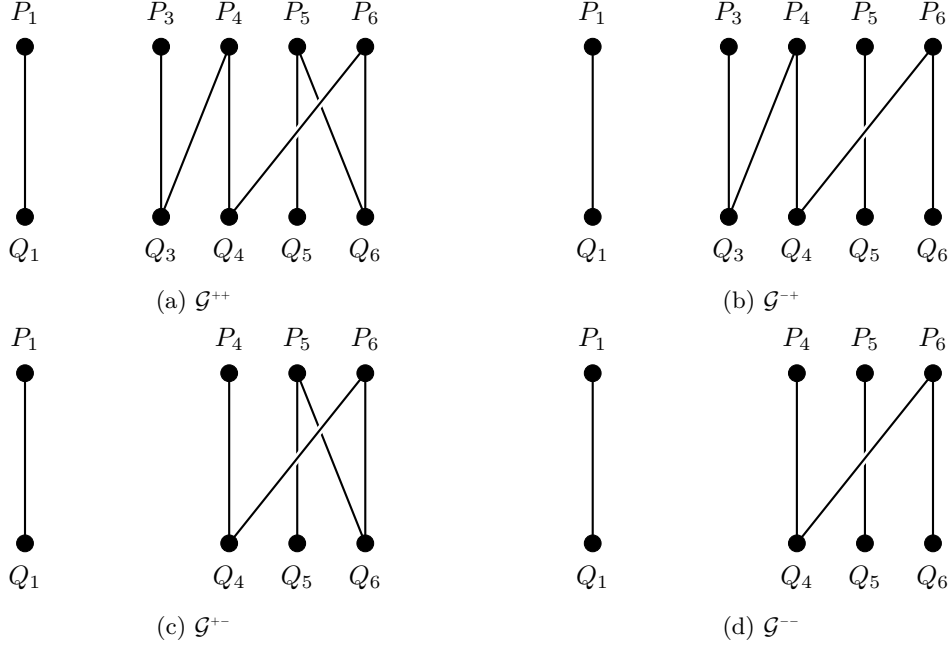


Figure 4: An example of \mathcal{G}^x for $x \in \{++, +-, --\}$, where $q = 6$, $\mathcal{I} = \{1, 3, 4, 5, 6\}$ and $\mathcal{J} = (5, 6, 4, 3)$.

For an index set $\mathcal{I} \subset [q]$ and $i \in [q]$, we define the following sets.

$$\begin{aligned} \mathcal{P}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \{j \in \mathcal{I} \mid j \stackrel{\mathcal{P}}{\sim} i \text{ and } j \neq i\}, \\ \mathcal{Q}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \{j \in \mathcal{I} \mid j \stackrel{\mathcal{Q}}{\sim} i \text{ and } j \neq i\}, \\ \mathcal{R}_i[\mathcal{I}] &\stackrel{\text{def}}{=} \{j \in \mathcal{I} \mid j \stackrel{\mathcal{P}}{\sim} i, j \stackrel{\mathcal{Q}}{\sim} i, Z_j = Z_i \text{ and } j \neq i\}. \end{aligned}$$

When $\mathcal{I} = [\alpha]$ for some $\alpha \in [q]$, we will simply write \mathcal{P}_α , \mathcal{Q}_α , and \mathcal{R}_α to denote $\mathcal{P}_\alpha[\mathcal{I}]$, $\mathcal{Q}_\alpha[\mathcal{I}]$, and $\mathcal{R}_\alpha[\mathcal{I}]$, respectively.² Note that $\mathcal{R}_\alpha \subset \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ for any $\alpha \in [q]$.

ORANGE EQUATION. We can recursively compute $h(\mathcal{G}_\alpha)$ using the following lemma.

Lemma 4. *For any positive integer $\alpha \in [q]$, one has*

$$h(\mathcal{G}_\alpha) = (2^n - |\mathcal{P}_\alpha| - |\mathcal{Q}_\alpha| + |\mathcal{R}_\alpha|)h(\mathcal{G}_{\alpha-1}) + \sum_{E \in \mathbb{L}[\mathcal{G}_\alpha]} h(\mathcal{G}_{\alpha-1} \cup \{E\}) \quad (5)$$

where

$$\mathbb{L}[\mathcal{G}_\alpha] = \{(P_i, Q_j, Z_\alpha) \mid i \in \mathcal{P}_\alpha, j \in \mathcal{Q}_\alpha, i \neq j, h(\mathcal{G}_{\alpha-1} \cup \{(P_i, Q_j, Z_\alpha)\}) > 0\}.$$

Recurrence relation (5) is called the *Orange equation* in Mirror theory. The proof of Lemma 4 is given in Section 4.2. The Orange equation can be easily generalized as follows: to any set of indices \mathcal{I} such that $|\mathcal{I}| = \alpha$ and $j \in \mathcal{I}$,

$$h(\mathcal{G}^{++}) = (2^n - |\mathcal{P}_j[\mathcal{I}]| - |\mathcal{Q}_j[\mathcal{I}]| + |\mathcal{R}_j[\mathcal{I}]|)h(\mathcal{G}^{+-}) + \sum_{E \in \mathbb{L}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\})$$

²This notation is consistent with the previous definition of \mathcal{P}_i and \mathcal{Q}_i in (2).

where $\mathcal{G}^{++} = \mathcal{G}[\mathcal{I}, \mathcal{J}, \emptyset] (= \mathcal{G}[\mathcal{I}])$ with $\mathcal{J} = (j)$ and

$$\mathbb{L}[\mathcal{G}^{++}] = \{(P_k, Q_l, Z_j) \mid k \in \mathcal{P}_j[\mathcal{I}], l \in \mathcal{Q}_j[\mathcal{I}], k \neq l\}.$$

Example 1. For $n = 2$ and $q = 3$, let $\mathcal{P}^{(1)} = \{1, 3\}$, $\mathcal{P}^{(2)} = \{2\}$, $\mathcal{Q}^{(1)} = \{1\}$, $\mathcal{Q}^{(2)} = \{2, 3\}$, $Z_1 = 00$, $Z_2 = 01$ and $Z_3 = 10$. For $\alpha = 3$, we see that

$$\mathcal{P}_3 = \{1\}, \mathcal{Q}_3 = \{2\}, \mathcal{R}_3 = \emptyset.$$

Hence, it follows that

$$\mathbb{L}[\mathcal{G}_3] = \{(P_1, Q_2, 10)\},$$

and therefore,

$$\begin{aligned} h(\mathcal{G}_3) &= (4 - 1 - 1 + 0)h(\mathcal{G}_2) + h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}) \\ &= 2 \cdot h(\mathcal{G}_2) + h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}). \end{aligned} \quad (6)$$

Graphs \mathcal{G}_3 and $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ are pictorially represented in Figure 5. Since \mathcal{G}_2 consists of two independent equations, namely, $P_1 \oplus Q_1 = 00$ and $P_2 \oplus Q_2 = 01$, we have

$$h(\mathcal{G}_2) = (2^n)^2 = 16.$$

On the other hand, $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ consists of a single connected component, and assignment of an arbitrary value to a fixed vertex determines all the other unknowns. So, we have

$$h(\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}) = 2^n = 4.$$

By (6), we have $h(\mathcal{G}_3) = 36$.



Figure 5: Graphs \mathcal{G}_3 and $\mathcal{G}_2 \cup \{(P_1, Q_2, 10)\}$ in Example 1. Vertices in the same block are represented by the same shape.

PURPLE EQUATION. In order to use Lemma 4, we need to sharply lower bound $h(\mathcal{G}_{\alpha-1} \cup \mathcal{E})$ for a certain set of edges \mathcal{E} . We can recursively estimate $h(\mathcal{G}_{\alpha-1} \cup \mathcal{E})$ using graphs with a smaller number of connected components.

Lemma 5. Fix integers α and β such that $1 \leq \beta < \alpha \leq q$, an index set $\mathcal{I} \subset [q]$ such that $|\mathcal{I}| = \alpha$, a sequence of distinct indices $\mathcal{J} = (j_1, \dots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$, and a sequence of weights $\mathcal{L} = (L_1, \dots, L_\beta) \in (\{0, 1\}^n)^\beta$. If $\mathcal{G}^{++} (= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$ is valid, then one has

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}). \quad (7)$$

where

$$\begin{aligned} \mathbb{M}[\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]] &= \{E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}}) \mid \\ &\quad k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], h(\mathcal{G}^{+-} \cup \{E\}) > 0\} \\ &\cup \{E = (P_{j_\beta}, Q_k, L_\beta) \mid k \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], h(\mathcal{G}^{+-} \cup \{E\}) > 0\}, \\ \mathbb{N}[\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]] &= \{\{E, E'\} = \{(P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}}), (P_k, Q_l, Z_{j_{\beta+1}})\} \mid \\ &\quad k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], l \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}], k \neq l, h(\mathcal{G}^{+-} \cup \{E, E'\}) > 0\}. \end{aligned}$$

Recurrence relation (7) is called the *Purple equation*. The proof of Lemma 5 is given in Section 4.3.

Example 2. For $n = 2$ and $q = 6$, let

$$\begin{aligned} \mathcal{P}^{(1)} &= \{1, 3, 4\}, \quad \mathcal{P}^{(2)} = \{2\}, \quad \mathcal{P}^{(3)} = \{5, 6\}, \\ \mathcal{Q}^{(1)} &= \{1, 5, 6\}, \quad \mathcal{Q}^{(2)} = \{2, 3, 4\}, \\ Z_1 &= 00, \quad Z_2 = 01, \quad Z_3 = 10, \quad Z_4 = 10, \quad Z_5 = 11, \quad Z_6 = 11. \end{aligned}$$

For $\alpha = m = 6$ and $\beta = 2$, let

$$\begin{aligned} \mathcal{I} &= \{1, 2, 3, 4, 5, 6\}, \\ \mathcal{J} &= (5, 6, 4) \text{ (with } j_1 = 5, j_2 = 6, j_3 = 4\text{)}, \\ \mathcal{L} &= (10, 01). \end{aligned}$$

One can see that \mathcal{G}^{++} is valid and,

$$\begin{aligned} \mathcal{F}[\mathcal{J}, \mathcal{L}] &= \{(P_5, Q_6, 10), (P_6, Q_4, 01)\}, \\ \mathcal{G}^{+-} &= \mathcal{G}[\{1, 2, 3, 5, 6\}] \cup \{(P_5, Q_6, 10)\}, \\ \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}] &= \mathcal{P}_4[\{1, 2, 3\}] = \{1, 3\}, \\ \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}] &= \mathcal{Q}_4[\{1, 2, 3\}] = \{2, 3\}. \end{aligned}$$

Then we have

$$\mathbb{M}[\mathcal{G}^{++}] = \{(P_6, Q_1, 11), (P_6, Q_2, 01), (P_6, Q_3, 01)\}, \quad \mathbb{N}[\mathcal{G}^{++}] = \{\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3\},$$

where

$$\begin{aligned} \mathcal{E}_1 &= \{(P_6, Q_1, 11), (P_1, Q_2, 10)\}, \\ \mathcal{E}_2 &= \{(P_6, Q_1, 11), (P_1, Q_3, 10)\}, \\ \mathcal{E}_3 &= \{(P_6, Q_3, 01), (P_3, Q_2, 10)\}. \end{aligned}$$

Note that $\mathcal{G}^{+-} \cup \{(P_6, Q_1, 11)\}$ is invalid since it implies $Q_1 \oplus Q_6 = 0$. Since $\mathcal{G}^{+-} \cup \mathcal{E}_1$ and $\mathcal{G}^{+-} \cup \mathcal{E}_2$ are also invalid, we have

$$\begin{aligned} h(\mathcal{G}^{++}) &= h(\mathcal{G}^{+-}) - h(\mathcal{G}^{+-} \cup \{(P_6, Q_2, 01)\}) \\ &\quad - h(\mathcal{G}^{+-} \cup \{(P_6, Q_3, 01)\}) + h(\mathcal{G}^{+-} \cup \{(P_6, Q_3, 01), (P_3, Q_2, 10)\}). \end{aligned}$$

See Figure 6 for a pictorial representation of this example.

