IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2018, No. 1, pp. 314–335. DOI:10.13154/tosc.v2018.i1.314-335

Revisiting Variable Output Length XOR Pseudorandom Function

Srimanta Bhattacharya, Mridul Nandi

Indian Statistical Institute, Kolkata, India.
mail.srimanta@gmail.com,mridul.nandi@gmail.com

Abstract. Let σ be some positive integer and $\mathscr{C} \subseteq \{(i,j) : 1 \leq i < j \leq \sigma\}$. The theory behind finding a lower bound on the number of distinct blocks $P_1, \ldots, P_\sigma \in \{0,1\}^n$ satisfying a set of linear equations $\{P_i \oplus P_j = c_{i,j} : (i,j) \in \mathscr{C}\}$ for some $c_{i,j} \in \{0,1\}^n$, is called *mirror theory*. Patarin introduced the mirror theory and provided a proof for this. However, the proof, even for a special class of equations, is complex and contains several non-trivial gaps. As an application of mirror theory, $\mathsf{XORP}[w]$ (known as XOR construction) returning $(w-1)$ block output, is a *pseudorandom function* (PRF) for some parameter w, called *width*. The XOR construction can be seen as a basic structure of some encryption algorithms, e.g., the CENC encryption and the CHM authenticated encryption, proposed by Iwata in 2006. Due to potential application of $\mathsf{XORP}[w]$ and the nontrivial gaps in the proof of mirror theory, an alternative simpler analysis of PRF-security of $\mathsf{XORP}[w]$ would be much desired. Recently (in Crypto 2017) Dai *et al.* introduced a tool, called the χ^2 method, for analyzing PRF-security. Using this tool, the authors have provided a proof of PRF-security of $\mathsf{XORP}[2]$ without relying on the mirror theory. In this paper, we resolve the general case; we apply the χ^2 method to obtain *a simpler security proof of* $\mathsf{XORP}[w]$ *for any* $w \geq 2$. For $w = 2$, we obtain *a tighter bound for a wider range of parameters* than that of Dai *et al.*. Moreover, we consider variable width construction $\mathsf{XORP}[*]$ (in which the widths are chosen by adversaries adaptively), and also provide *variable output length pseudorandom function* (VOLPRF) security analysis for it. As an application of VOLPRF, we propose *an authenticated encryption which is a simple variant of CHM or AES-GCM and provides much higher security* than those at the cost of one extra blockcipher call for every message.

Keywords: PRF, PRP, χ^2 method, mirror theory, CENC.

1 Introduction

Let $\mathscr{G}$ be a set of size N. Suppose a *without replacement* (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$ is given. Based on this sample, we want to derive σ pseudorandom elements for some $\sigma \leq \bar{\sigma}$. Here, we measure the pseudorandomness of a distribution by the *total variation* (also known as the statistical distance) between the distribution and the uniform distribution. Of course, the original sample would be a choice for pseudorandom sample from $\mathscr{G}$ (in this case $\bar{\sigma} = \sigma$). However, the total variation between random WOR sample and a random WR sample is about $\sigma(\sigma-1)/2N$ which is the *collision probability* of a true random sample of size σ. So, the total variation is negligible only when $\sigma \ll \sqrt{N}$. Therefore, a natural question arises: can we generate a sample for which the total variation remains negligible even for $\sigma > \sqrt{N}$?

The above problem is well motivated in symmetric key cryptography due to its relevance in constructing *pseudorandom functions* (PRFs) from *pseudorandom permutations* (PRPs)[1].

[1] This line of work was initiated by Bellare *et al.* in [BKR98], who termed it "Luby-Rackoff backwards".

Received: 2017-09-01, Revised: 2017-11-23, Accepted: 2018-01-23, Published: 2018-03-01

More specifically, a *blockcipher* is modeled as a PRP, i.e., ideally it generates a random WOR sample. On the other hand, a PRF ideally generates a random WR sample. So, constructing a PRF based on a blockcipher requires to generate a pseudorandom sample from a random WOR sample. In this context, N is the size of the domain and range of the blockcipher and σ is the total number of blocks an adversary can query. Hence, negligible total variation (which is an upper bound of the *distinguishing advantage* of the adversary) for larger choices of σ would be always desired. There are several known blockcipher based PRF constructions; some of them can be found in [BKR00, Nan09, IK03, BR02, LPTY16]. All these constructions suffer from the *birthday attack*. There are few deterministic blokcipher based *beyond birthday* constructions, namely PMAC_Plus [Yas11, DDN+17], LightMAC+ [Nai17] and 3kf9 [ZWSW12].

Now, we describe two known and very basic strategies to generate almost random sample, i.e., pseudorandom sample based on a WOR random sample $T_1, \ldots T_{\bar{\sigma}}$ from $\mathcal{G}$ and their applications to cryptography. The first method is based on truncation of a WOR sample and the second method is based on taking differences of a WOR sample. Our focus in this work is on the latter one.

1. Truncation of a WOR Sample. This has been studied by Stam (in a statistical context) in 1978 [Sta78] and later by many others (e.g., [GG16, GGM17, HWKS98]). Suppose $\mathcal{G}'$ is a set of size M such that M divides N. Let $f : \mathcal{G} \to \mathcal{G}'$ be a *regular function* (i.e., for all $y \in \mathcal{G}'$, there are exactly N/M elements $x \in \mathcal{G}$ such that $f(x) = y$). For example, when $\mathcal{G} = \{0,1\}^n$, the *truncation function* trunc_m which chops $(n-m)$ bits of its input to return an m-bit output is a regular function. Now, consider the new sample $S_1, \ldots, S_{\bar{\sigma}}$, where $S_i = \mathsf{trunc}_m(T_i)$ for $1 \le i \le \bar{\sigma}$ (in this case $\sigma = \bar{\sigma}$). Stam showed that total variation between $(S_1, \ldots, S_{\bar{\sigma}})$ and a true random sample $(R_1, \ldots, R_{\bar{\sigma}})$ over $\mathcal{G}'$ is at most $\bar{\sigma}\sqrt{M/N^2}$. This bound has been recently shown to be tight in [GG16, GGM17].[2]

As an application to cryptography, let $e_K : \{0,1\}^n \to \{0,1\}^n$ be a blockcipher, modeled to be pseudorandom permutation for a randomly chosen key K. Then, for $m \le n$, the truncated blokcipher $\mathsf{trunc}_m(e_K(x))$ has the maximum distinguishing advantage $\bar{\sigma}/2^{n-\frac{m}{2}}$, where $\bar{\sigma}$ is the total number of queries. The truncation of blockcipher is used for the key derivation function of the AES-GCM construction [GLL17, GL17, IS17].

2. Differences of WOR Samples. Let us assume that $\mathcal{G}$ is an abelian group under the group operation "+"(with $-$ as the inverse). Let $\bar{\sigma} = cw$ for some integers c and $w \ge 2$. Let us denote the WOR sample of size $\bar{\sigma}$ as $\mathsf{T} := (T_{i,j} : 1 \le i \le c, 1 \le j \le w)$. We call the sub-sample $(T_{i,1}, \ldots, T_{i,w})$ the i^{th} chunk of the sample. For each chunk, we derive $w-1$ pseudorandom elements of $\mathcal{G}$ as follows.

$$S_{i,1} = T_{i,1} - T_{i,w}, S_{i,2} = T_{i,2} - T_{i,w}, \ldots, S_{i,w-1} = T_{i,w-1} - T_{i,w}.$$

Thus, we get a new sample $\mathsf{S} := (S_{i,j} : 1 \le i \le c, 1 \le j \le w-1)$ of size $\sigma = c(w-1)$ from a sample of size $\bar{\sigma}$. Our main focus in this work is to upper bound the total variation between S and a true random sample of size σ.

$\mathsf{XORP}[w]$ **Construction**. Let us take $\mathcal{G} = \{0,1\}^n$ with the group operation being the bit-wise $\oplus$. The above computation of S-values can be viewed as the following PRF construction $\mathsf{XORP}[w]$ for different inputs.

$$\mathsf{XORP}[w](x) = \big(e_K(x\|\langle 0\rangle_s) \oplus e_K(x\|\langle 1\rangle_s)\big)\| \cdots \|\big(e_K(x\|\langle 0\rangle_s) \oplus e_K(x\|\langle w-1\rangle_s)\big),$$

where $s \le \lceil \log_2 w \rceil$, $x \in \{0,1\}^{n-s}$ and $\langle i\rangle_s$ is the s-bit representation of i. In particular, when we compute $\mathsf{XORP}[w](x_1), \ldots, \mathsf{XORP}[w](x_c)$, we evaluate $T_{i,j+1} := e_K(x_i\|\langle j\rangle_s)$, for

[2] Similar claim had been made long time back by Hall et al. [HWKS98] when they study truncation of output of a pseudorandom permutation. If $\mathcal{G} = \{0,1\}^n$ and $\mathcal{G}' = \{0,1\}^m$ then one can take the function f to be the truncation function which truncates, say the last $(n-m)$ bits.

$1 \leq i \leq c$ and $1 \leq j \leq w-1$ and then we compute $S_{i,j} = T_{i,j} \oplus T_{i,w}$. Note that $T_{i,j}$ values are random WOR in case we replace the blockcipher by an ideal blockcipher (random permutation). This construction and specifically $\mathsf{XORP}[2]$ was studied by several authors independently (see [Pat08b, Pat10, Luc00, BI99]).

Mirror Theory. Patarin introduced a combinatorial problem motivated from the PRF-security of $\mathsf{XORP}[w]$ type constructions. Informally, mirror theory (see [Pat10]) provides a suitable lower bound on the number of solutions of distinct blocks $P_1, \ldots, P_{\bar{\sigma}} \in \{0,1\}^n$ satisfying a system of linear equations involving only two variables at a time. For example, we may consider the following system of equations

$$\{P_{(i-1)w+j} \oplus P_{iw} = c_{i,j} : 1 \leq i \leq c, 1 \leq j \leq w-1\}$$

motivated from $\mathsf{XORP}[w]$ construction (with a renaming of $P_{(i-1)w+j}$ as $P_{i,j}$) for some nonzero $c_{i,j} \in \{0,1\}^n$ so that $c_{i,1}, \ldots, c_{i,w-1}$ are distinct for every i. Patarin showed a lower bound on the number of such solutions. As an application of coefficient-H technique [Vau03, Pat08a, IMV16], this leads to a bound of PRF distinguishing advantage of XORP. Mirror theory seems to be very powerful as it can be applied to prove optimum security for many constructions such as EDM, EWCDM etc. [MN17]. However, the proof of the mirror theory is quite complex and contains several nontrivial gaps. In fact, Patarin later provided an alternative proof for PRF-security of xor of k independent blockcipher constructions [CLP14], which is simpler but sub-optimal and follows easily from the mirror theory.

