A Note on the Chi-square Method : A Tool for Proving Cryptographic Security

Srimanta Bhattacharya, Mridul Nandi

Indian Statistical Institute, Kolkata, India.

Abstract. In CRYPTO 2017, Dai, Hoang, and Tessaro introduced the *Chi-square method* (χ^2 method) which can be applied to obtain an upper bound on the statistical distance between two joint probability distributions. The authors applied this method to prove the *pseudorandom function security* (PRF-security) of sum of two random permutations. In this work, we revisit their proof and find a non-trivial gap in the proof and describe how to plug this gap as well; this has already been done by Dai *et al.* in the revised version of their CRYPTO 2017 paper. A complete, correct, and transparent proof of the full security of the sum of two random permutations construction is much desirable, especially due to its importance and two decades old legacy. The proposed χ^2 method seems to have potential for application to similar problems, where a similar gap may creep into a proof. These considerations motivate us to communicate our observation in a formal way.
On the positive side, we provide a very simple proof of the PRF-security of the *truncated random permutation* construction (a method to construct PRF from a random permutation) using the χ^2 method. We note that a proof of the PRF-security due to Stam is already known for this construction in a purely statistical context. However, the use of the χ^2 method makes the proof much simpler.

Keywords. random permutation, pseudorandom function, χ^2-distance, KL divergence, total variation distance, Pinsker's inequality, sum of random permutation, truncated random permutation.

1 Introduction

Different tools from probability and statistics are now heavily used in different areas in cryptography. In this paper, we focus on a statistical tool, termed χ^2 method, which was introduced by Dai, Hoang, and Tessaro in CRYPTO 2017 ([DHT17a]). Although a method which is essentially similar to the χ^2 method is known in statistics (since 1978), we believe that the χ^2 method is new in the context of cryptography. In [DHT17a], this method has been used to show pseudorandom function security (PRF-security) of two well known constructions, namely sum of random permutations ([Pat08b,Pat10,BI99,Luc00]) and encrypted Davis-Meyer (EDM) ([CS16,MN17]). Further, we feel that this method may help us to obtain tight (and simplified) proofs for certain constructions where proofs so far have evaded more classical methods, such as the H-coefficient method ([Pat08a]).

χ^2 Method. The *distinguishing advantage* of a family of keyed functions is bounded by the total variation (also known as *statistical distance*) between the output distribution of the family and the output distribution of a random function. Total variation between two probability distributions $\mathbf{P_0}$ and $\mathbf{P_1}$ over a sample space Ω, denoted $d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1})$, is defined as the half of L_1-norm $\|\mathbf{P_0} - \mathbf{P_1}\|_1 := \sum_{x \in \Omega} |\mathbf{P_0}(x) - \mathbf{P_1}(x)|$. In [DHT17a], the authors revisited a variation of the additivity property of the KL divergence between two joint distributions. The authors termed it χ^2 method. When $\mathbf{P_0}$ and $\mathbf{P_1}$ are joint distributions, this method provides an upper bound on $\|\mathbf{P_0} - \mathbf{P_1}\|_1$ based on the χ^2-distances between the conditional distributions of $\mathbf{P_0}$ and $\mathbf{P_1}$. Next, we recall the definition of χ^2-distance. In what follows, we use the convention that $0/0 = 0$.

Definition 1. *The χ^2-distance between distributions $\mathbf{P_0}$ and $\mathbf{P_1}$ (over a sample space Ω) with $\mathbf{P_0} \ll \mathbf{P_1}$ (i.e., the support of $\mathbf{P_0}$ is contained in the support of $\mathbf{P_1}$) is defined as*

$$d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1}) := \sum_{x \in \Omega} \frac{(\mathbf{P_0}(x) - \mathbf{P_1}(x))^2}{\mathbf{P_1}(x)}.$$

χ^2-distance has its origin in mathematical statistics dating back to Pearson (see [LV87] for some history). It can be seen that χ^2-distance is not symmetric and hence it is not a metric. However, this is useful for bounding other metrics, e.g., total variation. In the following, we briefly describe the χ^2 method (see Section A for details and proof).

Let $\mathsf{X} = (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{Y} = (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$ be two multivariate random variables taking values from Ω^q. In order to simplify the notation, we denote by X^{i-1} the joint random variable $(\mathsf{X}_1, \ldots, \mathsf{X}_{i-1})$. Let $\mathbf{P_0}_{x_1,\ldots,x_{i-1}}$ denote the conditional probability distribution of X_i given $\mathsf{X}_1 = x_1$, …, $\mathsf{X}_{i-1} = x_{i-1}$. We similarly write $\mathbf{P_1}_{x_1,\ldots,x_{i-1}}$ for the distribution of Y_i given $\mathsf{Y}_1 = x_1$, …, $\mathsf{Y}_{i-1} = x_{i-1}$. Then the χ^2 method says

$$d_{\mathrm{TV}}(\mathsf{X}, \mathsf{Y}) \leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}_1, \ldots, \mathsf{X}_{i-1})] \right)^{\frac{1}{2}}, \tag{1}$$

where $\chi^2(x_1, \ldots, x_{i-1}) = d_{\chi^2}(\mathbf{P_0}_{x_1,\ldots,x_{i-1}}, \mathbf{P_1}_{x_1,\ldots,x_{i-1}})$ and for all $x_1, \ldots, x_{i-1}$, $\mathbf{P_0}_{x_1,\ldots,x_{i-1}} \ll \mathbf{P_1}_{x_1,\ldots,x_{i-1}}$. Note that we need this condition to define d_{χ^2}.

XOR of Two Random Permutations. *XOR or sum of two random permutations* is a well known construction, proposed and studied by Hall *et al.* in [HWKS98], for conversion of *pseudorandom permutations* (PRPs) into *pseudorandom functions* (PRFs) [1]. Given a permutation $\pi : \{0,1\}^n \mapsto \{0,1\}^n$, the construction creates a function $f : \{0,1\}^{n-1} \to \{0,1\}^n$, defined as $f(x) = \pi(0||x) \oplus \pi(1||x)$. When π is chosen uniformly at random from Perm_n, the set of all permutations of $\{0,1\}^n$, how well does f resemble (in a certain well defined sense) a random function with the same domain and range (a function chosen uniformly from the set of all functions from the domain to the range)? A satisfactory answer to this question remained elusive for over two decades. There have been attempts ([Luc00,BI99,Pat08b,Pat10]) to prove *information-theoretic security* of the construction. However, the proofs either fell short of proving *full security* (to be made precise in the next section) of the construction([Luc00]) or were sketchy ([BI99]) or contained non-trivial gaps and were difficult to follow ([Pat08b,Pat10]) as was also observed by the authors of [DHT17a].[2] Also, as a related problem, Cogliati, Lampe, and Patarin [CLP14] gave weaker bounds for the case of the sum of at least three permutations. The XOR construction is important since it has been used to obtain some constructions achieving beyond birthday (or sometimes almost full) security (e.g., CENC [Iwa06], PMAC_Plus [BR02] and ZMAC [IMPS17]).

1.1 Main Results in the Paper

In [DHT17a], Dai *et al.* used the χ^2 method to prove full security of the XOR construction (XOR of two random permutations). In this paper, we have a closer inspection of the proof and we find a non-trivial gap in it. The gap is due to incorrect equalities involving conditional expectations. In [DHT17b], the authors have fixed this gap. We describe this fix in Lemma 1 in a slightly different way.

In this note, we communicate the above observation formally. This serves two purposes:(*a*) to motivate a flawless proof of this problem, especially owing to its importance and a two-decades old legacy, (*b*) to prevent these types of loopholes from creeping into the proofs involving the χ^2 method, especially since the method seems to have potential for application to similar problems.