SIZE LEMMA. Our next step is to estimate the size of sets $\mathbb{L}[\mathcal{G}_\alpha]$, $\mathbb{M}[\mathcal{G}^{++}]$ and $\mathbb{N}[\mathcal{G}^{++}]$ appearing in Lemmas 4 and 5. In order to state Lemma 6, we need to reorder the indices of \mathcal{G}_q ; any reordering of the indices does not affect the number of solutions to \mathcal{G}_q .

For $k = 1, \dots, q$, there is a unique pair $(i_k, j_k) \in [a] \times [b]$ such that $k \in \mathcal{P}^{(i_k)} \cap \mathcal{Q}^{(j_k)}$. In this way, we can define an ordered multiset of q elements $\{(i_1, j_1, Z_1), \dots, (i_q, j_q, Z_q)\}$.

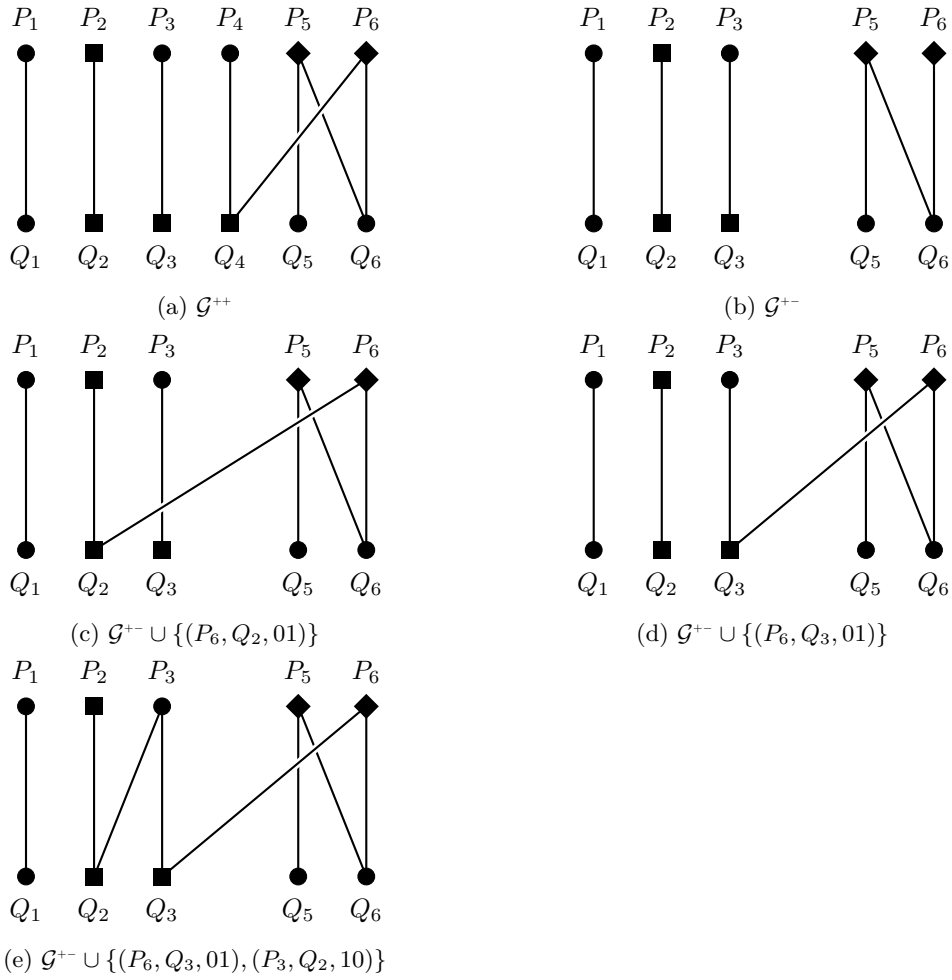


Figure 6: Graphs appearing in Example 2. Vertices in the same block are represented by the same shape.

From this multiset, we choose as many different elements as possible, put them in a separate list, remove them from the multiset, and recursively perform the same procedure for the remaining elements. This reordering of triples obviously defines a reordering of the edges (indices) since we can associate each triple with a unique $k \in [q]$. With this reordering of the indices, we have

$$\max_{\substack{i,j \in [\alpha], \\ Z \in \{0,1\}^n}} |\{k \in \mathcal{P}_i \cap \mathcal{Q}_j \mid Z_k = Z\}| \leq |\mathcal{R}_{\alpha+1}|. \quad (8)$$

Example 3. For $n = 1$ and $q = 6$, graph \mathcal{G}_q and partitions \mathbb{P} and \mathbb{Q} are defined as follows.

$$\begin{aligned} \mathcal{P}^{(1)} &= \{1, 2, 3, 4, 5\}, \quad \mathcal{P}^{(2)} = \{6\}, \\ \mathcal{Q}^{(1)} &= \{1, 2, 3, 6\}, \quad \mathcal{Q}^{(2)} = \{4, 5\}, \\ Z_1 &= 0, \quad Z_2 = 0, \quad Z_3 = 0, \quad Z_4 = 0, \quad Z_5 = 1, \quad Z_6 = 0. \end{aligned}$$

Then we can define an ordered multiset

$$\{(1, 1, 0), (1, 1, 0), (1, 1, 0), (1, 2, 0), (1, 2, 1), (2, 1, 0)\},$$

where the k -th element is associated with index k for $k \in [6]$. By the procedure described above, we can reorder the elements of the multiset as follows.

$$\{(1, 1, 0), (1, 2, 0), (1, 2, 1), (2, 1, 0), (1, 1, 0), (1, 1, 0)\}$$

This reordering corresponds to a permutation π on the set of indices, where $\pi(1) = 1$, $\pi(2) = 5$, $\pi(3) = 6$, $\pi(4) = 2$, $\pi(5) = 3$, $\pi(6) = 4$ (though such a correspondence is not unique). With this permutation, we obtain the following partitions and sequence of weights.

$$\begin{aligned} \mathcal{P}^{(1)} &= \{1, 2, 3, 5, 6\}, \quad \mathcal{P}^{(2)} = \{4\}, \\ \mathcal{Q}^{(1)} &= \{1, 4, 5, 6\}, \quad \mathcal{Q}^{(2)} = \{2, 3\}, \\ Z_1 &= 0, \quad Z_2 = 0, \quad Z_3 = 1, \quad Z_4 = 0, \quad Z_5 = 0, \quad Z_6 = 0. \end{aligned}$$

For the reordered graph, we have

$$\mathcal{R}_1 = \mathcal{R}_2 = \mathcal{R}_3 = \mathcal{R}_4 = \emptyset, \quad \mathcal{R}_5 = \{1\}, \quad \mathcal{R}_6 = \{1, 5\}.$$

Assuming (8), we can prove the following lemma.

Lemma 6. Fix positive integers α, β and m such that $2 \leq \beta < \alpha \leq m \leq q$. Then one has

$$|\mathbb{L}[\mathcal{G}_\alpha]| = (|\mathcal{P}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|) - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| + |\mathcal{R}_\alpha|.$$

For an index set $\mathcal{I} \subset [m]$ such that $|\mathcal{I}| = \alpha$, a sequence of distinct indices $\mathcal{J} = (j_1, \dots, j_{\beta+1}) \in \mathcal{I}^{\beta+1}$, and a sequence of weights $\mathcal{L} \in (\{0, 1\}^n)^\beta$ such that $\mathcal{G}^{++} (= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$ is valid, one has

$$\begin{aligned} |\mathbb{M}[\mathcal{G}^+]| - 2(|\mathcal{R}_{m+1}| + 1) &\leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A, \\ |\mathbb{N}[\mathcal{G}^+]| - 2A(|\mathcal{R}_{m+1}| + 1) &\leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2. \end{aligned}$$

When $\beta = 1$, one has

$$\begin{aligned} |\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - 2(|\mathcal{R}_{m+1}| + 1) &\leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A, \\ |\mathbb{L}[\mathcal{G}^+]| - 2A(|\mathcal{R}_{m+1}| + 1) &\leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2. \end{aligned}$$

Lemma 6 is called the Size Lemma. Its proof is given in Section 4.4

ADDING A SINGLE EDGE TO \mathcal{G}_α . Fix a positive integer m such that $m \leq q$. We will define a two-dimensional sequence $D_{\alpha,\beta}^m$, where $1 \leq \alpha \leq m$ and β is an integer, as follows.

- When $1 \leq \beta \leq \alpha - 1$,

$$D_{\alpha,\beta}^m = \max_{\mathcal{I}, \mathcal{J}, \mathcal{L}} \left\{ \left| \frac{h(\mathcal{G}^+[\mathcal{I}, \mathcal{J}, \mathcal{L}])}{2^n} - h(\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]) \right| \right\},$$

where the maximum is taken over all possible index sets $\mathcal{I} \subset [m]$ such that $|\mathcal{I}| = \alpha$, sequences of distinct indices $\mathcal{J} \in \mathcal{I}^{\beta+1}$, and sequences of weights $\mathcal{L} \in (\{0, 1\}^n)^\beta$ such that $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ is valid.

- When $\beta \leq 0$,

$$D_{\alpha,\beta}^m = 0.$$

In order to upper bound $D_{\alpha,\beta}^m$, we begin with the following lemma.

Lemma 7. *For any $\mathcal{I} \subset [m]$, $\mathcal{J} \in \mathcal{I}^{\beta+1}$, $\mathcal{L} \in (\{0, 1\}^n)^\beta$ such that $|\mathcal{I}| = \alpha$ and $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ is valid, one has*

$$h(\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]) \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}.$$

The proof of Lemma 7 is given in Section 4.5. For $h(\mathcal{G}^{++})(= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$,

$$\frac{h(\mathcal{G}^{++})}{2^n} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta-1} \cdot 2^n} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}.$$

Therefore, we have

$$D_{\alpha,\beta}^m \leq \max \left\{ \frac{h(\mathcal{G}^{++})}{2^n}, h(\mathcal{G}^{++}) \right\} \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+\beta}}. \quad (9)$$

When $\beta = 1$, we have a sharper upper bound on $D_{\alpha,1}^\alpha$ as follows.

