Luby-Rackoff Backwards with More Users and More Security

Srimanta Bhattacharya[1] Mridul Nandi[2]

[1] SIAS, Krea University

[2] Indian Statistical Institute, Kolkata

December 1, 2021

Presentation Outline

Luby-Rackoff Backwards: Motivation

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.

Luby-Rackoff Backwards: Motivation

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 $O(2^{\frac{n}{2}})$ queries.

Luby-Rackoff Backwards: Motivation

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.

Luby-Rackoff Backwards: Motivation

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 $O(2^{\frac{n}{2}})$ 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 $O(2^{\frac{n}{2}})$ 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

Setting

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

Setting

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

Constructions

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

Setting

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

Constructions

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

xor

Concatenation

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

Setting

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

Constructions

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

xor

Concatenation

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

[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

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

xor

Concatenation

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

[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

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

Setting

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

Constructions

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

xor

Concatenation

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

[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

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

Generalizations

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

Setting

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

Constructions

xor

Concatenation

$\mathsf{XORP} : \{0,1\}^{n-1} \to \{0,1\}^n$

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

[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

$\mathsf{XORP}[3] : \{0,1\}^{n-2} \to \{0,1\}^n$ Generalizations

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

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

Sum of Permutations (Contd.)

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

$\mathsf{XORP}[3]' : \{0,1\}^{n-3} \to \{0,1\}^n$

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

Sum of Permutations (Contd.)

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

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

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

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

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

$\mathsf{XORP}[3]$ *requires* 6 *calls*

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

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

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

$\mathsf{XORP}[3]$ *requires* 6 *calls*

- Efficient than $\mathsf{XORP}[3]$ - 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

Sum of Permutations (contd.)

$\mathsf{XORP}[3]' : \{0,1\}^{n-3} \to \{0,1\}^n$

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

$\mathsf{XORP}[3]$ *requires* 6 *calls*

- Efficient than $\mathsf{XORP}[3]$ - 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 $\mathsf{XORP}[k]$ and $\mathsf{XORP}'[k]$ ($\mathsf{XORP} = \mathsf{XORP}[2]$).

$\mathsf{XORP}[3]' : \{0,1\}^{n-3} \to \{0,1\}^n$

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

$\mathsf{XORP}[3]$ *requires* 6 *calls*

- Efficient than $\mathsf{XORP}[3]$ - 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 $\mathsf{XORP}[k]$ and $\mathsf{XORP}'[k]$ $(\mathsf{XORP} = \mathsf{XORP}[2])$.

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]