Truncation of Random Permutation. Although the application (in [DHT17a]) of the χ^2 method to the XOR construction contains gap, this technique can be powerful for bounding PRF-security of other constructions. In fact, in [DHT17a], the authors applied this method to bound the PRF-security of the EDM (or encrypted Davis-Meyer) construction. In this note, we apply this technique to the **truncated random permutation** construction and obtain a very simple proof of the known tight bound on the PRF-security of the construction. This has been studied by Stam (in a statistical context) in 1978 [Sta78] and later by many others (e.g., [GG15,GG16,GGM17,HWKS98,BI99]). Stam's proof technique is very close to the χ^2 method. However, the other proofs are very different and produce different results. The difference between the proof methods of the relevant results from [HWKS98], [BI99], [GG15] and [Sta78]

[1] This line of work was initiated by Bellare *et al.* in [BKR98] who coined the term "Luby-Rackoff backwards" for such conversion.

[2] A quote from the paper [DHT17a] "`Patarin's tight proof is very involved, with some claims remaining open or unproved.`"

is discussed in [GGM17]. Our proof approach is more modular and uses the χ^2 method explicitly. We discuss these very briefly in Remark 1 and Remark 2

The PRF property of the truncated random permutation construction has recently been used in the key derivation for the AES-GCM, Counter based authenticated encryption constructions [GLL17].

1.2 Comparison with [BN18a]

This article is a somewhat updated version of [BN18a]. Here we prove Lemma 1 (the proof is similar (but not same) as the one given (in the proof of Theorem 3) in [DHT17b]) and omit Section 4 of [BN18a] where we proved Lemma 1 for two special cases. Also, we add Section 5 where we mention some recent applications of the χ^2-method.

1.3 Organization of the Paper

The rest of the paper is organized as follows. In the next section, we provide a brief overview of relevant security notions and the χ^2 method. There we also discuss the two constructions: XOR of two random permuations construction and trucated random permutation construction. Section 3 is devoted to the proof of Theorem 2. In Section 4, we discuss the proof, by Dai *et al.*, of the full security of the XOR of two random permutation construction, where we also point out the gap in it and explain its fix (in a slightly different way than was done in [DHT17b]). In Section 5, we briefly mention some of the more recent applications of the χ^2 method. Finally, in Appendix A, we provide a self-contained proof of the χ^2 method; essential ingredients of the proof is same as that of [DHT17a], however, we also cover the finer details (such as the proof of the Pinsker's inequality).

2 Preliminaries

Notation and Convention. We use the short-hand notation X^t to denote a tuple $(X_1, \ldots, X_t)$. We also write $\mathcal{S}^t$ to denote the t-fold Cartesian product of the set $\mathcal{S}$ with itself. It will be clear from the context whether X^t means a t-tuple (when X is a tuple) or product set (when X is a set).

We use notations $\mathsf{X}, \mathsf{Y}, \mathsf{Z}$ etc. (possibly with suffix) to represent random variables over some sets. Following the above notational convention, X^t would represent a t-tuple of random variables or random vector $(\mathsf{X}_1, \ldots, \mathsf{X}_t)$. We use $\mathcal{E}, \mathcal{S}, \mathcal{T}$ etc. (possibly with suffix) to denote sets. $\mathcal{A}$ will always represent an adversary.

In this paper, we fix a positive integer n, and we denote 2^n by N.

2.1 PRF-Security Definition

Pseudorandom function (PRF) is a very popular security notion in cryptography. While analyzing a message authentication code (MAC), we mostly study its PRF-security as it is a stronger notion than MAC. It has also been used to define encryption schemes, authenticated encryptions, and other cryptographic algorithms.

Now we formally define the *PRF-advantage* of an algorithm or a keyed function. By $\mathsf{X} \leftarrow_\$ \mathcal{S}$ we mean that X is sampled uniformly from a finite set $\mathcal{S}$. Let m and p be positive integers. Let RP_m denote the random permutation chosen uniformly from Perm_m, the set of all permutations on $\{0,1\}^m$, i.e., $\mathsf{RP}_m \leftarrow_\$ \mathsf{Perm}_m$. Similarly, let $\mathsf{RF}_{m \to p} \leftarrow_\$ \mathsf{Func}_{m \to p}$ (the set of all functions from $\{0,1\}^m$ to $\{0,1\}^p$). Let $\mathcal{K}$ be a finite set (it is the key space of the construction). Given a function $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^p$ and for every $k \in \mathcal{K}$, we denote f_k to represent the function (also called keyed function) $f(k, \cdot) \in \mathsf{Func}_{m \to p}$. We now define the PRF-advantage of an oracle adversary $\mathcal{A}$ against f as follows.

Definition 2 (PRF-advantage). *Let $\mathcal{A}$ be a distinguisher (oracle algorithm) and $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^p$. Then, the PRF-advantage of $\mathcal{A}$ against f is defined as*

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}) = |\mathbf{P}[\mathcal{A}^{f_{\mathsf{K}}} \to 1 \ : \ \mathsf{K} \leftarrow_\$ \mathcal{K}] - \mathbf{P}[\mathcal{A}^{\mathsf{RF}_{m \to p}} \to 1]|.$$

As we restrict to only deterministic keyed functions (i.e., functions which give same output on same input) we can assume, without loss of generality, that the adversary does not repeat its queries. In other words, if $\mathsf{Q}_1, \ldots, \mathsf{Q}_q$ are all queries then these are distinct. We can also assume that $\mathcal{A}$ is deterministic as it can always run with the best random coins which maximize the advantage. Suppose $\mathcal{A}$ makes q distinct queries adaptively, denoted $\mathsf{Q}_1, \ldots, \mathsf{Q}_q$, and obtains responses $\mathsf{U}_1, \ldots, \mathsf{U}_q$. So, when $\mathcal{A}$ in interacting with $\mathsf{RF}_{m \to p}$, the outputs are uniformly and independently distributed over $\{0,1\}^p$ which we denote as $\mathsf{U}_1, \ldots, \mathsf{U}_q \leftarrow_{\$} \{0,1\}^p$.

Similarly, let $\mathsf{X}_1, \ldots, \mathsf{X}_q$ denote the outputs of f_{K} where $\mathsf{K} \leftarrow_{\$} \mathcal{K}$. We denote the probability distributions associated with $\mathsf{U}_1, \ldots, \mathsf{U}_q$ and $\mathsf{X}_1, \ldots, \mathsf{X}_q$ by $\mathbf{P_1}$ and $\mathbf{P_0}$ respectively. Thus,

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}) = |\mathbf{P_1}(\mathcal{E}) - \mathbf{P_0}(\mathcal{E})| \tag{2}$$

where $\mathcal{E}$ is the set of all q-tuple of responses $x^q := (x_1, \ldots, x_q) \in (\{0,1\}^n)^q$ for which $\mathcal{A}$ returns 1. From the definition the total variation (also known as the *statistical distance*) between $\mathbf{P_0}$ and $\mathbf{P_1}$ is

$$d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) \overset{\mathrm{def}}{=} \frac{1}{2} \sum_{x^q \in (\{0,1\}^n)^q} |\mathbf{P_0}(x^q) - \mathbf{P_1}(x^q)| = \max_{\mathcal{E} \subseteq \Omega} (\mathbf{P_0}(\mathcal{E}) - \mathbf{P_1}(\mathcal{E})). \tag{3}$$

Hence,

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}) \leq d_{\mathrm{TV}}(\mathbf{P_1}, \mathbf{P_0}).^3$$

Thus, the main cryptographic objective (that of determining the PRF-advantage $\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A})$) turns out to be a purely probability or statistical problem. Next, we discuss the χ^2 method which provides an upper bound of total variation between two joint distributions.

