Luby-Rackoff Backwards with More Users and More Security

Srimanta Bhattacharya[1] † and Mridul Nandi[2]

[1] SIAS, KREA University.
[2] Indian Statistical Institute, Kolkata.

Abstract. It is known, from the work of Dai *et al.* (in CRYPTO'17), that the PRF advantage of XORP (bitwise-xor of two outputs of n-bit random permutations with domain separated inputs), against an adversary making q queries, is about $q/2^n$ for $q \leq 2^{n-5}$. The same bound can be easily shown to hold for XORP$[k]$ (bitwise-xor of k outputs n-bit pseudorandom random permutations with domain separated inputs), for $k \geq 3$. In this work, we first consider multi-user security of XORP[3]. We show that the multi-user PRF advantage of XORP[3] is about $\sqrt{uq_{\max}}/2^n$ for all $q_{\max} \leq 2^n/12$, where u is the number of users and $q_{\max}$ is the maximum number of queries the adversary can make to each user. In the multi-user setup, this implies that XORP[3] gives security for $O(2^n)$ users even allowing almost $O(2^n)$ queries to each user. This also indicates significant improvement in the single-user setup (*i.e.,* when $u = 1$), where the distinguishing advantage of the adversary even after making $O(2^n)$ queries is $O(\frac{1}{\sqrt{2^n}})$, *i.e.,* negligible. Subsequently, we consider a simple efficient variant of XORP[3] in which we use five calls to produce $2n$ bit output (instead of six calls in the case of XORP[3]). This variant also achieves similar level of security. As an immediate application, we can construct a variant of block cipher based counter mode which provides much higher security (both in the single-user and the multi-user setup) compared to the security of the encryption part of GCM at the cost of efficiency.

Keywords: Random permutation, PRF security, multi-user security, χ^2 method, XOR construction.

1 Introduction

Luby-Rackoff Backwards. *Pseudorandom functions* (PRFs) are important cryptographic primitives. Construction of PRFs using other primitives is an intriguing problem in cryptography. In the context of symmetric-key cryptography, construction of PRFs from *pseudorandom permutations* (PRPs) is commonly termed "Luby-Rackoff Backwards" [BKR98].[3]

† The work was carried out when the author was affiliated with the Indian Statistical Institute, Kolkata.

[3] In reference to the seminal work by Luby and Rackoff ([LR88]) who considered the converse problem and showed how to construct a PRP from a PRF.

A potential drawback of block ciphers (modeled as a PRP) is that they merely achieve *birthday bound* security, *i.e.,* a block cipher becomes distinguishable from a PRF when it is queried $O(2^{n/2})$ times, where n is the block size. Achieving security *beyond the birthday bound* (BBB) is very much desirable but non-trivial. Bellare, Krovetz, and Rogaway ([BKR98]) and Hall, Wagner, Kelsey, and Schneier ([HWKS98]) initiated the study of constructions of good PRFs from block ciphers with BBB security. Since then the problem has received a lot of attention and at present, it is an intensely investigated area of research.

Different constructions have been proposed in the literature that achieve varying level of BBB security. A particularly simple construction which we refer to as the XORP construction, has received much attention in this context. Given an n-bit random permutation RP, the construction is given by $\mathsf{XORP} : \{0,1\}^{n-1} \to \{0,1\}^n;\ \mathsf{XORP}(x) = \mathsf{RP}(0\|x) \oplus \mathsf{RP}(1\|x)$.

In a generalized version of XORP, denoted by $\mathsf{XORP}[k]$, xor of k independent n-bit random permutations is considered (though in this work, we will consider its domain separated version). Lucks [Luc00] showed BBB security for $\mathsf{XORP}[k]$ for all $k \geq 2$. More precisely, he showed that the construction is secure up to $O(2^{\frac{kn}{k+1}})$ queries. This was further improved in a sequence of papers [BI99,CLP14,Pat10,Pat08,DHT17]. In particular, in [DHT17], it was shown that the PRF advantage of an adversary making at most q queries to the XORP construction is at most $\frac{q}{2^n} + 3(\frac{q}{2^n})^{1.5}$ indicating that XORP is secure up to $O(2^n)$ queries.

On the other hand, Mennink *et al.* [MP15] showed a reduction proving that the security of $\mathsf{XORP}[k]$ can be reduced to that of XORP for any $k \geq 3$. Hence, $\mathsf{XORP}[k]$ also achieves n-bit security. So, to begin with, PRF security of $\mathsf{XORP}[k]$ for $k \geq 2$ looks settled. But we show that further improvement is possible (in terms of the distinguishing advantage of the adversary) even in the case of $\mathsf{XORP}[3]$. Consideration of XORP (or its general version $\mathsf{XORP}[k]$) is important since it has been used to obtain some constructions achieving BBB (or sometimes almost full) security (e.g., CENC [Iwa06,BN18c], PMAC_Plus [Yas11], and ZMAC [IMPS17]).

Multi-user Security. In the multi-user PRF setting of $\mathsf{XORP}[k]$, the adversary can query multiple independent random functions in the ideal world or multiple independent $\mathsf{XORP}[k]$'s (by independent choice of underlying random permutation) in the *real world.* In the present-day scenario, multi-user security (first considered in [BBM00] in the context of public-key cryptography) of a cryptographic primitive is a prudent goal to achieve. Perhaps, due to the large scale deployment of primitives over the internet it deserves more urgent attention. Quite a few recent works ([BT16,HTT18,BHT18,HT17,ML15]) have addressed this area.

Multi User Security of $\mathsf{XORP}[k]$. To motivate its significance in a concrete manner let us further investigate the multi-user security of $\mathsf{XORP}[k]$. Until now, the best single-user PRF advantage for $\mathsf{XORP}[k]$ is $q/2^n$ for any $k \geq 2$ (ignoring the other lower order terms). By using standard hybrid reduction, multi-user PRF bound of $\mathsf{XORP}[k]$ is $uq_{max}/2^n$, where u is the number of users and q_{max}

is the maximum number of queries per user. When we use AES (so $n = 128$) as the underlying block cipher, we have to limit u and q_{max} such that $uq_{max} \leq 2^{96}$ if we tolerable distinguishing advantage is at most 2^{-32}. Even though the limit is reasonable for the time being, it may be a concern as the number of users as well as amount of usage of the internet is growing at a huge pace. One option to boost the security is to increase the block size n. Unfortunately, AES does not support block size other than 128 [4]. The other option could be to come up with some construction which provides stronger security. In this work, we investigate the second option.

1.1 Our Contribution

In this paper, we investigate the multi-user PRF security of $\mathsf{XORP}[3]$ construction. We show that, for any adversary, making at most q_{max} queries to any user, the multi-user PRF advantage for $\mathsf{XORP}[3]$ is at most $20\sqrt{uq_{max}}/2^n$, where u is the number of users and $q_{max} \leq 2^n/12$. The result shows that $\mathsf{XORP}[3]$ can be simultaneously used by $O(2^n)$ users even after allowing the adversary to make almost $O(2^n)$ queries to each user (provided the keys, *i.e* the underlying random permutations of $\mathsf{XORP}[3]$ are chosen independently by each user); though in practice the random permutation should be instantiated with a block cipher with sufficiently long key (see [ML15]). For a single user, *i.e.,* when $u = 1$, the result says that even if the adversary is allowed to query almost all inputs of the block cipher, its distinguishing advantage is $O\left(\frac{1}{\sqrt{2^n}}\right)$, which is negligible in n. To the best of our knowledge, this is the first result (in the standard model) showing negligible advantage for an adversary that is allowed to query almost the entire domain.

We also analyze the single-user PRF security of a simple variant of $\mathsf{XORP}[3]$, which we denote as $\mathsf{XORP}'[3]$. This construction makes 5 calls to the underlying block cipher (instead of 6 in case of $\mathsf{XORP}[3]$) to generate 2 output blocks. Even with a saving in the number of block cipher calls we show that the PRF security of $\mathsf{XORP}'[3]$ is very similar to that of $\mathsf{XORP}[3]$. In particular, we show that the PRF advantage of the construction is bounded by $\frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{\frac{3}{2}}}$. Though we have analyzed the single-user case for the sake of simplicity, multi-user PRF security of $\mathsf{XORP}'[3]$ can be analyzed in the same way as that of $\mathsf{XORP}[3]$.

In order to emphasize our contribution further, we mention that multi-user PRF advantage of $\mathsf{XORP}[2]$ (obtained in [HS20] using the χ^2 method) and $\mathsf{XORP}'[2]$ (obtained in [Cog18] using Patarin's Mirror theory) are at most $O\left(\frac{\sqrt{n}q}{2^n}\right)$ and $O\left(\frac{q}{2^n}\right)$, where q is the total number of queries made to all the users.

1.2 Our Technique

We use the χ^2 method, introduced in [DHT17], which has of late emerged as a potent tool for bounding *statistical distance* between two joint distributions.

[4] However, Rijndael has variants with larger block sizes.

Though relatively new, it has so far been effectively applied in quite a few other works ([BN18c,BN18a,CLL19,Men19,GM20]). Although its application to bound PRF advantage of an adversary for $\mathsf{XORP}[k]$ is not novel, in the present case of $\mathsf{XORP}[3]$ and $\mathsf{XORP}'[3]$, the analyses become significantly intricate. In the case of $\mathsf{XORP}[3]$, we need to handle the multi-user scenario with subtle but important adjustments. On the other hand, in case of $\mathsf{XORP}'[3]$, calculations are quite involved. However, as discussed above, by applying this method we get significantly better bounds than the existing ones. We give technical description of the χ^2 method in Section 2.3.

2 Preliminaries

2.1 Notation

In this paper, we denote 2^n by N. We fix $\mathcal{G}$ to be the group $\mathbb{F}_2^n$, and denote the group addition (*i.e.,* bit-wise `xor`) by $+$. For an element $\mathsf{g} \in \mathcal{G}$ and a subset $\mathcal{H} \in \mathcal{G}$, we denote by $\mathsf{g} + \mathcal{H}$ the subset $\{\mathsf{g} + \mathsf{h} | \mathsf{h} \in \mathcal{H}\}$. Sometimes (will be clear from context) we will term the elements of $\mathcal{G}$ as *blocks*.[5]

For a positive integer s, we denote an s-tuple $(\mathsf{x}_1, \ldots, \mathsf{x}_s)$ as x^s; however, when the value of s is clear from the context we will drop it (for notational simplicity) and denote the tuple as x. Also, when a sequence x^s is partitioned into subsequences (in a way that will be appropriately specified), we will denote the i-th subsequence by $\widehat{\mathsf{x}}_i$. Moreover, by slightly abusing the notation we will denote by $(\mathsf{x}^s \setminus \widehat{\mathsf{x}}_i)$ the subsequence of x^s formed (maintaining the same order of x^s) by removing the elements of $\widehat{\mathsf{x}}_i$.

For a random variable X, we write $\mathbf{Pr}_{\mathsf{X}}$ to denote the probability distribution (or function) corresponding to X. Sample space of a random variable X is a set Ω so that $\mathbf{Pr}_{\mathsf{X}}(\Omega) = 1$. Support of X is the sample space Ω of X so that for all $x \in \Omega$, $\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}) > 0$. Given a set $\mathcal{S}$ and the tuple $\mathsf{X}^s := (\mathsf{X}_1, \ldots, \mathsf{X}_s)$, we will write $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow_{\$} \mathcal{S}$ 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 $\mathsf{x}^s := (\mathsf{x}_1, \ldots, \mathsf{x}_s)$.

With and Without Replacement. Let $\mathcal{S}$ be a set of size M and s be a positive integer. To distinguish between *with replacement* (WR) sampling and *without replacement* (WOR) sampling (when they appear in the same context) we write $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow_{\mathrm{wr}} \mathcal{S}$ to represent that $\mathsf{X}_1, \ldots, \mathsf{X}_s$ are chosen randomly in WR manner from $\mathcal{S}$ (*i.e.*, $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow_{\$} \mathcal{S}$), and we write $\mathsf{X}_1, \ldots, \mathsf{X}_s \leftarrow_{\mathrm{wor}} \mathcal{S}$ to mean that X_i's are randomly sampled in WOR manner from the set $\mathcal{S}$. Let

$$\mathcal{S}^{\underline{s}} = \{(\mathsf{x}_1, \ldots, \mathsf{x}_s) : \mathsf{x}_i\text{'s are distinct elements of } \mathcal{S}\}$$

[5] We do not reserve the term 'block' solely for this purpose. However, its presence in other contexts will not create any ambiguity.

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

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

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

Definition 1 (Random Set). *A subset $\mathcal{V}_r \subseteq \mathcal{G}$ of size r is called a random r-set if it is chosen uniformly from the set of all r sized subsets of $\mathcal{G}$. Thus, for every $\mathcal{V} \subseteq \mathcal{G}$, with $|\mathcal{V}| = r$,*

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

Throughout the paper we denote a random r-set in $\mathcal{G}$ as $\mathcal{V}_r$. A random r-set can be constructed by drawing a random WOR sample, *i.e.*, $\mathcal{V}_r = \{\mathsf{X}_1, \ldots, \mathsf{X}_r\}$, where $(\mathsf{X}_1, \ldots, \mathsf{X}_r) \leftarrow_{\text{wor}} \mathcal{G}$. Note that the complement set $\mathcal{G} \setminus \mathcal{V}_r$ is a random $(N-r)$-set. We will require the following estimate from [BN18c].