χ^2 Method and Its Application to $\mathsf{XORP}[2]$. Recently (in [DHT17]), Dai *et al.* provided optimum security proof for $\mathsf{XORP}[2]$ construction using a method which they term χ^2 method. This method was implicitly used by Stam ([Sta78]) while proving the bound on the total variation between the truncated WOR sample and the true random sample. While the context of Stam's work is purely statistical, the work of Dai *et al.* explicitly demonstrated the usefulness of the χ^2 method in cryptographic context. We will provide a brief overview of this method in Section 2.

Our Contribution. A simpler and transparent proof of mirror theory in general, and PRF-security of $\mathsf{XORP}[w]$ construction in particular, is well desired. In this paper, we focus on the PRF-security of $\mathsf{XORP}[w]$ construction for any $w \geq 2$, and its variable width version $\mathsf{XORP}[*]$ (in which the width would be given as an input of the construction). In particular, using the χ^2 method we show that the PRF-advantage of $\mathsf{XORP}[w]$ against an adversary making at most q queries is bounded by

$$\frac{\sqrt{2}w^2q}{N} + \frac{w(w-1)q}{2N}.$$

Moreover, when $w = 2$ and $(\mathscr{G}, +) = (\{0,1\}^n, \oplus)$ (and so $N = 2^n$), the upper bound on the PRF-advantage can be further improved to

$$\left(\frac{2(N-1)q^3}{(N-2q)^4}\right)^{\frac{1}{2}} + \frac{q}{N}.$$

Dai *et al.* proved that the PRF-advantage for $\mathsf{XORP}[2]$ is at most $\frac{1.5q+3\sqrt{q}}{2^n}$ provided $q < 2^{n-5}$. So, our bound is an improvement, and works even when $q > 2^{n-5}$. We also describe a simple adversary with advantage at least about $\frac{w(w-1)q}{2N}$, and hence our bound is tight. For $\mathsf{XORP}[*]$, we show that its PRF-advantage of an adversary making queries with widths $w_1, \ldots, w_q$ is at most

$$\frac{(1+\sqrt{2})w_{max}\bar{\sigma}}{N},$$

where $w_{max} = \max_i w_i$, and $\bar{\sigma} = \sum_i w_i$. Formal statement of our results are given as Theorem 2 and Theorem 3.

An immediate application of our result is the improvement of the PRF-security of CENC [Iwa06]. Also, we consider a variant of the GCM authenticated encryption [MV04] (can also be viewed as a variant of CHM or CIP authenticated encryption [Iwa06, Iwa08]). For this variant, we obtain beyond birthday security with one extra blockcipher call when the message length is not too large.

Organization of the Paper. The paper is organized as follows. In the next section, we discuss preliminaries; there we formalize the notation that we use throughout the paper, briefly cover the required security notions and provide a brief outline of the χ^2 method. In Section 3, we state and prove our main results. Subsequently, in Section 4, we present applications of our results. Finally we conclude in Section 5.

2 Preliminaries

2.1 Notation and Setup

In this paper we fix an *abelian group* $\mathscr{G}$ of size N. We use "+" to denote the group addition and "−" to denote its inverse operation. We denote the identity element as $\mathtt{0}$. We call elements of $\mathscr{G}$ blocks. The most popular choice of the group in cryptography is $\mathscr{G} = \{0,1\}^n$, for some positive integer n, with bit-wise xor as an addition. In this case, 0^n is the identity $\mathtt{0}$ and $N = 2^n$.

For a positive integer s, we denote an s-tuple $(x_1, \ldots, x_s)$ as x^s. In this paper we consider an integer parameter $w \geq 2$ (called *width*). A w-tuple $z = (z_1, \ldots, z_w) \in \mathscr{C} := \mathscr{G}^w$ is called *chunk*. We use a shorthand notation $[c]$ to denote the set $\{1, 2, \ldots, c\}$ for every positive integer c. A c-tuple of chunks $x^c = (x_1, \ldots, x_c) \in \mathscr{C}^c$ is also denoted as $(x_{i,j} : i \in [c], j \in [w])$, where $x_i := (x_{i,1}, \ldots, x_{i,w}) \in \mathscr{G}^w$ for all i. In general for a set I of size s, $(x_i : i \in I) \in \mathscr{G}^s$ is a block tuple. A tuple of blocks $(x_i : i \in I) \in \mathscr{G}^s$ is called *block-wise distinct* if all x_i's are distinct.

For a random variable X, we write $\Pr_X$ to denote the probability distribution (or function) corresponding to X. Sample space of a random variable X is a set Ω so that $\Pr_X(\Omega) = 1$. Support of X is the sample space Ω of X so that for all $x \in \Omega$, $\Pr_X(x) > 0$. Given a set $\mathcal{S}$ and the tuple $X^s := (X_1, \ldots, X_s)$, we will write $(X_1, \ldots, X_s) \leftarrow\!\!\$\ \mathcal{S}$ to mean that X_i's are sampled uniformly and independently from the set $\mathcal{S}$. Moreover, these are also independent with all other previously sampled random variables in the context. A sample, i.e., a particular realization of X^s will be denoted by $x^s := (x_1, \ldots, x_s)$.

Let $\mathcal{S}$ be a set of size M and s be a positive integer. We write $(X_1, \ldots, X_s) \leftarrow_{\mathrm{wr}} \mathcal{S}$ to represent that $X_1, \ldots, X_s$ are chosen randomly in WR manner from $\mathcal{S}$ (i.e., $X_1, \ldots, X_s \leftarrow\!\!\$\ \mathcal{S}$). Similarly, we write $(X_1, \ldots, X_s) \leftarrow_{\mathrm{wor}} \mathcal{S}$ to mean that X_i's are randomly sampled in WOR manner from the set $\mathcal{S}$. Let

$$\mathcal{S}^{\underline{s}} = \{(x_1, \ldots, x_s) : x_i\text{'s are distinct elements of } \mathcal{S}\}$$

be the set of all block-wise distinct s tuples of blocks. Note that $|\mathcal{S}^{\underline{s}}| = M(M-1)\cdots(M-s+1)$. We use short hand notation $M^{\underline{s}} := M(M-1)\cdots(M-s+1)$. In this notation, a WOR sample X^s is chosen uniformly from $\mathcal{S}^{\underline{s}}$, i.e., $X^s \leftarrow_{\mathrm{wor}} \mathcal{S}^{\underline{s}}$. In other words,

$$\Pr[X^s = a^s] = \frac{1}{|\mathcal{S}|^{\underline{s}}}, \text{ for all } a^s \in \mathcal{S}^{\underline{s}}.$$

So $\mathcal{S}^{\underline{s}}$ is the support of X^s.

A subset $\boldsymbol{\mathscr{V}}_r \subseteq \mathscr{G}$ of size r is called a random r-set if it is chosen uniformly from the set of all r sized subsets of $\mathscr{G}$. Thus, for every $\mathscr{V} \subseteq \mathscr{G}$,

$$\Pr[\boldsymbol{\mathcal{V}}_r = \mathcal{V}] = \binom{N}{r}^{-1}.$$

Throughout the paper we denote a random r-set in $\mathcal{G}$ as $\boldsymbol{\mathcal{V}}_r$. A random r-set can be constructed by drawing a random WOR sample, i.e., $\boldsymbol{\mathcal{V}}_r = \{X_1, \ldots, X_r\}$, where $(X_1, \ldots, X_r) \leftarrow_{\text{wor}} \mathcal{G}$. Note that the complement set $\mathcal{G} \setminus \boldsymbol{\mathcal{V}}_r$ is a random $(N-r)$-set.

2.2 Security Definitions

Pseudorandom function (or PRF) is a very important security notion in cryptography. For example, while analyzing message authentication code (MAC), we mostly study 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 PRF and PRP-advantage of a *keyed function*. Let m and p be positive integers.

1. Let RP_m denote the m bit random permutation chosen uniformly from Perm_m, the set of all permutations on $\{0,1\}^m$, i.e., in notation $\mathsf{RP}_m \leftarrow_{\$} \mathsf{Perm}_m$.

2. Similarly, $\mathsf{RF}_{m\to p} \leftarrow_{\$} \mathsf{Func}_{m\to p}$, where $\mathsf{Func}_{m\to p}$ is the set of all functions from $\{0,1\}^m$ to $\{0,1\}^p$, and we call $\mathsf{RF}_{m\to p}$ random function (from m bits to p bits).

Let $\mathscr{K}$ be a finite set. Given a function $f : \mathscr{K} \times \{0,1\}^m \to \{0,1\}^p$, for every $k \in \mathscr{K}$, we denote by f_k the function (also termed a *keyed function*) $f(k,\cdot) \in \mathsf{Func}_{m\to p}$. We call the set $\mathscr{K}$ the *key space* of the keyed function.