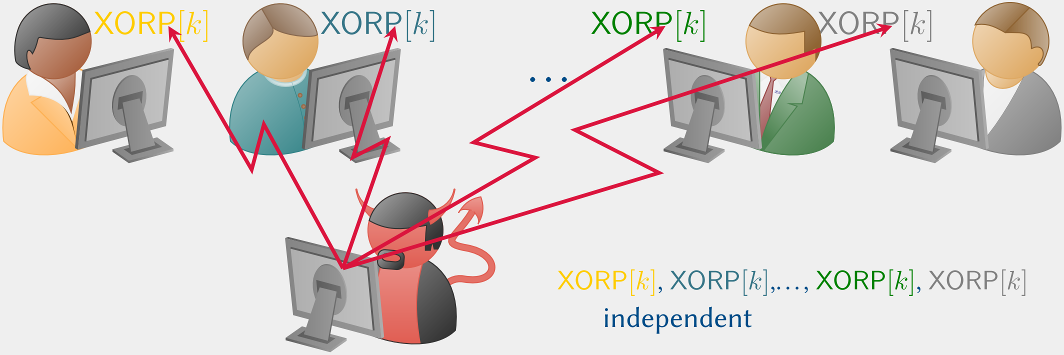
independent

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

XORP$[k]$, XORP$[k]$,…, XORP$[k]$, XORP$[k]$

independent

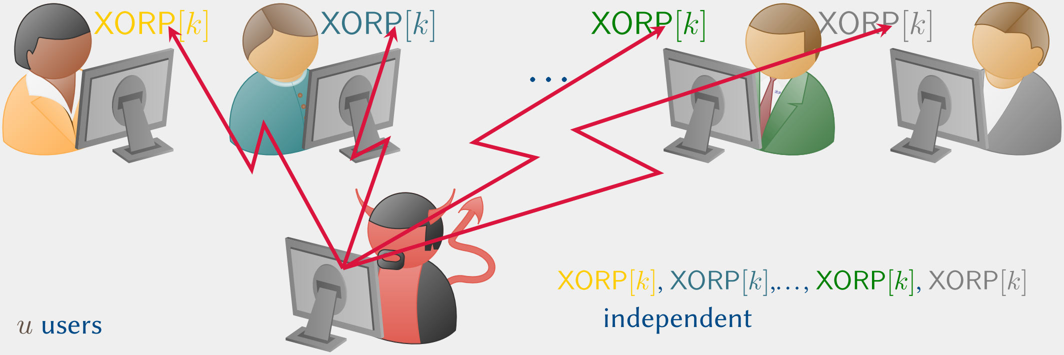
Multi-user PRF-Security of XORP$[k]$: A Concern