Lemma 1 ([BN18c]). *If $2w < N$ then $1 - \frac{(N-r)^{\underline{w}}}{N^{\underline{w}}} \leq \frac{2rw}{N}$.*

2.2 Adversary and advantage

Here, we recall the notion of adversarial advantage in the context of a generic *indistinguishability game.* An *oracle adversary* or *oracle distinguisher* $\mathcal{A}$ is an *oracle algorithm* that interacts with an *oracle* $\mathcal{O}$ through a set of (potentially adaptive) queries and responses. Finally, it returns a bit $b \in \{0,1\}$. We express this as $\mathcal{A}^{\mathcal{O}} \to b$. In an *indistinguishability game*, $\mathcal{A}$ interacts with two oracles $\mathcal{O}_1$ and $\mathcal{O}_2$. The goal of $\mathcal{A}$ is to distinguish between $\mathcal{O}_1$ and $\mathcal{O}_2$ only from the corresponding queries and responses. The *advantage* of the adversary in this game, denoted $\mathsf{Adv}_{\mathcal{A}}(\mathcal{O}_1, \mathcal{O}_2)$, is given by

$$\mathsf{Adv}^{\text{dist}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) := |\mathbf{Pr}[\mathcal{A}^{\mathcal{O}_1} \to 1] - \mathbf{Pr}[\mathcal{A}^{\mathcal{O}_2} \to 1]|,$$

where the probabilities are taken over the random coins of $\mathcal{A}, \mathcal{O}_1$, and $\mathcal{O}_2$.

Pseudorandom function (PRF) is a very important cryptographic primitive. 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. PRF security is quantified by *PRF advantage.* Below we describe the PRF advantage of a *keyed function* which is relevant for this work.

Let m and n be positive integers. Let $\mathsf{Func}_{m\to n}$ is the set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$, and let $\mathsf{RF}_{m\to n} \leftarrow_{\$} \mathsf{Func}_{m\to n}$, *i.e.*, $\mathsf{RF}_{m\to n}$ is a function chosen uniformly at random from $\mathsf{Func}_{m\to n}$. Also, let $\mathcal{K}$ be a finite set, termed the *key space.* Given a function $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$, for every $\mathsf{k} \in \mathcal{K}$, we denote by f_{k} the function (also termed a *keyed function*) $f(\mathsf{k}, \cdot) \in \mathsf{Func}_{m\to n}$. The PRF advantage of an oracle adversary $\mathcal{A}$ against f is defined as follows.

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

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}) := \mathsf{Adv}_{f,RF}^{\mathrm{dist}}(\mathcal{A}) \ = |\mathbf{Pr}[\mathcal{A}^{f_{\mathsf{K}}} \to 1 \ : \ \mathsf{K} \leftarrow\!\!\$\, \mathcal{K}] - \ \mathbf{Pr}[\mathcal{A}^{RF_{m\to n}} \to 1]|.$$

PRP Advantage is defined in an analogous manner. Here, instead of a random function oracle the adversary $\mathcal{A}$ interacts with a random permutation oracle $\mathsf{RP}_n \leftarrow\!\!\$\, \mathsf{Perm}_n$, where Perm_n is the set of all permutations on $\{0,1\}^n$. PRP advantage is relevant in the context of a *block cipher* which is modeled as a *pseudorandom permutation.* More formally, an n-bit block cipher is a function $e : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ such that for all $\mathsf{K} \in \mathcal{K}$, $e_{\mathsf{K}} := e(\mathsf{K}, \cdot)$ is a permutation on $\{0,1\}^n$. The PRP advantage of $\mathcal{A}$ against e is defined as

$$\mathbf{Adv}_e^{\mathrm{prp}}(\mathcal{A}) = \mathsf{Adv}_{e,\mathsf{RP}}^{\mathrm{dist}}(\mathcal{A}) = \ |\mathbf{Pr}[\mathcal{A}^{e_{\mathsf{K}}} \to 1 \ : \ \mathsf{K} \leftarrow\!\!\$\, \mathcal{K}] - \ \mathbf{Pr}[\mathcal{A}^{\mathsf{RP}_n} \to 1]|.$$

We write $\mathbf{Adv}_f^{\mathrm{prf}}(q,t) \ = \max_{\mathcal{A}} \mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A})$ where maximum is taken over all adversaries making at most q queries and runs in time t. We similarly define $\mathbf{Adv}_f^{\mathrm{prp}}(q,t)$ for PRP advantage.

Since we are concerned with information theoretic security (with the only restriction that the adversary makes total q queries), w.l.o.g we assume that the adversary is deterministic and does not repeat its queries.

When $\mathcal{A}$ is interacting with $\mathsf{RF}_{m\to\ n}$, the outputs follow uniform and independent distributions over $\{0,1\}^n$ which we denote as $\mathsf{U}_1, \ldots, \mathsf{U}_q \leftarrow\!\!\$\, \{0,1\}^n$. Similarly, $\mathsf{X}_1, \ldots, \mathsf{X}_q$ denote the outputs of f_{K} where $\mathsf{K} \leftarrow\!\!\$\, \mathcal{K}$. We denote the probability distributions associated to $\mathsf{U}_1, \ldots, \mathsf{U}_q$ and $\mathsf{X}_1, \ldots, \mathsf{X}_q$ by $\Pr_{\mathsf{U}}$ and $\Pr_{\mathsf{X}}$ respectively. Thus,

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathcal{A}) = |\mathbf{Pr}_{\mathsf{X}}(\mathcal{E}) - \mathbf{Pr}_{\mathsf{U}}(\mathcal{E})|, \tag{1}$$

where $\mathcal{E}$ is the set of all q-tuple responses $\mathsf{x}^q = (\mathsf{x}_1, \ldots, \mathsf{x}_q) \in (\{0,1\}^n)^q$ at which $\mathcal{A}$ returns 1. It is well known that the statistical distance between the distributions $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{U}}$ is given by

$$\|\mathbf{Pr}_{\mathsf{U}} - \mathbf{Pr}_{\mathsf{X}}\| \overset{\mathrm{def}}{=} \frac{1}{2} \sum_{\mathsf{x}^q \in (\{0,1\}^n)^q} |\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}^q) - \mathbf{Pr}_{\mathsf{U}}(\mathsf{x}^q)| = \max_{\mathcal{E} \subseteq (\{0,1\}^n)^q} (\mathbf{Pr}_{\mathsf{X}}(\mathcal{E}) - \mathbf{Pr}_{\mathsf{U}}(\mathcal{E})). \tag{2}$$

Multi-user PRF Advantage is a generalization of the PRF advantage of a keyed function to the multi-user scenario. Let u be the number of users denoted by the elements of $[u]$. With a keyed function $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$, we associate its multi-user extension $f^{(u)} : \mathcal{K}^u \times [u] \times \{0,1\}^m \to \{0,1\}^n$ mapping (k^u, i, x) to $f_{\mathsf{k}_i}(x)$, for all $\mathsf{k}^u \in \mathcal{K}^u, i \in [u]$. Let RF denote the random function from $[u] \times \{0,1\}^m$ to $\{0,1\}^n$. We define the multi-user advantage against f for u users as

$$\mathbf{Adv}_f^{\mathrm{mu\text{-}prf}}(u, q_{\max}, q, t) = \max_{\mathcal{A}} \mathsf{Adv}_{f^{(u)},\mathsf{RF}}^{\mathrm{dist}}(\mathcal{A}),$$

where the maximum is taken over all adversaries $\mathcal{A}$ that run in time t making at most $q_{\max}$ queries to each user and q queries altogether to all users. To simplify our analysis, w.l.o.g. we allow $\mathscr{A}$ to make exactly q_{max} queries to each user in $[u]$. Indeed, this can only increase $\mathscr{A}$'s advantage which we are going to upper bound. So, with this convention, we have $q = u \times q_{max}$. Also, following the same considerations made for the single-user case we assume, w.l.o.g, that $\mathscr{A}$ makes distinct queries to individual users.

2.3 χ^2 Method

Given a set Ω, let $\mathsf{X}^q := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$ and $\mathsf{Z}^q := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q)$ be two random vectors distributed over $\Omega^q = \Omega \times \cdots \times \Omega$ (q times) according to the distributions $\Pr_{\mathsf{X}}$ and $\Pr_{\mathsf{Z}}$ respectively. In what follows, we will require the following conditional distributions.

$$\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}_1 = \mathsf{x}_1, \ldots, \mathsf{X}_{i-1} = \mathsf{x}_{i-1}],$$
$$\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{Z}_i = \mathsf{x}_i \mid \mathsf{Z}_1 = \mathsf{x}_1, \ldots, \mathsf{Z}_{i-1} = \mathsf{x}_{i-1}].$$

When $i = 1$, $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_1)$ represents $\mathbf{Pr}[X_1 = \mathsf{x}_1]$. Similarly, for $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_1)$. Let $\mathsf{x}^{i-1} \in \Omega^{i-1}$, $i \geq 1$. The χ^2-distance between these two conditional probability distributions is defined as

$$\chi^2(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}, \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}) := \sum_{x_i \in \Omega} \frac{(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) - \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i))^2}{\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i)}, \tag{3}$$

with the assumption that the support of the distribution $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}$ be contained within the support of the distribution $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}$. Further, when the distributions $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}$ and $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}$ are clear from the context we will use the notation $\chi^2(\mathsf{x}^{i-1})$ for $\chi^2(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}, \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}})$. Then the crux of the χ^2 method is the following theorem from [DHT17] (see also [BN18b]).

Theorem 1 ([DHT17]). *Following the notation as above and suppose the support of the distribution $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}$ is contained within the support of the distribution $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}$ for all x^{i-1}, then*

$$\|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Z}}\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}}, \tag{4}$$

where for each i, the expectation is over the $(i-1)$-th marginal distribution of $\mathbf{Pr}_{\mathsf{X}}$.

3 Multi-User PRF Security of $\mathsf{XORP}[3]$

In this section, we analyze the multi-user PRF security of $\mathsf{XORP}[3](x)$. Formally, the output of $\mathsf{XORP}[3]$ is given by $\mathsf{XORP}[3](x) := \mathsf{RP}(x\|00) \oplus \mathsf{RP}(x\|01) \oplus \mathsf{RP}(x\|10)$, where RP is an n-bit random permutation and $x \in \{0,1\}^{n-2}$. In the multi-user setting of $\mathsf{XORP}[3]$, we let $\mathscr{A}$ to interact with u users $[u] : \{1, \ldots, u\}$.

In the real world, each of the u users holds an independent copy of the underlying random permutation RP. In the ideal world, there is a random function $\mathsf{RF} : [u] \times \{0,1\}^{n-2} \to \{0,1\}^n$. We allow $\mathscr{A}$ to make total q queries of the form (u_i, x_i) with $u_i \in [u], \mathsf{x}_i \in \{0,1\}^{n-2}$ for $i \in [q]$. Repeating our assumptions for multi-user security in this setting we have (i) For all $v \in [u]$ if $(v, \mathsf{x}_i), (v, \mathsf{x}_j)$ are two queries then $\mathsf{x}_i \neq \mathsf{x}_j$ (ii) For all $v \in [u]$ the number of queries of the form (v, x) is q_{max}. So, we have $q = u \times q_{max}$.

Let the transcript of replies be $\mathsf{P} := (\mathsf{P}_1, \ldots, \mathsf{P}_q)$ when $\mathscr{A}$ is interacting in the real world and $\mathsf{R} := (\mathsf{R}_1, \ldots, \mathsf{R}_q)$ when it is interacting in the ideal world, where $\mathsf{P}_i, \mathsf{R}_i \in \mathcal{G}$ are the replies to the i-th query. Therefore, here our goal is to upper bound $\|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$. Here, it is important to observe that the q_{max} replies given by any user is distributed independently of the other replies. For example, suppose w.l.o.g. that user 1's reply is the sequence $(\mathsf{P}_1, \ldots, \mathsf{P}_{q_{max}})$. Then $(\mathsf{P}_1, \ldots, \mathsf{P}_{q_{max}})$ is independent of $(\mathsf{P}_{q_{max}+1}, \ldots, \mathsf{P}_q)$. Indeed, this follows from the fact that each user in $[u]$ holds an independent copy of RP.

Now, there is a subtle technical difficulty involved while working with the distributions $\mathbf{Pr}_{\mathsf{P}}$ and $\mathbf{Pr}_{\mathsf{R}}$ in the setting of the χ^2-method. The difficulty arises because user U_i for the i-th query is not completely dependent on i. We will highlight and elaborate more on the issue at the appropriate place in our proof of Theorem 2 (see the discussion immediately following (7)).

In order to overcome the difficulty, we reorder the samples P and R to get new samples S and U respectively. In S, P_i's are grouped into a sequence of u blocks, where each block comprises of q_{max} P_i's output by the same user; similarly for the distribution U (though we note that R and U are the same, because any reordering of a sequence of q outputs of a random function is identical to itself).[6] Now it is easy to see that in S and U each $i \in [q]$ uniquely identifies $U_i \in [u]$. In Fig. 3.1, we present a precise description of the samples U and S together with a formal explanation presented below.

For $i \in [u]$, let $\mathrm{I}_i := \{(i-1)q_{max} + j : j \in [q_{max}]\}$. So, the sequence $(\mathrm{I}_i)_{i \in [u]}$ partitions $[q]$. Let $\mathsf{U} := (\mathsf{U}_1, \mathsf{U}_2, \ldots, \mathsf{U}_q)$, be a WR or with replacement sample (represented as a tuple) of size q, each U_i is sampled from $\mathcal{G}$ uniformly and independently. In other words, we have $\mathsf{U} \leftarrow\!\!\$\, \mathcal{G}^q$. On the other hand, the sample $\mathsf{S} := (\mathsf{S}_1, \mathsf{S}_2, \ldots, \mathsf{S}_q)$ is generated (as described in Fig. 3.1) as follows. First, for each $i \in [u]$, a WOR or without replacement sample $\widehat{\mathsf{T}}_i = (\mathsf{T}_{j,k} : j \in \mathrm{I}_i, k \in [3])$ of size $3q_{max}$ is generated, where $\widehat{\mathsf{T}}_i$ is independent of $\widehat{\mathsf{T}}_j$ for each $1 \le j \le i-1$.

