Multi-User Security of the Sum of Truncated Random Permutations (Full Version)

Wonseok Choi[1]*, Hwigyeom Kim[2], Jooyoung Lee[2]**, and Yeongmin Lee[2]

[1] KIAS, Seoul, Korea
{wonseok}@kias.re.kr
[2] KAIST, Daejeon, Korea
{buddha93,hicalf,dudals4780}@kaist.ac.kr

Abstract. For several decades, constructing pseudorandom functions from pseudorandom permutations, so-called Luby-Rackoff backward construction, has been a popular cryptographic problem. Two methods are well-known and comprehensively studied for this problem: summing two random permutations and truncating partial bits of the output from a random permutation. In this paper, by combining both summation and truncation, we propose new Luby-Rackoff backward constructions, dubbed SaT1 and SaT2, respectively.

SaT2 is obtained by partially truncating output bits from the sum of two independent random permutations, and SaT1 is its single permutation-based variant using domain separation. The distinguishing advantage against SaT1 and SaT2 is upper bounded by $O(\sqrt{\mu q_{\max}}/2^{n-0.5m})$ and $O(\sqrt{\mu} q_{\max}^{1.5}/2^{2n-0.5m})$, respectively, in the multi-user setting, where n is the size of the underlying permutation, m is the output size of the construction, μ is the number of users, and $q_{\max}$ is the maximum number of queries per user. We also prove the distinguishing advantage against a variant of XORP[3] (studied by Bhattacharya and Nandi at Asiacrypt 2021) using independent permutations, dubbed SoP3-2, is upper bounded by $O(\sqrt{\mu} q_{\max}^2/2^{2.5n})$.

In the multi-user setting with $\mu = O(2^{n-m})$, a truncated random permutation provides only the birthday bound security, while SaT1 and SaT2 are fully secure, i.e., allowing $O(2^n)$ queries for each user. It is the same security level as XORP[3] using three permutation calls, while SaT1 and SaT2 need only two permutation calls.

Keywords: pseudorandom function, Luby-Rackoff backward, sum of permutations, truncated random permutation, multi-user security

* supported by a KIAS Individual Grant CG089501 at Korea Institute for Advanced Study

** This work was supported by Institute for Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2022-0-01202 , Regional strategic industry convergence security core talent training business)

1 Introduction

Block ciphers are usually considered to be pseudorandom permutations (PRPs) from a cryptographic perspective. That means someone cannot distinguish a secure block cipher from a random permutation before performing a certain number of encryption and decryption queries in a black-box manner. On the other hand, various cryptographic constructions such as the Wegman-Carter message authentication scheme use a pseudorandom function (PRF) as their building primitives to achieve beyond-birthday-bound security. When the underlying PRF is instantiated with a block cipher, the security of the resulting construction (e.g., the Wegman-Carter-Shoup construction) might be degraded down to the birthday bound [2,3,4].

In order to address the problem of security degradation, there has been a significant amount of research on construction of beyond-birthday-bound secure PRFs from (sufficiently secure) PRPs [1,3,5,9,14,16,19,20,23,30,31]. Among such *Luby-Rackoff backward* constructions, two constructions are well-known and have been comprehensively studied: summing two random permutations and truncating partial bits of the output from a random permutation.

Sum of Random Permutations. Given two n-bit (keyed) PRPs P_1 and P_2, their sum, denoted SoP, maps $x \in \{0,1\}^n$ to

$$\mathsf{SoP}[\mathsf{P}_1, \mathsf{P}_2](x) \stackrel{\text{def}}{=} \mathsf{P}_1(x) \oplus \mathsf{P}_2(x).$$

This construction was first introduced by Bellare et al. [3], and its security has been proved up to $2^{2n/3}$ queries by Lucks [24]. A series of works followed [11,27,30], culminating with the proof by Dai et al. [14] that the sum of two n-bit random permutations is (fully) secure up to $O(2^n)$ queries.

Sum of Three or More Random Permutations. $\mathsf{SoP}[k]$ is a generalization of SoP. With k random permutations, $\mathsf{SoP}[k]$ returns its output by summing outputs of k random permutations. Lucks [24] showed that $\mathsf{SoP}[k]$ is secure up to $O(2^{kn/(k+1)})$ queries, and Mennink and Preneel [27] showed that $\mathsf{SoP}[k]$ is not weaker than SoP. Since SoP is fully secure in terms of indistinguishability, this problem seemed to be settled. However, a single permutation variant of $\mathsf{SoP}[3]$ with domain separation, originally dubbed $\mathsf{XORP}[3]$, but denoted $\mathsf{SoP3\text{-}1}$ throughout this paper, was revisited by Bhattacharya and Nandi [6], where they proved its n-bit security in the multi-user setting with $O(2^n)$ users.

Truncated Random Permutations. Let n and m be positive integers such that $m < n$. The TRP construction is defined as

$$\mathsf{TRP}[\mathsf{P}] \stackrel{\text{def}}{=} \mathsf{Tr}_m(\mathsf{P}(\cdot)),$$

where P is an n-bit permutation (modeled as a random secret permutation) and

$$\begin{aligned} \mathsf{Tr}_m : \{0,1\}^n &\longrightarrow \{0,1\}^m \\ x &\longmapsto x_L, \end{aligned}$$

when $x \in \{0,1\}^n$ is written as $x_L \parallel x_R$ for $x_L \in \{0,1\}^m$ and $x_R \in \{0,1\}^{n-m}$. Truncating a random permutation was first considered by Hall et al. [20] and proved secure up to $O(2^{(n+m)/2})$ adversarial queries [16]. Besides, the authors realized that their security bound follows from the result of Stam [32] which was already published in 1978. This bound turns out to be tight as they also present matching attacks. Mennink [25] generalized truncation functions used in TRP and showed that the security of such constructions could not exceed that of the original TRP.

Multi-User Security. In the real world, multiple users use the same cryptographic scheme with independent keys. Even if a cryptographic scheme is proved to be secure in the single-user setting, it does not generally guarantee its multi-user security, where an adversary access multiple instances, each of which uses a distinct key. Multi-user security of symmetric-key constructions was firstly considered by Mouha et al. [28], by proving the multi-user security of the Even-Mansour cipher. Since then, various constructions have been analyzed in the multi-user setting [7,21,22,33].

1.1 Related Work

There have been some other approaches to building a PRF on top of PRPs. In this section, P_1 and P_2 are independent n-bit permutations.

Encrypted Davis-Meyer. Cogliati and Seurin [12] introduced a PRF construction, dubbed Encrypted Davis-Meyer (EDM), defined as

$$\mathsf{EDM}[\mathsf{P}_1, \mathsf{P}_2](x) \stackrel{\text{def}}{=} \mathsf{P}_2(\mathsf{P}_1(x) \oplus x).$$

They proved PRF-security of EDM up to $O\left(2^{2n/3}\right)$ queries. Later, Dai et al. [14] improved this bound up to $O\left(2^{3n/4}\right)$ via the chi-squared method. Mennink and Neves [26] introduced a dual construction of EDM, dubbed Encrypted Davis-Meyer Dual (EDMD), defined as

$$\mathsf{EDMD}[\mathsf{P}_1, \mathsf{P}_2](x) \stackrel{\text{def}}{=} \mathsf{P}_2(\mathsf{P}_1(x)) \oplus \mathsf{P}_1(x).$$

They claimed both EDM and EDMD are secure up to (almost) 2^n queries. However, the proof depends on Patarin's Mirror theory, which has not been fully verified. Cogliati and Seurin [13] proved that the single permutation variant of EDM is secure up to $2^{2n/3}$ queries.

Summation-Truncation Hybrid. Gunsing and Mennink [19] proposed the so-called Summation Truncation Hybrid (STH) construction. The idea of this construction is concatenating outputs of two independent TRPs and sum of discarded bits from those TRPs. They proved that STH is asymptotically as secure as TRP, which implies that the use of discarded bits does not degrade the security.

Sum of Even-Mansour. Sum of Even-Mansour (SoEM) [8] is a PRF built from public permutations. When P_1 and P_2 are public permutations, the construction is defined as

$$\mathsf{SoEM}[\mathsf{P}_1, \mathsf{P}_2, k_1, k_2](x) \stackrel{\text{def}}{=} \mathsf{P}_1(x \oplus k_1) \oplus k_1 \oplus \mathsf{P}_2(x \oplus k_2) \oplus k_2,$$

where k_1 and k_2 are secret keys. The authors proved that SoEM with independent permutations and keys achieves $2n/3$-bit security, which is tight. They also proposed another PRF construction, dubbed SoKAC, however, Nandi [29] pointed out a flaw from the security proof of SoKAC and this construction is disclaimed.

1.2 Our Contribution

In this paper, we propose new Luby-Rackoff backward constructions: SaT1 and SaT2. Let P, P_1 and P_2 be n-bit permutations. For a positive integer m such that $m < n$, SaT1 and SaT2 are defined as follows (see Figure 1).

$$\begin{aligned} \mathsf{SaT1}[\mathsf{P}] : \{0,1\}^{n-1} &\longrightarrow \{0,1\}^m \\ x &\longmapsto \mathsf{Tr}_m(\mathsf{P}(0 \,\|\, x) \oplus \mathsf{P}(1 \,\|\, x)), \\ \mathsf{SaT2}[\mathsf{P}_1, \mathsf{P}_2] : \{0,1\}^{n} &\longrightarrow \{0,1\}^m \\ x &\longmapsto \mathsf{Tr}_m(\mathsf{P}_1(x) \oplus \mathsf{P}_2(x)). \end{aligned}$$

We also propose a variant of SoP[3] using three independent permutations, dubbed SoP3-2. For n-bit permutations P, P_1, P_2 and P_3, SoP3-1 and SoP3-2 are defined as follows (see Figure 2).

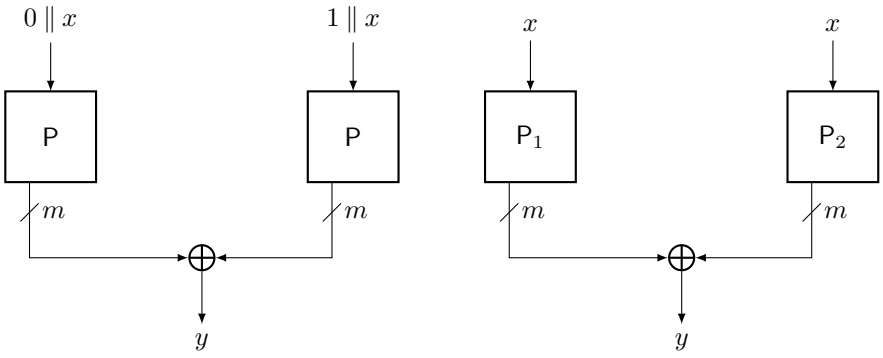
$$\begin{aligned} \mathsf{SoP3\text{-}1}[\mathsf{P}] : \{0,1\}^{n-2} &\longrightarrow \{0,1\}^n \\ x &\longmapsto \mathsf{P}(00 \,\|\, x) \oplus \mathsf{P}(01 \,\|\, x) \oplus \mathsf{P}(10 \,\|\, x), \\ \mathsf{SoP3\text{-}2}[\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3] : \{0,1\}^{n} &\longrightarrow \{0,1\}^n \\ x &\longmapsto \mathsf{P}_1(x) \oplus \mathsf{P}_2(x) \oplus \mathsf{P}_3(x). \end{aligned}$$

The multi-user security of SaT1, SaT2, and SoP3-2 is summarized in Table 1. Note that the single-user security bound of SaT1 and SaT2 can be obtained from our bound by setting $\mu = 1$, while the generic multi-user bound is obtained by multiplying μ to the single-user bound. Our security bound is proportional to $\mu^{1/2}$, which is better than the one from the hybrid argument.

