entropy

MDPI

Article

Constructions of Beyond-Birthday Secure PRFs from Random Permutations, Revisited

Jiehui Nan [1,*], Ping Zhang [2] and Honggang Hu [1]

[1] Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China; hghu2005@ustc.edu.cn

[2] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; zhgp@njupt.edu.cn

* Correspondence: ustcnjh@mail.ustc.edu.cn

Abstract: In CRYPTO 2019, Chen et al. showed how to construct pseudorandom functions (PRFs) from random permutations (RPs), and they gave one beyond-birthday secure construction from sum of Even-Mansour, namely SoEM22 in the single-key setting. In this paper, we improve their work by proving the multi-key security of SoEM22, and further tweaking SoEM22 but still preserving beyond birthday bound (BBB) security. Furthermore, we use only one random permutation to construct parallelizable and succinct beyond-birthday secure PRFs in the multi-key setting, and then tweak this new construction. Moreover, with a slight modification of our constructions of tweakable PRFs, two parallelizable nonce based MACs for variable length messages are obtained.

Keywords: beyond birthday bound; multi-key security; H-Coefficient technique; nonce based MACs

Citation: Nan, J.; Zhang, P.; Hu, H. Constructions of Beyond-Birthday Secure PRFs from Random Permutations, Revisited. *Entropy* **2021**, *23*, 1296. https://doi.org/10.3390/e23101296

Academic Editor: Luis Javier Garcia Villalba

Received: 9 September 2021
Accepted: 28 September 2021
Published: 30 September 2021

1. Introduction

Random numbers are widely used in engineering practice. In particular, randomization is central to cryptography. One can generate random numbers by using physical random sources such as chaos-based [1] and quantum-based [2] random number generator. However, obtaining random numbers from physical phenomena requires high quality of the entropy source, and is also device-dependent so that the corresponding cost is not cheap. Besides, in some cryptographic applications, the way of generating random numbers above is not friendly due to its uncontrollability. Motivated by cryptographic applications, Blum and Micali [3] and Yao [4] formalized the modern notation of pseudorandom generators from the perspectives in computational complexity. Later, Goldreich et al. [5] proposed the concept of pseudorandom functions (PRFs). Informally, $F(K,\cdot)$ is said to be a PRF where K is a uniformly random string with enough entropy, if for any input x, $F(K,x)$ can be computed efficiently and can not be distinguished from a truly random value. PRFs are important in cryptography with fruitful applications in encryption, identification, and authentication.

In theory, PRFs can be obtained from one-way functions [5,6], but this general transformation is not practical. Some other algebraic constructions, such as number theory-based [7,8] or lattice-based PRFs [9–11], are still inefficient. Therefore, it is significant to construct PRFs from symmetric primitives both in theory and practice. There are a series of works to build the PRFs from pseudorandom permutations (PRPs)/block ciphers [12–14]. Recently, Chen et al. [15] proposed a method to construct PRFs from random permutations (RPs). In [15], the construction SoEM22 (which means sum of one-round Even-Mansour based on two independent permutations) was proved beyond-birthday secure in the single-key setting.

About SoEM22, there are three questions we may ask: (i) Is SoEM22 beyond-birthday secure in the multi-key setting? (ii) Can SoEM22 be tweaked while preserving BBB security? (iii) If the underlying random permutations can be computed efficiently in both forward

and inverse directions, can we construct beyond-birthday secure PRFs by using only one permutation in both multi-key and tweakable cases?

Fortunately, we can give positive answers to these questions. First, we prove that SoEM22 is beyond-birthday secure in the multi-key setting. Informally, it means that for any distinguisher who distinguishes m independent n-to-n-bit keyed functions from m independent ideal random functions, its advantage does not depend on m. However, in this case the distinguisher still needs to make at least $\mathcal{O}(2^{2n/3})$ queries to achieve a noticeable advantage.

Second, we tweak the construction SoEM22, inspired by the work [16]. A tweakable PRF, $F : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, means that one can associate a tweak space $\mathcal{T}$ to the key space $\mathcal{K}$. For any key k randomly sampled from $\mathcal{K}$, one can choose different tweaks $t \in \mathcal{T}$ to compute $y = F(k,t,x)$ even on the same input x.

Following the idea in [17], we solve the third question, and construct beyond-birthday secure PRFs in the multi-key setting from one bidirectionally efficient random permutation. Then this new construction from a single permutation can also be tweaked while preserving BBB security.

1.1. Our Contributions

In this paper, we enhance the security of SoEM22 [15] by showing that

$$F^{P_1,P_2}_{K_1,K_2}(x) = P_1(x \oplus K_1) \oplus P_2(x \oplus K_2) \oplus K_1 \oplus K_2 \tag{1}$$

is beyond-birthday secure in the multi-key setting, where $\oplus$ denotes the bitwise XOR operator, P_1 and P_2 are two independent random permutations, x is an n-bit input, and K_1 and K_2 are two n-bit uniformly random strings. Furthermore, we can tweak the construction SoEM22, while preserving BBB security, as

$$\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}(t,x) = P_1(x \oplus H_{K_h^1}(t)) \oplus P_2(x \oplus H_{K_h^2}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t), \tag{2}$$

where $H_{K_h^1}$ and $H_{K_h^2}$ are uniformly and independently sampled from the regular and almost-XOR universal (AXU) keyed hash family, t is a tweak, and x is an n-bit input.

Chen et al. [15] first constructed beyond-birthday secure PRFs from random permutations. Later, Chakraborti et al. [18] suggested and designed minimally structured beyond-birthday secure RPFs (i.e. by using only one random permutation). Following this line of study, we design a parallelizable beyond-birthday secure PRF in the multi-key setting from one bidirectionally efficient random permutation P as

$$F^{P}_{K_1,K_2}(x) = P(x \oplus K_1) \oplus P^{-1}(x \oplus K_2) \oplus K_1 \oplus K_2, \tag{3}$$

where K_1, K_2, and x are the same as those in Equation (1). We tweak this new construction as

$$\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}(t,x) = P(x \oplus H_{K_h^1}(t)) \oplus P^{-1}(x \oplus H_{K_h^2}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t), \tag{4}$$

where $H_{K_h^1}$, $H_{K_h^2}$, x, and t are the same as those in Equation (2).

Moreover, from our two constructions of tweakble PRFs, we can give two nonce based MACs for variable length messages. In particular, when one replaces the input x (resp. the tweak t) in Equations (2) and (4) by an n-bit nonce N (resp. a message M), one can obtain two parallelizable beyond-birthday secure nonce based MACs as

$$T = P_1(N \oplus H_{K_h^1}(M)) \oplus P_2(N \oplus H_{K_h^2}(M)) \oplus H_{K_h^1}(M) \oplus H_{K_h^2}(M) \tag{5}$$

and

$$T = P(N \oplus H_{K_h^1}(M)) \oplus P^{-1}(N \oplus H_{K_h^2}(M)) \oplus H_{K_h^1}(M) \oplus H_{K_h^2}(M). \tag{6}$$

1.2. Related Works

Based on two random permutations P_1 and P_2, Cogliati et al. [16] constructed a beyond-birthday secure tweakable Even-Mansour (TEM) as

$$\mathsf{TEM}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}(t,x) = P_2(P_1(x \oplus H_{K_h^1}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t)) \oplus H_{K_h^2}(t), \tag{7}$$

where $H_{K_h^1}$ and $H_{K_h^2}$ are uniformly and independently sampled from the uniform and AXU keyed hash family, t is a tweak, and x is an n-bit input. Later, Dutta [17] gave a beyond-birthday secure TEM from one permutation as

$$\mathsf{TEM}^{P}_{H_{K_h^1},H_{K_h^2}}(t,x) = P(P(x \oplus H_{K_h^1}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t)) \oplus H_{K_h^2}(t), \tag{8}$$

where P is a random permutation, and $H_{K_h^1}$, $H_{K_h^1}$, t, and x are the same as those in (7). Compared with Equations (7) and (8), our constructions in Equations (2) and (4) are parallelizable.

Chakraborti et al. [18] constructed beyond-birthday secure PRFs from random permutations with minimal structure (i.e. from one random permutation P) as

$$P^{-1}(P(K \oplus x) \oplus 3K \oplus x) \oplus 2K,$$

where K is an n-bit key, x is an n-bit input, and 2 is a primitive element in the finite field $\mathbb{F}_{2^n}$ so that $2K$ denotes the multiplication of 2 and K over $\mathbb{F}_{2^n}$. Recently, Dutta et al. [19] proved that the construction

$$P(P(K_1 \oplus x) \oplus K_2 \oplus K_1 \oplus x) \oplus K_1$$

is also a beyond-birthday secure PRF, where K_1 and K_2 are two n-bit uniformly random strings. However, all these two constructions were proved beyond-birthday secure only in the single-key setting. Compared with them, Equation (3) is parallelizable and can be proved beyond-birthday secure in the multi-key setting.

Besides, Chakraborti et al. [18] also gave a nonce based MAC for variable length messages as

$$T = P^{-1}(P(K \oplus N) \oplus 3K \oplus N \oplus H_{K_h}(M)) \oplus 2K,$$

where K is an n-bit key, N is an n-bit nonce, M is a variable length message, and H_{K_h} is uniformly sampled from the keyed hash family with three properties: regular, AXU, and 3-way regular.

1.3. Technical Overview

The basic technique to prove the BBB security of our constructions is the H-Coefficient technique [20,21]. As an example, we intuitively introduce the core idea of the security proof for the construction $\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}$ in Equation (4). Let Φ be a random function from $\mathcal{T} \times \{0,1\}^n$ to $\{0,1\}^n$, where $\mathcal{T}$ is the tweakable space. Denote $\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}} : \mathcal{T} \times \{0,1\}^n \mapsto \{0,1\}^n$ as in Equation (4). Given a deterministic distinguisher D who has access query to the primitive oracle P and to the construction oracle $\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}$ or Φ, the goal of D is to distinguish which construction oracle it interacts with. Set $\bar{\mathcal{Q}}_P = \{(u_1,v_1),\ldots,(u_p,v_p)\}$ as all p query-response tuples for the primitive oracle, and $\bar{\mathcal{Q}}_F = \{(t_1,x_1,y_1),\ldots,(t_q,x_q,y_q)\}$ as all q query-response tuples for the construction oracle. Then, $\bar{\mathcal{Q}}_F$ and $\bar{\mathcal{Q}}_P$ along with $H_{K_h^1}$ and $H_{K_h^2}$ are called a transcript, denoted by $\bar{\tau} = \{\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (H_{K_h^1}, H_{K_h^2})\}$. When D interacts with Φ, the transcript $\bar{\tau}$ is said in the ideal world; otherwise, $\bar{\tau}$ is said in the real world.

In general, all possible transcripts are divided into bad transcripts and good transcripts. The key to use the H-Coefficient technique is to define bad transcripts in the ideal world with a low proportion. Furthermore, one also needs to show that the probability of any good transcript in the ideal world is close to its probability in the real world. After observing the transcript, the distinguisher will use this information to test whether it is compatible with $\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}$. Based on this fact, one can briefly interpret how to define bad transcripts by

the following example. Assume that there exist $(t,x,y) \in \bar{\mathcal{Q}}_F$ and $(u_1,v_1),(u_2,v_2) \in \bar{\mathcal{Q}}_P$ such that $H_{K_h^1}(t) \oplus x = u_1$ and $H_{K_h^2}(t) \oplus x = v_2$ (this event is denoted by Bad_1). Then in the real world, one must have $y = v_1 \oplus u_2 \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t)$. However, in the ideal world, the probability that this equation holds is at most $1/2^n$. In this case, the distinguisher has a significant advantage. If $H_{K_h^1}$ and $H_{K_h^2}$ are independently chosen from the uniform keyed hash family, then one has

$$\Pr[(H_{K_h^1}(t) = x \oplus u_1) \wedge (H_{K_h^2}(t) = x \oplus v_2)] \leq \frac{1}{2^{2n}}.$$

By union bound, the probability of Bad_1 in the ideal world can be upper bounded by $qp^2/2^{2n}$. This advantage is secure roughly up to $p = q = \mathcal{O}(2^{2n/3})$ adversarial queries. We illustrate some other bad cases for transcript $\bar{\tau}$ in Figure 1, where (1) in Figure 1 is for the above example.

For any good transcript, to prove that its probability in the real world is almost close to the one in the ideal world, it needs to show that the number of choices for unfixed maps of P is large enough. Let $U = \{u_1 \in \{0,1\}^n : (u_1,v_1) \in \bar{\mathcal{Q}}_P\}$, $V = \{v_1 \in \{0,1\}^n : (u_1,v_1) \in \bar{\mathcal{Q}}_P\}$, $U_F = \{H_{K_h^1}(t) \oplus x : (t,x,y) \in \bar{\mathcal{Q}}_F\}$, and $V_F = \{H_{K_h^2}(t) \oplus x : (t,x,y) \in \bar{\mathcal{Q}}_F\}$. Then the good transcript ensures that $U \cap U_F = \emptyset$ (resp. $V \cap V_F = \emptyset$) and all items in U_F (resp. V_F) are distinct. The next goal is to choose distinct values for $\{P(H_{K_h^1}(t) \oplus x) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$ (resp. $\{P^{-1}(H_{K_h^2}(t) \oplus x) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$) such that $\{P(H_{K_h^1}(t) \oplus x) : (t,x,y) \in \bar{\mathcal{Q}}_F\} \cap (V \cup V_F) = \emptyset$, $\{P(H_{K_h^1}(t) \oplus x) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F\} \cap (U \cup U_F) = \emptyset$, and all items in $\{P(H_{K_h^1}(t) \oplus x) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F\}$ are distinct (resp. $\{P^{-1}(H_{K_h^2}(t) \oplus x) : (t,x,y) \in \bar{\mathcal{Q}}_F\} \cap (U \cup U_F) = \emptyset$, $\{P^{-1}(H_{K_h^2}(t) \oplus x) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F\} \cap (V \cup V_F) = \emptyset$, and all items in $\{P^{-1}(H_{K_h^2}(t) \oplus x) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F\}$ are distinct). However, this strategy is not enough to achieve the BBB security. To deal with this problem, we adopt the main idea in [17,22] to count more possible choices for unfixed maps of P, and this idea allows that $\{P(H_{K_h^1}(t) \oplus x) : (t,x,y) \in \bar{\mathcal{Q}}_F\} \cap V_F \neq \emptyset$. Informally, it means that there exist some pairs $((t,x,y),(t',x',y')) \in \bar{\mathcal{Q}}_F \times \bar{\mathcal{Q}}_F$ such that $P(x \oplus H_{K_h^1}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y = x' \oplus H_{K_h^1}(t')$ or $P^{-1}(x \oplus H_{K_h^2}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y = x' \oplus H_{K_h^2}(t')$. Take the first case for example, one has

$$\begin{cases} x \oplus H_{K_h^1}(t) \xmapsto{P} x' \oplus H_{K_h^1}(t') \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y, \\ x' \oplus H_{K_h^1}(t') \xmapsto{P} x \oplus H_{K_h^2}(t), \\ x \oplus H_{K_h^2}(t) \oplus H_{K_h^1}(t') \oplus H_{K_h^2}(t') \oplus y' \xmapsto{P} x' \oplus H_{K_h^2}(t'). \end{cases} \tag{9}$$

To ensure that the maps in (9) are valid, $x' \oplus H_{K_h^1}(t') \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t) \oplus y$ can not be equal to previous fixed inputs of P, and $x \oplus H_{K_h^2}(t) \oplus H_{K_h^1}(t') \oplus H_{K_h^2}(t') \oplus y'$ can not be equal to previous fixed outputs of P. Since Φ is a random function from $\mathcal{T} \times \{0,1\}^n$ to $\{0,1\}^n$, then $y = \Phi(t,x)$ is uniformly and independently distributed for each distinct query (t,x) in the ideal world. Due to this property, one can define the good transcripts to ensure that the number of rational maps in (9) is large enough. At the same time, it guarantees that the proportion of the corresponding bad transcripts in the ideal world can also achieve a beyond birthday bound. For more details, please refer to Section 4.

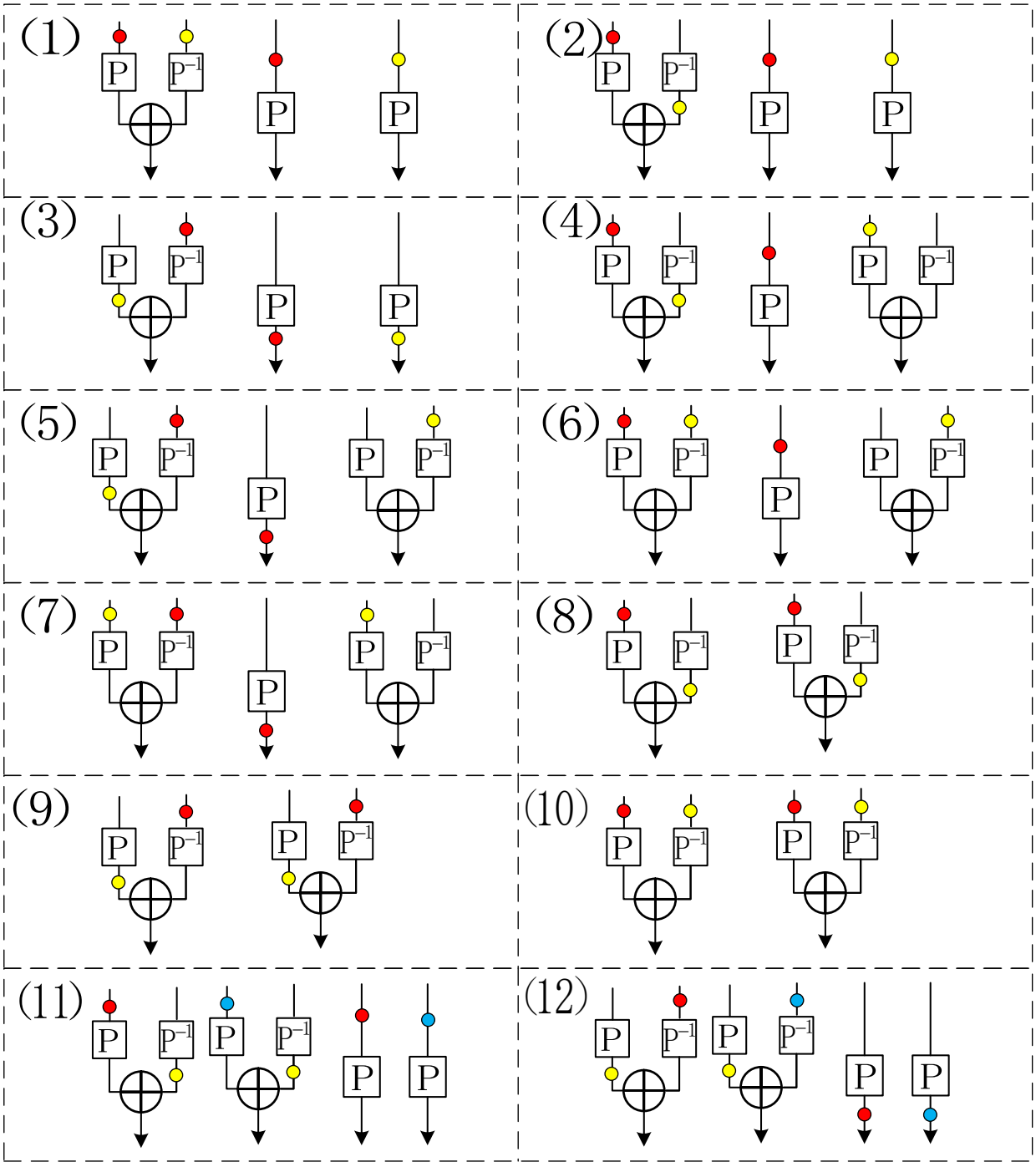

Figure 1. Graphical representation of the motivation to define bad cases for the transcript in the ideal world, which corresponds to the bad conditions from (C-1) to (C-12) in Section 4. In this graph, the same color in different lines means that there exists a collision between these places.

1.4. Organization

The rest of this paper is organized as follows. In Section 2, we introduce some necessary notations and basic tools. In Section 3, we prove the multi-key security of SoEM22, further tweak the construction SoEM22, and finally construct parallelizable nonce based MACs from two permutations. The constructions of beyond-birthday secure PRFs from one permutation in both multi-key and tweakable settings are given in Section 4, and we also design parallelizable nonce based MACs from one permutation in this section. Finally, Section 5 concludes this paper.

2. Preliminaries

2.1. Notations

For any $n \in \mathbb{Z}$, we simplify the set $\{1, \ldots, n\}$ as $[n]$, and denote the set of all n-bit strings by $\{0,1\}^n$. For any finite set $\mathcal{S}$, $s \xleftarrow{\$} \mathcal{S}$ means that s is sampled uniformly from $\mathcal{S}$. Besides, $|S|$ denotes the size of S. For any sets $\mathcal{X}$ and $\mathcal{Y}$, $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ includes all functions from $\mathcal{X}$ to $\mathcal{Y}$, and we simply write $\mathsf{Func}(n)$ for $\mathsf{Func}(\{0,1\}^n, \{0,1\}^n)$. Furthermore, $\mathsf{Perm}(n)$ denotes the set of all permutations on $\{0,1\}^n$. For any two integers q and N such that $1 \le q \le N$, define $(N)_q = N(N-1)\ldots(N-q+1)$. In particular, $(N)_0 = 1$.

$\mathcal{Q} = \{(x_1, y_1), \ldots, (x_p, y_p)\}$ is said a well-defined n-bit permutation-compatible set if $x_1, \ldots, x_p \in \{0,1\}^n$ (resp. $y_1, \ldots, y_p \in \{0,1\}^n$) are all distinct. Given a well-defined permutation-compatible set $\mathcal{Q}$, we say that the permutation $P \in \mathsf{Perm}(n)$ extends $\mathcal{Q}$, denoted by $P \vdash \mathcal{Q}$, if $P(x_i) = y_i$ for all $i \in [p]$. For another well-defined n-bit permutation-compatible set $\mathcal{Q}' = \{(x'_1, y'_1), \ldots, (x'_{p'}, y'_{p'})\}$, $\mathcal{Q}'$ and $\mathcal{Q}$ are called disjoint if $x_i \neq x'_j$ and $y_i \neq y'_j$ for any $i \in [p]$ and $j \in [p']$. Given the disjoint n-bit permutation-compatible set $\mathcal{Q}$ and $\mathcal{Q}'$, for any random permutation $P \xleftarrow{\$} \mathsf{Perm}(n)$ satisfying $P \vdash \mathcal{Q}$, the probability of $P \vdash \mathcal{Q}'$ is $1/(2^n - p)_{p'}$, which is denoted by

$$\Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : P \vdash \mathcal{Q}' | P \vdash \mathcal{Q}] = \frac{1}{(2^n - p)_{p'}}.$$

For any function $F : \mathcal{D} \to \mathcal{V}$, given the set $\mathcal{S} = \{(x_1, y_1), \ldots, (x_q, y_q) : (x_i, y_i) \in \mathcal{D} \times \mathcal{V}\}$, $F \vdash \mathcal{S}$ means that $F(x_i) = y_i$ for any $(x_i, y_i) \in \mathcal{S}$.

Given two sets U and U', we say that U is disjoint with U' if $U \cap U' = \emptyset$. Let $\mathcal{U} = \{U_1, \ldots, U_m\}$ be a collection of finite sets. Then $\mathcal{U}$ is called a disjoint collection if for any $i \neq j \in [m]$, U_i is disjoint with U_j. In this case, the size of $\mathcal{U}$ is defined as $|\mathcal{U}| = |U_1| + \ldots + |U_m|$. Two disjoint collections $\mathcal{U} = \{U_1, \ldots, U_m\}$ and $\mathcal{U}' = \{U'_1, \ldots, U'_n\}$ are called inner disjoint if $U_i \cap U'_{i'} = \emptyset$ for any $i \in [m], i' \in [n]$. Let S_{mul} be a multi-set, and let $\delta_{S_{\mathsf{mul}}}(x)$ denote the multiplicity of x in S_{mul}. When S_{mul} is called a set, it means that all the repeated items in it are viewed as a unique item. Throughout this paper, when we discuss the size of S_{mul}, which is denoted by $|S_{\mathsf{mul}}|$, the items in S_{mul} are counted without considering the multiplicity.

Definition 1 (Universal Hash Functions)**.** *Let n be a positive integer. Assume that $\mathcal{K}_H$ and $\mathcal{X}$ are two finite sets. Let $\mathcal{H} = (H_{K_h})_{K_h \in \mathcal{K}_H}$ be a keyed hash family from $\mathcal{X}$ to $\{0,1\}^n$, where $\mathcal{K}_H$ is the hash key space. $\mathcal{H}$ is called ϵ_1-regular if for any $t \in \mathcal{X}$ and any $y \in \{0,1\}^n$, it holds that*

$$\Pr[K_h \xleftarrow{\$} \mathcal{K}_H : H_{K_h}(t) = y] \le \epsilon_1.$$

$\mathcal{H}$ is called ϵ_2-almost XOR-universal (ϵ_2-AXU) if for any distinct $t, t' \in \mathcal{X}$ and any $y \in \{0,1\}^n$, it holds that

$$\Pr[K_h \xleftarrow{\$} \mathcal{K}_H : H_{K_h}(t) \oplus H_{K_h}(t') = y] \le \epsilon_2.$$

$\mathcal{H}$ is said XOR-universal (resp. uniform) if it is 2^{-n}-AXU (resp. 2^{-n}-regular).

Next, we briefly describe an example of $\frac{l}{2^n}$-regular and $\frac{l}{2^n}$-AXU keyed hash family [18,23] for some constant $l \in \mathbb{N}$. Let M be any binary string with $|M| < l \cdot n$, and set $\mathcal{K}_H = \{0,1\}^n$. Then we pad M as $M||10^s = M_1||\ldots||M_l$, where $s = l \cdot n - |M| - 1$, 0^s denotes the all zero s bits, and $M_i \in \{0,1\}^n$ for each $i \in [l]$. For any $K_h \in \mathcal{K}_H$, the keyed hash is defined as:

$$\mathsf{Poly}_{H_{K_h}}(M) = M_l \cdot K_h \oplus M_{l-1} \cdot K_h^2 \oplus \ldots \oplus M_1 \cdot K_h^l, \tag{10}$$

where K_h and M_i ($i \in [l]$) are viewed as the elements in $\mathbb{F}_{2^n}$, and $\cdot$ denotes the multiplication in $\mathbb{F}_{2^n}$.

Remark 1. *The keyed hash family $\mathcal{H}$ is said to be ϵ-3-way regular, if for any $y \in \{0,1\}^n$ and any three distinct inputs t, t', and $t'' \in \mathcal{X}$, it holds that*

$$\Pr[K_h \xleftarrow{\$} \mathcal{K}_H : H_{K_h}(t) \oplus H_{K_h}(t') \oplus H_{K_h}(t'') = y] \leq \epsilon.$$

2.2. The H-Coefficient Technique

One important tool used in our proofs is the H-Coefficient technique [21], which can be used to upper bound the statistical distance between the query-answers from two interactive systems. For convenience, we focus on the modernization version of Chen and Steinberger [20].

