Luby-Rackoff Backwards with More Users and More Security

Srimanta Bhattacharya\textsuperscript{1} Mridul Nandi\textsuperscript{2}

\textsuperscript{1} SIAS, Krea University
\textsuperscript{2} Indian Statistical Institute, Kolkata

December 1, 2021
1 Motivation: PRF and Its Multi-user Security

2 Technical Background and Our Results (Statements)

3 Multi-user PRF-Security of XORP[3]: Proof Outline

4 References
Presentation Outline

1 Motivation: PRF and Its Multi-user Security

2 Technical Background and Our Results (Statements)

3 Multi-user PRF-Security of XORP[3]: Proof Outline

4 References
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.

Can we use them as PRFs?
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.

Can we use them as PRFs?

\( n \)-bit PRF can be distinguished from \( n \)-bit PRP with \( O(2^{n/2}) \) queries.
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.

Can we use them as PRFs? Birthday Bound

$n$-bit PRF can be distinguished from $n$-bit PRP with $O(2^{n/2})$ queries.
**Pseudorandom function** (PRF): Important cryptographic primitive.

*Encryption, Authentication, …*

How do we get them?

Good block ciphers (*pseudorandom permutations* (PRPs)) are available.

Can we use them as PRFs? *Birthday Bound*

\(n\)-bit PRF can be distinguished from \(n\)-bit PRP with \(O(2^{\frac{n}{2}})\) queries.

Can we go past the birthday barrier?
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, …

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.

Can we use them as PRFs? Birthday Bound

$n$-bit PRF can be distinguished from $n$-bit PRP with $O(2^{n/2})$ queries.

Can we go past the birthday barrier?

PRP to PRF Conversion: [Bellare et al., 1998] Luby-Rackoff backwards.
Pseudorandom function (PRF): Important cryptographic primitive.

Encryption, Authentication, ...

How do we get them?

Good block ciphers (pseudorandom permutations (PRPs)) are available.

Can we use them as PRFs? *Birthday Bound*

$n$-bit PRF can be distinguished from $n$-bit PRP with $O(2^{n/2})$ queries.

Can we go past the birthday barrier?

**PRP to PRF Conversion:** [Bellare et al., 1998] Luby-Rackoff backwards.

[Luby and Rackoff, 1988]: PRF to PRP
Construction: Sum of Permutations

Setting

RP: Random permutation on $\{0, 1\}^n$
Setting

RP: Random permutation on \(\{0, 1\}^n\)

Constructions

\[
\text{XORP}(x) = \text{RP}(0\|x) \oplus \text{RP}(1\|x).
\]
Setting
RP: Random permutation on \(\{0, 1\}^n\)

Constructions
\[\text{XORP} : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^n\]
\[\text{XORP}(x) = \text{RP}(0\|x) \oplus \text{RP}(1\|x).\]
Setting

RP: Random permutation on \( \{0, 1\}^n \)

Constructions

\[
\text{XORP : } \{0, 1\}^{n-1} \rightarrow \{0, 1\}^n \\
\text{XORP}(x) = \text{RP}(0\|x) \oplus \text{RP}(1\|x).
\]

[Bellare and Impagliazzo, 1999, Cogliati et al., 2014, Patarin, 2010, Patarin, 2008, Dai et al., 2017]: XORP is secure up to \( O(2^n) \) queries
**Construction: Sum of Permutations**

### Setting

**RP:** Random permutation on \( \{0, 1\}^n \)

### Constructions

\[
\text{XORP} : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^n
\]

\[
\text{XORP}(x) = \text{RP}(0||x) \oplus \text{RP}(1||x).
\]


### Generalizations

\[
\text{XORP}[3](x) = \text{RP}(x||00) \oplus \text{RP}(x||01) \oplus \text{RP}(x||10)
\]
**Setting**

RP: Random permutation on $\{0, 1\}^n$

**Constructions**

$\text{XORP}: \{0, 1\}^{n-1} \rightarrow \{0, 1\}^n$

$\text{XORP}(x) = \text{RP}(0|x) \oplus \text{RP}(1|x)$.

[Bellare and Impagliazzo, 1999, Cogliati et al., 2014, Patarin, 2010, Patarin, 2008, Dai et al., 2017]: XORP is secure up to $O(2^n)$ queries

**Generalizations**

$\text{XORP}[3]: \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n$

$\text{XORP}[3](x) = \text{RP}(x|00) \oplus \text{RP}(x|01) \oplus \text{RP}(x|10)$
**Construction: Sum of Permutations**

**Setting**

RP: Random permutation on \(\{0, 1\}^n\)

**Constructions**

\[
\text{XORP} : \{0, 1\}^{n-1} \rightarrow \{0, 1\}^n
\]

\[
\text{XORP}(x) = \text{RP}(0\|x) \oplus \text{RP}(1\|x).
\]

[Bellare and Impagliazzo, 1999, Cogliati et al., 2014, Patarin, 2010, Patarin, 2008, Dai et al., 2017]: XORP is secure up to \(O(2^n)\) queries

**Generalizations**

\[
\text{XORP}[3] : \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n
\]

\[
\text{XORP}[3](x) = \text{RP}(x\|00) \oplus \text{RP}(x\|01) \oplus \text{RP}(x\|10)
\]

[Lucks, 2000, Mennink and Preneel, 2015]: Security same as XORP \(\Rightarrow\) Secure up to \(O(2^n)\) queries
Sum of Permutations (Contd.)

\[ \text{XORP}'[3](x) = \text{RP}(x || 000) \oplus \text{RP}(x || 001) \oplus \text{RP}(x || 010) \oplus \text{RP}(x || 000) \oplus \text{RP}(x || 101) \oplus \text{RP}(x || 110) \]
Sum of Permutations (Contd.)

\[ \text{XORP'[3]}(x) = \text{RP}(x||000) \oplus \text{RP}(x||001) \oplus \text{RP}(x||010) \parallel \text{RP}(x||000) \oplus \text{RP}(x||101) \oplus \text{RP}(x||110) \]

XORP'[3] : \{0, 1\}^{n-3} \rightarrow \{0, 1\}^n
Efficient than XORP[3] - requires 5 block cipher calls for $2n$-bit output
\textbf{Sum of Permutations (Contd.)}

\[
\text{XORP}'[3](x) = \text{RP}(x\|000) \oplus \text{RP}(x\|001) \oplus \text{RP}(x\|010) \parallel \text{RP}(x\|000) \oplus \text{RP}(x\|101) \oplus \text{RP}(x\|110)
\]

- Efficient than \text{XORP}[3] - requires 5 block cipher calls for $2n$-bit output
XORP[3]': $\{0, 1\}^{n-3} \rightarrow \{0, 1\}^n$

$\text{XORP}'[3](x) = \text{RP}(x\|000) \oplus \text{RP}(x\|001) \oplus \text{RP}(x\|010) \parallel \text{RP}(x\|000) \oplus \text{RP}(x\|101) \oplus \text{RP}(x\|110)$

Efficient than XORP[3] - requires 5 block cipher calls for $2n$-bit output

[Patarin, 2010, Cogliati et al., 2014, Bhattacharya and Nandi, 2018b]: Secure up to $O(2^n)$ queries
XORP\([3]' : \{0, 1\}^{n-3} \rightarrow \{0, 1\}^n\]

\[
\text{XORP}'[3](x) = \text{RP}(x\|000) \oplus \text{RP}(x\|001) \oplus \text{RP}(x\|010) \oplus \text{RP}(x\|000) \oplus \text{RP}(x\|101) \oplus \text{RP}(x\|110)
\]

Efficient than XORP\([3]\) - requires 5 block cipher calls for \(2n\)-bit output

[Patarin, 2010, Cogliati et al., 2014, Bhattacharya and Nandi, 2018b]: Secure up to \(O(2^n)\) queries

Can be generalized to XORP\([k]\) and XORP\('[k]\) (XORP = XORP\([2]\)).
Sum of Permutations (Contd.)

\[ \text{XORP}'[3](x) = \text{RP}(x||000) \oplus \text{RP}(x||001) \oplus \text{RP}(x||010) \parallel \text{RP}(x||000) \oplus \text{RP}(x||101) \oplus \text{RP}(x||110) \]

- Efficient than XORP[3] - requires 5 block cipher calls for \(2^n\)-bit output

[Pa\text{tarin}, 2010, Cogliati et al., 2014, Bhattacharya and Nandi, 2018b]: Secure up to \(O(2^n)\) queries

Can be generalized to XORP\([k]\) and XORP\('[k]\) (XORP = XORP[2]).

Our focus \(k = 3\).