Lemma 8. *If $2n + 2 \leq m < q$, then one has*

$$D_{m,1}^m \leq \frac{(15 |\mathcal{R}_{m+1}| + 17)h(\mathcal{G}_m)}{2^{2n}}.$$

The proof is given in Section 4.6. Lemma 5 and 7 are used to prove this lemma. Note that $D_{m,1}^m$ compares the number of solutions between a graph $\mathcal{G}_m (= \mathcal{G}^+[\mathcal{I}, \mathcal{J}, \mathcal{L}])$ and the graph obtained by adding a single edge to \mathcal{G}_m , namely $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$, and Lemma 8 upper bounds their difference.

PROOF OF THEOREM 1. For $m \geq 0$, let

$$H_m = 2^{nm} h(\mathcal{G}_m),$$

$$J_m = \prod_{i=1}^m (2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|).$$

If $\frac{H_q}{J_q} \geq 1 - \varepsilon$ for some $\varepsilon \geq 0$, then we have

$$h(\mathcal{G}_q) = \frac{H_q}{J_q} \cdot \frac{\prod_{i=1}^q (2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^{nq}}$$

$$\geq (1 - \varepsilon) \cdot \prod_{i=1}^q \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n} \right). \quad (10)$$

On the other hand, by Lemma 4, for any $m \leq q - 1$, we have

$$h(\mathcal{G}_{m+1}) = (2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}| + |\mathcal{R}_{m+1}|)h(\mathcal{G}_m) + \sum_{E \in \mathbb{L}[\mathcal{G}_{m+1}]} h(\mathcal{G}_m \cup \{E\}). \quad (11)$$

If $m \geq 2n + 2$ and $(P_i, Q_j, Z_{m+1}) \in \mathbb{L}[\mathcal{G}_{m+1}]$, then we have

$$\left| \frac{h(\mathcal{G}_m)}{2^n} - h(\mathcal{G}_m \cup \{(P_i, Q_j, Z_{m+1})\}) \right| \leq \frac{(15|\mathcal{R}_{m+1}| + 17)h(\mathcal{G}_m)}{2^{2n}}$$

by Lemma 8. So we have

$$h(\mathcal{G}_m \cup \{(P_i, Q_j, Z_{m+1})\}) \geq \frac{h(\mathcal{G}_m)}{2^n} \left(1 - \frac{15|\mathcal{R}_{m+1}| + 17}{2^n} \right). \quad (12)$$

In the following computation, we simply write $a = |\mathcal{P}_{m+1}|$, $b = |\mathcal{Q}_{m+1}|$, $c = |\mathcal{P}_{m+1} \cap \mathcal{Q}_{m+1}|$, and $d = |\mathcal{R}_{m+1}|$. Combining (11), (12) and Lemma 6, we have

$$\frac{h(\mathcal{G}_{m+1})}{h(\mathcal{G}_m)} \geq 2^n - a - b + d + \frac{(a-d)(b-d) - c + d}{2^n} \left(1 - \frac{15d + 17}{2^n} \right).$$

Since $(a-d)(b-d) - c + d \leq ab$, $2^n - a - b - \frac{15ab}{2^n} \geq 0$ and $a, b \leq \frac{2^n}{13}$, we have

$$\begin{aligned} \frac{H_{m+1}}{J_{m+1}} &\geq \frac{2^{2n} - (a+b-d)2^n + ((a-d)(b-d) - c + d) \left(1 - \frac{15d+17}{2^n} \right)}{(2^n - a)(2^n - b)} \cdot \frac{H_m}{J_m} \\ &\geq \left(1 + \frac{d(2^n - a - b - \frac{15ab}{2^n}) - c + d^2 + d - \frac{17ab}{2^n}}{(2^n - a)(2^n - b)} \right) \frac{H_m}{J_m} \\ &\geq \left(1 - \frac{c + \frac{17ab}{2^n}}{(2^n - a)(2^n - b)} \right) \frac{H_m}{J_m} \\ &\geq \left(1 - \frac{2c}{2^{2n}} - \frac{20ab}{2^{3n}} \right) \frac{H_m}{J_m}. \end{aligned}$$

Therefore we have

$$\begin{aligned} \frac{H_q}{J_q} &\geq \prod_{i=2n+3}^q \left(1 - \frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} - \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}} \right) \frac{H_{2n+2}}{J_{2n+2}} \\ &\geq \left(1 - \sum_{i=2n+3}^q \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}} \right) \right) \frac{H_{2n+2}}{J_{2n+2}}. \end{aligned} \quad (13)$$

If $m \leq 2n + 1$, then we have

$$h(\mathcal{G}_{m+1}) \geq (2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}|)h(\mathcal{G}_m)$$

by Lemma 4. Then it follows that

$$\begin{aligned} \frac{H_{m+1}}{J_{m+1}} &\geq \frac{2^n(2^n - |\mathcal{P}_{m+1}| - |\mathcal{Q}_{m+1}|)}{(2^n - |\mathcal{P}_{m+1}|)(2^n - |\mathcal{Q}_{m+1}|)} \cdot \frac{H_m}{J_m} \\ &\geq \left(1 - \frac{|\mathcal{P}_{m+1}||\mathcal{Q}_{m+1}|}{(2^n - |\mathcal{P}_{m+1}|)(2^n - |\mathcal{Q}_{m+1}|)} \right) \frac{H_m}{J_m}. \end{aligned}$$

Since $|\mathcal{P}_{m+1}|, |\mathcal{Q}_{m+1}| \leq \min\{m, \frac{2^n}{13}\}$ and $H_1 = J_1 = 2^{2n}$, we have

$$\begin{aligned} \frac{H_{2n+2}}{J_{2n+2}} &\geq \left(1 - 2 \sum_{i=1}^{2n+1} \frac{i^2}{2^{2n}}\right) \frac{H_1}{J_1} \\ &\geq 1 - \frac{(2n+1)(2n+2)(4n+3)}{3} \cdot \frac{1}{2^{2n}} \geq 1 - \frac{6(n+1)^3}{2^{2n}}. \end{aligned} \quad (14)$$

By combining (13) and (14), we have

$$\begin{aligned} \frac{H_q}{J_q} &\geq \left(1 - \sum_{i=2n+3}^q \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}}\right)\right) \left(1 - \frac{6(n+1)^3}{2^{2n}}\right) \\ &\geq 1 - \sum_{i=1}^q \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}}\right) - \frac{6(n+1)^3}{2^{2n}}. \end{aligned}$$

Setting $\varepsilon = \sum_{i=1}^q \left(\frac{2|\mathcal{P}_i \cap \mathcal{Q}_i|}{2^{2n}} + \frac{20|\mathcal{P}_i||\mathcal{Q}_i|}{2^{3n}}\right) + \frac{6(n+1)^3}{2^{2n}}$ in (10), the proof is completed.

4.2 Proof of Lemma 4

For each solution $S = (X_1, Y_1, \dots, X_{\alpha-1}, Y_{\alpha-1}) \in (\{0, 1\}^n)^{2\alpha-2}$ to $\mathcal{G}_{\alpha-1}$, let

$$\begin{aligned} \mathcal{X} &= \{X_i \mid i \in \mathcal{P}_\alpha\}, \\ \mathcal{Y} &= \{Y_j \oplus Z_\alpha \mid j \in \mathcal{Q}_\alpha\}. \end{aligned}$$

Once S is fixed, one should choose P_α from $\{0, 1\}^n \setminus (\mathcal{X} \cup \mathcal{Y})$. Therefore we have

$$\begin{aligned} h(\mathcal{G}_\alpha) &= \sum_{S \in \mathbb{S}} (2^n - |\mathcal{X} \cup \mathcal{Y}|) \\ &= \sum_{S \in \mathbb{S}} (2^n - |\mathcal{P}_\alpha| - |\mathcal{Q}_\alpha| + |\mathcal{X} \cap \mathcal{Y}|) \\ &= (2^n - |\mathcal{P}_\alpha| - |\mathcal{Q}_\alpha|)h(\mathcal{G}_{\alpha-1}) + \sum_{S \in \mathbb{S}} |\mathcal{X} \cap \mathcal{Y}|, \end{aligned} \quad (15)$$

where \mathbb{S} denotes the set of all solutions to $\mathcal{G}_{\alpha-1}$. In particular, we have

$$\sum_{S \in \mathbb{S}} |\mathcal{X} \cap \mathcal{Y}| = \sum_{S \in \mathbb{S}} \sum_{\substack{i \in \mathcal{P}_\alpha \\ j \in \mathcal{Q}_\alpha}} \mathbf{1}(X_i \oplus Y_j = Z_\alpha).$$

1. If $X_i \oplus Y_i = Z_\alpha$ for $i \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$, then it should be the case that $i \in \mathcal{R}_\alpha$. For each $i \in \mathcal{R}_\alpha$, we have

$$\sum_{S \in \mathbb{S}} \mathbf{1}(X_i \oplus Y_i = Z_\alpha) = \sum_{S \in \mathbb{S}} 1 = h(\mathcal{G}_{\alpha-1}).$$

2. If $i \in \mathcal{P}_\alpha, j \in \mathcal{Q}_\alpha$ and $i \neq j$, then we have

$$\sum_{S \in \mathbb{S}} \mathbf{1}(X_i \oplus Y_j = Z_\alpha) = h(\mathcal{G}_{\alpha-1} \cup \{(P_i, Q_j, Z_\alpha)\}).$$

To summarize, we have

$$\sum_{S \in \mathbb{S}} \sum_{\substack{i \in \mathcal{P}_\alpha \\ j \in \mathcal{Q}_\alpha}} \mathbf{1}(X_i \oplus Y_j = Z_\alpha) = \sum_{S \in \mathbb{S}} \sum_{i \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha} \mathbf{1}(X_i \oplus Y_i = Z_\alpha)$$

$$\begin{aligned}
& + \sum_{S \in \mathbb{S}} \sum_{\substack{i \in \mathcal{P}_\alpha \\ j \in \mathcal{Q}_\alpha \\ i \neq j}} \mathbb{1}(X_i \oplus Y_j = Z_\alpha) \\
& = |\mathcal{R}_\alpha| h(\mathcal{G}_{\alpha-1}) + \sum_{E \in \mathbb{L}[\mathcal{G}_\alpha]} h(\mathcal{G}_{\alpha-1} \cup \{E\}). \quad (16)
\end{aligned}$$

Lemma 4 follows from (15) and (16).