Let $P_1, \ldots, P_r \xleftarrow{\$} \mathsf{Perm}(n)$ be r independent random permutations, and $\mathcal{K}$ be the key space. In this paper, we only consider the case $r \in \{1,2\}$ and $\mathcal{K} = \{0,1\}^{2n}$. The randomly sampled $2n$-bit key can be parsed as $(K_1, K_2) \xleftarrow{\$} \{0,1\}^{2n}$, where K_1 and K_2 are two independent n-bit uniformly random strings. Then based on r public permutations $P_1, \ldots, P_r$, $F^{P_1,\ldots,P_r}_{K_1,K_2} : \{0,1\}^n \to \{0,1\}^n$ denotes the keyed function indexed by $(K_1, K_2) \in \{0,1\}^{2n}$. Besides, let $\varphi \xleftarrow{\$} \mathsf{Func}(n)$ be an ideal random function. Then for any deterministic distinguisher $\mathcal{D}$ who has query access to the oracle $\mathcal{O}_{\mathsf{re}} = (F^{P_1,\ldots,P_r}_{K_1,K_2}; P_1^{\pm}, \ldots, P_r^{\pm})$ in the real world, or the oracle $\mathcal{O}_{\mathsf{id}} = (\varphi; P_1^{\pm}, \ldots, P_r^{\pm})$ in the ideal world, the advantage of $\mathcal{D}$ to distinguish which oracle it has access to is defined by

$$\mathbf{Adv}_F(\mathcal{D}) = |\Pr[\mathcal{D}^{\mathcal{O}_{\mathsf{re}}} = 1] - \Pr[\mathcal{D}^{\mathcal{O}_{\mathsf{id}}} = 1]|. \tag{11}$$

As shown in Figure 2, in the multi-key setting, the goal of distinguisher $\mathcal{D}$ is to distinguish m keyed functions $(F^{P_1,\ldots,P_r}_{K_1^1,K_2^1}, \ldots, F^{P_1,\ldots,P_r}_{K_1^m,K_2^m})$ from m independent ideal random functions $\varphi_1, \ldots, \varphi_m \xleftarrow{\$} \mathsf{Func}(n)$, where $(K_1^1, K_2^1), \ldots, (K_1^m, K_2^m) \xleftarrow{\$} \{0,1\}^{2n}$ are m independent keys. In this case, let $\mathcal{O}_{\mathsf{id}} = (\varphi_1, \ldots, \varphi_m, P_1^{\pm}, \ldots, P_r^{\pm})$ be the oracle in the ideal world, and $\mathcal{O}_{\mathsf{re}} = (F^{P_1,\ldots,P_r}_{K_1^1,K_2^1}, \ldots, F^{P_1,\ldots,P_r}_{K_1^m,K_2^m}, P_1^{\pm}, \ldots, P_r^{\pm})$ be the oracle in the real world. The advantage of the distinguisher $\mathcal{D}$ to distinguish these two oracles can be defined as the same in (11), but here we use $\mathbf{Adv}^{mk}_{F^{P_1,\ldots,P_r}_{K_1,K_2}}(\mathcal{D})$ to identify the multi-key case.

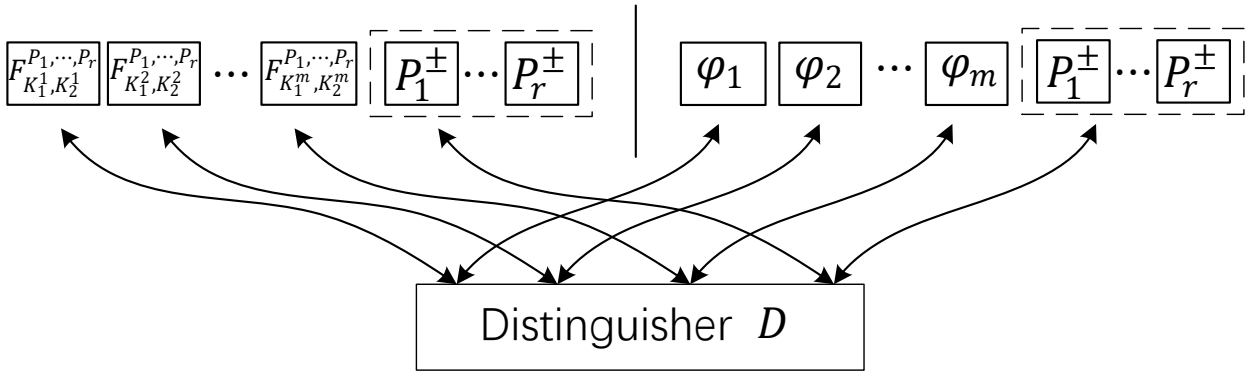

Figure 2. The illustration of the RP-based keyed function $F^{P_1,\ldots,P_r}_{K_1,K_2}$ in the multi-key setting, where the distinguisher D interacts with the real oracle at left, and with the ideal oracle at right.

Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{T}$ to $\{0,1\}^n$. Then we use two independent keyed hash functions $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$ to tweak the keyed function $F^{P_1,\ldots,P_r}_{K_1,K_2}$ as $\mathsf{TPRF}^{P_1,\ldots,P_r}_{H_{K_h^1},H_{K_h^2}} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ such that $\mathsf{TPRF}^{P_1,\ldots,P_r}_{H_{K_h^1},H_{K_h^2}}(t,x) = F^{P_1,\ldots,P_r}_{(H_{K_h^1}(t),H_{K_h^2}(t))}(x)$. In addition, the ideal tweakable random function can be denoted as $\Phi : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, i.e. $\Phi \xleftarrow{\$} \mathsf{Func}(\mathcal{T} \times \{0,1\}^n, \{0,1\}^n)$. In this case, let $\mathcal{O}_{\mathsf{re}} = (\mathsf{TPRF}^{P_1,\ldots,P_r}_{H_{K_1},H_{K_2}}, P_1^{\pm}, \ldots, P_r^{\pm})$ be the oracle in the real world, and $\mathcal{O}_{\mathsf{id}} = (\Phi, P_1^{\pm}, \ldots, P_r^{\pm})$ be

the oracle in the ideal world. For any distinguisher $\mathcal{D}$, its advantage can be defined as the same in (11), but here we use $\mathbf{Adv}^{tweak}_{\mathsf{TPRF}^{P_1,\ldots,P_r}_{H^1_{K^1_h},H^2_{K^2_h}}}(\mathcal{D})$ to identify the tweakable case.

The security proofs in both multi-key and tweakable settings are similar. Therefore, we prove these two cases in a unified approach. For two independently and randomly sampled functions f_1 and f_2 from $\mathsf{Func}(\mathcal{T},\{0,1\}^n)$, (f_1,f_2) is said a good (ϵ_1,ϵ_2)-key-derivation pair if it satisfies two properties in the following:

(i) ϵ_1-**Regular**. For any $t \in \mathcal{T}$ and any $y \in \{0,1\}^n$, it holds that
$$\Pr[f_i(t) = y] \leq \epsilon_1, \text{ for } i \in \{1,2\}.$$

(ii) ϵ_2-**AXU**. For any distinct $t, t' \in \mathcal{T}$ and any $y \in \{0,1\}^n$, it holds that
$$\Pr[f_i(t) \oplus f_i(t') = y] \leq \epsilon_2, \text{ for } i \in \{1,2\}.$$

The above two properties are enough for the security proofs in both tweakable and multi-key settings. In the tweakable setting, $(H_{K^1_h}, H_{K^2_h})$ is a good (ϵ_1,ϵ_2)-key-derivation pair, where $(H_{K^1_h}, H_{K^2_h}) \xleftarrow{\$} \mathcal{H}^2$. In the multi-key setting, set $\mathcal{T} = [m]$, and uniformly and randomly sample two independent random functions $f_1, f_2 \xleftarrow{\$} \mathsf{Func}(\mathcal{T},\{0,1\}^n)$. Then (f_1,f_2) is a good $(2^{-n},2^{-n})$-key-derivation pair. To show the security of the constructions in both tweakable and multi-key settings, we only need to prove the BBB security of the following "unified" function

$$F^{P_1,\ldots,P_r}_{f_1,f_2} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n,$$

where (f_1,f_2) is a good (ϵ_1,ϵ_2)-key-derivation pair and $P_1,\ldots,P_r$ ($r \in \{1,2\}$) are r independent random permutations. In this case, let $\mathcal{O}_{\mathsf{re}} = (F^{P_1,\ldots,P_r}_{f_1,f_2}, P_1^{\pm},\ldots,P_r^{\pm})$ be the oracle in the real world, and $\mathcal{O}_{\mathsf{id}} = (\Phi, P_1^{\pm},\ldots,P_r^{\pm})$ be the oracle in the ideal world, where $\Phi \xleftarrow{\$} \mathsf{Func}(\mathcal{T}\times\{0,1\}^n,\{0,1\}^n)$. When the distinguisher $\mathcal{D}$ interactes with $\mathcal{O}_{\mathsf{re}}$ or $\mathcal{O}_{\mathsf{id}}$, any query-responses along with the good (ϵ_1,ϵ_2)-key-derivation pair $(f_1,f_2) \in \mathsf{Func}(\mathcal{T},\{0,1\}^n)^2$ are called a transcript, denoted by $\tau = (Q_F, Q_{P_1},\ldots,Q_{P_r},(f_1,f_2))$. In addition, Q_F (resp. Q_{P_i}, for $1 \leq i \leq r$) records query-responses when the distinguisher D interacts with the construction oracle (resp. the primitive oracle P_i for $1 \leq i \leq r$). Furthermore, T_{re} (resp. T_{id}) denotes the probability distribution of the interacting transcripts between $\mathcal{D}$ and $\mathcal{O}_{\mathsf{re}}$ (resp. $\mathcal{O}_{\mathsf{id}}$). A transcript τ is said attainable if $\Pr[T_{\mathsf{id}} = \tau] > 0$. Finally, the advantage of the distinguisher $\mathcal{D}$, to distinguish which oracle it has access to, can be defined as the same in (11), but here we use $\mathbf{Adv}^{unify}_{F^{P_1,\ldots,P_r}_{f_1,f_2}}(\mathcal{D})$ to identify this unified description.

Let $\Gamma = \Gamma_{\mathsf{good}} \cup \Gamma_{\mathsf{bad}}$ be a partition for the set Γ consisting of all attainable transcripts, where Γ_{good} (resp. Γ_{bad}) contains all "good" (resp. "bad") transcripts. Then the main result of the H-Coefficient technique can be described as the following lemma.

Lemma 1 (H-Coefficient Technique [20,21])**.** *Let D be a deterministic distinguisher, and T_{re} (resp. T_{id}) be the probability distribution of transcripts in the real world (resp. in the ideal world). Let Γ_{good} and Γ_{bad} be defined above. Assume that there exists $0 \leq \epsilon_{\mathsf{ratio}} \leq 1$ such that for any $\tau \in \Gamma_{\mathsf{good}}$, it holds that*
$$\frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} \geq 1 - \epsilon_{\mathsf{ratio}}.$$

Then, $\mathbf{Adv}^{unify}_{F^{P_1,\ldots,P_r}_{f_1,f_2}}(\mathcal{D}) \leq \epsilon_{\mathsf{ratio}} + \Pr[T_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}]$.

2.3. Useful Tools

Assume that there are g "rational" items in an N-size set S. When one samples s items from S without replacement, H denotes the random variable which counts the number

of "rational" items among these s items. Then we say that H follows the hypergeometric distribution with parameters N, s, and g, denoted by $\mathsf{H} \sim \mathsf{Hyp}_{N,\mathsf{s},\mathsf{g}}$. For $0 \le \alpha \le \mathsf{g}$, one has

$$\Pr[\mathsf{H} = \alpha] = \frac{\binom{\mathsf{g}}{\alpha} \cdot \binom{N-\mathsf{g}}{\mathsf{s}-\alpha}}{\binom{N}{\mathsf{s}}}.$$

In addition, the expectation value of H is sg/N, i.e., $\mathbb{E}(\mathsf{H}) = \mathsf{sg}/N$.

The following lemma is useful in our proofs.

Lemma 2. *Let A, B, C, and N be positive integers satisfying $A + B \le N/2$ and $A + C \le N/2$. Then we have*

$$\prod_{j=0}^{A-1} \frac{N(N-B-C-2j)}{(N-B-j)(N-C-j)} \ge 1 - \frac{4A(A+B)(A+C)}{N^2}.$$

Proof.

$$\begin{aligned}
\prod_{j=0}^{A-1} \frac{N(N-B-C-2j)}{(N-B-j)(N-C-j)} &= \prod_{j=0}^{A-1} \frac{(N-B-j)(N-C-j) - (B+j)(C+j)}{(N-B-j)(N-C-j)} \\
&= \prod_{j=0}^{A-1} \left(1 - \frac{(B+j)(C+j)}{(N-B-j)(N-C-j)}\right) \\
&\ge \prod_{j=0}^{A-1} \left(1 - \frac{(B+A)(C+A)}{(N-B-A)(N-C-A)}\right) \\
&\overset{(*)}{\ge} \prod_{j=0}^{A-1} \left(1 - \frac{4(B+A)(C+A)}{N^2}\right) \\
&\ge \left(1 - \frac{4A(B+A)(C+A)}{N^2}\right),
\end{aligned}$$

where $(*)$ holds since $A + B \le N/2$ and $A + C \le N/2$. □

3. Multi-Key and Tweakable Secure PRFs from Two Random Permutations

In this section, we prove that the construction SoEM22 from two random permutations $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$ in [15], namely

$$F^{P_1,P_2}_{K_1,K_2}(x) = P_1(x \oplus K_1) \oplus P_2(x \oplus K_2) \oplus K_1 \oplus K_2, \tag{12}$$

is beyond-birthday secure in the multi-key setting, where $(K_1, K_2) \xleftarrow{\$} \{0,1\}^{2n}$ and $x \in \{0,1\}^n$.

Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{T}$ to $\{0,1\}^n$. Then we can tweak SoEM22 as

$$\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}(t,x) = P_1(x \oplus H_{K_h^1}(t)) \oplus P_2(x \oplus H_{K_h^2}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t), \tag{13}$$

where $t \in \mathcal{T}$, $x \in \{0,1\}^n$, and $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$.

To show the security of SoEM22 in both multi-key and tweakable settings above, we only need to prove the BBB security of the following "unified" function

$$F^{P_1,P_2}_{f_1,f_2}(t,x) = P_1(x \oplus f_1(t)) \oplus P_2(x \oplus f_2(t)) \oplus f_1(t) \oplus f_2(t), \tag{14}$$

where $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$, $(f_1, f_2) \in \mathsf{Func}(\mathcal{T}, \{0,1\}^n)^2$ is a good (ϵ_1, ϵ_2)-key-derivation pair, $t \in \mathcal{T}$, and $x \in \{0,1\}^n$.

Theorem 1. *Let $n \in \mathbb{N}$, and $(f_1, f_2) \in \mathsf{Func}(\mathcal{T}, \{0,1\}^n)^2$ be a good (ϵ_1, ϵ_2)-key-derivation pair. Consider the function $F^{P_1,P_2}_{f_1,f_2} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ defined in (14) based on two random*

permutations $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$. *For any deterministic distinguisher* $\mathcal{D}$ *making at most* p_1 *queries to* P_1, p_2 *queries to* P_2, *and* q *queries to construction oracle* $F^{P_1,P_2}_{f_1,f_2}$ *or* Φ *such that* $p_1 + p_2 + 3q \leq 2^{n-1}$, *we have*

$$\begin{aligned}\mathbf{Adv}^{unify}_{F^{P_1,P_2}_{f_1,f_2}}(\mathcal{D}) \leq & 3qp_1p_2\epsilon_1^2 + \frac{\epsilon_1(\epsilon_2 q^2 + 2\sqrt{q})(p_1+p_2)}{2} + 2\epsilon_2^2 q^3 + \epsilon_2 q^{3/2} \\ & + \frac{4q(p_1+p_2+2q)^2}{2^{2n}} + \frac{2\sqrt{q}(p_1+p_2)}{2^n} + \frac{11q}{2^n}.\end{aligned} \tag{15}$$

In the multi-key setting, one sets $\mathcal{T} = [m]$ corresponding to m independent random keys, and randomly samples two independent random functions $f_1, f_2 \xleftarrow{\$} \mathsf{Func}([m], \{0,1\}^n)$. Then we can easily conclude that (f_1, f_2) is a good $(2^{-n}, 2^{-n})$-key-derivation pair. By this fact, one can obtain the following corollary.

Corollary 1. *Let* $n, m \in \mathbb{N}$. *Consider the keyed function* $F^{P_1,P_2}_{K_1,K_2} : \{0,1\}^n \to \{0,1\}^n$ *defined in* (12) *based on two random permutations* $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$. *For any deterministic distinguisher* $\mathcal{D}$ *making at most* p_1 *queries to* P_1, p_2 *queries to* P_2, *and totally* q *queries to* $F^{P_1,P_2}_{K_1^1,K_2^1}, \ldots, F^{P_1,P_2}_{K_1^m,K_2^m}$ *(resp. m independent ideal random functions* $\varphi_1, \ldots, \varphi_m$ *) such that* $p_1 + p_2 + 3q \leq 2^{n-1}$, *we have*

$$\begin{aligned}\mathbf{Adv}^{mk}_{F^{P_1,P_2}_{K_1,K_2}}(\mathcal{D}) \leq & \frac{3p_1p_2q}{2^{2n}} + \frac{q^2(p_1+p_2)}{2^{2n+1}} + \frac{2q^3}{2^{2n}} + \frac{q^{3/2}}{2^n} \\ & + \frac{4q(p_1+p_2+2q)^2}{2^{2n}} + \frac{3\sqrt{q}(p_1+p_2)}{2^n} + \frac{11q}{2^n}.\end{aligned} \tag{16}$$

Corollary 1 shows that the construction SoEM22 in (12) is secure roughly up to $p_1 = p_2 = q = \mathcal{O}(2^{2n/3})$ adversarial queries in the multi-key setting.

Similarly, given an ϵ_1-regular and ϵ_2-AXU keyed hash family $\mathcal{H}$ from $\mathcal{T}$ to $\{0,1\}^n$, one can obtain a good (ϵ_1, ϵ_2)-key-derivation pair $(H_{K_h^1}, H_{K_h^2})$ for $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$, and finally conclude the following corollary.

Corollary 2. *Let* $n \in \mathbb{N}$, *and* $\mathcal{H}$ *be an* ϵ_1*-regular and* ϵ_2*-AXU keyed hash family from* $\mathcal{T}$ *to* $\{0,1\}^n$. *Consider the tweakable function* $\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ *defined in* (13) *from two random permutations* $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$. *For any deterministic distinguisher* $\mathcal{D}$ *making at most* p_1 *queries to* P_1, p_2 *queries to* P_2, *and* q *queries to* $\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}$ *or* Φ *such that* $p_1 + p_2 + 3q \leq 2^{n-1}$, *we have*

$$\begin{aligned}\mathbf{Adv}^{tweak}_{\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}}(\mathcal{D}) \leq & 3qp_1p_2\epsilon_1^2 + \frac{\epsilon_1(\epsilon_2 q^2 + 2\sqrt{q})(p_1+p_2)}{2} + 2\epsilon_2^2 q^3 + \epsilon_2 q^{3/2} \\ & + \frac{4q(p_1+p_2+2q)^2}{2^{2n}} + \frac{2\sqrt{q}(p_1+p_2)}{2^n} + \frac{11q}{2^n}.\end{aligned} \tag{17}$$

Assume that $\mathcal{H}$ is uniform (i.e. 2^{-n}-regular) and XOR-universal (i.e., 2^{-n}-AXU). Then Corollary 2 shows that $\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}$ in Equation (13) is secure roughly up to $p_1 = p_2 = q = \mathcal{O}(2^{2n/3})$ adversarial queries. This means that $\mathsf{TPRF}^{P_1,P_2}_{H_{K_h^1},H_{K_h^2}}$ is a beyond-birthday secure tweakable PRF.

Finally, let $\mathcal{M}$ denote a message space. Given an ϵ_1-regular and ϵ_2-AXU keyed hash family $\mathcal{H}$ from $\mathcal{M}$ to $\{0,1\}^n$, we can construct a nonce based MAC (denoted by Sum2PMAC), from two random permutations $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$ and $\mathcal{H}$, as

$$T = P_1(N \oplus H_{K_h^1}(M)) \oplus P_2(N \oplus H_{K_h^2}(M)) \oplus H_{K_h^1}(M) \oplus H_{K_h^2}(M), \tag{18}$$

where $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$, $M \in \mathcal{M}$ is message, and $N \in \{0,1\}^n$ is a nonce. Due to assumption of $\mathcal{H}$, when we set $\mathcal{T} = \mathcal{M}$, then $(H_{K_h^1}, H_{K_h^2})$ is a good (ϵ_1, ϵ_2)-key-derivation pair. Therefore, the following corollary holds.

Corollary 3. *Let $n \in \mathbb{N}$, and $\mathcal{M}$ be a message space. Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{M}$ to $\{0,1\}^n$. Consider the nonce based MAC* Sum2PMAC *defined in (18) from two random permutations $P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n)$. For any deterministic distinguisher $\mathcal{D}$ making at most p_1 queries to P_1, p_2 queries to P_2, and q evaluation queries, we have*

$$\begin{aligned}\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{Sum2PMAC}}(\mathcal{D}) \leq & 3qp_1p_2\epsilon_1^2 + \frac{\epsilon_1(\epsilon_2 q^2 + 2\sqrt{q})(p_1+p_2)}{2} + 2\epsilon_2^2 q^3 + \epsilon_2 q^{3/2} \\ & + \frac{4q(p_1+p_2+2q)^2}{2^{2n}} + \frac{2\sqrt{q}(p_1+p_2)}{2^n} + \frac{11q}{2^n}.\end{aligned} \tag{19}$$

Assume that for any message $M \in \mathcal{M}$, one has $|M| < n \cdot l$ for some integer $l \in \mathbb{N}$. Then the keyed hash family from $\mathcal{M}$ to $\{0,1\}^n$ can be instantiated by the $\mathsf{Poly}_{H_{K_h}}$ defined in (10), which is $\frac{l}{2^n}$-regular and $\frac{l}{2^n}$-AXU. In this case, when one sets $p_1 = p_2 = q$, then $\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{Sum2PMAC}}(\mathcal{D})$ in (19) can be bounded as

$$\frac{(6l^2+64)q^3}{2^{2n}} + \frac{(3l+4)q^{3/2}}{2^n} + \frac{11q}{2^n}.$$

If l is a constant, then Sum2PMAC is a beyond-birthday secure MAC.

Proof of Theorem 1. For convenience, we follow some notations in [16,17] in this proof. Let $\tau = (\mathcal{Q}_F, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (f_1, f_2))$ be an attainable transcript, where $|\mathcal{Q}_F| = q$, $|\mathcal{Q}_{P_1}| = p_1$, and $|\mathcal{Q}_{P_2}| = p_2$. In addition, we write these sets more clearly as:

$$\begin{aligned}\mathcal{Q}_F &= \{(t_1, x_1, y_1), \ldots, (t_q, x_q, y_q)\}, \\ \mathcal{Q}_{P_1} &= \{(u_{1,1}, v_{1,1}), \ldots, (u_{1,p_1}, v_{1,p_1})\}, \\ \mathcal{Q}_{P_2} &= \{(u_{2,1}, v_{2,1}), \ldots, (u_{2,p_2}, v_{2,p_2})\}.\end{aligned}$$

We denote

$$U_1 = \{u_1 \in \{0,1\}^n : (u_1, v_1) \in \mathcal{Q}_{P_1}\}, \quad V_1 = \{v_1 \in \{0,1\}^n : (u_1, v_1) \in \mathcal{Q}_{P_1}\},$$

and

$$U_2 = \{u_2 \in \{0,1\}^n : (u_2, v_2) \in \mathcal{Q}_{P_2}\}, \quad V_2 = \{v_2 \in \{0,1\}^n : (u_2, v_2) \in \mathcal{Q}_{P_2}\}.$$

For each $u \in \{0,1\}^n$, two associated sets can be defined as:

$$X_u^1 = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_1(t) = u\}, \quad X_u^2 = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_2(t) = u\}.$$

Now we define four parameters for transcript $\tau = (\mathcal{Q}_F, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (f_1, f_2))$ as

$$\begin{aligned}\alpha_1 &\overset{def}{=} |\{(t,x,y) \in \mathcal{Q}_F : x \oplus f_1(t) \in U_1\}|, \\ \alpha_2 &\overset{def}{=} |\{(t,x,y) \in \mathcal{Q}_F : x \oplus f_2(t) \in U_2\}|, \\ \beta_1 &\overset{def}{=} |\{(t,x,y) \in \mathcal{Q}_F : \exists (t,x,y) \neq (t',x',y'), x \oplus f_1(t) = x' \oplus f_1(t')\}|, \\ \beta_2 &\overset{def}{=} |\{(t,x,y) \in \mathcal{Q}_F : \exists (t,x,y) \neq (t',x',y'), x \oplus f_2(t) = x' \oplus f_2(t')\}|.\end{aligned}$$

β_1 and β_2 can be also expressed as

$$\beta_1 = \sum_{\substack{x \in \{0,1\}^n: \\ \delta_{D_1}(x) > 1}} \delta_{D_1}(x), \quad \beta_2 = \sum_{\substack{x \in \{0,1\}^n: \\ \delta_{D_2}(x) > 1}} \delta_{D_2}(x),$$

where $D_1 = \{x \oplus f_1(t) : (t,x,y) \in \mathcal{Q}_F\}$ and $D_2 = \{x \oplus f_2(t) : (t,x,y) \in \mathcal{Q}_F\}$.