SaT1 and SaT2 can be regarded as the sum of two TRPs. Also, SaT2 (resp. SaT1) can be obtained by truncating SoP (resp. SoP based on a single permutation with domain separation). If we apply our proof technique to TRP, the security bound would be

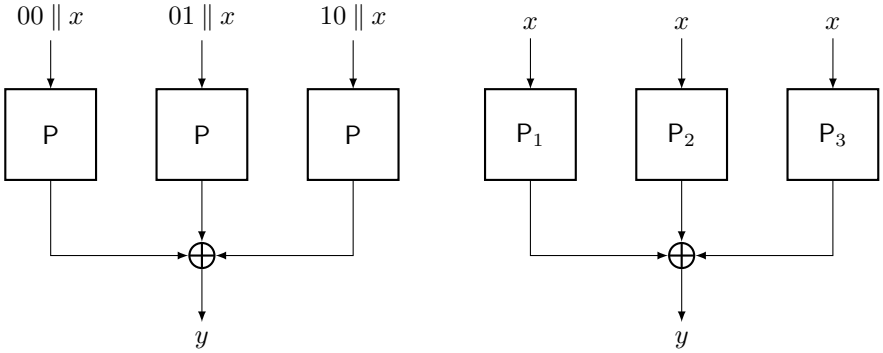
$$O\left(\frac{\sqrt{\mu} q_{\max}}{2^{n-\frac{m}{2}}}\right).$$

We omit the proof, but proving the above bound would be straightforward. TRP cannot achieve full security with respect to the permutation size in the multi-user setting. For $m = n/2$ and $\mu = O(2^{n/2})$, TRP is secure up to $O(2^{n/2})$ queries



(a) SaT1[P] (b) SaT2[$\mathsf{P}_1, \mathsf{P}_2$]

Fig. 1: SaT1 and SaT2 constructions



(a) SoP3-1[P] (b) SoP3-2[$\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$]

Fig. 2: SoP3-1 and SoP3-2 constructions

for each user, while SaT1 and SaT2 are secure up to $O(2^n)$ queries for each user. Compared to SoP3-1, SaT1 and SaT2 can be made more secure at the cost of a lower rate, or conversely, can be made more efficient according to the acceptable level of security or the number of users. If $\mu \ll 2^{n/3}$, SaT1 and SaT2 can allow $O(2^n)$ queries per user and the rate is higher than $n/3$ (the rate of SoP3-1) by setting $m = n - \log_2 \mu$.

As a concrete example, when $n = 128$, $m = 64$ and $\mu = 2^{64}$, both SaT1 and SaT2 are optimally secure, i.e., $(128 - \epsilon)$-bit secure for all $\mu = 2^{64}$ users, where ϵ is a small constant from our security bounds. If more output bits are needed, one can truncate only 16 bits (with $m = 112$), in which case SaT1 enjoys 80-bit security, and SaT2 is even better, enjoying 112-bit security. Hence, SaT2 outputs 112-bit blocks with 112-bit security, while SoP3-1 outputs 128-bit blocks

Construction	Security bound	Rate	Number of Keys	Reference
SaT1	$\sqrt{\mu q_{\max}}/2^{n-0.5m}$	$m/2$	1	Ours
SaT2	$\sqrt{\mu} q_{\max}^{1.5}/2^{2n-0.5m}$	$m/2$	2	Ours
SoP3-1	$\sqrt{\mu q_{\max}}/2^{n}$	$n/3$	1	[6]
SoP3-2	$\sqrt{\mu} q_{\max}^{2}/2^{2.5n}$	$n/3$	3	Ours

Table 1: Multi-user security and efficiency of SaT and SoP[3] constructions. Constants are ignored in the security bounds. μ is the number of users and $q_{\max}$ is the maximum number of queries per user. Rate is the number of output bits per permutation call.

with 128-bit security for 2^{64} users, at the cost of two primitive calls and three primitive calls, respectively.

When $\mu \gg O(2^{n-m})$, we note that SaT2 can accept significantly more queries than SaT1. We also see our security bound of SoP3-2 is better than SoP3-1, while the tightness of these security bounds is still open.

Proof Technique. Compared to SoP, it is not straightforward to compute the expectation of the χ^2-divergence for truncated values. We addressed this issue by modifying the domain over which the expectation is taken. Moreover, we had to precisely compute the expectation rather than loosely upper bounding it, which was possible by using more involved counting - we take into account almost all the terms appearing in our computation, and make them cancel out each other.

Application. The key-generation algorithm in AES-GCM-SIV [7,17,18] can be replaced by SaT1 or SaT2. GCM-SIV and other authenticated encryption schemes such as CWC+ [15] and SCM [10] use synthetic IVs derived from secure PRFs. We expect that those constructions would perform better in the multi-user setting when combined with SaT1 or SaT2, while proving their overall security would be an independent topic of interest.

2 Preliminaries

Notation. Throughout this paper, we fix positive integers n, m, and μ such that $m < n$ to denote the block size, the number of output bits (after truncation), and number of users, respectively. We denote 0^m (i.e., m-bit string of all zeros) by $\mathbf{0}$. Given a non-empty finite set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that x is chosen uniformly at random from $\mathcal{X}$. $|\mathcal{X}|$ means the number of elements in $\mathcal{X}$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. The set of all functions with domain $\{0,1\}^n$ and codomain $\{0,1\}^m$ is simply denoted by $\mathsf{Func}(n,m)$. For a keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ with key space $\mathcal{K}$ and non-empty sets $\mathcal{X}$ and $\mathcal{Y}$, we will denote $F(K,\cdot)$ by $F_K(\cdot)$ for $K \in \mathcal{K}$. A truncating function is defined as

follows:

$$\begin{aligned}\mathsf{Tr}_m : \{0,1\}^n &\longrightarrow \{0,1\}^m \\ x &\longmapsto x_L,\end{aligned}$$

where $x \in \{0,1\}^n$ is written as $x_L \parallel x_R$ for $x_L \in \{0,1\}^m$ and $x_R \in \{0,1\}^{n-m}$.

Multi-User Pseudorandom Function. Let $\mathsf{C} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$ be a keyed function with key space $\mathcal{K}$. We will consider an information theoretic distinguisher $\mathcal{A}$ that makes oracle queries to C, and returns a single bit. The advantage of $\mathcal{A}$ in breaking the mu-prf security of C, i.e., in distinguishing $\mathsf{C}(K_1,\cdot),\ldots,\mathsf{C}(K_\mu,\cdot)$ where $K_1,\ldots,K_\mu \leftarrow_\$ \mathcal{K}$ from uniformly chosen functions $\mathsf{F}_1,\ldots,\mathsf{F}_\mu \leftarrow_\$ \mathsf{Func}(n,m)$, is defined as

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(\mathcal{A}) = \Big|&\Pr\left[K_1,\ldots,K_\mu \leftarrow_\$ \mathcal{K} : \mathcal{A}^{\mathsf{C}_{K_1}(\cdot),\ldots,\mathsf{C}_{K_\mu}(\cdot)} = 1\right] \\ &- \Pr\left[\mathsf{F}_1,\ldots,\mathsf{F}_\mu \leftarrow_\$ \mathsf{Func}(n,m) : \mathcal{A}^{\mathsf{F}_1(\cdot),\ldots,\mathsf{F}_\mu(\cdot)} = 1\right]\Big|.\end{aligned}$$

We define $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(\mu, q_{\max}, t)$ as the maximum of $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{C}}(\mathcal{A})$ over all the distinguishers against C for μ users making at most $q_{\max}$ queries to each user and running in time at most t. When we consider information theoretic security, we will drop the parameter t.

Multi-User Pseudorandom Permutation. Let $\mathsf{E} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be an n-bit block cipher with key space $\mathcal{K}$. We will consider an information theoretic distinguisher $\mathcal{A}$ that makes oracle queries to E, and returns a single bit. The advantage of $\mathcal{A}$ in breaking the mu-prp security of E is defined as

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}prp}}_{\mathsf{E}}(\mathcal{A}) = \Big|&\Pr\left[K_1,\ldots,K_\mu \leftarrow_\$ \mathcal{K} : \mathcal{A}^{\mathsf{E}_{K_1}(\cdot),\ldots,\mathsf{E}_{K_\mu}(\cdot)} = 1\right] \\ &- \Pr\left[\mathsf{P}_1,\ldots,\mathsf{P}_\mu \leftarrow_\$ \mathsf{Perm}(n) : \mathcal{A}^{\mathsf{P}_1(\cdot),\ldots,\mathsf{P}_\mu(\cdot)} = 1\right]\Big|.\end{aligned}$$

Similarly to the mu-prf security, we define $\mathbf{Adv}^{\mathsf{mu\text{-}prp}}_{\mathsf{E}}(\mu, q_{\max}, t)$.

The Chi-squared Method. We give here all the necessary background on the chi-squared method [14] that we will use throughout this paper.

We fix a set of random systems, a deterministic distinguisher $\mathcal{A}$ that makes q oracle queries to one of the random systems, and a set Ω that contains all possible answers for oracle queries to the random systems. For a random system $\mathcal{S}$ and $i \in \{1,\ldots,q\}$, let $Z_{\mathcal{S},i}$ be the random variable over Ω that follows the distribution of the i-th answer obtained by $\mathcal{A}$ interacting with $\mathcal{S}$. Let

$$\mathbf{Z}^i_{\mathcal{S}} \stackrel{\text{def}}{=} (Z_{\mathcal{S},1},\ldots,Z_{\mathcal{S},i}),$$

and let

$$\mathsf{p}^i_{\mathcal{S}}(\mathbf{z}) \stackrel{\text{def}}{=} \Pr\left[\mathbf{Z}^i_{\mathcal{S}} = \mathbf{z}\right]$$

for $\mathbf{z} \in \Omega^i$. For $i \leq q$ and $\mathbf{z} = (z_1, \ldots, z_{i-1}) \in \Omega^{i-1}$ such that $\mathsf{p}_{\mathcal{S}}^{i-1}(\mathbf{z}) > 0$, the probability distribution of $Z_{\mathcal{S},i}$ conditioned on $\mathbf{Z}_{\mathcal{S}}^{i-1} = \mathbf{z}$ will be denoted $\mathsf{p}_{\mathcal{S},i}^{\mathbf{z}}(\cdot)$, namely for $z \in \Omega$,

$$\mathsf{p}_{\mathcal{S},i}^{\mathbf{z}}(z) \stackrel{\text{def}}{=} \Pr\left[Z_{\mathcal{S},i} = z \mid \mathbf{Z}_{\mathcal{S}}^{i-1} = \mathbf{z}\right].$$

For two random systems $\mathcal{S}_0$ and $\mathcal{S}_1$, and for $i < q$ and $\mathbf{z} = (z_1, \ldots, z_{i-1}) \in \Omega^{i-1}$ such that $\mathsf{p}_{\mathcal{S}_0}^{i-1}(\mathbf{z})$, $\mathsf{p}_{\mathcal{S}_1}^{i-1}(\mathbf{z}) > 0$, the χ^2-*divergence* for $\mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(\cdot)$ and $\mathsf{p}_{\mathcal{S}_1,i}^{\mathbf{z}}(\cdot)$ is defined as follows.

$$\chi^2\left(\mathsf{p}_{\mathcal{S}_1,i}^{\mathbf{z}}(\cdot), \mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(\cdot)\right) \stackrel{\text{def}}{=} \sum_{\substack{z \in \Omega \text{ such that} \\ \mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(z) > 0}} \frac{\left(\mathsf{p}_{\mathcal{S}_1,i}^{\mathbf{z}}(z) - \mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(z)\right)^2}{\mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(z)}.$$

We will simply write $\chi^2(\mathbf{z}) = \chi^2\left(\mathsf{p}_{\mathcal{S}_1,i}^{\mathbf{z}}(\cdot), \mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(\cdot)\right)$ when the random systems are clear from the context. If the support of $\mathsf{p}_{\mathcal{S}_1}^{i-1}(\cdot)$ is contained in the support of $\mathsf{p}_{\mathcal{S}_0}^{i-1}(\cdot)$, then we can view $\chi^2\left(\mathsf{p}_{\mathcal{S}_1,i}^{\mathbf{z}}(\cdot), \mathsf{p}_{\mathcal{S}_0,i}^{\mathbf{z}}(\cdot)\right)$ as a random variable, denoted $\chi^2\left(\mathbf{Z}_{\mathcal{S}_1}^{i-1}\right)$, where $\mathbf{z}$ follows the distribution of $\mathbf{Z}_{\mathcal{S}_1}^{i-1}$.