Definition 1 (PRF and PRP-advantage)**.** Let $\mathscr{A}$ be a distinguisher (i.e. an oracle algorithm[3]) and $f : \mathscr{K} \times \{0,1\}^m \to \{0,1\}^p$ be a keyed function. Then, the PRF-advantage of $\mathscr{A}$ against f is defined as

$$\mathbf{Adv}_f^{\text{prf}}(\mathscr{A}) = |\Pr[\mathscr{A}^{f_K} \to 1 \ : \ K \leftarrow_{\$} \mathscr{K}] - \Pr[\mathscr{A}^{\mathsf{RF}_{m\to p}} \to 1]|.$$

Similarly, the PRP-advantage of $\mathscr{A}$ against a keyed permutation f (in this case $m = p$) is defined as

$$\mathbf{Adv}_f^{\text{prp}}(\mathscr{A}) = |\Pr[\mathscr{A}^{f_K} \to 1 \ : \ K \leftarrow_{\$} \mathscr{K}] - \Pr[\mathscr{A}^{\mathsf{RP}_p} \to 1]|.$$

As we restrict to only deterministic keyed function (i.e., it returns identical outputs on same queries) there is no loss of generality to assume that the adversary does not repeat its queries. In other words, *if $Q_1, \ldots, Q_q$ are all queries then these must be distinct.* For information theoretic security, we assume $\mathscr{A}$ to be computationally unbounded. Therefore, we can also assume that $\mathscr{A}$ is deterministic as it can always run with the best random coins which maximizes the advantage. Suppose $\mathscr{A}$ makes q distinct queries $Q_1, \ldots, Q_q$ adaptively to the random function $\mathsf{RF}_{m\to p}$ (or the keyed function f_K with $K \leftarrow_{\$} \mathscr{K}$) and obtains responses $R_1, \ldots, R_q$ (or $X_1, \ldots, X_q$ respectively). Note that $R_1, \ldots, R_q \leftarrow_{\text{wr}} \{0,1\}^p$. We denote the probability distributions associated to $\mathsf{R} = (R_1, \ldots, R_q)$ and $\mathsf{X} = (X_1, \ldots, X_q)$ by $\Pr_{\mathsf{R}}$ and $\Pr_{\mathsf{X}}$ respectively. Thus, from the definition of PRF-advantage we have

$$\mathbf{Adv}_f^{\text{prf}}(\mathscr{A}) = |\Pr_{\mathsf{R}}(\mathscr{E}) - \Pr_{\mathsf{X}}(\mathscr{E})|,$$

where $\mathscr{E}$ is the set of all q-tuple responses $x^q = (x_1, \ldots, x_q) \in (\{0,1\}^p)^q$ at which $\mathscr{A}$ returns 1. Similarly, when $\mathscr{A}$ is interacting with RP_m and obtains responses $T_1, \ldots, T_q$ then it is easy to see that $(T_1, \ldots, T_q) \leftarrow_{\text{wor}} \{0,1\}^m$.

[3] An oracle distinguisher sends queries $Q_1, \ldots, Q_q$ to an oracle adaptively and obtains the corresponding responses $X_1, \ldots, X_q$. Finally it returns 0 or 1.

It is well known that the *statistical distance* or *total variation distance* between two distributions $\mathbf{P_0}$ and $\mathbf{P_1}$ satisfies the following relation:

$$\|\mathbf{P_1} - \mathbf{P_0}\| \stackrel{\text{def}}{=} \frac{1}{2} \sum_{x^q \in (\{0,1\}^p)^q} |\mathbf{P_0}(x^q) - \mathbf{P_1}(x^q)| = \max_{\mathscr{E}' \subseteq (\{0,1\}^p)^q} (\mathbf{P_0}(\mathscr{E}') - \mathbf{P_1}(\mathscr{E}')). \quad (1)$$

Hence,

$$\mathbf{Adv}_f^{\text{prf}}(\mathscr{A}) = |\Pr_{\mathsf{R}}(\mathscr{E}) - \Pr_{\mathsf{X}}(\mathscr{E})| \le \|\Pr_{\mathsf{R}} - \Pr_{\mathsf{X}}\|.$$

Therefore, $\|\Pr_{\mathsf{R}} - \Pr_{\mathsf{X}}\|$ serves as an upper bound on the PRF-advantage of the adversary $\mathscr{A}$ against f. In this work, we will obtain an upper bound on $\|\Pr_{\mathsf{R}} - \Pr_{\mathsf{X}}\|$ for some keyed function f (to be described in the next section).

2.3 χ^2 Method for Bounding Total Variation

We now describe a recently introduced tool to bound total variation between two random vectors. Given a set Ω, let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q. For every $i \in [q]$, we write $\Pr_{\mathsf{X}}(x_i|x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$. Similarly, we denote $\Pr_{\mathsf{Y}}(x_i|x^{i-1})$. For the special case when $i = 1$, we define $\Pr_{\mathsf{X}}(x_1|x^0) := \Pr[X_1 = x_1]$ and $\Pr_{\mathsf{Y}}(x_1|x^0) := \Pr[Y_1 = x_1]$.

Definition 2. Let Ω_i denote the support of the random variable X^i, for all i. Suppose for every i, the support of Y^i contains Ω_i. For every $x^{i-1} \in \Omega_{i-1}$, $i \ge 1$, χ^2-distance[4] between these two conditional probability distributions is defined as

$$\chi^2(x^{i-1}) := \sum_{x_i \in \Omega_{x^{i-1}}} \frac{\left(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1})\right)^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})} \quad (2)$$

where $\Omega_{x^{i-1}} = \{x_i : x^i \in \Omega_i\}$.

Note that for the above definition to work, x^{i-1} should be in the support of both X^{i-1} and Y^{i-1} (otherwise conditional probabilities are not well defined) and the denominator should be positive. So it is required to assume that the support of X^i is contained in the support of Y^i for all i.

Dai, Hoang, and Tessaro [DHT17] introduced a new method, which they term χ^2 method, to bound the statistical distance between two joint distributions in terms of the expectations of the χ^2-distances of corresponding conditional distributions. More specifically, in terms of our notation and setting, crux of the χ^2 method is the following theorem.

Theorem 1 ([DHT17])**.** *Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then*

$$\|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\| \le \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}}$$

where $\chi^2(\cdot)$ function is computed as in Definition 2 for the probability functions $\Pr_{\mathsf{X}}$ and $\Pr_{\mathsf{Y}}$.

As an aside, we mention that main ingredients of the proof of Theorem 1 are (*i*) Pinsker's inequality, (*ii*) chain rule of *Kullback-Leibler divergence* (KL divergence) [5], and (*iii*) Jensen's inequality : Pinsker's inequality upper bounds the statistical distance between two (joint)

[4] χ^2-distance is a well known metric in statistics dating back to Pearson. See [LV87] for some history.
[5] See [CT06] for background on these topics

distributions by their KL divergence, chain rule of KL divergence expresses the KL divergence of two joint distributions as the sum of the KL divergences between corresponding conditional distributions, and finally Jensen's inequality is used to upper bound the KL divergence between two distributions by their χ^2-divergence.

In [DHT17], Dai *et al.* have applied Theorem 1 to show PRF-security of two well known constructions, namely XORP[2] ([Pat08b, Pat10, BI99, Luc00]) and *encrypted Davies-Meyer* (EDM) ([CS16, MN17]). This method seems to have potential for further application to obtain better bounds (and simplified proofs) on the PRF- security of other constructions where proofs so far have evaded more classical methods, such as the H-coefficient method ([Pat08a]). In fact, much earlier, Stam ([Sta78]) used this method, implicitly and in a purely statistical context, to obtain PRF-security bound of the truncated random permutation construction described in the previous section.

2.4 Some Inequalities

The following inequalities will be used in proofs of our results. Here, we assume N, r, w to be positive integers such that $r, w \geq 2$.

Lemma 1. *If* $(r+w)w \leq N$ *then* $\frac{(N-1)^{\underline{w-1}}}{(N-r)^{\underline{w}}} \leq \frac{4}{N}$.

Proof.

$$\begin{aligned}
\frac{(N-1)^{\underline{w-1}}}{(N-r)^{\underline{w}}} &= \frac{1}{N-r} \times \left(\frac{(N-1)^{\underline{w-1}}}{(N-r)^{\underline{w-1}}} \right) \\
&\leq \frac{1}{N-r} \times \left(\frac{N+1-w}{N-r-w} \right)^{w-1} \\
&\leq \frac{1}{N-\frac{N}{w}} \times \left(\frac{N}{N-r-w} \right)^{w-1} \text{ since } rw < N \\
&\leq \frac{1}{N} \times \frac{1}{\left(1-\frac{1}{w}\right)^{w}} \text{ since } r+w \leq N/w \\
&\leq \frac{4}{N} \text{ since } \left(1-\tfrac{1}{w}\right)^{-w} \leq 4 \text{ for } w \geq 2
\end{aligned}$$

The last inequality $\left(1-\frac{1}{w}\right)^{-w} \leq 4$ for $w \geq 2$ follows from standard calculus.

Lemma 2. *If* $2w < N$ *then* $1 - \frac{(N-r)^{\underline{w}}}{N^{\underline{w}}} \leq \frac{2rw}{N}$.

Proof. Note that $\frac{(N-r)^{\underline{w}}}{N^{\underline{w}}} = \prod_{i=0}^{w-1}(1-\frac{r}{N-i}) \geq (1-\frac{r}{N-w})^w \geq 1-\frac{wr}{N-w}$. The last inequality follows from the fact that $(1-x)^w \geq 1-wx$ for all $0 < x < 1$. So $\frac{(N-r)^{\underline{w}}}{N^{\underline{w}}} \geq 1-\frac{2rw}{N}$ (since $2w \leq N$). This completes the proof. .

3 Main Results

3.1 Pseudorandomness of Fixed Width XOR of WOR Sample

Let $w \geq 2$ (will be called width parameter) and $q \geq 1$ (will denote the number of queries) be integers. Our main results are stated in Theorem 2 and Theorem 3 (a variant of Theorem 2 with variable width). In Theorem 2, we bound the total variation between the probability distributions of the random vectors S and R defined over the same sample space $\mathcal{G}^{q(w-1)}$. The formal description of these random variables are given in Fig 3.1. The random vector

$$\mathsf{R} := (R_{1,1}, R_{1,2}, \ldots, R_{1,w-1}, R_{2,1}, R_{2,2}, \ldots, R_{2,w-1}, \ldots, R_{q,1}, R_{q,2}, \ldots, R_{q,w-1})$$

is a WR sample (represented as a vector) of size $q(w-1)$, each $R_{i,j}$ is sampled from $\mathscr{G}$. In other words, $\mathsf{R} \leftarrow_{\mathrm{wr}} \mathscr{G}^{q(w-1)}$. Whereas,

$$\mathsf{S} := (S_{1,1}, S_{1,2}, \ldots, S_{1,w-1}, S_{2,1}, S_{2,2}, \ldots, S_{2,w-1}, \ldots, S_{q,1}, S_{q,2}, \ldots, S_{q,w-1})$$

is a linear function (described in Fig. 3.1) of a WOR sample

$$\mathsf{T} := (T_{1,1}, T_{1,2}, \ldots, T_{1,w}, T_{2,1}, T_{2,2}, \ldots, T_{2,w}, \ldots, T_{q,1}, T_{q,2}, \ldots, T_{q,w})$$

of size qw, each $T_{i,j}$ is sampled from $\mathscr{G}$. More precisely, $S_{i,j} = T_{i,j} - T_{i,w}$ for all $1 \le i \le q$ and $1 \le j \le w-1$. So both R and S have same sample space $\mathscr{G}^{q(w-1)}$. However, they clearly don't have same support. The support of R is the whole sample space, i.e., $\mathscr{G}^{q(w-1)}$. On the other hand, as $T_{i,j}$'s are distinct, we have

1. $S_{i,j} \neq \mathsf{0}$ for all i, j, and
2. for any i and for all $j \neq j' \le w-1$, $S_{i,j} \neq S_{i,j'}$.