An attainable transcript $\tau = (\mathcal{Q}_F, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (f_1, f_2))$ is said bad if any one of the following conditions is satisfied:

- (B-1): $\exists i \in [q], j \in [p_1], j' \in [p_2]$ for $(t_i, x_i, y_i) \in \mathcal{Q}_F$, $u_{1,j} \in U_1$, and $u_{2,j'} \in U_2$ such that $x_i \oplus f_1(t_i) = u_{1,j}$ and $x_i \oplus f_2(t_i) = u_{2,j'}$.
- (B-2): $\exists i \in [q], j \in [p_1], j' \in [p_2]$ for $(t_i, x_i, y_i) \in \mathcal{Q}_F$, $(u_{1,j}, v_{1,j}) \in \mathcal{Q}_{P_1}$, and $v_{2,j'} \in V_2$ such that $x_i \oplus f_1(t_i) = u_{1,j}$ and $v_{1,j} \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{2,j'}$.
- (B-3): $\exists i \in [q], j \in [p_1], j' \in [p_2]$ for $(t_i, x_i, y_i) \in \mathcal{Q}_F$, $v_{1,j} \in V_1$, and $(u_{2,j'}, v_{2,j'}) \in \mathcal{Q}_{P_2}$ such that $x_i \oplus f_2(t_i) = u_{2,j'}$ and $v_{2,j'} \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{1,j}$.
- (B-4): $\exists i, i' \in [q]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ such that $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$ and $y_i \oplus f_1(t_i) \oplus f_2(t_i) = y_{i'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'})$.
- (B-5): $\exists i, i' \in [q]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ such that $x_i \oplus f_2(t_i) = x_{i'} \oplus f_2(t_{i'})$ and $y_i \oplus f_1(t_i) \oplus f_2(t_i) = y_{i'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'})$.
- (B-6): $\exists i, i' \in [q], j \in [p_1]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$, and $u_{1,j} \in U_1$ such that $x_i \oplus f_1(t_i) = u_{1,j}$ and $x_i \oplus f_2(t_i) = x_{i'} \oplus f_2(t_{i'})$.
- (B-7): $\exists i, i' \in [q], j \in [p_2]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$, and $u_{2,j} \in U_2$ such that $x_i \oplus f_2(t_i) = u_{2,j}$ and $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$.
- (B-8): $\exists i, i', i'' \in [q]$ for distinct tuples $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (t_{i''}, x_{i''}, y_{i''}) \in \mathcal{Q}_F$, such that $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$ and $x_i \oplus f_2(t_i) = x_{i''} \oplus f_2(t_{i''})$.
- (B-9): $\exists i, i' \in [q], j, j' \in [p_1]$ for $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ and $(u_{1,j}, v_{1,j}), (u_{1,j'}, v_{1,j'}) \in \mathcal{Q}_{P_1}$ such that $x_i \oplus f_1(t_i) = u_{1,j}$, $x_{i'} \oplus f_1(t_{i'}) = u_{1,j'}$, and $f_1(t_i) \oplus f_2(t_i) \oplus v_{1,j} \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus v_{1,j'} \oplus y_{i'}$.
- (B-10): $\exists i, i' \in [q], j, j' \in [p_2]$ for $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ and $(u_{2,j}, v_{2,j}), (u_{2,j'}, v_{2,j'}) \in \mathcal{Q}_{P_2}$ such that $x_i \oplus f_2(t_i) = u_{2,j}$, $x_{i'} \oplus f_2(t_{i'}) = u_{2,j'}$, and $f_1(t_i) \oplus f_2(t_i) \oplus v_{2,j} \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus v_{2,j'} \oplus y_{i'}$.
- (B-11): $\alpha_1 \geq \sqrt{q}$.
- (B-12): $\alpha_2 \geq \sqrt{q}$.
- (B-13): $\beta_1 \geq \sqrt{q}$ or $\beta_2 \geq \sqrt{q}$.

Otherwise, we call τ a good transcript.

3.1. Analysis of Bad Transcripts

The proportion of all bad transcripts in the ideal world is upper bounded by the following lemma.

Lemma 3. *Let T_{id} be the probability distribution of transcript $\tau = (\mathcal{Q}_F, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (f_1, f_2))$ in the ideal world, where $|\mathcal{Q}_{P_1}| = p_1$, $|\mathcal{Q}_{P_2}| = p_2$, $|\mathcal{Q}_F| = q$, and (f_1, f_2) is a good (ϵ_1, ϵ_2)-key-derivation pair. Then we have*

$$\Pr[T_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}] \leq 3qp_1p_2\epsilon_1^2 + \frac{\epsilon_1(\epsilon_2 q^2 + 2\sqrt{q})(p_1+p_2)}{2} + 2\epsilon_2^2 q^3 + \frac{q}{2^n} + \epsilon_2 q^{3/2}.$$

Proof. Here we assume that there exists no repeated items in $\mathcal{Q}_{P_1}$, $\mathcal{Q}_{P_2}$, and $\mathcal{Q}_F$ w.l.o.g. Then for each distinct construction query $(t,x,y) \in \mathcal{Q}_F$, y is sampled uniformly and independently from $\{0,1\}^n$ in the ideal world. For each $i \in [13]$, the set of all transcripts satisfying (B-i) is denoted by Γ_i. By union bound, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}] \leq \sum_{i=1}^{13} \Pr[T_{\mathsf{id}} \in \Gamma_i]. \tag{20}$$

For each $i \in [13]$, the way to upper bound $\Pr[T_{\mathsf{id}} \in \Gamma_i]$ is similar to that in [16,17,22]. Hence, we give the details in Appendix A. By combining these upper bounds together, the proof of Lemma 3 is finished. □

3.2. Analysis of Good Transcripts

In Lemma 4, we show that the probability of any good transcript τ in the real world is close to its probability in the ideal world.

Lemma 4. *Let T_{id} be the probability distribution of transcripts in the ideal world, and T_{re} be the probability distribution in the real world. Then for any good transcript $\tau = (\mathcal{Q}_F, \mathcal{Q}_{P_1}, \mathcal{Q}_{P_2}, (f_1, f_2))$ with parameters p_1, p_2, and q satisfying $p_1 + p_2 + 3q \le 2^{n-1}$, one has*

$$\frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} \ge 1 - \frac{4q(p_1 + p_2 + 2q)^2}{2^{2n}} - \frac{2\sqrt{q}(p_1 + p_2)}{2^n} - \frac{10q}{2^n}.$$

Proof. Given a good transcript τ, we define the following probability

$$\mathsf{p}(\tau) \stackrel{\mathsf{def}}{=} \Pr[P_1, P_2 \xleftarrow{\$} \mathsf{Perm}(n) : F^{P_1,P_2}_{f_1,f_2} \vdash \mathcal{Q}_F \mid P_1 \vdash \mathcal{Q}_{P_1} \wedge P_2 \vdash \mathcal{Q}_{P_2}].$$

By a simple combinatorial argument, we have

$$\frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} = 2^{nq}\mathsf{p}(\tau). \tag{21}$$

The next goal is to lower bound $\mathsf{p}(\tau)$. For convenience, define five subsets of $\mathcal{Q}_F$ as follows:

$$\begin{aligned}
&\mathcal{Q}_{U_1} = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_1(t) \in U_1\}, \ \ \mathcal{Q}_{U_2} = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_2(t) \in U_2\},\\
&\mathcal{Q}_{X_1} = \{(t,x,y) \in \mathcal{Q}_F : \delta_{D_1}(x \oplus f_1(t)) > 1 \text{ and } x \oplus f_1(t) \notin U_1\},\\
&\mathcal{Q}_{X_2} = \{(t,x,y) \in \mathcal{Q}_F : \delta_{D_2}(x \oplus f_2(t)) > 1 \text{ and } x \oplus f_2(t) \notin U_2\},\\
&\mathcal{Q}_0 = \{(t,x,y) \in \mathcal{Q}_F : \delta_{D_1}(x \oplus h_1(t)) = \delta_{D_2}(x \oplus f_2(t)) = 1,\ x \oplus f_1(t) \notin U_1,\\
&\qquad \text{and } x \oplus f_2(t) \notin U_2\}.
\end{aligned}$$

Note that $|\mathcal{Q}_{U_1}| = \alpha_1$ and $|\mathcal{Q}_{U_2}| = \alpha_2$. The following proposition tells us that these sets form a partition of $\mathcal{Q}_F$.

Proposition 1. *Let $\tau \in \Gamma_{\mathsf{good}}$ be a good transcript. Then the sets $(\mathcal{Q}_{U_1}, \mathcal{Q}_{U_2}, \mathcal{Q}_{X_1}, \mathcal{Q}_{X_2}, \mathcal{Q}_0)$ defined above are pairwise disjoint.*

Proof. By definition, we have $\mathcal{Q}_{U_1} \cap \mathcal{Q}_{X_1} = \emptyset$, $\mathcal{Q}_{U_2} \cap \mathcal{Q}_{X_2} = \emptyset$, and $\mathcal{Q}_{U_1} \cap \mathcal{Q}_0 = \mathcal{Q}_{U_2} \cap \mathcal{Q}_0 = \mathcal{Q}_{X_1} \cap \mathcal{Q}_0 = \mathcal{Q}_{X_2} \cap \mathcal{Q}_0 = \emptyset$. Since τ does not satisfy (B-1), we have $\mathcal{Q}_{U_1} \cap \mathcal{Q}_{U_2} = \emptyset$. Moreover, $\mathcal{Q}_{U_1} \cap \mathcal{Q}_{X_2} = \emptyset$ (resp. $\mathcal{Q}_{U_2} \cap \mathcal{Q}_{X_1} = \emptyset$) since τ does not satisfy (B-6) (resp. (B-7)). Finally, $\mathcal{Q}_{X_1} \cap \mathcal{Q}_{X_2} = \emptyset$ holds due to the fact $\tau \notin \Gamma_8$. □

We use $E_{U_1}, E_{U_2}, E_{X_1}, E_{X_2}$, and E_0 to denote the events that $F^{P_1,P_2}_{f_1,f_2} \vdash \mathcal{Q}_{U_1}, \mathcal{Q}_{U_2}, \mathcal{Q}_{X_1}, \mathcal{Q}_{X_2}$, and $\mathcal{Q}_0$, respectively. Then $F^{P_1,P_2}_{f_1,f_2} \vdash \mathcal{Q}_F$ is equivalent to $E_{U_1} \wedge E_{U_2} \wedge E_{X_1} \wedge E_{X_2} \wedge E_0$. Hence, it holds that

$$\begin{aligned}
\mathsf{p}(\tau) &= \Pr[F^{P_1,P_2}_{f_1,f_2} \vdash \mathcal{Q}_F \mid P_i \vdash \mathcal{Q}_{P_i}, i = 1,2]\\
&= \Pr[E_{U_1} \wedge E_{U_2} \wedge E_{X_1} \wedge E_{X_2} \wedge E_0 \mid P_i \vdash \mathcal{Q}_{P_i}, i = 1,2]\\
&= \mathsf{p}'(\tau)\mathsf{p}''(\tau),
\end{aligned}$$

where

$$\mathsf{p}'(\tau) = \Pr[E_{U_1} \wedge E_{U_2} \mid P_i \vdash \mathcal{Q}_{P_i}, i = 1,2],$$

and

$$\mathsf{p}''(\tau) = \Pr[E_{X_1} \wedge E_{X_2} \wedge E_0 \mid E_{U_1} \wedge E_{U_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1,2)].$$

The way to compute $\mathsf{p}'(\tau)$ and $\mathsf{p}''(\tau)$, and the way to lower bound $\frac{\Pr[T_{\mathsf{re}}=\tau]}{\Pr[T_{\mathsf{id}}=\tau]}$ are similar to those in [16] so that we show the details in Appendix B. □

Finally, by Lemmas 1, 3, and 4, Theorem 1 can be proved. □

4. Multi-Key and Tweakable Secure PRFs from One Random Permutation

In this section, we first use one bidirectionally efficient random permutation $P \xleftarrow{\$} \mathsf{Perm}(n)$ to construct beyond-birthday and multi-key secure PRFs with a parallelizable structure as

$$F^P_{K_1,K_2}(x) = P(x \oplus K_1) \oplus P^{-1}(x \oplus K_2) \oplus K_1 \oplus K_2 \tag{22}$$

where $(K_1, K_2) \xleftarrow{\$} \{0,1\}^{2n}$ is the key and $x \in \{0,1\}^n$ is the input.

Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{T}$ to $\{0,1\}^n$. Then we can tweak the construction $F^P_{K_1,K_2}$ in Equation (22) as

$$\mathsf{TPRF}^P_{H_{K_h^1},H_{K_h^2}}(t,x) = P(x \oplus H_{K_h^1}(t)) \oplus P^{-1}(x \oplus H_{K_h^2}(t)) \oplus H_{K_h^1}(t) \oplus H_{K_h^2}(t), \tag{23}$$

where $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$, $t \in \mathcal{T}$, and $x \in \{0,1\}^n$.

As mentioned before, one can simultaneously show that the above two constructions are beyond-birthday secure in the multi-key and the tweakable settings by proving the BBB security of the "unified"function,

$$F^P_{f_1,f_2}(t,x) = P(x \oplus f_1(t)) \oplus P^{-1}(x \oplus f_2(t)) \oplus f_1(t) \oplus f_2(t), \tag{24}$$

where $(f_1, f_2) \in \mathsf{Func}(\mathcal{T}, \{0,1\}^n)^2$ is a good (ϵ_1, ϵ_2)-key-derivation pair, $P \xleftarrow{\$} \mathsf{Perm}(n)$, $t \in \mathcal{T}$, and $x \in \{0,1\}^n$.

Theorem 2. *Assume that $n \geq 6$ and $q \geq 64$ are two positive integers. Let $(f_1, f_2) \in \mathsf{Func}(\mathcal{T}, \{0,1\}^n)^2$ be a good (ϵ_1, ϵ_2)-key-derivation pair, and $P \xleftarrow{\$} \mathsf{Perm}(n)$ be a random permutation. Consider the function $F^P_{f_1,f_2} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ defined in* Equation (24)*. For any deterministic distinguisher $\mathcal{D}$ making at most p queries to P and q queries to the construction oracle $F^P_{f_1,f_2}$ or Φ such that $p + 2q + 6\sqrt{q} \leq 2^{n-1}$, one has*

$$\begin{aligned}\mathbf{Adv}^{unify}_{F^P_{f_1,f_2}}(\mathcal{D}) \leq & (3qp^2 + 2q^2p)\epsilon_1^2 + 2q^3\epsilon_2^2 + 2q^2p\epsilon_1\epsilon_2 + q^{3/2}\epsilon_2 + 2p\sqrt{q}\epsilon_1 + \frac{12q}{2^{2n/3}} \\ & + \frac{4q(p+2q+6\sqrt{q})^2 + q^3}{2^{2n}} + \frac{18q^{3/2} + 6p\sqrt{q} + 9q}{2^n} + \frac{16\sqrt{q}}{2^{n/3}}.\end{aligned} \tag{25}$$

Same to Corollary 1, the following corollary holds.

Corollary 4. *Assume $n \geq 6$ and $q \geq 64$ are two positive integers. Let $P \xleftarrow{\$} \mathsf{Perm}(n)$ be an n-bit random permutation. Consider the keyed function $F^P_{K_1,K_2} : \{0,1\}^n \to \{0,1\}^n$ defined in* (22)*. For any deterministic distinguisher $\mathcal{D}$ making at most p queries to P and at most totally q queries to $F^P_{K_1^1,K_2^1}, \ldots, F^P_{K_1^m,K_2^m}$ (resp. m independent ideal random functions $\varphi_1, \ldots, \varphi_m$) satisfying $p + 2q + 6\sqrt{q} \leq 2^{n-1}$, we have*

$$\begin{aligned}\mathbf{Adv}^{mk}_{F^P_{K_1,K_2}}(\mathcal{D}) \leq & \frac{4q(p+2q+6\sqrt{q})^2}{2^{2n}} + \frac{3q^3 + 3qp^2 + 4pq^2}{2^{2n}} \\ & + \frac{19q^{3/2} + 8p\sqrt{q} + 9q}{2^n} + \frac{16\sqrt{q}}{2^{n/3}} + \frac{12q}{2^{2n/3}}.\end{aligned} \tag{26}$$

Similarly, given an ϵ_1-regular and ϵ_2-AXU keyed hash family $\mathcal{H}$ from $\mathcal{T}$ to $\{0,1\}^n$, the following corollary holds.

Corollary 5. *Assume $n \geq 6$ and $q \geq 64$. Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{T}$ to $\{0,1\}^n$, and $P \xleftarrow{\$} \mathsf{Perm}(n)$ be an n-bit random permutation. Consider the tweakable function $\mathsf{TPRF}^P_{H_{K_h^1},H_{K_h^2}} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ defined in* (23)*. For any deterministic*

distinguisher $\mathcal{D}$ *making at most* p *queries to* P *and* q *queries to* $\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}$ *or* Φ *such that* $p+2q+6\sqrt{q} \le 2^{n-1}$, *we have*

$$\begin{aligned}\mathbf{Adv}^{tweak}_{\mathsf{TPRF}^{P}_{H_{K_h^1},H_{K_h^2}}}(\mathcal{D}) \le & (3qp^2+2q^2p)\epsilon_1^2+2q^3\epsilon_2^2+2q^2p\epsilon_1\epsilon_2+q^{3/2}\epsilon_2+2p\sqrt{q}\epsilon_1+\frac{12q}{2^{2n/3}} \\ & +\frac{4q(p+2q+6\sqrt{q})^2+q^3}{2^{2n}}+\frac{18q^{3/2}+6p\sqrt{q}+9q}{2^n}+\frac{16\sqrt{q}}{2^{n/3}}.\end{aligned} \tag{27}$$

Denote $\mathcal{M}$ as a message space. Let $\mathcal{H}$ be an ϵ_1-regular and ϵ_2-AXU keyed hash family from $\mathcal{M}$ to $\{0,1\}^n$. Then we can construct a nonce based MAC denoted by Sum1PMAC), from one random permutation $P \xleftarrow{\$} \mathsf{Perm}(n)$ as

$$T = P(N \oplus H_{K_h^1}(M)) \oplus P^{-1}(N \oplus H_{K_h^2}(M)) \oplus H_{K_h^1}(M) \oplus H_{K_h^2}(M), \tag{28}$$

where $(H_{K_h^1}, H_{K_h^2}) \xleftarrow{\$} \mathcal{H}^2$, $M \in \mathcal{M}$ is message, and $N \in \{0,1\}^n$ is a nonce. In this case, $(H_{K_h^1}, H_{K_h^2})$ is a good (ϵ_1,ϵ_2)-key-derivation pair, and we can obtain the following corollary.

Corollary 6. *Assume* $n \ge 3$ *and* $q \ge 64$. *Let* $\mathcal{H}$ *be an* ϵ_1*-regular and* ϵ_2*-AXU keyed hash family from* $\mathcal{M}$ *to* $\{0,1\}^n$. *Consider the nonce based MAC* Sum1PMAC *defined in* (28) *based on a random permutation* $P \xleftarrow{\$} \mathsf{Perm}(n)$ *and* $\mathcal{H}$. *For any deterministic distinguisher* $\mathcal{D}$ *making at most* p *queries to* P *and* q *evaluation queries, we have*

$$\begin{aligned}\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{Sum1PMAC}}(\mathcal{D}) \le & (3qp^2+2q^2p)\epsilon_1^2+2q^3\epsilon_2^2+2q^2p\epsilon_1\epsilon_2+q^{3/2}\epsilon_2+2p\sqrt{q}\epsilon_1+\frac{12q}{2^{2n/3}} \\ & +\frac{4q(p+2q+6\sqrt{q})^2+q^3}{2^{2n}}+\frac{18q^{3/2}+6p\sqrt{q}+9q}{2^n}+\frac{16\sqrt{q}}{2^{n/3}}.\end{aligned} \tag{29}$$

Let $\mathcal{M}$ denote a message space, where for some $l \in \mathbb{N}$, $|M| < n \cdot l$ holds for each message $M \in \mathcal{M}$. Then, the keyed hash family from $\mathcal{M}$ to $\{0,1\}^n$ can be instantiated by the $\mathsf{Poly}_{H_{K_h}}$ defined in (10), which is $\frac{l}{2^n}$-regular and $\frac{l}{2^n}$-AXU. In this setting, when l is set to a constant, then Sum1PMAC is a beyond-birthday secure MAC.

Proof of Theorem 2. In this proof, we follow some notations in [16,17] for convenience. Let $\bar{\tau} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2))$ be an attainable transcript with $|\bar{\mathcal{Q}}_F| = q$ and $|\bar{\mathcal{Q}}_P| = p$. We write these sets more clearly as follows:

$$\begin{aligned}\bar{\mathcal{Q}}_F &= \{(t_1,x_1,y_1),\ldots,(t_q,x_q,y_q)\},\\ \bar{\mathcal{Q}}_P &= \{(u_1,v_1),\ldots,(u_p,v_p)\}.\end{aligned}$$

We also denote

$$U = \{u_1 \in \{0,1\}^n : (u_1,v_1) \in \bar{\mathcal{Q}}_P\} \text{ and } V = \{v_1 \in \{0,1\}^n : (u_1,v_1) \in \bar{\mathcal{Q}}_P\}$$

as domain and range of $\bar{\mathcal{Q}}_P$ respectively. For each $u \in \{0,1\}^n$, two associated sets can be defined as:

$$\bar{X}^1_u = \{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) = u\} \text{ and } \bar{X}^2_u = \{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) = u\}.$$

Now we define four parameters for transcript $\bar{\tau} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2))$ as

$$\begin{aligned}\bar{\alpha}_1 &\overset{def}{=} |\{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \in U\}|,\\ \bar{\alpha}_2 &\overset{def}{=} |\{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) \in V\}|,\\ \bar{\beta}_1 &\overset{def}{=} |\{(t,x,y) \in \bar{\mathcal{Q}}_F : \exists (t,x,y) \ne (t',x',y'), x \oplus f_1(t) = x' \oplus f_1(t')\}|,\\ \bar{\beta}_2 &\overset{def}{=} |\{(t,x,y) \in \bar{\mathcal{Q}}_F : \exists (t,x,y) \ne (t',x',y'), x \oplus f_2(t) = x' \oplus f_2(t')\}|,\end{aligned}$$

where $\bar{\beta}_1$ and $\bar{\beta}_2$ can be also expressed as

$$\bar{\beta}_1 = \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{\bar{D}_1}(x)>1}} \delta_{\bar{D}_1}(x) \text{ and } \bar{\beta}_2 = \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{\bar{D}_2}(x)>1}} \delta_{\bar{D}_2}(x),$$

where $\bar{D}_1 = \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$ and $\bar{D}_2 = \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$.

An attainable transcript $\bar{\tau} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2))$ is said bad if any one of the following conditions is satisfied:

- (C-1): $\exists i \in [q]$ and $j, j' \in [p]$ for $(t_i, x_i, y_i) \in \bar{\mathcal{Q}}_F$, $u_j \in U$, and $v_{j'} \in V$ such that $x_i \oplus f_1(t_i) = u_j$ and $x_i \oplus f_2(t_i) = v_{j'}$.
- (C-2): $\exists i \in [q]$ and $j, j' \in [p]$ for $(t_i, x_i, y_i) \in \bar{\mathcal{Q}}_F$, $(u_j, v_j) \in \bar{\mathcal{Q}}_P$, and $u_{j'} \in U$ such that $x_i \oplus f_1(t_i) = u_j$ and $v_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = u_{j'}$.
- (C-3): $\exists i \in [q]$ and $j, j' \in [p]$ for $(t_i, x_i, y_i) \in \bar{\mathcal{Q}}_F$, $(u_j, v_j) \in \bar{\mathcal{Q}}_P$, and $v_{j'} \in V$ such that $x_i \oplus f_2(t_i) = v_j$ and $u_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{j'}$.
- (C-4): $\exists i, i' \in [q]$ and $j \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $(u_j, v_j) \in \bar{\mathcal{Q}}_P$ such that $x_i \oplus f_1(t_i) = u_j$ and $v_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = x_{i'} \oplus f_1(t_{i'})$.
- (C-5): $\exists i, i' \in [q]$ and $j \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $(u_j, v_j) \in \bar{\mathcal{Q}}_P$ such that $x_i \oplus f_2(t_i) = v_j$ and $u_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = x_{i'} \oplus f_2(t_{i'})$.
- (C-6): $\exists i, i' \in [q]$ and $j \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $u_j \in U$ such that $x_i \oplus f_1(t_i) = u_j$ and $x_i \oplus f_2(t_i) = x_{i'} \oplus f_2(t_{i'})$.
- (C-7): $\exists i, i' \in [q]$ and $j \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $v_j \in V$ such that $x_i \oplus f_2(t_i) = v_j$ and $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$.
- (C-8): $\exists i, i' \in [q]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ such that $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$ and $f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}$.
- (C-9): $\exists i, i' \in [q]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ such that $x_i \oplus f_2(t_i) = x_{i'} \oplus f_2(t_{i'})$ and $f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}$.
- (C-10):$\exists i, i'$, and $i'' \in [q]$ for pairwise distinct (t_i, x_i, y_i), $(t_{i'}, x_{i'}, y_{i'})$, and $(t_{i''}, x_{i''}, y_{i''}) \in \bar{\mathcal{Q}}_F$ such that $x_i \oplus f_1(t_i) = x_{i'} \oplus f_1(t_{i'})$ and $x_i \oplus f_2(t_i) = x_{i''} \oplus f_2(t_{i''})$.
- (C-11): $\exists i, i' \in [p]$ and $j, j' \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and (u_j, v_j),$(u_{j'}, v_{j'}) \in \bar{\mathcal{Q}}_P$ such that $x_i \oplus f_1(t_i) = u_j$, $x_{i'} \oplus f_1(t_{i'}) = u_{j'}$ and $v_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{j'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}$.
- (C-12): $\exists i, i' \in [p]$ and $j, j' \in [p]$ for $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and (u_j, v_j),$(u_{j'}, v_{j'}) \in \bar{\mathcal{Q}}_P$ such that $x_i \oplus f_2(t_i) = v_j$, $x_{i'} \oplus f_2(t_{i'}) = v_{j'}$ and $u_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = u_{j'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}$.
- (C-13): $\bar{\alpha}_1 \geq \sqrt{q}$.
- (C-14): $\bar{\alpha}_2 \geq \sqrt{q}$.
- (C-15): $\bar{\beta}_1 \geq \sqrt{q}$ or $\bar{\beta}_2 \geq \sqrt{q}$.
- (C-16): $\exists i, i'$, and $i'' \in [q]$ for pairwise distinct (t_i, x_i, y_i), $(t_{i'}, x_{i'}, y_{i'})$, and $(t_{i''}, x_{i''}, y_{i''}) \in \bar{\mathcal{Q}}_F$ such that $f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}$ and $f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i''}) \oplus f_2(t_{i''}) \oplus y_{i''}$.
- (C-17): For sets $\bar{\mathcal{Q}}_0 = \{(t,x,y) \in \bar{\mathcal{Q}}_F : \delta_{\bar{D}_1}(x \oplus f_1(t)) = \delta_{\bar{D}_2}(x \oplus f_2(t)) = 1, x \oplus f_1(t) \notin U, x \oplus f_2(t) \notin V\}$, $\hat{U} = U \cup \{v \oplus f_1(t) \oplus f_2(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F, (u,v) \in \bar{\mathcal{Q}}_P, x \oplus f_1(t) = u \in U\} \cup \{x \oplus f_1(t) : (t,x,y) \in \mathcal{Q}_F, x \oplus f_1(t) \notin U\}$, and $\hat{V} = V \cup \{u \oplus f_1(t) \oplus f_2(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_F, (u,v) \in \bar{\mathcal{Q}}_P, x \oplus f_2(t) = v \in V\} \cup \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_F, x \oplus f_2(t) \notin V\}$ derived from the transcript, $D_{\hat{U}} \stackrel{def}{=} |\{x_i \oplus f_2(t_i) \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'} \in \hat{U} : (t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_0\}| \geq q^{3/2}$ or $D_{\hat{V}} \stackrel{def}{=} |\{x_i \oplus f_1(t_i) \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'} \in \hat{V} : (t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_0\}| \geq q^{3/2}$.