Then $\mathcal{A}$'s distinguishing advantage is upper bounded by the *total variation distance* of $\mathsf{p}_{\mathcal{S}_0}^q(\cdot)$ and $\mathsf{p}_{\mathcal{S}_1}^q(\cdot)$, denoted $\|\mathsf{p}_{\mathcal{S}_0}^q(\cdot) - \mathsf{p}_{\mathcal{S}_1}^q(\cdot)\|$, and we also have

$$\|\mathsf{p}_{\mathcal{S}_0}^q(\cdot) - \mathsf{p}_{\mathcal{S}_1}^q(\cdot)\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}\left[\chi^2\left(\mathbf{Z}_{\mathcal{S}_1}^{i-1}\right)\right]\right)^{\frac{1}{2}}. \tag{1}$$

See [14] for the proof of (1).

3 Summation-and-Truncation

In this section, we propose new PRF constructions based on PRPs. We will prove that these constructions are fully secure (secure after almost 2^n queries made for each user) with 2^{n-m} users. Let

$$\begin{aligned} \mathsf{SaT1}[\mathsf{P}] : \{0,1\}^{n-1} &\longrightarrow \{0,1\}^m \\ x &\longmapsto \mathsf{Tr}_m(\mathsf{P}(0 \,\|\, x) \oplus \mathsf{P}(1 \,\|\, x)) \end{aligned}$$

where Tr_m is defined in Section 2 and P is an n-bit random permutation from $\mathsf{Perm}(n)$. The mu-prf security of $\mathsf{SaT1}$ is represented by the following theorem.

Theorem 1. *Let n, m, μ, and q_{max} be positive integers such that $m < n$ and $q_{\max} \leq 2^{n-3}$. Then one has*

$$\mathbf{Adv}_{\mathsf{SaT1}}^{\mathsf{mu\text{-}prf}}(\mu, q_{\max}) \leq \left(\frac{20\mu q_{\max}^3}{2^{4n-m}} + \frac{21\mu q_{\max}}{2^{2n-m}}\right)^{\frac{1}{2}}.$$

The proof is given in Section 4.

Remark 1. When $m = n$, it is well known that the mu-prf advantage of SaT1 (equivalently, SoP) is about $\mu q_{\max}/2^n$ since SaT1 never outputs $\mathbf{0}$ which is distinguished from a random function.

We also define SaT2 which is a variant of SaT1 on two independent random permutations. Let

$$\begin{aligned}\mathsf{SaT2}[\mathsf{P}_1, \mathsf{P}_2] : \{0,1\}^n &\longrightarrow \{0,1\}^m \\ x &\longmapsto \mathsf{Tr}_m(\mathsf{P}_1(x) \oplus \mathsf{P}_2(x))\end{aligned}$$

where Tr_m is defined in Section 2 and P_1 and P_2 are two independent random permutations from $\mathsf{Perm}(n)$. The mu-prf security of SaT2 is represented by the following theorem.

Theorem 2. *Let n, m, μ, and q_{max} be positive integers such that $m \leq n$ and $q_{\max} \leq 2^{n-2}$. Then one has*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{SaT2}}(\mu, q_{\max}) \leq \left(\frac{2\mu q_{\max}^3}{2^{4n-m}}\right)^{\frac{1}{2}}.$$

The proof is given in Section 5.

One can consider SaT1 and SaT2 based on an n-bit block cipher $\mathsf{E} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ with key space $\mathcal{K}$, which is defined as

- For $x \in \{0,1\}^{n-1}$ and $K \in \mathcal{K}$,

$$\mathsf{SaT1}[\mathsf{E}](K, x) = \mathsf{Tr}_m(\mathsf{E}_K(0 \,\|\, x) \oplus \mathsf{E}_K(1 \,\|\, x));$$

- For $x \in \{0,1\}^n$ and $K_1, K_2 \in \mathcal{K}$,

$$\mathsf{SaT2}[\mathsf{E}](K_1, K_2, x) = \mathsf{Tr}_m(\mathsf{E}_{K_1}(x) \oplus \mathsf{E}_{K_2}(x)).$$

Up to the mu-prp security of E, one can derive the multi-user security of SaT1[E] and SaT2[E].

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{SaT1[E]}}(\mu, q_{\max}, t) \leq \mathbf{Adv}^{\mathsf{mu\text{-}prp}}_{\mathsf{E}}(\mu, 2q_{\max}, t') + \left(\frac{20\mu q_{\max}^3}{2^{4n-m}} + \frac{21\mu q_{\max}}{2^{2n-m}}\right)^{\frac{1}{2}},$$

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{SaT2[E]}}(\mu, q_{\max}, t) \leq \mathbf{Adv}^{\mathsf{mu\text{-}prp}}_{\mathsf{E}}(2\mu, q_{\max}, t') + \left(\frac{2\mu q_{\max}^3}{2^{4n-m}}\right)^{\frac{1}{2}}$$

where $t' \approx t + 2\mu q_{\max}$.

4 Proof of Theorem 1

Before proving the security of SaT1, we define random experiments to make it possible to prove it with the chi-squared method in Algorithm 1.

Algorithm 1 Experiments for SaT1

Experiment $\mathcal{B}_0$

for $j \leftarrow 1$ to μ **do**
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^m$
  $\mathbf{Z}^j \leftarrow (y_1^j, \cdots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{B}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_{2i-1}^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_{2i-1}^j\}$
    $u_{2i}^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_{2i}^j\}$
    $r_{2i-1}^j \leftarrow \mathsf{Tr}_m(u_{2i-1}^j)$, $r_{2i}^j \leftarrow \mathsf{Tr}_m(u_{2i}^j)$
    $y_i^j \leftarrow r_{2i-1}^j \oplus r_{2i}^j$
  $\mathbf{Z}^j \leftarrow (y_1^j, \cdots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_0$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^m$
    $\mathcal{T}_i^j(y_i^j) \leftarrow \{(u,v) : u, v \in \mathcal{R}_u, u \neq v, \mathsf{Tr}_m(u \oplus v) = y_i^j\}$
    if $\left|\mathcal{T}_i^j(y_i^j)\right| > 0$ **then**
      $(u_{2i-1}^j, u_{2i}^j) \leftarrow_{\$} \mathcal{T}_i^j(y_i^j)$
    else
      $(u_{2i-1}^j, u_{2i}^j) \leftarrow (\perp, \perp)$
    $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_{2i-1}^j, u_{2i}^j\}$
    $r_{2i-1}^j \leftarrow \mathsf{Tr}_m(u_{2i-1}^j)$, $r_{2i}^j \leftarrow \mathsf{Tr}_m(u_{2i}^j)$
    $z_i^j \leftarrow (r_{2i-1}^j, y_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \cdots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_{2i-1}^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_{2i-1}^j\}$
    $u_{2i}^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_{2i}^j\}$
    $r_{2i-1}^j \leftarrow \mathsf{Tr}_m(u_{2i-1}^j)$, $r_{2i}^j \leftarrow \mathsf{Tr}_m(u_{2i}^j)$
    $y_i^j \leftarrow r_{2i-1}^j \oplus r_{2i}^j$
    $z_i^j \leftarrow (r_{2i-1}^j, y_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \cdots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \cdots, \mathbf{Z}^\mu)$

The main purpose of the algorithm is to transform the distinguishing game between $\mathcal{S}_0$ and $\mathcal{S}_1$ into the game between $\mathcal{C}_0$ and $\mathcal{C}_1$ (see equation (2)) in order to evaluate the distinguishing advantage using the chi-squared method. The game between $\mathcal{C}_0$ and $\mathcal{C}_1$ has two major differences from the game between $\mathcal{S}_0$ and $\mathcal{S}_1$:

1. $\mathcal{C}_0$ and $\mathcal{C}_1$ take no input, which can be seen as a reduction from an adaptive adversary to a non-adaptive adversary and this reduction makes it easy to apply the chi-squared method.
2. The outputs of $\mathcal{C}_0$ and $\mathcal{C}_1$ have additional information, namely r^j_{2i-1}.

Note that $\mathcal{B}_0$ and $\mathcal{B}_1$ are intermediate games that yield equation (2).

For Experiment $\mathcal{C}_0$ in Algorithm 1, the following lemma holds.

Lemma 1. *For any $q_{\max} \leq 2^{n-3}$, Experiment $\mathcal{C}_0$ in Algorithm 1 never returns $(\perp, \perp)$.*

Proof. We suppose any $j \in [\mu]$ and omit j for simplicity. If $i = 1$, it is trivial that $|\mathcal{T}_i(y_i)| > 0$ since $|\mathcal{T}_i(y_i)| = 2^n(2^{n-m} - 1)$ for $y_i = \mathbf{0}$ and $|\mathcal{T}_i(y_i)| = 2^{2n-m}$ for $y_i \neq \mathbf{0}$. For $2 \leq i \leq q_{\max}$, we have $|\mathcal{R}_u| = 2^n - 2(i-1)$ and therefore $|\mathcal{T}_i(y_i)| \geq 2^{2n-m} - (4i-3)2^{n-m} > 0$ since $i \leq q_{\max} \leq 2^{n-3}$ by our assumption. □

Let $\mathcal{S}_0$ be a random oracle with $\mathsf{Func}(n-1, m)$ and $\mathcal{S}_1$ be a random oracle with $\mathsf{SaT1}$. It is obvious that transcripts for $\mathcal{S}_0$ (or $\mathcal{S}_1$) has same probability distribution with the output of $\mathcal{B}_0$ (or $\mathcal{B}_1$). Secondly, statistical distance between $\mathcal{C}_0$ and $\mathcal{C}_1$ is larger than statistical distance between $\mathcal{B}_0$ and $\mathcal{B}_1$ since the outputs of $\mathcal{C}_0$ (or $\mathcal{C}_1$) contains the outputs of $\mathcal{B}_0$ (or $\mathcal{B}_1$), respectively. The two facts make following inequality to be held.

$$\|\mathsf{p}^q_{\mathcal{S}_0}(\cdot) - \mathsf{p}^q_{\mathcal{S}_1}(\cdot)\| = \|\mathsf{p}^q_{\mathcal{B}_0}(\cdot) - \mathsf{p}^q_{\mathcal{B}_1}(\cdot)\| \leq \|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\|. \tag{2}$$

By (2) and lemma 2, we can prove theorem 1.