So, for every i, $S_{i,1}, S_{i,2}, \ldots, S_{i,w-1}$ are distinct elements from $\mathscr{G} \setminus \{\mathsf{0}\}$. Now, we define another random variable

$$\mathsf{U} := (U_{1,1}, U_{1,2}, \ldots, U_{1,w-1}, U_{2,1}, U_{2,2}, \ldots, U_{2,w-1}, \ldots, U_{q,1}, U_{q,2}, \ldots, U_{q,w-1})$$

which have the same support as S and also very close to the uniform random vector R (see Lemma 3). More precisely, for every $1 \le i \le q$, $U_i := (U_{i,1}, \ldots, U_{i,w-1}) \leftarrow_{\mathrm{wor}} \mathscr{G} \setminus \{\mathsf{0}\}$ and $U_1, \ldots, U_q$ are jointly independent. Following lemma provides an upper bound on the total variation between U and R.

Lemma 3. *The random vectors R and S are as described in Fig 3.1. Then*

$$\|\Pr_{\mathsf{R}} - \Pr_{\mathsf{U}}\| \le \frac{w(w-1)q}{2N}.$$

Proof. It is easy to see that U is identical with R until (i) for some i, j, $R_{i,j} = \mathsf{0}$ or (ii) for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$. The probability of the first event is at most $\frac{q(w-1)}{N}$ (by applying the union bound), whereas the probability of the second event is at most $q \times \frac{(w-1)(w-2)}{2N}$ by using the union bound and the birthday collision probability. This completes the proof.

Random Experiment for R

$\mathsf{R} := (R_{i,j} : i \in [q], j \in [w-1]) \leftarrow_{\mathrm{wr}} \mathscr{G}$
return R

Random Experiment for U

for $1 \le i \le q$
  $U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\mathrm{wor}} \mathscr{G} \setminus \{\mathsf{0}\}$
return $\mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])$

Random Experiment for S

$\mathsf{T} := (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\mathrm{wor}} \mathscr{G}$
for $1 \le i \le q$
  for $1 \le j \le w-1$
    $S_{i,j} = T_{i,j} - T_{i,w}$
return $\mathsf{S} := (S_{i,j} : i \in [q], j \in [w-1])$

Figure 3.1: Description of sampling methods of random variables R, S and U.

Now, we state our main theorem which provides an upper bound on the total variation between R and S. In other words, it shows the distribution of S is very close to uniform even though it is computed from a non-uniform distribution.

Theorem 2 (Pseudorandomness of S)**.** *Let R and S be the random vectors as described in Fig. 3.1. Then,*

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \leq \frac{\sqrt{2}w^2}{N} + \frac{w(w-1)q}{2N}.$$

Moreover when $w = 2$ and $(\mathscr{G}, +) = (\{0,1\}^n, \oplus)$, we have

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \leq \left(\frac{2(N-1)q^3}{(N-2q)^4}\right)^{\frac{1}{2}} + \frac{q}{N}.$$

Proof. First, in Figure 3.2, we describe the extended random variables X and Y which extends S and U respectively. Here, by extension we mean that S and U are marginal random variables of X and Y respectively. Note that in line 5 of the random experiment for Y, the execution following **else** will not be required in our paper. We will be interested in all those choices of realization of Y for which **else** condition will not be satisfied. It is kept only for the sake of the completeness of the definition.

Random Experiment for X

1 : $\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathscr{G}$
2 : **for** $1 \leq i \leq q$
3 : **for** $1 \leq j \leq w-1$
4 : $S_{i,j} = T_{i,j} - T_{i,w}$
5 : $X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w})$
6 : $S_i = (S_{i,1}, \ldots, S_{i,w-1})$
7 : **return** $\mathsf{X} := (X_1, \ldots, X_q)$

Random Experiment for Y

1 : **initialize** $\mathcal{S}_0 = \mathscr{G}$
2 : **for** $1 \leq i \leq q$
3 : $U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\text{wor}} \mathscr{G} \setminus \{0\}$
4 : $\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
5 : **if** $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \leftarrow_{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
6 : $Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
7 : $\mathcal{S}_i = \mathscr{G} \setminus \big(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\big)$
8 : **return** $\mathsf{Y} := (Y_1, \ldots, Y_q)$

Figure 3.2: X and Y are extended random variables of S and U respectively.

Let $\mathscr{C} = \mathscr{G}^w$ denote the set of all chunks. To understand the probability distributions of the random vectors X and Y and their supports we consider the following permutation ρ over the chunk set $\mathscr{C}$ mapping $(z_1, \ldots, z_w)$ to $(z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$. It is easy to see that ρ is a permutation and $\rho^{-1}(z'_1, \ldots, z'_w) = (z'_1 - z'_w, \ldots, z'_{w-1} - z'_w, z'_w)$. We extend the definition of ρ over $\mathscr{C}^c$ for any c as $\rho^*(x_1, \ldots, x_c) = (\rho(x_1), \ldots, \rho(x_c))$. From the random experiments, it is trivial to see that

1. $\rho(X_i) = T_i := (T_{i,1}, \ldots, T_{i,w})$ and
2. $\rho(Y_i) = V_i := (V_{i,1}, \ldots, V_{i,w})$.

So, for every $i \leq q$, $\rho^*(X^i) = T^i$ and $\rho^*(Y^i) = V^i$. In other words, the random variables X and Y are equivalent to T and $\mathsf{V} := (V_{i,j}, i \in [q], j \in [w])$ respectively. In the first case, we first sample T and then define X by applying ρ^{-1} on each chunk. Whereas, in the second case, we first sample Y and then we define V by applying ρ on each chunk. So for every i, the support of T^i is the set of all block-wise distinct tuples $(a_{i',j} : i' \in [i], j \in [w])$. Hence, the support of X^i, denoted as Ω_i, would be the set of all such iw tuples

$$\Omega_i := \{(x_{i',j} : i' \in [i], j \in [w]) \in \mathscr{G}^{iw} : (a_{i',j} : i' \in [i], j \in [w]) \text{ is block-wise distinct}\},$$

where $\rho(x_{i'}) = a_{i'} := (a_{i',j} : j \in [w])$ for all i'. In fact, for every $x^i \in \Omega_i$, the conditional probability for X can be expressed as

$$\begin{aligned}\Pr_{\mathsf{X}}(x_i \mid x^{i-1}) &\stackrel{\text{def}}{=} \Pr[X_i = x_i \mid X^{i-1} = x^{i-1}] \\ &= \Pr[T_i = a_i \mid T^{i-1} = a^{i-1}] \\ &= \frac{1}{(N-(i-1)w)^{\underline{w}}}. \end{aligned} \tag{3}$$

Now, we show that the support of Y^i contains Ω_i for all i. For all $(x_1, \ldots, x_i) \in \Omega_i$, let us denote $u_i = (x_{i,1}, \ldots, x_{i,w-1})$. So, $x_i = (u_i, x_{i,w})$. As before, let $\rho(x_{i'}) = a_{i'}$ for every $i' \in [i]$. So, $a_{i',j}$'s are distinct. Let $\mathcal{S}_{i-1} = \mathcal{G} \setminus \{a_{i',j} : i' < i, j \in [w]\}$. We define one more set

$$\mathcal{N}^{u_i}(x^{i-1}) := \{v \in \mathcal{S}_{i-1} : v + a_{i,k} \in \mathcal{S}_{i-1} \ \forall k \in [w-1]\}.$$

Given that $U^i = u^i$ and $Y^{i-1} = x^{i-1}$, the set $\mathcal{N}_i$ (defined in the line 5 for the random experiment of Y in Figure 3.2) is exactly the same as the set $\mathcal{N}^{u_i}(x^{i-1})$ defined above. It is easy to observe the following:

If $x^i \in \Omega_i$ then the set $\mathcal{N}^{u_i}(x^{i-1})$ is nonempty as $x_{i,w} \in \mathcal{N}^{u_i}(x^{i-1})$.

So, in this case, we don't execute the else statement in line 5 of the random experiment Y. With these notations, now we prove our next claim on the support of Y.

Claim. For all $x^i \in \Omega_i$,

$$\Pr_{\mathsf{Y}}(x_i \mid x^{i-1}) \stackrel{\text{def}}{=} \Pr[Y_i = x_i \mid Y^{i-1} = x^{i-1}] = \frac{1}{(N-1)^{\underline{w-1}}} \times \frac{1}{|\mathcal{N}^{u_i}(x^{i-1})|}.$$

Since for all $j < i$, $x^j \in \Omega_j$, we have $\Pr[Y^j = x^j] > 0$.