[6] It is not difficult to conceive a bijection between P and S effected by the reordering described here (since R and U are identical we only focus on P and S). Indeed, for this purpose one can consider an extended transcript $\mathsf{P}' := ((\mathsf{P}_1, U_1), \ldots, (\mathsf{P}_q, U_q))$ which also contains the user U_i associated with the i-th query, and subsequently express the bijection in an explicit manner. However, we will not do that here in order to reduce notational complexity. More so, because we will not refer to this bijection in the subsequent discussion.

Then for each $\ell \in [q]$, S_ℓ is computed as

$$\mathsf{S}_\ell = \mathsf{T}_{\ell,1} + \mathsf{T}_{\ell,2} + \mathsf{T}_{\ell,3}.$$

So both U and S have the same sample space $\mathscr{G}^q$, and since they are permutations of R and P respectively, we note that

$$\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| = \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \tag{5}$$

Here it can be noted that the reordering works in the case of XORP[3] because the distribution of the output of any query does not depend on the input value in both worlds. Moreover, we assumed with no loss of advantage for the adversary, the number of queries to each user is constant (maximum allowed for each user).

```
Random Experiment for $\mathsf{U}$
$\mathsf{U} := (\mathsf{U}_i : i \in [q]) \leftarrow_{\text{wr}} \mathscr{G}$
return $\mathsf{U}$
```

```
Random Experiment for $\mathsf{S}$
for $1 \le i \le u$
    $\widehat{\mathsf{T}}_i := (\mathsf{T}_{j,k} : j \in [\mathrm{I}_i], k \in [3]) \leftarrow_{\text{wor}} \mathscr{G}$
    // $\widehat{\mathsf{T}}_i$ is sampled independent of $\widehat{\mathsf{T}}_j$,  $1 \le j \le i-1$
for $1 \le \ell \le q$
    $\mathsf{S}_\ell = \mathsf{T}_{\ell,1} + \mathsf{T}_{\ell,2} + \mathsf{T}_{\ell,3}$
return $\mathsf{S} := (\mathsf{S}_\ell : \ell \in [q])$
```

Fig. 3.1: Description of sampling methods of random variables U, S.

Now, we state our main theorem which provides an upper bound on the statistical distance $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$. The theorem shows that the sample S is very close to the uniform sample U even though it is computed from a non-uniform sample.

Theorem 2 (Pseudorandomness of S). *Let U and S be the random vectors as described in Fig. 3.1. Then, for all $q_{max} \le N/12$*

$$\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| \le \frac{20\sqrt{uq_{max}}}{N}$$

We postpone the proof to Section 3.4.

3.1 Application to Single-user PRF Security of XORP[3]

We now describe the cryptographic implications of the result from Theorem 2. Let us define $\mathsf{XORP}[3]$ construction based on a single keyed n-bit block cipher $e : \mathscr{K} \times \{0,1\}^n \to \{0,1\}^n$ with key-space $\mathscr{K}$. For $x \in \{0,1\}^{n-2}$ and $\mathsf{k} \in \mathscr{K}$, we define

$$\mathsf{XORP}_e[3](\mathsf{k}, x) = e_{\mathsf{k}}(x\|00) \oplus e_{\mathsf{k}}(x\|01) \oplus e_{\mathsf{k}}(x\|10) \tag{6}$$

Using the hybrid argument we can replace e by a random permutation at the cost of PRP advantage. Then we can apply our result to get the following corollary.

Corollary 1. *For all $q \leq 2^n/12$,*

$$\mathbf{Adv}^{\text{prf}}_{\mathsf{XORP}_e[3]}(q,t) \leq \mathbf{Adv}^{\text{prp}}_{e}(3q,t') + \frac{20\sqrt{q}}{2^n}$$

where $t' \approx t + 3q$.

The above corollary is a simple hybrid argument where we replace the underlying block cipher e by a random permutation. We note that outputs of a random permutation for distinct inputs is exactly a WOR or without replacement sample and hence we apply Theorem 2.

3.2 Application to Multi-user PRF Security of XORP[3]

Similarly, we state multi-user security of XORP construction.

$$\mathbf{Adv}^{\text{mu\_prf}}_{\mathsf{XORP}_e[3]}(u, q_{\max}, q, t) \leq \mathbf{Adv}^{\text{mu\_prp}}_{e}(u, 3q_{\max}, t') + \frac{20\sqrt{uq_{\max}}}{N}$$

where u denotes the number of users.

3.3 Application to Counter Mode Encryption

Parity method encryption scheme introduced by Bellare-Goldreich-Krawczyk in [BGK99] is a probabilistic encryption scheme based on a pseudorandom function. Let $F_{\mathsf{K}} : \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Then for message $\mathsf{m} \in \{0,1\}^n$ and randomness $\mathsf{r}^t := (\mathsf{r}_1, \ldots, \mathsf{r}_t) \in (\{0,1\}^n)^t$, the ciphertext of the parity method encryption scheme is given by $(\mathsf{r}^t, F_{\mathsf{K}}(\mathsf{r}_1) \oplus \cdots \oplus F_{\mathsf{K}}(\mathsf{r}_t) \oplus \mathsf{m})$. For all $q \leq N/(e^2 t)$, the PRF-advantage of this construction is shown to be $O(q^2/N^t) + O(q^3/N^{3t/2})$ for even t and $O(q^2/N^t) + O(q^4/N^{2t})$ for odd t. Thus, for $t = 2$, the construction achieves n-bit security and for $t = 4$, it achieves beyond n-bit security. However, the construction requires a pseudorandom function and random coins.

Counter mode encryption is a practical alternative to the above scheme. In counter mode encryption, we replace the random coins by some nonce (which does not repeat over all executions). More precisely, for nonce N and message m, the ciphertext of the counter mode encryption is $(\mathsf{N}, F_{\mathsf{K}}(\mathsf{N}) \oplus \mathsf{m})$. If the nonce does not repeat then the security of the encryption relies on the PRF security of F_{K}.

As the counter mode is quite popular and has wide applications, the multi-user security of the counter mode is also of considerable significance. Now, $\mathsf{XORP}[3]$, which uses pseudorandom permutations, can be seen to be the following counter mode encryption scheme.

Let s be the size of the counter (maximum message length is at most $n2^s$).

1. Given a message $\mathsf{m} = (\mathsf{m}_1, \ldots, \mathsf{m}_\ell) \in \{0,1\}^{n\ell}$, and a nonce $\mathsf{N} \in \{0,1\}^{n-s-2}$, we define $\mathsf{x}_{i,j} = \mathsf{N} \| \langle j \rangle_2 \| \langle i \rangle_s$, for all $j \in [3], i \in [\ell]$.
2. Let $\mathsf{z}_i = e_{\mathsf{K}}(\mathsf{x}_{i,1}) \oplus e_{\mathsf{K}}(\mathsf{x}_{i,2}) \oplus e_{\mathsf{K}}(\mathsf{x}_{i,3})$ for all $i \in [\ell]$.
3. The ciphertext is defined as $(\mathsf{N}, \mathsf{z}_1 \oplus \mathsf{m}_1, \ldots, \mathsf{z}_\ell \oplus \mathsf{m}_\ell)$.

The multi-user PRF security of the above encryption scheme is the same as the multi-user PRF security of XORP[3]. More precisely, the u-user privacy advantage of the counter mode encryption scheme (provided the nonce does not repeat) for an adversary making (i) at most $q_{\max}$ queries to each user, (ii) maximum number of message blocks is at most ℓ, and (iii) total q queries made to all usersis given by (following the same hybrid argument as before)

$$\mathbf{Adv}_e^{\text{mu-prp}}(u, 3\ell q, t') + \frac{20\sqrt{uq_{max}}}{N}$$

.

3.4 Proof of Theorem 2

First, in Fig. 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 7 of the random experiment for Y, the execution following **else** will not be required in our paper. It is kept only for the sake of the completeness of the definition. We will formally show this in Claim 1.

Random Experiment for X

```
1 : for $1 \le i \le u$
2 :   $\widehat{\mathsf{T}}_i := (\mathsf{T}_{j,k} : j \in [\mathrm{I}_i], k \in [3]) \leftarrow_{\text{wor}} \mathcal{G}$
      // $\widehat{\mathsf{T}}_i$ is independent of $\widehat{\mathsf{T}}_\ell, 1 \le \ell \le i-1$
3 : for $1 \le i \le q$
4 :   $\mathsf{S}_i = \mathsf{T}_{i,1} + \mathsf{T}_{i,2} + \mathsf{T}_{i,3}$
5 :   $\mathsf{X}_i = (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i)$
6 : return $\mathsf{X} := (\mathsf{X}_i : i \in [q])$
```

Random Experiment for Y

```
1 : for $1 \le i \le u$
2 :   initialize $\mathcal{S}_i^0 = \mathcal{G}$
3 :   for $j \in \mathrm{I}_i$
4 :     $k = j - (i-1)q_{max}$
5 :     $\mathsf{U}_j \leftarrow_{\$} \mathcal{G}$
6 :     $\mathcal{n}_j = \{(\mathsf{v}_1, \mathsf{v}_2) |$
            $\mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_j + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{S}_i^{k-1}$,
            $\mathsf{U}_j + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2$ distinct$\}$
7 :     if $\mathcal{n}_j \neq \emptyset$ then $(\mathsf{V}_{j,1}, \mathsf{V}_{j,2}) \leftarrow_{\$} \mathcal{n}_j$
8 :     else $(\mathsf{V}_{j,1}, \mathsf{V}_{j,2}) = (0, 0)$
9 :     $\mathsf{Y}_j = (\mathsf{V}_{j,1}, \mathsf{V}_{j,2}, \mathsf{U}_j)$
10 :    $\mathcal{S}_i^k = \mathcal{S}_i^{k-1} \setminus \{\mathsf{V}_{j,1}, \mathsf{V}_{j,2},$
11 :          $\mathsf{V}_{j,3} := \mathsf{U}_j + \mathsf{V}_{j,1} + \mathsf{V}_{j,2}\}$
12 : return $\mathsf{Y} := (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$
```

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

Claim 1 *In the Random Experiment for* Y *(in Fig. 3.2),* $\mathcal{N}_j \neq \emptyset$ *holds for all* j*. Therefore, line 8 (following* ***else****) never executes.*

Proof of claim. Without loss of generality first we fix user i. Then it is sufficient to show that for any $\mathsf{u}_j \in \mathcal{G}$, we can choose distinct $\mathsf{v}_1, \mathsf{v}_2 \in \mathcal{S}_i^{k-1}$ such that $\mathsf{u}_j + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{S}_i^{k-1} \setminus \{\mathsf{v}_1, \mathsf{v}_2\}$ for $k \leq q_{max}$. To do this, we fix $\mathsf{u}_j \in \mathcal{G}$. Note that the distinctness of $\mathsf{v}_1, \mathsf{v}_2, \mathsf{u}_j + \mathsf{v}_1 + \mathsf{v}_2$ is equivalent to the distinctness of $\mathsf{v}_1, \mathsf{v}_2, \mathsf{u}_j$. Now, we choose v_1 arbitrarily from the set $\mathcal{S}_i^{k-1} \setminus \{\mathsf{u}_j\}$. This is clearly possible as we have that $|\mathcal{S}_i^{k-1} \setminus \{\mathsf{u}_j\}| \geq N - 3(k-1) > N - 3q_{max} \geq \frac{3N}{4}$, since $q_{max} \leq \frac{N}{12}$ by our assumption. Next, we choose v_2 arbitrarily from the set $\mathcal{D} = \mathcal{S}_i^{k-1} \setminus \{\{\mathsf{u}_j, \mathsf{v}_1\} \cup \{(\mathsf{u}_j + \mathsf{v}_1) + \{\mathcal{G} \setminus \mathcal{S}_i^{k-1}\}\}\}$. This is also possible since $|\mathcal{D}| \geq N - (2 \times 3(k-1) + 2) > N - 6q_{max} \geq \frac{N}{2}$. Then it is easy to see that, for the given u_j, the choice of v_1 and v_2 satisfies the desired condition. ■

Let $\mathcal{C} = \mathcal{G}^3$ denote the set of all 3-tuples of $\mathcal{G}$. To understand the probability distributions of the random vectors X and Y and their supports we consider the following involution (a permutation with self inverse) ρ over the set $\mathcal{C}$ mapping $(\mathsf{x}_1, \mathsf{x}_2, \mathsf{x}_3)$ to $(\mathsf{x}_1, \mathsf{x}_2, \mathsf{x}_1 + \mathsf{x}_2 + \mathsf{x}_3)$.