Lemma 2. *For any $q_{\max} \leq 2^{n-3}$, let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the experiments described in Algorithm 1. Then we have*

$$\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| \leq \left(\frac{20\mu q^3_{\max}}{2^{4n-m}} + \frac{21\mu q_{\max}}{2^{2n-m}}\right)^{\frac{1}{2}}.$$

4.1 Proof of Lemma 2

Let $q = \mu q_{\max}$. For $i \in [q]$ where $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$, the response of the i-th query is seen as $z_i = z^j_k$. Then, we can easily check that the support of $\mathsf{p}^{i-1}_{\mathcal{C}_1}(\cdot)$ is contained in the support of $\mathsf{p}^{i-1}_{\mathcal{C}_0}(\cdot)$ for $i = 1, \ldots, q$, allowing us to use the chi-squared method.

Let $\Omega = \{0,1\}^m \times \{0,1\}^m$. For fixed $i \in \{1,\ldots,q\}$ and $\mathbf{z} \in \Omega^{i-1}$ such $\mathsf{p}^{i-1}_{\mathcal{C}_1}(\mathbf{z}) > 0$, we will compute

$$\begin{aligned}\chi^2(\mathbf{z}) &= \sum_{\substack{z\in\Omega \text{ such that} \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \frac{\left(\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z) - \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\right)^2}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)} \\ &= \sum_{\substack{z\in\Omega \text{ such that} \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\left(1 - \frac{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z)}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)}\right)^2\end{aligned}$$

Firstly, note that $\mathbf{z} = (z_1,\ldots,z_{i-1})$ and $z_l = (r_{2l-1}, y_l)$ for $l = 1,\ldots,i-1$. Let $\hat{\Omega} = \{0,1\}^n \times \{0,1\}^n$, $h_l = (u_{2l-1}, y'_l) \in \hat{\Omega}$ and $\mathbf{h} = (h_1,\ldots,h_{i-1})$ for $l = 1,\ldots,i-1$. Note that $\mathbf{h}$ includes $\mathbf{z}$. Let $H_{\mathcal{C}_1,i}$ be the random variable over $\hat{\Omega}$ that follows the distribution of the internal values (u,y') in $\mathcal{C}_1$ interacting the i-th query by $\mathcal{A}$. Let

$$\mathbf{H}^{i-1}_{\mathcal{C}_1} \stackrel{\text{def}}{=} (H_{\mathcal{C}_1,1},\ldots,H_{\mathcal{C}_1,i-1})$$

for $\mathbf{h} \in \hat{\Omega}^{i-1}$. For a fixed $\mathbf{z} = ((r_1,y_1),(r_3,y_2),\ldots,(r_{2i-3},y_{i-1}))$, we denote $\mathbf{h} \vdash \mathbf{z}$ if and only if $h_l = (u_{2l-1}, y'_l)$ satisfies $\mathsf{Tr}_m(u_{2l-1}) = r_{2l-1}$ and $\mathsf{Tr}_m(y'_l) = y_l$ for all $l = 1,\ldots,i-1$, where $\mathbf{h} = (h_1,h_2,\ldots,h_{i-1})$. Then one has

$$\begin{aligned}\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\chi^2(\mathbf{z})\right] &= \sum_{\mathbf{z}\in\Omega^{i-1}} \mathsf{p}^{i}_{\mathcal{C}_1}(\mathbf{z})\cdot\chi^2(\mathbf{z}) \\ &= \sum_{\mathbf{z}\in\Omega^{i-1}} \sum_{\substack{\mathbf{h}\in\hat{\Omega}^{i-1} \text{ such} \\ \text{that } \mathbf{h}\vdash\mathbf{z}}} \mathsf{p}^{i}_{\mathcal{C}_1}(\mathbf{z})\cdot\Pr\left[\mathbf{H}^{i-1}_{\mathcal{C}_1} = \mathbf{h} \mid \mathbf{Z}^{i-1}_{\mathcal{C}_1} = \mathbf{z}\right]\cdot\chi^2(\mathbf{z}) \\ &= \sum_{\mathbf{h}\in\hat{\Omega}^{i-1}} \Pr\left[\mathbf{H}^{i-1}_{\mathcal{C}_1} = \mathbf{h}\right]\cdot\chi^2(\mathbf{z}) \\ &= \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\chi^2(\mathbf{z})\right] \qquad (3)\end{aligned}$$

where the last expectation is taken over the distribution $\mathbf{H}^{i-1}_{\mathcal{C}_1}$. Furthermore, let $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$. For $\alpha \in \{0,1\}^m$, we define $U^j_k(\alpha)$ as the number of elements α in $(r^j_l)_{l=1,\ldots,2k-2}$. In other words,

$$U^j_k(\alpha) = \left|\{l \in [2k-2] \mid \alpha = r^j_l\}\right|.$$

Also, for $y \in \{0,1\}^m$, let $T^j_k(y) = \left|\mathcal{T}^j_k(y)\right|$. Note that, for any $j' \in [j-1]$, z_i is independent with $\mathbf{Z}^{j'}$. Therefore, we see that, for $y = \mathbf{0}$,

$$\begin{aligned}\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,\mathbf{0}) &= \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r) - 1)}{2^m T^j_k(\mathbf{0})}, \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(r,\mathbf{0}) &= \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r) - 1)}{(2^n - 2k + 2)(2^n - 2k + 1)},\end{aligned}$$

and otherwise ($y \neq \mathbf{0}$),

$$\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,y) = \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r \oplus y))}{2^m T^j_k(y)},$$
$$\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(r,y) = \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r \oplus y))}{(2^n - 2k + 2)(2^n - 2k + 1)}.$$

For any $y \in \{0,1\}^m$,

$$\begin{aligned} T^j_k(y) &\geq \sum_{\alpha \in \{0,1\}^m} (2^{n-m} - U^j_k(\alpha))(2^{n-m} - U^j_k(\alpha \oplus y) - 1) \\ &\geq 2^{2n-m} - (4k-3)2^{n-m}. \end{aligned}$$

Let

$$G^j_k(y) \stackrel{\text{def}}{=} \left(\frac{(2^n - 2k + 2)_2}{2^m} - T^j_k(y) \right)^2.$$

Then we have,

$$\begin{aligned} \chi^2(\mathbf{z}) = &\sum_{\substack{z=(r,y)\in\Omega \text{ such that} \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0 \text{ and } y\neq\mathbf{0}}} \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r \oplus y))}{2^m T^j_k(y)} \left(1 - \frac{2^m T^j_k(y)}{(2^n - 2k + 2)_2}\right)^2 \\ &+ \sum_{\substack{z=(r,\mathbf{0})\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \frac{(2^{n-m} - U^j_k(r))(2^{n-m} - U^j_k(r) - 1)}{2^m T^j_k(\mathbf{0})} \left(1 - \frac{2^m T^j_k(\mathbf{0})}{(2^n - 2k + 2)_2}\right)^2 \\ \leq &\sum_{\substack{(r,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,y)>0}} \frac{2^{2n-2m}\left((2^n - 2k + 2)_2 - 2^m T^j_k(y)\right)^2}{2^m T^j_k(y)\left((2^n - 2k + 2)_2\right)^2} \\ \leq &\sum_{y\in\{0,1\}^m} \frac{7 G^j_k(y)}{2^{4n-m}}. \end{aligned} \tag{4}$$

since $k \leq q_{\max} \leq 2^{n-3}$. We claim the following lemma.

Lemma 3. *For any $y \neq \mathbf{0}$, one has*

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G^j_k(y)\right] \leq \frac{8(k-1)^2}{2^m} + 3 \cdot 2^{2n-2m},$$
$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G^j_k(\mathbf{0})\right] \leq 8(k-1)^2 + 3 \cdot 2^{2n}.$$

The proof of Lemma 3 is deferred to Section 7.1. From (4) and Lemma 3, it follows that

$$\begin{aligned}\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\chi^2(\mathbf{z})\right] &\le \frac{7}{2^{4n-m}}\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\sum_{y\in\{0,1\}^m\setminus\mathbf{0}} G_k^j(y)\right) + G_k^j(\mathbf{0})\right] \\ &\le \frac{112(k-1)^2}{2^{4n-m}} + \frac{42}{2^{2n-m}}\end{aligned}$$

and finally, we have

$$\begin{aligned}\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| &\le \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\le \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}}\mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\le \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}}\frac{112(k-1)^2}{2^{4n-m}} + \frac{42}{2^{2n-m}}\right)^{\frac{1}{2}} \\ &\le \left(\frac{20\mu q_{\max}^3}{2^{4n-m}} + \frac{21\mu q_{\max}}{2^{2n-m}}\right)^{\frac{1}{2}}.\end{aligned}$$

5 Proof of Theorem 2

Similarly to Section 4, we define random experiments. See Algorithm 2. For Experiment $\mathcal{C}_0$ in Algorithm 2, the following lemma holds.

Lemma 4. *For any $q_{\max} \le 2^{n-2}$, Experiment $\mathcal{C}_0$ in Algorithm 2 never returns $(\perp, \perp)$.*

Proof. We suppose any $j \in [\mu]$ and omit y for simplicity. If $i = 1$, it is trivial that $|\mathcal{T}_i(y_i)| = 2^{2n-m} > 0$. For $2 \le i \le q_{\max}$, we have $\left|\mathcal{R}^U\right| = \left|\mathcal{R}^V\right| = 2^n - (i-1)$ and therefore $|\mathcal{T}_i(y_i)| \ge 2^{2n-m} - 2(i-1)2^{n-m} > 0$ since $i \le q_{\max} \le 2^{n-2}$ by our assumption. □

Let $\mathcal{S}_0$ be a random oracle with $\mathsf{Func}(n, m)$ and $\mathcal{S}_1$ be a random oracle with $\mathsf{SaT2}$. Similarly to the reasoning of (2), one has

$$\|\mathsf{p}^q_{\mathcal{S}_0}(\cdot) - \mathsf{p}^q_{\mathcal{S}_1}(\cdot)\| = \|\mathsf{p}^q_{\mathcal{B}_0}(\cdot) - \mathsf{p}^q_{\mathcal{B}_1}(\cdot)\| \le \|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\|. \tag{5}$$

By (5) and lemma 5, we can prove theorem 2.