4.3 Proof of Lemma 5

Without loss of generality, we assume that $\mathcal{I} = [\alpha]$, $\mathcal{J} = (\alpha - \beta, \alpha - \beta + 1, \dots, \alpha)$. Let $\mathbb{S} \subset (\{0, 1\}^n)^{2\alpha}$ and $\mathbb{S}' \subset (\{0, 1\}^n)^{2\alpha-2}$ denote the sets of solutions to \mathcal{G}^{++} and \mathcal{G}^+ , respectively. Each solution $(X_1, Y_1, \dots, X_\alpha, Y_\alpha) \in \mathbb{S}$ uniquely determines a solution to \mathcal{G}^+ , namely $(X_1, Y_1, \dots, X_{\alpha-1}, Y_{\alpha-1}) \in \mathbb{S}'$. On the other hand, for each solution $(X_1, Y_1, \dots, X_{\alpha-1}, Y_{\alpha-1}) \in \mathbb{S}'$, let

$$\begin{aligned}
X_\alpha &= X_{\alpha-1} \oplus L_\beta \oplus Z_\alpha, \\
Y_\alpha &= X_{\alpha-1} \oplus L_\beta.
\end{aligned}$$

Then $(X_1, Y_1, \dots, X_\alpha, Y_\alpha)$ is a solution to \mathcal{G}^{++} if and only if X_α and Y_α do not violate the constraints due to the relations $\overset{P}{\sim}$ and $\overset{Q}{\sim}$. For this condition to hold, it should be the case that

$$X_\alpha \neq X_k \Leftrightarrow X_{\alpha-1} \oplus L_\beta \oplus Z_\alpha \neq X_k \Leftrightarrow X_{\alpha-1} \neq X_k \oplus L_\beta \oplus Z_\alpha$$

for any index k such that $k \overset{P}{\sim} \alpha$. Furthermore, for an index k such $k \overset{Q}{\sim} \alpha$, the following non-equation is also required.

$$Y_\alpha \neq Y_k \Leftrightarrow X_{\alpha-1} \neq Y_k \oplus L_\beta.$$

So, for each solution $(X_1, Y_1, \dots, X_{\alpha-1}, Y_{\alpha-1}) \in \mathbb{S}'$, $(X_1, Y_1, \dots, X_\alpha, Y_\alpha)$ becomes a solution to \mathcal{G}^{++} if and only if $X_{\alpha-1} \in \{0, 1\}^n \setminus (\mathcal{X} \cup \mathcal{Y})$, where

$$\begin{aligned}
\mathcal{X} &\stackrel{\text{def}}{=} \{X_k \oplus L_\beta \oplus Z_\alpha \mid k \in \mathcal{P}_\alpha\}, \\
\mathcal{Y} &\stackrel{\text{def}}{=} \{Y_k \oplus L_\beta \mid k \in \mathcal{Q}_\alpha\}.
\end{aligned}$$

Therefore we have

$$\begin{aligned}
h(\mathcal{G}^{++}) &= \sum_{S \in \mathbb{S}'} (1 - \mathbb{1}(X_{\alpha-1} \in \mathcal{X} \cup \mathcal{Y})) \\
&= h(\mathcal{G}^+) - \sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X}) \\
&\quad - \sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{Y}) + \sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X} \cap \mathcal{Y}). \quad (17)
\end{aligned}$$

Suppose that $X_{\alpha-1} \in \mathcal{X}$, in which case $X_\alpha = X_k$ for some $k \in \mathcal{P}_\alpha$.

1. If $k \in \mathcal{P}_\alpha[\mathcal{J}]$, then there exists a trail $T(X_k, X_\alpha)$ such that

$$w(T(X_k, X_\alpha)) \neq \mathbf{0}$$

since \mathcal{G}^{++} is a valid graph. It implies that $X_\alpha \neq X_k$, which is a contradiction.

2. If $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]$, then a solution to \mathcal{G}^{+-} such that $X_\alpha = X_k$ becomes a solution to

$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta \oplus Z_k \oplus Z_\alpha)\}.$$

Suppose that $X_{\alpha-1} \in \mathcal{Y}$, in which case $Y_\alpha = Y_k$ for some $k \in \mathcal{Q}_\alpha$. Then it follows that $k \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$. Furthermore, a solution to \mathcal{G}^{+-} such that $Y_\alpha = Y_k$ becomes a solution to a graph

$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta)\}.$$

To summarize, we have

$$\sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X}) = \sum_{E \in \mathbb{M}_1} h(\mathcal{G}^{+-} \cup \{E\}), \quad (18)$$

$$\sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{Y}) = \sum_{E \in \mathbb{M}_2} h(\mathcal{G}^{+-} \cup \{E\}), \quad (19)$$

where

$$\begin{aligned} \mathbb{M}_1 &\stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta \oplus Z_k \oplus Z_\alpha) \mid k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]\}, \\ \mathbb{M}_2 &\stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta) \mid k \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]\}. \end{aligned}$$

Suppose that $X_{\alpha-1} \in \mathcal{X} \cap \mathcal{Y}$, in which case

$$\begin{aligned} X_{\alpha-1} &= X_k \oplus L_\beta \oplus Z_\alpha, \\ X_{\alpha-1} &= Y_l \oplus L_\beta \end{aligned}$$

for some $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$. Replacing X_k by $Y_k \oplus Z_k$ in the first equation, and $X_{\alpha-1}$ by $X_k \oplus L_\beta \oplus Z_\alpha$ in the second equation, we have

$$\begin{aligned} X_{\alpha-1} \oplus Y_k &= L_\beta \oplus Z_k \oplus Z_\alpha, \\ X_k \oplus Y_l &= Z_\alpha. \end{aligned}$$

There are two cases.

1. If $k \neq l$, then a solution to \mathcal{G}^{+-} such that $X_{\alpha-1} \oplus Y_k = L_\beta \oplus Z_k \oplus Z_\alpha$ and $X_k \oplus Y_l = Z_\alpha$ is a solution to a graph

$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta \oplus Z_k \oplus Z_\alpha), (X_k, Y_l, Z_\alpha)\}.$$

2. If $k = l$, then $k \in \mathcal{P}_\alpha[\mathcal{I} \setminus \mathcal{J}] \cap \mathcal{Q}_\alpha[\mathcal{I} \setminus \mathcal{J}]$.

- (a) If $Z_k = Z_\alpha$, then edge (X_k, Y_l, Z_α) is redundant. Therefore, a solution to \mathcal{G}^{+-} such that $X_{\alpha-1} \oplus Y_k = L_\beta \oplus Z_k \oplus Z_\alpha$ and $X_k \oplus Y_l = Z_\alpha$ is a solution to a graph

$$\mathcal{G}^{+-} \cup \{(X_{\alpha-1}, Y_k, L_\beta)\}.$$

- (b) If $Z_k \neq Z_\alpha$, then there is no solution to the graph.

Therefore we have

$$\sum_{S \in \mathbb{S}'} \mathbb{1}(X_{\alpha-1} \in \mathcal{X} \cap \mathcal{Y}) = \sum_{E \in \mathbb{M}_3} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}) \quad (20)$$

where

$$\mathbb{M}_3 \stackrel{\text{def}}{=} \{(P_{\alpha-1}, Q_k, L_\beta) \mid k \in \mathcal{R}_\alpha[\mathcal{I} \setminus \mathcal{J}]\}.$$

Since

$$\begin{aligned} \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{++} \cup \{E\}) &= \sum_{E \in \mathbb{M}_1 \cup \mathbb{M}_2} h(\mathcal{G}^{++} \cup \{E\}) \\ &= \sum_{E \in \mathbb{M}_1} h(\mathcal{G}^{++} \cup \{E\}) + \sum_{E \in \mathbb{M}_2} h(\mathcal{G}^{++} \cup \{E\}) - \sum_{E \in \mathbb{M}_3} h(\mathcal{G}^{++} \cup \{E\}) \end{aligned}$$

and by (17), (18), (19) and (20), the proof is complete.

4.4 Proof of Lemma 6

We can prove the five (in)equalities as follows.

1. Each edge $(P_i, Q_j, Z_\alpha) \in \mathbb{L}[\mathcal{G}_\alpha]$ falls into one of the following four cases.

- Case 1: $i \in \mathcal{P}_\alpha \setminus \mathcal{Q}_\alpha$ and $j \in \mathcal{Q}_\alpha \setminus \mathcal{P}_\alpha$. Note that $\mathcal{G}_\alpha \cup \{(P_i, Q_j, Z_\alpha)\}$ is valid. The number of edges of this type is

$$(|\mathcal{P}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$

- Case 2: $i \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ and $j \in \mathcal{Q}_\alpha \setminus \mathcal{P}_\alpha$. Equations $P_i \oplus Q_j = Z_\alpha$ and $P_i \oplus Q_i = Z_i$ imply $Q_i \oplus Q_j = Z_\alpha \oplus Z_i$. Since $i \stackrel{\mathcal{Q}}{\sim} j$, it should be the case that $Z_i \neq Z_\alpha$. The number of such edges is

$$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$

- Case 3: $i \in \mathcal{P}_\alpha \setminus \mathcal{Q}_\alpha$ and $j \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$. Similarly to Case 2, we see that the number of edges of this type is

$$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{P}_\alpha| - |\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha|).$$

- Case 4: $i, j \in \mathcal{P}_\alpha \cap \mathcal{Q}_\alpha$ where $i \neq j$. It should be the case that $Z_i \neq Z_\alpha$ and $Z_j \neq Z_\alpha$ since otherwise the resulting graph is invalid. The number of such edges is

$$(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha| - 1).$$

Therefore, we conclude that

$$|\mathbb{L}[\mathcal{G}_\alpha]| = (|\mathcal{P}_\alpha| - |\mathcal{R}_\alpha|)(|\mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|) - (|\mathcal{P}_\alpha \cap \mathcal{Q}_\alpha| - |\mathcal{R}_\alpha|).$$

2. Note that $\mathbb{M}[\mathcal{G}^{++}] \subset \mathbb{M}[\mathcal{G}^{+}]$ when $\beta \geq 2$. Each edge E in $\mathbb{M}[\mathcal{G}^{+}] \setminus \mathbb{M}[\mathcal{G}^{++}]$ is of the form either $(P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$ or $(P_{j_\beta}, Q_k, L_\beta)$ for $k \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Such an edge falls into at least one of the following three cases.

- Case 1: $k = j_1$. At most two edges fall into this case.

- Case 2: $E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for $k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Since $E \in \mathbb{M}[\mathcal{G}^+] \setminus \mathbb{M}[\mathcal{G}^{++}]$, \mathcal{G}^{++} and $\mathcal{G}^{--} \cup \{E\}$ are valid, while $\mathcal{G}^{+-} \cup \{E\}$ is invalid, which means that $k \stackrel{Q}{\sim} j_1$, and $w(T(Q_{j_1}, Q_k)) = \mathbf{0}$ for a (unique) trail $T(Q_{j_1}, Q_k)$ connecting Q_{j_1} and Q_k , which means

$$Z_k = Z_{j_1} \oplus \dots \oplus Z_{j_{\beta+1}} \oplus L_1 \oplus \dots \oplus L_\beta \stackrel{\text{def}}{=} Z.$$

The number of such edges E is at most $|\{k \in \mathcal{P}_{j_{\beta+1}} \cap \mathcal{Q}_{j_1} \mid Z_k = Z\}|$, where by (8)

$$|\{k \in \mathcal{P}_{j_{\beta+1}} \cap \mathcal{Q}_{j_1} \mid Z_k = Z\}| \leq |\mathcal{R}_{m+1}|.$$

- Case 3: $E = (P_{j_\beta}, Q_k, L_\beta)$ for $k \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Similarly to Case 2, we see that the number of edges of this type is at most $|\mathcal{R}_{m+1}|$.