We extend the definition of the mapping ρ to a mapping ρ^* which is defined over $\mathcal{C}^c$ for any c. Formally, we define $\rho^*(\mathsf{z}_1, \ldots, \mathsf{z}_c) := (\rho(\mathsf{z}_1), \ldots, \rho(\mathsf{z}_c))$. From the random experiments, it is trivial to see that

$$\rho(\mathsf{X}_i) = \mathsf{T}_i := (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{T}_{i,3}) \qquad \rho(\mathsf{Y}_i) = \mathsf{V}_i := (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3})$$

where $\mathsf{V}_{i,3} = \mathsf{U}_i + \mathsf{V}_{i,1} + \mathsf{V}_{i,2}$. So, for every $i \in [q]$, $\rho^*(\mathsf{X}^i) = \mathsf{T}^i$ and $\rho^*(\mathsf{Y}^i) = \mathsf{V}^i$. In other words, the random variables X and Y are equivalent to the random variables T and $\mathsf{V} := ((\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}), i \in [q])$ respectively. More precisely, in the first case, for each $i \in [u]$, we first have WOR sample $\widehat{\mathsf{T}}_i$ and then define $\widehat{\mathsf{X}}_i$ by applying ρ on each block. Whereas, in the second case, for each $i \in [u]$, we first sample $\widehat{\mathsf{Y}}_i$ (extending a WR sample $\widehat{\mathsf{U}}_i$) and then we define $\widehat{\mathsf{V}}_i$ by applying ρ on each block. However, $\widehat{\mathsf{V}}_i$ behaves like a WOR sample (though it is not perfect WOR sample, it would have same support as a WOR sample). So for every $i \in [u]$ and every $j \in [q_{max}]$, the support of $\widehat{\mathsf{T}}_i^j$ (as well as $\widehat{\mathsf{V}}_i^j$) is the set

$$\widehat{\Gamma}_i^j := \{((\mathsf{a}_{i',1}, \mathsf{a}_{i',2}, \mathsf{a}_{i',3}) : i' \in [j]) : \mathsf{a}'_{i',k}s \text{ are distinct for all } i' \in [j], k \in [3]\}.$$

Hence, the support of $\widehat{\mathsf{X}}_i^j$ (as well as $\widehat{\mathsf{Y}}_i^j$), denoted as $\widehat{\Omega}_i^j$, would be the set of all such $3j$ tuples

$$\begin{aligned}\widehat{\Omega}_i^j := \{(\mathsf{x}_{i',j} : i' \in [j], k \in [3]) \in \mathcal{G}^{3i} :& ((\mathsf{a}_{i',1}, \mathsf{a}_{i',2}, \mathsf{a}_{i',3}) : i' \in [j]) \in \widehat{\Gamma}_i^j \\ & \rho(\mathsf{a}_{i',1}, \mathsf{a}_{i',2}, \mathsf{a}_{i',3}) = (\mathsf{x}_{i',1}, \mathsf{x}_{i',2}, \mathsf{x}_{i',3})\}.\end{aligned}$$

Therefore, the support of vectors X and Y is given by $\Omega = (\widehat{\Omega}_i^{q_{max}} | i \in [u])$.

Next, for a fixed $i \in [q]$ let $i = (j-1)q_{max} + k,\ j \in [u], k \in [q_{max}]$. Then it follows that $\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k} \in \widehat{\mathsf{X}}_j^k$. Then for every $\mathsf{x}^i \in \Omega^i$, the conditional probability for X can be expressed as

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\overset{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \ | \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\
&= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \ | \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}], \qquad (7) \\
&\quad \text{since } \widehat{\mathsf{X}}_j \text{ is independent of } (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) \\
&= \mathbf{Pr}[\widehat{\mathsf{T}}_{j,k} = \widehat{\mathsf{t}}_{j,k} \ | \widehat{\mathsf{T}}_j^{k-1} = \widehat{\mathsf{t}}_j^{k-1}] \\
&= \frac{1}{(N - 3(k-1))^{\underline{3}}}. \qquad (8)
\end{aligned}$$

Here, we take a small but important detour in our proof to explain the technical issue involving the distributions $\mathbf{Pr}_{\mathsf{P}}$ and $\mathbf{Pr}_{\mathsf{R}}$ mentioned in the beginning. Note that in (7) the independence of $\widehat{\mathsf{X}}_j$ from $(\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j)$ follows because the user number u_i is completely determined by i. This is not the case for the original distribution $\mathbf{Pr}_{\mathsf{P}}$. Indeed, for this distribution $\mathcal{A}$ can make adaptive choice of user u_i for the i-th query based on all the previous queries, and hence P_i may depend on the entire P^{i-1}. By reordering P into S (and correspondingly X) we make u_i completely determined by i, and hence the independence of $\widehat{\mathsf{X}}_j$ from $(\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j)$. Similar observation holds in (9) corresponding to the reordering of the distribution R into U (and subsequently into Y).

Now, we introduce some notations for the random experiment Y.

For all $i \in [q]$, let us denote $\mathsf{u}_i = \mathsf{x}_{i,3}$, *i.e.,* $\mathsf{x}_i = (\mathsf{x}_{i,1}, \mathsf{x}_{i,2}, \mathsf{u}_i)$. As before, let $\rho(\mathsf{x}_{i'}) = \mathsf{t}_{i'}$ for every $i' \in [i]$. So, $\mathsf{t}_{i',j}$'s are distinct. Now, we define the two crucial sets for our analysis. For $j \in [u], k \in [q_{max}]$ let us denote

$$\mathcal{S}_j^k = \mathcal{G} \setminus \{\mathsf{t}_{\ell,p} : \ell \in [\mathrm{I}_j], p \in [3]\}, \text{ with } \mathcal{S}_j^0 = \mathcal{G},$$
$$\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1}) := \{\mathsf{v}_1, \mathsf{v}_2 \in \mathcal{S}_j^{k-1} : \mathsf{u}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{S}_j^{k-1} \text{ and } \mathsf{v}_1, \mathsf{v}_2, \mathsf{u}_i \text{ distinct }^7\}.$$

Now, for $\mathsf{U}_i = \mathsf{u}_i$ and $\widehat{\mathsf{Y}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}$, the set $\mathcal{N}_i$ and the set $\mathcal{S}_j^k$ (defined in the line 5 and line 9 of the random experiment of Y in Fig. 3.2) is exactly the same as the set $\mathcal{N}^{u_i}(\widehat{\mathsf{x}}_j^{k-1})$ and $\mathcal{S}_j^k$ defined above. It is easy to observe the following:

$$\text{If } \widehat{\mathsf{x}}_j^{k-1} \in \widehat{\Omega}_j^{k-1} \text{ then the set } \mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1}) \text{ is nonempty as } \mathsf{x}_{i,1}, \mathsf{x}_{i,2} \in \mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1}).$$

Recall that in Claim 1 we have already justified that the set $\mathcal{N}_i$ is non-empty (and hence line 8 of the Random Experiment for Y is never executed) using a different argument. Now, we compute the conditional probability on the support of Y.

[7] As noted earlier in Claim 1, the condition that $\mathsf{v}_1, \mathsf{v}_2, \mathsf{u}_i$ are distinct is equivalent to the condition that $\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_1 + \mathsf{v}_2 + \mathsf{u}_i$ are distinct.

Claim 2 *Let $i = (j-1)q_{max} + k$, with $i \in [q], j \in [u], k \in [q_{max}]$. Then for all $\mathsf{x}^i \in \Omega^i$ we have,*

$$\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) \overset{\text{def}}{=} \mathbf{Pr}[\mathsf{Y}_i = \mathsf{x}_i \mid \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] = \frac{1}{N} \times \frac{1}{|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|}.$$

$\mathsf{Proof\ of\ claim.}$ First, note that $\mathsf{x}^{i-1} \in \Omega^{i-1}$, and $\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})$ cannot be the empty set as $\mathsf{x}_{i,1}, \mathsf{x}_{i,2} \in \mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})$. So,

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\overset{\text{def}}{=} \mathbf{Pr}[\mathsf{Y}_i = \mathsf{x}_i \mid \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] \\
&= \mathbf{Pr}[\widehat{\mathsf{Y}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{Y}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{Y}^{i-1} \setminus \widehat{\mathsf{Y}}_j^{k-1}) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})], \qquad (9) \\
&\quad \text{(since } (\mathsf{Y}^{i-1} \setminus \widehat{\mathsf{Y}}_j^{k-1}) \text{ is independent of } \widehat{\mathsf{Y}}_j^{k-1} \text{ and } \widehat{\mathsf{Y}}_{j,k}) \\
&= \mathbf{Pr}[\widehat{\mathsf{Y}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{Y}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}] \\
&= \mathbf{Pr}[\mathsf{U}_i = \mathsf{u}_i \mid \widehat{\mathsf{Y}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}] \times \mathbf{Pr}[(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) = (\mathsf{x}_{i,1}, \mathsf{x}_{i,2}) \mid \\
&\quad \mathsf{U}_i = \mathsf{u}_i \wedge \widehat{\mathsf{Y}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}] \\
&= \frac{1}{N} \times \frac{1}{|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})}. \qquad (10)
\end{aligned}$$

The last equality follows from the definition of sampling of U_i and $(\mathsf{V}_{i,1}, \mathsf{V}_{i,2})$.■

We now apply the χ^2 method to X and Y.

$$\begin{aligned}
\chi^2(\mathsf{x}^{i-1}) &:= \sum_{\mathsf{x}_i} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1})} \\
&=_{(a)} \sum_{\mathsf{x}_i = (\mathsf{x}_{i,1}, \mathsf{x}_{i,2}, \mathsf{u}_i)} \frac{\left(\frac{1}{(N-3(k-1))^{\underline{3}}} - \frac{1}{N|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|}\right)^2}{\frac{1}{N|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|}} \\
&=_{(b)} C \times \sum_{\mathsf{u}_i} \sum_{(\mathsf{x}_{i,1}, \mathsf{x}_{i,2})} \frac{\left(|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D\right)^2}{|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|} \\
&=_{(c)} C \times \sum_{\mathsf{u}_i} \left(|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D\right)^2, \qquad (11)
\end{aligned}$$

where $C = \frac{N}{((N-3(k-1))^{\underline{3}})^2}$, and $D = \frac{(N-3(k-1))^3}{N}$. The equality (a) follows by plugging the conditional probabilities derived in (8) and (10). The expression on the r.h.s. of (b) is obtained by algebraic simplification. The equation (c) follows from the observation that

(1) $\frac{\left(|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D\right)^2}{|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|}$ is functionally independent of $(\mathsf{x}_{i,1}, \mathsf{x}_{i,2})$,

and (2) for each u_i, the number of choices of $(\mathsf{x}_{i,1}, \mathsf{x}_{i,2})$ is $|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|$.

Next, in order to apply Theorem 1, we compute $\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]$ which (from (11)) is given by

$$C \times \sum_{\mathsf{u}_i} \mathbf{Ex}[\big(|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{X}}_j^{k-1})| - D\big)^2].$$

Note that $|\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|$ is a function of $\widehat{\mathsf{x}}_j^{k-1}$, and so, it is also a function of $\widehat{\mathsf{t}}_j^{k-1}$. When $\widehat{\mathsf{x}}_j^{k-1}$ is sampled according to $\widehat{\mathsf{X}}_j^{k-1}$, $\widehat{\mathsf{t}}_j^{k-1}$ would be sampled according to $\widehat{\mathsf{T}}_j^{k-1}$ (WOR sample).

For notational simplicity, let $r = N - 3(k-1)$ and $r' = N - r = 3(k-1)$. Note that $D = \frac{r^{\underline{3}}}{N}$. Also, let

$$\mathcal{V}_r = \mathcal{G} \setminus \{\mathsf{T}_{\ell,p} : \ell \in \mathrm{I}_j, \ell \le i, p \in [3]\},$$

which is a random r-set in $\mathcal{G}$. Then the set $\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})$ is same as the set

$$\{\mathsf{v}_1, \mathsf{v}_2 \in \mathcal{V}_r : \mathsf{u}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{V}_r, \text{ and } \mathsf{u}, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct}\}.$$

We denote the size of the set by $\mathbf{N}_r^{\mathsf{u}_i}$. Then we have

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] = C \times \sum_{u_i} \mathbf{Ex}[\big(\mathbf{N}_r^{\mathsf{u}_i} - D\big)^2]. \tag{12}$$

Next, we apply the following core lemma (its proof is postponed to section 3.5) to get an upper bound on the r.h.s. of (12).

Lemma 2 (core lemma for XORP). *Let C, r, r' be defined as above, where $r' \le \frac{N}{4}$. Then for every $\mathsf{b} \in \mathcal{G}$, we have*

$$\mathbf{Ex}[\mathbf{N}_r^{\mathsf{b}}] = \frac{r^{\underline{3}}}{N}, \quad \textit{and} \quad \mathbf{Ex}[(\mathbf{N}_r^{\mathsf{b}} - \frac{r^{\underline{3}}}{N})^2] \le \frac{1}{C}\left(\frac{576}{N^3} + \frac{4^8(r')^3}{27N^6}\right). \tag{13}$$

Subsequently, for $r' \le \frac{N}{4}$ we have

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \le \frac{576}{N^2} + \frac{4^8(r')^3}{27N^5}.$$

Now, we continue to bound the statistical distance between X and Y using the χ^2-method as follows. Since $q_{max} \le N/12$, we have $r' \le N/4$ (a required condition for our core lemma). Therefore

$$\begin{aligned}
\|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\| &\le \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}} \\
&= \left(\frac{1}{2}\sum_{j=1}^{u}\sum_{k=1}^{q_{max}} \mathbf{Ex}[\chi^2(\mathsf{X}^{k-1})]\right)^{\frac{1}{2}} \\
&\le \left(\sum_{j=1}^{u}\sum_{k=1}^{q_{max}} \frac{288}{N^2} + \frac{4^8(r')^3}{54N^5}\right)^{\frac{1}{2}}
\end{aligned}$$

$$\begin{aligned}
&\leq \left(\sum_{j=1}^{u} \sum_{k=1}^{q_{max}} \frac{288}{N^2} + \frac{4^8(k-1)^3}{2N^5} \right)^{\frac{1}{2}} \quad \text{, since } r' = 3(k-1) \\
&\leq \left(\sum_{j=1}^{u} \frac{288q_{max}}{N^2} + \frac{4^7 {q_{max}}^4}{2N^5} \right)^{\frac{1}{2}} \\
&\leq \left(\frac{288uq_{max}}{N^2} + \frac{4^7 u{q_{max}}^4}{2N^5} \right)^{\frac{1}{2}} \\
&\leq \frac{12\sqrt{2uq_{max}}}{N} + \frac{64\sqrt{2u}{q_{max}}^2}{N^{\frac{5}{2}}}. \\
&\leq \frac{12\sqrt{2uq_{max}}}{N}(1 + 6/(12)^{1.5}) \text{ , since } q_{max} \leq N/12 \\
&\leq \frac{20\sqrt{uq_{max}}}{N}.
\end{aligned}$$

Therefore, we finally have

$$\|\mathbf{Pr}_{\mathsf{Q}} - \mathbf{Pr}_{\mathsf{S}}\| \leq \|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\| \leq \frac{20\sqrt{uq_{max}}}{N}.$$

■

3.5 Proof of Lemma 2

Let r, N be positive integers such that $r' = N - r \leq \frac{N}{4}$. Let $\mathcal{G}$ be a group of size N, and $\mathcal{V}_r$ be a random r-set in $\mathcal{G}$.