2.2 χ^2 Method

Let $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{Z} := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q)$ are two random vectors of size q distributed over Ω^q. Let us denote the probability distributions of X and Z as $\mathbf{P_0}$ and $\mathbf{P_1}$ respectively. We denote the conditional probability distributions as follows.

$$\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i) = \mathbf{P}(\mathsf{X}_i = x_i | \mathsf{X}_1 = x_1, \ldots, \mathsf{X}_{i-1} = x_{i-1})$$
$$\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i) = \mathbf{P}(\mathsf{Z}_i = x_i | \mathsf{Z}_1 = x_1, \ldots, \mathsf{Z}_{i-1} = x_{i-1})$$

When $i = 1$, $\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_1)$ represents $\mathbf{P}(\mathsf{X}_1 = x_1)$. Similarly, for $\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_1)$. Let $x^{i-1} \in \Omega^{i-1}$, $i \geq 1$. Let us denote the χ^2-distance between $\mathbf{P}_{\mathbf{0}|x^{i-1}}$ and $\mathbf{P}_{\mathbf{1}|x^{i-1}}$ as $\chi^2(x^{i-1})$, i.e.,

$$\chi^2(x^{i-1}) := d_{\chi^2}(\mathbf{P}_{\mathbf{0}|x^{i-1}}, \mathbf{P}_{\mathbf{1}|x^{i-1}}).$$

Thus, χ^2 is a real valued function. The next theorem is the crux of the χ^2 method; it bounds the total variation between two joint distributions in terms of the χ^2-distance between the corresponding conditional distributions.

Theorem 1 ([DHT17a]). *Suppose* $\mathbf{P_0}$ *and* $\mathbf{P_1}$ *denote probability distributions of* $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ *and* $\mathsf{Z} := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q)$ *and for all* $x_1, \ldots, x_{i-1}$*, we have* $\mathbf{P}_{\mathbf{0}|x^{i-1}} \ll \mathbf{P}_{\mathbf{1}|x^{i-1}}$*. Then*

$$d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) \leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \right)^{\frac{1}{2}}.$$

For the sake of completeness, we provide a complete proof of this theorem in Appendix A. In our setup, note that $\mathsf{Z}_1, \ldots, \mathsf{Z}_q \leftarrow_{\$} \{0,1\}^p$ for some p and hence $\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i) = \frac{1}{2^p}$ for all x^i. So,

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] = 2^p \sum_{x_i} \mathbf{Ex}_{\mathsf{X}^{i-1}} \left[\left(\mathbf{P}(\mathsf{X}_i = x_i | \mathsf{X}_1, \ldots, \mathsf{X}_{i-1}) - \frac{1}{2^p} \right)^2 \right].$$

In the following subsection, we describe two constructions for which this method was applied.

[3] In fact, in this setting, i.e, for information theoretic security, there always exists an adversary $\mathcal{A}'$ such that $\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}') = d_{\mathrm{TV}}(\mathbf{P_1}, \mathbf{P_0})$; $\mathcal{A}'$ returns 1 for any $x^q \in \mathcal{E}'$, where $\mathcal{E}'$ is such that $d_{\mathrm{TV}}(\mathbf{P_1}, \mathbf{P_0}) = \mathbf{P_0}(\mathcal{E}') - \mathbf{P_1}(\mathcal{E}')$.

2.3 Two Random Permutation Based Constructions

In this paper, we mainly deal with two constructions based on a random permutation RP_n. Similar to a random function, if all queries to a random permutation RP_n are distinct and depends only on the previous responses (which is the case for an adversary), the outputs $\mathsf{V}_1, \ldots, \mathsf{V}_q$ behave like a random sample without replacement (WOR) from $\{0,1\}^n$. We write $\mathsf{V}_1, \ldots, \mathsf{V}_q \leftarrow_{\mathrm{wor}} \{0,1\}^n$ to denote this. More formally, for all *distinct* $x_1, \ldots, x_q \in \{0,1\}^n$, $\mathbf{P}(\mathsf{V}_1 = x_1, \ldots \mathsf{V}_q = x_q) = \frac{1}{(N)_q}$, where $(N)_q = N(N-1)\cdots(N-q+1)$. Now, we briefly describe the constructions.

(1) XOR **Construction.** Define $\mathsf{XOR}_\pi : \{0,1\}^{n-1} \to \{0,1\}^n$ to be the construction that takes a permutation $\pi \in \mathsf{Perm}_n$ as a key, and on input $x \in \{0,1\}^{n-1}$ it returns $\pi(x\|0) \oplus \pi(x\|1)$. Thus, XOR construction based on a random permutation RP_n returns $\mathsf{X}_1, \ldots, \mathsf{X}_q$ where $\mathsf{X}_1 := \mathsf{V}_1 \oplus \mathsf{V}_2$, …, $\mathsf{X}_q := \mathsf{V}_{2q-1} \oplus \mathsf{V}_{2q}$ and $\mathsf{V}_1, \ldots, \mathsf{V}_{2q} \leftarrow_{\mathrm{wor}} \{0,1\}^n$.

(2) trRP **Construction.** Let $m \leq n$ and trunc_m denotes the *truncation function* which returns the first m bits of $x \in \{0,1\}^n$. Truncated random permutation is a composition of random permutation followed by a truncation function. More formally, we define for every $x \in \{0,1\}^n$,

$$\mathsf{trRP}_m(x) = \mathsf{trunc}_m(\mathsf{RP}_n(x)).$$

Note that it is a function family, keyed by random permutation, mapping the set of all n-bit sequences to the set of all m-bit sequences. Let $\mathsf{X}_1, \ldots, \mathsf{X}_q$ denote the q outputs of trRP_m. Then $\mathsf{X}_i = \mathsf{trunc}_m(\mathsf{V}_i)$ for all i.

PRF-security of this construction has been studied by Stam in 1978, though in a much broader context (see [Sta78] for details), and later by others (e.g., [HWKS98,BI99,GG15,GG16,GGM17]). In particular, Stam proved the following statement.

Theorem 2 ([Sta78]). *Let* $\mathsf{V}_1, \ldots, \mathsf{V}_q \leftarrow_{\mathrm{wor}} \{0,1\}^n$, $\mathsf{U}_1, \ldots, \mathsf{U}_q \leftarrow_{\$} \{0,1\}^m$ *and* $\mathsf{X}_i = \mathsf{trunc}_m(\mathsf{V}_i)$ *for all* i. *Then*

$$d_{\mathrm{TV}}(\mathsf{X}, \mathsf{U}) \leq \frac{1}{2}\left(\frac{(M-1)q(q-1)}{(N-1)(N-q+1)}\right)^{\frac{1}{2}}$$

where $\mathsf{X} = (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ *and* $\mathsf{U} = (\mathsf{U}_1, \ldots, \mathsf{U}_q)$.

The following corollary (though not proved by Stam) is immediate from the relationship between PRF-advantage and total variation.

Corollary 1. *Let* $M = 2^m$, $N = 2^n$ *and* $m \leq n$. *For any adversary* $\mathcal{A}$ *making* q *queries we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{trRP}_m}(\mathcal{A}) \leq \frac{1}{2}\left(\frac{(M-1)q(q-1)}{(N-1)(N-q+1)}\right)^{\frac{1}{2}}.$$

Remark 1. The upper bounds on the PRF-advantage of the trRP Construction given in [HWKS98,GG15] are different (and weaker) than the one obtained by Stam. Although the bounds are similar for some choices of parameters. In [GGM17], all these results are mentioned, and the proofs are briefly surveyed. In [GGM17], a general tight lower bound on the PRF-advantage has been proved (improving on the lower bound declared in [HWKS98]).

3 Proof of Theorem 2 Using the χ^2 Method

Now we provide an alternative proof of Theorem 2 using the χ^2 method. We briefly recall the setup. Here $\mathsf{V}_1, \ldots, \mathsf{V}_q \leftarrow_{\mathrm{wor}} \{0,1\}^n$ and $\mathsf{X}_i = \mathsf{trunc}_m(\mathsf{V}_i)$. Let $x \in \{0,1\}^m$, $i \geq 1$ be an integer, and $K = N/M$. Also, let H denote the number of $j < i$, for which $\mathsf{trunc}_m(\mathsf{V}_j) = x$. The probability distribution of H is well known as the hypergeometric distribution $\mathsf{HG}(N, K, i-1)$. For every $\max(0, s+K-N) \leq a \leq \min(K, s)$ we have

$$\mathbf{P}(\mathsf{H} = a) = \frac{\binom{K}{a} \times \binom{N-K}{s-a}}{\binom{N}{s}}.$$

The following fact states the expectation and variance formula of a hypergeometric distribution. Its proof can be found in standard probability theory text books and hence we skip it.