Proof. First, note that $x^{i-1} \in \Omega_{i-1}$, $a_{i,j}$'s are distinct and $x_{i,1}, \ldots, x_{i,w-1}$ are nonzero distinct elements. Moreover, $\mathcal{S}_i$ cannot be the empty set as $x_{i,w} \in \mathcal{S}_i$. So,

$$\begin{aligned}\Pr_{\mathsf{Y}}(x_i \mid x^{i-1}) &\stackrel{\text{def}}{=} \Pr[Y_i = x_i \mid Y^{i-1} = x^{i-1}] \\ &= \Pr[U_i = u_i \mid Y^{i-1} = x^{i-1}] \times \Pr[V_{i,w} = x_{i,w} \mid U_i = u_i \wedge Y^{i-1} = x^{i-1}] \\ &= \frac{1}{(N-1)^{\underline{w-1}}} \times \frac{1}{|\mathcal{N}^{u_i}(x^{i-1})|}. \end{aligned} \tag{4}$$

The last equality follows from the definition of sampling of U_i's and V_i's. ■

We now apply χ^2 method to X and Y.

$$\begin{aligned}\chi^2(x^{i-1}) &:= \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{X}}(x_i|x^{i-1})} \\ &=_{(a)} \sum_{x_i=(u_i,x_{i,w})} \frac{\left(\frac{1}{(N-(i-1)w)^{\underline{w}}} - \frac{1}{(N-1)^{\underline{w-1}}|\mathcal{N}^{u_i}(x^{i-1})|}\right)^2}{\frac{1}{(N-1)^{\underline{w-1}}|\mathcal{N}^{u_i}(x^{i-1})|}} \\ &=_{(b)} \mathsf{C} \times \sum_{u_i} \sum_{x_{i,w}} \frac{\left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2}{|\mathcal{N}^{u_i}(x^{i-1})|} \\ &=_{(c)} \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2, \end{aligned} \tag{5}$$

where $\mathsf{C} = \frac{(N-1)^{\underline{w-1}}}{((N-(i-1)w)^{\underline{w}})^2}$, and $\mathsf{D} = \frac{(N-(i-1)w)^{\underline{w}}}{(N-1)^{\underline{w-1}}}$. The equality (a) follows by plugging the conditional probabilities derived in (3) and (4). The expression on the r.h.s. of (b) is obtained by algebraic simplification. The equation (c) follows from the observation that

$\frac{\left(|\mathscr{N}^{u_i}(x^{i-1})|-\mathsf{D}\right)^2}{|\mathscr{N}^{u_i}(x^{i-1})|}$ is functionally independent of $x_{i,w}$,

and for each u_i, the number of choices of $x_{i,w}$ is $|\mathscr{N}^{u_i}(x^{i-1})|$. Next, in order to apply Theorem 1, we compute $\mathbf{Ex}[\chi^2(X^{i-1})]$ which (from (5)) is given by

$$\mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\left(|\mathscr{N}^{u_i}(X^{i-1})| - \mathsf{D}\right)^2].$$

Note that $|\mathscr{N}^{u_i}(x^{i-1})|$ is a function of x^{i-1}, and so, it is also a function of a^{i-1}. When x^{i-1} is sampled according to X^{i-1}, a^{i-1} would be sampled according to T^{i-1} (WOR sample).

For notational simplicity, let $r = (i-1)w$ and $r' = N - r$. Also, let $\boldsymbol{\mathscr{V}}_{r'} = \mathscr{G} \setminus \{T_{i',j} : i' \in [i], j \in [w]\}$ which is a random r'-set in $\mathscr{G}$. Then the set $\mathscr{N}^{u_i}(X^{i-1})$ is same as the set

$$\{g \in \boldsymbol{\mathscr{V}}_{r'} : g + u_{i,j} \in \boldsymbol{\mathscr{V}}_{r'} \text{ for all } j \in [w-1]\}.$$

We denote the size of the set by $\mathbf{N}^{u_i}_{r'}$. Then we have

$$\mathbf{Ex}[\chi^2(X^{i-1})] = \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\left(\mathbf{N}^{u_i}_{r'} - \mathsf{D}\right)^2]. \tag{6}$$

Next, we apply the following lemma to get an upper bound on the r.h.s. of (6).

Lemma 4. *Let $b := (b_1, \ldots, b_{w-1}) \in (\mathscr{G} \setminus \{0\})^{\underline{w-1}}$ (i.e., b_i's are nonzero distinct elements). Then, with the notations described above,*

$$\mathbf{Ex}[\mathbf{N}^b_{r'}] = \frac{r'^{\underline{w}}}{(N-1)^{\underline{w-1}}} := \mathsf{D} \tag{7}$$

$$\mathbf{Var}[\mathbf{N}^b_{r'}] \le w^2 \times \frac{r'^{\underline{w}}}{(N-1)^{\underline{w-1}}} \times \left(1 - \frac{r'^{\underline{w}}}{N^{\underline{w}}}\right). \tag{8}$$

When $(\mathscr{G}, +) = (\{0,1\}^n, \oplus)$ and $w = 2$ we have

$$\mathbf{Var}[\mathbf{N}^b_{r'}] \le \min\left\{\frac{2r(r-1)}{N-1}, \frac{2r'(r'-1)}{N-1}\right\}. \tag{9}$$

We postpone the proof of Lemma 4 to Subsection 3.4. By using (7), we get from (6)

$$\mathbf{Ex}[\chi^2(X^{i-1})] = \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\left(\mathbf{N}^{u_i}_{r'} - \mathsf{D}\right)^2] = \mathsf{C} \times \sum_{u_i} \mathbf{Var}[\mathbf{N}^{u_i}_{r'}]. \tag{10}$$

Next, by applying (8) to upper bound $\mathbf{Var}[\mathbf{N}^{u_i}_{r'}]$, we have

$$\begin{aligned}
\mathbf{Ex}[\chi^2(Z^{i-1})] &\le \frac{(N-1)^{\underline{w-1}}}{((N-r)^{\underline{w}})^2} \times (N-1)^{\underline{w-1}} \times \left(w^2 \times \frac{(N-r)^{\underline{w}}}{(N-1)^{\underline{w-1}}} \times \left(1 - \frac{(N-r)^{\underline{w}}}{N^{\underline{w}}}\right)\right) \\
&= w^2 \times \frac{(N-1)^{\underline{w-1}}}{(N-r)^{\underline{w}}} \times \left(1 - \frac{(N-r)^{\underline{w}}}{N^{\underline{w}}}\right) \\
&\le \frac{8rw^3}{N^2}
\end{aligned} \tag{11}$$

The last inequality follows from Lemma 1 and Lemma 2. Finally, from Theorem 1, we get

$$\begin{aligned}\|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\| &\le \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}} \\ &\le \left(\sum_{i=1}^{q}\frac{4w^3r}{N^2}\right)^{\frac{1}{2}} \\ &\le \left(\sum_{i=1}^{q}\frac{4w^4(i-1)}{N^2}\right)^{\frac{1}{2}} \\ &\le \left(\frac{2w^4q^2}{N^2}\right)^{\frac{1}{2}} \\ &= \frac{\sqrt{2}w^2q}{N}.\end{aligned}$$

Now, we assume that $w = 2$ and $\mathscr{G}$ is the set $\{0,1\}^n$ with $\oplus$ as the group operation. In this case, we apply our improved bound on $\mathbf{Var}[\mathbf{N}^b_{r'}]$ given by (9); we have $\mathbf{Var}[\mathbf{N}^b_{r'}] \le \frac{2r(r-1)}{N-1}$. So,

$$\begin{aligned}\mathbf{Ex}[\chi^2(X^{i-1})] &= \mathsf{C} \times \sum_{u_i}\mathbf{Var}(\mathbf{N}^{u_i}) \\ &\le \frac{(N-1)^2}{(N-r)^2(N-r-1)^2} \times \frac{2r(r-1)}{N-1} \\ &\le \frac{2(N-1)r^2}{(N-2q)^4}\end{aligned}$$

Now, we get by Theorem 1,

$$\begin{aligned}\|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\| &\le \left(\frac{1}{2}\sum_{i=1}^{q}\mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}} \\ &\le \left(\sum_{i=1}^{q}\frac{4(N-1)(i-1)^2}{(N-2q)^4}\right)^{\frac{1}{2}} \\ &\le \left(\frac{2(N-1)q^3}{(N-2q)^4}\right)^{\frac{1}{2}}.\end{aligned}$$

So far, we have provided an upper bound on $\|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\|$. As X and Y are the extended random variables of S and U respectively, we have $\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| \le \|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\|$. Now, we complete the proof by using triangle inequality on the total variation. We have

$$\begin{aligned}\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| &\le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\| \\ &\le \|\Pr_{\mathsf{X}} - \Pr_{\mathsf{Y}}\| + \frac{w(w-1)q}{2N},\end{aligned}$$

where the last inequality follows from Lemma 3.

3.2 Pseudorandomness of Variable Width XOR of WOR Sample

Theorem 3. *Let $w_1, w_2, \ldots, w_c \ge 2$, $\bar{\sigma} = \sum_i w_i$, and $w_{max} = \max_i w_i$. Then,*

$$\|\Pr_{\mathsf{S}'} - \Pr_{\mathsf{R}'}\| \le \frac{(1+\sqrt{2})\bar{\sigma}w_{max}}{N}$$

where R' and S' are defined in the Fig 3.3.

Random Experiment for R'

$\mathsf{R}' := (R'_{i,j} : i \in [q], j \in [w_i - 1]) \leftarrow_{\text{wr}} \mathscr{G}$
return R'

Random Experiment for U'

for $1 \le i \le q$
  $U'_i := (U'_{i,1}, U'_{i,2}, \ldots, U'_{i,w_i-1}) \leftarrow_{\text{wor}} \mathscr{G} \setminus \{0\}$
return $\mathsf{U}' := (U'_{i,j} : i \in [q], j \in [w_i - 1])$

Random Experiment for S'

$\mathsf{T}' := (T'_{i,j} : i \in [q], j \in [w_i]) \leftarrow_{\text{wor}} \mathscr{G}$
for $1 \le i \le q$
  for $1 \le j \le w_i - 1$
    $S'_{i,j} = T'_{i,j} - T'_{i,w_i}$
return $\mathsf{S}' := (S'_{i,j} : i \in [q], j \in [w_i - 1])$

Figure 3.3: Description of sampling methods of random variables R', S' and U' for variable widths $w_1, \ldots, w_q$.

Proof. Proof of Theorem 3 is almost same as the proof of Theorem 2. So, here we only outline their main differences. Proof of Theorem 2 is split into two total variation computations (due to triangle inequality). Likewise, here we have $\|\Pr_{\mathsf{S}'} - \Pr_{\mathsf{R}'}\| \le \|\Pr_{\mathsf{U}'} - \Pr_{\mathsf{R}'}\| + \|\Pr_{\mathsf{S}'} - \Pr_{\mathsf{U}'}\|$. Similar to Lemma 3, we have $\|\Pr_{\mathsf{U}'} - \Pr_{\mathsf{R}'}\| \le \frac{\bar{\sigma} w_{max}}{N}$. Now, to bound the other term, we consider the extended random vectors X' and Y' in exactly the same way.