Otherwise, τ is said a good transcript.

4.1. Analysis of Bad Transcripts

Let Γ'_i be the set of all transcripts satisfying (C-i) for $i \in [17]$. The proportion of all bad transcripts in the ideal world can be upper bounded in the following lemma.

Lemma 5. *Let T_{id} be the probability distribution of transcript $\bar{\tau} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2))$ in the ideal world, where $|\bar{\mathcal{Q}}_P| = p$, $|\bar{\mathcal{Q}}_F| = q$, and (f_1, f_2) is a good (ϵ_1, ϵ_2)-key-derivation pair. Then we have*

$$\begin{aligned}\Pr[T_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}] \leq & (3qp^2 + 2q^2p)\epsilon_1^2 + 2q^3\epsilon_2^2 + 2q^2p\epsilon_1\epsilon_2 + q^{3/2}\epsilon_2 \\ & + 2p\sqrt{q}\epsilon_1 + \frac{q + 2\sqrt{q}(p+q)}{2^n} + \frac{q^3}{2^{2n}}.\end{aligned}$$

Proof. Let $T_{\mathsf{id}} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2))$ be any attainable transcript in the ideal world, where $\bar{\mathcal{Q}}_P$ includes p permutation pairs from the interaction between distinguisher D and P. For each distinct construction query $(t, x, y) \in \bar{\mathcal{Q}}_F$, y is sampled uniformly and independently from $\{0,1\}^n$. Without loss of generality, we assume that there exists no repeated items in $\bar{\mathcal{Q}}_F$ and $\bar{\mathcal{Q}}_P$.

The probabilities of T_{id} in Γ_{bad} can be upper bounded as

$$\Pr[T_{\mathsf{id}} \in \Gamma_{\mathsf{bad}}] \leq \underbrace{\sum_{i=1}^{15} \Pr[T_{\mathsf{id}} \in \Gamma'_i]}_{\mathsf{Bad}_{M_1}} + \underbrace{\Pr[T_{\mathsf{id}} \in \Gamma'_{16}] + \Pr[T_{\mathsf{id}} \in \Gamma'_{17}]}_{\mathsf{Bad}_{M_2}}. \tag{30}$$

For Bad_{M_1}, one can obtain the following upper bound

$$\mathsf{Bad}_{M_1} \leq (3qp^2 + 2q^2p)\epsilon_1^2 + 2q^3\epsilon_2^2 + 2q^2p\epsilon_1\epsilon_2 + 2p\sqrt{q}\epsilon_1 + q^{3/2}\epsilon_2 + \frac{q}{2^n}, \tag{31}$$

and more details can be found in Appendix C.

For Bad_{M_2}, we need to study (C-16) and (C-17), respectively.

Bounding (C-16) : For any three distinct construction queries (t_i, x_i, y_i), $(t_{i'}, x_{i'}, y_{i'})$, and $(t_{i''}, x_{i''}, y_{i''}) \in \bar{\mathcal{Q}}_F$, $y_{i'}$ and $y_{i''}$ are independently and uniformly sampled from $\{0,1\}^n$. Hence, we have

$$\begin{aligned}\Pr[&(f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}) \wedge \\ &(f_1(t_i) \oplus f_2(t_i) \oplus y_i = f_1(t_{i''}) \oplus f_2(t_{i''}) \oplus y_{i''})] \leq \frac{1}{2^{2n}}.\end{aligned}$$

Since the number of all possible tuples for $((t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (t_{i''}, x_{i''}, y_{i''})) \in \bar{\mathcal{Q}}_F \times \bar{\mathcal{Q}}_F \times \bar{\mathcal{Q}}_F$ is at most q^3, by union bound, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{16}] \leq \frac{q^3}{2^{2n}}.$$

Bounding (C-17): First, we have $\{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \in U\} \cap \{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \notin U\} = \emptyset$ (which means $|\hat{U}| \leq p + q$). Hence, by the definition of $\bar{\mathcal{Q}}_0$, it holds that $\{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \in U\} \cap \bar{\mathcal{Q}}_0 = \emptyset$. Similarly, we also have $\{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) \in V\} \cap \{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) \notin V\} = \emptyset$ (which means $|\hat{V}| \leq p + q$) and $\{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) \in V\} \cap \bar{\mathcal{Q}}_0 = \emptyset$. By combing these facts and the definitions of $\hat{U}$, $\hat{V}$, and $\bar{\mathcal{Q}}_0$, the random value y for each $(t, x, y) \in \bar{\mathcal{Q}}_0$ in the ideal world is independent of any elements in $\hat{U}$ and $\hat{V}$. Therefore, for each pair $((t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'})) \in \bar{\mathcal{Q}}_0 \times \bar{\mathcal{Q}}_0$, one has

$$\Pr[x_i \oplus f_2(t_i) \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'} \in \hat{U}] \leq \frac{|\hat{U}|}{2^n} \leq \frac{p+q}{2^n}.$$

Then the expectation value of random variable $D_{\hat{U}}$ can be bounded as

$$\begin{aligned}\mathbb{E}[D_{\hat{U}}] &\leq \sum_{((t_i,x_i,y_i),(t_{i'},x_{i'},y_{i'})) \in \bar{\mathcal{Q}}_0^2 :} \Pr[x_i \oplus f_2(t_i) \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'} \in \hat{U}] \\ &\leq \frac{|\bar{\mathcal{Q}}_0|^2(p+q)}{2^n} \leq \frac{q^2(p+q)}{2^n}.\end{aligned}$$

By Markov's inequality, we have

$$\Pr[D_{\hat{U}} \geq q^{3/2}] \leq \frac{\mathbb{E}[D_{\hat{U}}]}{q^{3/2}} \leq \frac{\sqrt{q}(p+q)}{2^n}.$$

Similarly, it holds that

$$\Pr[D_{\hat{V}} \geq q^{3/2}] \leq \frac{\sqrt{q}(p+q)}{2^n}.$$

Therefore, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{17}] \leq \frac{2\sqrt{q}(p+q)}{2^n}.$$

Finally, by combining the upper bounds on Bad_{M_1} and Bad_{M_2} together, by (30), the proof of Lemma 5 is finished. □

4.2. Analysis of Good Transcripts

In this part, we prove that for any good transcript $\bar{\tau}$, the probability to sample it in the real world is close to that in the ideal world, and this result can be formally stated in the following lemma.

Lemma 6. *Assume that $n \geq 6$ and $q \geq 64$. Let T_{id} be the probability distribution of transcripts in the ideal world, and T_{re} be in the real world. Then for any good transcript $\bar{\tau} = (\bar{\mathcal{Q}}_F, \bar{\mathcal{Q}}_P, (f_1, f_2)) \in \Gamma_{\mathsf{good}}$ with parameters p and q satisfying $p + 2q + 6\sqrt{q} \leq 2^{n-1}$, one has*

$$\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} \geq 1 - \epsilon,$$

where $\epsilon = \frac{4q(p+2q+6\sqrt{q})^2}{2^{2n}} + \frac{16q^{3/2}+4p\sqrt{q}+8q}{2^n} + \frac{16\sqrt{q}}{2^{n/3}} + \frac{12q}{2^{2n/3}}$.

Proof. Given a good transcript $\bar{\tau}$, we define the following probability

$$\mathsf{p}(\bar{\tau}) \stackrel{\mathsf{def}}{=} \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : F^P_{f_1,f_2} \vdash \bar{\mathcal{Q}}_F \mid P \vdash \bar{\mathcal{Q}}_P].$$

By a simple combinatorial argument, it holds that

$$\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} = 2^{nq}\mathsf{p}(\bar{\tau}).$$

We first introduce some subsets of $\bar{\mathcal{Q}}_F$ as follows:

$$\begin{aligned}
&\bar{\mathcal{Q}}_U = \{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \in U\}, \;\; \bar{\mathcal{Q}}_V = \{(t,x,y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) \in V\},\\
&\bar{\mathcal{Q}}_{X_1} = \{(t,x,y) \in \bar{\mathcal{Q}}_F : \delta_{\bar{D}_1}(x \oplus f_1(t)) > 1 \text{ and } x \oplus f_1(t) \notin U\},\\
&\bar{\mathcal{Q}}_{X_2} = \{(t,x,y) \in \bar{\mathcal{Q}}_F : \delta_{\bar{D}_2}(x \oplus f_2(t)) > 1 \text{ and } x \oplus f_2(t) \notin V\},\\
&\bar{\mathcal{Q}}_0 = \{(t,x,y) \in \bar{\mathcal{Q}}_F : \delta_{\bar{D}_1}(x \oplus f_1(t)) = \delta_{\bar{D}_2}(x \oplus f_2(t)) = 1,\\
&\qquad x \oplus f_1(t) \notin U, \text{ and } x \oplus f_2(t) \notin V\}.
\end{aligned}$$

Note that $|\bar{\mathcal{Q}}_U| = \bar{\alpha}_1$, $|\bar{\mathcal{Q}}_V| = \bar{\alpha}_2$, and $\bar{\mathcal{Q}}_0$ has been defined in (C-17). In fact, these sets form a partition of $\bar{\mathcal{Q}}_F$.

Proposition 2. *Let $\bar{\tau} \in \Gamma_{\mathsf{good}}$ be a good transcript. Then $(\bar{\mathcal{Q}}_U, \bar{\mathcal{Q}}_V, \bar{\mathcal{Q}}_{X_1}, \bar{\mathcal{Q}}_{X_2}, \bar{\mathcal{Q}}_0)$ defined above are pairwise disjoint.*

Proof. By the definition of these five subsets, it holds that $\bar{\mathcal{Q}}_U \cap \bar{\mathcal{Q}}_{X_1} = \emptyset$, $\bar{\mathcal{Q}}_V \cap \bar{\mathcal{Q}}_{X_2} = \emptyset$, and $\bar{\mathcal{Q}}_U \cap \bar{\mathcal{Q}}_0 = \bar{\mathcal{Q}}_V \cap \bar{\mathcal{Q}}_0 = \bar{\mathcal{Q}}_{X_1} \cap \bar{\mathcal{Q}}_0 = \bar{\mathcal{Q}}_{X_2} \cap \bar{\mathcal{Q}}_0 = \emptyset$. Since $\bar{\tau}$ does not satisfy (C-1), one has $\bar{\mathcal{Q}}_U \cap \bar{\mathcal{Q}}_V = \emptyset$. Besides, $\bar{\mathcal{Q}}_U \cap \bar{\mathcal{Q}}_{X_2} = \emptyset$ (resp. $\bar{\mathcal{Q}}_V \cap \bar{\mathcal{Q}}_{X_1} = \emptyset$) holds since $\bar{\tau}$ does not satisfy (C-6) (resp. (C-7)). Finally, $\bar{\mathcal{Q}}_{X_1} \cap \bar{\mathcal{Q}}_{X_2} = \emptyset$ since $\bar{\tau} \notin \Gamma'_{10}$. □

We use $\bar{E}_U$, $\bar{E}_V$, $\bar{E}_{X_1}$, $\bar{E}_{X_2}$, and $\bar{E}_0$ to denote the events $F^P_{f_1,f_2} \vdash \bar{\mathcal{Q}}_U$, $\bar{\mathcal{Q}}_V$, $\bar{\mathcal{Q}}_{X_1}$, $\bar{\mathcal{Q}}_{X_2}$, and $\bar{\mathcal{Q}}_0$, respectively. Note that $F^P_{f_1,f_2} \vdash \bar{\mathcal{Q}}_F$ is equivalent to $\bar{E}_U \wedge \bar{E}_V \wedge \bar{E}_{X_1} \wedge \bar{E}_{X_2} \wedge \bar{E}_0$. Therefore, it holds that

$$\begin{aligned}\mathsf{p}(\bar{\tau}) &= \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : F^{P}_{f_1,f_2} \vdash \bar{\mathcal{Q}}_F \mid P \vdash \bar{\mathcal{Q}}_P] \\ &= \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : \bar{E}_U \wedge \bar{E}_V \wedge \bar{E}_{X_1} \wedge \bar{E}_{X_2} \wedge \bar{E}_0 \mid P \vdash \bar{\mathcal{Q}}_P] \\ &= \mathsf{p}'(\bar{\tau}) \cdot \mathsf{p}''(\bar{\tau}),\end{aligned}$$

where

$$\mathsf{p}'(\bar{\tau}) = \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : \bar{E}_U \wedge \bar{E}_V \mid P \vdash \bar{\mathcal{Q}}_P],$$

and

$$\mathsf{p}''(\bar{\tau}) = \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : \bar{E}_{X_1} \wedge \bar{E}_{X_2} \wedge \bar{E}_0 \mid \bar{E}_U \wedge \bar{E}_V \wedge (P \vdash \bar{\mathcal{Q}}_P)].$$

The next goal is to lower bound $\mathsf{p}'(\bar{\tau})$ and $\mathsf{p}''(\bar{\tau})$.

Lower Bounding $\mathsf{p}'(\bar{\tau})$. Conditioned on $P \vdash \bar{\mathcal{Q}}_P$, P is fixed on exactly p input-output pairs from U to V. For each $(t,x,y) \in \bar{\mathcal{Q}}_U$, there exists a unique $(u,v) \in \bar{\mathcal{Q}}_P$ satisfying $x \oplus f_1(t) = u$. Hence, $P(x \oplus f_1(t)) = P(u) = v$. Then we define two sets:

$$\begin{aligned}\bar{U}_1 &= \{P(x \oplus f_1(t)) \oplus f_1(t) \oplus f_2(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_U\}, \\ \bar{V}_1 &= \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_U\}.\end{aligned}$$

All values in $\bar{U}_1$ (resp. $\bar{V}_1$) are distinct since τ does not satisfy (C-11) (resp. (C-6)). Moreover, since $\bar{\tau} \notin \Gamma'_2$ and $\bar{\tau} \notin \Gamma'_1$, one has $\bar{U}_1 \cap U = \emptyset$ and $\bar{V}_1 \cap V = \emptyset$ respectively.

For each $(t,x,y) \in \bar{\mathcal{Q}}_V$, there exists a unique $(u,v) \in \bar{\mathcal{Q}}_P$ satisfying $x \oplus f_2(t) = v$. In this case, $P^{-1}(x \oplus f_2(t)) = u$. Then we can define two sets:

$$\begin{aligned}\bar{U}_2 &= \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_V\}, \\ \bar{V}_2 &= \{P^{-1}(x \oplus f_2(t)) \oplus f_1(t) \oplus f_2(t) \oplus y : (t,x,y) \in \bar{\mathcal{Q}}_V\}.\end{aligned}$$

All elements in $\bar{U}_2$ (resp. $\bar{V}_2$) are distinct since $\bar{\tau}$ does not satisfy (C-7) (resp. (C-12)). Due to the fact $\bar{\tau} \notin \Gamma'_1$ and $\bar{\tau} \notin \Gamma'_3$, one has $\bar{U}_2 \cap U = \emptyset$ and $\bar{V}_2 \cap V = \emptyset$, respectively. Moreover, $\bar{U}_2 \cap \bar{U}_1 = \emptyset$ (resp. $\bar{V}_2 \cap \bar{V}_1 = \emptyset$) since $\bar{\tau} \notin \Gamma'_4$ (resp. $\bar{\tau} \notin \Gamma'_5$). Besides, it holds that $|\bar{U}_1| = |\bar{V}_1| = |\bar{\mathcal{Q}}_U| = \bar{\alpha}_1$ and $|\bar{U}_2| = |\bar{V}_2| = |\bar{\mathcal{Q}}_V| = \bar{\alpha}_2$. Therefore, one can obtain that

$$\mathsf{p}'(\bar{\tau}) = \Pr[P \xleftarrow{\$} \mathsf{Perm}(n) : E_U \wedge E_V \mid P \vdash \bar{\mathcal{Q}}_P] = \frac{1}{(2^n - p)_{\bar{\alpha}_1 + \bar{\alpha}_2}}. \tag{32}$$

Now, we can define two disjoint collections $\mathcal{U} \stackrel{\mathsf{def}}{=} (U, \bar{U}_1, \bar{U}_2)$ and $\mathcal{V} \stackrel{\mathsf{def}}{=} (V, \bar{V}_1, \bar{V}_2)$. In this case, P is fixed on exactly $p + \bar{\alpha}_1 + \bar{\alpha}_2$ input-output pairs from $U \cup \bar{U}_1 \cup \bar{U}_2$ to $V \cup \bar{V}_1 \cup \bar{V}_2$.

Lower Bounding $\mathsf{p}''(\bar{\tau})$. When conditioned on $\bar{E}_U \wedge \bar{E}_V \wedge (P \vdash \bar{\mathcal{Q}}_P)$, we next lower bound the number of all possible "new" and distinct input-output pairs of P such that the event $\bar{E}_{X_1} \wedge \bar{E}_{X_2} \wedge \bar{E}_0$ happens. First, one can define some multi-sets associated to $\bar{\mathcal{Q}}_{X_1}$ and $\bar{\mathcal{Q}}_{X_2}$ as follows:

$$\begin{aligned}U_3 &= \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_{X_1}\}, \;\; U_5 = \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_{X_2}\}, \\ V_4 &= \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_{X_1}\}, \;\; V_6 = \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_{X_2}\}.\end{aligned}$$

Let $\alpha_3 = |U_3|$, $\alpha_4 = |V_4|$, $\alpha_5 = |U_5|$, and $\alpha_6 = |V_6|$. For convenience, we rewrite these sets as:

$$\begin{aligned}U_3 &= \{u_{3,1}, \ldots, u_{3,\alpha_3}\}, \;\; U_5 = \{u_{5,1}, \ldots, u_{5,\alpha_5}\}, \\ V_4 &= \{v_{4,1}, \ldots, v_{4,\alpha_4}\}, \;\; V_6 = \{v_{6,1}, \ldots, v_{6,\alpha_6}\}.\end{aligned}$$

Let $V_3 = P(U_3)$, $U_4 = P^{-1}(V_4)$, $V_5 = P(U_5)$, and $U_6 = P^{-1}(V_6)$. These sets can be written more clearly as:

$$\begin{aligned}V_3 &= \{P(x \oplus f_1(t)) : (t,x,y) \in \bar{\mathcal{Q}}_{X_1}\}, \;\; V_5 = \{P(x \oplus f_1(t)) : (t,x,y) \in \bar{\mathcal{Q}}_{X_2}\}, \\ U_4 &= \{P^{-1}(x \oplus f_2(t)) : (t,x,y) \in \bar{\mathcal{Q}}_{X_1}\}, \;\; U_6 = \{P^{-1}(x \oplus f_2(t)) : (t,x,y) \in \bar{\mathcal{Q}}_{X_2}\}.\end{aligned}$$

Recall that $\bar{D}_1 = \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$ and $\bar{D}_2 = \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_F\}$. Then, we get

$$\alpha_3 \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{\bar{D}_1}(x)>1}} 1 \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{\bar{D}_1}(x)>1}} \frac{\delta_{\bar{D}_1}(x)}{2} = \frac{\bar{\beta}_1}{2} \leq \frac{\sqrt{q}}{2},$$

$$\alpha_4 \leq \sum_{i=1}^{\alpha_3} \delta_{\bar{D}_1}(u_{3,i}) \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{\bar{D}_1}(x)>1}} \delta_{\bar{D}_1}(x) = \bar{\beta}_1 \leq \sqrt{q}.$$

Similarly, it also holds that $\alpha_6 \leq \frac{\sqrt{q}}{2}$ and $\alpha_5 \leq \sqrt{q}$. Since $\bar{\tau} \notin \Gamma'_{10}$, there exists no repeated items in V_4 and U_5. Hence, one can conclude that $\alpha_4 = |\bar{\mathcal{Q}}_{X_1}|$ and $\alpha_5 = |\bar{\mathcal{Q}}_{X_2}|$. Now we define two multi-sets associated to $\bar{\mathcal{Q}}_0$ as

$$U_7 = \{x \oplus f_1(t) : (t,x,y) \in \bar{\mathcal{Q}}_0\},\ \ V_8 = \{x \oplus f_2(t) : (t,x,y) \in \bar{\mathcal{Q}}_0\}.$$

By the definition of $\bar{\mathcal{Q}}_0$, there exists no repeated items in U_7 and V_8. Based on these two sets, one can define two corresponding sets as:

$$V_7 = P(U_7) = \{P(x \oplus f_1(t)) : (t,x,y) \in \bar{\mathcal{Q}}_0\},$$
$$U_8 = P^{-1}(V_8) = \{P^{-1}(x \oplus f_2(t)) : (t,x,y) \in \bar{\mathcal{Q}}_0\}.$$

Set $\mathcal{U}^+ = (U_3, U_5, U_7)$ and $\mathcal{V}^+ = (V_4, V_6, V_8)$ as two set collections. Then we can conclude the following proposition.

Proposition 3. *With notations as above, one has*

(i) All sets in $\mathcal{U}^+$ (resp. $\mathcal{V}^+$) are disjoint, i.e. $U_3 \cap U_5 = \emptyset$, $U_3 \cap U_7 = \emptyset$, and $U_5 \cap U_7 = \emptyset$ (resp. $V_4 \cap V_6 = \emptyset$, $V_4 \cap V_8 = \emptyset$, and $V_6 \cap V_8 = \emptyset$).

(ii) $\mathcal{U}^+$ is inner disjoint with $\mathcal{U}$, and $\mathcal{V}^+$ is inner disjoint with $\mathcal{V}$.

Proof. We first prove (i). From the fact $\bar{\tau} \notin \Gamma'_{10}$, we have $U_3 \cap U_5 = \emptyset$. By the definition of $\bar{\mathcal{Q}}_{X_1}$ and $\bar{\mathcal{Q}}_0$, one can conclude that $U_3 \cap U_7 = \emptyset$. $U_5 \cap U_7 = \emptyset$ holds due to the fact $\bar{\tau} \notin \Gamma'_{10}$, and the disjoint property of $\bar{\mathcal{Q}}_{X_1}$ and $\bar{\mathcal{Q}}_0$. We can conclude that $V_4 \cap V_6 = \emptyset$, $V_4 \cap V_8 = \emptyset$, and $V_6 \cap V_8 = \emptyset$ in a similar way.

Next we prove (ii) by enumerating all possible cases. For U_3, the definition of $\bar{\mathcal{Q}}_{X_1}$ means that $U_3 \cap U = \emptyset$; $U_3 \cap \bar{U}_1 = \emptyset$ comes from the fact $\bar{\tau} \notin \Gamma'_4$; $U_3 \cap \bar{U}_2 = \emptyset$ holds due to the disjoint property between $\bar{\mathcal{Q}}_{X_1}$ and $\bar{\mathcal{Q}}_V$, and the fact $\bar{\tau} \notin \Gamma'_7$. For U_5, $U_5 \cap U = \emptyset$ comes from the fact $\bar{\tau} \notin \Gamma'_6$, and the definition of $\bar{\mathcal{Q}}_{X_2}$; $U_5 \cap \bar{U}_1 = \emptyset$ comes from the fact $\bar{\tau} \notin \Gamma'_4$; By the disjoint property between $\bar{\mathcal{Q}}_{X_2}$ and $\bar{\mathcal{Q}}_V$, and the fact $\bar{\tau} \notin \Gamma'_7$, we have $U_5 \cap \bar{U}_2 = \emptyset$. For U_7, the definition of $\bar{\mathcal{Q}}_0$ means $U_7 \cap U = \emptyset$; $U_7 \cap \bar{U}_1 = \emptyset$ comes from the fact that $\bar{\tau} \notin \Gamma'_4$; By the disjoint property between $\bar{\mathcal{Q}}_0$ and $\bar{\mathcal{Q}}_V$, and the fact $\bar{\tau} \notin \Gamma'_7$, we has $U_7 \cap \bar{U}_2 = \emptyset$.

For V_4, $V_4 \cap V = \emptyset$ comes from the fact $\bar{\tau} \notin \Gamma'_7$, and the definition of $\bar{\mathcal{Q}}_{X_1}$; $V_4 \cap \bar{V}_1 = \emptyset$ can be derived from the disjoint property between $\bar{\mathcal{Q}}_{X_1}$ and $\bar{\mathcal{Q}}_U$, and the fact $\bar{\tau} \notin \Gamma'_6$; The fact $\bar{\tau} \notin \Gamma'_5$ means $V_4 \cap \bar{V}_2 = \emptyset$. For V_6, $V_6 \cap V = \emptyset$ holds from definition of $\bar{\mathcal{Q}}_{X_2}$; $V_6 \cap V_1 = \emptyset$ comes from the definition of $\bar{\mathcal{Q}}_{X_2}$, and the fact $\bar{\tau} \notin \Gamma'_6$; The fact $\bar{\tau} \notin \Gamma'_5$ means $V_6 \cap \bar{V}_2 = \emptyset$. For V_8, $V_8 \cap V = \emptyset$ comes from definition of $\bar{\mathcal{Q}}_0$; $V_8 \cap \bar{V}_1 = \emptyset$ holds due to the disjoint property between $\bar{\mathcal{Q}}_0$ and $\bar{\mathcal{Q}}_U$, and the fact $\bar{\tau} \notin \Gamma'_6$; Finally the fact $\bar{\tau} \notin \Gamma'_5$ means $V_8 \cap \bar{V}_2 = \emptyset$. □

Now we define two disjoint union sets $U^{++} = U \cup \bar{U}_1 \cup \bar{U}_2 \cup U_3 \cup U_5 \cup U_7$ (which equals to $\hat{U}$ in (C-17)), and $V^{++} = V \cup \bar{V}_1 \cup \bar{V}_2 \cup V_4 \cup V_6 \cup V_8$ (which equals to $\hat{V}$ in (C-17)).