Fact 1 *Let* H *follow hypergeometric distribution* $\mathsf{HG}(N, K, s)$ *and let* p *denote* $\frac{K}{N}$*. Then,*

$$\begin{aligned}\mathbf{Ex}[\mathsf{H}] &= sp. &(4)\\ \mathbf{Var}[\mathsf{H}] := \mathbf{Ex}[\mathsf{H} - \mathbf{Ex}[\mathsf{H}]]^2 &= sp(1-p) \times \frac{N-s}{N-1}. &(5)\end{aligned}$$

As an aside, we mention that the factor $\frac{N-s}{N-1}$ is also known as the finite sampling correction factor. Up to this factor, the expression of variance is same as that of the binomial distribution.

Now, we apply the χ^2 method to bound the total variation $d_{\mathrm{TV}}(\mathsf{X}, \mathsf{U})$, where $\mathsf{U}_1, \ldots, \mathsf{U}_q \leftarrow_{\$} \{0,1\}^m$. Let $\mathbf{P_0}$ and $\mathbf{P_1}$ denote the probability distributions of X and U respectively. Note that

$$\begin{aligned}\mathbf{P}_{\mathbf{0}|x^{i-1}}(x) &= \mathbf{P}(\mathsf{X}_i = x \mid \mathsf{X}_1 = x_1, \ldots, \mathsf{X}_{i-1} = x_{i-1})\\ &= \mathbf{P}(\mathsf{V}_i \notin \mathcal{S}), \quad \text{where } \mathcal{S}_{i,x}(x^{i-1}) = \{v \in \{0,1\}^n : \exists j < i \ \mathsf{trunc}_m(v) = x_j\}\\ &= \frac{\frac{N}{M} - |\mathcal{S}_{i,x}(x^{i-1})|}{N-i+1}.\end{aligned}$$

Let $N_{i,x}(x^{i-1}) := |\mathcal{S}_{i,x}(x^{i-1})|$ and $\mathsf{H}_{i,x} = N_{i,x}(\mathsf{X}^{i-1})$. Then it is easy to see from the definition of the heypergeometric distribution that $\mathsf{H}_{i,x}$ follows $\mathsf{HG}(N, N/M, (i-1))$. Now, we compute the χ^2 function evaluated at x^{i-1}.

$$\begin{aligned}\chi^2(x^{i-1}) &= \sum_{x \in [M]} M \left(\frac{\frac{N}{M} - N_{i,x}(x^{i-1})}{N-i+1} - \frac{1}{M} \right)^2\\ &= \sum_{x \in [M]} \frac{M}{(N-i+1)^2} \times \left(N_{i,x}(x^{i-1}) - \frac{i-1}{M} \right)^2.\end{aligned}$$

Hence,

$$\begin{aligned}\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] &= \mathbf{Ex}\left[\sum_{x \in [M]} \frac{M}{(N-i+1)^2} \times \left(\mathsf{H}_{i,x} - \frac{i-1}{M} \right)^2 \right]\\ &= \sum_{x \in [M]} \frac{M}{(N-i+1)^2} \times \mathbf{Var}[\mathsf{H}_{i,x}]. &(6)\end{aligned}$$

This follows from the linearity of the expectation and the fact that $\mathbf{Ex}[\mathsf{H}_{i,x}] = (i-1)/M$. By substituting the value of $\mathbf{Var}[N_x]$ as described in the Fact 1, we obtain

$$\begin{aligned}\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] &= \frac{M^2}{(N-i+1)^2} \times \frac{i-1}{M} \times \left(1 - \frac{1}{M}\right) \times \frac{N-i+1}{N-1}\\ &= \frac{(M-1)(i-1)}{(N-1)(N-i+1)}.\end{aligned}$$

Now by using Theorem 1 we have

$$\begin{aligned}d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) &\leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \right)^{\frac{1}{2}}\\ &= \left(\frac{1}{2} \sum_{i=1}^{q} \frac{(M-1)(i-1)}{(N-1)(N-i+1)} \right)^{\frac{1}{2}}\\ &\leq \left(\frac{1}{2} \sum_{i=1}^{q} \frac{(M-1)(i-1)}{(N-1)(N-q+1)} \right)^{\frac{1}{2}}\\ &= \frac{1}{2} \left(\frac{(M-1)q(q-1)}{(N-1)(N-q+1)} \right)^{\frac{1}{2}}. \qquad \square\end{aligned}$$

Remark 2. In order to draw comparison between our proof (using the χ^2 method) of Theorem 2 and the proof due to Stam, we remark that the main ideas of both the proofs are same; namely both use the chain rule of the KL divergence, concavity of the logarithm function, and also the hypergeometric distribution. However, unlike in our case (in (6)) Stam did not make explicit use of variance of the hypergeometric distribution. Instead, he used Jensen's inequality. Moreover, our proof is simpler and modular compared to Stam's proof with a more direct approach.

4 Overview of the Proof by Dai *et al.* and its Flaw

In this section, we provide a brief overview of the proof by Dai *et al.* to precisely point out the gap in their proof. In order to better emphasize, we provide a brief sketch of the proof due to Dai et al. We mostly follow the notation by the authors along with our notational convention. For example, we mostly use N instead of 2^n. Moreover, for simplicity we write the set $\{0,1\}^n \setminus \{0^n\}$ as $[N]^*$.

Theorem 3 ([DHT17a]). *Fix an integer $n \geq 8$ and let $N = 2^n$. For any adversary $\mathcal{A}$ that makes $q \leq \frac{N}{32}$ queries we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}}(\mathcal{A}) \leq \frac{1.5q + 3\sqrt{q}}{N}.$$

Proof due to Dai et al in [DHT17a]. Let $\mathcal{A}$ be an adversary making exactly q distinct queries adaptively. As we have observed before, the output distributions of random function and XOR function do not depend on $\mathcal{A}$. In fact, $\mathsf{U}'_1, \ldots, \mathsf{U}'_q \leftarrow_{\$} \{0,1\}^n$ and $\mathsf{X}_1 := \mathsf{V}_1 \oplus \mathsf{V}_2, \ldots, \mathsf{X}_q := \mathsf{V}_{2q-1} \oplus \mathsf{V}_{2q}$ are the outputs of random function and XOR construction respectively, where $\mathsf{V}_1, \ldots, \mathsf{V}_{2q} \leftarrow_{\mathrm{wor}} \{0,1\}^n$. Let $\mathbf{P_1}$ and $\mathbf{P_2}$ denote the output distributions of $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{U}' := (\mathsf{U}'_1, \ldots, \mathsf{U}'_q)$ respectively. Thus,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}}(\mathcal{A}) \leq d_{\mathrm{TV}}(\mathbf{P_1}, \mathbf{P_2}).$$

Now, we note that X_i's cannot take 0^n and hence it is natural to consider the q-tuple of random variables $\mathsf{U}_1, \ldots, \mathsf{U}_q \leftarrow_{\$} [N]^* := \{0,1\}^n \setminus \{0^n\}$. Let us denote by $\mathbf{P_0}$ the probability distribution of $\mathsf{U}_1, \ldots, \mathsf{U}_q$. By simple algebra, we have $d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_2}) \leq q/2^n$. Also, using triangle inequality[4], we have

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XOR}}(\mathcal{A}) \leq d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) + q/2^n.$$

At this point, the χ^2 method (i.e., Theorem 1) gives an upper bound on $d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1})$. The rest of the proof is devoted to show $d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) \leq \frac{0.5q+3\sqrt{q}}{2^n}$.