Lemma 5. *For any $q_{\max} \le 2^{n-2}$, let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the experiments described in Algorithm 2. Then we have*

$$\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| \le \left(\frac{2\mu q_{\max}^3}{2^{4n-m}}\right)^{\frac{1}{2}}.$$

Algorithm 2 Experiments for SaT2

Experiment $\mathcal{B}_0$

for $j \leftarrow 1$ to μ **do**
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^m$
  $\mathbf{Z}^j \leftarrow (y_1^j, \ldots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{B}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_i^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$
    $v_i^j \leftarrow_{\$} \mathcal{R}_v$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$
    $r_i^j \leftarrow \mathsf{Tr}_m(u_i^j)$, $s_i^j \leftarrow \mathsf{Tr}_m(v_i^j)$
    $y_i^j \leftarrow r_i^j \oplus s_i^j$
  $\mathbf{Z}^j \leftarrow (y_1^j, \ldots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_0$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^m$
    $\mathcal{T}_i^j(y_i^j) \leftarrow \{(u,v) : u \in \mathcal{R}_u, v \in \mathcal{R}_v, \mathsf{Tr}_m(u \oplus v) = y_i^j\}$
    if $\left|\mathcal{T}_i^j(y_i^j)\right| > 0$ **then**
      $(u_i^j, v_i^j) \leftarrow_{\$} \mathcal{T}_i^j(y_i^j)$
    else
      $(u_i^j, v_i^j) \leftarrow (\perp, \perp)$
    $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$
    $r_i^j \leftarrow \mathsf{Tr}_m(u_i^j)$, $s_i^j \leftarrow \mathsf{Tr}_m(v_i^j)$
    $z_i^j \leftarrow (r_i^j, y_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \ldots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_i^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$
    $v_i^j \leftarrow_{\$} \mathcal{R}_v$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$
    $r_i^j \leftarrow \mathsf{Tr}_m(u_i^j)$, $s_i^j \leftarrow \mathsf{Tr}_m(v_i^j)$
    $y_i^j \leftarrow r_i^j \oplus s_i^j$
    $z_i^j \leftarrow (r_i^j, y_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \ldots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

5.1 Proof of Lemma 5

Let $q = \mu q_{\max}$. For $i \in [q]$, where $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$, the response of the i-th query is seen as $z_i = z_k^j$. Then, we can easily check that the support of $\mathsf{p}_{\mathcal{C}_1}^{i-1}(\cdot)$ is contained in the support of $\mathsf{p}_{\mathcal{C}_0}^{i-1}(\cdot)$ for $i = 1, \ldots, q$, allowing us to use the chi-squared method. Let $\Omega = \{0,1\}^m \times \{0,1\}^m$. For fixed $i \in \{1, \ldots, q\}$ and $\mathbf{z} \in \Omega^{i-1}$ such $\mathsf{p}_{\mathcal{C}_1}^{i-1}(\mathbf{z}) > 0$, we will compute

$$\begin{aligned}\chi^2(\mathbf{z}) &= \sum_{\substack{z \in \Omega \text{ such that} \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z) > 0}} \frac{\left(\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z) - \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\right)^2}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)} \\ &= \sum_{\substack{z \in \Omega \text{ such that} \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z) > 0}} \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z) \left(1 - \frac{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z)}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)}\right)^2\end{aligned}$$

Firstly, note that $\mathbf{z} = (z_1, \ldots, z_{i-1})$ and $z_l = (r_l, y_l)$ for $l = 1, \ldots, i-1$. Let $\hat{\Omega} = \{0,1\}^n \times \{0,1\}^n$, $h_l = (u_l, y'_l) \in \hat{\Omega}$ and $\mathbf{h} = (h_1, \ldots, h_{i-1})$ for $l = 1, \ldots, i-1$. Let $H_{\mathcal{C}_1,i}$ be the random variable over $\hat{\Omega}$ that follows the distribution of the internal values (u, y') in $\mathcal{C}_1$ interacting the i-th query by $\mathcal{A}$. Let

$$\mathbf{H}_{\mathcal{C}_1}^{i-1} \stackrel{\text{def}}{=} (H_{\mathcal{C}_1,1}, \ldots, H_{\mathcal{C}_1,i-1})$$

for $\mathbf{h} \in \hat{\Omega}^{i-1}$. Similarly to (3), one has

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\chi^2(\mathbf{z})\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\chi^2(\mathbf{z})\right]$$

where the last expectation is taken over the distribution $\mathbf{H}_{\mathcal{C}_1}^{i-1}$. Furthermore, let $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$. For $\alpha \in \{0,1\}^m$, we define $U_k^j(\alpha)$ and $V_k^j(\alpha)$ be the number of elements α in $(r_l^j)_{l=1,\ldots,k-1}$ and $(s_l^j)_{l=1,\ldots,k-1}$, respectively. In other words,

$$\begin{aligned}U_k^j(\alpha) &= \left|\left\{l \in [k-1] \mid \alpha = r_l^j\right\}\right|, \\ V_k^j(\alpha) &= \left|\left\{l \in [k-1] \mid \alpha = s_l^j\right\}\right|.\end{aligned}$$

Also, for $y \in \{0,1\}^m$, let $T_k^j(y) = \left|\mathcal{T}_k^j(y)\right|$. Note that, for any $j' \in [j-1]$, z_i is independent with $\mathbf{Z}^{j'}$. Therefore, we see that

$$\begin{aligned}\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,y) &= \frac{(2^{n-m} - U_k^j(r))(2^{n-m} - V_k^j(r \oplus y))}{2^m T_k^j(y)}, \\ \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(r,y) &= \frac{(2^{n-m} - U_k^j(r))(2^{n-m} - V_k^j(r \oplus y))}{(2^n - k + 1)^2},\end{aligned}$$

and

$$\begin{aligned} T_k^j(y) &= \sum_{\alpha\in\{0,1\}^m} (2^{n-m} - U_k^j(\alpha))(2^{n-m} - V_k^j(\alpha\oplus y)) \\ &= 2^{2n-m} - 2(k-1)2^{n-m} + \sum_{\alpha\in\{0,1\}^m} U_k^j(\alpha)V_k^j(\alpha\oplus y) \\ &\geq 2^{2n-m} - 2(k-1)2^{n-m}. \end{aligned}$$

Therefore,

$$\begin{aligned} \chi^2(\mathbf{z}) &= \sum_{\substack{z=(r,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \frac{(2^{n-m} - U_k^j(r))(2^{n-m} - V_k^j(r\oplus y))}{2^m T_k^j(y)} \left(1 - \frac{2^m T_k^j(y)}{(2^n-k+1)^2}\right)^2 \\ &\leq \sum_{\substack{(r,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,y)>0}} \frac{2^{2n-2m}\left((2^n-k+1)^2 - 2^m T_k^j(y)\right)^2}{2^m T_k^j(y)(2^n-k+1)^4} \\ &\leq \sum_{\substack{(r,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(r,y)>0}} \frac{7\left((2^n-k+1)^2 - 2^m T_k^j(y)\right)^2}{2^{4n+2m}} \\ &\leq \sum_{y\in\{0,1\}^m} \frac{7}{2^{4n-m}} \left(\frac{(2^n-k+1)^2}{2^m} - T_k^j(y)\right)^2. \end{aligned} \tag{6}$$

since $k \leq q_{\max} \leq 2^{n-2}$. We claim the following lemma.

Lemma 6. *One has*

$$\begin{aligned} \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[T_k^j(y)\right] &= \frac{(2^n-k+1)^2}{2^m}, \\ \mathop{\mathbf{Var}}_{\mathbf{h}}\left[T_k^j(y)\right] &\leq \frac{(k-1)^2}{2^m}. \end{aligned}$$

The proof of Lemma 6 is deferred to Section 7.2. From (6) and Lemma 6, it follows that

$$\begin{aligned} \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\chi^2(\mathbf{z})\right] &\leq \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{y\in\{0,1\}^m} \frac{7}{2^{4n-m}} \left(\frac{(2^n-k+1)^2}{2^m} - T_k^j(y)\right)^2\right] \\ &\leq \frac{7}{2^{4n-m}} \sum_{y\in\{0,1\}^m} \mathop{\mathbf{Var}}_{\mathbf{h}}\left[T_k^j(y)\right] \\ &\leq \frac{7(k-1)^2}{2^{4n-m}} \end{aligned}$$

and finally, we have

$$\begin{aligned}\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| &\le \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\le \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}} \mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\le \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}} \frac{7(k-1)^2}{2^{4n-m}}\right)^{\frac{1}{2}} \\ &\le \left(\frac{2\mu q_{\max}^3}{2^{4n-m}}\right)^{\frac{1}{2}}.\end{aligned}$$

6 Multi-user PRF security of SoP3-2

In this section, we prove the security of SoP3-2. Bhattacharya and Nandi [6] proved mu-prf advantage of SoP3-1 is upper bounded by

$$\frac{20\sqrt{\mu q_{\max}}}{2^n}$$

for all $q_{\max} \le 2^n/12$. However, to the best of our knowledge, the security of SoP3-2 has not been analyzed. Let

$$\begin{aligned}\mathsf{SoP3\text{-}2}[\mathsf{P}_1,\mathsf{P}_2,\mathsf{P}_3] : \{0,1\}^n &\longrightarrow \{0,1\}^n \\ x &\longmapsto \mathsf{P}_1(x) \oplus \mathsf{P}_2(x) \oplus \mathsf{P}_3(x)\end{aligned}$$

where P_1, P_2 and P_3 are three independent random permutations from $\mathsf{Perm}(n)$. The mu-prf security of SoP3-2 is represented by the following theorem.

Theorem 3. *Let n, μ, and $q_{\max}$ be positive integers such that $q_{\max} \le 2^{n-2}$. Then one has*

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{SoP3\text{-}2}}(\mu, q_{\max}) \le \left(\frac{3\mu q_{\max}^4}{2^{5n}}\right)^{\frac{1}{2}}.$$

One can consider SoP3-2 based on an n-bit block cipher $\mathsf{E} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ with key space $\mathcal{K}$, which is defined as

$$\mathsf{SoP3\text{-}2}[\mathsf{E}](K_1, K_2, K_3, x) = \mathsf{E}_{K_1}(x) \oplus \mathsf{E}_{K_2}(x) \oplus \mathsf{E}_{K_3}(x).$$

Up to the mu-prp security of E, one can derive the multi-user security of SoP3-2[E].

$$\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{SoP3\text{-}2[E]}}(\mu, q_{\max}, t) \le \mathbf{Adv}^{\mathsf{mu\text{-}prp}}_{\mathsf{E}}(3\mu, q_{\max}, t') + \left(\frac{3\mu q_{\max}^4}{2^{5n}}\right)^{\frac{1}{2}}.$$

where $t' \approx t + 3\mu q_{\max}$.

6.1 Proof of Theorem 3

Similarly to Section 4, we define random experiments. See Algorithm 3. For Experiment $\mathcal{C}_0$ in Algorithm 3, the following lemma holds.

Lemma 7. *For any $q_{\max} \leq 2^{n-2}$, Experiment $\mathcal{C}_0$ in Algorithm 3 never returns $(\perp, \perp, \perp)$.*

Proof. We suppose any $j \in [\mu]$ and omit y for simplicity. If $i = 1$, it is trivial that $|\mathcal{T}_i(y_i)| = 2^{2n} > 0$. For $2 \leq i \leq q_{\max}$, we have $|\mathcal{R}_U| = |\mathcal{R}_V| = |\mathcal{R}_W| = 2^n - (i-1)$ and therefore $|\mathcal{T}_i(y_i)| \geq 2^{2n} - 3(i-1) \cdot 2^n > 0$ since $i \leq q_{\max} \leq 2^{n-2}$ by our assumption. □

Let $\mathcal{S}_0$ be a random oracle with $\mathsf{Func}(n, n)$ and $\mathcal{S}_1$ be a random oracle with SoP3-2. Similarly to the reasoning of (2), one has

$$\|\mathsf{p}^q_{\mathcal{S}_0}(\cdot) - \mathsf{p}^q_{\mathcal{S}_1}(\cdot)\| = \|\mathsf{p}^q_{\mathcal{B}_0}(\cdot) - \mathsf{p}^q_{\mathcal{B}_1}(\cdot)\| \leq \|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\|. \tag{7}$$

By (7) and lemma 8, we can prove theorem 3.

Lemma 8. *For any $q_{\max} \leq 2^{n-2}$, let $\mathcal{C}_0$ and $\mathcal{C}_1$ be the experiments described in Algorithm 3. Then we have*

$$\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| \leq \left(\frac{3\mu q^4_{\max}}{2^{5n}}\right)^{\frac{1}{2}}.$$

6.2 Proof of Lemma 8

Let $q = \mu q_{\max}$. For $i \in [q]$ where $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$, the response of the i-th query is seen as $z_i = z^j_k$. We can easily check that the support of $\mathsf{p}^{i-1}_{\mathcal{C}_1}(\cdot)$ is contained in the support of $\mathsf{p}^{i-1}_{\mathcal{C}_0}(\cdot)$ for $i = 1, \ldots, q$, allowing us to use the chi-squared method. Let $\Omega = \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$.