Let $\bar{q}' = |\bar{\mathcal{Q}}_0| = q - (|\bar{\mathcal{Q}}_U| + |\bar{\mathcal{Q}}_V| + |\bar{\mathcal{Q}}_{X_1}| + |\bar{\mathcal{Q}}_{X_2}|) = q - (\bar{\alpha}_1 + \bar{\alpha}_2 + \alpha_4 + \alpha_5)$ (actually, $\bar{q}' = |U_7| = |V_8|$) and $M = \lfloor \frac{\bar{q}'}{2^{n/3}} \rfloor$. Then it holds that $\bar{q}' - 2M \geq \bar{q}'/2$ if $n \geq 6$. Next we try to sample "new" values for V_7 and U_8 by allowing that there exist many construction queries $(t,x,y), (t',x',y') \in \bar{\mathcal{Q}}_0$ such that $P(x \oplus f_1(t)) \oplus f_1(t) \oplus f_2(t) \oplus y = x' \oplus f_1(t')$ or $P^{-1}(x \oplus f_2(t)) \oplus f_1(t) \oplus f_2(t) \oplus y = x' \oplus f_2(t')$ holds. In the first case, we can obtain three maps like

$$\begin{cases} x \oplus f_1(t) \xmapsto{P} x' \oplus f_1(t') \oplus f_1(t) \oplus f_2(t) \oplus y, \\ x' \oplus f_1(t') \xmapsto{P} x \oplus f_2(t), \\ x \oplus f_2(t) \oplus f_1(t') \oplus f_2(t') \oplus y' \xmapsto{P} x' \oplus f_2(t'). \end{cases}$$

In the second case, we have

$$\begin{cases} x' \oplus f_1(t') \xmapsto{P} x \oplus f_1(t) \oplus f_1(t') \oplus f_2(t') \oplus y', \\ x \oplus f_1(t) \xmapsto{P} x' \oplus f_2(t'), \\ x' \oplus f_2(t') \oplus f_1(t) \oplus f_2(t) \oplus y \xmapsto{P} x \oplus f_2(t). \end{cases}$$

If $x \oplus f_2(t) \oplus f_1(t') \oplus f_2(t') \oplus y' \notin U^{++}$ and $x' \oplus f_1(t') \oplus f_1(t) \oplus f_2(t) \oplus y \notin V^{++}$, or $x' \oplus f_2(t') \oplus f_1(t) \oplus f_2(t) \oplus y \notin U^{++}$ and $x \oplus f_1(t) \oplus f_1(t') \oplus f_2(t') \oplus y' \notin V^{++}$, then the above permutation maps are compatible with $\bar{\mathcal{Q}}_F$ and $\bar{\mathcal{Q}}_P$. Intuitively, when we consider the above "collision" maps, there would be as many permutations chosen to be compatible with $\bar{\mathcal{Q}}_F$ and $\bar{\mathcal{Q}}_P$ as possible so that our construction can achieve BBB security.

Conditioned on $\bar{E}_U \wedge \bar{E}_V \wedge (P \vdash \bar{\mathcal{Q}}_P)$, we next describe all possible permutations satisfying $E_{X_1} \wedge E_{X_2} \wedge E_0$, and finally compute and lower bound $\mathsf{p}''(\bar{\tau})$.

For each $\alpha \in [M]$, we define the following set

$$S = \{((\sigma_1, \xi_1), (\sigma_1', \xi_1')), \ldots, ((\sigma_\alpha, \xi_\alpha), (\sigma_\alpha', \xi_\alpha'))\},$$

where for each $1 \le k \le \alpha$, one has $\sigma_k = x_k \oplus f_1(t_k)$ (resp. $\xi_k = x_k \oplus f_2(t_k)$) for some query $(t_k, x_k, y_k) \in \bar{\mathcal{Q}}_0$ and $\sigma_k' = x_k' \oplus f_1(t_k')$ (resp. $\xi_k' = x_k' \oplus f_2(t_k')$) for another query $(t_k', x_k', y_k') \in \bar{\mathcal{Q}}_0$.

Definition 2. *We say* $S = \{((\sigma_1, \xi_1), (\sigma_1', \xi_1')), \ldots, ((\sigma_\alpha, \xi_\alpha), (\sigma_\alpha', \xi_\alpha'))\}$ *a "good" set if the following four conditions are all satisfied*

(1) $x_k \oplus f_2(t_k) \oplus f_1(t_k') \oplus f_2(t_k') \oplus y_k' \notin U^{++}$,
(2) $x_k' \oplus f_1(t_k') \oplus f_1(t_k) \oplus f_2(t_k) \oplus y_k \notin V^{++}$,
(3) $x_k \oplus f_2(t_k) \oplus f_1(t_k') \oplus f_2(t_k') \oplus y_k' \neq x_{k'} \oplus f_2(t_{k'}) \oplus f_1(t_{k'}') \oplus f_2(t_{k'}') \oplus y_{k'}'$, *for any* $k' < k$,
(4) $x_k' \oplus f_1(t_k') \oplus f_1(t_k) \oplus f_2(t_k) \oplus y_k \neq x_{k'}' \oplus f_1(t_{k'}') \oplus f_1(t_{k'}) \oplus f_2(t_{k'}) \oplus y_{k'}$, *for any* $k' < k$.

The next lemma shows that for each $\alpha \in [M]$, the number of all possible "good" sets derived from $\bar{\mathcal{Q}}_0$ is close to $(\bar{q}')_{2\alpha}/\alpha!$.

Lemma 7. *Assume that* $q \ge 64$ *and* $n \ge 6$. *Let* α *be an integer with* $0 \le \alpha \le M = \lfloor \frac{\bar{q}'}{2^{n/3}} \rfloor$. *Let* $\mathcal{N}_S(\alpha)$ *be the number of all "good" sets derived from* $\bar{\mathcal{Q}}_0$. *Then we have*

$$\mathcal{N}_S(\alpha) \ge \frac{(\bar{q}')_{2\alpha}}{\alpha!}(1 - \epsilon_0),$$

where $\epsilon_0 = \frac{6q}{2^{2n/3}} + \frac{16\sqrt{q}}{2^{n/3}}$.

Proof. We count all possible pairs in a "good" set step by step as follows. First, we decide all possible pairs for $((\sigma_1, \xi_1), (\sigma_1', \xi_1'))$. There are $\bar{q}'(\bar{q}' - 1)$ possible pairs to be chosen for $((\sigma_1, \xi_1), (\sigma_1', \xi_1'))$. Since $\tau \notin \Gamma_{17}'$, there are at most $2q^{3/2}$ pairs not satisfying the first two conditions in Definition 2. Then we can choose at least $\bar{q}'(\bar{q}' - 1) - 2q^{3/2}$ possible pairs for $((\sigma_1, \xi_1), (\sigma_1', \xi_1'))$.

After choosing $(\sigma_1, \xi_1), (\sigma_1', \xi_1')$, we decide all possible $((\sigma_2, \xi_2), (\sigma_2', \xi_2'))$ in the following way. We first choose (σ_2, ξ_2) from the remaining $\bar{q}' - 2$ possible pairs, and then choose the corresponding pair (σ_2', ξ_2') outside of (σ_1, ξ_1), (σ_1', ξ_1'), and (σ_2', ξ_2') to satisfy all four conditions in Definition 2. To satisfy the last two conditions 3) and 4) in Definition 2, σ_2' and ξ_2' should chosen such that

$$\begin{cases} \xi_2 \neq \xi_1 \oplus f_1(t_1') \oplus f_2(t_1') \oplus y_1' \oplus f_1(t_2') \oplus f_2(t_2') \oplus y_2', \\ \sigma_2' \neq \sigma_1' \oplus f_1(t_1) \oplus f_2(t_1) \oplus y_1 \oplus f_1(t_2) \oplus f_2(t_2) \oplus y_2. \end{cases}$$

In this case, from the definition of $\bar{\mathcal{Q}}_0$ and the fact $\bar{\tau} \notin \Gamma'_{16}$, it excludes at most 3 possibilities to be chosen for (σ'_2, ξ'_2). Then there are at least $(\bar{q}'-2)(\bar{q}'-6)$ possibilities to be chosen for $((\sigma_2,\xi_2),(\sigma'_2,\xi'_2))$, when we only consider the last two conditions in Definition 2. Finally, from the fact $\tau \notin \Gamma'_{17}$, there are at most $2q^{3/2}$ pairs to be removed for all possibilities $((\sigma_2,\xi_2),(\sigma'_2,\xi'_2))$ if we want them to satisfy the first two conditions 1) and 2) in Definition 2. Overall, there are at least $(\bar{q}'-2)(\bar{q}'-6)-2q^{3/2}$ possible pairs to be chosen for $((\sigma_2,\xi_2),(\sigma'_2,\xi'_2))$.

After choosing $k-1$ pairs $((\sigma_1,\xi_1),(\sigma'_1,\xi'_1)),\ldots,((\sigma_{k-1},\xi_{k-1}),(\sigma'_{k-1},\xi'_{k-1}))$, there are at least $(\bar{q}'-2k)(\bar{q}'-5k-1)-2q^{3/2}$ possible pairs to be chosen for $((\sigma_k,\xi_k),(\sigma'_k,\xi'_k))$ by repeating the above step.

When we finish the choice of all possible cases for $(((\sigma_1,\xi_1),(\sigma'_1,\xi'_1)),\ldots,((\sigma_\alpha,\xi_\alpha),(\sigma'_\alpha,\xi'_\alpha)))$ satisfying all four conditions in Definition 2, one can conclude that

$$\mathcal{N}_S(\alpha) \geq \frac{1}{\alpha!}\prod_{k=0}^{\alpha-1}((\bar{q}'-2k)(\bar{q}'-5k-1)-2q^{3/2}), \tag{33}$$

where the term $\alpha!$ appears because the set S is unordered.

Furthermore, $\mathcal{N}_S(\alpha)$ can be lower bounded as follows

$$\begin{aligned}
\mathcal{N}_S(\alpha) &\geq \frac{1}{\alpha!}\prod_{k=0}^{\alpha-1}((\bar{q}'-2k)(\bar{q}'-5k-1)-2q^{3/2}) \\
&\geq \frac{(\bar{q}')_{2\alpha}}{\alpha!}\prod_{k=0}^{\alpha-1}\frac{(\bar{q}'-2k)(\bar{q}'-5k-1)-2q^{3/2}}{(\bar{q}'-2k)(\bar{q}'-2k-1)} \\
&\geq \frac{(\bar{q}')_{2\alpha}}{\alpha!}\prod_{k=0}^{\alpha-1}\left(1-\frac{3k\bar{q}'-6k^2+2q^{3/2}}{(\bar{q}'-2k)(\bar{q}'-2k-1)}\right) \\
&\overset{(i)}{\geq} \frac{(\bar{q}')_{2\alpha}}{\alpha!}\prod_{k=0}^{\alpha-1}\left(1-\frac{3k\bar{q}'+2q^{3/2}}{(\bar{q}'-2M)^2}\right) \\
&\geq \frac{(\bar{q}')_{2\alpha}}{\alpha!}\left(1-\frac{3\bar{q}'M^2/2+2q^{3/2}M}{(\bar{q}'-2M)^2}\right) \\
&\overset{(ii)}{\geq} \frac{(\bar{q}')_{2\alpha}}{\alpha!}\left(1-\frac{6\bar{q}'M^2+8q^{3/2}M}{\bar{q}'^2}\right) \\
&\overset{(iii)}{\geq} \frac{(\bar{q}')_{2\alpha}}{\alpha!}\left(1-\frac{6\bar{q}'}{2^{2n/3}}-\frac{8q^{3/2}}{q'2^{n/3}}\right) \\
&\overset{(iv)}{\geq} \frac{(\bar{q}')_{2\alpha}}{\alpha!}\left(1-\frac{6q}{2^{2n/3}}-\frac{16\sqrt{q}}{2^{n/3}}\right),
\end{aligned}$$

where (i) follows as $\bar{q}'-2k, q'-2k-1 \geq \bar{q}'-2\alpha \geq \bar{q}'-2M$, (ii) follows as $\bar{q}'-2M > \bar{q}'/2$, (iii) follows as $M \leq \frac{\bar{q}'}{2^{n/3}}$, and (iv) follows as $q/2 \leq q-4\sqrt{q} \leq \bar{q}'$ if $q > 64$. □

For a fixed α with $0 \leq \alpha \leq M$ and a corresponding "good" set

$$S = \{((\sigma_1,\xi_1),(\sigma'_1,\xi'_1)),\ldots,((\sigma_\alpha,\xi_\alpha),(\sigma'_\alpha,\xi'_\alpha))\},$$

the following assignment (34) for P is well-defined by the definition of S:

$$\forall k \in [\alpha] \quad \begin{cases} \sigma_k \overset{P}{\longmapsto} \sigma'_k \oplus f_1(t_k) \oplus f_2(t_k) \oplus y_k, \\ \sigma'_k \overset{P}{\longmapsto} \xi_k, \\ \xi_k \oplus f_1(t'_k) \oplus f_2(t'_k) \oplus y'_k \overset{P}{\longmapsto} \xi'_k. \end{cases} \tag{34}$$

Furthermore, based on the "good" set S, we define two subsets of $\mathcal{U}_7$ and $\mathcal{V}_8$ as

$$\begin{aligned}
\mathcal{U}_{7,1} &\overset{def}{=} \{\sigma_1 = x_1 \oplus f_1(t_1), \sigma'_1 = x'_1 \oplus f_1(t'_1), \ldots, \sigma_\alpha = x_\alpha \oplus f_1(t_\alpha), \sigma'_\alpha = x'_\alpha \oplus f_1(t'_\alpha)\}, \\
\mathcal{V}_{8,1} &\overset{def}{=} \{\xi_1 = x_1 \oplus f_2(t_1), \xi'_1 = x'_1 \oplus f_2(t'_1), \ldots, \xi_\alpha = x_\alpha \oplus f_2(t_\alpha), \xi'_\alpha = x'_\alpha \oplus f_2(t'_\alpha)\}.
\end{aligned}$$

Besides, we can also denote two additional sets as

$$U'_{7,1} \stackrel{def}{=} \{\xi_1 \oplus f_1(t'_1) \oplus f_2(t'_1) \oplus y'_1, \ldots, \xi_\alpha \oplus f_1(t'_\alpha) \oplus f_2(t'_\alpha) \oplus y'_\alpha\},$$
$$V'_{8,1} \stackrel{def}{=} \{\sigma'_1 \oplus f_1(t_1) \oplus f_2(t_1) \oplus y_1, \ldots, \sigma'_\alpha \oplus f_1(t_\alpha) \oplus f_2(t_\alpha) \oplus y_\alpha\},$$

where $U'_{7,1} \cap U^{++} = \emptyset$ (resp. $V'_{8,1} \cap V^{++} = \emptyset$) and all items in $U'_{7,1}$ (resp. $V'_{8,1}$) are distinct. After the assignment (34) for P, P is fixed on 3α input-ouput pairs from $U_{7,1} \cup U'_{7,1}$ to $V_{8,1} \cup V'_{8,1}$. In addition, we can define the corresponding co-subset of $U_{7,1}$ and $V_{8,1}$ as $U_{7,2} \stackrel{def}{=} U_7 \setminus U_{7,1}$ and $V_{8,2} \stackrel{def}{=} V_8 \setminus V_{8,2}$, respectively.

Until now, the random permutation P is fixed on p input-output pairs from U to V, $\bar{\alpha}_1$ input-output pairs from $\bar{U}_1$ to $\bar{V}_1$, $\bar{\alpha}_2$ input-output pairs from $\bar{U}_2$ to $\bar{V}_2$, and 3α input-output pairs from $U_{7,1} \cup U'_{7,1}$ to $V_{8,1} \cup V'_{8,1}$. Based on these facts, the next work is to choose all other possible compatible items for $V_3 = P(U_3)$, $U_4 = P^{-1}(V_4)$, $V_5 = P(U_5)$, $U_6 = P^{-1}(V_6)$, $V_{7,2} = P(U_{7,2})$ and $U_{8,2} = P^{-1}(V_{8,2})$ to extend the fixed input-output pairs of P.

Note that once the items in $V_3 = P(U_3)$ are fixed, the corresponding items in $U_4 = P^{-1}(V_4)$ are uniquely determined since these two sets are both derived from $\bar{\mathcal{Q}}_{X_1}$. Similarly, the items in $V_5 = P(U_5)$ (resp. $V_{7,2} = P(U_{7,2})$) uniquely determine the items in $U_6 = P^{-1}(V_6)$ (resp. $U_{8,2} = P^{-1}(V_{8,2})$). Then we sample all possible items for these sets through three steps.

Step I. Construct $\mathbf{V_3 = P(U_3)}$ and $\mathbf{U_4 = P^{-1}(V_4)}$.

Let $U^{3+} = U^{++} \cup U'_{7,1}$ and $V^{3+} = V^{++} \cup V'_{8,1}$. The size of U^{3+} is $\Delta_1 = p + \bar{\alpha}_1 + \bar{\alpha}_2 + \alpha_3 + \alpha_5 + \bar{q}' + \alpha$, and the size of V^{3+} is $\Delta_2 = p + \bar{\alpha}_1 + \bar{\alpha}_2 + \alpha_4 + \alpha_6 + \bar{q}' + \alpha$. Recall that $\bar{X}^1_u = \{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) = u\}$ and $\bar{X}^2_u = \{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_2(t) = u\}$. Let $\mathcal{N}_1(\alpha)$ be the number of distinct tuples $(v_{3,1}, \ldots, v_{3,\alpha_3})$ in $\{0,1\}^n \setminus V^{3+}$ such that the following two conditions are satisfied

(i) $\forall k \in [\alpha_3]$, for each $(t, x, y) \in \bar{X}^1_{u_{3,k}}$ where $u_{3,k} \in U_3$, $v_{3,k} \oplus f_1(t) \oplus f_2(t) \oplus y \notin U^{3+}$.

(ii) $\forall k', k \in [\alpha_3]$ with $k' < k$, for each $(t, x, y) \in \bar{X}^1_{u_{3,k}}$, $v_{3,k} \oplus f_1(t) \oplus f_2(t) \oplus y \neq v_{3,k'} \oplus f_1(t') \oplus f_2(t') \oplus y'$ should be satisfied for each $(t', x', y') \in \bar{X}^1_{u_{3,k'}}$.

Now we count the number of all possible distinct tuples $(v_{3,1}, \ldots, v_{3,\alpha_3}) \in \{0,1\}^n \setminus V^{3+}$ satisfying these two conditions. First, one has $|\{0,1\}^n \setminus V^{3+}| = 2^n - (p + \bar{\alpha}_1 + \bar{\alpha}_2 + \alpha_4 + \alpha_6 + \bar{q}' + \alpha)$. The first condition can remove at most $(p + \bar{\alpha}_1 + \bar{\alpha}_2 + \alpha_3 + \alpha_5 + \bar{q}' + \alpha)|\bar{X}^1_{u_{3,k}}|$ items for each k, and the second condition can exclude at most $|\bar{X}^1_{u_{3,k}}|(|\bar{X}^1_{u_{3,1}}| + \ldots + |\bar{X}^1_{u_{3,k-1}}|) \leq \alpha_4 \cdot |\bar{X}^1_{u_{3,k}}|$ values for each choice of $v_{3,k}$. By the choice of $v_{3,k}$ above, we obtain that

$$\mathcal{N}_1(\alpha) \geq \prod_{k=0}^{\alpha_3 - 1} \Big(2^n - \Delta_2 - k - (\Delta_1 + \alpha_4) \cdot |\bar{X}^1_{u_{3,k+1}}|\Big). \tag{35}$$

Let $V_3 = \{v_{3,1}, \ldots, v_{3,\alpha_3}\}$ and $U_4 = \{v_{3,k} \oplus f_1(t) \oplus f_2(t) \oplus y : k \in [\alpha_3], (t, x, y) \in \bar{X}^1_{u_{3,k}}\}$. The first condition ensures that U_4 is disjoint with U^{3+}. Items in U_4 are distinct due to the second condition and the fact $\bar{\tau} \notin \Gamma'_8$. This fact tells us that for each $k \in [\alpha_3]$ and $(t, x, y) \neq (t', x', y') \in \bar{X}^1_{u_{3,k}}$, it holds that $x \oplus f_1(t) = x' \oplus f_1(t') = u_{3,k}$ but $f_1(t) \oplus f_2(t) \oplus y \neq f_1(t') \oplus f_2(t') \oplus y'$, which means that $v_{3,k} \oplus f_1(t) \oplus f_2(t) \oplus y \neq v_{3,k} \oplus f_1(t') \oplus f_2(t') \oplus y'$. Moreover, items in V_3 are distinct, and V_3 is disjoint with V^{3+} by the choice of $(v_{3,1}, \ldots, v_{3,\alpha_3})$. Let $U^{4+} = U^{3+} \cup U_4$, and $V^{4+} = V^{3+} \cup V_3$. The size of U^{4+} is $\Delta_3 = \Delta_1 + \alpha_4$, and the size of V^{4+} is $\Delta_4 = \Delta_2 + \alpha_3$.

Step II. Construct $\mathbf{V_5 = P(U_5)}$, and $\mathbf{U_6 = P^{-1}(V_6)}$.

Recall that $V_6 = \{v_{6,1}, \ldots, v_{6,\alpha_6}\}$. Let $\mathcal{N}_2(\alpha)$ be the number of all distinct tuples $(u_{6,1}, \ldots, u_{6,\alpha_6})$ in $\{0,1\}^n \setminus U^{4+}$ satisfying the following two conditions:

(i) $\forall k \in [\alpha_6]$, for each $(t, x, y) \in \bar{X}^2_{v_{6,k}}$, $u_{6,k} \oplus f_1(t) \oplus f_2(t) \oplus y \notin V^{4+}$.

(ii) $\forall k', k \in [\alpha_6]$ with $k' < k$, for each $(t, x, y) \in X^2_{v_{6,k}}$, $u_{6,k} \oplus f_1(t) \oplus f_2(t) \oplus y \neq u_{6,k'} \oplus f_1(t') \oplus f_2(t') \oplus y'$ should be satisfied for each $(t', x', y') \in X^2_{v_{6,k'}}$.

Now we count the number of all possible distinct tuples $(u_{6,1},\ldots,u_{6,\alpha_6}) \in \{0,1\}^n \setminus U^{4+}$ satisfying these two conditions. Similarly, one has $|\{0,1\}^n \setminus U^{4+}| = 2^n - (p+\bar{\alpha}_1+\bar{\alpha}_2+\alpha_3+\alpha_5+\bar{q}'+\alpha+\alpha_4)$. The first condition can remove at most $(p+\bar{\alpha}_1+\bar{\alpha}_2+\alpha_4+\alpha_6+\bar{q}'+\alpha+\alpha_3)\cdot|\bar{X}^2_{v_{6,k}}|$ values for each k, and the second condition can exclude at most $(|\bar{X}^2_{v_{6,1}}|+\ldots+|\bar{X}^2_{v_{6,k-1}}|)\cdot|\bar{X}^2_{v_{6,k}}| \le \alpha_5\cdot|\bar{X}^2_{v_{6,k}}|$ items for each choice of $u_{6,k}$. By the choice of $(u_{6,k})_{k\in[\alpha_6]}$, we obtain that

$$\mathcal{N}_2(\alpha) \ge \prod_{k=0}^{\alpha_6-1}\left(2^n-\Delta_3-k-(\Delta_4+\alpha_5)\cdot|\bar{X}^2_{v_{6,k}}|\right). \tag{36}$$

Let $U_6 = P^{-1}(V_6) \overset{def}{=} \{u_{6,1},\ldots,u_{6,\alpha_6}\}$, and $V_5 = P(U_5) \overset{def}{=} \{u_{6,k}\oplus f_1(t)\oplus f_2(t)\oplus y : k\in[\alpha_6],(t,x,y)\in X^2_{v_{6,k}}\}$. It holds that items in $P^{-1}(V_6)$ are distinct. Furthermore, $P^{-1}(V_6)$ is disjoint with U^{4+} by the choice of $(u_{6,1},\ldots,u_{6,\alpha_6})$. Let $U^{5+} = U^{4+}\cup U_6$, and $V^{5+} = V^{4+}\cup V_5$. The size of U^{5+} is $\Delta_5 = \Delta_3+\alpha_6$, and the size of V^{5+} is $\Delta_6 = \Delta_4+\alpha_5$.

Step III. Construct $\mathbf{V_{7,2}} = \mathbf{P(U_{7,2})}$, and $\mathbf{U_{8,2}} = \mathbf{P^{-1}(V_{8,2})}$.

Let $\bar{q}'' = \bar{q}'-2\alpha$ ($\bar{q}'' = |U_{7,2}| = |V_{8,2}|$). Let m be the number of all distinct tweaks appearing in $\bar{\mathcal{Q}}_F$, and then we use $\bar{t}_1,\ldots,\bar{t}_m$ to denote these m distinct tweaks. We denote $\widetilde{\mathcal{Q}_{0,i}} = \{(\bar{t}_i,x,y)\in\bar{\mathcal{Q}}_0 : x\oplus f_1(\bar{t}_i)\in U_{7,2}\wedge x\oplus f_2(\bar{t}_i)\in V_{8,2}\}$ and $\bar{q}''_i = |\widetilde{\mathcal{Q}_{0,i}}|$. In this case, it holds that $\bar{q}'' = \sum_{i=1}^m \bar{q}''_i$. For convenience to count, we denote $\widetilde{\mathcal{Q}_0} = \bigcup_{i=1}^m \widetilde{\mathcal{Q}_{0,i}}$ and rewrite the items in $\widetilde{\mathcal{Q}_0}$ indexed by the m distinct tweaks as

$$\widetilde{\mathcal{Q}_0} = \{(\bar{t}_1,x_{1,1},y_{1,1}),\ldots,(\bar{t}_1,x_{1,\bar{q}''_1},y_{1,\bar{q}''_1}),\ldots,(\bar{t}_m,x_{m,1},y_{m,1}),\ldots,(\bar{t}_m,x_{m,\bar{q}''_m},y_{m,\bar{q}''_m})\}.$$

For $i=1,\ldots,m$ and $j=1,\ldots,\bar{q}''_i$, denote

$$u_{7,i,j} = x_{i,j}\oplus f_1(\bar{t}_i) \text{ and } v_{8,i,j} = x_{i,j}\oplus f_2(\bar{t}_i).$$

For convenience, $U_{7,2}$ and $V_{8,2}$ can be written as $U_{7,2} = \{u_{7,i,j}\}_{1\le i\le m,1\le j\le\bar{q}''_i}$ and $V_{8,2} = \{v_{8,i,j}\}_{1\le i\le m,1\le j\le\bar{q}''_i}$, respectively. Let $(v_{7,i,j})_{1\le i\le m,1\le j\le\bar{q}''_i}$ be all possible different tuples in $\{0,1\}^n\setminus V^{5+}$ such that the following two conditions are satisfied.

(i) For each $i=1,\ldots,m$ and $j=1,\ldots,\bar{q}''_i$, $v_{7,i,j}\oplus f_1(\bar{t}_i)\oplus f_2(\bar{t}_i)\oplus y_{i,j}\notin U^{5+}$.

(ii) For each $i=1,\ldots,m$ and $j=1,\ldots,\bar{q}''_i$, $v_{7,i,j}\oplus f_1(\bar{t}_i)\oplus f_2(\bar{t}_i)\oplus y_{i,j}$ is distinct from the values $v_{7,k,l}\oplus f_1(\bar{t}_k)\oplus f_2(\bar{t}_k)\oplus y_{k,l}$ for $k<i$ and $l\in[\bar{q}''_k]$. Furthermore, $v_{7,i,j}\oplus f_1(\bar{t}_i)\oplus f_2(\bar{t}_i)\oplus y_{i,j}$ should be distinct from the values $v_{7,i,j'}\oplus f_1(\bar{t}_i)\oplus f_2(\bar{t}_i)\oplus y_{i,j'}$ for $j'\in[\bar{q}''_i]$ with $j'<j$.