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

independent

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

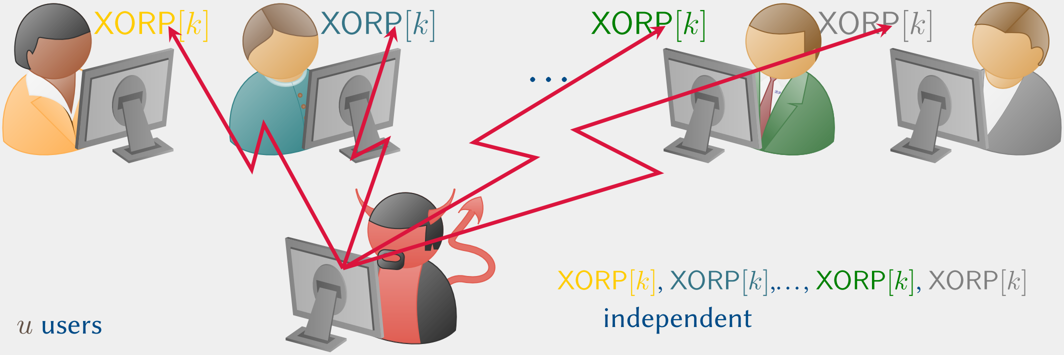


XORP[k], XORP[k],. . . , XORP[k], XORP[k]
independent

u users

q_{max} queries per user

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



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

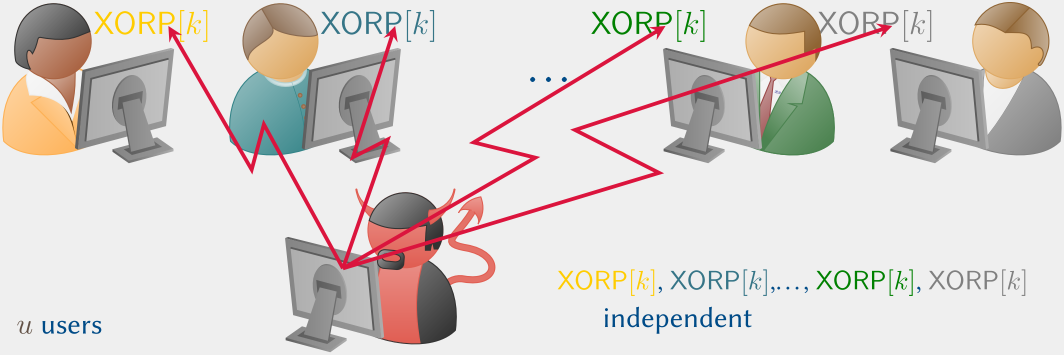
independent

u users

q_{max} 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



XORP[k], XORP[k],…, XORP[k], XORP[k]
independent

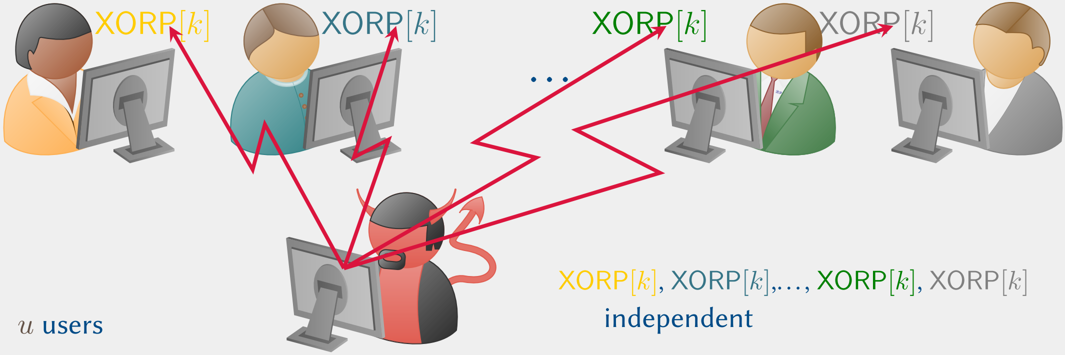
u users

q_{max} queries per user

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

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

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



XORP[k], XORP[k],..., XORP[k], XORP[k]
independent

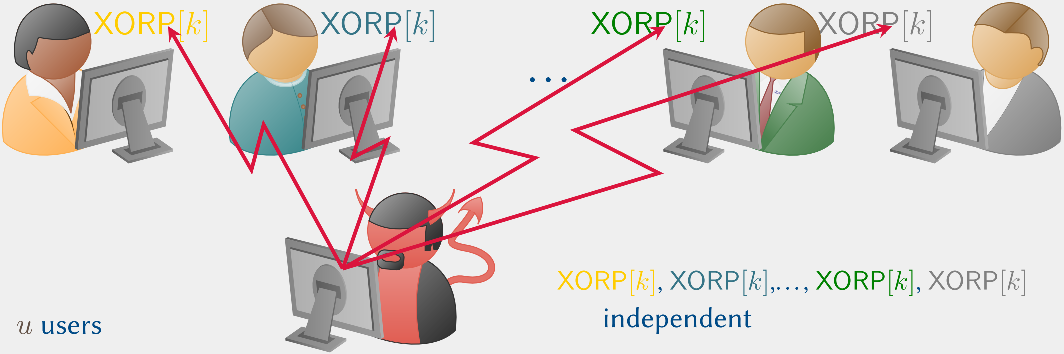
u users

q_{max} queries per user

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

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

Scale and growth of internet and other technologies is a concern



u users

XORP[k], XORP[k],..., XORP[k], XORP[k]
independent

q_{max} queries per user

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

AES: Secure for $uq_{max} < O(2^{96})$ (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 $q_{max} \sim O(2^n)$
  - Substantial improvement over $u \sim O(2^{\frac{n}{2}})$ and $q_{max} \sim O(2^{\frac{n}{2}})$

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)

- $\mathsf{XORP}[3]$ 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 $\mathsf{XORP}[3]$: 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 $q_{max} \sim O(2^n)$
  - 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
- XORP$'[3]$ provides same level of security

Presentation Outline

Setting

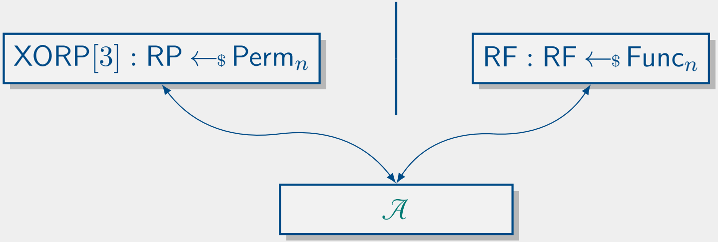
Func_n: All functions from $\{0,1\}^{n-2}$ to $\{0,1\}^n$.
Perm_n: All permutations from $\{0,1\}^n$ to $\{0,1\}^n$.