Random Experiment for X'

$\mathsf{T}' = (T'_{i,j} : i \in [q], j \in [w_i]) \leftarrow_{\text{wor}} \mathscr{G}$
for $1 \le i \le q$
  for $1 \le j \le w_i - 1$
    $S'_{i,j} = T'_{i,j} - T'_{i,w_i}$
  $X'_i = (S'_{i,1}, \ldots, S'_{i,w_i-1}, T'_{i,w_i})$
  $S'_i = (S'_{i,1}, \ldots, S'_{i,w_i-1})$
return $\mathsf{X}' := (X'_1, \ldots, X'_q)$

Random Experiment for Y'

initialize $\mathcal{S}_0 = \mathscr{G}$
for $1 \le i \le q$
  $U'_i := (U'_{i,1}, U'_{i,2}, \ldots, U'_{i,w_i-1}) \leftarrow_{\text{wor}} \mathscr{G} \setminus \{0\}$
  $\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U'_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w_i - 1]\}$
  if $\mathcal{N}_i \neq \emptyset$ **then** $V'_{i,w_i} \leftarrow_{\text{wr}} \mathcal{N}_i$ **else** $V'_{i,w_i} = 0$
  $Y'_i = (U'_{i,1}, U'_{i,2}, \ldots, U'_{i,w_i-1}, V'_{i,w_i})$
  $\mathcal{S}_i = \mathscr{G} \setminus \big(\{V'_{i',j} := U'_{i',j} + V'_{i',w_i} : i' \in [i], j \in [w_i - 1]\} \cup \{V'_{1,w_1}, \ldots, V'_{i,w_i}\}\big)$
return $\mathsf{Y}' := (Y'_1, \ldots, Y'_q)$

Figure 3.4: X' and Y' are extended random variables of S' and U' respectively. These are similarly defined as in the fixed width case

Let $r = \sum_{j=1}^{i-1} w_j$. Following identical argument we get (analogous to (11)) the following.

$$\mathbf{Ex}[\chi^2(X'^{i-1})] \le w_i^2 \times \frac{(N-1)^{\underline{w_i - 1}}}{(N-r)^{\underline{w_i}}} \times \left(1 - \frac{(N-r)^{\underline{w_i}}}{N^{\underline{w_i}}}\right) \tag{12}$$

As in (11), second term in the r.h.s. of (12) can be bounded, using Lemma 1, by $\frac{4}{N}$; and

the third term can be bounded, using Lemma 2, by $\frac{2rw_i}{N}$. Therefore,

$$\begin{aligned}
\|\mathrm{Pr}_{\mathsf{X}'} - \mathrm{Pr}_{\mathsf{Y}'}\| &\le \left(\frac{1}{2}\sum_{i=1}^{c} \mathbf{Ex}[\chi^2(X'^{i-1})]\right)^{\frac{1}{2}} \\
&\le \left(\sum_{i=1}^{c} \frac{4w_i^3 \sum_{j=1}^{i-1} w_j}{N^2}\right)^{\frac{1}{2}} \\
&\le \left(\sum_{i=1}^{c} \frac{2w_{max}^2(2w_i \sum_{j=1}^{i-1} w_j)}{N^2}\right)^{\frac{1}{2}} \\
&= \frac{\sqrt{2}w_{max}}{N}\left(\sum_{i\neq j} w_i w_j\right)^{\frac{1}{2}} \\
&= \frac{\sqrt{2}\bar{\sigma}w_{max}}{N}, \quad \text{since } \bar{\sigma} = \sum_i w_i.
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\|\mathrm{Pr}_{\mathsf{S}'} - \mathrm{Pr}_{\mathsf{R}'}\| &\le \|\mathrm{Pr}_{\mathsf{S}'} - \mathrm{Pr}_{\mathsf{U}'}\| + \|\mathrm{Pr}_{\mathsf{U}'} - \mathrm{Pr}_{\mathsf{R}'}\| \\
&\le \|\mathrm{Pr}_{\mathsf{X}'} - \mathrm{Pr}_{\mathsf{Y}'}\| + \frac{w(w-1)q}{2N}.
\end{aligned}$$

Hence, the theorem follows.

3.3 On the Tightness of Our Bounds: An Attack on XORP

Here, we briefly describe a distinguisher (adversary $\mathscr{A}$) to show tightness of our bounds. Let $x_1, \ldots, x_q$ be distinct queries made by $\mathscr{A}$. For every $i \in [q]$, let $Z_i = (Z_{i,1}, \ldots, Z_{i,w-1})$ be the response of the i-th query. Also, let $Z_i, i \in [q]$, be distributed according to the distributions Pr_0 and Pr_1 in the real and the ideal world respectively. Finally, $\mathscr{A}$ returns 1 if one of the following holds;

1. $Z_{i,j} = \mathsf{0}$ for some j,
2. for some $i \in [q]$, $j \neq j' \in [w-1]$, $Z_{i,j} = Z_{i,j'}$.

As we have observed before, $\mathscr{A}$ never returns 1 while interacting in the real world. So, $\mathrm{Pr}_0(\mathscr{A} \to 1) = 0$. In the ideal world, however, $Z_{i,j}$'s are all uniformly and independently distributed. Therefore, $\mathrm{Pr}_1(\mathscr{A} \to 1) \approx \frac{q}{N} + \frac{q(w-1)(w-2)}{N}$. Thus, $\mathbf{Adv}_f^{\mathrm{prf}}(\mathscr{A}) \approx \frac{q}{N} + \frac{q(w-1)(w-2)}{N}$.

3.4 Proof of Lemma 4

Let r, w, N be a positive integers such that $r < N$, and $w \ge 2$. Let $\mathscr{G}$ be a group of size N, and $\boldsymbol{\mathscr{V}}_r$ be a random r-set in $\mathscr{G}$.

Definition 3. Let $b := (b_1, \ldots, b_{w-1}) \in (\mathscr{G} \setminus \{\mathsf{0}\})^{\underline{w-1}}$ (i.e., b_i's are nonzero distinct elements), we associate a random variable $\mathbf{N}_r^b$ defined as the size of the following set

$$\mathscr{N}^b := \{g \in \boldsymbol{\mathscr{V}}_r : g + b_i \in \boldsymbol{\mathscr{V}}_r \text{ for all } i \in [w-1]\}.$$

Now, we restate and prove Lemma 4.

Lemma 4. For every $b \in (\mathscr{G} \setminus \{0\})^{\underline{w-1}}$, we have

$$\mathbf{Ex}[\mathbf{N}_r^b] = \frac{r^{\underline{w}}}{(N-1)^{\underline{w-1}}}$$
$$\mathbf{Var}[\mathbf{N}_r^b] \leq w^2 \times \frac{r^{\underline{w}}}{(N-1)^{\underline{w-1}}} \times \left(1 - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right).$$

When $(\mathscr{G}, +) = (\{0,1\}^n, \oplus)$ and $w = 2$ we have

$$\mathbf{Var}[\mathbf{N}_r^b] \leq \min\left\{\frac{2r(r-1)}{N-1}, \frac{2(N-r)(N-r-1)}{N-1}\right\}.$$

Remark 1. Note that the upper bound on $\mathbf{Var}[\mathbf{N}_r^b]$ for the special case $(\mathscr{G}, +) = (\{0,1\}^n, \oplus)$ and $w = 2$, is better than the upper bound given by the general case.

Proof. We represent $\mathbf{N}_r^b$ as a sum of indicator random variables; this will be useful to compute its expectation and variance. We write

$$\mathbf{N}_r^b = \sum_{g \in \mathscr{G}} \mathtt{I}_g, \tag{13}$$

where the indicator random variable $\mathtt{I}_g$ is defined as

$$\mathtt{I}_g = \begin{cases} 1 \text{ if } g + b_1, \ldots, g + b_{w-1}, g \in \mathscr{V}_r, \\ 0 \text{ otherwise.} \end{cases}$$

We note that $g+b_1, \ldots, g+b_{w-1}$ and g are all w distinct elements of $\mathscr{G}$ since b_i's are nonzero distinct elements. So, the number of r-sets that contain the w elements $g+b_1, \ldots, g+b_{w-1}, g$ is exactly $\binom{N-w}{r-w}$. Thus,

$$\begin{aligned} \mathbf{Ex}[\mathtt{I}_g] &= \mathbf{Pr}[\{g + b_1, \ldots, g + b_{w-1}, g\} \subseteq \mathscr{V}_r] \\ &= \frac{\binom{N-w}{r-w}}{\binom{N}{r}} \\ &= \frac{r^{\underline{w}}}{N^{\underline{w}}}. \end{aligned} \tag{14}$$

By using the linearity of expectation, we have

$$\mathbf{Ex}[\mathbf{N}_r^b] \;=\; \sum_g \mathbf{Ex}[\mathtt{I}_g] \;=\; \sum_{g \in \mathscr{G}} \frac{r^{\underline{w}}}{N^{\underline{w}}} = \frac{r^{\underline{w}}}{(N-1)^{\underline{w-1}}}.$$

Now, we compute the variance using the following relation.

$$\mathbf{Var}[\sum_g \mathtt{I}_g] = \sum_g \mathbf{Var}[\mathtt{I}_g] + \sum_{g \neq g'} \mathbf{Cov}(\mathtt{I}_g, \mathtt{I}_{g'}).$$

For the sake of notational simplicity, we denote the set $\{g + b_1, \ldots, g + b_{w-1}, g\}$ as $\mathscr{S}_g$ for every $g \in \mathscr{G}$. In (14), we have shown that $\mathbf{Ex}[\mathtt{I}_g] = \frac{r^{\underline{w}}}{N^{\underline{w}}}$. As $\mathtt{I}_g$ is a $0-1$ random variable, $\mathbf{Ex}[\mathtt{I}_g^2] = \mathbf{Ex}[\mathtt{I}_g]$. Thus,

$$\begin{aligned} \mathbf{Var}[\mathtt{I}_g] &= \mathbf{Ex}[\mathtt{I}_g^2] - \mathbf{Ex}[\mathtt{I}_g]^2 \\ &= \mathbf{Ex}[\mathtt{I}_g](1 - \mathbf{Ex}[\mathtt{I}_g]) \\ &= \frac{r^{\underline{w}}}{N^{\underline{w}}} \times \left(1 - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right) \end{aligned} \tag{15}$$

Now, we compute the covariance term. Note that $\mathtt{I}_g\mathtt{I}_{g'} = 1$ if and only if $\mathcal{S}_g \cup \mathcal{S}_{g'} \subseteq \mathscr{V}_r$. So,

$$\begin{aligned}\mathbf{Ex}[\mathtt{I}_g\mathtt{I}_{g'}] &= \mathbf{Pr}[\mathcal{S}_g \cup \mathcal{S}_{g'} \subseteq \mathscr{V}_r] \\ &= \frac{r^{\underline{w'}}}{N^{\underline{w'}}},\end{aligned}$$

where w' is size of the set $\mathcal{S}_g \cup \mathcal{S}_{g'}$. We compute the covariance term in two cases for $g \neq g'$.