Definition 3. *For* $\mathsf{u} \in \mathcal{G}$ *we associate a random variable* $\mathbf{N}_r^{\mathsf{u}}$ *defined as the size of the following set*

$$\mathcal{N}_r^{\mathsf{u}} := \{\mathsf{g}_1 \neq \mathsf{g}_2 \in \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r, \mathsf{g}_1 \neq \mathsf{u} \neq \mathsf{g}_2.\}$$

We would like to note that $\mathbf{N}_r^{\mathsf{u}}$ as defined above is equivalent to the previous definition since $\mathcal{V}_r$ is a random r'-set. We represent $\mathbf{N}_r^{\mathsf{u}}$ as a sum of indicator random variables. To do so we define the set $\mathcal{G}_{\mathsf{u}}$ of tuples of distinct elements of $\mathcal{G}$ as

$$\mathcal{G}_{\mathsf{u}} = \{(\mathsf{g}_1, \mathsf{g}_2) | \mathsf{g}_1 \neq \mathsf{g}_2 \in \mathcal{G} \setminus \{\mathsf{u}\}\}.$$

So, $|\mathcal{G}_{\mathsf{u}}| = (N-1)(N-2)$. Then we have

$$\mathbf{N}_r^{\mathsf{u}} = \sum_{\mathsf{g} \in \mathcal{G}_{\mathsf{u}}} \mathtt{I}_{\mathsf{g}}, \tag{14}$$

where, for $\mathsf{g} = (\mathsf{g}_1, \mathsf{g}_2)$, the indicator random variable $\mathtt{I}_{\mathsf{g}}$ is defined as

$$\mathtt{I}_{\mathsf{g}} = \begin{cases} 1 \text{ if } \mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r, \text{ and } \mathsf{g}_1 \neq \mathsf{u} \neq \mathsf{g}_2 \\ 0 \text{ otherwise.} \end{cases}$$

We note that $\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2$ are distinct elements of $\mathcal{G}$ since $\mathsf{g}_1 \neq \mathsf{u} \neq \mathsf{g}_2$. So, the number of r-sets that contain the three distinct elements $\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2$ is exactly $\binom{N-3}{r-3}$. Thus,

$$\mathbf{Ex}[\mathtt{I}_\mathsf{g}] = \mathbf{Pr}[\{\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2\} \subseteq \mathcal{V}_r] = \frac{\binom{N-3}{r-3}}{\binom{N}{r}} = \frac{r^{\underline{3}}}{N^{\underline{3}}}. \tag{15}$$

By using the linearity of expectation, we have

$$\begin{aligned}\mathbf{Ex}[\mathbf{N}_r^\mathsf{u}] &= \sum_{\mathsf{g} \in \mathcal{G}_\mathsf{u}} \mathbf{Ex}[\mathtt{I}_\mathsf{g}] \\ &= \sum_{\mathsf{g} \in \mathcal{G}_\mathsf{u}} \frac{r^{\underline{3}}}{N^{\underline{3}}} = |\mathcal{G}_\mathsf{u}| \times \frac{r^{\underline{3}}}{N^{\underline{3}}} = \frac{r^{\underline{3}}}{N}.\end{aligned}$$

Now, we compute the second part of the lemma which gives a bound on the variance of $\mathbf{N}_r^\mathsf{u}$. Since $\mathbf{N}_r^\mathsf{u}$ is sum of indicator random variables, we can write

$$\begin{aligned}\mathbf{Var}[\mathbf{N}_r^\mathsf{u}] &= \mathbf{Var}[\sum_{\mathsf{g} \in \mathcal{G}_\mathsf{u}} \mathtt{I}_\mathsf{g}] \\ &= \sum_{\mathsf{g} \in \mathcal{G}_\mathsf{u}} \mathbf{Var}[\mathtt{I}_\mathsf{g}] + \sum_{\mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_\mathsf{u}} \mathbf{Cov}(\mathtt{I}_\mathsf{g}, \mathtt{I}_{\mathsf{g}'}).\end{aligned}$$

For the sake of notational simplicity, we denote the set $\{\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2\}$ as $\mathcal{S}_\mathsf{u}^\mathsf{g}$ for every $\mathsf{g} \in \mathcal{G}_\mathsf{u}$. In (15), we have shown that $\mathbf{Ex}[\mathtt{I}_\mathsf{g}] = \frac{r^{\underline{3}}}{N^{\underline{3}}}$. As $\mathtt{I}_\mathsf{g}$ is a $0-1$ random variable, $\mathbf{Ex}[\mathtt{I}_\mathsf{g}^2] = \mathbf{Ex}[\mathtt{I}_\mathsf{g}]$. Thus,

$$\begin{aligned}\mathbf{Var}[\mathtt{I}_\mathsf{g}] &= \mathbf{Ex}[\mathtt{I}_\mathsf{g}^2] - \mathbf{Ex}[\mathtt{I}_\mathsf{g}]^2 \\ &= \mathbf{Ex}[\mathtt{I}_\mathsf{g}](1 - \mathbf{Ex}[\mathtt{I}_\mathsf{g}]) \\ &= \frac{r^{\underline{3}}}{N^{\underline{3}}} \times \left(1 - \frac{r^{\underline{3}}}{N^{\underline{3}}}\right).\end{aligned} \tag{16}$$

Therefore,

$$\begin{aligned}\sum_{\mathsf{g} \in \mathcal{G}_\mathsf{u}} \mathbf{Var}[\mathtt{I}_\mathsf{g}] &= |\mathcal{G}_\mathsf{u}| \times \frac{r^{\underline{3}}}{N^{\underline{3}}} \times \left(1 - \frac{r^{\underline{3}}}{N^{\underline{3}}}\right) \\ &\leq \frac{6r^2(r-1)(r-2)}{N^2} \text{ by employing Lemma } 1^8.\end{aligned} \tag{17}$$

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

$$\mathbf{Ex}[\mathtt{I}_\mathsf{g}\mathtt{I}_{\mathsf{g}'}] = \mathbf{Pr}[\mathcal{S}_\mathsf{u}^\mathsf{g} \cup \mathcal{S}_\mathsf{u}^{\mathsf{g}'} \subseteq \mathcal{V}_r] = \frac{r^{\underline{w}}}{N^{\underline{w}}},$$

where $w = |\mathcal{S}_\mathsf{u}^\mathsf{g} \cup \mathcal{S}_\mathsf{u}^{\mathsf{g}'}|$. Here, it is not difficult to see that the possible values taken by w are $3, 5$, and 6. Indeed, for $w = 4$ it is necessary to have $|\mathcal{S}_\mathsf{u}^\mathsf{g} \cap \mathcal{S}_\mathsf{u}^{\mathsf{g}'}| = 2$.

[8] Considering $r' \leq \frac{N}{4} < \frac{3N}{4} \leq r$, here we settle for a weaker bound which is sufficient for our purpose.

But this implies $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} = \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ (since any two elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ or $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ determines the third element), which violates the fact that $w = 4$.

Accordingly, we can partition the sum of covariances as follows.

$$\sum_{\mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_{\mathsf{u}}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}) = \sum_{w \in \{3,5,6\}} \sum_{\substack{\mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_{\mathsf{u}} \\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| = w}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}). \tag{18}$$

Now, we consider the three possible cases according to the value of w.

Case $w = 3$: In this case, we have

$$|\{(\mathsf{g}, \mathsf{g}') |\ \mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_{\mathsf{u}},\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| = 3\}| = 5(N-1)(N-2).$$

To arrive at the above expression note that the choice of $\mathsf{g} = (\mathsf{g}_1, \mathsf{g}_2)$ can be made in $(N-1)(N-2)$ ways (since $\mathsf{u} \notin \{\mathsf{g}_1, \mathsf{g}_2\}$). Now, after fixing g the potential number of ordered choices for $\mathsf{g}' = (\mathsf{g}_1', \mathsf{g}_2')$ from the elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ can be seen to be 6. Finally, from these 6 choices we discount the choice $(\mathsf{g}_1', \mathsf{g}_2') = (\mathsf{g}_1, \mathsf{g}_2)$.

Now, since $w = 3$, we have

$$\begin{aligned}
\mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}) &= \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}\mathtt{I}_{\mathsf{g}'}] - \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}]\mathbf{Ex}[\mathtt{I}_{\mathsf{g}'}] \\
&= \frac{r^{\underline{3}}}{N^{\underline{3}}} - \left(\frac{r^{\underline{3}}}{N^{\underline{3}}}\right)^2 \\
&= \frac{r^{\underline{3}}}{N^{\underline{3}}} \times \left(1 - \frac{r^{\underline{3}}}{N^{\underline{3}}}\right)
\end{aligned}$$

Therefore, similar to (17) we get

$$\sum_{\substack{\mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_{\mathsf{u}} \\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| = 3}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}) \leq \frac{30r^2(r-1)(r-2)}{N^2} \tag{19}$$

Case $w = 5$: Here, we have

$$|\{(\mathsf{g}, \mathsf{g}') |\ \mathsf{g} \neq \mathsf{g}' \in \mathcal{G}_{\mathsf{u}},\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| = 5\}| = 9(N-1)(N-2)(N-4).$$

To justify the above expression, observe that after fixing g in $(N-1)(N-2)$ ways the common element between the sets $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$and $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$can be determined in $3 \times 3 = 9$ ways (note that in this case we necessarily have $|\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cap \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| = 1$). Following this, one of the two remaining elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$can be chosen (from outside of the set $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \{\mathsf{u}\}$) in $N-4$ ways. This fixes g'.

Next, for $w = 5$ we have

$$\mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}) = \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}\mathtt{I}_{\mathsf{g}'}] - \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}]\mathbf{Ex}[\mathtt{I}_{\mathsf{g}'}] = \frac{r^{\underline{5}}}{N^{\underline{5}}} - \left(\frac{r^{\underline{3}}}{N^{\underline{3}}}\right)^2.$$

Therefore,

$$\sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}\\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=5}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}},\mathtt{I}_{\mathsf{g}'}) = 9(N-1)(N-2)(N-4)\left(\frac{r^{\underline{5}}}{N^{\underline{5}}}-\left(\frac{r^{\underline{3}}}{N^{\underline{3}}}\right)^2\right) \tag{20}$$

<u>Case $w=6$:</u> In this case, the sets $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$and $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$are necessarily disjoint. Ensuring this condition the choice of $\mathsf{g}_1,\mathsf{g}_2,\mathsf{g}_1'$ can be made (following similar argument as in the $w=5$ case) in $(N-1)(N-2)(N-4)$ ways. Now, letting $\mathcal{S}:=\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\{\mathsf{u},\mathsf{g}_1'\}$, it can be seen that the choice of g_2' should be made from outside of the set $\mathcal{S}\cup\{\mathsf{u}+\mathsf{g}_1'+\mathsf{s}|\mathsf{s}\in\mathcal{S}\}$ which has cardinality 8. Therefore, we have the following.

$$|\{(\mathsf{g},\mathsf{g}')|\ \mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}},\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=6\}| = (N-1)(N-2)(N-4)(N-8).$$

So, for $w=6$ we have

$$\sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}\\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=6}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}},\mathtt{I}_{\mathsf{g}'}) = (N-1)(N-2)(N-4)(N-8)\left(\frac{r^{\underline{6}}}{N^{\underline{6}}}-\left(\frac{r^{\underline{3}}}{N^{\underline{3}}}\right)^2\right) \tag{21}$$

Next, to express the upper bound on $\mathbf{Var}[\sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}}\mathtt{I}_{\mathsf{g}}]$ in terms of r' we consider the sum of (17) and (19) together and (20) and (21) together.

$$\begin{aligned} C\times(\sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}}\mathbf{Var}[\mathtt{I}_{\mathsf{g}}] + \sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}\\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=3}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}},\mathtt{I}_{\mathsf{g}'})) &\leq \frac{N}{(r^{\underline{3}})^2}\times\frac{36r^2(r-1)(r-2)}{N^2} \\ &= \frac{36}{N(r-1)(r-2)} \\ &\leq \frac{576}{N^3} \end{aligned} \tag{22}$$

The last inequality follows from $(r-2)\geq\frac{N}{4}$. Suppressing the simplification, we get

$$\begin{aligned} C\times(\sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}\\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=5}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}},\mathtt{I}_{\mathsf{g}'})) + \sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}\\ |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}\cup\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|=6}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}},\mathtt{I}_{\mathsf{g}'})) &\leq \frac{N}{(r^{\underline{3}})^2}\times(\frac{r^{\underline{3}}}{N^{\underline{3}}})\times\left(\frac{12N(r')^3}{(N-3)(N-5)}\right) \\ &\leq \frac{4^8(r')^3}{27N^6}. \end{aligned} \tag{23}$$

For the last inequality note that $(r-2)>\frac{N}{4}$ and $(N-5)>\frac{3N}{4}$ for $N\geq 32$. So, we have $r(r-1)(r-2)>(\frac{N}{4})^3$, and $(N-1)(N-2)(N-3)(N-5)>(\frac{3N}{4})^4$. Hence, the upper bound.