For every non-zero $x_1, \ldots, x_i$, we clearly have $\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i) = 1/(N-1)$. For simplicity, let us denote by $Y_{i,x}$ the conditional probability $\mathbf{P}_{\mathbf{1}|x^{i-1}}(x)$ which is also a function over x^{i-1}. When x^{i-1} is chosen following the distribution of X^{i-1}, we denote $Y_{i,x}$ as $\mathsf{Y}_{i,x}$. From the definition of χ^2 function corresponding to $(\mathsf{V}_1, \ldots, \mathsf{V}_q)$ and $(\mathsf{U}_1, \ldots, \mathsf{U}_q)$, we have

$$\chi^2(x^{i-1}) = \sum_{x \neq 0^n} (N-1)(Y_{i,x} - \frac{1}{N-1})^2. \tag{7}$$

Now, we give a brief description of the rest but critical part of the proof where the authors provided an upper bound on $\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]$. We keep the authors' flow (suppressing some calculation which will be denoted as $***$) and wordings. However, we change some of their notations in order to make them consistent with our notation. Authors complete the proof as described below.

We now expand $Y_{i,x}$ into a more expressive and convenient formula to work with. $***$ Let $\mathsf{S} = \{\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}\}$. Let $\mathsf{D}_{i,x}$ be the number of pairs $(u, u \oplus x)$ such that both u and $u \oplus x$ belongs to S. Note that S and $\mathsf{D}_{i,x}$ are both random variables, and in fact functions of the random variables $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$. $***$ Hence,

$$\mathsf{Y}_{i,x} = \frac{N - 4(i-1) + \mathsf{D}_{i,x}}{(N-2i+1)(N-2i)}. \tag{8}$$

[4] Triangle inequality of total variation metric can be easily shown from the triangle inequality in real numbers.

* * *

$$\left(\mathsf{Y}_{i,x} - \frac{1}{N-1}\right)^2 \leq \frac{3(\mathsf{D}_{i,x} - 4(i-1)^2/N)^2 + 18}{N^4}.$$

From Eq. 7,

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \leq \sum_{x \neq 0^n} N \cdot \mathbf{Ex}\left[\left(\mathsf{Y}_{i,x} - \frac{1}{N-1}\right)^2\right] \tag{9}$$

$$\leq \sum_{x \neq 0^n} \frac{18}{N^3} + \frac{3}{N^3} \cdot \mathbf{Ex}\left[\left(\mathsf{D}_{i,x} - \frac{4(i-1)^2}{N}\right)^2\right] \tag{10}$$

In the last formula, it is helpful to think of each $\mathsf{D}_{i,x}$ as a function of $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$, and the expectation is taken over the choices of $\mathsf{V}_1, \mathsf{V}_2, \ldots, \mathsf{V}_{2i-2}$ sampled uniformly without replacement from $\{0,1\}^n$. We will show that[5] for any $x \in \{0,1\}^n \setminus \{0^n\}$,

$$\mathbf{Ex}\left[\left(\mathsf{D}_{i,x} - \frac{4(i-1)^2}{N}\right)^2\right] \leq \frac{4(i-1)^2}{N} \tag{11}$$

and thus

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \leq \frac{18}{N^2} + \frac{12(i-1)^2}{N^3}.$$

Summing up, from χ^2-method

$$d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}}$$

$$\leq \frac{3\sqrt{q} + .5q}{N}. \qquad \square$$

4.1 Flaw in the Above Proof and its Repair

Let us revisit Eq. 8. Let us fix distinct $v_1, \ldots, v_{2i-2}$ and define the set $\mathcal{S} = \{v_1, \ldots, v_{2i-2}\}$. Let $D_{i,x}$ denote the number of pairs $(u, u \oplus x)$ such that both u and $u \oplus x$ belong to $\mathcal{S}$. Let $x_1 = v_1 \oplus v_2, \ldots, x_{i-1} = v_{2i-3} \oplus v_{2i-2}$. Now, it is easy to see that

$$\mathbf{P}(\mathsf{X}_i = x | \mathsf{V}_1 = v_1, \ldots, \mathsf{V}_{2i-2} = v_{2i-2}) = \frac{N - 4(i-1) + D_{i,x}}{(N-2i+1)(N-2i)} \tag{12}$$

which appeared in the right hand side of Eq. 8. Whereas the left hand side of the equation is $\mathbf{P}(\mathsf{X}_i = x | \mathsf{X}_1 = x_1, \ldots, \mathsf{X}_{i-1} = x_{i-1})$. Note that in general,

$$\mathbf{P}(\mathsf{X}_i = x | \mathsf{V}_1 = v_1, \ldots, \mathsf{V}_{2i-2} = v_{2i-2}) = \mathbf{P}(\mathsf{X}_i = x | \mathsf{X}_1 = x_1, \ldots, \mathsf{X}_{i-1} = x_{i-1}) \tag{13}$$

does not hold for every $v_1, \ldots, v_{2i-2}$. Hence Eq. 8 is incorrect.

After observing this flaw in the proof, let us see how we can fix it. If we can prove Eq. 10 in some other way, we can still continue with the rest of the proof. This can be proved if we can prove a variant of the Eq. 8 as follows:

$$\sum_x \mathbf{Ex}[(\mathsf{Y}_{i,x} - c)^2] = \sum_x \mathbf{Ex}\left[\left(\frac{N - 4(i-1) + \mathsf{D}_{i,x}}{(N-2i+1)(N-2i)} - c\right)^2\right],$$

[5] Which has been shown later in the proof given by Dai et al. In this paper we don't provide details on this claim and so we skip this proof here.

where $c = 1/(N-1)$. In other words,

$$\sum_x \mathbf{Ex}[(\mathbf{P}(\mathsf{X}_i = x|\mathsf{X}^{i-1}) - c)^2] = \sum_x \mathbf{Ex}[(\mathbf{P}(\mathsf{X}_i = x|\mathsf{V}^{2i-2}) - c)^2].$$

The above equation is equivalent to

$$\mathop{\mathbf{Ex}}_{\mathsf{V}^{2i-2}}[\sum_{x\in[N]^*} \mathbf{P}(\mathsf{X}_i = x|\mathsf{V}^{2i-2})^2] = \mathop{\mathbf{Ex}}_{\mathsf{X}^{i-1}}[\sum_{x\in[N]^*} \mathbf{P}(\mathsf{X}_i = x|\mathsf{X}^{i-1})^2] \tag{14}$$

It has been shown in Theorem 5 of [BN18a] that (14) is actually not true and strict inequality holds in place of equality. However, the proof survives because of the following result. In [DHT17b], the authors show this as part of the proof of Theorem 3 in a slightly different way using Jensen's inequality.

Lemma 1 (Adapted from [DHT17b]).

$$\mathop{\mathbf{Ex}}_{\mathsf{V}^{2i-2}}[\sum_{x\in[N]^*} \mathbf{P}(\mathsf{X}_i = x|\mathsf{V}^{2i-2})^2] \geq \mathop{\mathbf{Ex}}_{\mathsf{X}^{i-1}}[\sum_{x\in[N]^*} \mathbf{P}(\mathsf{X}_i = x|\mathsf{X}^{i-1})^2]$$

Proof. Let $\mathcal{V}^{2i-2}$ and $\mathcal{X}^{i-1}$ be the supports of V^{2i-2} and X^{i-1} repectively. Therefore, $\mathcal{V}^{2i-2} = \{(v_1, \ldots, v_{2i-2})|v_1, \ldots, v_{2i-2} \in [N] \text{ are distinct}\}$ and $\mathcal{X}^{i-1} = \{(v_1 \oplus v_2, \ldots, v_{2i-3} \oplus v_{2i-2})|v^{2i-2} \in \mathcal{V}^{2i-2}\}$. Essentially we need to show the following.

$$\sum_{v^{2i-2}\in\mathcal{V}^{2i-2}} \sum_{x\in[N]^*} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{V}^{2i-2} = v^{2i-2})^2}{\mathbf{P}(\mathsf{V}^{2i-2} = v^{2i-2})} \geq \sum_{x^{i-1}\in\mathcal{X}^{i-1}} \sum_{x\in[N]^*} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{X}^{i-1} = x^{i-1})^2}{\mathbf{P}(\mathsf{X}^{i-1} = x^{i-1})} \tag{15}$$