Case $\mathcal{S}_g \cap \mathcal{S}_{g'} = \emptyset$. In this case, the size of the set $\mathcal{S}_g \cup \mathcal{S}_{g'}$ is $w' = 2w$. So,

$$\begin{aligned}\mathbf{Cov}(\mathtt{I}_g, \mathtt{I}_{g'}) &= \mathbf{Ex}[\mathtt{I}_g\mathtt{I}_{g'}] - \mathbf{Ex}[\mathtt{I}_g]\mathbf{Ex}[\mathtt{I}_{g'}] \\ &= \frac{r^{\underline{2w}}}{N^{\underline{2w}}} - \left(\frac{r^{\underline{w}}}{N^{\underline{w}}}\right)^2 \\ &= \frac{r^{\underline{w}}}{N^{\underline{w}}} \times \left(\frac{(r-w)^{\underline{w}}}{(N-w)^{\underline{w}}} - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right) \\ &< 0. \end{aligned} \tag{16}$$

Case $\mathcal{S}_g \cap \mathcal{S}_{g'} \neq \emptyset$. In this case, the size of the set $\mathcal{S}_g \cup \mathcal{S}_{g'}$ is $w \leq w' < 2w$. So,

$$\begin{aligned}\mathbf{Cov}(\mathtt{I}_g, \mathtt{I}_{g'}) &= \mathbf{Ex}[\mathtt{I}_g\mathtt{I}_{g'}] - \mathbf{Ex}[\mathtt{I}_g]\mathbf{Ex}[\mathtt{I}_{g'}] \\ &= \frac{r^{\underline{w'}}}{N^{\underline{w'}}} - \left(\frac{r^{\underline{w}}}{N^{\underline{w}}}\right)^2 \\ &= \frac{r^{\underline{w}}}{N^{\underline{w}}} \times \left(\frac{(r-w)^{\underline{w'-w}}}{(N-w)^{\underline{w'-w}}} - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right) \\ &\leq \frac{r^{\underline{w}}}{N^{\underline{w}}} \times \left(1 - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right). \end{aligned} \tag{17}$$

The number of choices of pairs (g, g') with $g \neq g'$ such that this case holds is at most $(w^2-1)N$. This is easy to see, since, for every g, number of g' is at most $w^2 - 1$. By adding (15), (16), (17) we obtain

$$\mathbf{Var}[\sum_g \mathtt{I}_g] \leq w^2 \times \frac{r^{\underline{w}}}{(N-1)^{\underline{w-1}}} \times \left(1 - \frac{r^{\underline{w}}}{N^{\underline{w}}}\right).$$

To prove the specific case, let us assume that our group is $\{0,1\}^n$ with bit-wise xor ($\oplus$) as addition and $w = 2$. Then, for $g \neq g'$, $\mathcal{S}_g = \{g, g + b_1\}$ intersects $\mathcal{S}_{g'} = \{g', g' + b_1\}$ if and only if $g \oplus g' = b_1$. So, the number of choices of pairs (g, g') with $g \neq g'$ such that this case holds is exactly N. Thus, the sum of the covariance terms is at most $\frac{r(r-1)}{(N-1)} \times \left(1 - \frac{r(r-1)}{N(N-1)}\right)$. Similarly, the sum of the variance term has been shown to be at most $\frac{r(r-1)}{(N-1)} \times \left(1 - \frac{r(r-1)}{N(N-1)}\right)$. So,

$$\begin{aligned}\mathbf{Var}[\sum_g \mathtt{I}_g] &\leq \sum_g \mathbf{Var}[\mathtt{I}_g] + \sum_{(g,g')} \mathbf{Cov}(\mathtt{I}_g, \mathtt{I}_{g'}) \\ &\leq \frac{2r(r-1)}{(N-1)} \times \left(1 - \frac{r(r-1)}{N(N-1)}\right) \\ &\leq \frac{2r(r-1)}{(N-1)} \end{aligned} \tag{18}$$

Therefore, it remains to show that $\mathbf{Var}[\sum_g \mathtt{I}_g] \le \frac{2(N-r)(N-r-1)}{(N-1)}$. Note that $\mathscr{V}_r^c := \mathscr{G} \setminus \mathscr{V}_r$ is a random $(N-r)$-set.

By definition, $\mathbf{N}_r^b$ is the size of the set

$$\mathscr{N}_r^b := \{g \in \mathscr{V}_r : g \oplus b_1 \in \mathscr{V}_r\} = \mathscr{V}_r \cap (\mathscr{V}_r \oplus b_1),$$

where $\mathscr{V}_r \oplus b_1$ is the set $\{g \oplus b_1 : g \in \mathscr{G}\}$. So, $N - \mathbf{N}_r^b$ is the size of the set $\mathscr{V}_r^c \cup (\mathscr{V}_r \oplus b_1)^c$. It is easy to see that $(\mathscr{V}_r \oplus b_1)^c = \{g \in \mathscr{G} : g \oplus b_i \in \mathscr{V}_r^c\}$, and hence, $N - \mathbf{N}_r^b$ is same as $\mathbf{N}_{N-r}^b$. So, we can apply (18) and the fact that $\mathbf{Var}[N - \mathbf{N}_r^b] = \mathbf{Var}[\mathbf{N}_r^b]$. This completes the proof of the lemma.

4 Application of Our Theorems

As an immediate application of Theorem 2 we provide PRF-security analysis of the construction $\mathsf{XORP}^{e_K}[w] : \{0,1\}^{n-s} \to \{0,1\}^{n(w-1)}$ based on an n-bit blockcipher (i.e., pseudorandom permutation) e_K, where $s = \lceil \log_2(w+1) \rceil < n$ (the last inequality is ensured by restricting the width parameter w). The construction is defined as

$$\mathsf{XORP}^{e_K}[w](x) = \Big\|_{i=1}^{w-1} \big(e_K(x\|\langle 0\rangle_s) \oplus e_K(x\|\langle i\rangle_s)\big), \text{ for all } x \in \{0,1\}^{n-s} \tag{19}$$

Here $\langle i\rangle_s$ is the s-bit representation of i. It is called XOR construction or more specifically, fixed-length-output XOR construction. In the following corollary, we state PRF-security of the construction.

Corollary 1. *Let e_K be a blockcipher over $\{0,1\}^n$ with a randomly chosen key K. For any adversary $\mathscr{A}$ making at most q queries to $\mathsf{XORP}^{e_K}[w]$ or to the random function $\mathsf{RF}_{(n-s)\to n(w-1)}$, there is an adversary $\mathscr{B}$ making at most qw queries to e_K or to the random permutation RP_n such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}^{e_K}[w]}(\mathscr{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{e_K}(\mathscr{B}) + \frac{(1+\sqrt{2})qw^2}{N}.$$

Proof. By using the standard hybrid technique, we can show the existence of adversaries $\mathscr{B}$ and $\mathscr{C}$ such that

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}^{e_K}[w]}(\mathscr{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{e_K}(\mathscr{B}) + \mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}^{\mathsf{RP}_n}[w]}(\mathscr{C}).$$

Without loss of generality, we can assume that $\mathscr{C}$ makes q distinct queries. So the probability distributions of q outputs of $\mathsf{XORP}^{\mathsf{RP}_n}[w]$ is same as the distribution of S of Theorem 2 in which $\mathscr{G} = \{0,1\}^n$ and the group operation is the bit-wise xor ($\oplus$). As in Theorem 2, let R denote the output vector of a random function. Hence, the PRF-advantage $\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}^{\mathsf{RP}_n}[w]}(\mathscr{C})$ is bounded by the total variation between output distribution of XORP (same as that of S) and random outputs (i.e. R). Our corollary follows from the upper bound of $\|\mathrm{Pr}_{\mathsf{S}} - \mathrm{Pr}_{\mathsf{R}}\|$ given in Theorem 2.

The above construction returns a fixed length output. A generalization of the construction takes the value of width w as an input and returns $(w-1)n$ bits output. More formally, we define an arbitrary width construction $\mathsf{XORP}^{e_K}[*]$ over the domain $\mathscr{M} := \{0,1\}^{n-s} \times \{2,3,\ldots,2^s-1\}$, where $s = \lceil \log_2(w+1) \rceil$. Given an input $(x,w) \in \mathscr{M}$ we define

$$\mathsf{XORP}^{e_K}[*](x,w) = \mathsf{XORP}^{e_K}[w](x) = \Big\|_{i=1}^{w} (e_K(x\|\langle 0\rangle_s) \oplus e_K(x\|\langle i\rangle_s)). \tag{20}$$

A similar corollary can be derived for an arbitrary width construction $\mathsf{XORP}^{e_K}[*]$ over the domain $\mathscr{M}$. For an input $(x,w) \in \mathscr{M}$, we call w the width input and x *nonce*.