Security 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

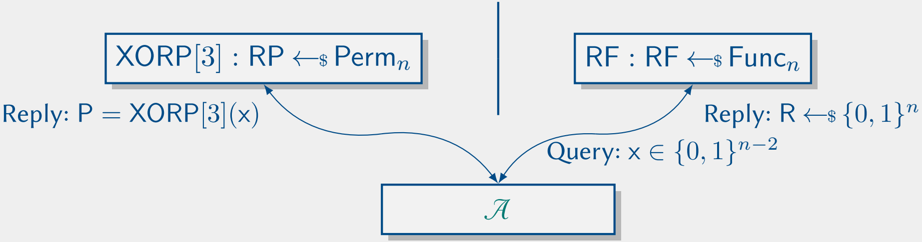


Security Notion: Indistinguishability

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

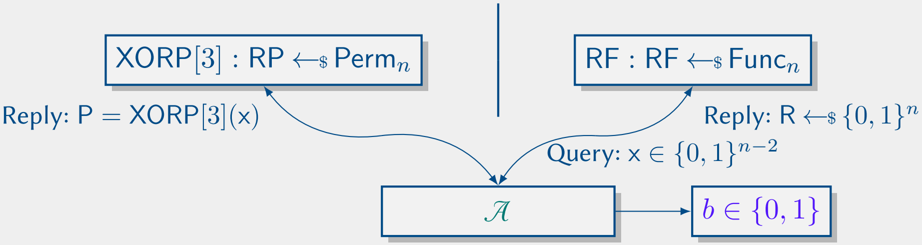


Security Notion: Indistinguishability

Setting

Func_n: All functions from $\{0,1\}^{n-2}$ to $\{0,1\}^n$.
Perm_n: All permutations from $\{0,1\}^n$ to $\{0,1\}^n$.

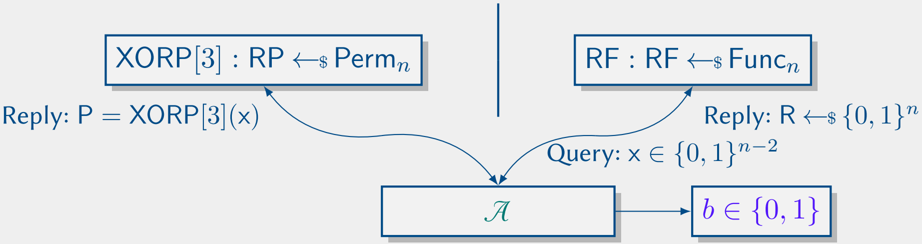
Security Game



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



Quantifying Security: Advantage

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[3]}(\mathscr{A}) := |\mathbf{Pr}[\mathscr{A}^{\mathsf{XORP}[3]} \rightarrow 1] - \mathbf{Pr}[\mathscr{A}^{\mathsf{RF}} \rightarrow 1]|$$

- Focus on information theoretic security of XORP[3].
  - $\mathcal{A}$ comuptationally 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 $\mathsf{XORP}[3]$.
  - $\mathcal{A}$ comuptationally 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.