Except these two conditions, each $v_{7,i,j}$ must be different from each other. By a simple computation, one has $|V^{5+}| = |U^{5+}| = p'+\bar{q}'+\alpha$, where $p' = p+\bar{\alpha}_1+\bar{\alpha}_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6$ and $\bar{q}' = q-(\bar{\alpha}_1+\bar{\alpha}_2+\alpha_4+\alpha_5)$. So $|\{0,1\}^n\setminus V^{5+}| = 2^n-(p'+\bar{q}'+\alpha)$. Now we bound the number of all possible distinct tuples $(v_{7,i,j})_{1\le i\le m,1\le j\le\bar{q}''_i}$ satisfying these two conditions. The first condition excludes at most $p'+\bar{q}'+\alpha$ values, and the second condition excludes at most $\sum_{k=1}^{i-1}\bar{q}''_k-j+1$ values for each choice of $v_{7,i,j}$. Furthermore, $v_{7,i,j}$ should not be same as any one of previous $\sum_{k=1}^{i-1}\bar{q}''_k-j+1$ items. By combining these facts, one can conclude that

$$\mathcal{N}_0(\alpha) \ge \prod_{i=1}^{m}\prod_{j=0}^{\bar{q}''_i-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}''_k-2j). \tag{37}$$

Overall, by combining (33), (35), (36), and (37), one has

$$\mathsf{p}''(\bar{\tau}) = \sum_{0\le\alpha\le M}\frac{\mathcal{N}_S(\alpha)\cdot\mathcal{N}_1(\alpha)\cdot\mathcal{N}_2(\alpha)\cdot\mathcal{N}_0(\alpha)}{(2^n-p-\bar{\alpha}_1-\bar{\alpha}_2)_{\alpha_3+\alpha_4+\alpha_5+\alpha_6+2\bar{q}''+3\alpha}}. \tag{38}$$

By combining (32) and (38), we have

$$\mathsf{p}(\bar{\tau}) = \sum_{0\le\alpha\le M}\frac{N_S(\alpha)\cdot\mathcal{N}_1(\alpha)\cdot\mathcal{N}_2(\alpha)\cdot\mathcal{N}_0(\alpha)}{(2^n-p)_{\bar{\alpha}_1+\bar{\alpha}_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6+2\bar{q}''+3\alpha}}. \tag{39}$$

Recall that

$$\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} = 2^{nq}\mathsf{p}(\bar{\tau}). \tag{40}$$

By combining (39) and (40), we conclude that

$$\begin{aligned}\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} &\geq \sum_{0\leq\alpha\leq M} \frac{2^{nq}\cdot\mathcal{N}_S(\alpha)\cdot\mathcal{N}_1(\alpha)\cdot\mathcal{N}_2(\alpha)\cdot\mathcal{N}_0(\alpha)}{(2^n-p)_{\bar{\alpha}_1+\bar{\alpha}_2+\alpha_3+\alpha_4+\alpha_5+\alpha_6+2q''+3\alpha}} \\ &= \sum_{0\leq\alpha\leq M} \underbrace{\frac{\mathcal{N}_1(\alpha)}{(2^n-p)_{\alpha_3}}}_{R_1(\alpha)} \cdot \underbrace{\frac{\mathcal{N}_2(\alpha)}{(2^n-p-\alpha_3)_{\alpha_6}}}_{R_2(\alpha)} \\ &\quad \cdot \underbrace{\frac{2^{n(q-\bar{q}')}}{(2^n-p-\alpha_3-\alpha_6)_{\bar{\alpha}_1+\bar{\alpha}_2+\alpha_4+\alpha_5}}}_{\geq 1\,(*)} \\ &\quad \cdot \underbrace{\frac{2^{n\bar{q}'}\cdot\mathcal{N}_S(\alpha)\cdot\mathcal{N}_0(\alpha)}{(2^n-p-\bar{\alpha}_1-\bar{\alpha}_2-\alpha_3-\alpha_4-\alpha_5-\alpha_6)_{2\bar{q}''+3\alpha}}}_{R_0(\alpha)},\end{aligned} \tag{41}$$

where $(*)$ follows as $q-\bar{q}' = \bar{\alpha}_1+\bar{\alpha}_2+\alpha_4+\alpha_5$.

Lower bounds on $R_1(\alpha)$, $R_2(\alpha)$, and $R_0(\alpha)$ are given in Appendix D, and the results are showed as follows:

$$R_1(\alpha) \geq 1-\epsilon_1, \text{ where } \epsilon_1 = \frac{8q^{3/2}}{2^n} + \frac{2p\sqrt{q}}{2^n} + \frac{4q}{2^n}. \tag{42}$$

$$R_2(\alpha) \geq 1-\epsilon_2, \text{ where } \epsilon_2 = \frac{8q^{3/2}}{2^n} + \frac{2p\sqrt{q}}{2^n} + \frac{4q}{2^n}. \tag{43}$$

$$R_0(\alpha) \geq (1-\epsilon_0)\cdot(1-\epsilon_3)\cdot(1-\epsilon_4)\cdot\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha), \tag{44}$$

where $\epsilon_0 = \frac{6q}{2^{2n/3}} + \frac{16\sqrt{q}}{2^{n/3}}$, $\epsilon_3 = \frac{4q}{2^{2n/3}}$, and $\epsilon_4 = \frac{4q(p+2q+6\sqrt{q})^2}{2^{2n}}$.

Putting (42), (43), and (44) into (41), we obtain

$$\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} \geq (1-\epsilon_0)(1-\epsilon_1)(1-\epsilon_2)(1-\epsilon_3)(1-\epsilon_4)\sum_{0\leq\alpha\leq M}\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha). \tag{45}$$

The last term in (45) can be bounded as

$$\begin{aligned}\sum_{0\leq\alpha\leq M}\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha) &= 1 - \sum_{\alpha>\bar{q}'/2^{n/3}}\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha) \\ &\overset{(v)}{\geq} \left(1 - \frac{\mathbb{E}[\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha)]}{\bar{q}'/2^{n/3}}\right) \\ &= \left(1 - \frac{(\bar{q}')^2}{(2^n-p')\bar{q}'/2^{n/3}}\right) \\ &= \left(1 - \frac{\bar{q}'\cdot 2^{\frac{n}{3}}}{2^n-p'}\right) \\ &\overset{(vi)}{\geq} \left(1 - \frac{2q}{2^{2n/3}}\right),\end{aligned} \tag{46}$$

where (v) follows as Markov's inequality and (vi) follows as $2^n - p' \geq 2^n - p - 6\sqrt{q} \geq 2^{n-1}$ which comes from the assumption $p + 6\sqrt{q} \leq p + 6\sqrt{q} + 2q \leq 2^{n-1}$ and the fact $\bar{q}' \leq q$. Let $\epsilon_5 = \frac{2q}{2^{2n/3}}$. Then we can write (45) as

$$\begin{aligned}\frac{\Pr[T_{\mathsf{re}} = \bar{\tau}]}{\Pr[T_{\mathsf{id}} = \bar{\tau}]} &\geq (1-\epsilon_0)(1-\epsilon_1)(1-\epsilon_2)(1-\epsilon_3)(1-\epsilon_4)(1-\epsilon_5) \\ &\geq (1-\epsilon_0-\epsilon_1-\epsilon_2-\epsilon_3-\epsilon_4-\epsilon_5).\end{aligned} \tag{47}$$

Combing all these facts together, the proof of Lemma 6 is finished. □

Finally, by Lemmas 1, 5 and 6, Theorem 2 follows. □

5. Conclusions

In this paper, we first prove the BBB security of the construction SoEM22 in the multi-key setting, and further tweak this construction. When the bidirectionally efficient public random permutations are considered, we build the parallelizable beyond-birthday secure PRFs from one permutation in the multi-key setting, and also tweak this new construction while preserving BBB security. By a slight modification of two tweakable PRFs, we obtain two parallelizable nonce based MACs for variable length messages. In fact, the constructions mentioned above come from sum of two Even-Mansours. It is natural to generalize SoEM22 to sum of s Even-Mansours, namely

$$F^{P_1,\ldots,P_s}_{K_1,\ldots,K_s}(x) = P_1(x \oplus K_1) \oplus K_1 \oplus \cdots \oplus P_s(x \oplus K_s) \oplus K_s,$$

where $P_1, \ldots, P_s \xleftarrow{\$} \mathsf{Perm}(n)$ are s independent random permutations, and $K_1, \ldots, K_s$ are s n-bit uniformly random strings. Obliviously, this generalization is at least as secure as SoEM22 even in the multi-key setting. However, the detailed analysis of its security is not easy to see, and we leave it as a future work.

Author Contributions: Writing—original draft, J.N.; Writing—review & editing, P.Z. and H.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the National Natural Science Foundation of China (Nos. 61632013 and 61972370), and by Fundamental Research Funds for Central Universities in China (No. WK3480000007).

Informed Consent Statement: Informed consent was obtained from all authors included in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Upper Bound on $\mathbf{Pr}[T_{\mathsf{id}} \in \Gamma_{\mathbf{bad}}]$ in Lemma 3

For each $i \in [13]$, we upper bound $\Pr[T_{\mathsf{id}} \in \Gamma_i]$ as follows.

Bounding (B-1), (B-2), and **(B-3)**: First, we consider (B-1). For any $(t_i, x_i, y_i) \in \mathcal{Q}_F$, $u_{1,j} \in U_1$, and $u_{2,j'} \in U_2$, by the ϵ_1-regular property of (f_1, f_2), one has

$$\Pr[(f_1(t_i) = x_i \oplus u_{1,j}) \wedge (f_2(t_i) = x_i \oplus u_{2,j'})] \le \epsilon_1^2.$$

Since the number of all possible tuples for $((t_i, x_i, y_i), u_{1,j}, u_{2,j'})_{i\in[q],j\in[p_1],j'\in[p_2]}$ is qp_1p_2, by union bound, it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma_1] \le qp_1p_2\epsilon_1^2.$$

Similarly, we can bound the probabilities of (B-2) and (B-3) as

$$\Pr[T_{\mathsf{id}} \in \Gamma_2] \le qp_1p_2\epsilon_1^2 \text{ and } \Pr[T_{\mathsf{id}} \in \Gamma_3] \le qp_1p_2\epsilon_1^2.$$

Bounding (B-4) and **(B-5)**: For any two distinct queries $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$, by the ϵ_2-AXU property of pair (f_1, f_2), we have

$$\Pr[(f_1(t_i) \oplus f_1(t_{i'}) = x_i \oplus x_{i'}) \wedge (f_2(t_i) \oplus f_2(t_{i'}) = f_1(t_i) \oplus f_1(t_{i'}) \oplus y_i \oplus y_{i'})] \le \epsilon_2^2.$$

Since there are $q(q-1)/2$ possible unordered pairs for $\{(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'})\}_{i\neq i'\in[q]}$, by union bound, one can obtain that

$$\Pr[T_{\mathsf{id}} \in \Gamma_4] \le \frac{\epsilon_2^2 q^2}{2}, \text{ and similarly, } \Pr[T_{\mathsf{id}} \in \Gamma_5] \le \frac{\epsilon_2^2 q^2}{2}.$$

Bounding (B-6) and **(B-7)**: For any two distinct construction queries $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ and any $u_{1,j} \in U_1$, by the ϵ_1-regular and ϵ_2-AXU properties of (f_1, f_2), we have

$$\Pr[(f_1(t_i) = x_i \oplus u_{1,j}) \wedge (f_2(t_i) \oplus f_2(t_{i'}) = x_i \oplus x_{i'})] \leq \epsilon_1\epsilon_2.$$

Then, summing over all $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ and $u_{1,j} \in U_1$, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_6] \leq \frac{\epsilon_1\epsilon_2 q^2 p_1}{2}, \text{ and similarly, } \Pr[T_{\mathsf{id}} \in \Gamma_7] \leq \frac{\epsilon_1\epsilon_2 q^2 p_2}{2}.$$

Bounding (B-8): For any $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (t_{i''}, x_{i''}, y_{i''}) \in \mathcal{Q}_F$ with $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'})$ and $(t_i, x_i, y_i) \neq (t_{i''}, x_{i''}, y_{i''})$, by the ϵ_2-AXU property of (f_1, f_2), one concludes that

$$\Pr[(f_1(t_i) \oplus f_1(t_{i'}) = x_i \oplus x_{i'}) \wedge (f_2(t_i) \oplus f_2(t_{i''}) = x_i \oplus x_{i''})] \leq \epsilon_2^2.$$

Note that the above inequality also holds for the case $t_i = t_{i'}$ (resp. $t_i = t_{i''}$) since we have $x_i \neq x_{i'}$ (resp. $x_i \neq x_{i''}$) i.e. $x_i \oplus x_{i'} = 0$ (resp. $x_i \oplus x_{i''} = 0$). It is easy to count that the number of all possible $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (t_{i''}, x_{i''}, y_{i''})$ is at most q^3, which means that

$$\Pr[T_{\mathsf{id}} \in \Gamma_8] \leq \epsilon_2^2 q^3.$$

Bounding (B-9), **(B-10)**, **(B-11)**, and **(B-12)**: We deal with bad conditions (B-9) and (B-11) together by using the fact that

$$\Pr[T_{\mathsf{id}} \in \Gamma_9 \cup \Gamma_{11}] \leq \Pr[T_{\mathsf{id}} \in \Gamma_{11}] + \Pr[T_{\mathsf{id}} \in \Gamma_9 \setminus \Gamma_{11}].$$

We first consider how to upper bound $\Pr[T_{\mathsf{id}} \in \Gamma_{11}]$. For the random variable $\alpha_1 = |\{(t, x, y) \in \mathcal{Q}_F : x \oplus f_1(t) \in U_1\}|$ (the randomness from the choice of f_1), its expectation value can be computed as

$$\mathbb{E}[\alpha_1] \leq \sum_{(t,x,y)\in\mathcal{Q}_F:} \sum_{u_1\in U_1:} \Pr[x \oplus f_1(t) = u_1] \leq \epsilon_1 q p_1,$$

due to the ϵ_1-regular property of (f_1, f_2). By Markov's inequality, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_{11}] \leq \frac{\mathbb{E}[\alpha_1]}{\sqrt{q}} \leq \epsilon_1\sqrt{q}p_1.$$

Under the condition $\alpha_1 \leq \sqrt{q}$, there are at most $q/2$ pairs $\{((t_i, x_i, y_i), u_{1,j}), ((t_{i'}, x_{i'}, y_{i'}), u_{1,j'})\}$ such that $x_i \oplus f_1(t_i) = u_{1,j}$ and $x_{i'} \oplus f_1(t_{i'}) = u_{1,j'}$ where $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \mathcal{Q}_F$ and $(u_{1,j}, v_{1,j}), (u_{1,j'}, v_{1,j'}) \in \mathcal{Q}_{P_1}$. In this case, the corresponding y_i and $y_{i'}$ are two independently uniform random variables over $\{0,1\}^n$ so that we have

$$\Pr[v_{1,j} \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{1,j'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}] \leq \frac{1}{2^n}.$$

By summing over all the $q/2$ possible pairs, one can obtain that

$$\Pr[T_{\mathsf{id}} \in \Gamma_9 \setminus \Gamma_{11}] \leq \frac{q}{2^{n+1}}.$$

Finally, it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma_9 \cup \Gamma_{11}] \leq \epsilon_1\sqrt{q}p_1 + \frac{q}{2^{n+1}}.$$

Similarly, we obtain

$$\Pr[T_{\mathsf{id}} \in \Gamma_{10} \cup \Gamma_{12}] \leq \epsilon_1\sqrt{q}p_2 + \frac{q}{2^{n+1}}.$$

Bounding (B-13) : To bound $\Pr[\beta_1 \geq \sqrt{q}]$, we first define the random variable $T_F = |\{((t, x, y), (t', x', y')) \in \mathcal{Q}_F \times \mathcal{Q}_F : (t, x, y) \neq (t', x', y'), x \oplus f_1(t) = x' \oplus f_1(t')\}|$. By definition of β_1, one has

$$\beta_1 = |\{(t, x, y) \in \mathcal{Q}_F : \exists (t, x, y) \neq (t', x', y'), x \oplus f_1(t) = x' \oplus f_1(t')\}| \leq T_F.$$

Hence, $\mathbb{E}[\beta_1] \leq \mathbb{E}[T_F]$. We can compute the expectation value of T_F as

$$\mathbb{E}[T_F] = \sum_{(t,x,y)\neq(t',x',y'):} \Pr[x \oplus f_1(t) = x' \oplus f_1(t')] \leq \frac{\epsilon_2 q^2}{2}$$

from the ϵ_2-AXU property of (f_1, f_2). By Markov's inequality, one has

$$\Pr[\beta_1 \geq \sqrt{q}] \leq \frac{\mathbb{E}[\beta_1]}{\sqrt{q}} \leq \frac{\mathbb{E}[T_F]}{\sqrt{q}} \leq \frac{\epsilon_2 q^{3/2}}{2}, \text{ and similarly, } \Pr[\beta_2 \geq \sqrt{q}] \leq \frac{\epsilon_2 q^{3/2}}{2}.$$

Finally, we obtain

$$\Pr[T_{\mathsf{id}} \in \Gamma_{13}] = \Pr[(\beta_1 \geq \sqrt{q}) \vee (\beta_2 \geq \sqrt{q})] \leq \epsilon_2 q^{3/2}.$$

Appendix B. More Details in Proof of Lemma 4

Lower Bounding $\mathsf{p}'(\tau)$. Conditioned on $P_1 \vdash \mathcal{Q}_{P_1}$ and $P_2 \vdash \mathcal{Q}_{P_2}$, P_1 (resp. P_2) is fixed on exactly p_1 (resp. p_2) input-output pairs. For each $(t, x, y) \in \mathcal{Q}_{U_1}$, there exists a unique $(u_1, v_1) \in \mathcal{Q}_{P_1}$ satisfying $x \oplus f_1(t) = u_1$ so that $P_1(x \oplus f_1(t)) = P_1(u_1) = v_1$. Then we can define two corresponding multi-sets as:

$$\widetilde{U}_2 = \{x \oplus f_2(t) : (t, x, y) \in \mathcal{Q}_{U_1}\},$$
$$\widetilde{V}_2 = \{P_1(x \oplus f_1(t)) \oplus f_1(t) \oplus f_2(t) \oplus y : (t, x, y) \in \mathcal{Q}_{U_1}\}.$$

Note that all values in $\widetilde{U}_2$ (resp. $\widetilde{V}_2$) are distinct since otherwise τ would satisfy (B-6) (resp. (B-9)). Then it holds that $|\widetilde{U}_2| = |\widetilde{V}_2| = |\mathcal{Q}_{U_1}| = \alpha_1$. Moreover, since $\tau \notin \Gamma_1$ and $\tau \notin \Gamma_2$, one conclude that $U_2 \cap \widetilde{U}_2 = \emptyset$ and $V_2 \cap \widetilde{V}_2 = \emptyset$, respectively. Then we get

$$\Pr[E_{U_1} \mid P_2 \vdash \mathcal{Q}_{P_2}] = \frac{1}{(2^n - p_2)_{\alpha_1}}. \tag{A1}$$

Similarly, for each $(t, x, y) \in \mathcal{Q}_{U_2}$, there exists a unique $(u_2, v_2) \in \mathcal{Q}_{P_2}$ satisfying $x \oplus f_2(t) = u_2$, which means $P_2(x \oplus f_2(t)) = v_2$. Then two corresponding multi-sets can be defined as:

$$\widetilde{U}_1 = \{x \oplus f_1(t) : (t, x, y) \in \mathcal{Q}_{U_2}\},$$
$$\widetilde{V}_1 = \{P_2(x \oplus f_2(t)) \oplus f_1(t) \oplus f_2(t) \oplus y : (t, x, y) \in \mathcal{Q}_{U_2}\}.$$

All values in $\widetilde{U}_1$ (resp. $\widetilde{V}_1$) are distinct since otherwise τ would satisfy (B-7) (resp. (B-10)). Then one has $|\widetilde{U}_1| = |\widetilde{V}_1| = |\mathcal{Q}_{U_2}| = \alpha_2$. Moreover, since $\tau \notin \Gamma_1$ and $\tau \notin \Gamma_3$, it holds that $U_1 \cap \widetilde{U}_1 = \emptyset$ and $V_1 \cap \widetilde{V}_1 = \emptyset$, respectively. Hence,

$$\Pr[E_{U_2} \mid P_1 \vdash \mathcal{Q}_{P_1}] = \frac{1}{(2^n - p_1)_{\alpha_2}}. \tag{A2}$$

By combing (A1) and (A2), one can conclude that

$$\mathsf{p}'(\tau) = \frac{1}{(2^n - p_2)_{\alpha_1}(2^n - p_1)_{\alpha_2}}. \tag{A3}$$

Now it holds that $|\widetilde{U}_1| = |\widetilde{V}_1| = \alpha_2$ and $|\widetilde{U}_2| = |\widetilde{V}_2| = \alpha_1$. Then we define four disjoint collections $\mathcal{U}_1 \stackrel{\mathsf{def}}{=} (U_1, \widetilde{U}_1)$, $\mathcal{V}_1 \stackrel{\mathsf{def}}{=} (V_1, \widetilde{V}_1)$, $\mathcal{U}_2 \stackrel{\mathsf{def}}{=} (U_2, \widetilde{U}_2)$, and $\mathcal{V}_2 \stackrel{\mathsf{def}}{=} (V_2, \widetilde{V}_2)$. Notice that when conditioned on $E_{U_1} \wedge E_{U_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1, 2)$, P_1 is fixed on exactly $p_1 + \alpha_2$ input-output pairs and P_2 is fixed on exactly $p_2 + \alpha_1$ input-output pairs.

Lower Bounding $\mathsf{p}''(\tau)$. Conditioned on $E_{U_1} \wedge E_{U_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1, 2)$ we next lower bound the number of all possible "new" and distinct input-output pairs of P_1 and P_2 such that the event $E_{X_1} \wedge E_{X_2} \wedge E_0$ happens. We first define four multi-sets derived from $\mathcal{Q}_{X_1}$ and $\mathcal{Q}_{X_2}$ as:

$$U_{1,1} = \{x \oplus f_1(t) : (t, x, y) \in \mathcal{Q}_{X_1}\}, \quad U_{2,1} = \{x \oplus f_1(t) : (t, x, y) \in \mathcal{Q}_{X_2}\},$$
$$U_{1,2} = \{x \oplus f_2(t) : (t, x, y) \in \mathcal{Q}_{X_1}\}, \quad U_{2,2} = \{x \oplus f_2(t) : (t, x, y) \in \mathcal{Q}_{X_2}\}.$$

The size of four sets above can be denoted as $\alpha_{1,1} = |U_{1,1}|$, $\alpha_{1,2} = |U_{1,2}|$, $\alpha_{2,1} = |U_{2,1}|$, and $\alpha_{2,2} = |U_{2,2}|$. We also denote four additional sets as $V_{1,1} = P(U_{1,1})$, $V_{1,2} = P(U_{1,2})$, $V_{2,1} = P(U_{2,1})$, and $V_{2,2} = P(U_{2,2})$, which can be wrote more clearly as:

$$V_{1,1} = \{P(x \oplus f_1(t)) : (t, x, y) \in \mathcal{Q}_{X_1}\}, \quad V_{2,1} = \{P(x \oplus f_1(t)) : (t, x, y) \in \mathcal{Q}_{X_2}\},$$
$$V_{1,2} = \{P(x \oplus f_2(t)) : (t, x, y) \in \mathcal{Q}_{X_1}\}, \quad V_{2,2} = \{P(x \oplus f_2(t)) : (t, x, y) \in \mathcal{Q}_{X_2}\}.$$

For convenience, we rewrite $U_{1,1}$ and $U_{2,2}$ as:

$$U_{1,1} = \{u_{1,1}, \ldots, u_{1,\alpha_{1,1}}\},\ U_{2,2} = \{u_{2,1}, \ldots, u_{2,\alpha_{2,2}}\}.$$

Recall that $D_1 = \{x \oplus f_1(t) : (t,x,y) \in \mathcal{Q}_F\}$ and $D_2 = \{x \oplus f_2(t) : (t,x,y) \in \mathcal{Q}_F\}$. Then $\alpha_{1,1}$ and $\alpha_{1,2}$ can be bounded as:

$$\alpha_{1,1} \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{D_1}(x)>1}} 1 \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{D_1}(x)>1}} \frac{\delta_{D_1}(x)}{2} = \frac{\beta_1}{2} \leq \frac{\sqrt{q}}{2},$$

$$\alpha_{1,2} \leq \sum_{i=1}^{\alpha_{1,1}} \delta_{D_1}(u_{1,i}) \leq \sum_{\substack{x\in\{0,1\}^n:\\ \delta_{D_1}(x)>1}} \delta_{D_1}(x) = \beta_1 \leq \sqrt{q}.$$

Similarly, we obtain $\alpha_{2,2} \leq \frac{\sqrt{q}}{2}$ and $\alpha_{2,1} \leq \sqrt{q}$. From the fact $\tau \notin \Gamma_8$, one has that any items in the $U_{1,2}$ (resp.$U_{2,1}$) are distinct so that $\alpha_{1,2} = |\mathcal{Q}_{X_1}|$ (resp. $\alpha_{2,1} = |\mathcal{Q}_{X_2}|$) holds. Finally, we define two multi-sets derived from $\mathcal{Q}_0$ as

$$U_0^1 = \{x \oplus f_1(t) : (t,x,y) \in \mathcal{Q}_0\} \text{ and } U_0^2 = \{x \oplus f_2(t) : (t,x,y) \in \mathcal{Q}_0\}.$$

Due to the definition of $\mathcal{Q}_0$, it holds that any items in U_0^1 (resp. U_0^2) are distinct. We can also denote two additional sets as

$$V_0^1 = P(U_0^1) = \{P(x \oplus f_1(t)) : (t,x,y) \in \mathcal{Q}_0\},$$
$$V_0^2 = P(U_0^2) = \{P(x \oplus f_2(t)) : (t,x,y) \in \mathcal{Q}_0\}.$$

Let $q' \stackrel{\text{def}}{=} |\mathcal{Q}_0| = q - (|\mathcal{Q}_U| + |\mathcal{Q}_V| + |\mathcal{Q}_{X_1}| + |\mathcal{Q}_{X_2}|) = q - (\alpha_1 + \alpha_2 + \alpha_{1,2} + \alpha_{2,1})$ (besides, $q' = |U_0^1| = |U_0^2|$). Let m be the number of all distinct tweaks appearing in $\mathcal{Q}_F$, and then we use $\hat{t}_1, \ldots, \hat{t}_m$ to denote these m distinct tweaks. Furthermore, write $\mathcal{Q}_{0,i}$ as a set consisting of all the query-response tuples indexed by the tweak $\hat{t}_i$ in $\mathcal{Q}_0$ and denote $q_i' = |\mathcal{Q}_{0,i}|$ (q_i' might be zero for some i). Then it holds that $\mathcal{Q}_0 = \bigcup_{i=1}^m \mathcal{Q}_{0,i}$ and respectively $q' = \sum_{i=1}^m q_i'$. For convenience to count, we rearrange the items in $\mathcal{Q}_0$ as

$$\mathcal{Q}_0 = \{(\hat{t}_1, x_{1,1}, y_{1,1}), \ldots, (\hat{t}_1, x_{1,q_1'}, y_{1,q_1'}), \ldots, (\hat{t}_m, x_{m,1}, y_{m,1}), \ldots, (\hat{t}_m, x_{m,q_m'}, y_{m,q_m'})\}.$$

For $i = 1, \ldots, m$ and $j = 1, \ldots, q_i'$, we denote

$$\hat{u}_{1,i,j} = x_{i,j} \oplus f_1(\hat{t}_i) \text{ and } \hat{u}_{2,i,j} = x_{i,j} \oplus f_2(\hat{t}_i).$$

For convenience to describe, we rewrite the sets U_0^1 and U_0^2 as

$$U_0^1 = \{\hat{u}_{1,i,j} : 1 \leq i \leq m, 1 \leq j \leq q_i'\} \text{ and } U_0^2 = \{\hat{u}_{2,i,j} : 1 \leq i \leq m, 1 \leq j \leq q_i'\}.$$

Let $\mathcal{U}_1^+ = (U_{1,1}, U_{2,1}, U_0^1)$ and $\mathcal{U}_2^+ = (U_{2,2}, U_{1,2}, U_0^2)$. Then the following proposition holds.