It is easy to see that $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$. Therefore, we conclude that

$$|\mathbb{M}[\mathcal{G}^+]| - 2(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A.$$

- Note that $\mathbb{N}[\mathcal{G}^{++}] \subset \mathbb{N}[\mathcal{G}^+]$ when $\beta \geq 2$. For each pair of edges $\{E, E'\}$ in $\mathbb{N}[\mathcal{G}^+] \setminus \mathbb{N}[\mathcal{G}^{++}]$, we can assume that $E = (P_{j_\beta}, Q_k, L_\beta \oplus Z_k \oplus Z_{j_{\beta+1}})$ for some $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$, and $E' = (P_k, Q_l, Z_{j_{\beta+1}})$ for some l such that $l \neq k$ and $l \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Such a pair (E, E') falls into at least one of the following three cases.

- Case 1: $k \in \mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$ and $l = j_1$. Since

$$|\mathcal{P}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]| \leq A,$$

and the number of pairs of edges of this type is at most A .

- Case 2: $k = j_1$ and $l \in \mathcal{Q}_{j_{\beta+1}}[(\mathcal{I} \setminus \mathcal{J}) \cup \{j_1\}]$. Similarly to Case 1, the number of pairs of edges of this type is at most A .
- Case 3: $k \in \mathcal{P}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_{j_{\beta+1}}[\mathcal{I} \setminus \mathcal{J}]$. Since $\mathcal{G}^{+-} \cup \{E, E'\}$ is invalid, there exist $k', l' \in \{j_1, \dots, j_\beta, k, l\}$ such that either

$$k' \stackrel{Q}{\sim} l' \wedge w(T(Q_{k'}, Q_{l'})) = \mathbf{0}$$

for a (unique) trail $T(Q_{k'}, Q_{l'})$ connecting $Q_{k'}$ and $Q_{l'}$, or

$$k' \stackrel{P}{\sim} l' \wedge w(T(P_{k'}, P_{l'})) = \mathbf{0}$$

for a (unique) trail $T(P_{k'}, P_{l'})$ connecting $P_{k'}$ and $P_{l'}$. Since \mathcal{G}^{++} and $\mathcal{G}^{--} \cup \{E, E'\}$ are valid, two possibilities remain as follows.

- $k \stackrel{Q}{\sim} j_1$ and $w(T(Q_k, Q_{j_1})) = \mathbf{0}$ for a (unique) trail $T(Q_k, Q_{j_1})$ connecting Q_{j_1} and Q_k , which means

$$Z_k = Z_{j_1} \oplus \dots \oplus Z_{j_{\beta+1}} \oplus L_1 \oplus \dots \oplus L_\beta.$$

The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|A$.

- $l \stackrel{P}{\sim} j_1$ and $w(T(P_l, P_{j_1})) = \mathbf{0}$ for a (unique) trail $T(P_l, P_{j_1})$ connecting P_{j_1} and P_l , which means

$$Z_l = Z_{j_2} \oplus \dots \oplus Z_{j_\beta} \oplus L_1 \oplus \dots \oplus L_\beta.$$

The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|A$.

It is easy to see that $|\mathbb{N}[\mathcal{G}^{++}]| \leq A^2$. Therefore, we conclude that

$$|\mathbb{N}[\mathcal{G}^{++}]| - 2A(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2.$$

4. Suppose that $\beta = 1$. Let \mathbb{M}' be the set of edges of the form either (P_{j_1}, Q_k, L_1) for $k \in \mathcal{Q}_{j_2}[\mathcal{I}]$ or $(P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ for $k \in \mathcal{P}_{j_2}[\mathcal{I}]$. Note that $|\mathbb{M}'| = |\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]|$ and $\mathbb{M}[\mathcal{G}^{++}] \subset \mathbb{M}'$. Each edge E in $\mathbb{M}' \setminus \mathbb{M}[\mathcal{G}^{++}]$ falls into at least one of the following three cases.

- Case 1: $k = j_1$. At most two edges fall into this case.
- Case 2: $E = (P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ for $k \in \mathcal{P}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Since $E \in \mathbb{M}' \setminus \mathbb{M}[\mathcal{G}^{++}]$, \mathcal{G}^{++} is valid, while $\mathcal{G}^{++} \cup \{E\}$ is invalid, which means that $k \stackrel{Q}{\sim} j_1$, and $w(T(Q_{j_1}, Q_k)) = \mathbf{0}$ for a (unique) trail $T(Q_{j_1}, Q_k)$ connecting Q_{j_1} and Q_k , which means

$$Z_k = Z_{j_1} \oplus Z_{j_2} \oplus L_1 \stackrel{\text{def}}{=} Z'.$$

The number of such edges E is at most $|\{k \in \mathcal{P}_{j_2} \cap \mathcal{Q}_{j_1} \mid Z_k = Z'\}|$, where by (8)

$$|\{k \in \mathcal{P}_{j_2} \cap \mathcal{Q}_{j_1} \mid Z_k = Z'\}| \leq |\mathcal{R}_{m+1}|.$$

- Case 3: $E = (P_{j_1}, Q_k, L_1)$ for $k \in \mathcal{Q}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Similarly to Case 2, we see that the number of edges of this type is at most $|\mathcal{R}_{m+1}|$.

It is easy to see that $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$. Therefore, we conclude that

$$|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - 2(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{M}[\mathcal{G}^{++}]| \leq 2A.$$

5. Suppose that $\beta = 1$. Let \mathbb{N}' denote the set of pairs of edges $\{E, E'\}$ where $E = (P_{j_1}, Q_k, L_1 \oplus Z_k \oplus Z_{j_2})$ and $E' = (P_l, Q_l, Z_{j_2})$ such that $k \in \mathcal{P}_{j_2}[\mathcal{I}]$, $l \in \mathcal{Q}_{j_2}[\mathcal{I}]$, $k \neq l$ and $h(\mathcal{G}^{++} \cup \{E'\}) > 0$. Then we have $\mathbb{N}[\mathcal{G}^{++}] \subset \mathbb{N}'$ and $|\mathbb{N}'| = |\mathbb{L}[\mathcal{G}^{++}]|$ since $\mathbb{L}[\mathcal{G}^{++}]$ is obtained by collecting E' for all $\{E, E'\} \in \mathbb{N}'$. Each pair $\{E, E'\} \in \mathbb{N}' \setminus \mathbb{N}[\mathcal{G}^{++}]$ falls into at least one of the following three cases.

- Case 1: $k \in \mathcal{P}_{j_2}[\mathcal{I}]$ and $l = j_1$. Since $|\mathcal{P}_{j_2}[\mathcal{I}]| \leq A$, the number of pairs of edges of this type is at most A .
- Case 2: $k = j_1$ and $l \in \mathcal{Q}_{j_2}[\mathcal{I}]$. Similarly to Case 1, the number of pairs of edges of this type is at most A .
- Case 3: $k \in \mathcal{P}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$ and $l \in \mathcal{Q}_{j_2}[\mathcal{I} \setminus \mathcal{J}]$. Since $\{E, E'\} \in \mathbb{N}' \setminus \mathbb{N}[\mathcal{G}^{++}]$, \mathcal{G}^{++} and $\mathcal{G}^{++} \cup \{E'\}$ are valid, while $\mathcal{G}^{++} \cup \{E, E'\}$ is invalid. Then at least one of the following two conditions holds:
 - (a) $k \stackrel{Q}{\sim} j_1$ and $w(T(Q_k, Q_{j_1})) = \mathbf{0}$ for a (unique) trail $T(Q_k, Q_{j_1})$ connecting Q_{j_1} and Q_k , which means $Z_k = Z_{j_1} \oplus Z_{j_2} \oplus L_1$. The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|A$.
 - (b) $l \stackrel{P}{\sim} j_1$ and $w(T(P_l, P_{j_1})) = \mathbf{0}$ for a (unique) trail $T(P_l, P_{j_1})$ connecting P_{j_1} and P_l , which means $Z_l = L_1$. The number of pairs of edges of this type is at most $|\mathcal{R}_{m+1}|A$.

It is easy to see that $|\mathbb{N}[\mathcal{G}^{++}]| \leq A^2$. Therefore we conclude that

$$|\mathbb{L}[\mathcal{G}^{++}]| - 2A(|\mathcal{R}_{m+1}| + 1) \leq |\mathbb{N}[\mathcal{G}^{++}]| \leq A^2.$$

4.5 Proof of Lemma 7

Without loss of generality, we assume that $\mathcal{I} = [\alpha]$. Let \mathbb{S} denote the set of solutions to \mathcal{G}_α . For each solution $(X_1, Y_1, \dots, X_\alpha, Y_\alpha) \in \mathbb{S}$, $(X_1, Y_1, \dots, X_{\alpha+1}, Y_{\alpha+1})$ becomes a solution to $\mathcal{G}_{\alpha+1}$ if and only if $X_{\alpha+1} \in \{0, 1\}^n \setminus (\mathcal{X} \cup \mathcal{Y})$, where

$$\begin{aligned}\mathcal{X} &\stackrel{\text{def}}{=} \left\{ X_i \mid i \stackrel{\mathcal{P}}{\sim} (\alpha + 1), i \in [\alpha] \right\}, \\ \mathcal{Y} &\stackrel{\text{def}}{=} \left\{ Y_i \oplus Z_{\alpha+1} \mid i \stackrel{\mathcal{Q}}{\sim} (\alpha + 1), i \in [\alpha] \right\}.\end{aligned}$$

Therefore, we have

$$h(\mathcal{G}_{\alpha+1}) \geq \sum_{S \in \mathbb{S}} (2^n - |\mathcal{X} \cup \mathcal{Y}|) \geq (2^n - 2A)h(\mathcal{G}_\alpha).$$

By repeatedly applying the above inequality, we have

$$h(\mathcal{G}_\alpha) \leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha}}, \quad (21)$$

which completes the proof of Lemma 7 when $\beta = 0$.