$\mathsf{XORP}[3]$ transcript $\mathsf{P} := (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_q)$; RF transcript $\mathsf{R} := (\mathsf{R}_1, \mathsf{R}_2, \ldots, \mathsf{R}_q)$

$$\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$$

Setting

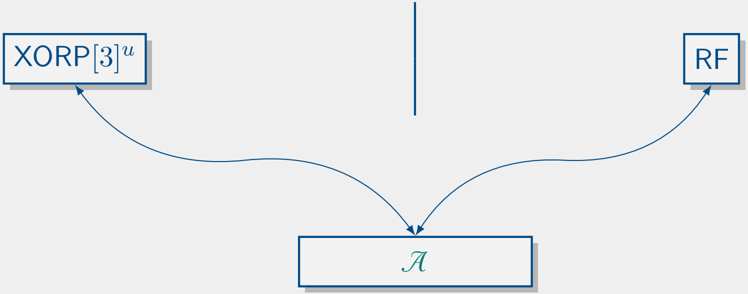
$\mathsf{Func}_n^u := \{f | f : [u] \times \{0,1\}^{n-2} \mapsto \{0,1\}^n\}$, $\mathsf{RF} \leftarrow_{\$} \mathsf{Func}_n^u$
$\mathsf{RP}_1, \mathsf{RP}_2, \ldots, \mathsf{RP}_u \leftarrow_{\$} \mathsf{Perm}_n$

Security Notion: Multi-user Indistinguishability

Setting

$\mathsf{Func}_n^u := \{f | f : [u] \times \{0,1\}^{n-2} \mapsto \{0,1\}^n\}$, $\mathsf{RF} \leftarrow_\$ \mathsf{Func}_n^u$
$\mathsf{RP}_1, \mathsf{RP}_2, \ldots, \mathsf{RP}_u \leftarrow_\$ \mathsf{Perm}_n$

Security Game



Setting

$\mathsf{Func}_n^u := \{f \mid f : [u] \times \{0,1\}^{n-2} \mapsto \{0,1\}^n\}, \mathsf{RF} \leftarrow_\$ \mathsf{Func}_n^u$

$\mathsf{RP}_1, \mathsf{RP}_2, \ldots, \mathsf{RP}_u \leftarrow_\$ \mathsf{Perm}_n$

Security Game

$= \mathsf{RP}_i(\mathsf{x}\|00) \oplus \mathsf{RP}_i(\mathsf{x}\|01) \oplus \mathsf{RP}_i(\mathsf{x}\|10)$

$\mathsf{XORP}[3]^u$

RF

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

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

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

$\mathcal{A}$

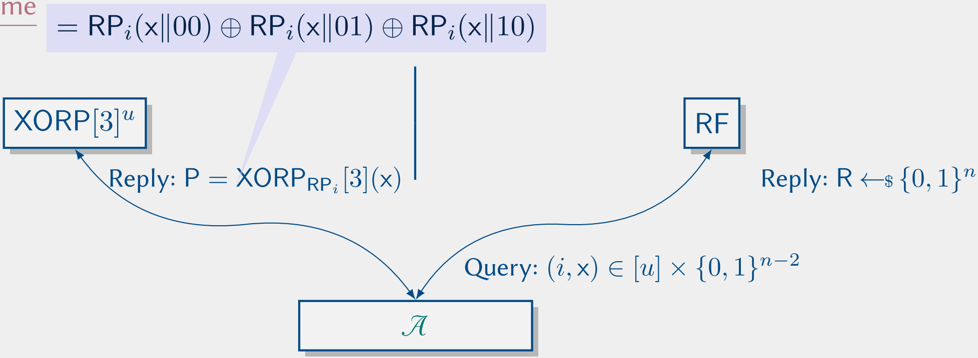
Security Notion: Multi-user Indistinguishability

Setting

$\mathsf{Func}_n^u := \{f \mid f : [u] \times \{0,1\}^{n-2} \mapsto \{0,1\}^n\}$, $\mathsf{RF} \leftarrow_\$ \mathsf{Func}_n^u$

$\mathsf{RP}_1, \mathsf{RP}_2, \ldots, \mathsf{RP}_u \leftarrow_\$ \mathsf{Perm}_n$