Application

CENC [Iwata, 2006, Bhattacharya and Nandi, 2018b], PMAC_Plus [Yasuda, 2011], ZMAC [Iwata et al., 2017].
Multi-user PRF-Security of XORP[$k$]: A Concern

XORP[$k$], XORP[$k$], ..., XORP[$k$], XORP[$k$]

independent
Multi-user PRF-Security of XORP[^k]: A Concern

XORP[^k], XORP[^k],…, XORP[^k], XORP[^k]

independent
Multi-user PRF-Security of XORP[\(k\)]: A Concern

- XORP[\(k\)], XORP[\(k\)], ..., XORP[\(k\)], XORP[\(k\)]

independent
Multi-user PRF-Security of XORP[$k$]: A Concern

$u$ users

$Q_{max}$ queries per user

$\text{XORP}[k], \text{XORP}[k], \ldots, \text{XORP}[k], \text{XORP}[k]$ independent

(ABy hybrid reduction) Secure up to $u \sim O(2^n^2)$ and $Q_{max} \sim O(2^n^2)$

AES: Secure for $uq_{max} < O(2^{96})$ (for an advantage $1/2^{32}$)

Scale and growth of internet and other technologies is a concern
Multi-user PRF-Security of XORP\([k]\): A Concern

\[ u \text{ users} \]

\[ q_{max} \text{ queries per user} \]

(By hybrid reduction) Secure up to \( u \sim O(2^{\frac{n}{2}}) \) and \( q_{max} \sim O(2^{\frac{n}{2}}) \)
Multi-user PRF-Security of XORP[^k^]: A Concern

\(u\) users

\(q_{max}\) queries per user

(By hybrid reduction) Secure up to \(u \sim O\left(2^{\frac{n}{2}}\right)\) and \(q_{max} \sim O\left(2^{\frac{n}{2}}\right)\)

AES: Secure for \(uq_{max} < O\left(2^{96}\right)\) (for an advantage \(\frac{1}{2^{32}}\))
Multi-user PRF-Security of XORP[κ]: A Concern

\[ \text{XORP}[k], \text{XORP}[k], \ldots, \text{XORP}[k], \text{XORP}[k] \]

\( u \) users

\( q_{\text{max}} \) queries per user

(By hybrid reduction) Secure up to \( u \sim O(2^{n/2}) \) and \( q_{\text{max}} \sim O(2^{n/2}) \)

AES: Secure for \( uq_{\text{max}} < O(2^{96}) \) (for an advantage \( \frac{1}{2^{32}} \))

Scale and growth of internet and other technologies is a concern
Multi-user PRF-Security of XORP\([k]\): A Concern

\(u\) users

\(q_{\text{max}}\) queries per user

(By hybrid reduction) Secure up to \(u \sim O(2^{\frac{n}{2}})\) and \(q_{\text{max}} \sim O(2^{\frac{n}{2}})\)

AES: Secure for \(u q_{\text{max}} < O(2^{96})\) (for an advantage \(\frac{1}{2^{32}}\))

Scale and growth of internet and other technologies is a concern

Possible fix: Increase the block length of the cipher

Block ciphers like AES come with fixed block length
Our Contribution (Informal)

- XORP[3] is secure up to $u \sim O(2^n)$ and $q_{max} \sim O(2^n)$
Our Contribution (Informal)

- XORP\([3]\) is secure up to \(u \sim O(2^n)\) and \(q_{\text{max}} \sim O(2^n)\)
  - Substantial improvement over \(u \sim O(2^{\frac{n}{2}})\) and \(q_{\text{max}} \sim O(2^{\frac{n}{2}})\)
Our Contribution (Informal)

- XORP[3] is secure up to $u \sim O(2^n)$ and $q_{max} \sim O(2^n)$
  - Substantial improvement over $u \sim O(2^\frac{n}{2})$ and $q_{max} \sim O(2^\frac{n}{2})$
- Single-user XORP[3]: Adversary’s advantage is negligible even after $O(2^n)$ queries
Our Contribution (Informal)

- XORP[3] is secure up to $u \sim O(2^n)$ and $q_{max} \sim O(2^n)$
  - Substantial improvement over $u \sim O(2^{\frac{n}{2}})$ and $q_{max} \sim O(2^{\frac{n}{2}})$
- Single-user XORP[3]: Adversary’s advantage is negligible even after $O(2^n)$ queries
  - Seems novel in the literature
Our Contribution (Informal)

- XORP[3] is secure up to $u \sim O(2^n)$ and $q_{\text{max}} \sim O(2^n)$
  - Substantial improvement over $u \sim O(2^{\frac{n}{2}})$ and $q_{\text{max}} \sim O(2^{\frac{n}{2}})$

- Single-user XORP[3]: Adversary’s advantage is negligible even after $O(2^n)$ queries
  - Seems novel in the literature

- XORP'[3] provides same level of security
1 Motivation: PRF and Its Multi-user Security

2 Technical Background and Our Results (Statements)

3 Multi-user PRF-Security of XORP[3]: Proof Outline

4 References
Security Notion: Indistinguishability

Setting

$\text{Func}_n$: All functions from $\{0, 1\}^{n-2}$ to $\{0, 1\}^n$.
$\text{Perm}_n$: All permutations from $\{0, 1\}^n$ to $\{0, 1\}^n$. 
Security Notion: Indistinguishability

**Setting**

$\text{Func}_n$: All functions from $\{0, 1\}^{n-2}$ to $\{0, 1\}^n$.

$\text{Perm}_n$: All permutations from $\{0, 1\}^n$ to $\{0, 1\}^n$.

**Security Game**

\[ \text{XORP}[3]: \text{RP} \leftarrow \text{Perm}_n \]

\[ \text{RF}: \text{RF} \leftarrow \text{Func}_n \]
**Security Notion: Indistinguishability**

**Setting**

Func$_n$: All functions from $\{0, 1\}^{n-2}$ to $\{0, 1\}^n$.

Perm$_n$: All permutations from $\{0, 1\}^n$ to $\{0, 1\}^n$.

**Security Game**

Security Game XORP$[3]$: RP $\leftarrow$ Perm$_n$

Reply: $P = \text{XORP}[3](x)$

Query: $x \in \{0, 1\}^{n-2}$

RF : RF $\leftarrow$ Func$_n$

Reply: $R \leftarrow \{0, 1\}^n$
Security Notion: Indistinguishability

Setting

Func$_n$: All functions from $\{0, 1\}^{n-2}$ to $\{0, 1\}^n$.
Perm$_n$: All permutations from $\{0, 1\}^n$ to $\{0, 1\}^n$.

Security Game

$XORP[3]: \text{RP} \leftarrow \$ \text{Perm}_n$

Reply: $P = XORP[3](x)$

$RF: \text{RF} \leftarrow \$ \text{Func}_n$

Reply: $R \leftarrow \$ \{0, 1\}^n$

Query: $x \in \{0, 1\}^{n-2}$

$A$

$b \in \{0, 1\}$
**Security Notion: Indistinguishability**

**Setting**

\( \text{Func}_n \): All functions from \( \{0, 1\}^{n-2} \) to \( \{0, 1\}^n \).

\( \text{Perm}_n \): All permutations from \( \{0, 1\}^n \) to \( \{0, 1\}^n \).

**Security Game**

\[ \text{XORP}[3] : \text{RP} \leftarrow \$ \text{Perm}_n \]

Reply: \( P = \text{XORP}[3](x) \)

Query: \( x \in \{0, 1\}^{n-2} \)

\[ \text{RF} : \text{RF} \leftarrow \$ \text{Func}_n \]

Reply: \( R \leftarrow \{0, 1\}^n \)

\( \mathcal{A} \)

\( b \in \{0, 1\} \)

**Quantifying Security: Advantage**

\[ \text{Adv}^{\text{prf}}_{\text{XORP}[3]}(\mathcal{A}) := |\Pr[\mathcal{A}^{\text{XORP}[3]} \rightarrow 1] - \Pr[\mathcal{A}^{\text{RF}} \rightarrow 1]| \]
Focus on information theoretic security of XORP[3].

- $\mathcal{A}$ computationally unbounded $\Rightarrow$ $\mathcal{A}$ is deterministic (runs with best coins)

Restrict $\mathcal{A}$ to $q$ queries.

- W.l.o.g. $\mathcal{A}$ does not repeat queries.
Focus on information theoretic security of XORP[3].

- $\mathcal{A}$ computationally unbounded $\Rightarrow$ $\mathcal{A}$ is deterministic (runs with best coins)

Restrict $\mathcal{A}$ to $q$ queries.

- W.l.o.g. $\mathcal{A}$ does not repeat queries.