For a fixed $i \in \{1, \ldots, q\}$, let $i \in [q]$ where $i = (j-1)q_{\max} + k$ such that $j \in [\mu]$ and $k \in [q_{\max}]$. Fix $\mathbf{z} \in \Omega^{i-1}$ such that $\mathsf{p}^{i-1}_{\mathcal{C}_1}(\mathbf{z}) > 0$. Then, we will compute

$$\begin{aligned}
\chi^2(\mathbf{z}) &= \sum_{\substack{z=(u,v,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \frac{\left(\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z) - \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\right)^2}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)} \\
&= \sum_{\substack{z=(u,v,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)>0}} \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)\left(1 - \frac{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_1,i}(z)}{\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_0,i}(z)}\right)^2
\end{aligned}$$

Algorithm 3 Experiments for SoP3-2

Experiment $\mathcal{B}_0$

for $j \leftarrow 1$ to μ **do**
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^n$
  $\mathbf{Z}^j \leftarrow (y_1^j, \ldots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{B}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v, \mathcal{R}_w \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_i^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$
    $v_i^j \leftarrow_{\$} \mathcal{R}_v$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$
    $w_i^j \leftarrow_{\$} \mathcal{R}_w$, $\mathcal{R}_w \leftarrow \mathcal{R}_w \setminus \{w_i^j\}$
    $y_i^j \leftarrow u_i^j \oplus v_i^j \oplus w_i^j$
  $\mathbf{Z}^j \leftarrow (y_1^j, \ldots, y_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_0$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v, \mathcal{R}_w \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $y_i^j \leftarrow_{\$} \{0,1\}^n$
    $\mathcal{T}_i^j(y_i^j) \leftarrow \{(u,v,w) : u \in \mathcal{R}_u, v \in \mathcal{R}_v, w \in \mathcal{R}_w, u \oplus v \oplus w = y_i^j\}$
    if $\left|\mathcal{T}_i^j(y_i^j)\right| > 0$ **then**
      $(u_i^j, v_i^j, w_i^j) \leftarrow_{\$} \mathcal{T}_i^j(y_i^j)$
    else
      $(u_i^j, v_i^j, w_i^j) \leftarrow (\bot, \bot, \bot)$
    $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$, $\mathcal{R}_w \leftarrow \mathcal{R}_w \setminus \{w_i^j\}$
    $z_i^j \leftarrow (u_i^j, v_i^j, y_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \ldots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

Experiment $\mathcal{C}_1$

for $j \leftarrow 1$ to μ **do**
  $\mathcal{R}_u, \mathcal{R}_v, \mathcal{R}_w \leftarrow \{0,1\}^n$
  for $i \leftarrow 1$ to $q_{\max}$ **do**
    $u_i^j \leftarrow_{\$} \mathcal{R}_u$, $\mathcal{R}_u \leftarrow \mathcal{R}_u \setminus \{u_i^j\}$
    $v_i^j \leftarrow_{\$} \mathcal{R}_v$, $\mathcal{R}_v \leftarrow \mathcal{R}_v \setminus \{v_i^j\}$
    $w_i^j \leftarrow_{\$} \mathcal{R}_w$, $\mathcal{R}_w \leftarrow \mathcal{R}_w \setminus \{w_i^j\}$
    $z_i^j \leftarrow (u_i^j, v_i^j, u_i^j \oplus v_i^j \oplus w_i^j)$
  $\mathbf{Z}^j \leftarrow (z_1^j, \ldots, z_{q_{\max}}^j)$
return $(\mathbf{Z}^1, \ldots, \mathbf{Z}^\mu)$

For $y \in \{0,1\}^n$, let $T_k^j(y) = \left|\mathcal{T}_k^j(y)\right|$. From the proof of Lemma 7, we have

$$T_k^j(y) \geq 2^{2n} - 3(k-1)2^n.$$

Moreover, we see that

$$\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_{0,i}}(u,v,y) = \frac{1}{2^n T_k^j(y)},$$
$$\mathsf{p}^{\mathbf{z}}_{\mathcal{C}_{1,i}}(u,v,y) = \frac{1}{(2^n-k+1)^3}.$$

Therefore,

$$\begin{aligned}
\chi^2(\mathbf{z}) &= \sum_{\substack{z=(u,v,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_{0,i}}(z)>0}} \frac{1}{2^m T_k^j(y)} \left(1 - \frac{2^n T_k^j(y)}{(2^n-k+1)^3}\right)^2 \\
&\leq \sum_{\substack{(u,v,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_{0,i}}(u,v,y)>0}} \frac{\left((2^n-k+1)^3 - 2^n T_k^j(y)\right)^2}{2^n T_k^j(y)(2^n-k+1)S^6} \\
&\leq \sum_{\substack{(u,v,y)\in\Omega \text{ such} \\ \text{that } \mathsf{p}^{\mathbf{z}}_{\mathcal{C}_{0,i}}(u,v,y)>0}} \frac{23\left((2^n-k+1)^3 - 2^n T_k^j(y)\right)^2}{2^{9n}} \\
&\leq \frac{23}{2^{5n}} \sum_{y\in\{0,1\}^n} \left(\frac{(2^n-k+1)^3}{2^n} - T_k^j(y)\right)^2. \qquad (8)
\end{aligned}$$

since $k \leq q_{\max} \leq 2^{n-2}$. We claim the following lemma.

Lemma 9. *One has*

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[T_k^j(y)\right] = \frac{(2^n-k+1)^3}{2^n},$$
$$\mathop{\mathbf{Var}}_{\mathbf{z}}\left[T_k^j(y)\right] \leq \frac{(k-1)^3}{2^n}.$$

The proof of Lemma 9 is deferred to Section 7.3. From (8) and Lemma 9, it follows that

$$\begin{aligned}
\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\chi^2(\mathbf{z})\right] &\leq \frac{23}{2^{5n}} \mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\sum_{y\in\{0,1\}^n} \left(\frac{(2^n-k+1)^3}{2^n} - T_k^j(y)\right)^2\right] \\
&\leq \frac{23}{2^{5n}} \sum_{y\in\{0,1\}^n} \mathop{\mathbf{Var}}_{\mathbf{z}}\left[T_k^j(y)\right] \\
&\leq \frac{23(k-1)^3}{2^{5n}}
\end{aligned}$$

and finally, we have

$$\begin{aligned}\|\mathsf{p}^q_{\mathcal{C}_0}(\cdot) - \mathsf{p}^q_{\mathcal{C}_1}(\cdot)\| &\leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\leq \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}} \mathbf{Ex}\left[\chi^2(\mathbf{z})\right]\right)^{\frac{1}{2}} \\ &\leq \left(\frac{1}{2}\sum_{j=1}^{\mu}\sum_{k=1}^{q_{\max}} \frac{23(k-1)^3}{2^{5n}}\right)^{\frac{1}{2}} \\ &\leq \left(\frac{3\mu q_{\max}^4}{2^{5n}}\right)^{\frac{1}{2}}.\end{aligned}$$

7 Proving Expectation Value Lemmas

In this section, we give proof of expectation value lemmas which are used in the security proofs of our constructions.

7.1 Proof of Lemma 3

First, suppose $y \neq \mathbf{0}$. Let $\Psi = \{0,1\}^m \times \{0,1\}^{n-m} \times \{0,1\}^{n-m}$ and fix j, k, $\mathbf{h}$ and y. Let I_ψ where $\psi = (\alpha, \beta, \gamma) \in \Psi$ be an indicator variable

$$I_\psi = 1 \Leftrightarrow (\alpha \,\|\, \beta), (\alpha \oplus y \,\|\, \gamma) \in \{0,1\}^n \setminus \{u_l^j\}_{l\in[2k-2]}.$$

Observe that

$$T_k^j(y) = \sum_{\psi\in\Psi} I_\psi$$

and

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[I_\psi\right] = \frac{(2^n-2k+2)(2^n-2k+1)}{2^n(2^n-1)}.$$

Thus, we have

$$\begin{aligned}\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[T_k^j(y)\right] &= \sum_{\psi\in\Psi} \frac{(2^n-2k+2)(2^n-2k+1)}{2^n(2^n-1)} \\ &= \frac{2^n(2^n-2k+2)(2^n-2k+1)}{2^m(2^n-1)}. \qquad (9)\end{aligned}$$

Now, we compute the following expectation

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(T_k^j(y)\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\sum_{\psi\in\Psi} I_\psi\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi')\in\Psi^2} I_\psi I_{\psi'}\right].$$

For $\psi = (\alpha, \beta, \gamma)$ and $\psi' = (\alpha', \beta', \gamma')$, let r be the size of the following set

$$\{\alpha \parallel \beta, \alpha' \parallel \beta', (\alpha \oplus y) \parallel \gamma, (\alpha' \oplus y) \parallel \gamma'\}.$$

We see that, for $r = 2, \ldots, 4$,

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] = \frac{(2^n - 2k + 2)_r}{(2^n)_r}.$$

For a fixed $\psi \in \Psi$, we have

$$\begin{aligned}
|\{\psi' \in \Psi \mid r = 2\}| &= 2, \\
|\{\psi' \in \Psi \mid r = 3\}| &= 2^{n-m+2} - 4, \\
|\{\psi' \in \Psi \mid r = 4\}| &= 2^{2n-m} - 2^{n-m+2} + 2.
\end{aligned}$$

It follows that

$$\begin{aligned}
\sum_{\substack{\psi' \in \Psi, \\ r=2}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= 2\frac{(2^n - 2k + 2)_2}{(2^n)_2}, \\
\sum_{\substack{\psi' \in \Psi, \\ r=3}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{n-m+2} - 4)\left(1 - \frac{2k-2}{2^n - 2}\right)\frac{(2^n - 2k + 2)_2}{(2^n)_2}, \\
\sum_{\substack{\psi' \in \Psi, \\ r=4}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{2n-m} - 2^{n-m+2} + 2)\left(1 - \frac{2k-2}{2^n - 2}\right) \\
&\quad \times \left(1 - \frac{2k-2}{2^n - 3}\right)\frac{(2^n - 2k + 2)_2}{(2^n)_2}.
\end{aligned}$$

As $\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi') \in \Psi^2} I_\psi I_{\psi'}\right] = \sum_{(\psi,\psi') \in \Psi^2} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] = \sum_{\psi \in \Psi} \sum_{\psi' \in \Psi} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}]$ and the sum is divided into three cases according to the value of r, the sum of the expectations is given as

$$\begin{aligned}
\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi') \in \Psi^2} I_\psi I_{\psi'}\right] = 2^{2n-m}\Bigg(&\sum_{\substack{\psi' \in \Psi, \\ r=2}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] + \sum_{\substack{\psi' \in \Psi, \\ r=3}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] \\
&+ \sum_{\substack{\psi' \in \Psi, \\ r=4}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}]\Bigg). \qquad (10)
\end{aligned}$$

Therefore, by (10), we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi')\in\Psi^2} I_\psi I_{\psi'}\right] = \frac{(2^n-2k+2)_2}{2^n-1}\Big(2^{3n-2m} - (2^{2n-2m+1}+2^{n-2m})(2k-2) + 2^{n-2m}(2k-2)^2 + (2^{2n-2m}-6\cdot 2^{n-2m}+2^{n-m+1})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)}\Big)$$

and

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\frac{(2^n-2k+2)(2^n-2k+1)}{2^m}\cdot T_k^j(y)\right] = \frac{2^n(2^n-2k+2)^2(2^n-2k+1)^2}{2^{2m}(2^n-1)}.$$