Security Game

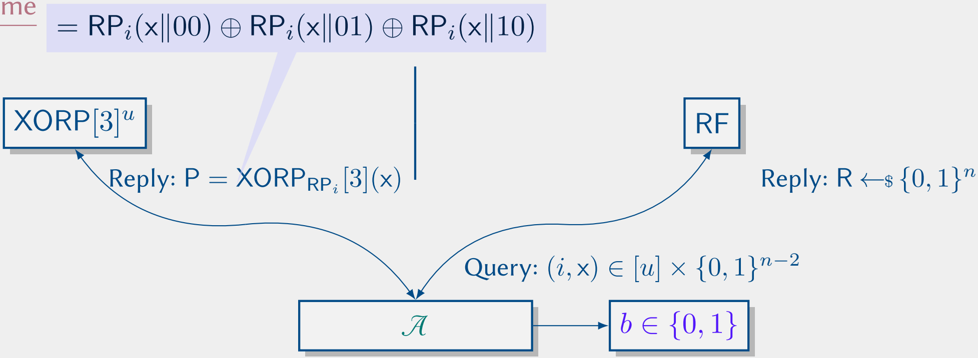


Setting

$\mathsf{Func}_n^u := \{f \mid f : [u] \times \{0,1\}^{n-2} \mapsto \{0,1\}^n\}, \mathsf{RF} \leftarrow_\$ \mathsf{Func}_n^u$

$\mathsf{RP}_1, \mathsf{RP}_2, \ldots, \mathsf{RP}_u \leftarrow_\$ \mathsf{Perm}_n$

Security Game

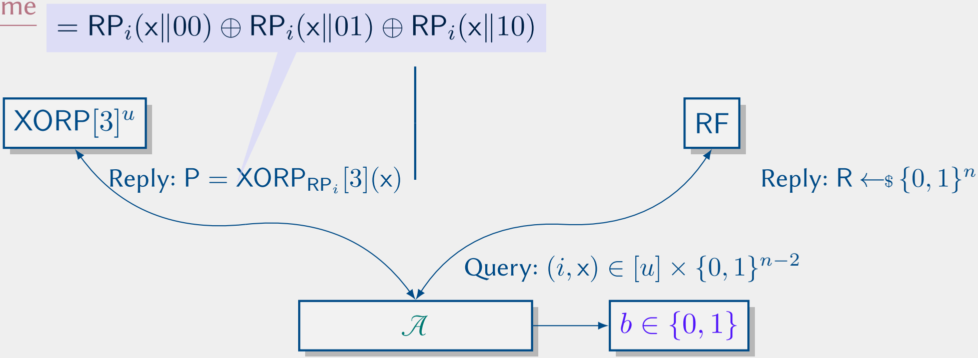


Security Notion: Multi-user Indistinguishability

Setting

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

Security Game



Quantifying Security: Advantage

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) := \left|\mathbf{Pr}[\mathcal{A}^{\mathsf{XORP}[3]^u} \rightarrow 1] - \mathbf{Pr}[\mathcal{A}^{\mathsf{RF}} \rightarrow 1]\right|$$

- 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.

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

$\mathsf{XORP}[3]^u$ transcript $\mathsf{P} := (\mathsf{P}_1, \mathsf{P}_2, \ldots, \mathsf{P}_q)$; RF transcript $\mathsf{R} := (\mathsf{R}_1, \mathsf{R}_2, \ldots, \mathsf{R}_q)$

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathscr{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$$

Our Contribution (Formal) and Application

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

Our Contribution (Formal) and Application

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

  - 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

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

  - 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

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

  - 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.

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

Our Contribution (Formal) and Application

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

  - 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.

- $\mathsf{Adv}^{\text{prf}}_{\mathsf{XORP}'[3]}(\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{\frac{3}{2}}}$
  - Multi-user analysis (not given) will produce similar type of bound as $\mathsf{XORP}[3]$.

Our Contribution (Formal) and Application

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

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

  - 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.