XORP[3] transcript $P := (P_1, P_2, \ldots, P_q)$; RF transcript $R := (R_1, R_2, \ldots, R_q)$

$$Adv_{XORP[3]}^{\text{prf}}(\mathcal{A}) \leq \| \Pr_P - \Pr_R \|$$
Security Notion: Multi-user Indistinguishability

Setting

\[ \text{Func}^u_n := \{ f \mid f : [u] \times \{0, 1\}^{n-2} \mapsto \{0, 1\}^n \}, \text{RF} \leftarrow \text{Func}^u_n \]

\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow \text{Perm}_n \]
**Security Notion: Multi-user Indistinguishability**

### Setting

\[ \text{Func}_n^u := \{ f | f : [u] \times \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n \}, \ RF \leftarrow \text{Func}_n^u \]

\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow \text{Perm}_n \]

### Security Game

A diagram illustrating the security game with nodes labeled:

- XORP[3]^u
- RF
- A

The diagram shows the interaction between these nodes, with arrows indicating the flow of the game.
Security Notion: Multi-user Indistinguishability

**Setting**

\[ \text{Func}^u_n := \{ f \mid f : [u] \times \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n \}, \ RF \leftarrow \text{Func}^u_n \]

\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow \text{Perm}_n \]

**Security Game**

\[ = \text{RP}_i(x||00) \oplus \text{RP}_i(x||01) \oplus \text{RP}_i(x||10) \]

\[ \text{Query: } (i, x) \in [u] \times \{0, 1\}^{n-2} \]

\[ \text{Reply: } P = \text{XORP}_{\text{RP}_i[3]}(x) \]

\[ \text{Reply: } R \leftarrow \{0, 1\}^n \]
**Security Notion: Multi-user Indistinguishability**

**Setting**

\[ \text{Func}_n^u := \{ f | f : [u] \times \{0, 1\}^{n-2} \mapsto \{0, 1\}^n \}, \text{RF} \leftarrow $ Func_n^u \]

\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow $ \text{Perm}_n \]

**Security Game**

\[ = \text{RP}_i(x||00) \oplus \text{RP}_i(x||01) \oplus \text{RP}_i(x||10) \]

Query: \((i, x) \in [u] \times \{0, 1\}^{n-2}\)

Reply: \(P = \text{XORP}_{\text{RP}_i}[3](x)\)

Reply: \(R \leftarrow \{0, 1\}^n\)
Setting

\[ \text{Func}_n^u := \{ f \mid f : [u] \times \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n \}, \text{RF} \leftarrow \text{Func}_n^u \]

\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow \text{Perm}_n \]

Security Game

Query: \( (i, x) \in [u] \times \{0, 1\}^{n-2} \)

Reply: \( P = \text{XORP}_{\text{RP}_i}[3](x) \)

Reply: \( R \leftarrow \{0, 1\}^n \)

\[ = \text{RP}_i(x\|00) \oplus \text{RP}_i(x\|01) \oplus \text{RP}_i(x\|10) \]

\[ \text{Adv}_{\text{mu}_{\text{prf}}}^{XORP[3]^u}(\mathcal{A}) := |\Pr[\mathcal{A} \text{ XORP}[3]^u \rightarrow 1] - \Pr[\mathcal{A} \text{ RF} \rightarrow 1]| \]
Security Notion: Multi-user Indistinguishability

Setting

\[ \text{Func}_n^u := \{ f \mid f : [u] \times \{0, 1\}^{n-2} \rightarrow \{0, 1\}^n \}, \text{RF} \leftarrow \$ \text{Func}_n^u \]
\[ \text{RP}_1, \text{RP}_2, \ldots, \text{RP}_u \leftarrow \$ \text{Perm}_n \]

Security Game

\[ = \text{RP}_i(x||00) \oplus \text{RP}_i(x||01) \oplus \text{RP}_i(x||10) \]

Quantifying Security: Advantage

\[ \text{Adv}^{\text{mu-prf}}_{\text{XORP}[3]}(\mathcal{A}) := |\text{Pr}[\mathcal{A}^{\text{XORP}[3]} \rightarrow 1] - \text{Pr}[\mathcal{A}^{\text{RF}} \rightarrow 1]| \]
Allow $\mathcal{A}$ to make $q_{\text{max}}$ queries to each user (more advantage to $\mathcal{A}$) $\Rightarrow q = q_{\text{max}} \times u$.

- $\mathcal{A}$'s queries to the same user are distinct.
- Each user holds independent copy of $\text{RP} \Rightarrow$ Reply of each user independent.
Allow $\mathcal{A}$ to make $q_{max}$ queries to each user (more advantage to $\mathcal{A}$) $\Rightarrow q = q_{max} \times u$.

- $\mathcal{A}$’s queries to the same user are distinct.
- Each user holds independent copy of $RP \Rightarrow$ Reply of each user independent.

$XORP[3]^u$ transcript $P := (P_1, P_2, \ldots, P_q)$; RF transcript $R := (R_1, R_2, \ldots, R_q)$

$$Adv_{XORP[3]}^{\mu_{prf}}(\mathcal{A}) \leq \|Pr_P - Pr_R\|$$
• \( \text{Adv}^{\text{mu-prf}}_{\text{XORP}[3]}(\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}}/2^n \) \((q_{\text{max}} \leq 2^n/12)\)
Our Contribution (Formal) and Application

\[ \text{Adv}^{\text{mu-prf}}_{\text{XORP}[3]}(\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}/2^n} \quad (q_{\text{max}} \leq 2^n/12) \]

- Can be used by \( O(2^n) \) users and adversary is allowed to make \( O(2^n) \) queries per user.
Our Contribution (Formal) and Application

\[ \text{Adv}_{\text{mu}_{\text{prf}}}^{\text{XORP}[3]}(\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}}/2^n \quad (q_{\text{max}} \leq 2^n/12) \]

- Can be used by \( O(2^n) \) users and adversary is allowed to make \( O(2^n) \) queries per user.
- For single user, adversary’s advantage is \( O \left( \frac{1}{\sqrt{2^n}} \right) \) even after making \( O(2^n) \) queries.
Our Contribution (Formal) and Application

- \( \text{Adv}_{\text{XORP}[3]}^{\mu_{\text{prf}}} (\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}}/2^n \) \((q_{\text{max}} \leq 2^n/12)\)

  - Can be used by \(O(2^n)\) users and adversary is allowed to make \(O(2^n)\) queries per user.
  - For single user, adversary’s advantage is \(O\left(\frac{1}{\sqrt{2^n}}\right)\) even after making \(O(2^n)\) queries.

- \( \text{Adv}_{\text{XORP'}[3]}^{\text{prf}} (\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{3/2}} \)

Application

- Counter-mode encryption using XORP\([3]\)
- Multi-user security similar to XORP\([3]\) (when instantiated with a good block cipher)

[Bellare et al., 1999]: Parity-method encryption
- similar security, but requires additional randomness
Our Contribution (Formal) and Application

- $\text{Adv}_{\text{XORP[3]}}^{\mu\text{-prf}}(\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}}/2^n$ ($q_{\text{max}} \leq 2^n/12$)

  - Can be used by $O(2^n)$ users and adversary is allowed to make $O(2^n)$ queries per user.
  - For single user, adversary’s advantage is $O\left(\frac{1}{\sqrt{2^n}}\right)$ even after making $O(2^n)$ queries.

- $\text{Adv}_{\text{XORP'[3]}}^{\text{prf}}(\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{3/2}}$

  - Multi-user analysis (not given) will produce similar type of bound as XORP[3].
Our Contribution (Formal) and Application

- \( \text{Adv}^{\text{mu-prf}}_{\text{XORP}[3]}(A) \leq 20\sqrt{uq_{\text{max}}}/2^n \ (q_{\text{max}} \leq 2^n/12) \)

  [Hoang and Shen, 2020]: \( \text{Adv}^{\text{mu-prf}}_{\text{XORP}[2]}(A) = O\left(\frac{\sqrt{nq}}{2^n}\right) \)

  - Can be used by \( O(2^n) \) users and adversary is allowed to make \( O(2^n) \) queries per user.
  - For single user, adversary’s advantage is \( O\left(\frac{1}{\sqrt{2^n}}\right) \) even after making \( O(2^n) \) queries.

- \( \text{Adv}^{\text{prf}}_{\text{XORP'}[3]}(A) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^3} \)

  - Multi-user analysis (not given) will produce similar type of bound as XORP[3].

Application

Our Contribution (Formal) and Application

- $\text{Adv}_{\text{XORP}[3]}^{\mu_{\text{prf}}} (A) \leq 20\sqrt{uq_{\text{max}}}/2^n \ (q_{\text{max}} \leq 2^n/12)$

  [Hoang and Shen, 2020]: $\text{Adv}_{\text{XORP}[2]}^{\mu_{\text{prf}}} (A) = O \left( \frac{\sqrt{nq}}{2^n} \right)$

  ▶ Can be used by $O(2^n)$ users and adversary is allowed to make $O(2^n)$ queries per user.

  ▶ For single user, adversary’s advantage is $O \left( \frac{1}{\sqrt{2^n}} \right)$ even after making $O(2^n)$ queries.

- $\text{Adv}_{\text{XORP'}[3]}^{\text{prf}} (A) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{3/2}}$

  ▶ Multi-user analysis (not given) will produce similar type of bound as XORP[3].