Therefore, finally we get

$$\begin{aligned}\mathbf{Ex}[\chi^2(X^{i-1})] &= C \times \sum_{u_i} \mathbf{Ex}[\left(\mathbf{N}_r^{u_i} - D\right)^2] \\ &= C \times \sum_{u_i} \mathbf{Var}[\mathbf{N}_r^{u_i}] \\ &= \sum_{u_i} C \times \mathbf{Var}[\mathbf{N}_r^{u_i}] \\ &\le \frac{576}{N^2} + \frac{4^8 (r')^3}{27 N^5}. \end{aligned} \tag{24}$$

■

4 An Efficient Variant of $\mathsf{XORP}[3]$

In this section, we consider an efficient version of $\mathsf{XORP}[3]$, which we term $\mathsf{XORP}'[3]$. Formally, given an n-bit random permutation RP and an input $x \in \{0,1\}^{n-3}$, the output of $\mathsf{XORP}'[3]$ is given by

$$\mathsf{RP}(x\|000) \oplus \mathsf{RP}(x\|001) \oplus \mathsf{RP}(x\|010) \;\|\; \mathsf{RP}(x\|000) \oplus \mathsf{RP}(x\|101) \oplus \mathsf{RP}(x\|110).$$

So, for $2n$-bit output $\mathsf{XORP}'[3]$ makes 5 calls to the underlying random permutation RP - a saving of one call compared to $\mathsf{XORP}[3]$.

In Theorem 3, which is our main result of this section, we bound the total variation between the probability distributions of the random vectors S and U defined over the same sample space $\mathcal{G}^{2q}$. The formal description of these random variables is given in Fig. 4.1. The random vector

$$\mathsf{U} := (\mathsf{U}_{1,1}, \mathsf{U}_{1,2}, \mathsf{U}_{2,1}, \mathsf{U}_{2,2}, \ldots, \mathsf{U}_{q,1}, \mathsf{U}_{q,2})$$

is a WR sample (represented as a vector) of size $2q$, each $\mathsf{U}_{i,j}$ is sampled from $\mathcal{G}$. Whereas,

$$\mathsf{S} := (\mathsf{S}_{1,1}, \mathsf{S}_{1,2}, \mathsf{S}_{2,1}, \mathsf{S}_{2,2}, \ldots, \mathsf{S}_{q,1}, \mathsf{S}_{q,2})$$

is generated (as described in Fig. 4.1) from a WOR sample

$$\mathsf{T} := (\mathsf{T}_{1,1}, \mathsf{T}_{1,2}, \ldots, \mathsf{T}_{1,5}, \mathsf{T}_{2,1}, \mathsf{T}_{2,2}, \ldots, \mathsf{T}_{2,5}, \ldots, \mathsf{T}_{q,1}, \mathsf{T}_{q,2}, \ldots, \mathsf{T}_{q,5})$$

of size $5q$, each $\mathsf{T}_{i,j}$ is sampled from $\mathcal{G}$. More precisely, $\mathsf{S}_{i,j} = \mathsf{T}_{i,1} + \mathsf{T}_{i,2j} + \mathsf{T}_{i,2j+1}$ for all $1 \le i \le q, 1 \le j \le 2$. So both U and S have the same sample space $\mathcal{G}^{2q}$.

Now, we state our main theorem which provides an upper bound on the total variation between U 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 3 (Pseudorandomness of S). *Let U and S be the random vectors as described in Fig. 4.1. Then, for all $q \le N/8$,*

$$\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| \le \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{\frac{3}{2}}}$$

Clearly, the PRF advantage of the above construction (when block cipher is replaced by a random permutation) is at most $\frac{5\sqrt{q}}{2^n} + \frac{256q}{2^{2n}} + \frac{8192q}{2^{\frac{3n}{2}}}$ for all $q \le 2^{n-3}$.

```
Random Experiment for $\mathsf{U}$
1 : $\mathsf{U} := (\mathsf{U}_{i,j} : i \in [q], j \in [2]) \xleftarrow{\text{wr}} \mathcal{G}$
2 : return $\mathsf{U}$
```

```
Random Experiment for $\mathsf{S}$
1 : $\mathsf{T} := (\mathsf{T}_{i,j} : i \in [q], j \in [5]) \xleftarrow{\text{wor}} \mathcal{G}$
2 : for $1 \leq i \leq q$
3 :     for $1 \leq j \leq 2$
4 :         $\mathsf{S}_{i,j} = \mathsf{T}_{i,1} + \mathsf{T}_{i,2j} + \mathsf{T}_{i,2j+1}$
5 : return $\mathsf{S} := (\mathsf{S}_{i,j} : i \in [q], j \in [2])$
```

Fig. 4.1: Description of sampling methods of random variables U, S.

4.1 Proof of Theorem 3

Proof will follow in a similar path as the proof of $\mathsf{XORP}[3]$. First, in Fig. 4.2, 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. By using similar argument as in Claim 1, which we do not present due to lack of space, we can show that the set $\mathcal{N}_i$ is always non-empty. Hence, execution of the part following **else** in line 5 of the Random Experiment for Y will never happen. It is kept only for the sake of the completeness of the definition.

```
Random Experiment for $\mathsf{X}$
1 : $\mathsf{T} = (\mathsf{T}_{i,j} : i \in [q], j \in [5]) \xleftarrow{\text{wor}} \mathcal{G}$
2 : for $1 \leq i \leq q$
3 :     for $1 \leq j \leq 2$
4 :         $\mathsf{S}_{i,j} = \mathsf{T}_{i,1} + \mathsf{T}_{i,2j} + \mathsf{T}_{i,2j+1}$
5 :         $\mathsf{X}_i = (\mathsf{S}_{i,1}, \mathsf{S}_{i,2}, \mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{T}_{i,4})$
6 :     $\mathsf{S}_i = (\mathsf{S}_{i,1}, \ldots, \mathsf{S}_{i,w})$
7 : return $\mathsf{X} := (\mathsf{X}_1, \ldots, \mathsf{X}_q)$
```

```
Random Experiment for $\mathsf{Y}$
1 : initialize $\mathcal{S}_0 = \mathcal{G}$
2 : for $1 \leq i \leq q$
3 :     $\mathsf{U}_i := (\mathsf{U}_{i,1}, \mathsf{U}_{i,2}) \xleftarrow{\$} \mathcal{G}$
4 :     $\mathcal{N}_i = \{(\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3) | \; \mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3,$
        $\mathsf{U}_{i,1} + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{U}_{i,2} + \mathsf{v}_1 + \mathsf{v}_3 \subseteq \mathcal{S}_{i-1},$
        and distinct$\}$
5 :     if $\mathcal{N}_i \neq \emptyset$ then $(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}) \xleftarrow{\$} \mathcal{N}_i$
        else $(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}) = (0, 0, 0)$
6 :     $\mathsf{Y}_i = (\mathsf{U}_{i,1}, \mathsf{U}_{i,2}, \mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3})$
7 :     $\mathcal{S}_i = \mathcal{S}_{i-1} \setminus \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3},$
        $\mathsf{U}_{i,1} + \mathsf{V}_{i,1} + \mathsf{V}_{i,2}, \mathsf{U}_{i,2} + \mathsf{V}_{i,1} + \mathsf{V}_{i,3}\}$
8 : return $\mathsf{Y} := (\mathsf{Y}_1, \ldots, \mathsf{Y}_q)$
```

Fig. 4.2: X and Y are extended random variables of S and U respectively.

Let $\mathcal{C} = \mathcal{G}^5$ denote the set of all 5-tuples of $\mathcal{G}$. To understand the probability distributions $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$ of the random vectors X and Y (respectively), and their supports we consider the following permutation ρ over the set $\mathcal{C}$ which maps the tuple $(\mathsf{x}_1, \ldots, \mathsf{x}_5)$ to $(\mathsf{x}_1+\mathsf{x}_2+\mathsf{x}_3, \mathsf{x}_1+\mathsf{x}_4+\mathsf{x}_5, \mathsf{x}_1, \mathsf{x}_2, \mathsf{x}_4)$. It is easy to see that ρ is a permutation and $\rho^{-1}(\mathsf{x}'_1, \mathsf{x}'_2, \ldots, \mathsf{x}'_5) = (\mathsf{x}'_3, \mathsf{x}'_4, \mathsf{x}'_1+\mathsf{x}'_3+\mathsf{x}'_4, \mathsf{x}'_5, \mathsf{x}'_2+\mathsf{x}'_3+\mathsf{x}'_5)$. We extend the definition of ρ over C^c for any c as $\rho^*(\mathsf{z}_1, \ldots, \mathsf{z}_c) = (\rho(\mathsf{z}_1), \ldots, \rho(\mathsf{z}_c))$. From the random experiments, it is trivial to see that

1. $\rho(\mathsf{X}_i) = \mathsf{T}_i := (\mathsf{T}_{i,1}, \ldots, \mathsf{T}_{i,5})$ and
2. $\rho(\mathsf{Y}_i) = \mathsf{V}_i := (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_{i,1} + \mathsf{V}_{i,1} + \mathsf{V}_{i,2}, \mathsf{V}_{i,3}, \mathsf{U}_{i,2} + \mathsf{V}_{i,1} + \mathsf{V}_{i,3})$.

So, for every $i \leq q$, $\rho^*(\mathsf{X}^i) = \mathsf{T}^i$ and $\rho^*(\mathsf{Y}^i) = \mathsf{V}^i$. In other words, the random variables X and Y are equivalent to T and $\mathsf{V} := (\mathsf{V}_{i,j}, i \in [q], j \in [5])$ respectively. In the first case, we first sample T and then define X by applying ρ^{-1} on each block. Whereas, in the second case, we first sample Y and then we define V by applying ρ on each block. So, for every i, the support of T^i is the set of all block-wise distinct tuples $(\mathsf{a}_{i',j} : i' \in [i], j \in [w])$. Hence, the support of X^i, denoted as Ω_i, would be the set of all such iw tuples

$$\Omega_i := \{(\mathsf{x}_{i',j} : i' \in [i], j \in [w]) \in \mathcal{G}^{iw} : (\mathsf{a}_{i',j} : i' \in [i], j \in [5]) \text{ is block-wise distinct}\},$$

where $\rho(\mathsf{x}_{i'}) = \mathsf{a}_{i'} := (\mathsf{a}_{i',j} : j \in [5])$ for all i'. In fact, for every $\mathsf{x}^i \in \Omega_i$, the conditional probability for X can be expressed as

$$\begin{aligned}\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\overset{\text{def}}{=} \Pr[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}^{i-1} = \mathsf{x}^{i-1}] \\ &= \Pr[\mathsf{T}_i = \mathsf{t}_i \mid \mathsf{T}^{i-1} = \mathsf{t}^{i-1}] \\ &= \frac{1}{(N - 5(i-1))^{\underline{5}}}. \end{aligned} \tag{25}$$

Now, we are going to argue that the support of Y^i contains Ω_i for all i. First, for all $(\mathsf{x}_1, \ldots, \mathsf{x}_i) \in \Omega_i$, let us denote $\mathsf{u}_i := (\mathsf{u}_{i,1}, \mathsf{u}_{i,2}) = (\mathsf{x}_{i,1}, \mathsf{x}_{i,2})$. Next, let $\mathsf{x}^i = (\mathsf{x}_1, \ldots, \mathsf{x}_i) \in \Omega_i$ be a fixed i-tuple of blocks with $\mathsf{x}_i = (\mathsf{u}_i, \mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5})$. As before, let $\rho(\mathsf{x}_{i'}) = \mathsf{t}_{i'}$ for every $i' \in [i]$. So, $\mathsf{t}_{i',j}$'s are distinct. Next, we define the following set

$$\begin{aligned}\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1}) := \{(\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3) : \mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3, \mathsf{u}_{i,1} + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{u}_{i,2} + \mathsf{v}_1 + \mathsf{v}_3 \in \mathcal{S}_{i-1} \text{ ,and} \\ \mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3, \mathsf{u}_{i,1} + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{u}_{i,2} + \mathsf{v}_1 + \mathsf{v}_3 \text{ distinct}\},\end{aligned}$$

where $\mathcal{S}_{i-1} = \mathcal{G} \setminus \{\mathsf{t}_{i',j} : i' < i, j \in [5]\}$. Given that $\mathsf{U}_i = \mathsf{u}_i$ and $\mathsf{Y}^{i-1} = \mathsf{x}^{i-1}$, the set $\mathcal{N}_i$ (defined in the line 4 of the random experiment of Y in Fig. 4.2) is exactly the same as the set $\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})$ defined above. It is easy to observe the following:

If $\mathsf{x}^i \in \Omega_i$ then the set $\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})$ is nonempty as $\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5} \in \mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})$,

and $\mathsf{x}^i \in \Omega_i$ is indeed in the support of Y^i. Now, we have the following claim on the support of Y.[9]

[9] As noted in the beginning of this proof, $\mathcal{N}_i$ can be shown to be non-empty by an argument similar to Claim 1.