Therefore, it is sufficient to show that the inequality in (15) is maintained for any fixed value of $x \in [N]^*$. For $x^{i-1} \in \mathcal{X}^{i-1}$ let $\mathcal{D}_{x^{i-1}} := \{v^{2i-2} \in \mathcal{V}^{2i-2}|x_1 = v_1 \oplus v_2, \ldots, x_{i-1} = v_{2i-3} \oplus v_{2i-2}\}$. Then $\mathcal{D}_{x^{i-1}}$ is non-empty for each $x^{i-1} \in \mathcal{X}^{i-1}$ and $\{\mathcal{D}_{x^{i-1}}|x^{i-1} \in ([N]^*)^{i-1}\}$ is a partition of $\mathcal{V}^{2i-2}$. Now, for fixed $x \in [N]^*$, we have

$$\sum_{v^{2i-2}\in\mathcal{V}^{2i-2}} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{V}^{2i-2} = v^{2i-2})^2}{\mathbf{P}(\mathsf{V}^{2i-2} = v^{2i-2})} = \sum_{x^{i-1}\in\mathcal{X}^{i-1}} \sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{V}^{2i-2} = v^{2i-2})^2}{\mathbf{P}(\mathsf{V}^{2i-2} = v^{2i-2})}$$

Further,

$$\sum_{x^{i-1}\in\mathcal{X}^{i-1}} \sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{V}^{2i-2} = v^{2i-2})^2}{\mathbf{P}(\mathsf{V}^{2i-2} = v^{2i-2})} = \sum_{x^{i-1}\in\mathcal{X}^{i-1}} \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{X}^{i-1} = x^{i-1})^2}{\mathbf{P}(\mathsf{X}^{i-1} = x^{i-1})} \sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \frac{\mathsf{NUM}^2_{v^{2i-2}}}{\mathsf{DEN}_{v^{2i-2}}},$$

where $\mathsf{NUM}_{v^{2i-2}} = \frac{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{V}^{2i-2} = v^{2i-2})}{\mathbf{P}(\mathsf{X}_i = x \wedge \mathsf{X}^{i-1} = x^{i-1})}$ and $\mathsf{DEN}_{v^{2i-2}} = \frac{\mathbf{P}(\mathsf{V}^{2i-2} = v^{2i-2})}{\mathbf{P}(\mathsf{X}^{i-1} = x^{i-1})}$. Here, we mention that for $\mathsf{NUM}_{v^{2i-2}}$ and $\mathsf{DEN}_{v^{2i-2}}$, numerator is zero only if the denominator is zero. Finally, it suffices to show that $\sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \frac{\mathsf{NUM}^2_{v^{2i-2}}}{\mathsf{DEN}_{v^{2i-2}}} \geq 1$. But this follows from the Cauchy-Schwarz inequality by noting that $\sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \mathsf{NUM}_{v^{2i-2}} = \sum_{v^{2i-2}\in\mathcal{D}_{x^{i-1}}} \mathsf{DEN}_{v^{2i-2}} = 1$. □

5 Subsequent Work

Subsequent to the publication of [BN18a] there have been few other applications of the χ^2 method. Below, we briefly outline the results obtained using this method. Recall that $\mathsf{RP}_n \leftarrow\!\!\$\ \mathsf{Perm}_n$ is a random permutation of $\{0,1\}^n$.

1. In [Men19], the author studies a generalized truncation function. More precisely, the function is given by

$$\mathsf{GTrunc}^p(x) = \mathsf{post}(x, \mathsf{RP}_n(x)),$$

where $\mathsf{post} : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^m$ is a post-processing function. Here, it may be noted that the post-processing function post takes the input (to the construction) as one of its inputs. When post is balanced (that is, when each point in its image has the same number of preimages), the author prove the folloiwng bound.

Theorem 4 ([Men19]). *Let $q, n, m \in \mathbb{N}$ be such that $m \leq n$. For any distinguisher $\mathcal{A}$ making at most q queries,*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{GTrunc}}(\mathcal{A}) \leq \frac{1}{2}\left(\frac{(2^m-1)q(q-1)}{(2^n-1)(2^n-q+1)}\right)^{\frac{1}{2}}.$$

Similar type of bound was also shown for the case when post is not balanced.

2. In [CLL], the authors prove indifferentiability of the truncation function. More precisely, their truncation function is defined as follows.

$$\mathsf{TRP}[\mathsf{RP}_n] = \mathsf{Tr}_m(\mathsf{RP}_n(c||.)),$$

where $c \in \{0,1\}^\ell$ is a fixed prefix, and $\mathsf{Tr}_m : \{0,1\}^n \mapsto \{0,1\}^{n-m}$ returns the rightmost $n-m$ bits of its input.
The authors prove that the construction is regularly indifferentiable up to $\min\{2^{\frac{n+m}{3}}, 2^m, 2^\ell\}$ queries, and publicly indifferentiable [6] up to $\min\{\max\{2^{\frac{n+m}{3}}, 2^{\frac{n}{2}}\}, 2^\ell\}$ queries. The previous best-known bound (obtained in [DRRS09]) for regular indifferentiability of the construction was $\min\{2^{\frac{m}{2}}, 2^\ell\}$ queries.

3. In [CLMP17], the authors have introduced a length doubling construction [7] using tweakable block ciphers (LDT). They have shown a birthday-bound (*i.e.,* $\frac{n}{2}$-bit) security of the construction. They have also given an attack in $2^{n-\frac{s}{2}}$ queries, where s is a parameter of the construction.
In [CMN18], the authors have used the χ^2 method to show that the construction, in fact, achieves beyond-birthday-bound security under certain conditions; the achieved security level goes up to $\frac{2n}{3}$-bit. Further, they have shown that 3-round LDT (the original LDT construction of [CLMP17] is composed of 2 rounds) achieves n-bit security under certain conditions.

Acknowledgement We thank the reviewers of the journal Cryptography and Communications for their comments and suggestions which have improved the quality of our manuscript.

References

BI99. M. Bellare and R. Impagliazzo, *A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion*, IACR Cryptology ePrint Archive **1999**, 24 (1999).

BKR98. M. Bellare, T. Krovetz and P. Rogaway, Luby-Rackoff backwards: Increasing security by making block ciphers non-invertible, pages 266–280, Springer, 1998.

BN18a. S. Bhattacharya and M. Nandi, *A note on the chi-square method: A tool for proving cryptographic security*, Cryptography and Communications **10**(5), 935–957 (Sep 2018).

BN18b. S. Bhattacharya and M. Nandi, *A note on the chi-square method: A tool for proving cryptographic security*, Cryptography and Communications **10**(5), 935–957 (2018).

BR02. J. Black and P. Rogaway, A Block-Cipher Mode of Operation for Parallelizable Message Authentication, in *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 384–397, Springer, 2002.

CLL. W. Choi, B. Lee and J. Lee, Indifferentiability of Truncated Random Permutations, in *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, to appear.*

CLMP17. Y. L. Chen, A. Luykx, B. Mennink and B. Preneel, *Efficient Length Doubling From Tweakable Block Ciphers*, IACR Trans. Symmetric Cryptol. **2017**(3), 253–270 (2017).

CLP14. B. Cogliati, R. Lampe and J. Patarin, The Indistinguishability of the XOR of k Permutations, in *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, edited by C. Cid and C. Rechberger, volume 8540 of *Lecture Notes in Computer Science*, pages 285–302, Springer, 2014.

CMN18. Y. L. Chen, B. Mennink and M. Nandi, Short Variable Length Domain Extenders with Beyond Birthday Bound Security, in *Advances in Cryptology – ASIACRYPT 2018*, edited by T. Peyrin and S. Galbraith, pages 244–274, Cham, 2018, Springer International Publishing.

[6] This type of indifferentiability has been studied in [DRS09,YMO08,MPS12].