  [Cogliati, 2018]: $\text{Adv}_{\text{XORP'}[2]}^{\mu_{\text{prf}}} (A) = O \left( \frac{q}{2^n} \right)$
Our Contribution (Formal) and Application

- \( \text{Adv}_{\text{XORP}^{[3]}}^\text{mu-prf}(\mathcal{A}) \leq 20\sqrt{uq_{\text{max}}}/2^n \) \( (q_{\text{max}} \leq 2^n/12) \)

[Hoang and Shen, 2020]: \( \text{Adv}_{\text{XORP}^{[2]}}^\text{mu-prf}(\mathcal{A}) = O\left( \frac{\sqrt{nq}}{2^n} \right) \)

- Can be used by \( O(2^n) \) users and adversary is allowed to make \( O(2^n) \) queries per user.
- For single user, adversary’s advantage is \( O\left( \frac{1}{\sqrt{2^n}} \right) \) even after making \( O(2^n) \) queries.

- \( \text{Adv}_{\text{XORP'}^{[3]}}^\text{prf}(\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^3} \)

- Multi-user analysis (not given) will produce similar type of bound as XORP\([3]\).

[Cogliati, 2018]: \( \text{Adv}_{\text{XORP'}^{[2]}}^\text{mu-prf}(\mathcal{A}) = O\left( \frac{q}{2^n} \right) \)

Application

Counter-mode encryption using XORP\([3]\)
Our Contribution (Formal) and Application

- $\text{Adv}_{\text{XORP}[3]}^{\mu_{\text{prf}}}(\mathcal{A}) \leq 20\sqrt{uq_{\max}/2^n} \quad (q_{\max} \leq 2^n/12)$

  [Hoang and Shen, 2020]: $\text{Adv}_{\text{XORP}[2]}^{\mu_{\text{prf}}}(\mathcal{A}) = O \left( \frac{\sqrt{nq}}{2^n} \right)$

  ▶ Can be used by $O(2^n)$ users and adversary is allowed to make $O(2^n)$ queries per user.
  ▶ For single user, adversary’s advantage is $O \left( \frac{1}{\sqrt{2^n}} \right)$ even after making $O(2^n)$ queries.

- $\text{Adv}_{\text{XORP'}[3]}^{\text{prf}}(\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{3/2}}$

  ▶ Multi-user analysis (not given) will produce similar type of bound as XORP[3].

  [Cogliati, 2018]: $\text{Adv}_{\text{XORP'}[2]}^{\mu_{\text{prf}}}(\mathcal{A}) = O \left( \frac{q}{2^n} \right)$

Application

Counter-mode encryption using XORP[3]

- Multi-user security similar to XORP[3] (when instantiated with a good block cipher)

  [Bellare et al., 1999]: Parity-method encryption

  ▶ similar security, but requires additional randomness
Our Technique: $\chi^2$-method

- $X^q := (X_1, \ldots, X_q) \sim \Pr_X$, and $Z^q := (Z_1, \ldots, Z_q) \sim \Pr_Z$ over $\Omega \times \cdots \times \Omega$.
- $\Pr_{X|_{X_{i-1}}}(x_i) := \Pr[X_i = x_i \mid X_1 = x_1, \ldots, X_{i-1} = x_{i-1}]$,
  $\Pr_{Z|_{Z_{i-1}}}(x_i) := \Pr[Z_i = x_i \mid Z_1 = x_1, \ldots, Z_{i-1} = x_{i-1}]$. 

Theorem ([Dai et al., 2017])

If $\Pr_{X|_{X_{i-1}}}$ is contained within the support of the distribution $\Pr_{Z|_{Z_{i-1}}}$ for all $x_{i-1}$, then

$\|\Pr_X - \Pr_Z\| \leq \frac{1}{2} q \sum_{i=1}^{\infty} \mathbb{E}_{X_i} [\chi^2(X_i - 1)]$. 

(1)

Effectively applied in [Bhattacharya and Nandi, 2018b, Bhattacharya and Nandi, 2018a, Choi et al., 2019, Mennink, 2019, Gunsing and Mennink, 2020].
**Our Technique: $\chi^2$-method**

- $X^q := (X_1, \ldots, X_q) \sim \text{Pr}_X$, and $Z^q := (Z_1, \ldots, Z_q) \sim \text{Pr}_Z$ over $\Omega \times \cdots \times \Omega$.
- $\text{Pr}_{X|x_{i-1}}(x_i) := \text{Pr}[X_i = x_i \mid X_1 = x_1, \ldots, X_{i-1} = x_{i-1}]$, 
  $\text{Pr}_{Z|x_{i-1}}(x_i) := \text{Pr}[Z_i = x_i \mid Z_1 = x_1, \ldots, Z_{i-1} = x_{i-1}]$.
- $\chi^2(x_i) := \chi^2(\text{Pr}_{X|x_{i-1}}, \text{Pr}_{Z|x_{i-1}}) = \sum_{x_i \in \Omega} \frac{(\text{Pr}_{X|x_{i-1}}(x_i) - \text{Pr}_{Z|x_{i-1}}(x_i))^2}{\text{Pr}_{Z|x_{i-1}}(x_i)}$
Our Technique: $\chi^2$-method

- $X^q := (X_1, \ldots, X_q) \sim \Pr_X$, and $Z^q := (Z_1, \ldots, Z_q) \sim \Pr_Z$ over $\Omega \times \cdots \times \Omega$.
- $\Pr_{X|x_{i-1}}(x_i) := \Pr[X_i = x_i | X_1 = x_1, \ldots, X_{i-1} = x_{i-1}]$, $\Pr_{Z|x_{i-1}}(x_i) := \Pr[Z_i = x_i | Z_1 = x_1, \ldots, Z_{i-1} = x_{i-1}]$.
- $\chi^2(x_i) := \chi^2(\Pr_{X|x_{i-1}}, \Pr_{Z|x_{i-1}}) = \sum_{x_i \in \Omega} \frac{(\Pr_{X|x_{i-1}}(x_i) - \Pr_{Z|x_{i-1}}(x_i))^2}{\Pr_{Z|x_{i-1}}(x_i)}$

Theorem ([Dai et al., 2017])

*If $\Pr_{X|x_{i-1}}$ is contained within the support of the distribution $\Pr_{Z|x_{i-1}}$ for all $x_{i-1}$, then*

$$\|\Pr_X - \Pr_Z\| \leq \left( \frac{1}{2} \sum_{i=1}^{q} \text{Ex}[\chi^2(X^{i-1})] \right)^{\frac{1}{2}} \tag{1}$$
Our Technique: $\chi^2$-method

- $X^q := (X_1, \ldots, X_q) \sim \Pr_X$, and $Z^q := (Z_1, \ldots, Z_q) \sim \Pr_Z$ over $\Omega \times \cdots \times \Omega$.
- $\Pr_{X|\mathbf{x}^{i-1}}(x_i) := \Pr[X_i = x_i \mid X_1 = x_1, \ldots, X_{i-1} = x_{i-1}]$, $\Pr_{Z|\mathbf{x}^{i-1}}(x_i) := \Pr[Z_i = x_i \mid Z_1 = x_1, \ldots, Z_{i-1} = x_{i-1}]$.
- $\chi^2(x_i) := \chi^2(\Pr_{X|\mathbf{x}^{i-1}}, \Pr_{Z|\mathbf{x}^{i-1}}) = \sum_{x_i \in \Omega} \frac{(\Pr_{X|\mathbf{x}^{i-1}}(x_i) - \Pr_{Z|\mathbf{x}^{i-1}}(x_i))^2}{\Pr_{Z|\mathbf{x}^{i-1}}(x_i)}$.

Theorem ([Dai et al., 2017])

If $\Pr_{X|\mathbf{x}^{i-1}}$ is contained within the support of the distribution $\Pr_{Z|\mathbf{x}^{i-1}}$ for all $\mathbf{x}^{i-1}$, then

$$\|\Pr_X - \Pr_Z\| \leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbb{E}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}}.$$ (1)

Effectively applied in [Bhattacharya and Nandi, 2018b, Bhattacharya and Nandi, 2018a, Choi et al., 2019, Mennink, 2019, Gunsing and Mennink, 2020].
1 Motivation: PRF and Its Multi-user Security

2 Technical Background and Our Results (Statements)

3 Multi-user PRF-Security of XORP[3]: Proof Outline

4 References
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

$$\text{Adv}_{\text{XORP}[3]}^{\text{mu-prf}}(\mathcal{A}) \leq \|\text{Pr}_P - \text{Pr}_R\|$$
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

\[
\text{Adv}_{\text{XORP}[3]}^{\mu_{\text{prf}}} (\mathcal{A}) \leq \| \Pr_P - \Pr_R \| \leq ?
\]
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

$$\text{Adv}_{\text{XORP}[3]}^{\text{mu-prf}}(\mathcal{A}) \leq \|\Pr_P - \Pr_R\| \leq ?$$

Can we apply the $\chi^2$-method to upper bound $\|\Pr_P - \Pr_R\|$?
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

\[ \text{Adv}^\mu_{\text{prf}}_{\text{XORP}[3]}(\mathcal{A}) \leq \| \text{Pr}_P - \text{Pr}_R \| \leq ? \]

Can we apply the $\chi^2$-method to upper bound $\| \text{Pr}_P - \text{Pr}_R \|$?