Claim 3 *For all* $\mathsf{x}^i \in \Omega_i$,

$$\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) \overset{\text{def}}{=} \Pr[\mathsf{Y}_i = \mathsf{x}_i \mid \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] = \frac{1}{N^2} \times \frac{1}{|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|}.$$

Proof of claim. First, note that $\mathsf{x}^{i-1} \in \Omega_{i-1}$, and $\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})$ cannot be the empty set as $\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5} \in \mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})$. So,

$$\begin{aligned}\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\overset{\text{def}}{=} \Pr[\mathsf{Y}_i = \mathsf{x}_i \mid \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] \\ &= \Pr[\mathsf{U}_i = \mathsf{u}_i | \ \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] \times \Pr[(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}) = (\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5}) \mid \\ &\qquad \mathsf{U}_i = \mathsf{u}_i \wedge \mathsf{Y}^{i-1} = \mathsf{x}^{i-1}] \\ &= \frac{1}{N^2} \times \frac{1}{|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|}, \end{aligned} \tag{26}$$

where the last equality follows from the definition of sampling of U_i and $(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3})$ in the Random Experiment for Y (see Fig. 4.2). ■

We now apply the χ^2 method to X and Y.

$$\begin{aligned}\chi^2(\mathsf{x}^{i-1}) &:= \sum_{\mathsf{x}_i} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\mathsf{x}^{i-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\mathsf{x}^{i-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\mathsf{x}^{i-1})} \\ &=_{(a)} \sum_{\mathsf{x}_i = (\mathsf{u}_i, \mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5})} \frac{\left(\frac{1}{(N-5(i-1))^{\underline{5}}} - \frac{1}{N^2|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|}\right)^2}{\frac{1}{N^2|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|}} \\ &=_{(b)} C \times \sum_{\mathsf{u}_i} \sum_{(\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5})} \frac{\left(|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})| - D\right)^2}{|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|} \\ &=_{(c)} C \times \sum_{\mathsf{u}_i} \left(|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})| - D\right)^2, \end{aligned} \tag{27}$$

where $C = \frac{N^2}{((N-5(i-1))^{\underline{5}})^2}$, and $D = \frac{(N-5(i-1))^{\underline{5}}}{N^2}$. The equality (a) follows by plugging the conditional probabilities derived in (25) and (26). The expression on the r.h.s. of (b) is obtained by algebraic simplification. The equation (c) follows from the observation that $\frac{\left(|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})| - D\right)^2}{|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|}$ is functionally independent of $(\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5})$, and for each u_i, the number of choices of $(\mathsf{x}_{i,3}, \mathsf{x}_{i,4}, \mathsf{x}_{i,5})$ is $|\mathcal{N}^{\mathsf{u}_i}(\mathsf{x}^{i-1})|$. Next, in order to apply Theorem 1, we compute $\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]$ which (from (27)) is given by

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

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

For notational simplicity, let $r = N - 5(i-1)$ and $r' = N - r = 5(i-1)$. Also, let $\mathcal{V}_r = \mathcal{G} \setminus \{\mathsf{T}_{i',j} : i' \in [i-1], j \in [5]\}$ which is a random r-set in $\mathcal{G}$. Then the set $\mathcal{N}^{\mathsf{u}_i}(\mathsf{X}^{i-1})$ is same as the set

$$\{(\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3) : \mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3, \mathsf{u}_{i,1} + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{u}_{i,2} + \mathsf{v}_1 + \mathsf{v}_3 \in \mathcal{V}_r,$$
$$\mathsf{v}_1, \mathsf{v}_2, \mathsf{v}_3, \mathsf{u}_{i,1} + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{u}_{i,1} + \mathsf{v}_1 + \mathsf{v}_3 \text{ distinct}\}$$

We denote the size of the set by $\mathbf{N}_r^{\mathsf{u}_i}$. Then we have

$$\begin{aligned}
\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] &= C \times \sum_{\mathsf{u}_i} \mathbf{Ex}[\big(\mathbf{N}_r^{\mathsf{u}_i} - D\big)^2] \\
&= C \times \sum_{\mathsf{u}_i} \Big(\mathbf{Ex}[\big(\mathbf{N}_r^{\mathsf{u}_i} - \mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}_i}]\big)^2] + (\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}_i}] - D)^2\Big) \\
&= \sum_{\mathsf{u}_i} C \times \mathbf{Var}[\mathbf{N}_r^{\mathsf{u}_i}] + \sum_{\mathsf{u}_i} C \times (\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}_i}] - D)^2. \qquad (28)
\end{aligned}$$

Next, we apply the following lemma to get an upper bound on the r.h.s. of (28).

Lemma 3. *For every $\mathsf{u} \in \mathcal{G}^2$, we have*

$$C \times (\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}] - D)^2 \le \frac{25}{N^4},$$
$$C \times \mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}] \le \frac{2^{14} r'}{N^6} + \frac{2^{24} r'}{N^5} \textit{ for } N \ge 100.$$

Subsequently, when $N \ge 100$ and $r' \le \frac{5N}{8}$ we have

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \le \frac{2^{14} r'}{N^4} + \frac{2^{24} r'}{N^3} + \frac{25}{N^2}.$$

We defer the proof of the lemma to Section 4.2.

Finally, from Theorem 1 and Lemma 3, we get

$$\begin{aligned}
\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| &\le \|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\| \qquad (29) \\
&\le \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})]\right)^{\frac{1}{2}} \\
&\le \left(\sum_{i=1}^{q} \frac{25}{N^2} + \frac{4^7 r'}{N^4} + \frac{2^{24} r'}{N^3}\right)^{\frac{1}{2}} \text{ since } r' = 5(i-1) \le 5q \le 5N/8 \\
&\le \left(\sum_{i=1}^{q} \frac{25}{N^2} + \frac{4^7 5(i-1)}{N^4} + \frac{2^{24} 5(i-1)}{N^3}\right)^{\frac{1}{2}} \text{ since } r' = 5(i-1) \\
&\le \left(\frac{25q}{N^2} + \frac{4^8 q^2}{N^4} + \frac{2^{26} q^2}{N^3}\right)^{\frac{1}{2}} \\
&\le \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{\frac{3}{2}}} \text{ for } N \ge 100. \qquad (30)
\end{aligned}$$

■

4.2 Proof of Lemma 3

Let r, N be positive integers such that $r' = N - r \leq \frac{5N}{8}$. Let $\mathcal{G}$ be a group of size N, and $\mathcal{V}_r$ be a random r-set in $\mathcal{G}$. For $\mathsf{u} = (\mathsf{u}_1, \mathsf{u}_2) \in \mathcal{G}^2$ we associate a random variable $\mathbf{N}_r^{\mathsf{u}}$ defined as the size of the following set

$$\mathcal{N}_r^{\mathsf{u}} := \{(\mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3) \in \mathcal{G}^3 : \mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \in \mathcal{V}_r,\\ \mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \text{ distinct.}\}$$

We represent $\mathbf{N}_r^{\mathsf{u}}$ as a sum of indicator random variables. To do so we define the set $\mathcal{G}_{\mathsf{u}}$ of tuples of distinct elements of $\mathcal{G}$ as

$$\mathcal{G}_{\mathsf{u}} = \{(\mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3) : \mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \in \mathcal{G},\\ \mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \text{ distinct}\}.$$

Let $|\mathcal{G}_{\mathsf{u}}| = N_{\mathsf{u}}$. Then we have the following claim.

Claim 4 $N_{\mathsf{u}} \leq (N-1)(N-2)(N-3)$.

Proof of claim. It may be observed that for fixed u, $\mathsf{g}_1 \notin \{\mathsf{u}_1, \mathsf{u}_2\}$. Otherwise, either $\mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2 = \mathsf{g}_2$ or $\mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 = \mathsf{g}_3$ which contradicts the distinctness requirement. Discounting for the fact $\mathsf{u}_1, \mathsf{u}_2$ may be equal we get that the number of choices for g_1 is at most $(N-1)$. Similarly, we have that $\mathsf{g}_2 \notin \{\mathsf{u}_1, \mathsf{g}_1\}$ and $\mathsf{g}_3 \notin \{\mathsf{g}_1, \mathsf{g}_2, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2\}$. Hence, the claim follows. ■

Next, we have

$$\mathbf{N}_r^{\mathsf{u}} = \sum_{\mathsf{g} \in \mathcal{G}_{\mathsf{u}}} \mathtt{I}_{\mathsf{g}}, \tag{31}$$

where, for $\mathsf{g} = (\mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3) \in \mathcal{G}_{\mathsf{u}}$, the indicator random variable $\mathtt{I}_{\mathsf{g}}$ is defined as follows.

$$\mathtt{I}_{\mathsf{g}} = \begin{cases} 1 \text{ if } \mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \in \mathcal{V}_r \text{ and distinct,} \\ 0 \text{ otherwise.} \end{cases}$$

So, we have

$$\begin{aligned} \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}] &= \mathbf{Pr}[\{\mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3 \in \mathcal{V}_r\} \subseteq \mathcal{V}_r] \\ &= \frac{\binom{N-5}{r-5}}{\binom{N}{r}} \\ &= \frac{r^{\underline{5}}}{N^{\underline{5}}}. \end{aligned} \tag{32}$$

By using the linearity of expectation, we have

$$\begin{aligned}
\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}] &= \sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}} \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}] \\
&= \sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}} \frac{r^{\underline{5}}}{N^{\underline{5}}} \\
&\leq \frac{r^{\underline{5}}}{N(N-4)} \text{ using Claim 4.}
\end{aligned}$$

Therefore, plugging in the values of C and D we have

$$\begin{aligned}
C \times (\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}] - D)^2 &\leq \frac{N^2}{(r^{\underline{5}})^2} \times \left(\frac{r^{\underline{5}}}{N(N-4)} - \frac{r^{\underline{5}}}{N^2} \right)^2 \\
&\leq \frac{16}{N^2(N-4)^2} \\
&\leq \frac{25}{N^4} \text{ for } N \geq 20. \qquad (33)
\end{aligned}$$

Now, we compute the variance using the following relation.

$$\mathbf{Var}[\sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}} \mathtt{I}_{\mathsf{g}}] = \sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}} \mathbf{Var}[\mathtt{I}_{\mathsf{g}}] + \sum_{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_{\mathsf{u}}} \mathbf{Cov}(\mathtt{I}_{\mathsf{g}}, \mathtt{I}_{\mathsf{g}'}). \qquad (34)$$

For the sake of notational simplicity, for every $\mathsf{g} \in \mathcal{G}_{\mathsf{u}}$, we denote the set $\{\mathsf{g}_1, \mathsf{g}_2, \mathsf{g}_3, \mathsf{u}_1 + \mathsf{g}_1 + \mathsf{g}_2, \mathsf{u}_2 + \mathsf{g}_1 + \mathsf{g}_3\}$ as $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$. In (32), we have obtained $\mathbf{Ex}[\mathtt{I}_{\mathsf{g}}] = \frac{r^{\underline{5}}}{N^{\underline{5}}}$. As $\mathtt{I}_{\mathsf{g}}$ is a $0-1$ random variable, $\mathbf{Ex}[\mathtt{I}_{\mathsf{g}}^2] = \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}]$. Thus,

$$\begin{aligned}
\mathbf{Var}[\mathtt{I}_{\mathsf{g}}] &= \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}^2] - \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}]^2 \\
&= \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}](1 - \mathbf{Ex}[\mathtt{I}_{\mathsf{g}}]) \\
&= \frac{r^{\underline{5}}}{N^{\underline{5}}} \times \left(1 - \frac{r^{\underline{5}}}{N^{\underline{5}}}\right) \qquad (35) \\
&\leq \frac{r^{\underline{5}}}{N^{\underline{5}}} \times \frac{10r'}{N} \text{ using Lemma 1.} \qquad (36)
\end{aligned}$$

Therefore, by using the estimate of N_{u} from Claim 4 we get

$$\begin{aligned}
C \times \sum_{\mathsf{g}\in\mathcal{G}_{\mathsf{u}}} \mathbf{Var}[\mathtt{I}_{\mathsf{g}}] &= \frac{N^2}{(r^{\underline{5}})^2} \times N_{\mathsf{u}} \times \frac{r^{\underline{5}}}{N^{\underline{5}}} \times \frac{10r'}{N}. \\
&\leq \frac{2^{14} r'}{N^6} \text{ for } N \geq 16. \qquad (37)
\end{aligned}$$

Now, we compute the covariance term of (34). Note that $\mathtt{I}_{\mathsf{g}}\mathtt{I}_{\mathsf{g}'} = 1$ if and only if $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'} \subseteq \mathcal{V}_r$. So,

$$\mathbf{Ex}[\mathtt{I}_{\mathsf{g}}\mathtt{I}_{\mathsf{g}'}] = \mathbf{Pr}[\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'} \subseteq \mathcal{V}_r] = \frac{r^{\underline{\ell}}}{N^{\underline{\ell}}},$$

where $\ell = |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}|$. Here, it is not difficult to observe that $\ell \in \{5, 6, 7, 8, 9, 10\}$.

Accordingly, we can partition the sum of covariances as follows.

$$\begin{aligned}\sum_{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_\mathsf{u}}\mathbf{Cov}(\mathtt{I}_\mathsf{g},\mathtt{I}_{\mathsf{g}'}) &= \sum_{\ell\in\{5,6,7,8,9,10\}}\ \sum_{\substack{\mathsf{g}\neq\mathsf{g}'\in\mathcal{G}_\mathsf{u}\\ |\mathcal{S}_\mathsf{u}^\mathsf{g}\cup\mathcal{S}_\mathsf{u}^{\mathsf{g}'}|=\ell}}\mathbf{Cov}(\mathtt{I}_\mathsf{g},\mathtt{I}_{\mathsf{g}'})\\ &= \sum_{\ell\in\{5,6,7,8,9,10\}}\varDelta_\ell^\mathsf{u}\mathtt{COV}_\ell,\end{aligned}\tag{38}$$

where

$$\varDelta_\ell^\mathsf{u} = \ |\{(\mathsf{g},\mathsf{g}')\in\mathcal{G}_\mathsf{u}\times\mathcal{G}_\mathsf{u}|\mathsf{g}\neq\mathsf{g}',|\mathcal{S}_\mathsf{u}^\mathsf{g}\cup\mathcal{S}_\mathsf{u}^{\mathsf{g}'}|=\ell\}|,$$

and

$$\begin{aligned}\mathtt{COV}_\ell &= \frac{r^{\underline{\ell}}}{N^{\underline{\ell}}}-\left(\frac{r^{\underline{5}}}{N^{\underline{5}}}\right)^2\\ &= \left(\frac{r^{\underline{5}}}{N^{\underline{5}}}\right)\left(\frac{(r-5)\dots(r-\ell+1)}{(N-5)\dots(N-\ell+1)}-\frac{r^{\underline{5}}}{N^{\underline{5}}}\right)\\ &= \left(\frac{r^{\underline{5}}}{N^{\underline{5}}}\right)\times\varGamma_\ell,\end{aligned}$$

where $\varGamma_\ell = \left(\frac{(r-5)\dots(r-\ell+1)}{(N-5)\dots(N-\ell+1)}-\frac{r^{\underline{5}}}{N^{\underline{5}}}\right)$. Therefore,

$$\begin{aligned}C\times\mathtt{COV}_\ell &= \frac{N}{r^{\underline{5}}(N-1)^{\underline{4}}}\times\varGamma_\ell\\ &\leq \frac{1024}{N^8}\times\varGamma_\ell \quad\text{for } N\geq 16.\end{aligned}\tag{39}$$

Now, we estimate the order of magnitude of $\varDelta_\ell^\mathsf{u}$ and $\varGamma_\ell$ for different values of ℓ through the following claims.