Suppose that $\beta \geq 1$. Fix $\mathcal{J} = (\alpha - \beta, \alpha - \beta + 1, \dots, \alpha)$ without loss of generality, and let $\mathcal{L} = (L_1, \dots, L_\beta) \in (\{0, 1\}^n)^\beta$. For each solution $(X_1, Y_1, \dots, X_\alpha, Y_\alpha)$ to $\mathcal{G}^{++} (= \mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}])$, $X_{\alpha-\beta}$ and $Y_{\alpha-\beta}$ can be replaced by $X'_{\alpha-\beta}$ and $Y'_{\alpha-\beta}$, respectively, giving a solution to \mathcal{G}^+ , if $X'_{\alpha-\beta} \in \{0, 1\}^n \setminus (\mathcal{X}' \cup \mathcal{Y}')$ and $Y'_{\alpha-\beta} = X'_{\alpha-\beta} \oplus Z_{\alpha-\beta}$, where

$$\begin{aligned}\mathcal{X}' &\stackrel{\text{def}}{=} \left\{ X_i \mid i \stackrel{\mathcal{P}}{\sim} (\alpha - \beta), i \in [\alpha] \setminus \{\alpha - \beta\} \right\}, \\ \mathcal{Y}' &\stackrel{\text{def}}{=} \left\{ Y_i \oplus Z_{\alpha-\beta} \mid i \stackrel{\mathcal{Q}}{\sim} (\alpha - \beta), i \in [\alpha] \setminus \{\alpha - \beta\} \right\}.\end{aligned}$$

Therefore, we have

$$h(\mathcal{G}^{++}) \geq \sum_{S \in \mathbb{S}'} (2^n - |\mathcal{X}' \cup \mathcal{Y}'|) \geq (2^n - 2A)h(\mathcal{G}^{++}),$$

where \mathbb{S}' denotes the set of all solutions to \mathcal{G}^{++} . By repeatedly applying the above inequality, we have

$$h(\mathcal{G}^{++}) \leq \frac{h(\mathcal{G}_\alpha)}{(2^n - 2A)^\beta} \quad (22)$$

The proof is complete by (21) and (22).

4.6 Proof of Lemma 8

We will prove that if $2 \leq \alpha \leq m$ and $\beta \leq \alpha - 3$, then

$$D_{\alpha,\beta}^m \leq D_{\alpha-1,\beta-1}^m + 2A \cdot D_{\alpha-1,\beta}^m + A^2 \cdot D_{\alpha-1,\beta+1}^m + \frac{C}{(2^n - 2A)^{m-\alpha+\beta}}, \quad (23)$$

where

$$C \stackrel{\text{def}}{=} \frac{(3|\mathcal{R}_{m+1}| + 3)h(\mathcal{G}_m)}{2^n}.$$

The proof of (23) will be given at the end of this section. Then, by Lemma 2, we obtain an upper bound on $D_{\alpha,1}^m$ as follows.

$$D_{\alpha,1}^m \leq \sum_{i=n}^{2n} \binom{2n}{i} A^i D_{\alpha-n,1+i-n}^m + \sum_{j=0}^{n-1} \sum_{i=j}^{2j} \binom{2j}{i} \frac{A^i C}{(2^n - 2A)^{m-\alpha+i+1}} \quad (24)$$

for $n \leq \frac{\alpha}{2} - 1$. Since $\binom{2n}{i} \leq \left(\frac{2en}{i}\right)^i \leq (2e)^i$ when $n \leq i \leq 2n$ and $\frac{2eA}{2^n - 2A} \leq \frac{1}{2}$, and by (9), we have

$$\begin{aligned} \sum_{i=n}^{2n} \binom{2n}{i} A^i D_{\alpha-n, 1+i-n}^m &\leq \sum_{i=n}^{2n} \binom{2n}{i} \frac{A^i h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+i+1}} \\ &\leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+1}} \sum_{i=n}^{2n} \left(\frac{2eA}{2^n - 2A}\right)^i \\ &\leq \frac{h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+1}} \sum_{i=n}^{\infty} \left(\frac{1}{2}\right)^i \\ &\leq \frac{2h(\mathcal{G}_m)}{(2^n - 2A)^{m-\alpha+1}} \cdot \frac{1}{2^n}. \end{aligned} \quad (25)$$

We also have

$$\begin{aligned} \sum_{j=0}^{n-1} \sum_{i=j}^{2j} \binom{2j}{i} \left(\frac{A}{2^n - 2A}\right)^i &\leq \sum_{j=0}^{n-1} \sum_{i=j}^{2j} \left(\frac{2eA}{2^n - 2A}\right)^i \\ &\leq 2 \sum_{j=0}^{\infty} \frac{1}{2^j} \leq 4. \end{aligned} \quad (26)$$

By (24), (25) and (26) with $\alpha = m$, we have

$$D_{m,1}^m \leq \frac{2h(\mathcal{G}_m)}{2^{2n}} + \frac{(12|\mathcal{R}_{m+1}| + 12)h(\mathcal{G}_m)}{(2^n - 2A)2^n} \leq \frac{(15|\mathcal{R}_{m+1}| + 17)h(\mathcal{G}_m)}{2^{2n}}.$$

PROOF OF (23). When $\alpha \in \{2, 3\}$, (23) trivially holds since $D_{\alpha,\beta}^m$ is nonnegative and $D_{\alpha,\beta}^m = 0$ when $\beta \leq 0$. So we can assume that $\alpha \geq 4$.

First, suppose that $2 \leq \beta \leq \alpha - 3$. For any $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ such that $|\mathcal{I}| = \alpha$, $\mathcal{J} \in \mathcal{I}^{\beta+1}$, and $\mathcal{L} \in \{0, 1\}^n$, we have

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}), \quad (27)$$

$$h(\mathcal{G}^{+-}) = h(\mathcal{G}^{--}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{+-}]} h(\mathcal{G}^{--} \cup \{E\}) + \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{+-}]} h(\mathcal{G}^{--} \cup \{E, E'\}) \quad (28)$$

by Lemma 5. Since $\mathcal{G}^{--} = (\mathcal{G}^{+-})^+$, we have

$$\left| \frac{h(\mathcal{G}^{--})}{2^n} - h(\mathcal{G}^{+-}) \right| \leq D_{\alpha-1, \beta-1}^m. \quad (29)$$

For each edge $E \in \mathbb{M}[\mathcal{G}^{++}]$, we have

$$\left| \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq D_{\alpha-1, \beta}^m.$$

Since $|\mathbb{M}[\mathcal{G}^{++}]| \leq 2A$ and $|\mathbb{M}[\mathcal{G}^{+-}] \setminus \mathbb{M}[\mathcal{G}^{++}]| \leq 2|\mathcal{R}_{m+1}| + 2$ by Lemma 6, and by Lemma 7, we have

$$\left| \sum_{E \in \mathbb{M}[\mathcal{G}^{+-}]} \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) \right|$$

$$\begin{aligned}
 &\leq \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} \left| \frac{h(\mathcal{G}^- \cup \{E\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E\}) \right| + \sum_{E \in \mathbb{M}[\mathcal{G}^{++}] \setminus \mathbb{M}[\mathcal{G}^{++}]} \left| \frac{h(\mathcal{G}^- \cup \{E\})}{2^n} \right| \\
 &\leq 2A \cdot D_{\alpha-1, \beta}^m + \frac{2(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta}}, \tag{30}
 \end{aligned}$$

where $\mathcal{G}^- \cup \{E\}$ can be seen as $\mathcal{G}[\mathcal{I}', \mathcal{J}', \mathcal{L}']$ for some \mathcal{I}' , \mathcal{J}' , and \mathcal{L}' such that $|\mathcal{I}'| = \alpha - 1$ and $|\mathcal{J}'| = \beta - 1$.

For each pair of edges $\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]$, we have $\mathcal{G}^- \cup \{E, E'\} = (\mathcal{G}^{+-} \cup \{E, E'\})^{-+}$, and hence

$$\left| \frac{h(\mathcal{G}^- \cup \{E, E'\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \leq D_{\alpha-1, \beta+1}^m.$$

Since $|\mathbb{N}[\mathcal{G}^{++}]| \leq A^2$ and $|\mathbb{N}[\mathcal{G}^{++}] \setminus \mathbb{N}[\mathcal{G}^{++}]| \leq 2A(|\mathcal{R}_{m+1}| + 1)$ by Lemma 6, and by Lemma 7, we have

$$\begin{aligned}
 &\left| \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} \frac{h(\mathcal{G}^- \cup \{E, E'\})}{2^n} - \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \\
 &\leq A^2 \cdot D_{\alpha-1, \beta+1}^m + \frac{2A(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta+1}}. \tag{31}
 \end{aligned}$$

By subtracting (27) from $\frac{1}{2^n} \times$ (28), combined with (29), (30) and (31), we have

$$\begin{aligned}
 \left| \frac{h(\mathcal{G}^{++})}{2^n} - h(\mathcal{G}^{++}) \right| &\leq D_{\alpha-1, \beta-1}^m + 2A \cdot D_{\alpha-1, \beta}^m + A^2 \cdot D_{\alpha-1, \beta+1}^m \\
 &\quad + \frac{(2|\mathcal{R}_{m+1}| + 2)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta}} + \frac{2A(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta+1}}.
 \end{aligned}$$

Since $\frac{2A}{2^n - 2A} \leq 1$, we have

$$D_{\alpha, \beta}^m \leq D_{\alpha-1, \beta-1}^m + 2A \cdot D_{\alpha-1, \beta}^m + A^2 \cdot D_{\alpha-1, \beta+1}^m + \frac{(3|\mathcal{R}_{m+1}| + 3)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta}}.$$

Next, suppose that $\beta = 1$. Consider $\mathcal{G}[\mathcal{I}, \mathcal{J}, \mathcal{L}]$ such that $|\mathcal{I}| = \alpha$, $\mathcal{J} = (j_1, j_2)$ for some $j_1, j_2 \in \mathcal{I}$, and $\mathcal{L} = (L)$ for some $L \in \{0, 1\}^n$. By definition, we have $\mathcal{G}^{++} = \mathcal{G}[\mathcal{I}]$ and $\mathcal{G}^{--} = \mathcal{G}[\mathcal{I} \setminus \{j_2\}]$. Applying the (generalized) Orange equation to \mathcal{G}^{++} , we have

$$h(\mathcal{G}^{++}) = h(\mathcal{G}^{+-}) - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) + \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}), \tag{32}$$

$$\begin{aligned}
 h(\mathcal{G}^{++}) &= (2^n - |\mathcal{P}_{j_2}[\mathcal{I}]| - |\mathcal{Q}_{j_2}[\mathcal{I}]| + |\mathcal{R}_{j_2}[\mathcal{I}]|)h(\mathcal{G}^{--}) \\
 &\quad + \sum_{E \in \mathbb{L}[\mathcal{G}^{++}]} h(\mathcal{G}^{--} \cup \{E\}). \tag{33}
 \end{aligned}$$

Since $\mathcal{G}^{+-} = \mathcal{G}^{--}$, we have

$$h(\mathcal{G}^{--}) - h(\mathcal{G}^{+-}) = 0. \tag{34}$$

For each edge $E \in \mathbb{M}[\mathcal{G}^{++}]$, we have

$$\left| \frac{h(\mathcal{G}^{--})}{2^n} - h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq D_{\alpha-1, 1}^m.$$