An oracle adversary $\mathscr{A}$ making queries to an oracle accepting inputs from $\mathscr{M}$ is called *nonce-respecting* if $\mathscr{A}$ makes queries with distinct nonces. Let $\mathsf{RF}[*]$ denote the random function which is sampled from the set of all functions from $\mathscr{M}$ to $\cup_{i=1}^{2^s-2}\{0,1\}^{n(i-1)}$ which maps an element (x,w) to $(\{0,1\}^n)^w$ for every $x \in \{0,1\}^{n-s}$. So a nonce respecting adversary $\mathscr{A}$ after making queries $(x_1,w_1),\ldots,(x_q,w_q)$ to $\mathsf{RF}[*]$, obtains responses

$$\mathsf{R}' := (R'_{i,j} : i \in [q], j \in [w_i - 1]) \leftarrow_{\text{wor}} \{0,1\}^n,$$

where $\sigma = \bar{\sigma} - q$ and $\bar{\sigma} = \sum_i w_i$. Then, by using the standard hybrid argument and Theorem 3, we obtain the following corollary in the same way as Corollary 1.

Corollary 2. *For any nonce-respecting adversary $\mathscr{A}$ making at most q queries with widths $w_1,\ldots,w_q$ to $\mathsf{XORP}^{e_K}[*]$ or to the random function $\mathsf{RF}[*]$, there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ queries to e_K or to the random permutation RP_n such that*

$$\mathbf{Adv}^{\text{prf}}_{\mathsf{XORP}^{e_K}[*]}(\mathscr{A}) \le \mathbf{Adv}^{\text{prp}}_{e_K}(\mathscr{B}) + \frac{(1+\sqrt{2})w_{max} \times \bar{\sigma}}{N}$$

where w_{max} denotes the maximum of $w_1,\ldots,w_q$.

Note that Corollary 1 follows from this result by setting $w_i = w$ for all i.

4.1 Applications to Privacy Security of Authenticated Encryption

4.1.1 On the Security of CENC

Let e_K be an n-bit block cipher. We fix the following parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$. Let us choose the above parameters in such a way that $m = n - (r+s) > 0$. Let $M = M_1 \| \cdots \| M_\ell \in (\{0,1\}^n)^\ell$ and $\ell \le \ell_{max}$. For the simplicity let us assume that $\ell = \ell' w$ for some ℓ'. Given a nonce $P \in \{0,1\}^m$ (which does not repeat over all queries), we define the ciphertext given by the CENC encryption as follows:

$$\mathsf{CENC}_K(P,M) := \|_{i=0}^{\ell'-1} \mathsf{XORP}^{e_K}[w](P \| \langle i \rangle_r) \oplus (M_{wi} \| \cdots M_{w(i+1)-1}).$$

In [IMV16], the authors obtained PRF-advantage of the CENC encryption scheme. PRF-advantage obtained by them is valid as long as $\bar{\sigma}(w-1) \le N/67$, where $\bar{\sigma}$ denotes the total number of blockcipher calls for all queries. We obtain similar PRF-advantage of CENC but with a larger range of $\bar{\sigma}$. The result is stated in the following theorem. Its proof directly follows from Corollary 1.

Theorem 4 (PRF-security of CENC)**.** *For every nonce-respecting distinguisher $\mathscr{A}$ making at most $\bar{\sigma}$ many queries there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ many queries such that*

$$\mathbf{Adv}^{\text{prf}}_{\mathsf{CENC}}(\mathscr{A}) \le \mathbf{Adv}^{\text{prp}}_{e_K}(\mathscr{B}) + \frac{(1+\sqrt{2})w\bar{\sigma}}{N}.$$

4.1.2 Boosting the Security Level of AES-GCM

AES-GCM is a nonce based authenticated encryption which provides birthday bound security [MV04]. It is very popular and CAESAR competition [CAE] for authenticated encryption is aimed to get constructions having advantages over AES-GCM. Here, we provide a simple modification of AES-GCM which provides higher security.

For the sake of simplicity, we only describe the basic structure of AES-GCM which only processes messages without considering associated data. The analysis can be extended to associated data also. Given a nonce $P \in \{0,1\}^{n-s}$ and message $M = (m_1,\ldots,m_\ell) \in$

$\{0,1\}^{n\ell}$, we define $c_i = m_i \oplus e_K(P\|\langle i\rangle_s)$, where s is an integer such that for the longest message $\ell \leq 2^s - 1$. Due to the *PRP-PRF switching lemma* the PRF-security of AES-GCM is the birthday security. A simple security boosting can be done by adding one more output of the block cipher to every ciphertext. This is structurally same as CENC except that we do not use any fixed width. In other words, it is a variable width encryption. More formally, we define the modified AES-GCM encryption algorithm, denoted as mGCM, as follows. Let π be the underlying random permutation and H be a *hash key* chosen uniformly at random from $\{0,1\}^n$. Let $M = (m_1, \ldots, m_\ell)$ be an ℓ-block message. We compute ciphertext $C = (c_1, \ldots, c_\ell)$ and tag T of mGCM as follows.

1. For $i = 1$ to ℓ,
$$c_i = m_i \oplus e_K(P\|\langle i\rangle_s) \oplus e_K(P\|\langle s-1\rangle_s).$$
2. Compute tag
$$T = (H^\ell c_1 \oplus \cdots \oplus H c_\ell) \oplus e_K(P\|\langle 0\rangle_s) \oplus e_K(P\|\langle s-1\rangle_s).$$

As an application of Corollary 2, we have the following result on the PRF-security of mGCM (an integrity security will also follow directly from the Carter-Wegman [WC81, CW79] message authentication security analysis).

Theorem 5 (PRF-security of mGCM)**.** *For every nonce-respecting distinguisher $\mathscr{A}$ making at most $\bar{\sigma}$ many queries, where the longest query has block length ℓ_{max}, there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ many queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{mGCM}}(\mathscr{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{e_K}(\mathscr{B}) + \frac{(1+\sqrt{2})\ell_{max}\bar{\sigma}}{N}.$$

5 Conclusion

In this work, we have revisited the problem of generating PRFs from PRPs with beyond birthday security. We have applied the recently introduced χ^2 method to obtain an optimal bound on the PRF-security of a general case of the sum of random permutations problem. As an application, we have re-established the PRF-security of the CENC encryption and a variant of the GCM authenticated encryption. Moreover, our bounds hold for a larger choice of parameters.

We feel that the proofs of our main results are more transparent than the existing proofs found in the literature. We also feel that the χ^2 method has potential for applications into similar types of problems and is worth further consideration and investigation.

Acknowledgements

We thank the reviewers for their helpful comments and suggestions which improved readability of this work. We are also grateful to the WISEKEY project for partly supporting this work.

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, in *Advances in Cryptology — EUROCRYPT'98*, edited by K. Nyberg, pages 266–280, Berlin, Heidelberg, 1998, Springer Berlin Heidelberg.

[BKR00] M. Bellare, J. Kilian and P. Rogaway, *The Security of the Cipher Block Chaining Message Authentication Code*, J. Comput. Syst. Sci. **61**(3), 362–399 (2000).

[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.

[CAE] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html/.

[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.

[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.

[CW79] L. Carter and M. N. Wegman, *Universal Classes of Hash Functions*, J. Comput. Syst. Sci. **18**(2), 143–154 (1979).

[DDN+17] N. Datta, A. Dutta, M. Nandi, G. Paul and L. Zhang, *Single Key Variant of PMAC_Plus*, To appear in IACR Transaction on Symmetric Key Cryptology (4) (2017).

[DHT17] W. Dai, V. T. Hoang and S. Tessaro, Information-Theoretic Indistinguishability via the Chi-Squared Method, In Katz and Shacham [KS17], pages 497–523.

[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).

[GL17] S. Gueron and Y. Lindell, Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 1019–1036, New York, NY, USA, 2017, ACM.

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

[HWKS98] C. Hall, D. Wagner, J. Kelsey and B. Schneier, Building PRFs from PRPs, in *Advances in Cryptology — CRYPTO '98*, pages 370–389, Springer Berlin Heidelberg, 1998.

[IK03] T. Iwata and K. Kurosawa, OMAC: One-Key CBC MAC, in *Fast Software Encryption, 2003*, volume 2887 of *LNCS*, pages 129–153, Springer, 2003.

[IMV16] T. Iwata, B. Mennink and D. Vizár, *CENC is Optimally Secure*, IACR Cryptology ePrint Archive **2016**, 1087 (2016).

[IS17] T. Iwata and Y. Seurin, *Reconsidering the Security Bound of AES-GCM-SIV*, IACR Transactions on Symmetric Cryptology **2017**(4), 240–267 (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.

[Iwa08] T. Iwata, Authenticated Encryption Mode for Beyond the Birthday Bound Security, in *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, edited by S. Vaudenay, volume 5023 of *Lecture Notes in Computer Science*, pages 125–142, Springer, 2008.

[KS17] J. Katz and H. Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, Springer, 2017.

[LPTY16] A. Luykx, B. Preneel, E. Tischhauser and K. Yasuda, A MAC Mode for Lightweight Block Ciphers, in *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, edited by T. Peyrin, volume 9783 of *Lecture Notes in Computer Science*, pages 43–59, Springer, 2016.

[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.

[MN17] B. Mennink and S. Neves, Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory, In Katz and Shacham [KS17], pages 556–583.

[MV04] D. A. McGrew and J. Viega, The Security and Performance of the Galois/Counter Mode (GCM) of Operation, in *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, edited by A. Canteaut and K. Viswanathan, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355, Springer, 2004.

[Nai17] Y. Naito, Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length, in *Advances in Cryptology – ASIACRYPT 2017*, edited by T. Takagi and T. Peyrin, pages 446–470, Cham, 2017, Springer International Publishing.

[Nan09] M. Nandi, Fast and Secure CBC-Type MAC Algorithms, in *Fast Software Encryption*, edited by O. Dunkelman, pages 375–393, Berlin, Heidelberg, 2009, 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.

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

[Vau03] S. Vaudenay, *Decorrelation: A Theory for Block Cipher Security*, J. Cryptology **16**(4), 249–286 (2003).

[WC81] M. N. Wegman and L. Carter, *New Hash Functions and Their Use in Authentication and Set Equality*, J. Comput. Syst. Sci. **22**(3), 265–279 (1981).

[Yas11] K. Yasuda, A New Variant of PMAC: Beyond the Birthday Bound, in *CRYPTO 2011*, pages 596–609, 2011.

[ZWSW12] L. Zhang, W. Wu, H. Sui and P. Wang, 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound, in *ASIACRYPT 2012*, pages 296–312, 2012.