$\mathcal{A}$ chooses user $U_i$ adaptively $\Rightarrow$ $U_i$ potentially depends on all the previous replies (from all the users)

Can not apply the $\chi^2$-method directly
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

$$\text{Adv}^{\text{mu\_prf}}_{\text{XORP}[3]}(\mathcal{A}) \leq \|\text{Pr}_P - \text{Pr}_R\| \leq ?$$

Can we apply the $\chi^2$-method to upper bound $\|\text{Pr}_P - \text{Pr}_R\|$?

$\mathcal{A}$ chooses user $U_i$ adaptively $\Rightarrow$ $U_i$ potentially depends on all the previous replies (from all the users)

Can not apply the $\chi^2$-method directly

Is there a way round?
Applying the $\chi^2$-method: Problem Due to Adaptive Choice

$$\text{Adv}_{\text{XORP}[3]}^{\mu_{\text{prf}}}(\mathcal{A}) \leq \| \text{Pr}_P - \text{Pr}_R \| \leq ?$$

Can we apply the $\chi^2$-method to upper bound $\| \text{Pr}_P - \text{Pr}_R \|$?

\(\mathcal{A}\) chooses user \(U_i\) adaptively \(\Rightarrow\) \(U_i\) potentially depends on all the previous replies (from all the users)

Can not apply the $\chi^2$-method directly

Is there a way round?

Reorder (permute) the transcript (P to S and R to U)

Club the replies from the same user together

More precisely ...
Random Experiment for $U$

\begin{align*}
1 & : \quad U := (U_i : i \in [q]) \leftarrow \text{wr } G \\
2 & : \quad \text{return } U
\end{align*}

Random Experiment for $S$

\begin{align*}
1 & : \quad \text{for } 1 \leq i \leq u \\
2 & : \quad \hat{T}_i := (T_{j,k} : j \in [I_i], k \in [3]) \leftarrow \text{wor } G \\
& \quad / \hat{T}_i \text{ is sampled independent of } \hat{T}_j, \ 1 \leq j \leq i - 1 \\
3 & : \quad \text{for } 1 \leq \ell \leq q \\
4 & : \quad S_\ell = T_{\ell,1} + T_{\ell,2} + T_{\ell,3} \\
5 & : \quad \text{return } S := (S_\ell : \ell \in [q])
\end{align*}
A Solution: Reordering the Transcript

Random Experiment for U

1: \( U := (U_i : i \in [q]) \leftarrow \text{wr} \, \mathcal{G} \)
2: \text{return } U

Random Experiment for S

1: \text{for } 1 \leq i \leq u
2: \( \hat{T}_i := (T_{j,k} : j \in [I_i], k \in [3]) \leftarrow \text{wor} \, \mathcal{G} \)
   \( / \hat{T}_i \text{ is sampled independent of } \hat{T}_j, \ 1 \leq j \leq i - 1 \)
3: \text{for } 1 \leq \ell \leq q
4: \( S_\ell = T_{\ell,1} + T_{\ell,2} + T_{\ell,3} \)
5: \text{return } S := (S_\ell : \ell \in [q])

Reordering R (random WR sample) to U (random WR sample): they are same.
A Solution: Reordering the Transcript

Random Experiment for $U$

1: $U := (U_i : i \in [q]) \leftarrow \text{wr } \mathcal{G}$
2: return $U$

Random Experiment for $S$

1: for $1 \leq i \leq u$
2: $\hat{T}_i := (T_{j,k} : j \in [I_i], k \in [3]) \leftarrow \text{wor } \mathcal{G}$
   / $\hat{T}_i$ is sampled independent of $\hat{T}_j$, $1 \leq j \leq i - 1$
3: for $1 \leq \ell \leq q$
4: $S_\ell = T_{\ell,1} + T_{\ell,2} + T_{\ell,3}$
5: return $S := (S_\ell : \ell \in [q])$

Reordering $R$ (random WR sample) to $U$ (random WR sample): they are same.

Reordering $P$ to $S$:

$S = S_1, S_2, \ldots, S_{q_{\max}}, S_{q_{\max}}+1 \ldots, S_{2q_{\max}}, \ldots, S_{(u-1)q_{\max}}+1 \ldots, S_{q=ug_{\max}}$
Two Observations

- Distribution of output is independent of input in both worlds.
- \( A \) makes same number (\( = q_{max} \)) of queries to each user.

Reordering (Contd.)
Two Observations

- Distribution of output is independent of input in both worlds.
- \( \mathcal{A} \) makes same number \( (= q_{max}) \) of queries to each user.

Makes reordering possible
Two Observations

- Distribution of output is independent of input in both worlds.
- $A$ makes same number ($= q_{max}$) of queries to each user.

Makes reordering possible

(In S) $U_i$ is uniquely determined by $i$

$$U_i = j \in [u] \text{ such that } i = (j - 1)q_{max} + k, k \in [q_{max}]$$
Two Observations

- Distribution of output is independent of input in both worlds.
- $\mathcal{A}$ makes same number ($= q_{max}$) of queries to each user.

**Makes reordering possible**

$U_i$ is uniquely determined by $i$

$U_i = j \in [u]$ such that $i = (j - 1)q_{max} + k$, $k \in [q_{max}]$

So, in particular

$\Pr\{S_i = (j-1)q_{max} + k | U=1\}$

$U=1$

$S_1, \ldots, S_{q_{max}}$ \quad $\quad S_{q_{max}+1} \ldots, S_{2q_{max}}$ \quad $\ldots, S_{(j-1)q_{max}+1} \ldots, S_{i-1}$

$U=2$

$U=j$

$\Pr\{S_{(j-1)q_{max}+1} \ldots, S_{i-1} | U=2\}$

$U=j$

$\Pr\{S_i | U=2\}$

$\Pr\{S_{(j-1)q_{max}+1} \ldots, S_{i-1}\}$ (RP$_j$ is independent of RP$_1$, RP$_2$, ...)

Reordering (Contd.)
Two Observations

- Distribution of output is independent of input in both worlds.
- \( \mathcal{A} \) makes same number (\( = q_{\text{max}} \)) of queries to each user.

**Makes reordering possible**

(In S) \( U_i \) is uniquely determined by \( i \)

\[ U_i = j \in [u] \text{ such that } i = (j - 1)q_{\text{max}} + k, \ k \in [q_{\text{max}}] \]

So, in particular

\[
\Pr \{ S_{(j-1)q_{\text{max}}+1} \ldots , S_{i-1} \mid U=1 \} = \Pr \{ S_{i} \mid S_{(j-1)q_{\text{max}}+1} \ldots , S_{i-1} \} \quad (\text{RP}_j \text{ is independent of } \text{RP}_1, \ \text{RP}_2, \ldots )
\]

This is needed for the application of the \( \chi^2 \)-method
Two Observations

- Distribution of output is independent of input in both worlds.
- \( \mathcal{A} \) makes same number (= \( q_{\text{max}} \)) of queries to each user.

**Makes reordering possible**

\( \text{(In S)} \) \( U_i \) is uniquely determined by \( i \)

\[ U_i = j \in [u] \text{ such that } i = (j - 1)q_{\text{max}} + k, k \in [q_{\text{max}}] \]

So, in particular

\[ \Pr\{ S_i = (j - 1)q_{\text{max}} + k \mid U = 1 \} = \Pr\{ S_j = (j - 1)q_{\text{max}} + k \mid U = 1 \} \]

\[ = \Pr\{ S_i \mid S_{(j-1)q_{\text{max}} + 1}, \ldots, S_{i-1} \} \quad (\text{RP}_j \text{ is independent of } \text{RP}_1, \text{RP}_2, \ldots) \]

This is needed for the application of the \( \chi^2 \)-method

Reordering preserves statistical distance:

\[ \| \Pr_S - \Pr_U \| = \| \Pr_P - \Pr_R \| \]
Enough to upper bound $\|\Pr_S - \Pr_U\|$
Enough to upper bound $\|\Pr_S - \Pr_U\|$?

Can $\chi^2$-method be applied to upper bound $\|\Pr_S - \Pr_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?
Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound \( \| \text{Pr}_S - \text{Pr}_U \| \)

Can \( \chi^2 \)-method be applied to upper bound \( \| \text{Pr}_S - \text{Pr}_U \| \)?

Support of \( S \subseteq \) Support of \( U \)?

How to ensure?

Extend \( S \) and \( U \) (to \( X \) and \( Y \) resp.)
Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$

Can $\chi^2$-method be applied to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

---

$S$ and $U$ are marginals of $X$ and $Y$ resp.
Enough to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$.

Can $\chi^2$-method be applied to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

How to extend?

S and U are marginals of X and Y resp.

$S$ and $U$ are marginals of $X$ and $Y$ resp.
Enough to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$.

Can $\chi^2$-method be applied to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

How to extend?

$X_i = (T_{i,1}, T_{i,2}, S_i)$

$Y_i = (V_{i,1}, V_{i,2}, U_i)$

for all $i \in [q]$
Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\Pr_S - \Pr_U\|$.