Since $\mathbb{M}[\mathcal{G}^{++}] \leq 2A$ and

$$|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| - |\mathbb{M}[\mathcal{G}^{++}]| \leq 2|\mathcal{R}_{m+1}| + 2$$

by Lemma 6, and by Lemma 7, we have

$$\left| \left(|\mathcal{P}_{j_2}[\mathcal{I}]| + |\mathcal{Q}_{j_2}[\mathcal{I}]| - |\mathcal{R}_{j_2}[\mathcal{I}]| \right) \frac{h(\mathcal{G}^{--})}{2^n} - \sum_{E \in \mathbb{M}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E\}) \right| \leq 2A \cdot D_{\alpha-1,1}^m + \frac{2(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+1}}. \quad (35)$$

Note that each edge $E = (P_k, Q_l, Z_{j_2}) \in \mathbb{L}[\mathcal{G}^{--}]$ uniquely determines an edge $E' = (P_{j_1}, Q_k, L \oplus Z_k \oplus Z_{j_2}) \in \mathbb{N}[\mathcal{G}^{++}]$. For such a pair of edges, we have

$$\left| \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \leq D_{\alpha-1,2}^m.$$

It implies that

$$\left| \sum_{E \in \mathbb{L}[\mathcal{G}^{--}]} \frac{h(\mathcal{G}^{--} \cup \{E\})}{2^n} - \sum_{\{E, E'\} \in \mathbb{N}[\mathcal{G}^{++}]} h(\mathcal{G}^{+-} \cup \{E, E'\}) \right| \leq A^2 \cdot D_{\alpha-1,\beta+1}^m + \frac{2A(|\mathcal{R}_{m+1}| + 1)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta+1}}. \quad (36)$$

By subtracting (32) from $\frac{1}{2^n} \times$ (33), combined with (34), (35) and (36), we have

$$D_{\alpha,1}^m \leq 2A \cdot D_{\alpha-1,1}^m + A^2 \cdot D_{\alpha-1,2}^m + \frac{(3|\mathcal{R}_{m+1}| + 3)h(\mathcal{G}_m)}{2^n(2^n - 2A)^{m-\alpha+\beta}}.$$

5 TPRP-based PRFs: MXoP_c and XoTP_c

In this section, we propose a PRF construction XoTP_c, and prove the security of MXoP_c and XoTP_c, where each construction is based on two n -bit TPRPs \tilde{P} and \tilde{Q} using t -bit tweaks. We will assume that they are independent TURPs.

5.1 MXoP: Multiple Instances of XoP

As stated in the introduction, similar proofs may be able to be followed from previous analyses of multi-user security of XoP. However, we could not find any explicit proof for full security of XoP in the multi-user setting.

Given a constant $C \in \{0, 1\}^c$ for an integer c such that $0 \leq c \leq n$, a $(t + n - c)$ -to- n bit pseudorandom function MXoP_c is defined as follows.

$$\text{MXoP}_c(X, Y) \stackrel{\text{def}}{=} \tilde{P}(Y, C \parallel X) \oplus \tilde{Q}(Y, C \parallel X)$$

for $X \in \{0, 1\}^{n-c}$ and $Y \in \{0, 1\}^t$.

SECURITY OF MXoP_c. Suppose that a distinguisher \mathcal{D} makes q queries $(X_i, Y_i) \in \{0, 1\}^{n-c} \times \{0, 1\}^t$, obtaining the corresponding responses Z_i for $i = 1, \dots, q$. In this way, \mathcal{D} obtains a transcript

$$\tau = ((X_1, Y_1, Z_1), \dots, (X_q, Y_q, Z_q)).$$

In the real world, $P_i \stackrel{\text{def}}{=} \tilde{\mathbb{P}}(Y_i, C \parallel X_i)$ and $Q_i \stackrel{\text{def}}{=} \tilde{\mathbb{Q}}(Y_i, C \parallel X_i)$ should be a solution to the following system of equations.

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \quad \quad \quad \vdots \\ P_q \oplus Q_q = Z_q, \end{cases}$$

subject to the partitions $\mathbb{P} = \{\mathcal{P}^{(M)}\}_{M \in \{0,1\}^t}$ and $\mathbb{Q} = \{\mathcal{Q}^{(M)}\}_{M \in \{0,1\}^t}$, where

$$(\mathcal{Q}^{(M)} =) \mathcal{P}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid Y_i = M\}$$

ignoring repetition of the same block. Since \mathcal{D} is allowed to make at most 2^{n-c} queries for each tweak,³ we have

$$\begin{aligned} A &= \max_{M \in \{0,1\}^t} \left\{ |\mathcal{P}^{(M)}|, |\mathcal{Q}^{(M)}| \right\} \leq 2^{n-c}, \\ B &= \max_{M, M' \in \{0,1\}^t} \left\{ |\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}| \right\} \leq 2^{n-c}. \end{aligned}$$

By Corollary 1, if $c \geq 4$ (and hence $A \leq 2^{n-4}$), then we have

$$\begin{aligned} h(\tau, \tilde{\mathcal{P}}, \tilde{\mathcal{Q}}) &\geq \left(1 - \frac{2q}{2^{n+c}} - \min \left\{ \frac{20q^2}{2^{2n+c}}, \frac{20q}{2^{n+2c}} \right\} - \frac{6(n+1)^3}{2^{2n}} \right) \\ &\quad \times \prod_{i=1}^q \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n} \right). \end{aligned}$$

Since

$$\begin{aligned} \Pr[\text{T}_{\text{re}} = \tau] &= \frac{h(\tau, \tilde{\mathcal{P}}, \tilde{\mathcal{Q}})}{\prod_{i=1}^q (2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}, \\ \Pr[\text{T}_{\text{id}} = \tau] &= \frac{1}{(2^n)^q}, \end{aligned}$$

we have

$$\begin{aligned} \frac{\Pr[\text{T}_{\text{re}} = \tau]}{\Pr[\text{T}_{\text{id}} = \tau]} &\geq 1 - \frac{2q}{2^{n+c}} - \min \left\{ \frac{20q^2}{2^{2n+c}}, \frac{20q}{2^{n+2c}} \right\} - \frac{6(n+1)^3}{2^{2n}} \\ &\geq 1 - \frac{2q}{2^{n+c}} - \frac{20q}{2^{n+2c}} - \frac{6(n+1)^3}{2^{2n}}. \end{aligned}$$

By Lemma 1, we obtain the following theorem.

Theorem 2. *Let n , t , c and q be positive integers such that $4 \leq c \leq n$. Then one has*

$$\mathbf{Adv}_{\text{MXoP}_c}^{\text{prf}}(q) \leq \frac{2q}{2^{n+c}} + \frac{20q}{2^{n+2c}} + \frac{6(n+1)^3}{2^{2n}}.$$

In particular, when $c = \frac{t}{2}$ and $t \leq 2n$, we have an $(n + \frac{t}{2})$ -to- n bit PRF $\text{MXoP}_{\frac{t}{2}}$ such that

$$\mathbf{Adv}_{\text{MXoP}_{\frac{t}{2}}}^{\text{prf}}(q) \leq \frac{22q}{2^{n+\frac{t}{2}}} + \frac{6(n+1)^3}{2^{2n}}.$$

³We can assume that \mathcal{D} makes no redundant query.

Remark 1. One can alternatively count the number of solutions by dividing Γ into sub-systems Γ_M , $M \in \{0, 1\}^t$, where Γ_M consists of equations $P_i \oplus Q_i = Z_i$ such that $i \in \mathcal{P}^{(M)}$. By multiplying all the number of solutions to Γ_M , $M \in \{0, 1\}^t$, one obtains

$$h(\Gamma, \tilde{\mathcal{P}}, \tilde{\mathcal{Q}}) = \prod_{M \in \{0, 1\}^t} h(\Gamma_M, \tilde{\mathcal{P}}, \tilde{\mathcal{Q}}).$$

By Theorem 1, the number of solutions to Γ_M is estimated as follows.

$$\begin{aligned} h(\Gamma_M, \tilde{\mathcal{P}}, \tilde{\mathcal{Q}}) &\geq \left(1 - \frac{2q_M^2}{2^{2n}} - \frac{20q_M^3}{2^{3n}} - \frac{6(n+1)^3}{2^{2n}}\right) \\ &\quad \times \prod_{i \in \mathcal{P}^{(M)}} \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n}\right) \end{aligned} \quad (37)$$

where $q_M = |\mathcal{P}^{(M)}|$. We note that (37) can also be obtained by recent results of Mirror theory [DNS22, CP20], while they do not apply to the security proof of XoTP to be discussed in the next section as equations are not partitioned according to distinct tweaks that determine independent random permutations.

5.2 XoTP: Xor of Tweakable Permutations with Input Switching

Given a constant $C \in \{0, 1\}^c$ for an integer c such that $0 \leq c \leq n$, a $(t + n - c)$ -to- n bit pseudorandom function XoTP_c is defined as follows.

- When $t \geq n - c$,

$$\text{XoTP}_c(X, Y, W) = \tilde{\text{P}}(W \parallel Y, C \parallel X) \oplus \tilde{\text{Q}}(W \parallel X, C \parallel Y)$$

for $X, Y \in \{0, 1\}^{n-c}$ and $W \in \{0, 1\}^{t-n+c}$.

- When $t < n - c$,

$$\text{XoTP}_c(X, Y, W) = \tilde{\text{P}}(Y, C \parallel W \parallel X) \oplus \tilde{\text{Q}}(X, C \parallel W \parallel Y)$$

for $X, Y \in \{0, 1\}^t$ and $W \in \{0, 1\}^{n-t-c}$.

SECURITY OF XoTP_c WHEN $t \geq n - c$. Suppose that a distinguisher \mathcal{D} makes q queries $(X_i, Y_i, W_i) \in \{0, 1\}^{n-c} \times \{0, 1\}^{n-c} \times \{0, 1\}^{t-n+c}$, obtaining the corresponding responses Z_i for $i = 1, \dots, q$. In this way, \mathcal{D} obtains a transcript

$$\tau = ((X_1, Y_1, W_1, Z_1), \dots, (X_q, Y_q, W_q, Z_q)).$$

In the real world, $P_i \stackrel{\text{def}}{=} \tilde{\text{P}}(W_i \parallel Y_i, C \parallel X_i)$ and $Q_i \stackrel{\text{def}}{=} \tilde{\text{Q}}(W_i \parallel X_i, C \parallel Y_i)$ should be a solution to the following system of equations.

$$\Gamma : \begin{cases} P_1 \oplus Q_1 = Z_1, \\ P_2 \oplus Q_2 = Z_2, \\ \vdots \\ P_q \oplus Q_q = Z_q, \end{cases}$$

subject to the partitions $\mathbb{P} = \{\mathcal{P}^{(M)}\}_{M \in \{0, 1\}^t}$ and $\mathbb{Q} = \{\mathcal{Q}^{(M)}\}_{M \in \{0, 1\}^t}$, where

$$\mathcal{P}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid W_i \parallel Y_i = M\},$$

$$\mathcal{Q}^{(M)} \stackrel{\text{def}}{=} \{i \in [q] \mid W_i \parallel X_i = M\}.$$

Using these partitions, we can define relations $\overset{P}{\sim}$ and $\overset{Q}{\sim}$. Since $i \overset{P}{\sim} j \Rightarrow i \not\overset{Q}{\sim} j$ and $i \overset{Q}{\sim} j \Rightarrow i \overset{P}{\sim} j$, we have $|\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}| = 1$ for any $M, M' \in \{0, 1\}^t$. Since \mathcal{D} is allowed to make at most 2^{n-c} queries for each tweak, we have

$$\begin{aligned} A &= \max_{M \in \{0, 1\}^t} \left\{ |\mathcal{P}^{(M)}|, |\mathcal{Q}^{(M)}| \right\} \leq 2^{n-c}, \\ B &= \max_{M, M' \in \{0, 1\}^t} \left\{ |\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}| \right\} = 1. \end{aligned}$$

By Corollary 1, if $c \geq 4$, then we have

$$\begin{aligned} h(\tau, \overset{P}{\sim}, \overset{Q}{\sim}) &\geq \left(1 - \min \left\{ \frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}} \right\} - \frac{6(n+1)^3}{2^{2n}} \right) \\ &\quad \times \prod_{i=1}^q \left(\frac{(2^n - |\mathcal{P}_i|)(2^n - |\mathcal{Q}_i|)}{2^n} \right). \end{aligned}$$

Similarly to the analysis of MXoP, we have

$$\frac{\Pr[\text{T}_{\text{re}} = \tau]}{\Pr[\text{T}_{\text{id}} = \tau]} \geq 1 - \min \left\{ \frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}} \right\} - \frac{6(n+1)^3}{2^{2n}}.$$

By Lemma 1, we obtain the following theorem.