[7] An enciphering scheme that can encrypt any bit string of length $[n \ldots 2n-1]$ as opposed to the ordinary block cipher that can encrypt a fixed length (n) string.

CS16. B. Cogliati and Y. Seurin, EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC, in *CRYPTO 2016, Proceedings, Part I*, pages 121–149, 2016.

CT06. T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*, Wiley-Interscience, 2006.

DHT17a. W. Dai, V. T. Hoang and S. Tessaro, Information-theoretic Indistinguishability via the Chi-squared Method, Cryptology ePrint Archive, Report 2017/537, 2017, `http://eprint.iacr.org/2017/537`.

DHT17b. W. Dai, V. T. Hoang and S. Tessaro, *Information-theoretic Indistinguishability via the Chi-squared Method*, IACR Cryptology ePrint Archive **2017**, 537 (2017).

DRRS09. Y. Dodis, L. Reyzin, R. L. Rivest and E. Shen, Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6, in *Fast Software Encryption*, edited by O. Dunkelman, pages 104–121, Berlin, Heidelberg, 2009, Springer Berlin Heidelberg.

DRS09. Y. Dodis, T. Ristenpart and T. Shrimpton, Salvaging Merkle-Damgård for Practical Applications, in *Advances in Cryptology - EUROCRYPT 2009*, edited by A. Joux, pages 371–388, Berlin, Heidelberg, 2009, Springer Berlin Heidelberg.

GG15. S. Gilboa and S. Gueron, *Distinguishing a truncated random permutation from a random function*, IACR Cryptology ePrint Archive **2015**, 773 (2015).

GG16. S. Gilboa and S. Gueron, *The Advantage of Truncated Permutations*, CoRR **abs/1610.02518** (2016).

GGM17. 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 (2017).

GLL17. S. Gueron, A. Langley and Y. Lindell, *AES-GCM-SIV: Specification and Analysis*, IACR Cryptology ePrint Archive **2017**, 168 (2017).

GS02. A. L. Gibbs and F. E. Su, *On Choosing and Bounding Probability Metrics*, International Statistical Review **70**(3), 419–435 (2002).

HWKS98. C. Hall, D. Wagner, J. Kelsey and B. Schneier, *Building PRFs from PRPs*, pages 370–389, Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.

IMPS17. T. Iwata, K. Minematsu, T. Peyrin and Y. Seurin, *ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication*, IACR Cryptology ePrint Archive **2017**, 535 (2017).

Iwa06. T. Iwata, New Blockcipher Modes of Operation with Beyond the Birthday Bound Security, in *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, edited by M. J. B. Robshaw, volume 4047 of *Lecture Notes in Computer Science*, pages 310–327, Springer, 2006.

KL51. S. Kullback and R. A. Leibler, *On Information and Sufficiency*, Ann. Math. Statist. **22**(1), 79–86 (1951).

Luc00. S. Lucks, The Sum of PRPs Is a Secure PRF, in *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 470–484, Springer, 2000.

LV87. F. Liese and I. Vajda, *Convex Statistical Distances*, Teubner, Leipzig, 1987.

Men19. B. Mennink, Linking Stam's Bounds with Generalized Truncation, in *Topics in Cryptology – CT-RSA 2019*, edited by M. Matsui, pages 313–329, Cham, 2019, Springer International Publishing.

MN17. B. Mennink and S. Neves, Encrypted Davies-Meyer and its dual: Towards optimal security using Mirror theory, Cryptology ePrint Archive, Report 2017/xxx, to be published in CRYPTO 2017, 2017, `http://eprint.iacr.org/2017/537`.

MPS12. A. Mandal, J. Patarin and Y. Seurin, On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction, in *Theory of Cryptography*, edited by R. Cramer, pages 285–302, Berlin, Heidelberg, 2012, Springer Berlin Heidelberg.

Pat08a. J. Patarin, The "Coefficients H" Technique, in *Selected Areas in Cryptography, 2008*, volume 5381 of *LNCS*, pages 328–345, Springer, 2008.

Pat08b. J. Patarin, A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations, in *ICITS 2008*, volume 5155 of *LNCS*, pages 232–248, Springer, 2008.

Pat10. J. Patarin, Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography., Cryptology ePrint Archive, Report 2017/287, 2010, `http://eprint.iacr.org/2010/287`.

Rei12. R.-D. Reiss, *Approximate distributions of order statistics: with applications to nonparametric statistics*, Springer Science & Business Media, 2012.

Sli16. A. Slivkins, Lecture Notes CMSC 858G: Bandits, Experts and Games (Lecture 3), September 2016, `http://www.cs.umd.edu/~slivkins/CMSC858G-fall16/Lecture3.pdf`.

Sta78. A. J. Stam, *Distance between sampling with and without replacement*, Statistica Neerlandica **32**(2), 81–91 (1978).

YMO08. K. Yoneyama, S. Miyagawa and K. Ohta, Leaky Random Oracle (Extended Abstract), in *Provable Security*, edited by J. Baek, F. Bao, K. Chen and X. Lai, pages 226–240, Berlin, Heidelberg, 2008, Springer Berlin Heidelberg.

Appendix A Proof of the χ^2 method

In this section we provide proof of Theorem 1, which is the heart of the χ^2 method. The proof is based on Lemma 2, Lemma 3, and Theorem 5. Along the way we also briefly mention some (relevant) facts of KL divergence and χ^2 distance.

KULLBACK-LEIBLER DIVERGENCE. *Kullback-Leibler divergence* (KL divergence) or *relative entropy* between $\mathbf{P_0}$ to $\mathbf{P_1}$ is defined as

$$d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1}) = \sum_{X \in \Omega} \mathbf{P_0}(X) \log \frac{\mathbf{P_0}(X)}{\mathbf{P_1}(X)}.$$

Note that the KL divergence is defined only if $\mathbf{P_0} \ll \mathbf{P_1}$ (with the convention that $0 \log \frac{0}{0} = 0$). It was first defined by Kullback and Leibler in 1951 ([KL51]) as a generalization of the entropy notion of Shannon (see [CT06]).

It can be shown that the KL divergence between any two distributions is always non-negative (known as *Gibbs' inequality*, see [CT06]). However, it is not symmetric (i.e., $d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1}) \neq d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1})$ in general) and does not satisfy the triangle inequality. Thus, KL divergence is not a metric.

Though not a metric, KL divergence has some useful properties. For example, the KL divergence between any two product distributions is additive over the corresponding marginals (see [CT06], [Rei12]). The KL divergence between two joint distribution can be obtained as the sum of the KL divergences of corresponding conditional distributions. This is known as the *chain rule of KL divergence.* It is one of the crucial parts of the χ^2 method. We elaborate it in more detail below.

Chain rule of KL divergence. Let $\mathbf{P_0^q}$ and $\mathbf{P_1^q}$ be two probability distributions over Ω^q. We denote $\mathbf{P_0^i}$ and $\mathbf{P_1^i}$ to represent the marginal probability distributions for first i coordinates of $\mathbf{P_0^q}$ and $\mathbf{P_1^q}$ respectively, $1 \le i \le q$. In other words, if $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{Y} := (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$ are two joint random variables following the probability distributions $\mathbf{P_0^q}$ and $\mathbf{P_1^q}$ then $\mathbf{P_0^i}$ and $\mathbf{P_1^i}$ represent the probability distributions of X^i and Y^i respectively. We recall that $\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)$ denotes the conditional distribution $\mathbf{P}(\mathsf{X}_i = x_i | \mathsf{X}^{i-1} = x^{i-1})$ and similarly $\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)$. Moreover, $\mathrm{KL}(x^{i-1}) = d_{\mathrm{KL}}(\mathbf{P}_{\mathbf{0}|x^{i-1}}, \mathbf{P}_{\mathbf{1}|x^{i-1}})$. Now we state chain rule of KL divergence.