Can $\chi^2$-method be applied to upper bound $\|\Pr_S - \Pr_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

How to extend?

\[
X_i = (T_{i,1}, T_{i,2}, S_i) \\
Y_i = (V_{i,1}, V_{i,2}, U_i)
\]

for all $i \in [q]$. 

$S$ and $U$ are marginals of $X$ and $Y$ resp.
Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\Pr_S - \Pr_U\|$.

Can $\chi^2$-method be applied to upper bound $\|\Pr_S - \Pr_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

How to extend?

$X_i = (T_{i,1}, T_{i,2}, S_i)$

$Y_i = (V_{i,1}, V_{i,2}, U_i)$ for all $i \in [q]$

$(V_{i,1}, V_{i,2}, V_{i,3}), \ i \in [q]$ behaves like a WOR sample
**Extending the Transcripts: Ensuring the Support Condition**

Enough to upper bound $\|\text{Pr}_S - \text{Pr}_U\|

Can $\chi^2$-method be applied to upper bound $\|\text{Pr}_S - \text{Pr}_U\|$?

Support of $S \subseteq$ Support of $U$?

How to ensure?

Extend $S$ and $U$ (to $X$ and $Y$ resp.)

How to extend?

$X_i = (T_{i,1}, T_{i,2}, S_i)$

$Y_i = (V_{i,1}, V_{i,2}, U_i)$

for all $i \in [q]

$S_i = T_{i,1} + T_{i,2} + T_{i,3}$

$V_{i,3} = V_{i,1} + V_{i,2} + U_i$

$(V_{i,1}, V_{i,2}, V_{i,3}), i \in [q]$ behaves like a WOR sample

$S$ and $U$ are marginals of $X$ and $Y$ resp.
Enough to upper bound $\|\Pr_S - \Pr_U\|$ 

Can $\chi^2$-method be applied to upper bound $\|\Pr_S - \Pr_U\|$? 

Support of $S \subseteq$ Support of $U$? 

How to ensure? 

Extend $S$ and $U$ (to $X$ and $Y$ resp.) 

How to extend? 

$X_i = (T_{i,1}, T_{i,2}, S_i)$ 

$Y_i = (V_{i,1}, V_{i,2}, U_i)$ 

$V_{i,3} = V_{i,1} + V_{i,2} + U_i$ 

$(V_{i,1}, V_{i,2}, V_{i,3}), \ i \in [q] \ behaves \ like \ a \ WOR \ sample$ 

What are $V_{i,1}, V_{i,2}$?
Extending the Transcripts: Details

\[ i = (j - 1)q_{\text{max}} + k \quad \Rightarrow \quad i\text{-th query} = j\text{-th user’s} \ k\text{-th query} \]
Extending the Transcripts: Details

\[ U_i = j \]

\[ i = (j - 1)q_{max} + k \quad \Rightarrow \quad i\text{-th query} = j\text{-th user’s } k\text{-th query} \]
Extending the Transcripts: Details

\[ i = (j - 1)q_{max} + k \Rightarrow i\text{-th query} = j\text{-th user’s } k\text{-th query} \]

\[ \mathcal{N}_i = \left\{ (v_1, v_2) \mid v_1, v_2, U_i + v_1 + v_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{ V_{i,1}, V_{i,2}, V_{i,3} \}, \right. \]

\[ U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \} \]
$U_i = j \quad i = (j - 1)q_{max} + k \quad \Rightarrow \quad i$-th query = $j$-th user’s $k$-th query

$$N_i = \left\{ (v_1, v_2) \mid \right.$$  

$\forall v_1, v_2, U_i + v_1 + v_2 \in G \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{ V_i,1, V_i,2, V_i,3 \}$,  

$U_i + v_1 + v_2, v_1, v_2$ distinct  

$$\left\} \right.$$  

All previous samples of the $j$-th user
$U_i = j$

$i = (j - 1)q_{max} + k \Rightarrow i$-th query = $j$-th user’s $k$-th query

$$\mathcal{N}_i = \left\{ (v_1, v_2) \mid v_1, v_2, U_i + v_1 + v_2 \in G \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{V_{i,1}, V_{i,2}, V_{i,3}\}, U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \right\}$$

$\text{(V}_{i,1}, \text{V}_{i,2}) \leftarrow \mathcal{N}_i$
 Extending the Transcripts: Details

\[ U_i = j \]

\[ i = (j - 1)q_{\text{max}} + k \quad \Rightarrow \quad \text{i-th query} = \text{j-th user’s k-th query} \]

\[ \mathcal{N}_i = \left\{ (v_1, v_2) | \begin{array}{c}
(v_1, v_2, U_i + v_1 + v_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{\text{max}}+1}^{(j-1)q_{\text{max}}+k-1} \{V_{i,1}, V_{i,2}, V_{i,3}\}, \\
U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \end{array} \right\} \]

All previous samples of the j-th user

After Extension

- Support of X = Support of Y
$U_i = j$  

\[ i = (j - 1)q_{max} + k \implies i\text{-th query} = j\text{-th user's } k\text{-th query} \]

\[ N_i = \left\{ (v_1, v_2) \mid \begin{array}{l} v_1, v_2, U_i + v_1 + v_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{V_{i,1}, V_{i,2}, V_{i,3}\}, \\ U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \end{array} \right\} \]

\[ (V_{i,1}, V_{i,2}) \leftarrow N_i \]

\textbf{After Extension}

- Support of $X = \text{Support of } Y$
- $S$ and $U$ are marginals of $X$ and $Y$ (resp.) \implies \|Pr_S - Pr_U\| \leq \|Pr_X - Pr_Y\|
Extending the Transcripts: Details

\[ U_i = j \]

\[ i = (j - 1)q_{\text{max}} + k \quad \Rightarrow \quad i\text{-th query} = j\text{-th user’s} \ k\text{-th query} \]

\[ \mathcal{N}_i = \left\{ (v_1, v_2) \mid \begin{array}{c}
v_1, v_2, U_i + v_1 + v_2 \in \mathcal{C} \setminus \\
(j-1)q_{\text{max}} + k - 1 \\
\bigcup_{i=(j-1)q_{\text{max}}+1} \{V_{i,1}, V_{i,2}, V_{i,3}\}, \\
U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \end{array} \right\} \]

\[ (V_{i,1}, V_{i,2}) \leftarrow \mathcal{N}_i \]

All previous samples of the \( j \)-th user

After Extension

- Support of \( X = \) Support of \( Y \)
- \( S \) and \( U \) are marginals of \( X \) and \( Y \) (resp.) \( \Rightarrow \quad \|\Pr_S - \Pr_U\| \leq \|\Pr_X - \Pr_Y\| \)
Extending the Transcripts: Details

\( U_i = j \quad \Rightarrow \quad i = (j - 1)q_{max} + k \)

\( i \)-th query = \( j \)-th user’s \( k \)-th query

\( \mathcal{N}_i = \left\{ (v_1, v_2) \mid v_1, v_2, U_i + v_1 + v_2 \in G \setminus \bigcup_{i = (j - 1)q_{max} + 1}^{(j - 1)q_{max} + k - 1} \{ V_{i,1}, V_{i,2}, V_{i,3} \}, U_i + v_1 + v_2, v_1, v_2 \text{ distinct} \right\} \)

\((V_{i,1}, V_{i,2}) \leftarrow \mathcal{N}_i \)

After Extension

- Support of X = Support of Y
- S and U are marginals of X and Y (resp.) \( \Rightarrow \) \( ||\text{Pr}_S - \text{Pr}_U|| \leq ||\text{Pr}_X - \text{Pr}_Y|| \)

Apply \( \chi^2 \)-method to upper bound \( ||\text{Pr}_X - \text{Pr}_Y|| \)
\( \chi^2 \)-Method: Steps

Setting

\[ X_1, \ldots, X_q \sim \text{Pr}_X \]
\[ Y_1, \ldots, Y_q \sim \text{Pr}_Y \]

\[ i = (j - 1)q_{max} + k \Rightarrow \text{\( i \)-th query = \( j \)-th user’s \( k \)-th query} \]
\[ X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \text{block of} \ X_i \text{’s for the} \ j \text{-th user} \]
\[ \hat{X}_{j}^{k-1} = \text{block of first} \ k - 1 \ X_i \text{’s for the} \ j \text{-th user}. \]
Setting

\[
X_1, \ldots, X_q \sim \Pr_X \\
Y_1, \ldots, Y_q \sim \Pr_Y
\]

\( i = (j - 1) q_{max} + k \Rightarrow \) \( i \)-th query = \( j \)-th user’s \( k \)-th query

\( X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \) block of \( X_i \)'s for the \( j \)-th user

\( \hat{X}_{j}^{k-1} = \) block of first \( k - 1 \) \( X_i \)'s for the \( j \)-th user.