Proposition A1. *With notations as above, we have*

(i) All sets in $\mathcal{U}_1^+$ (resp. $\mathcal{U}_2^+$) are disjoint, i.e. $U_{1,1} \cap U_{2,1} = \emptyset$, $U_{1,1} \cap U_0^1 = \emptyset$, and $U_{2,1} \cap U_0^1 = \emptyset$ (resp. $U_{2,2} \cap U_{1,2} = \emptyset$, $U_{2,2} \cap U_0^2 = \emptyset$, and $U_{1,2} \cap U_0^2 = \emptyset$).

(ii) $\mathcal{U}_1^+$ is inner disjoint with $\mathcal{U}_1$ and $\mathcal{U}_2^+$ is inner disjoint with $\mathcal{U}_2$.

Proof. We first prove (i). From the fact $\tau \notin \Gamma_8$, one can conclude that $U_{1,1} \cap U_{2,1} = \emptyset$. By definition of $\mathcal{Q}_{X_1}$ and $\mathcal{Q}_0$, $U_{1,1} \cap U_0^1 = \emptyset$ holds. By combining the fact $\tau \notin \Gamma_8$ and the disjoint property of $\mathcal{Q}_{X_2}$ and $\mathcal{Q}_0$, one has $U_{2,1} \cap U_0^1 = \emptyset$. We can conclude that $U_{2,2} \cap U_{1,2} = \emptyset$, $U_{2,2} \cap U_0^2 = \emptyset$, and $U_{1,2} \cap U_0^2 = \emptyset$ in a similar way.

Next we prove (ii) by enumerating all possible cases. For $U_{1,1}$, the definition of $\mathcal{Q}_{X_1}$ means that $U_{1,1} \cap U_1 = \emptyset$; $U_{1,1} \cap \widetilde{U}_1 = \emptyset$ comes from the fact $\tau \notin \Gamma_7$. For $U_{2,1}$, $U_{2,1} \cap U_1 = \emptyset$ holds due to the fact $\tau \notin \Gamma_6$; $U_{2,1} \cap \widetilde{U}_1 = \emptyset$ can be obtained from the fact

$\tau \notin \Gamma_8$ and the disjoint property between $\mathcal{Q}_{X_2}$ and $\mathcal{Q}_{U_2}$. For U_0^1, the definition of $\mathcal{Q}_0$ means $U_0^1 \cap U_1 = \emptyset$; $U_0^1 \cap \widetilde{U}_1 = \emptyset$ holds for the reason that $\tau \notin \Gamma_7$ and $\mathcal{Q}_0$ is disjoint with $\mathcal{Q}_{U_2}$.

For $U_{2,2}$, the definition of $\mathcal{Q}_{X_2}$ means that $U_{2,2} \cap U_2 = \emptyset$; $U_{2,2} \cap \widetilde{U}_2 = \emptyset$ comes from the fact $\tau \notin \Gamma_6$. For $U_{1,2}$, one has $U_{1,2} \cap U_2 = \emptyset$ since $\tau \notin \Gamma_7$; $U_{1,2} \cap \widetilde{U}_2 = \emptyset$ holds due to the fact $\tau \notin \Gamma_8$ and the disjoint property between $\mathcal{Q}_{X_1}$ and $\mathcal{Q}_{U_1}$. For U_0^2, one has $U_0^2 \cap U_2 = \emptyset$ by the definition of $\mathcal{Q}_0$; $U_0^2 \cap \widetilde{U}_2 = \emptyset$ holds for the reason that $\tau \notin \Gamma_6$ and $\mathcal{Q}_0$ is disjoint with $\mathcal{Q}_{U_1}$. □

Until now P is fixed on p_1 input-output pairs from U_1 to V_1, α_2 input-output pairs from $\widetilde{U}_1$ from $\widetilde{V}_1$, p_2 input-output pairs from U_2 to V_2, and α_1 input-output pairs from $\widetilde{U}_2$ to $\widetilde{V}_2$. Based on these facts, the next work is to choose other possible compatible items for $V_{1,1} = P_1(U_{1,1})$, $V_{2,1} = P_1(U_{2,1})$, $V_0^1 = P_1(U_0^1)$, $V_{1,2} = P_2(U_{1,2})$, $V_{2,2} = P_2(U_{2,2})$, and $V_0^2 = P_2(U_0^2)$ to extend the fixed input-output pairs of permutations P_1 and P_2, respectively.

Note that once the items in $V_{1,1} = P_1(U_{1,1})$ are fixed, then the corresponding items in $V_{1,2} = P_2(U_{1,2})$ are uniquely determined since these two sets are both derived from $\mathcal{Q}_{X_1}$. Similarly, the choices for items in $V_{2,2} = P_2(U_{2,2})$ (resp. $V_0^1 = P_1(U_0^1)$) uniquely determine the items in $V_{2,1} = P_1(U_{2,1})$ (resp. $V_0^2 = P_2(U_0^2)$). Then we sample all possible items for these sets through three steps.

Step I. **Construct $\mathbf{V_{1,1} = P_1(U_{1,1})}$ and $\mathbf{V_{1,2} = P_2(U_{1,2})}$** .

Recall that $X_u^1 = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_1(t) = u\}$ and $U_{1,1} = \{u_{1,1}, \ldots, u_{1,\alpha_{1,1}}\}$. Let N_{X_1} be the number of $\alpha_{1,1}$-wise tuples of distinct values $(v_{1,1}, \ldots, v_{1,\alpha_{1,1}})$ in $\{0,1\}^n \setminus V_1 \cup \widetilde{V}_1$ satisfying the following two conditions:

(i) For each $i \in [\alpha_{1,1}]$ and each $(t,x,y) \in X^1_{u_{1,i}}$, $v_{1,i} \oplus f_1(t) \oplus f_2(t) \oplus y \notin V_2 \cup \widetilde{V}_2$.

(ii) For each $i \in [\alpha_{1,1}]$ and $(t,x,y) \in X^1_{u_{1,i}}$, $v_{1,i} \oplus f_1(t) \oplus f_2(t) \oplus y$ is distinct from the values $v_{1,j} \oplus f_1(t') \oplus f_2(t') \oplus y'$, for $j < i$ and $(t',x',y') \in X^1_{u_{1,j}}$.

Now we count the number of all possible distinct tuples $(v_{1,1}, \ldots, v_{1,\alpha_{1,1}})$ in $\{0,1\}^n \setminus V_1 \cup \widetilde{V}_1$ satisfying the above two conditions. First, we have $|\{0,1\}^n \setminus V_1 \cup \widetilde{V}_1| = 2^n - (p_1 + \alpha_2)$. The first condition can remove at most $(|V_2| + |\widetilde{V}_2|) \cdot |X^1_{u_{1,i}}| = (p_2 + \alpha_1) \cdot |X^1_{u_{1,i}}|$ values, and the final condition can exclude at most $|X^1_{u_{1,i}}| \cdot \sum_{j=1}^{i-1} |X^1_{u_{1,j}}| \leq \alpha_{1,2} \cdot |X^1_{u_{1,i}}|$ values for each choice of $v_{1,i}$. By combining above facts, one gets that

$$N_{X_1} \geq \prod_{i=1}^{\alpha_{1,1}} (2^n - p_1 - \alpha_2 - (i-1) - (p_2 + \alpha_1 + \alpha_{1,2}) |X^1_{u_{1,i}}|). \tag{A4}$$

In Condition (ii), for each $i \in [\alpha_{1,1}]$ and $(t,x,y) \neq (t',x',y') \in X^1_{u_{1,i}}$, it holds that $v_{1,i} \oplus f_1(t) \oplus f_2(t) \oplus y \neq v_{1,i} \oplus f_1(t') \oplus f_2(t') \oplus y'$ (which is equivalent to $f_1(t) \oplus f_2(t) \oplus y \neq f_1(t') \oplus f_2(t') \oplus y'$) from the fact $\tau \notin \Gamma_4$. After choosing any tuple of distinct values $v_{1,i} \in \{0,1\}^n \setminus V_1 \cup \widetilde{V}_1$ such that Conditions (i) and (ii) hold, we define two corresponding sets as follows:

$$V_{1,1} = \{v_{1,1}, \ldots, v_{1,\alpha_{1,1}}\},$$
$$V_{1,2} = \{v_{1,i} \oplus f_1(t) \oplus f_2(t) \oplus y : i = 1, \ldots, \alpha_{1,1} \textit{ and } (t,x,y) \in X^1_{u_{1,i}}\}.$$

From the above discussion, we know that all values in $V_{1,1}$ are distinct, and all values in $V_{1,2}$ are also distinct. By the choice of $v_{1,i}$, it holds that $V_{1,1} \cap (V_1 \cup \widetilde{V}_1) = \emptyset$ and $V_{1,2} \cap (V_2 \cup \widetilde{V}_2) = \emptyset$. After this step, P_1 is fixed on $\alpha_{1,1}$ input-output pairs from $U_{1,1}$ to $V_{1,1}$, and P_2 is fixed on $\alpha_{1,2}$ input-output pairs from $U_{1,2}$ to $V_{1,2}$.

Step II. **Construct $\mathbf{V_{2,2} = P_2(U_{2,2})}$ and $\mathbf{V_{2,1} = P_1(U_{2,1})}$** .

We next deal with $\mathcal{Q}_{X_2}$. Recall that $U_{2,2} = \{u_{2,1}, \ldots, u_{2,\alpha_{2,2}}\}$ and $X_u^2 = \{(t,x,y) \in \mathcal{Q}_F : x \oplus f_2(t) = u\}$. Let N_{X_2} be the number of $\alpha_{2,2}$-wise tuples of distinct values $(v_{2,1}, \ldots, v_{2,\alpha_{2,2}})$ in $\{0,1\}^n \setminus V_2 \cup \widetilde{V}_2 \cup V_{1,2}$ such that the following two conditions hold:

(i) For each $i \in [\alpha_{2,2}]$ and each $(t,x,y) \in X^2_{u_{2,i}}$, $v_{2,i} \oplus f_1(t) \oplus f_2(t) \oplus y \notin V_1 \cup \widetilde{V}_1 \cup V_{1,1}$.

(ii) For each $i \in [\alpha_{2,2}]$ and $(t,x,y) \in X^2_{u_{2,i}}$, $v_{2,i} \oplus f_1(t) \oplus f_2(t) \oplus y$ is distinct from the values $v_{2,j} \oplus f_1(t') \oplus f_2(t') \oplus y'$, for $j < i$ and $(t',x',y') \in X^2_{u_{2,j}}$.

Now we count the number of all possible distinct tuples $(v_{2,1},\dots,v_{2,\alpha_{2,2}})$ in $\{0,1\}^n \setminus V_2 \cup \widetilde{V}_2 \cup V_{1,2}$ satisfying above two conditions. It is easy to see that $|\{0,1\}^n \setminus V_2 \cup \widetilde{V}_2 \cup V_{1,2}| = 2^n - (p_2+\alpha_1+\alpha_{1,2})$. The first condition can remove at most $(|V_1|+|\widetilde{V}_1|+|V_{1,1}|)\cdot|X^2_{u_{2,i}}| = (p_1+\alpha_2+\alpha_{1,1})\cdot|X^2_{u_{2,i}}|$ values, and the final condition can exclude at most $|X^2_{u_{2,i}}|\cdot\sum_{j=1}^{i-1}|X^2_{u_{2,j}}| \le \alpha_{2,1}\cdot|X^2_{u_{2,i}}|$ values for each choice of $v_{2,i}$. Then we can bound N_{X_2} as

$$N_{X_2} \ge \prod_{i=1}^{\alpha_{2,2}}(2^n - p_2 - \alpha_1 - \alpha_{1,2} - (i-1) - (p_1+\alpha_2+\alpha_{1,1}+\alpha_{2,1})|X^2_{u_{2,i}}|). \tag{A5}$$

In Condition (ii), for each i and $(t,x,y) \neq (t',x',y') \in X^2_{u_{2,i}}$, it holds that $v_{2,i} \oplus f_1(t) \oplus f_2(t) \oplus y \neq v_{2,i} \oplus f_1(t') \oplus f_2(t') \oplus y'$ (which is equivalent to $f_1(t) \oplus f_2(t) \oplus y \neq f_1(t') \oplus f_2(t') \oplus y'$) since otherwise τ would satisfy Condition (B-5). Similarly, we define two sets as:

$$V_{2,2} = \{v_{2,1},\dots,v_{2,\alpha_{2,2}}\},$$
$$V_{2,1} = \{v_{2,i} \oplus f_1(t) \oplus f_2(t) \oplus y : i = 1,\dots,\alpha_{2,2} \text{ and } (t,x,y) \in X^2_{u_{2,i}}\}.$$

By the discussion above, all values in $V_{2,1}$ are distinct and all values in $V_{2,2}$ are also distinct. Then $V_{2,1} \cap (V_1 \cup \widetilde{V}_1 \cup V_{1,1}) = \emptyset$ and $V_{2,2} \cap (V_2 \cup \widetilde{V}_2 \cup V_{1,2}) = \emptyset$ hold from the choice of $v_{2,i}$. After this step, P_2 is fixed on $\alpha_{2,2}$ input-output pairs from $U_{2,2}$ to $V_{2,2}$, and P_1 is fixed on $\alpha_{2,1}$ input-output pairs from $U_{2,1}$ to $V_{2,1}$.

Step III. **Construct $\mathbf{V_0^1 = P_1(U_0^1)}$ and $\mathbf{V_0^2 = P_2(U_0^2)}$** .

It remains to sample all possible compatible values in V_0^1 and V_0^2. First, we denote p_1' and p_2' as

$$p_1' = |V_1 \cup \widetilde{V}_1 \cup V_{1,1} \cup V_{2,1}| = p_1+\alpha_2+\alpha_{1,1}+\alpha_{2,1},$$
$$p_2' = |V_2 \cup \widetilde{V}_2 \cup V_{2,2} \cup V_{1,2}| = p_2+\alpha_1+\alpha_{1,2}+\alpha_{2,2}.$$

Recall that $U_0^1 = \{\hat{u}_{1,i,j} : 1 \le i \le m, 1 \le j \le q_i'\}$ and $U_0^2 = \{\hat{u}_{2,i,j} : 1 \le i \le m, 1 \le j \le q_i'\}$. Let N_0 be the number of q'-wise tuples of distinct values $(\hat{v}_{1,i,j})_{1\le i\le m, 1\le j\le q_i'}$ in $\{0,1\}^n \setminus V_1 \cup \widetilde{V}_1 \cup V_{1,1} \cup V_{2,1}$ such that the following two conditions hold:

(i) For each $i = 1,\dots,m$ and $j = 1,\dots,q_i'$, $\hat{v}_{1,i,j} \oplus f_1(\hat{t}_i) \oplus f_2(\hat{t}_i) \oplus y_{i,j} \notin V_2 \cup \widetilde{V}_2 \cup V_{1,2} \cup V_{2,2}$.

(ii) For each $i = 1,\dots,m$ and $j = 1,\dots,q_i'$, $\hat{v}_{1,i,j} \oplus f_1(\hat{t}_i) \oplus f_2(\hat{t}_i) \oplus y_{i,j}$ is distinct from the values $\hat{v}_{1,k,l} \oplus f_1(\hat{t}_k) \oplus f_2(\hat{t}_k) \oplus y_{k,l}$ for $k < i$ and $l \in [q_k']$. Furthermore, $\hat{v}_{1,i,j} \oplus f_1(\hat{t}_i) \oplus f_2(\hat{t}_i) \oplus y_{i,j}$ should also be distinct from the values $\hat{v}_{1,i,j'} \oplus f_1(\hat{t}_i) \oplus f_2(\hat{t}_i) \oplus y_{i,j'}$ with $j' < j$.

Except these two conditions, each $\hat{v}_{1,i,j}$ must be chosen distinctly from each other. First, one has $|\{0,1\}^n \setminus V_1 \cup \widetilde{V}_1 \cup V_{1,1} \cup V_{2,1}| = 2^n - p_1'$. Then we count the number of all possible distinct tuples $(\hat{v}_{1,i,j})_{1\le i\le m, 1\le j\le q_i'}$ satisfying above two conditions. The first condition can exclude at most p_2' values, and the second condition can exclude at most $\sum_{k=1}^{i-1} q_k' - j + 1$ values for each choice of $\hat{v}_{1,i,j}$. Furthermore, $\hat{v}_{1,i,j}$ should not be same to previous $\sum_{k=1}^{i-1} q_k' - j + 1$ items. Based on these facts, one can obtain that

$$N_0 \ge \prod_{i=1}^{m}\prod_{j=1}^{q_i'}(2^n - p_1' - p_2' - 2\sum_{k=1}^{i-1} q_k' - 2(j-1)). \tag{A6}$$

Until now, we have chosen $N_{X_1}\cdot N_{X_2}\cdot N_0$ possible values for $(v_{1,i})_{1\le i\le\alpha_{1,1}}$, $(v_{2,i})_{1\le i\le\alpha_{2,2}}$, and $(\hat{v}_{1,i,j})_{1\le i\le m, 1\le j\le q_i'}$ satisfying all above conditions. By this way, when conditioned on $E_{U_1} \wedge E_{U_2} \wedge (P_i \vdash \mathcal{Q}_{P_i}, i = 1,2)$, the event $E_{X_1} \wedge E_{X_2} \wedge E_0$ happens means that P_1 (resp. P_2) is fixed on exactly $\alpha_{1,1}+\alpha_{2,1}+q'$ (resp. $\alpha_{1,2}+\alpha_{2,2}+q'$) "new" input-output pairs from $U_{1,1} \cup U_{2,1} \cup U_0^1$ (resp. $U_{2,2} \cup U_{1,2} \cup U_0^2$) to $V_{1,1} \cup V_{2,1} \cup V_0^1$ (resp. $V_{2,2} \cup V_{1,2} \cup V_0^2$). Finally, we conclude that

$$\mathsf{p}''(\tau) \geq \frac{N_{X_1} \cdot N_{X_2} \cdot N_0}{(2^n - p_1 - \alpha_2)_{\alpha_{1,1}+\alpha_{2,1}+q'} (2^n - p_2 - \alpha_1)_{\alpha_{1,2}+\alpha_{2,2}+q'}}. \tag{A7}$$

From (*A3*) and (*A7*), one has

$$\mathsf{p}(\tau) \geq \frac{N_{X_1} \cdot N_{X_2} \cdot N_0}{(2^n - p_1)_{\alpha_2+\alpha_{1,1}+\alpha_{2,1}+q'} (2^n - p_2)_{\alpha_1+\alpha_{1,2}+\alpha_{2,2}+q'}}. \tag{A8}$$

Combining (21) and (*A8*), we get

$$\begin{aligned} \frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} &\geq \frac{N_{X_1} \cdot N_{X_2} \cdot N_0 \cdot 2^{nq}}{(2^n - p_1)_{\alpha_2+\alpha_{1,1}+\alpha_{2,1}+q'} (2^n - p_2)_{\alpha_1+\alpha_{1,2}+\alpha_{2,2}+q'}} \\ &= \underbrace{\frac{N_{X_1}}{(2^n - p_1 - \alpha_2)_{\alpha_{1,1}}}}_{R_{X_1}} \cdot \underbrace{\frac{N_{X_2}}{(2^n - p_2 - \alpha_1 - \alpha_{1,2})_{\alpha_{2,2}}}}_{R_{X_2}} \\ &\quad \cdot \underbrace{\frac{N_0 \cdot 2^{nq'}}{(2^n - p_1')_{q'} (2^n - p_2')_{q'}}}_{R_0} \\ &\quad \cdot \underbrace{\frac{2^{n(q-q')}}{(2^n - p_1)_{\alpha_2} \cdot (2^n - p_1 - \alpha_2 - \alpha_{1,1})_{\alpha_{2,1}} \cdot (2^n - p_2)_{\alpha_1+\alpha_{1,2}}}}_{\geq 1 (**)}, \end{aligned} \tag{A9}$$

where $(**)$ can be obtained from the fact $(2^n - p_1)_{\alpha_2} \cdot (2^n - p_1 - \alpha_2 - \alpha_{1,1})_{\alpha_{2,1}} \cdot (2^n - p_2)_{\alpha_1+\alpha_{1,2}} \leq 2^{n(\alpha_2+\alpha_{2,1}+\alpha_1+\alpha_{1,2})} = 2^{n(q-q')}$.

First, R_{X_1} can be bounded as follows:

$$\begin{aligned} R_{X_1} &\geq \frac{\prod_{i=1}^{\alpha_{1,1}} (2^n - p_1 - \alpha_2 - (i-1) - (p_2 + \alpha_1 + \alpha_{1,2}) |X^1_{u_{1,i}}|)}{(2^n - p_1 - \alpha_2)_{\alpha_{1,1}}} \\ &\geq \prod_{i=1}^{\alpha_{1,1}} \left(1 - \frac{(p_2 + \alpha_1 + \alpha_{1,2}) |X^1_{u_{1,i}}|}{2^n - p_1 - \alpha_2 - (i-1)}\right) \\ &\geq 1 - \frac{(p_2 + \alpha_1 + \alpha_{1,2}) \sum_{i=1}^{\alpha_{1,1}} |X^1_{u_{1,i}}|}{2^n - p_1 - \alpha_2 - \alpha_{1,1}} \\ &= 1 - \frac{(p_2 + \alpha_1 + \alpha_{1,2}) \alpha_{1,2}}{2^n - p_1 - \alpha_2 - \alpha_{1,1}} \\ &\geq 1 - \frac{2\sqrt{q}(p_2 + 2\sqrt{q})}{2^n}, \end{aligned} \tag{A10}$$

where the last equality holds from the fact $\alpha_1 \leq \sqrt{q}$, $\alpha_{1,2} \leq \sqrt{q}$, and $p_1 + \alpha_2 + \alpha_{1,1} \leq p_1 + 2q \leq p_1 + p_2 + 3q \leq 2^{n-1}$.

Next, we can bound R_{X_2} as

$$\begin{aligned} R_{X_2} &\geq \frac{\prod_{i=1}^{\alpha_{2,2}}(2^n - p_2 - \alpha_1 - \alpha_{1,2} - (i-1) - (p_1 + \alpha_2 + \alpha_{1,1} + \alpha_{2,1})|X^2_{u_{2,i}}|)}{(2^n - p_2 - \alpha_1 - \alpha_{1,2})_{\alpha_{2,2}}} \\ &\geq \prod_{i=1}^{\alpha_{2,2}}\left(1 - \frac{(p_1 + \alpha_2 + \alpha_{1,1} + \alpha_{2,1})|X^2_{u_{2,i}}|}{2^n - p_2 - \alpha_1 - \alpha_{1,2} - \alpha_{2,2}}\right) \\ &\geq 1 - \frac{(p_1 + \alpha_2 + \alpha_{1,1} + \alpha_{2,1})\sum_{i=1}^{\alpha_{2,2}}|X^2_{u_{2,i}}|}{2^n - p_2 - \alpha_1 - \alpha_{1,2} - \alpha_{2,2}} \\ &= 1 - \frac{(p_1 + \alpha_2 + \alpha_{1,1} + \alpha_{2,1})\alpha_{2,1}}{2^n - p_2 - \alpha_1 - \alpha_{1,2} - \alpha_{2,2}} \\ &\geq 1 - \frac{2\sqrt{q}(p_1 + 3\sqrt{q})}{2^n}, \end{aligned} \tag{A11}$$

where the last equality holds from the fact $\alpha_2 \leq \sqrt{q}$, $\alpha_{1,1} \leq \sqrt{q}$, $\alpha_{2,1} \leq \sqrt{q}$, and $p_2 + \alpha_1 + \alpha_{1,2} + \alpha_{2,2} \leq p_2 + 3q \leq p_1 + p_2 + 3q \leq 2^{n-1}$.

Finally, R_0 can be bounded in the following way:

$$\begin{aligned} R_0 &\geq \frac{\prod_{i=1}^{m} 2^{nq'_i} \cdot \prod_{j=0}^{q'_i-1}(2^n - p'_1 - p'_2 - 2\sum_{k=1}^{i-1} q'_k - 2j)}{(2^n - p'_1)_{q'}(2^n - p'_2)_{q'}} \\ &= \prod_{i=1}^{m}\left(\frac{2^{nq'_i} \cdot \prod_{j=0}^{q'_i-1}(2^n - p'_1 - p'_2 - 2\sum_{k=1}^{i-1} q'_k - 2j)}{\left(2^n - p'_1 - \sum_{k=1}^{i-1} q'_k\right)_{q'_i}\left(2^n - p'_2 - \sum_{k=1}^{i-1} q'_k\right)_{q'_i}}\right) \\ &= \prod_{i=1}^{m}\prod_{j=0}^{q'_i-1}\left(\frac{2^n(2^n - p'_1 - p'_2 - 2\sum_{k=1}^{i-1} q'_k - 2j)}{\left(2^n - p'_1 - \sum_{k=1}^{i-1} q'_k - j\right)\left(2^n - p'_2 - \sum_{k=1}^{i-1} q'_k - j\right)}\right) \\ &\overset{(a)}{\geq} \prod_{i=1}^{m}\left(1 - \frac{4q'_i(p'_1 + \sum_{k=1}^{i} q'_k)(p'_2 + \sum_{k=1}^{i} q'_k)}{2^{2n}}\right) \\ &\overset{(b)}{\geq} \prod_{i=1}^{m}\left(1 - \frac{4q'_i(p_1 + p_2 + 2q)^2}{2^{2n}}\right) \\ &\overset{(c)}{\geq} \left(1 - \frac{4q'(p_1 + p_2 + 2q)^2}{2^{2n}}\right) \\ &\geq \left(1 - \frac{4q(p_1 + p_2 + 2q)^2}{2^{2n}}\right), \end{aligned} \tag{A12}$$

where (a) holds by Lemma 2 when one sets $A = q'_i$, $B = p'_1 + \sum_{k=1}^{i-1} q'_k$, and $C = p'_2 + \sum_{k=1}^{i-1} q'_k$ such that $A + B \leq p'_1 + q' = p_1 + q + \alpha_{1,1} - \alpha_{1,2} - \alpha_1 \leq p_1 + q + \alpha_{1,1} \leq p_1 + 2q + p_2 \leq 2^{n-1}$ and $A + C \leq p_2 + q + \alpha_{2,2} \leq p_1 + 2q + p_2 \leq 2^{n-1}$, (b) follows as $p'_1 + \sum_{k=1}^{i} q'_k \leq p'_1 + q' \leq p_1 + q + \alpha_{1,1} \leq p_1 + 2q + p_2$ and $p'_2 + \sum_{k=1}^{i} q'_k \leq p'_2 + q' \leq p_2 + q + \alpha_{2,2} \leq p_1 + 2q + p_2$, and (c) follows as $q' = \sum_{k=1}^{m} q'_k$.