Hence, for $y \neq \mathbf{0}$, it follows that

$$\begin{aligned}\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G_k^j(y)\right] &= \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\frac{(2^n-2k+2)(2^n-2k+1)}{2^m} - T_k^j(y)\right)^2\right] \\ &= \frac{(2^n-2k+2)_2}{2^n-1}(A_y+B_y) \qquad (11)\end{aligned}$$

where

$$\begin{aligned}A_y &= 2^{3n-2m} - (2^{2n-2m+1}+2^{n-2m})(2k-2) + 2^{n-2m}(2k-2)^2 \\ &\quad + (2^{2n-2m}-6\cdot 2^{n-2m}+2^{n-m+1})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)}\end{aligned}$$

and

$$\begin{aligned}B_y &= -\frac{2^{n+1}(2^n-2k+2)(2^n-2k+1)}{2^{2m}} + \frac{(2^n-1)(2^n-2k+2)(2^n-2k+1)}{2^{2m}} \\ &= -2^{3n-2m} + 4k\cdot 2^{2n-2m} - 4\cdot 2^{2n-2m} + 4k\cdot 2^{n-2m} - 3\cdot 2^{n-2m} \\ &\quad - (2^{n-2m}+2^{-2m})(4k^2-6k+2).\end{aligned}$$

Therefore, we have

$$\begin{aligned}A_y + B_y &= 3\cdot 2^{n-2m} - 2^{n-2m+1} - 2^{-2m+2}(k-1) \\ &\quad + (2^{n-m+1} - 2^{n-2m} - 6\cdot 2^{-2m})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)} \\ &\leq \frac{8(k-1)^2}{2^{n+m}} + 3\cdot 2^{n-2m}. \qquad (12)\end{aligned}$$

By (11) and (12), conclude that

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G_k^j(y)\right] \leq \frac{8(k-1)^2}{2^m} + 3\cdot 2^{2n-2m}. \qquad (13)$$

On the other hand, suppose $y = \mathbf{0}$. Note that $I_\psi = 0$ if $\beta = \gamma$. So, for $\psi = (\alpha, \beta, \gamma) \in \Psi$ such that $\beta \neq \gamma$, we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi] = \frac{(2^n - 2k + 2)(2^n - 2k + 1)}{2^n(2^n - 1)}.$$

Thus, we have

$$\begin{aligned}\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[T_k^j(\mathbf{0})\right] &= \sum_{\psi\in\Psi} \frac{(2^n - 2k + 2)(2^n - 2k + 1)}{2^n(2^n - 1)} \\ &= \frac{(2^{n-m} - 1)(2^n - 2k + 2)(2^n - 2k + 1)}{2^n - 1}. \end{aligned} \tag{14}$$

Now, we compute the following expectation

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(T_k^j(\mathbf{0})\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\sum_{\psi\in\Psi} I_\psi\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi')\in\Psi^2} I_\psi I_{\psi'}\right].$$

For $\psi = (\alpha, \beta, \gamma)$ and $\psi' = (\alpha', \beta', \gamma')$, let r be the size of following set

$$\{\alpha \parallel \beta, \alpha' \parallel \beta', \alpha \parallel \gamma, \alpha' \parallel \gamma'\}.$$

We see that, for $r = 2, \ldots, 4$,

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] = \frac{(2^n - 2k + 2)_r}{(2^n)_r}.$$

For a fixed $\psi \in \Psi$, we have

$$\begin{aligned}&|\{\psi' \in \Psi \mid r = 2\}| = 2, \\ &|\{\psi' \in \Psi \mid r = 3\}| = 2^{n-m+2} - 8, \\ &|\{\psi' \in \Psi \mid r = 4\}| = 2^{2n-m} - 2^{n-m+2} - 2^n + 6.\end{aligned}$$

It follows that

$$\begin{aligned}\sum_{\substack{\psi'\in\Psi,\\ r=2}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= 2\frac{(2^n - 2k + 2)_2}{(2^n)_2}, \\ \sum_{\substack{\psi'\in\Psi,\\ r=3}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{n-m+2} - 8)\left(1 - \frac{2k-2}{2^n - 2}\right)\frac{(2^n - 2k + 2)_2}{(2^n)_2}, \\ \sum_{\substack{\psi'\in\Psi,\\ r=4}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{2n-m} - 2^{n-m+2} - 2^n + 6)\left(1 - \frac{2k-2}{2^n - 2}\right) \\ &\quad \times \left(1 - \frac{2k-2}{2^n - 3}\right)\frac{(2^n - 2k + 2)_2}{(2^n)_2}.\end{aligned}$$

Similarly to (10), we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi')\in\Psi^2} I_\psi I_{\psi'}\right] = \frac{(2^{n-m}-1)(2^n-2k+2)_2}{2^n-1}\Big(2^{2n-m}-2^n \\ -(2^{n-m+1}+2^{-m}-2)(2k-2)+2^{-m}(2k-2)^2 \\ +(2^{n-m}-2^n+6-6\cdot 2^{-m})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)}\Big)$$

Also, we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\frac{(2^n-2k+2)(2^n-2k+1)}{2^m}\cdot T_k^j(\mathbf{0})\right] = \frac{(2^{n-m}-1)\left((2^n-2k+2)_2\right)^2}{2^m(2^n-1)}.$$

So, for $y=\mathbf{0}$, we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G_k^j(\mathbf{0})\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\frac{(2^n-2k+2)_2}{2^m}-T_k^j(\mathbf{0})\right)^2\right] \\ = \frac{(2^n-2k+2)_2}{2^n-1}(A_{\mathbf{0}}+B_{\mathbf{0}}) \tag{15}$$

where

$$A_{\mathbf{0}} = (2^{n-m}-1)\Big(2^{2n-m}-2^n-(2^{n-m+1}+2^{-m}-2)(2k-2)+2^{-m}(2k-2)^2 \\ +(2^{n-m}-2^n+6-6\cdot 2^{-m})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)}\Big) \\ = 2^{3n-2m}-2^{2n-m+1}+2^n+(2^{n-2m}-2^{-m})(2k-2)^2 \\ -(2^{2n-2m+1}-2^{n-m+2}+2^{n-2m}-2^{-m}+2)(2k-2) \\ +(2^{n-m}-1)(2^{n-m}-2^n+6-6\cdot 2^{-m})\frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)}$$

and

$$B_{\mathbf{0}} = -\frac{(2^{n+1}-2^{m+1})(2^n-2k+2)_2}{2^{2m}}+\frac{(2^n-1)(2^n-2k+2)_2}{2^{2m}} \\ = -\frac{(2^n-2^{m+1}+1)(2^n-2k+2)_2}{2^{2m}} \\ = -2^{3n-2m}+4k\cdot 2^{2n-2m}-4\cdot 2^{2n-2m}+2^{2n-m+1}-4k\cdot 2^{n-m+1}+6\cdot 2^{n-m} \\ +4k\cdot 2^{n-2m}-3\cdot 2^{n-2m}-(2^{n-2m}-2^{-m+1}+2^{-2m})(2k-2)(2k-1).$$

Therefore, we have

$$\begin{aligned} A_{\mathbf{0}} + B_{\mathbf{0}} &= 2^n - 2^{n-m+1} + 2^{n-2m} - 4\left(1 - \frac{1}{2^m}\right)^2 (k-1) \\ &\quad + \left(1 - \frac{1}{2^m}\right)(2^n + 2^{n-m} - 6 + 6 \cdot 2^{-m}) \frac{(2k-2)(2k-3)}{(2^n-2)(2^n-3)} \\ &\leq \frac{8(k-1)^2}{2^n} + 3 \cdot 2^n. \end{aligned} \tag{16}$$

By (15) and (16), conclude that

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[G_k^j(\mathbf{0})\right] = 8(k-1)^2 + 3 \cdot 2^{2n}. \tag{17}$$

By (13) and (17), the proof completes.

7.2 Proof of Lemma 6

Let $\Psi = \{0,1\}^m \times \{0,1\}^{n-m} \times \{0,1\}^{n-m}$ and fix j, k, $\mathbf{h}$ and y. Let I_ψ where $\psi = (\alpha, \beta, \gamma) \in \Psi$ be an indicator variable such that

$$I_\psi = 1 \Leftrightarrow (\alpha \parallel \beta \in \{0,1\}^n \setminus \{u_l^j\}_{l \in [k-1]}) \wedge (\alpha \oplus y \parallel \gamma \in \{0,1\}^n \setminus \{v_l^j\}_{l \in [k-1]}).$$

Observe that

$$T_k^j(y) = \sum_{\psi \in \Psi} I_\psi$$

and

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi] = \frac{(2^n - k + 1)^2}{2^{2n}}.$$

Thus, we have

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[T_k^j(y)\right] = \sum_{\psi \in \Psi} \frac{(2^n - k + 1)^2}{2^{2n}} = \frac{(2^n - k + 1)^2}{2^m} \tag{18}$$

To compute the variance, we compute the following expectation

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(T_k^j(y)\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\left(\sum_{\psi \in \Psi} I_\psi\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi, \psi') \in \Psi^2} I_\psi I_{\psi'}\right].$$

For $\psi = (\alpha, \beta, \gamma)$ and $\psi' = (\alpha', \beta', \gamma')$, let r be the number of distinctness conditions among

1. $\alpha \parallel \beta \neq \alpha' \parallel \beta'$,
2. $\alpha \parallel \gamma \neq \alpha' \parallel \gamma'$.

Note that $\psi = \psi'$ if $r = 0$. We see that, for $r = 0, 1, 2$,

$$\mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] = \frac{(2^n-k)^r(2^n-k+1)^2}{(2^n-1)^r 2^{2n}} = \left(1-\frac{k-1}{2^n-1}\right)^r \left(\frac{2^n-k+1}{2^n}\right)^2.$$

For a fixed $\psi \in \Psi$, we have

$$\begin{aligned}
&|\{\psi' \in \Psi \mid r = 0\}| = 1,\\
&|\{\psi' \in \Psi \mid r = 1\}| = 2^{n-m+1} - 2,\\
&|\{\psi' \in \Psi \mid r = 2\}| = 2^{2n-m} - 2^{n-m+1} + 1.
\end{aligned}$$

It follows that

$$\begin{aligned}
\sum_{\substack{\psi' \in \Psi,\\ r=0}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= \left(\frac{2^n-k+1}{2^n}\right)^2,\\
\sum_{\substack{\psi' \in \Psi,\\ r=1}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{n-m+1}-2)\left(1-\frac{k-1}{2^n-1}\right)\left(\frac{2^n-k+1}{2^n}\right)^2,\\
\sum_{\substack{\psi' \in \Psi,\\ r=2}} \mathop{\mathbf{Ex}}_{\mathbf{h}}[I_\psi I_{\psi'}] &= (2^{2n-m}-2^{n-m+1}+1)\left(1-\frac{k-1}{2^n-1}\right)^2\left(\frac{2^n-k+1}{2^n}\right)^2.
\end{aligned}$$

Similarly to (10), we have

$$\begin{aligned}
\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{\psi' \in \Psi} I_\psi I_{\psi'}\right] &= \left(\frac{2^n-k+1}{2^n}\right)^2 \Bigg(2^{2n-m} - 2^{n-m+1}(k-1)\\
&\qquad + (2^{2n-m}-2^{n-m+1}+1)\left(\frac{k-1}{2^n-1}\right)^2\Bigg)\\
&= \left(\frac{2^n-k+1}{2^n}\right)^2 \left(\frac{(2^n-k+1)^2}{2^m} + \left(1-\frac{1}{2^m}\right)\left(\frac{k-1}{2^n-1}\right)^2\right)\\
&\le \frac{(2^n-k+1)^4}{2^{2n+m}} + \frac{(k-1)^2}{2^{2n}}
\end{aligned}$$

for a fixed ψ. By (18), conclude that

$$\begin{aligned}
\mathop{\mathbf{Var}}_{\mathbf{h}}\left[T_k^j(y)\right] &= \mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{(\psi,\psi') \in \Psi^2} I_\psi I_{\psi'}\right] - \left(\mathop{\mathbf{Ex}}_{\mathbf{h}}\left[\sum_{\psi \in \Psi} I_\psi\right]\right)^2\\
&\le \frac{(k-1)^2}{2^m}. \qquad (19)
\end{aligned}$$

By (18) and (19), the proof completes.