Conditional Probabilities Under \( \Pr_X \) and \( \Pr_Y \)

\[
\Pr_X(x_i | x_i^{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i | \hat{X}_j^{k-1} = \hat{x}_j^{k-1}, (X^{i-1} \setminus \hat{X}_j) = (x^{i-1} \setminus \hat{x}_j^{k-1})]
\]

\[
= \Pr[\hat{X}_{j,k} = \hat{x}_{j,k} | \hat{X}_j^{k-1} = \hat{x}_j^{k-1}],
\]

since \( (X^{i-1} \setminus \hat{X}_j) \) is independent of \( \hat{X}_j^{k-1} \) and \( \hat{X}_{j,k} \)

\[
= \frac{1}{(N - 3(k - 1))^3}
\]
**χ²-Method: Steps**

Setting
\[ X_1, \ldots, X_q \sim \Pr_X \]
\[ Y_1, \ldots, Y_q \sim \Pr_Y \]

\[ i = (j - 1)q_{max} + k \Rightarrow \text{ } i\text{-th query} = j\text{-th user’s } k\text{-th query} \]

\[ X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \text{block of } X_i\text{'s for the } j\text{-th user} \]

\[ \hat{X}_{j}^{k-1} = \text{block of first } k - 1 \text{ } X_i\text{'s for the } j\text{-th user.} \]

Conditional Probabilities Under \( \Pr_X \) and \( \Pr_Y \)

\[
\Pr_X(x_i \mid x_i^{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i \mid \hat{X}_j^{k-1} = \hat{x}_j^{k-1}, (X_i^{i-1} \setminus \hat{X}_j) = (x_i^{i-1} \setminus \hat{x}_j^{k-1})]
\]

\[
= \Pr[\hat{X}_{j,k} = \hat{x}_{j,k} \mid \hat{X}_j^{k-1} = \hat{x}_j^{k-1}],
\]

since \((X_i^{i-1} \setminus \hat{X}_j)\) is independent of \(\hat{X}_j^{k-1}\) and \(\hat{X}_{j,k}\)

\[
= \frac{1}{(N - 3(k - 1))^3}
\]

*Due to reordering.*
\[ \chi^2 \text{-Method: Steps} \]

Setting
\[ X_1, \ldots, X_q \sim \Pr_X \]
\[ Y_1, \ldots, Y_q \sim \Pr_Y \]
i = (j - 1)q_{max} + k \Rightarrow \ i\text{-th query} = j\text{-th user’s} k\text{-th query}
\[ X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \text{block of} \ X_i\text{’s for the} j\text{-th user} \]
\[ \hat{X}_{j}^{k-1} = \text{block of first} k - 1 \ X_i\text{’s for the} j\text{-th user}. \]

Conditional Probabilities Under \( \Pr_X \) and \( \Pr_Y \)

\[ \Pr_X(x_i \mid x_i^{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i \mid \hat{X}_{j}^{k-1} = \hat{x}_{j}^{k-1}, (X_i^{i-1} \setminus \hat{X}_j) = (x_i^{i-1} \setminus \hat{x}_{j}^{k-1})] \]

\[ = \Pr[\hat{X}_{j,k} = \hat{x}_{j,k} \mid \hat{X}_{j}^{k-1} = \hat{x}_{j}^{k-1}], \]

since \((X_i^{i-1} \setminus \hat{X}_j)\) is independent of \(\hat{X}_{j}^{k-1}\) and \(\hat{X}_{j,k}\)

\[ = \frac{1}{(N - 3(k - 1))^3} \quad \text{Falling factorial} \]
**χ²-Method: Steps**

Setting

\[
X_1, \ldots, X_q \sim \Pr_X, \quad Y_1, \ldots, Y_q \sim \Pr_Y
\]

\[i = (j - 1)q_{\text{max}} + k \Rightarrow i\text{-th query} = j\text{-th user’s } k\text{-th query}
\]

\[X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \text{block of } X_i\text{'s for the } j\text{-th user}
\]

\[\hat{X}_{j}^{k-1} = \text{block of first } k - 1 \text{ } X_i\text{'s for the } j\text{-th user.}
\]

**Conditional Probabilities Under \(\Pr_X\) and \(\Pr_Y\)**

\[
\Pr_X(x_i | x_i^{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i | \hat{X}_j^{k-1} = \hat{x}_j^{k-1}, (X_{i-1} \setminus \hat{X}_j) = (x_{i-1} \setminus \hat{x}_j^{k-1})]
\]

\[= \Pr[\hat{X}_{j,k} = \hat{x}_{j,k} | \hat{X}_j^{k-1} = \hat{x}_j^{k-1}], \quad \text{Due to reordering.}
\]

since \((X_i \setminus \hat{X}_j)\) is independent of \(\hat{X}_j^{k-1}\) and \(\hat{X}_{j,k}\)

\[= \frac{1}{(N - 3(k - 1))^3} \quad \text{Falling factorial}
\]

**Similarly for \(\Pr_Y\)**

\[
\Pr_Y(x_i | x_i^{i-1}) = \frac{1}{N} \times \frac{1}{|N_{ui}(\hat{x}_j^{k-1})|}
\]
\( \chi^2 \)-Method: Steps

**Setting**

\[ X_1, \ldots, X_q \sim \Pr_X \]
\[ Y_1, \ldots, Y_q \sim \Pr_Y \]

\( i = (j - 1)q_{\text{max}} + k \Rightarrow \) \( i \)-th query = \( j \)-th user’s \( k \)-th query

\( X_i = \hat{X}_{j,k}, \quad \hat{X}_j = \text{block of } X_i \text{'s for the } j \text{-th user} \)

\( \hat{X}_{j}^{k-1} = \text{block of first } k - 1 \text{ } X_i \text{'s for the } j \text{-th user}. \)

**Conditional Probabilities Under \( \Pr_X \) and \( \Pr_Y \)**

\[
\Pr_X(x_i \mid x_{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i \mid \hat{X}_j^{k-1} = \hat{x}_j^{k-1}, (X_{i-1} \setminus \hat{X}_j) = (x_{i-1} \setminus \hat{x}_j^{k-1})]
= \Pr[\hat{X}_{j,k} = \hat{x}_{j,k} \mid \hat{X}_j^{k-1} = \hat{x}_j^{k-1}],
\]

since \((X_{i-1} \setminus \hat{X}_j)\) is independent of \(\hat{X}_j^{k-1}\) and \(\hat{X}_{j,k}\)

\[ = \frac{1}{(N - 3(k - 1))^3} \quad \text{Falling factorial} \]

**Similarly for \( \Pr_Y \)**

\[
\Pr_Y(x_i \mid x_{i-1}) = \frac{1}{N} \times \frac{1}{|\mathcal{N}_u_i(\hat{x}_j^{k-1})|} \quad \text{Same as } n_i
\]
\(\chi^2\)-Method: The Expectation to Compute

\(\chi^2\) distance and its expectation

\[
\chi^2(x^{i-1}) := \sum_{x_i = (v_{i,1}, v_{i,2}, u_i)} \frac{(\Pr_X(x_i|\hat{x}^{k-1}_j) - \Pr_Y(x_i|\hat{x}^{k-1}_j))^2}{\Pr_Y(x_i|\hat{x}^{k-1}_j)}\]

\[
= C \times \sum_{u_i \in \{0,1\}^n} (|n_{u_i}(\hat{x}^{k-1}_j)| - D)
\]
\( \chi^2 \)-Method: The Expectation to Compute

\( \chi^2 \) distance and its expectation

\[
\chi^2(x_{i-1}) := \sum_{x_i = (v_{i,1}, v_{i,2}, u_i)} \frac{(\Pr_X(x_i | \hat{x}_{j}^{k-1}) - \Pr_Y(x_i | \hat{x}_{j}^{k-1}))^2}{\Pr_Y(x_i | \hat{x}_{j}^{k-1})}
\]

\[
= C \times \sum_{u_i \in \{0,1\}^n} (|N^u_i(\hat{x}_{j}^{k-1})| - D)
\]

\[
C = \frac{N}{((N-3(k-1))^2)^2}
\]

\[
D = \frac{(N-3(k-1))^3}{N}
\]
\( \chi^2 \)-Method: The Expectation to Compute

\( \chi^2 \) distance and its expectation

\[ \chi^2(x^{i-1}) := \sum_{x_i = (v_{i,1}, v_{i,2}, u_i)} \frac{(\Pr_X(x_i|\hat{x}_j^{k-1}) - \Pr_Y(x_i|\hat{x}_j^{k-1}))^2}{\Pr_Y(x_i|\hat{x}_j^{k-1})} \]

\[ = C \times \sum_{u_i \in \{0,1\}^n} (|N^u_i(\hat{x}_j^{k-1})| - D)^2 \]

\[ C = \frac{N}{((N-3(k-1))^2)^2} \]
\[ D = \frac{(N-3(k-1))^3}{N} \]

\[ \Rightarrow \]

\[ \mathbb{E}_X[\chi^2(X^{i-1})] = C \times \sum_{u_i} \mathbb{E}_X[(|N^u_i(\hat{x}_j^{k-1})| - D)^2] \]
\( \chi^2 \)-Method: The Expectation to Compute