Lemma 2 (Chain rule of KL divergence (see [CT06], Theorem 2.5.3)). *Following the above notations,*

$$d_{\mathrm{KL}}(\mathbf{P_0^q}, \mathbf{P_1^q}) = d_{\mathrm{KL}}(\mathbf{P_0^1}, \mathbf{P_1^1}) + \sum_{i=2}^{q} \mathbf{Ex}[\mathrm{KL}(\mathsf{X}^{i-1})].$$

Proof.

$$\begin{aligned}
d_{\mathrm{KL}}(\mathbf{P_0^q}, \mathbf{P_1^q}) &= \sum_{x^q \in \Omega^q} \mathbf{P_0^q}(x^q) \log \left(\frac{\mathbf{P_0^q}(x^q)}{\mathbf{P_1^q}(x^q)} \right) \\
&= \sum_{x^q \in \Omega^q} \mathbf{P_0^q}(x^q) \log \left(\frac{\prod_{i=1}^q \mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\prod_{i=1}^q \mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)} \right) \\
&= \sum_{x^q \in \Omega^q} \mathbf{P_0^q}(x^q) \sum_{i=1}^{q} \log \left(\frac{\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)} \right) \\
&= \sum_{i=1}^{q} \sum_{x^q \in \Omega^q} \mathbf{P_0^q}(x^q) \log \left(\frac{\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)} \right) \\
&= \sum_{i=1}^{q} \sum_{x^i \in \Omega^i} \mathbf{P_0^i}(x^i) \log \left(\frac{\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)} \right) \\
&= \sum_{i=1}^{q} \sum_{x^i \in \Omega^i} \mathbf{P_0^{i-1}}(x^{i-1}) \mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i) \log \left(\frac{\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)} \right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{q} \sum_{x^{i-1}\in\Omega^{i-1}} \mathbf{P}_{\mathbf{0}}^{\boldsymbol{i-1}}(x^{i-1}) \sum_{X_i} \mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i) \log\left(\frac{\mathbf{P}_{\mathbf{0}|x^{i-1}}(x_i)}{\mathbf{P}_{\mathbf{1}|x^{i-1}}(x_i)}\right) \\
&= \sum_{i=1}^{q} \sum_{x^{i-1}\in\Omega^{i-1}} \mathbf{P}_{\mathbf{0}}^{\boldsymbol{i-1}}(x^{i-1})\mathrm{KL}(x^{i-1}) \\
&= \sum_{i=1}^{q} \mathbf{Ex}[\mathrm{KL}(\mathsf{X}^{i-1})] \qquad \square
\end{aligned}
$$

The next inequality due to Pinsker (see [CT06]) gives an upper bound on the total variation distance between two distributions in terms of their KL divergence.

Theorem 5 (Pinsker's Inequality). *For every probability functions* $\mathbf{P_0}, \mathbf{P_1}$*,*

$$
d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) \le \sqrt{\frac{1}{2} d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1})}.
$$

Proof.We follow the steps of [Sli16]. Let $\Omega' = \{x \in \Omega | \mathbf{P_0}(x) \ge \mathbf{P_1}(x)\}$. Also, let $p_i = \sum_{x\in\Omega'} \boldsymbol{P_i}(x)$ for $i \in \{0,1\}$. So, $d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1}) = p_0 - p_1$. Also, by *logsum inequality*[8], we have $d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1}) \ge p_0 \log \frac{p_0}{p_1} + (1-p_0)\log\frac{(1-p_0)}{(1-p_1)}$. Therefore,

$$
\begin{aligned}
d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1}) &\ge p_0 \log \frac{p_0}{p_1} + (1-p_0)\log\frac{(1-p_0)}{(1-p_1)} \\
&= \int_{p_1}^{p_0} \left(\frac{p_0}{x} - \frac{(1-p_0)}{(1-x)}\right) dx \\
&= \int_{p_1}^{p_0} \frac{p_0 - x}{x(1-x)} dx \\
&\ge 2(p_0 - p_1)^2 = 2 d_{\mathrm{TV}}(\mathbf{P_0}, \mathbf{P_1})^2, \quad (\text{since } x(1-x) \le \frac{1}{4}).\square
\end{aligned}
$$

χ^2 DISTANCE. χ^2 distance has its origin in mathematical statistics dating back to Pearson (see [LV87] for some history). The χ^2 distance between $\mathbf{P_0}$ and $\mathbf{P_1}$, with $\mathbf{P_0} \ll \mathbf{P_1}$, is defined as

$$
d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1}) := \sum_{x\in\Omega} \frac{(\mathbf{P_0}(x) - \mathbf{P_1}(x))^2}{\mathbf{P_1}(x)}.
$$

It can be seen that χ^2 distance is not symmetric. Therefore, it is not a metric. However, like KL-divergence, χ^2 distance between product distributions can be bounded in terms of the χ^2 distances between their marginals (see [Rei12]). The following lemma shows that KL-divergence between two distributions can be upper bounded by their χ^2-distance. The first inequality can also be found in earlier works (see [GS02] for this and many other relations among various distances used in Statistics).

Lemma 3. $d_{\mathrm{KL}}(\mathbf{P_0}, \mathbf{P_1}) \le \log(1 + d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1})) \le d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1})$.

Proof. By the definition of χ^2-distance we have

$$
\begin{aligned}
\log(1 + d_{\chi^2}(\mathbf{P_0}, \mathbf{P_1})) &= \log\left(\sum_{x\in\Omega} \mathbf{P_0}(x)\frac{\mathbf{P_0}(x)}{\mathbf{P_1}(x)}\right) \\
&= \log\left(\mathbf{Ex}\left[\frac{\mathbf{P_0}(x)}{\mathbf{P_1}(x)}\right]\right)
\end{aligned}
$$

[8] Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be nonnegative numbers. We denote the sum $\sum_i a_i$ and $\sum_i b_i$ by a and b respectively. The log sum inequality states that $\sum_{i=1}^{n} a_i \log \frac{a_i}{b_i} \ge a \log \frac{a}{b}$.

$$
\begin{aligned}
&\geq \mathbf{Ex}\left[\log\left(\frac{\mathbf{P_0}(x)}{\mathbf{P_1}(x)}\right)\right] \text{ by Jensen's inequality}\\
&= \sum_{x\in\Omega}\mathbf{P_0}(x)\log\left(\frac{\mathbf{P_0}(x)}{\mathbf{P_1}(x)}\right)\\
&= d_{\mathrm{KL}}(\mathbf{P_0},\mathbf{P_1})
\end{aligned}
$$

The last inequality follows by observing that $d_{\chi^2}(\mathbf{P_0},\mathbf{P_1})) \geq 0$ and $\log(1+t) \leq t$ for $t \geq 0$. □

A.1 Proof of Theorem 1

We are now ready to show the upper bound on $d_{\mathrm{TV}}(\mathbf{P}_\mathbf{0}^{\boldsymbol{q}},\mathbf{P}_\mathbf{1}^{\boldsymbol{q}})$ in terms of expected value of χ^2-distance between the conditional distributions $\mathbf{P}_{\mathbf{0}|x^{i-1}}$ and $\mathbf{P}_{\mathbf{1}|x^{i-1}}$. We state and prove the χ^2 method, i.e. Theorem 1.

Proof of Theorem 1. The proof follows directly from Pinsker's inequality (Theorem 5), chain rule of KL divergence (Lemma 2), and Lemma 3. More precisely, we have

$$
\begin{aligned}
d_{\mathrm{TV}}(\mathbf{P}_\mathbf{0}^{\boldsymbol{q}},\mathbf{P}_\mathbf{1}^{\boldsymbol{q}}) &\leq \left(\frac{d_{\mathrm{KL}}(\mathbf{P}_\mathbf{0}^{\boldsymbol{q}},\mathbf{P}_\mathbf{1}^{\boldsymbol{q}})}{2}\right)^{\frac{1}{2}} \text{ by Theorem 5}\\
&= \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}[\mathrm{KL}(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}} \text{ by Lemma 2}\\
&\leq \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}} \text{ by Lemma 3} \qquad \square
\end{aligned}
$$