We finally lower bound $\frac{\Pr[T_{\mathsf{re}}=\tau]}{\Pr[T_{\mathsf{id}}=\tau]}$, from $(A9)$, $(A10)$, $(A11)$, and $(A12)$, as

$$\frac{\Pr[T_{\mathsf{re}} = \tau]}{\Pr[T_{\mathsf{id}} = \tau]} \geq 1 - \frac{4q(p_1 + p_2 + 2q)^2}{2^{2n}} - \frac{2\sqrt{q}(p_1 + p_2)}{2^n} - \frac{10q}{2^n}.$$

Appendix C. Upper Bound on $\mathbf{Bad}_{M_1}$

In this part, we upper bound each term $\Pr[T_{\mathsf{id}} \in \Gamma'_i]$ for $i \in [15]$ one by one.

Bounding (C-1), (C-2), and (C-3): For any $(t_i, x_i, y_i) \in \bar{\mathcal{Q}}_F$ and $(u_j, v_j), (u_{j'}, v_{j'}) \in \bar{\mathcal{Q}}_P$, by the ϵ_1-regular property of (f_1, f_2), one has

$$\Pr[(f_1(t_i) = x_i \oplus u_j) \wedge (f_2(t_i) = x_i \oplus v_{j'})] \leq \epsilon_1^2.$$

Since the number of all possible tuples for $((t_i, x_i, y_i), u_j, v_{j'})$ is at most qp^2, by union bound, it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma_1'] \leq qp^2\epsilon_1^2.$$

Similarly, we can bound the probabilities of (C-2) and (C-3) as

$$\Pr[T_{\mathsf{id}} \in \Gamma_2'] \leq qp^2\epsilon_1^2 \text{ and } \Pr[T_{\mathsf{id}} \in \Gamma_3'] \leq qp^2\epsilon_1^2.$$

Bounding (**C-4**) and (**C-5**): For any fixed construction queries (t_i, x_i, y_i), $(t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$, and $(u_j, v_j) \in \bar{\mathcal{Q}}_P$, by the same reason as above, we have

$$\Pr[(f_1(t_i) = x_i \oplus u_j) \wedge (f_2(t_i) = v_j \oplus f_1(t_i) \oplus y_i \oplus x_{i'} \oplus f_1(t_{i'}))] \leq \epsilon_1^2.$$

Since there are at most q^2p possible unordered pairs for $\{(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (u_j, v_j)\}$, by union bound, one obtains that

$$\Pr[T_{\mathsf{id}} \in \Gamma_4'] \leq q^2p\epsilon_1^2, \text{ and similarly, } \Pr[T_{\mathsf{id}} \in \Gamma_5'] \leq q^2p\epsilon_1^2.$$

Bounding (**C-6**) and (**C-7**): For any fixed distinct construction queries (t_i, x_i, y_i), $(t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $u_j \in U$, from the ϵ_1-regular and ϵ_2-AXU properties of (f_1, f_2), one has

$$\Pr[(f_1(t_i) = x_i \oplus u_j) \wedge (f_2(t_i) \oplus f_1(t_{i'}) = x_i \oplus x_{i'})] \leq \epsilon_1\epsilon_2.$$

Since there are at most q^2p possible unordered pairs for $\{(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), u_j\}$, by union bound, it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma_6'] \leq q^2p\epsilon_1\epsilon_2, \text{ and similarly, } \Pr[T_{\mathsf{id}} \in \Gamma_7'] \leq q^2p\epsilon_1\epsilon_2.$$

Bounding (**C-8**) and (**C-9**): For any two distinct construction queries $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$, one can conclude

$$\Pr[(f_1(t_i) \oplus f_1(t_{i'}) = x_i \oplus x_{i'}) \wedge (f_2(t_i) \oplus f_2(t_{i'}) = f_1(t_i) \oplus f_1(t_{i'}) \oplus y_i \oplus y_{i'})] \leq \epsilon_2^2$$

from the ϵ_2-AXU property of (f_1, f_2). In particular, when $t_i = t_{i'}$, the above probability is in fact zero since in this case we have $f_1(t_i) \oplus f_1(t_{i'}) = 0$ but $x_i \neq x_{i'}$. Then by summing over all $\binom{q}{2}$ possible unordered pairs $\{(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'})\}$, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_8'] \leq \binom{q}{2} \cdot \epsilon_2^2 \leq \frac{q^2\epsilon_2^2}{2}, \text{ and similarly, } \Pr[T_{\mathsf{id}} \in \Gamma_9'] \leq \frac{q^2\epsilon_2^2}{2}.$$

Bounding (**C-10**): For any $(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'})$, and $(t_{i''}, x_{i''}, y_{i''}) \in \bar{\mathcal{Q}}_F$ with $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'})$ and $(t_i, x_i, y_i) \neq (t_{i''}, x_{i''}, y_{i''})$, one can conclude, from the ϵ_2-AXU property of (f_1, f_2), that

$$\Pr[(f_1(t_i) \oplus f_1(t_{i'}) = x_i \oplus x_{i'}) \wedge (f_2(t_i) \oplus f_2(t_{i''}) = x_i \oplus x_{i''})] \leq \epsilon_2^2$$

Note that the number of all possible tuples $\{(t_i, x_i, y_i), (t_{i'}, x_{i'}, y_{i'}), (t_{i''}, x_{i''}, y_{i''})\}$ is at most q^3 so that one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_{10}'] \leq q^3\epsilon_2^2.$$

Bounding (**C-11**), (**C-12**), (**C-13**), and (**C-14**): We deal with bad conditions (C-11) and (C-13) together by using the fact that

$$\Pr[T_{\mathsf{id}} \in \Gamma_{11}' \cup \Gamma_{13}'] \leq \Pr[T_{\mathsf{id}} \in \Gamma_{13}'] + \Pr[T_{\mathsf{id}} \in \Gamma_{11}' \setminus \Gamma_{13}'].$$

We first consider how to upper bound $\Pr[T_{\mathsf{id}} \in \Gamma_{13}']$. Recall that $\bar{\alpha}_1 = |\{(t, x, y) \in \bar{\mathcal{Q}}_F : x \oplus f_1(t) \in U\}|$. Then the expectation value of $\bar{\alpha}_1$ can be computed as

$$\mathbb{E}[\bar{\alpha}_1] = \sum_{(t,x,y) \in \bar{\mathcal{Q}}_F:} \sum_{u \in U:} \Pr[x \oplus f_1(t) = u] \leq pq\epsilon_1$$

due to the ϵ_1-regular property of (f_1, f_2). By Markov's inequality, one has

$$\Pr[T_{\mathsf{id}} \in \Gamma_{13}'] \leq \frac{\mathbb{E}[\bar{\alpha}_1]}{\sqrt{q}} = p\sqrt{q}\epsilon_1.$$

Under the condition $\bar{\alpha}_1 \leq \sqrt{q}$, there are at most $q/2$ pairs $\{((t_i, x_i, y_i), u_j), ((t_{i'}, x_{i'}, y_{i'}), u_{j'})\}$ such that $x_i \oplus f_1(t_i) = u_j$ and $x_{i'} \oplus f_1(t_{i'}) = u_{j'}$ where $(t_i, x_i, y_i) \neq (t_{i'}, x_{i'}, y_{i'}) \in \bar{\mathcal{Q}}_F$ and $(u_j, v_j), (u_{j'}, v_{j'}) \in \bar{\mathcal{Q}}_P$. In this case, since the random variables y_i and $y_{i'}$ are independently and uniformly distributed over $\{0,1\}^n$, one can conclude that

$$\Pr[v_j \oplus f_1(t_i) \oplus f_2(t_i) \oplus y_i = v_{j'} \oplus f_1(t_{i'}) \oplus f_2(t_{i'}) \oplus y_{i'}] \leq \frac{1}{2^n}.$$

By summing over all these $q/2$ possible pairs, we have

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{11} \setminus \Gamma'_{13}] \leq \frac{q}{2^{n+1}}.$$

and so that it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{11} \cup \Gamma'_{13}] \leq p\sqrt{q}\epsilon_1 + \frac{q}{2^{n+1}}.$$

Similarly, we can obtain that

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{12} \cup \Gamma'_{14}] \leq p\sqrt{q}\epsilon_1 + \frac{q}{2^{n+1}}.$$

Bounding (C-15): To upper bound $\Pr[T_{\mathsf{id}} \in \Gamma'_{15}]$, we first define the random variable $\bar{T}_F = |\{((t,x,y),(t',x',y')) \in \bar{\mathcal{Q}}_F \times \bar{\mathcal{Q}}_F : (t,x,y) \neq (t',x',y'), x \oplus f_1(t) = x' \oplus f_1(t')\}|$. By definition of $\bar{\beta}_1$, it holds that

$$\bar{\beta}_1 = |\{(t,x,y) \in \bar{\mathcal{Q}}_F : \exists (t,x,y) \neq (t',x',y'), x \oplus f_1(t) = x' \oplus f_1(t')\}| \leq \bar{T}_F.$$

Thus, $\mathbb{E}[\bar{\beta}_1] \leq \mathbb{E}[\bar{T}_F]$. Then the expectation value of $\bar{T}_F$ can be bounded as

$$\mathbb{E}[\bar{T}_F] = \sum_{(t,x,y) \neq (t',x',y') \in \bar{\mathcal{Q}}_F^2:} \Pr[x \oplus f_1(t) = x' \oplus f_1(t')] \leq \frac{q^2\epsilon_2}{2}$$

from the ϵ_2-AXU property of (f_1, f_2). By Markov's inequality, we have

$$\Pr[\bar{\beta}_1 \geq \sqrt{q}] \leq \frac{\mathbb{E}[\beta_1]}{\sqrt{q}} \leq \frac{\mathbb{E}[\bar{T}_F]}{\sqrt{q}} \leq \frac{q^{3/2}\epsilon_2}{2}.$$

Similarly, one has

$$\Pr[\bar{\beta}_2 \geq \sqrt{q}] \leq \frac{q^{3/2}\epsilon_2}{2}.$$

Finally, by combining the above two facts, it holds that

$$\Pr[T_{\mathsf{id}} \in \Gamma'_{15}] \leq \Pr[(\bar{\beta}_1 \geq \sqrt{q}) \vee (\bar{\beta}_2 \geq \sqrt{q})] \leq q^{3/2}\epsilon_2.$$

Appendix D. More Details in Proof of Lemma 6

First we have

$$
\begin{aligned}
R_1(\alpha) &\geq \frac{\prod_{k=0}^{\alpha_3-1}\left(2^n-(q-\alpha_5+\alpha_6+\alpha)-p-k-(p+\alpha+q+\alpha_3)|\bar{X}^1_{u_{3,k+1}}|\right)}{\prod_{k=0}^{\alpha_3-1}(2^n-p-k)} \\
&\geq \prod_{k=0}^{\alpha_3-1}\left(1-\frac{q-\alpha_5+\alpha_6+\alpha}{2^n-p-k}-\frac{(p+\alpha+q+\alpha_3)|\bar{X}^1_{u_{3,k+1}}|}{2^n-p-k}\right) \\
&\geq \prod_{k=0}^{\alpha_3-1}\left(1-\frac{q+\alpha_6+\alpha}{2^n-p-\alpha_3}-\frac{(p+\alpha+q+\alpha_3)|\bar{X}^1_{u_{3,k+1}}|}{2^n-p-\alpha_3}\right) \\
&\geq 1-\frac{\alpha_3(q+\alpha_6+\alpha)}{2^n-p-\alpha_3}-\frac{(p+\alpha+q+\alpha_3)\sum_{k=0}^{\alpha_3-1}|\bar{X}^1_{u_{3,k+1}}|}{2^n-p-\alpha_3} \\
&\overset{(d)}{\geq} 1-\frac{2\alpha_3(q+\alpha_6+\alpha)}{2^n}-\frac{2(p+\alpha+q+\alpha_3)\alpha_4}{2^n} \\
&\overset{(e)}{\geq} 1-\frac{2\sqrt{q}(q+\sqrt{q}+q/2^{\frac{n}{3}})}{2^n}-\frac{2(p+q/2^{\frac{n}{3}}+q+\sqrt{q})\sqrt{q}}{2^n} \\
&= 1-\frac{4q^{3/2}}{2^n}-\frac{2p\sqrt{q}}{2^n}-\frac{4q}{2^n}-\frac{4q^{3/2}}{2^{\frac{4n}{3}}} \\
&\geq 1-\frac{8q^{3/2}}{2^n}-\frac{2p\sqrt{q}}{2^n}-\frac{4q}{2^n},
\end{aligned}
\tag{A13}
$$

where (d) follows as $p+\alpha_3 \leq p+\sqrt{q} \leq 2^{n-1}$ so that $2^n-p-\alpha_3 > 2^{n-1}$, and (e) follows as $\alpha_3, \alpha_4, \alpha_6 \leq \sqrt{q}$ and $\alpha \leq M \leq q/2^{\frac{n}{3}}$.

Then, the item $R_2(\alpha)$ can be bounded as

$$
\begin{aligned}
R_2(\alpha) &\geq \frac{\prod_{k=0}^{\alpha_6-1}\left(2^n-(p+\alpha_3+q+\alpha)-k-(p+q+\alpha_3+\alpha_6+\alpha)|\bar{X}^2_{v_{6,k+1}}|\right)}{\prod_{k=0}^{\alpha_6-1}(2^n-p-\alpha_3-k)} \\
&\geq \prod_{k=0}^{\alpha_6-1}\left(1-\frac{q+\alpha}{2^n-p-\alpha_3-k}-\frac{(p+q+\alpha_3+\alpha_6+\alpha)|\bar{X}^2_{v_{6,k+1}}|}{2^n-p-\alpha_3-k}\right) \\
&\overset{(f)}{\geq} 1-\frac{2(q+\alpha)\alpha_6}{2^n}-\frac{2(p+q+\alpha_3+\alpha_6+\alpha)\sum_{k=0}^{\alpha_6-1}|\bar{X}^2_{v_{6,k+1}}|}{2^n} \\
&\geq 1-\frac{2(q+\alpha)\alpha_6}{2^n}-\frac{2(p+q+\alpha_3+\alpha_6+\alpha)\alpha_5}{2^n} \\
&\overset{(g)}{\geq} 1-\frac{2(q+q/2^{\frac{n}{3}})\sqrt{q}}{2^n}-\frac{2(p+q+2\sqrt{q}+q/2^{\frac{n}{3}})\sqrt{q}}{2^n} \\
&\geq 1-\frac{8q^{3/2}}{2^n}-\frac{2p\sqrt{q}}{2^n}-\frac{4q}{2^n},
\end{aligned}
\tag{A14}
$$

where (f) follows as $p+\alpha_3+k \leq p+\alpha_3+\alpha_6 \leq p+2\sqrt{q} \leq 2^{n-1}$ so that $2^n-p-k > 2^{n-1}$ and (g) follows as $\alpha_3, \alpha_5, \alpha_6 \leq \sqrt{q}$ and $\alpha \leq M \leq q/2^{\frac{n}{3}}$.

Finally, $R_0(\alpha)$ can be bounded in the following.

$$
\begin{aligned}
R_0(\alpha) &= \frac{2^{n\bar{q}'}\cdot\mathcal{N}_S(\alpha)\cdot\mathcal{N}_0(\alpha)}{(2^n-p')_{2\bar{q}''+3\alpha}} \\
&\geq \frac{(\bar{q}')_{2\alpha}}{\alpha!}\cdot(1-\epsilon_0)\cdot\frac{\mathcal{N}_0(\alpha)\cdot 2^{n\bar{q}'}}{(2^n-p')_{2\bar{q}''+3\alpha}} \\
&= (1-\epsilon_0)\cdot\frac{(\bar{q}')_{2\alpha}}{\alpha!}\cdot\frac{2^{n\bar{q}'}\cdot\prod_{i=1}^{m}\prod_{j=0}^{\bar{q}_i''-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{(2^n-p')_{\bar{q}''+\alpha+\bar{q}'}} \\
&= (1-\epsilon_0)\cdot\frac{(\bar{q}')_{2\alpha}}{(\bar{q}')_{\alpha}(\bar{q}')_{\alpha}} \\
&\quad\cdot\frac{2^{n\bar{q}'}\cdot\prod_{i=1}^{m}\prod_{j=0}^{\bar{q}_i''-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{(2^n-p'-\bar{q}')_{\bar{q}''+\alpha}(2^n-p'-\bar{q}')_{\bar{q}''+\alpha}} \\
&\quad\cdot\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha) \\
&= (1-\epsilon_0)\cdot\underbrace{\frac{(\bar{q}')_{2\alpha}}{(\bar{q}')_{\alpha}(\bar{q}')_{\alpha}}}_{\mathcal{B}_1(\alpha)}\cdot\underbrace{\frac{(2^n)^{2\alpha}}{(2^n-p'-\bar{q}')_{\alpha}^2}}_{\geq 1}\cdot\mathsf{Hyp}_{2^n-p',\bar{q}',\bar{q}'}(\alpha) \\
&\quad\cdot\underbrace{\frac{2^{n\bar{q}''}\cdot\prod_{i=1}^{m}\prod_{j=0}^{\bar{q}_i''-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{(2^n-p'-\bar{q}'-\alpha)_{\bar{q}''}^2}}_{\mathcal{B}_2(\alpha)}
\end{aligned}
\tag{A15}
$$

For $\mathcal{B}_1(\alpha)$, we have

$$
\begin{aligned}
\mathcal{B}_1(\alpha) &\overset{(h)}{\geq} \frac{(\bar{q}'-2M)^{2\alpha}}{(\bar{q}')^{2\alpha}} = \left(1-\frac{2M}{\bar{q}'}\right)^{2\alpha} \\
&\geq 1-\frac{4M\alpha}{\bar{q}'} \geq 1-\frac{4\alpha}{2^{n/3}} \\
&\overset{(j)}{\geq} 1-\frac{4q}{2^{2n/3}},
\end{aligned}
\tag{A16}
$$

where (h) follows as $q-i\geq q-2M$ for $0\leq i\leq 2\alpha\leq 2M$ and $(\bar{q}')_{\alpha}\leq(\bar{q}')^{\alpha}$ and (j) follows as $\alpha\leq M\leq\frac{q}{2^{n/3}}$.

We then bound the $\mathcal{B}_2(\alpha)$ as

$$
\begin{aligned}
\mathcal{B}_2(\alpha) &= \frac{2^{n(\sum_{i=1}^{m}\bar{q}_i'')}\prod_{i=1}^{m}\prod_{j=0}^{\bar{q}_i''-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{\prod_{i=1}^{m}\left(2^n-p'-\bar{q}'-\alpha-\sum_{k=1}^{i-1}\bar{q}_k''\right)^2_{\bar{q}_i''}} \\
&= \prod_{i=1}^{m}\left(\frac{2^{n\bar{q}_i''}\prod_{j=0}^{\bar{q}_i''-1}(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{\left(2^n-p'-\bar{q}'-\alpha-\sum_{k=1}^{i-1}\bar{q}_k''\right)^2_{\bar{q}_i''}}\right) \\
&= \prod_{i=1}^{m}\prod_{j=0}^{\bar{q}_i''-1}\left(\frac{2^n(2^n-2p'-2\bar{q}'-2\alpha-2\sum_{k=1}^{i-1}\bar{q}_k''-2j)}{\left(2^n-p'-\bar{q}'-\alpha-\sum_{k=1}^{i-1}\bar{q}_k''-j\right)^2}\right) \\
&\overset{(k)}{\geq} \prod_{i=1}^{m}\left(1-\frac{4\bar{q}_i''(p'+\bar{q}'+\alpha+\sum_{k=1}^{i}\bar{q}_k'')^2}{2^{2n}}\right) \\
&\geq \prod_{i=1}^{m}\left(1-\frac{4\bar{q}_i''(p'+2\bar{q}')^2}{2^{2n}}\right) \\
&\overset{(l)}{\geq} \left(1-\frac{4\bar{q}''(p'+2\bar{q}')^2}{2^{2n}}\right) \\
&\geq \left(1-\frac{4q(p+2q+6\sqrt{q})^2}{2^{2n}}\right),
\end{aligned}
\tag{A17}
$$

where (k) follows as Lemma 2 when we set $N = 2^n$, $A = \bar{q}_i''$ and $B = C = p' + \bar{q}' + \alpha + \sum_{k=1}^{i-1}\bar{q}_k''$ where it satisfies $A + B = A + C = p' + \bar{q}' + \alpha + \sum_{k=1}^{i}\bar{q}_k'' \leq p' + 2\bar{q}' \leq p + 2q + 6\sqrt{q} \leq 2^{n-1}$ from the assumption and (l) follows as $\bar{q}'' = \sum_{i=1}^{m}\bar{q}_i''$.

References

1. Bonilla, L.L.; Alvaro, M.; Carretero, M. Chaos-based true random number generators. *J. Math. Ind.* **2016**, *7*, 191. [CrossRef]
2. Trejo, J.M.A.; Calude, C.S. A new quantum random number generator certified by value indefiniteness. *Theor. Comput. Sci.* **2021**, *862*, 3–13. [CrossRef]
3. Blum, M.; Micali, S. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. *SIAM J. Comput.* **1984**, *13*, 850–864. [CrossRef]
4. Yao, A.C.C. Theory and Applications of Trapdoor Functions. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), Chicago, IL, USA, 3–5 November 1982.
5. Goldreich, O.; Goldwasser, S.; Micali, S. How to Construct Random Functions. In Proceedings of the 25th Annual Symposium onFoundations of Computer Science, Singer Island, FL, USA, 24–26 October 1984.
6. Håstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. Construction of a Pseudo-Random Generator From Any One-Way Function. *SIAM J. Comput.* **1993**, *28*, 12–24.
7. Naor, M.; Reingold, O.; Rosen, A. Pseudorandom Functions and Factoring. *SIAM J. Comput.* **2002**, *31*, 1383–1404. [CrossRef]
8. Naor, M.; Reingold, O. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM* **2004**, *51*, 231–262. [CrossRef]
9. Banerjee, A.; Peikert, C.; Rosen, A. Pseudorandom Functions and Lattices. In *Advances in Cryptology—EUROCRYPT 2012*; Pointcheval, D., Johansson, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 719–737.
10. Boneh, D.; Lewi, K.; Montgomery, H.W.; Raghunathan, A. Key Homomorphic PRFs and Their Applications. In *Advances in Cryptology–CRYPTO 2013, Part I*; Canetti, R., Garay, J.A., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8042, pp. 410–428.
11. Banerjee, A.; Peikert, C. New and Improved Key-Homomorphic Pseudorandom Functions. In *Advances in Cryptology—CRYPTO 2014, Part I*; Garay, J.A., Gennaro, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8616, pp. 353–370.
12. Bellare, M.; Krovetz, T.; Rogaway, P. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In *Advances in Cryptology—EUROCRYPT'98*; Nyberg, K., Ed.; Springer: Berlin/Heidelberg, Germany, 1998, Volume 1403, pp. 266–280.
13. Cogliati, B.; Seurin, Y. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In *Advances in Cryptology—CRYPTO 2016, Part I*; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9814, pp. 121–149.

14. Mennink, B.; Neves, S. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In *Advances in Cryptology—CRYPTO 2017, Part III*; Katz, J., Shacham, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10403, pp. 556–583.
15. Chen, Y.L.; Lambooij, E.; Mennink, B. How to Build Pseudorandom Functions from Public Random Permutations. In *Advances in Cryptology—CRYPTO 2019, Part I*; Boldyreva, A., Micciancio, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11692, pp. 266–293.
16. Cogliati, B.; Lampe, R.; Seurin, Y. Tweaking Even-Mansour Ciphers. In *Advances in Cryptology—CRYPTO 2015, Part I*; Gennaro, R., Robshaw, M.J.B., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9215, pp. 189–208.
17. Dutta, A. Minimizing the Two-Round Tweakable Even-Mansour Cipher. In *Advances in Cryptology—ASIACRYPT 2020, Part I*; Moriai, S., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12491, pp. 601–629.
18. Chakraborti, A.; Nandi, M.; Talnikar, S.; Yasuda, K. On the Composition of Single-Keyed Tweakable Even-Mansour for Achieving BBB Security. *IACR Trans. Symm. Cryptol.* **2020**, *2020*, 1–39. [CrossRef]
19. Dutta, A.; Nandi, M.; Talnikar, S. Permutation Based EDM: An Inverse Free BBB Secure PRF. *IACR Trans. Symmetric Cryptol.* **2021**, *2021*, 31–70. [CrossRef]
20. Chen, S.; Steinberger, J.P. Tight Security Bounds for Key-Alternating Ciphers. In *Advances in Cryptology—EUROCRYPT 2014*; Nguyen, P.Q., Oswald, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume8441, pp. 327–350. [CrossRef]
21. Patarin, J. The "Coefficients H" Technique (Invited Talk). In *Selected Areas in Cryptography. SAC 2008*; Avanzi, R.M., Keliher, L., Sica, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5381, pp. 328–345. [CrossRef]
22. Chen, S.; Lampe, R.; Lee, J.; Seurin, Y.; Steinberger, J.P. Minimizing the Two-Round Even-Mansour Cipher. In *Advances in Cryptology—CRYPTO 2014, Part I*; Garay, J.A., Gennaro, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8616, pp. 39–56. [CrossRef]
23. Minematsu, K.; Iwata, T. Building Blockcipher from Tweakable Blockcipher: Extending FSE 2009 Proposal. In *Processings of 13th IMA International Conference on Cryptography and Coding (IMACC 2011)*; Chen, L., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7089, pp. 391–412.