\( \chi^2 \) distance and its expectation

\[
\chi^2(x^{i-1}) := \sum_{x_i=(v_{i,1},v_{i,2},u_i)} \frac{(\Pr_X(x_i|\hat{x}^{k-1}_j) - \Pr_Y(x_i|\hat{x}^{k-1}_j))^2}{\Pr_Y(x_i|\hat{x}^{k-1}_j)}
\]

\[
= C \times \sum_{u_i \in \{0,1\}^n} \left( |\mathcal{N}^u_i(\hat{x}^{k-1}_j)| - D \right)^2
\]

\[
\text{Ex}[\chi^2(X^{i-1})] = C \times \sum_{u_i} \text{Ex}[\left( |\mathcal{N}^u_i(\hat{x}^{k-1}_j)| - D \right)^2].
\]

Goal is to compute \( \text{Ex}[\left( |\mathcal{N}^u_i(\hat{x}^{k-1}_j)| - D \right)^2] \)
Setting: $\mathcal{G} := \mathbb{F}_{2^n}$ \quad $|\mathcal{G}| = N$ \quad $\mathcal{V}_r$: a random $r$-set in $\mathcal{G}$

For $u \in \mathcal{G}$

$$\{(g_1, g_2) \in \mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2$ distinct$\}$$
**Finishing the Proof: An Important Lemma**

**Setting:** \( \mathcal{G} := \mathbb{F}_{2^n} \) \( |\mathcal{G}| = N \) \( \mathcal{V}_r \): a random \( r \)-set in \( \mathcal{G} \)

For \( u \in \mathcal{G} \)

\[ \{(g_1, g_2) \in \mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2 \text{ distinct}\} \]
Setting: \( \mathcal{G} := \mathbb{F}_{2^n} \) \( |\mathcal{G}| = N \) \( \mathcal{V}_r: \) a random \( r \)-set in \( \mathcal{G} \)

For \( u \in \mathcal{G} \)

\[ \{ (\mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2 \text{ distinct} \} \]
Setting: \( \mathcal{G} := \mathbb{F}_{2^n} \) \quad |\mathcal{G}| = N \quad \mathcal{V}_r: a \text{ random } r\text{-set in } \mathcal{G} \\

For \( u \in \mathcal{G} \), \( N^u_r := |\{(g_1, g_2) \in \mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2 \text{ distinct}\}| \)
Finishing the Proof: An Important Lemma

Setting: \( \mathcal{G} := \mathbb{F}_{2^n} \) \[ |\mathcal{G}| = N \] \( \mathcal{V}_r \): a random \( r \)-set in \( \mathcal{G} \)

For \( u \in \mathcal{G} \)

\[ N^u_r := |\{(g_1, g_2) \in \mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2 \text{ distinct}\}| \]

To compute \( \mathbb{E}[N^u_r - D]^2] \)
Finishing the Proof: An Important Lemma

Setting: \( \mathcal{G} := \mathbb{F}_{2^n} \), \( |\mathcal{G}| = N \), \( \mathcal{V}_r \): a random \( r \)-set in \( \mathcal{G} \)

For \( u \in \mathcal{G} \)

\( N^u_r := |\{(g_1, g_2) \in \mathcal{V}_r \times \mathcal{V}_r : u + g_1 + g_2 \in \mathcal{V}_r; u, g_1, g_2 \text{ distinct}\}| \)

To compute \( \mathbb{E}[ (N^u_r - D)^2 ] \)

Computation of \( \mathbb{E}[N^u_r] \):

\( \mathcal{G}_u = \{g := (g_1, g_2) | g_1 \neq g_2 \in \mathcal{G} \setminus \{u\}\}. \)

\( I_g = \begin{cases} 
1 & \text{if } g_1, g_2, u + g_1 + g_2 \in \mathcal{V}_r, \text{ and } g_1 \neq u \neq g_2 \\
0 & \text{otherwise.} 
\end{cases} \)

\[ \mathbb{E}[N^u_r] = \mathbb{E}[\sum_{g \in \mathcal{G}_u} I_g] = \sum_{g \in \mathcal{G}_u} \mathbb{E}[I_g] = \Pr[\{g_1, g_2, u + g_1 + g_2 \subseteq \mathcal{V}_r\} = \frac{r^3}{N} = D. \]
From expectation to variance:

\[ \text{Ex}[(N_r^u - D)^2] = \text{Ex}[(N_r^u - \text{Ex}[N_r^u])^2] = \text{Var}[N_r^u] \]
From expectation to variance:

\[
\begin{align*}
\mathbb{E}[(N^u_r - D)^2] &= \mathbb{E}[(N^u_r - \mathbb{E}[N^u_r])^2] = \text{Var}[N^u_r]
\end{align*}
\]

To compute \( \mathbb{E}[(N^u_r - D)^2] \) \( \Rightarrow \) To compute \( \text{Var}[N^u_r] \)

How to compute \( \text{Var}[N^u_r] \)?
From expectation to variance:

\[ \text{Ex}[(N_r^u - D)^2] = \text{Ex}[(N_r^u - \text{Ex}[N_r^u])^2] = \text{Var}[N_r^u] \]

To compute \( \text{Ex}[(N_r^u - D)^2] \) implies To compute \( \text{Var}[N_r^u] \)

How to compute \( \text{Var}[N_r^u] \)?

Setting:

For \( g = (g_1, g_2) \), \( S_u^g = \{g_1, g_2, u + g_1 + g_2\} \)

Observation:

\[ w = |S_u^g \cup S_u^{g'}| \in \{3, 5, 6\} \]
An Important Lemma (Contd.)

Technicalities:

\[
\text{Var}[N^u_r] = \sum_{g \in G_u} \text{Var}[I_g] + \sum_{g \neq g' \in G_u} \text{Cov}(I_g, I_{g'})
\]

\[
\text{Var}[I_g] = \text{Ex}[I_g](1 - \text{Ex}[I_g])
\]

\[
\text{Cov}(I_g, I_{g'}) = \text{Ex}[I_g I_{g'}] - \text{Ex}[I_g] \text{Ex}[I_{g'}]
\]

\[
\text{Ex}[\chi^2(X^i - 1)] \leq \frac{576}{N^2} + \frac{4^8 (r')^3}{27CN^6} \Rightarrow \|\text{Pr}_P - \text{Pr}_R\| \leq \frac{20\sqrt{uq_{\text{max}}}}{N}
\]
Strong PRF security of XORP[3]

▶ Multi-user:
- Can be used simultaneously and independently by $O(2^n)$ users
- Adversary can make $O(2^n)$ queries per user

▶ Single-user: Adversary’s advantage is $O\left(\frac{1}{\sqrt{2^n}}\right)$ even after $O(2^n)$ queries
Strong PRF security of XORP\([3]\]

- **Multi-user:**
  - Can be used simultaneously and independently by \(O(2^n)\) users
  - Adversary can make \(O(2^n)\) queries per user

- **Single-user:** Adversary’s advantage is \(O\left(\frac{1}{\sqrt{2^n}}\right)\) even after \(O(2^n)\) queries

Strong PRF security of XORP'\([3]\]

- **Multi-user:** Same level of security. Analysis (not shown) similar to XORP\([3]\]

- **Single-user:** Adversary’s advantage is \(O\left(\frac{1}{\sqrt{2^n}}\right)\) even after \(O(2^n)\) queries
Thank You!
Acknowledgement for Slide Template

Rafael Vieira Westenberger, IMPA, Brazil

Available at: https://www.overleaf.com/latex/templates/impa-beamer-template/jbkhtxsdnqtb
1 Motivation: PRF and Its Multi-user Security
2 Technical Background and Our Results (Statements)
3 Multi-user PRF-Security of XORP[3]: Proof Outline
4 References


**References**

**Bhattacharya, S. and Nandi, M. (2018a).**

**Full indifferentiable security of the xor of two or more random permutations using the $\chi^2$-method.**


**Bhattacharya, S. and Nandi, M. (2018b).**

**Revisiting variable output length xor pseudorandom function.**


**Choi, W., Lee, B., and Lee, J. (2019).**

**Indifferentiability of truncated random permutations.**


**Cogliati, B. (2018).**

**Tweaking a block cipher: multi-user beyond-birthday-bound security in the standard model.**

The indistinguishability of the XOR of k permutations.  

Information-theoretic indistinguishability via the chi-squared method.  

The summation-truncation hybrid: Reusing discarded bits for free.  

Hoang, V. T. and Shen, Y. (2020).  
Security of streaming encryption in Google's Tink library.  
**References**


**New blockcipher modes of operation with beyond the birthday bound security.**


**ZMAC: A fast tweakable block cipher mode for highly secure message authentication.**


**How to construct pseudorandom permutations from pseudorandom functions.**


**The sum of prps is a secure PRF.**
**References**

**Mennink, B. (2019).**  
**Linking Stam’s bounds with generalized truncation.**  

**Mennink, B. and Preneel, B. (2015).**  
**On the xor of multiple random permutations.**  

**Patarin, J. (2008).**  
**A proof of security in o(2^n) for the xor of two random permutations.**  

**Patarin, J. (2010).**  
**Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography.**  