7.3 Proof of Lemma 9

Let $\Psi = \{0,1\}^n \times \{0,1\}^n$ and fix j, k, $\mathbf{z}$ and y. Let I_ψ where $\psi = (\alpha, \beta) \in \Psi$ be an indicator variable such that

$$I_\psi = 1 \Leftrightarrow (\alpha \in \{0,1\}^n \setminus \{u_l^j\}_{l\in[k-1]}) \wedge (\beta \in \{0,1\}^n \setminus \{v_l^j\}_{l\in[k-1]}) \\ \wedge (\alpha \oplus \beta \oplus y \in \{0,1\}^n \setminus \{w_l^j\}_{l\in[k-1]}).$$

Observe that

$$T_k^j(y) = \sum_{\psi\in\Psi} I_\psi$$

and

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}[I_\psi] = \frac{(2^n - k + 1)^3}{2^{3n}}. \tag{20}$$

Thus, we have

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[T_k^j(y)\right] = \sum_{\psi\in\Psi} \frac{(2^n - k + 1)^3}{2^{3n}} = \frac{(2^n - k + 1)^3}{2^n}.$$

To compute the variance, we compute the following expectation

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\left(T_k^j(y)\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\left(\sum_{\psi\in\Psi} I_\psi\right)^2\right] = \mathop{\mathbf{Ex}}_{\mathbf{z}}\left[\sum_{(\psi,\psi')\in\Psi^2} I_\psi I_{\psi'}\right].$$

For $\psi = (\alpha, \beta, \gamma)$ and $\psi' = (\alpha', \beta', \gamma')$, let r be the number of distinctness conditions among

1. $\alpha \neq \alpha'$,
2. $\beta \neq \beta'$,
3. $\alpha \oplus \beta \neq \alpha' \oplus \beta'$.

Note that $\psi = \psi'$ if $r = 0$. Note that $r \neq 1$ since two of the equality conditions implies the remaining equality. We see that, for $r = 0, 2, 3$,

$$\mathop{\mathbf{Ex}}_{\mathbf{z}}[I_\psi I_{\psi'}] = \frac{(2^n - k)^r (2^n - k + 1)^3}{(2^n - 1)^r 2^{3n}} = \left(1 - \frac{k-1}{2^n - 1}\right)^3 \left(\frac{2^n - k + 1}{2^n}\right)^3.$$

For a fixed $\psi \in \Psi$, we have

$$|\{\psi' \in \Psi \mid r = 0\}| = 1,$$
$$|\{\psi' \in \Psi \mid r = 2\}| = 3 \cdot 2^n - 3,$$
$$|\{\psi' \in \Psi \mid r = 3\}| = 2^{2n} - 3 \cdot 2^n + 2.$$

It follows that

$$\sum_{\substack{\psi' \in \Psi, \\ r=0}} \mathop{\mathbf{Ex}}_{\mathbf{z}} [I_\psi I_{\psi'}] = \left(\frac{2^n - k + 1}{2^n}\right)^3,$$

$$\sum_{\substack{\psi' \in \Psi, \\ r=2}} \mathop{\mathbf{Ex}}_{\mathbf{z}} [I_\psi I_{\psi'}] = (3 \cdot 2^n - 3)\left(1 - \frac{k-1}{2^n - 1}\right)^2 \left(\frac{2^n - k + 1}{2^n}\right)^3,$$

$$\sum_{\substack{\psi' \in \Psi, \\ r=3}} \mathop{\mathbf{Ex}}_{\mathbf{z}} [I_\psi I_{\psi'}] = (2^{2n} - 3 \cdot 2^n + 2)\left(1 - \frac{k-1}{2^n - 1}\right)^3 \left(\frac{2^n - k + 1}{2^n}\right)^3.$$

Similarly to (10), we have

$$\begin{aligned}
\mathop{\mathbf{Ex}}_{\mathbf{z}} \left[\sum_{\psi' \in \Psi} I_\psi I_{\psi'}\right] &= \left(\frac{2^n - k + 1}{2^n}\right)^3 \left(2^{2n} - 3 \cdot 2^n (k-1) + 3(k-1)^2 \right. \\
&\qquad \left. - (2^{2n} - 3 \cdot 2^n + 2)\left(\frac{k-1}{2^n - 1}\right)^3\right) \\
&= \left(\frac{2^n - k + 1}{2^n}\right)^3 \left(\frac{(2^n - k + 1)^3}{2^n} + \frac{(k-1)^3}{2^n(2^n - 1)^2}\right) \\
&\leq \frac{(2^n - k + 1)^6}{2^{4n}} + \frac{(k-1)^3}{2^{3n}}
\end{aligned}$$

for a fixed ψ. By (20), conclude that

$$\begin{aligned}
\mathop{\mathbf{Var}}_{\mathbf{z}} \left[T_k^j(y)\right] &= \mathop{\mathbf{Ex}}_{\mathbf{z}} \left[\sum_{(\psi, \psi') \in \Psi^2} I_\psi I_{\psi'}\right] - \left(\mathop{\mathbf{Ex}}_{\mathbf{z}} \left[\sum_{\psi \in \Psi} I_\psi\right]\right)^2 \\
&\leq \frac{(k-1)^3}{2^n}. \qquad (21)
\end{aligned}$$

By (20) and (21), the proof completes.

References

1. M. Bellare and R. Impagliazzo. A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to prp to prf conversion. Cryptology ePrint Archive, Paper 1999/024, 1999. `https://eprint.iacr.org/1999/024`.
2. M. Bellare, J. Kilian, and P. Rogaway. The Security of Cipher Block Chaining. In *Annual International Cryptology Conference*, pages 341–358. Springer, 1994.
3. M. Bellare, T. Krovetz, and P. Rogaway. Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In K. Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98*, volume 1403 of *LNCS*, pages 266–280. Springer, 1998.

4. M. Bellare and P. Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 409–426. Springer, 2006.
5. S. Bhattacharya and M. Nandi. Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the χ^2 Method. In J. B. Nielsen and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018 (Proceedings, Part I)*, volume 10820 of *LNCS*, pages 387–412. Springer, 2018.
6. S. Bhattacharya and M. Nandi. Luby-Rackoff Backwards with More Users and More Security. In *Advances in Cryptology – ASIACRYPT 2021*, pages 345–375. Springer, 2021.
7. P. Bose, V. T. Hoang, and S. Tessaro. Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 468–499. Springer, 2018.
8. Y. L. Chen, E. Lambooij, and B. Mennink. How to Build Pseudorandom Functions from Public Random Permutations. In *Advances in Cryptology - CRYPTO 2019*, volume 11692 of *Lecture Notes in Computer Science*, pages 266–293. Springer, 2019.
9. W. Choi, B. Lee, and J. Lee. Indifferentiability of Truncated Random Permutations. In S. D. Galbraith and S. Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019 (Proceedings, Part I)*, volume 11921 of *LNCS*, pages 175–195. Springer, 2019.
10. W. Choi, B. Lee, J. Lee, and Y. Lee. Toward a Fully Secure Authenticated Encryption Scheme From a Pseudorandom Permutation. In *Advances in Cryptology – ASIACRYPT 2021*. Springer-Verlag, 2021.
11. B. Cogliati, R. Lampe, and J. Patarin. The Indistinguishability of the XOR of k Permutations. In *FSE*, pages 285–302. Springer, 2014.
12. B. Cogliati and Y. Seurin. EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In *CRYPTO*, pages 121–149. Springer, 2016.
13. B. Cogliati and Y. Seurin. Analysis of the single-permutation encrypted Davies-Meyer construction. *Designs, Codes and Cryptography*, 86(12):2703–2723, Dec 2018.
14. W. Dai, V. T. Hoang, and S. Tessaro. Information-Theoretic Indistinguishability via the Chi-Squared Method. In J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2018 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.
15. A. Dutta, M. Nandi, and S. Talnikar. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 (Proceedings, Part I)*, volume 11476 of *LNCS*, pages 437–466. Springer, 2019.
16. S. Gilboa, S. Gueron, and B. Morris. How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function? *Journal of Cryptology*, 31(1):162–171, 2018.
17. S. Gueron, A. Langley, and Y. Lindell. AES-GCM-SIV: Specification and Analysis. IACR Cryptology ePrint Archive, Report 2017/168, 2017.
18. S. Gueron and Y. Lindell. GCM-SIV: Full nonce misuse-resistant authenticated encryption at under one cycle per byte. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 109–119, 2015.

19. A. Gunsing and B. Mennink. The Summation-Truncation Hybrid: Reusing Discarded Bits for Free. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020 (Proceedings, Part I)*, volume 12170 of *LNCS*, pages 187–217. Springer, 2020.
20. C. Hall, D. Wagner, J. Kelsey, and B. Schneier. Building PRFs from PRPs. In H. Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 370–389. Springer, 1998.
21. V. T. Hoang and S. Tessaro. Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In M. Robshaw and J. Katz, editors, *CRYPTO 2016*, pages 3–32, 2016.
22. V. T. Hoang and S. Tessaro. The Multi-User Security of Double Encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 381–411. Springer, 2017.
23. J. Lee. Indifferentiability of the Sum of Random Permutations Toward Optimal Security. *IEEE Transactions on Information Theory*, 63(6):4050–4054, 2017.
24. S. Lucks. The Sum of PRPs Is a Secure PRF. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 2000.
25. B. Mennink. Linking Stam's Bounds with Generalized Truncation. In M. Matsui, editor, *CT-RSA 2019*, pages 313–329, 2019.
26. B. Mennink and S. Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In *CRYPTO*, pages 556–583. Springer, 2017.
27. B. Mennink and B. Preneel. On the XOR of Multiple Random Permutations. In T. Malkin, V. Kolesnikov, A. B. Lewko, and M. Polychronakis, editors, *ACNS 2015*, pages 619–634, 2015.
28. N. Mouha and A. Luykx. Multi-Key Security: The Even-Mansour Construction Revisited. In *Annual Cryptology Conference*, pages 209–223. Springer, 2015.
29. M. Nandi. Mind the composition: Birthday bound attacks on ewcdmd and sokac21. In *39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings*, volume 12105 of *Lecture Notes in Computer Science*. Springer, 2020.
30. J. Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In R. Safavi-Naini, editor, *Information Theoretic Security*, pages 232–248, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
31. J. Patarin. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. IACR Cryptology ePrint Archive, Report 2010/287, 2010.
32. A. Stam. Distance Between Sampling with and without Replacement. *Statistica Neerlandica*, 32(2):81–91, 1978.
33. S. Tessaro. Optimally Secure Block Ciphers from Ideal Primitives. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 437–462. Springer, 2015.