Claim 5 *With the notations mentioned above we have the following upper bounds.*

1. $\varDelta_5^\mathsf{u}\leq 40N_\mathsf{u}$,
2. $\varDelta_6^\mathsf{u}\leq 600N_\mathsf{u}$,
3. $\varDelta_7^\mathsf{u}\leq 600NN_\mathsf{u}$,
4. $\varDelta_8^\mathsf{u}\leq 200NN_\mathsf{u}$,
5. $\varDelta_9^\mathsf{u}\leq 25N^2N_\mathsf{u}$,
6. $\varDelta_{10}^\mathsf{u}=(N^3-cN^2)N_\mathsf{u}$ *for some* c *with* $10\leq c\leq 36$ *and* $N\geq 15$.

Proof of claim. Below, we provide case by case justification of the above claim, although with significant compromise on the accuracy of the constants as our primary focus is on the order of magnitude of the considered variables. In each case, *i.e.* for $\ell\in\{5,6,7,8,9,10\}$, we fix some $\mathsf{g}\in\mathcal{G}_\mathsf{u}$ and consider the number of $\mathsf{g}'\in\mathcal{G}_\mathsf{u}$ for which $|\mathcal{S}_\mathsf{u}^\mathsf{g}\cap\mathcal{S}_\mathsf{u}^{\mathsf{g}'}|=\ell$, and then the final expression of $\varDelta_\ell^\mathsf{u}$ is obtained by multiplying with the cardinality (N_u) of $\mathcal{G}_\mathsf{u}$ (*i.e.*, the number of g). Here note that $\mathsf{u}=(\mathsf{u}_1,\mathsf{u}_2)$ is already fixed.

1. In this case, we have $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} = \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$. Now, with g fixed, $\mathsf{g}_1^{'}, \mathsf{g}_2^{'}$ can be fixed by the elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ in at most $5 \times 4 = 20$ ways. Not all such choices will be valid (because for some of them $\mathsf{g}_1^{'} + \mathsf{g}_2^{'} + \mathsf{u}_1 \notin \mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$). For each valid choice of $\mathsf{g}_1^{'}, \mathsf{g}_2^{'}$ there are at most 2 choices of $\mathsf{g}_3^{'}$ (indeed $\mathsf{g}_3^{'} \in \mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \setminus \{\mathsf{g}_1^{'}, \mathsf{g}_2^{'}, \mathsf{g}_1^{'} + \mathsf{g}_2^{'} + \mathsf{u}_1\}$). So, $\varDelta_5^{\mathsf{u}} \leq 40N_{\mathsf{u}}$.
2. In this case, 4 elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ can be chosen in 5 ways. These 4 elements can be assigned to the 4 elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ in at most $5 \times 4 \times 3 \times 2 = 120$ ways. This fixes the tuple g'. So, $\varDelta_6^{\mathsf{u}} \leq 120 \times 5 \times N_{\mathsf{u}} = 600N_{\mathsf{u}}$.
3. Here, 3 elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ can be chosen in 10 ways. The chosen elements can be assigned to 3 elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ in $5 \times 4 \times 3 = 60$ ways. Fixing any of the remaining 2 elements of $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ can be done in at most N ways. This fixes the tuple g'. So, we have $\varDelta_7^{\mathsf{u}} \leq 600NN_{\mathsf{u}}$.
4. Following an argument quite similar to the above, we get that $\varDelta_8^{\mathsf{u}} \leq 200NN_{\mathsf{u}}$.
5. In this case, the two sets $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ and $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ intersect in a single element. This can happen in 25 possible ways and fixing any two from $\{\mathsf{g}_1^{'}, \mathsf{g}_2^{'}, \mathsf{g}_3^{'}\} \setminus \mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ fixes the remaining one (among $\{\mathsf{g}_1^{'}, \mathsf{g}_2^{'}, \mathsf{g}_3^{'}\}$) if it is already not in $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$. Now, the two elements can be fixed in at most N^2 number of ways. So, the claim for this case is established.
6. In this case, the sets $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}}$ and $\mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}$ are disjoint. So, for fixed g the number of choices of $\mathsf{g}_i^{'}$ is $N - d_i$, for integers $d_i, 1 \leq i \leq 3$. Now, $d_1 = |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \{\mathsf{u}_1, \mathsf{u}_2\}|$. So, $5 \leq d_1 \leq 7$. Similarly, (conditioned on the choice of $\mathsf{g}_1^{'}$) we have that $d_2 = |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \{\mathsf{u}_1, \mathsf{g}_1^{'}\} \cup \mathsf{u}_1 + \mathsf{g}_1^{'} + \mathcal{S}_{\mathsf{u}}^{\mathsf{g}}|$. From this it follows that $5 \leq d_2 \leq 12$. Finally, following similar argument, and compromising on accuracy it follows that (conditioned on the choice of $\mathsf{g}_1^{'}$ and $\mathsf{g}_2^{'}$) $5 \leq d_3 \leq 17$. So, for this case, the possible number of choices of g' for fixed g is $(N - d_1)(N - d_2)(N - d_3)$ which is $(N^3 - cN^2)$ for some $10 \leq c \leq 36$ and $N \geq 15$. ■

Claim 6

$$\varGamma_\ell \leq \frac{10r'}{N}$$

for $\ell \in \{5, 6, 7, 8\}$

Proof of claim. This (weaker) bound follows from Lemma 1. ■

Claim 7

$$\varDelta_9^{\mathsf{u}}\varGamma_9 + \varDelta_{10}^{\mathsf{u}}\varGamma_{10} \leq 720r'N^3,$$

for $N \geq 100$

Proof of claim. Here we use the estimates of $\varDelta_9^{\mathsf{u}}$ and $\varDelta_{10}^{\mathsf{u}}$ from Claim 5 with $N_{\mathsf{u}} \leq N^3$. Also, we suppress the tedious calculation (verified using symbolic algebra package) and get the final upper bound $720r'N^3$ for $N \geq 100$. ■

Next, using the estimates form Claim 5, Claim 6, and Claim 7 together with (39) and $N_{\mathsf{u}} \leq N^3$ we get the following upper bound on the r.h.s. of (38).

$$
\begin{aligned}
C \times \sum_{\mathtt{g} \neq \mathtt{g}' \in \mathcal{G}_{\mathsf{u}}} \mathbf{Cov}(\mathtt{I}_{\mathtt{g}}, \mathtt{I}_{\mathtt{g}'}) &= C \times \sum_{\ell \in \{5,6,7,8,9,10\}} \mathit{\Delta}^{\mathsf{u}}_{\ell} \mathtt{COV}_{\ell} \\
&\leq \frac{1024}{N^8} \times \sum_{\ell \in \{5,6,7,8,9,10\}} \mathit{\Delta}^{\mathsf{u}}_{\ell} \mathit{\Gamma}_{\ell} \\
&\leq \frac{1024}{N^8} \times \left(640N^3 \times \frac{10r'}{N} + 800N^4 \times \frac{10r'}{N} + 720r'N^3 \right) \\
&\leq \frac{1024}{N^8} \times (6400r'N^2 + 8000r'N^3 + 720r'N^3) \\
&\leq \frac{2^{24}r'}{N^5} \text{ for } N \geq 100. \qquad (40)
\end{aligned}
$$

Finally, using (33),(37), and (40) the r.h.s. of (28) yields

$$
\begin{aligned}
\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] &\leq \sum_{\mathsf{u}} \frac{25}{N^4} + \frac{2^{14}r'}{N^6} + \frac{2^{24}r'}{N^5} \\
&= \frac{25}{N^2} + \frac{2^{14}r'}{N^4} + \frac{2^{24}r'}{N^3} \text{ for } N \geq 100. \qquad (41)
\end{aligned}
$$

■

5 Conclusion

In this paper, we have demonstrated much stronger PRF security gurarantee of a block cipher based PRF construction termed XORP[3] in the multi-user and single-user setting. With the choice of a sufficiently secure block cipher, the construction allows simultaneous (independent) use by $O(2^n)$ users even when the adversary makes almost $O(2^n)$ many queries to each user. In the single-user scenario our result implies $O\left(1/\sqrt{2^n}\right)$, *i.e.,* negligible distinguishing advantage for an adversary even allowing it to make almost $O(2^n)$ many queries. We have also considered an efficient version of XORP[3], termed XORP′[3] which uses less number of block cipher calls but achieves same level of security. We have also shown an application of our result to counter mode encryption. In the end, we invite the reader to investigate whether the variant XORP′[3] can be further extended to achieve still better security/ efficiency.

Acknowledgement. We are indebted to all the reviewers, Dr. Akinori Hosoyamada, and Mr. Abishanka Saha for carefully going through the manuscript, pointing out technical and editorial issues, and suggesting modifications leading to the final version.

The research was supported by the project "Study and Analysis of IoT Security" under Government of India at R.C.Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata.

References

BBM00. M. Bellare, A. Boldyreva and S. Micali, Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements, in *Advances in Cryptology - EUROCRYPT 2000*, edited by B. Preneel, volume 1807 of *LNCS*, pages 259–274, Springer, 2000.

BGK99. M. Bellare, O. Goldreich and H. Krawczyk, Stateless Evaluation of Pseudorandom Functions: Security beyond the Birthday Barrier, in *Advances in Cryptology - CRYPTO '99*, edited by M. J. Wiener, volume 1666 of *LNCS*, pages 270–287, Springer, 1999.

BHT18. P. Bose, V. T. Hoang and S. Tessaro, Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds, in *Advances in Cryptology - EUROCRYPT 2018*, edited by J. B. Nielsen and V. Rijmen, volume 10820 of *LNCS*, pages 468–499, Springer, 2018.

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, Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the χ^2-Method, in *Advances in Cryptology – EUROCRYPT 2018*, edited by J. B. Nielsen and V. Rijmen, pages 387–412, Cham, 2018, Springer International Publishing.

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 (Sep 2018).

BN18c. S. Bhattacharya and M. Nandi, *Revisiting Variable Output Length XOR Pseudorandom Function*, IACR Transactions on Symmetric Cryptology **2018**(1), 314–335 (2018).

BT16. M. Bellare and B. Tackmann, The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3, in *Advances in Cryptology - CRYPTO 2016*, edited by M. Robshaw and J. Katz, volume 9814 of *LNCS*, pages 247–276, Springer, 2016.

CLL19. W. Choi, B. Lee and J. Lee, Indifferentiability of Truncated Random Permutations, in *Advances in Cryptology - ASIACRYPT 2019*, edited by S. D. Galbraith and S. Moriai, volume 11921 of *LNCS*, pages 175–195, 2019.

CLP14. B. Cogliati, R. Lampe and J. Patarin, The Indistinguishability of the XOR of k Permutations, in *FSE 2014*, edited by C. Cid and C. Rechberger, volume 8540 of *LNCS*, pages 285–302, Springer, 2014.

Cog18. B. Cogliati, *Tweaking a block cipher: multi-user beyond-birthday-bound security in the standard model*, Designs, Codes and Cryptography **86**(12), 2747–2763 (2018).

DHT17. W. Dai, V. T. Hoang and S. Tessaro, Information-Theoretic Indistinguishability via the Chi-Squared Method, in *Advances in Cryptology - CRYPTO 2017*, edited by J. Katz and H. Shacham, volume 10403 of *LNCS*, pages 497–523, Springer, 2017.

GM20. A. Gunsing and B. Mennink, The Summation-Truncation Hybrid: Reusing Discarded Bits for Free, in *Advances in Cryptology - CRYPTO 2020*, edited by D. Micciancio and T. Ristenpart, volume 12170 of *LNCS*, pages 187–217, Springer, 2020.

HS20. V. T. Hoang and Y. Shen, Security of Streaming Encryption in Google's Tink Library, in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 243–262, 2020.

HT17. V. T. Hoang and S. Tessaro, The Multi-user Security of Double Encryption, in *Advances in Cryptology - EUROCRYPT 2017*, edited by J. Coron and J. B. Nielsen, volume 10211 of *LNCS*, pages 381–411, 2017.

HTT18. V. T. Hoang, S. Tessaro and A. Thiruvengadam, The Multi-user Security of GCM, Revisited: Tight Bounds for Nonce Randomization, in *CCS 2018*, pages 1429–1440, ACM, 2018.

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 *FSE 2006*, edited by M. J. B. Robshaw, volume 4047 of *LNCS*, pages 310–327, Springer, 2006.

LR88. M. Luby and C. Rackoff, *How to construct pseudorandom permutations from pseudorandom functions*, SIAM Journal on Computing **17**(2), 373–386 (1988).

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

Men19. B. Mennink, Linking Stam's Bounds with Generalized Truncation, in *Topics in Cryptology - CT-RSA 2019*, edited by M. Matsui, volume 11405 of *LNCS*, pages 313–329, Springer, 2019.

ML15. N. Mouha and A. Luykx, Multi-key Security: The Even-Mansour Construction Revisited, in *Advances in Cryptology - CRYPTO 2015*, edited by R. Gennaro and M. Robshaw, volume 9215 of *LNCS*, pages 209–223, Springer, 2015.

MP15. B. Mennink and B. Preneel, On the XOR of multiple random permutations, in *International Conference on Applied Cryptography and Network Security*, pages 619–634, Springer, 2015.

Pat08. 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`.

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