Theorem 3. Let n, t, c and q be positive integers such that $t \geq n - c$ and $4 \leq c \leq n$. Then one has

$$\text{Adv}_{\text{XoTP}_c}^{\text{prf}}(q) \leq \min \left\{ \frac{20q}{2^{n+2c}}, \frac{20q^2}{2^{3n}} \right\} + \frac{6(n+1)^3}{2^{2n}}.$$

When $c = \frac{t}{3}$ and $\frac{3n}{4} \leq t \leq 3n$, we have an $(n + \frac{2t}{3})$ -to- n bit PRF XoTP $_{\frac{t}{3}}$ such that

$$\text{Adv}_{\text{XoTP}_{\frac{t}{3}}}^{\text{prf}}(q) \leq \frac{20q}{2^{n+\frac{2t}{3}}} + \frac{6(n+1)^3}{2^{2n}}.$$

When $4 \leq c \leq \frac{n}{4}$, we have an $(n + t - c)$ -to- n bit PRF XoTP $_c$ such that

$$\text{Adv}_{\text{XoTP}_c}^{\text{prf}}(q) \leq \frac{20q^2}{2^{3n}} + \frac{6(n+1)^3}{2^{2n}}.$$

SECURITY OF XoTP $_c$ WHEN $t < n - c$. We can prove the security of XoTP $_c$ such that $t < n - c$ similarly to the case that $t \geq n - c$, where the main difference is that

$$\begin{aligned} A &= \max_{M \in \{0, 1\}^t} \left\{ |\mathcal{P}^{(M)}|, |\mathcal{Q}^{(M)}| \right\} \leq 2^{n-c}, \\ B &= \max_{M, M' \in \{0, 1\}^t} \left\{ |\mathcal{P}^{(M)} \cap \mathcal{Q}^{(M')}| \right\} \leq 2^{n-t-c}. \end{aligned}$$

Then, using Lemma 1, we can prove the following theorem.

Theorem 4. Let n, t, c and q be positive integers such that $t < n - c$ and $4 \leq c \leq n$. Then one has

$$\text{Adv}_{\text{XoTP}_c}^{\text{prf}}(q) \leq \frac{2q}{2^{n+t+c}} + \frac{20q}{2^{n+2c}} + \frac{6(n+1)^3}{2^{2n}}.$$

When $c = \frac{t}{3}$ and $12 \leq t < \frac{3n}{4}$, we have an $(n + \frac{2t}{3})$ -to- n bit PRF XoTP $_{\frac{t}{3}}$ such that

$$\text{Adv}_{\text{XoTP}_{\frac{t}{3}}}^{\text{prf}}(q) \leq \frac{22q}{2^{n+\frac{2t}{3}}} + \frac{6(n+1)^3}{2^{2n}}.$$

Acknowledgement. We would like to express our appreciation to the anonymous reviewers for their valuable feedback and insightful suggestions. Wonseok Choi was supported in part by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No.RS-2023-00239620), by AnalytiXIN, by Sunday Group, and by Algorand Foundation via the MEGA-ACE project. Jooyoung Lee was supported by Institute for Information & communications Technology Planning&Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2022-0-01202, Regional strategic industry convergence security core talent training business).

References

- [BI99] Mihir Bellare and Russell Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptology ePrint Archive, Report 1999/024, 1999. Available at <http://eprint.iacr.org/1999/024>.
- [BJK⁺16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016 (Proceedings, Part II)*, volume 9815 of *LNCS*, pages 123–153. Springer, 2016.
- [BKR98] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.
- [BN18] Srimanta Bhattacharya and Mridul Nandi. Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the χ^2 Method. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018 (Proceedings, Part I)*, volume 10820 of *LNCS*, pages 387–412. Springer, 2018.
- [BN21] Srimanta Bhattacharya and Mridul Nandi. Luby-rackoff backwards with more users and more security. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part III*, volume 13092 of *Lecture Notes in Computer Science*, pages 345–375. Springer, 2021.
- [CCL23] Yu Long Chen, Wonseok Choi, and Changmin Lee. Improved Multi-user Security Using the Squared-Ratio Method. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part II*, volume 14082 of *Lecture Notes in Computer Science*, pages 694–724. Springer, 2023.
- [CDN⁺23] Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of Mirror Theory for a Wide Range of ξ_{\max} . In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 470–501, Cham, 2023. Springer Nature Switzerland.

- [CHWZ23] Wonseok Choi, Minki Hhan, Yu Wei, and Vassilis Zikas. Fine-Tuning Ideal Worlds for the Xor of Two Permutation Outputs. Cryptology ePrint Archive, Paper 2023/1704, 2023. <https://eprint.iacr.org/2023/1704>.
- [CKLL22] Wonseok Choi, Hwigeom Kim, Jooyoung Lee, and Yeongmin Lee. Multi-user Security of the Sum of Truncated Random Permutations. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part II*, volume 13792 of *Lecture Notes in Computer Science*, pages 682–710. Springer, 2022.
- [CLL19] Wonseok Choi, Byeonghak Lee, and Jooyoung Lee. Indifferentiability of Truncated Random Permutations. In Steven D. Galbraith and Shihō Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 (Proceedings, Part I)*, volume 11921 of *LNCS*, pages 175–195. Springer, 2019.
- [CLS15] Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking Even-Mansour Ciphers. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 (Proceedings, Part I)*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015.
- [CLS17] Benoît Cogliati, Jooyoung Lee, and Yannick Seurin. New constructions of macs from (tweakable) block ciphers. *IACR Transactions on Symmetric Cryptology*, 2017(2):27–58, Jun. 2017.
- [CP20] Benoît Cogliati and Jacques Patarin. Mirror Theory: A simple proof of the $P_i \oplus P_j$ Theorem with $\xi_{\max} = 2$. IACR Cryptology ePrint Archive, Report 2020/734, 2020. Available at <https://eprint.iacr.org/2020/734>.
- [Cro00] Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.
- [DDNY18] Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part I)*, volume 10991 of *LNCS*, pages 631–661. Springer, 2018.
- [DHT17] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.
- [DNS22] Avijit Dutta, Mridul Nandi, and Abishanka Saha. Proof of Mirror Theory for $\xi_{\max} = 2$. *IEEE Transactions on Information Theory*, pages 1–1, 2022.
- [DNT19] Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 (Proceedings, Part I)*, volume 11476 of *LNCS*, pages 437–466. Springer, 2019.
- [FLS⁺10] Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. *Submission to NIST (round 3)*, 2010.

- [GGM18] Shoni Gilboa, Shay Gueron, and Ben Morris. How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function? *Journal of Cryptology*, 31(1):162–171, 2018.
- [GM20] Aldo Gunging and Bart Mennink. The Summation-Truncation Hybrid: Reusing Discarded Bits for Free. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020 (Proceedings, Part I)*, volume 12170 of *LNCS*, pages 187–217. Springer, 2020.
- [HS20] Viet Tung Hoang and Yaobin Shen. Security of Streaming Encryption in Google’s Tink Library. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS ’20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9–13, 2020*, pages 243–262. ACM, 2020.
- [HWKS98] Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building PRFs from PRPs. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO ’98*, volume 1462 of *LNCS*, pages 370–389. Springer, 1998.
- [IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.
- [Iwa06] Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In *International Workshop on Fast Software Encryption*, pages 310–327. Springer, 2006.
- [JN20] Ashwin Jha and Mridul Nandi. Tight Security of Cascaded LRW2. *Journal of Cryptology*, 33(3):1272–1317, 2020.
- [JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014 (Proceedings, Part II)*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.
- [JNPS16] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. Deoxys v1.41. *Submitted to CAESAR*, 2016.
- [KLL20] Seongkwang Kim, Byeonghak Lee, and Jooyoung Lee. Tight Security Bounds for Double-block Hash-then-Sum MACs. In *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings*, volume 12105 of *Lecture Notes in Computer Science*. Springer, 2020.
- [Lee17] Jooyoung Lee. Indifferentiability of the Sum of Random Permutations Toward Optimal Security. *IEEE Transactions on Information Theory*, 63(6):4050–4054, 2017.
- [LRW02] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.
- [LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.

- [Men16] Bart Mennink. XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In *Advances in Cryptology – CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 64–94. Springer, 2016.
- [MN17] Bart Mennink and Samuel Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 556–583. Springer, 2017.
- [Nai15] Yusuke Naito. Full PRF-secure message authentication code based on tweakable block cipher. In *International Conference on Provable Security*, pages 167–182. Springer, 2015.
- [Nai17] Yusuke Naito. Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security. *IACR Transactions on Symmetric Cryptology*, 2017, Issue 2:1–26, 2017.
- [Nan20] Mridul Nandi. Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 203–220. Springer, 2020.
- [Pat08a] Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In Reihaneh Safavi-Naini, editor, *Information Theoretic Security*, pages 232–248, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
- [Pat08b] Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In Reihaneh Safavi-Naini, editor, *ICITS 2008*, pages 232–248, 2008.
- [Pat10a] Jacques Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. IACR Cryptology ePrint Archive, Report 2010/287, 2010. Available at <http://eprint.iacr.org/2010/287>.
- [Pat10b] Jacques Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. In *IACR Cryptology ePrint Archive 2010/287*, 2010.
- [SGW20] Yaobin Shen, Chun Guo, and Lei Wang. Improved Security Bounds for Generalized Feistel Networks. *IACR Transactions on Symmetric Cryptology*, 2020, Issue 1:425–457, 2020.
- [SO98] Rich Schroeppel and Hilarie Orman. The Hasty Pudding Cipher. *AES candidate submitted to NIST*, 1998.