- $\mathsf{Adv}^{\mathrm{prf}}_{\mathsf{XORP}'[3]}(\mathcal{A}) \leq \frac{5\sqrt{q}}{N} + \frac{256q}{N^2} + \frac{8192q}{N^{\frac{3}{2}}}$
  - Multi-user analysis (not given) will produce similar type of bound as $\mathsf{XORP}[3]$.

Our Contribution (Formal) and Application

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

  [Hoang and Shen, 2020]: $\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[2]}(\mathcal{A}) = O\left(\frac{\sqrt{n}q}{2^n}\right)$

  - 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.

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

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

  [Cogliati, 2018]: $\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}'[2]}(\mathcal{A}) = O\left(\frac{q}{2^n}\right)$

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

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

  - 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.

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

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

  [Cogliati, 2018]: $\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}'[2]}(\mathcal{A}) = O\left(\frac{q}{2^n}\right)$

Application

Counter-mode encryption using $\mathsf{XORP}[3]$

Our Contribution (Formal) and Application

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

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

  - 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.

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

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

  [Cogliati, 2018]: $\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}'[2]}(\mathcal{A}) = O\left(\frac{q}{2^n}\right)$

Application

Counter-mode encryption using $\mathsf{XORP}[3]$

- Multi-user security similar to $\mathsf{XORP}[3]$ (when instantiated with a good block cipher)
- [Bellare et al., 1999]: Parity-method encryption
  - similar security, but requires additional randomness

Our Technique: χ^2-method

- $\mathsf{X}^q := (\mathsf{X}_1, \ldots, \mathsf{X}_q) \sim \mathrm{Pr}_{\mathsf{X}}$, and $\mathsf{Z}^q := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q) \sim \mathrm{Pr}_{\mathsf{Z}}$ over $\Omega \times \cdots \times \Omega$.
- $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}_1 = \mathsf{x}_1, \ldots, \mathsf{X}_{i-1} = \mathsf{x}_{i-1}]$,
  $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{Z}_i = \mathsf{x}_i \mid \mathsf{Z}_1 = \mathsf{x}_1, \ldots, \mathsf{Z}_{i-1} = \mathsf{x}_{i-1}]$.

Our Technique: χ^2-method

- $\mathsf{X}^q := (\mathsf{X}_1, \ldots, \mathsf{X}_q) \sim \mathrm{Pr}_{\mathsf{X}}$, and $\mathsf{Z}^q := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q) \sim \mathrm{Pr}_{\mathsf{Z}}$ over $\Omega \times \cdots \times \Omega$.
- $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}_1 = \mathsf{x}_1, \ldots, \mathsf{X}_{i-1} = \mathsf{x}_{i-1}]$,
  $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{Z}_i = \mathsf{x}_i \mid \mathsf{Z}_1 = \mathsf{x}_1, \ldots, \mathsf{Z}_{i-1} = \mathsf{x}_{i-1}]$.
- $\chi^2(\mathsf{x}_i) := \chi^2(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}, \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}) = \sum_{x_i \in \Omega} \frac{(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) - \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i))^2}{\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i)}$

Our Technique: χ^2-method

- $\mathsf{X}^q := (\mathsf{X}_1, \ldots, \mathsf{X}_q) \sim \Pr_{\mathsf{X}}$, and $\mathsf{Z}^q := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q) \sim \Pr_{\mathsf{Z}}$ over $\Omega \times \cdots \times \Omega$.
- $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}_1 = \mathsf{x}_1, \ldots, \mathsf{X}_{i-1} = \mathsf{x}_{i-1}]$,
  $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{Z}_i = \mathsf{x}_i \mid \mathsf{Z}_1 = \mathsf{x}_1, \ldots, \mathsf{Z}_{i-1} = \mathsf{x}_{i-1}]$.
- $\chi^2(\mathsf{x}_i) := \chi^2(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}, \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}) = \sum_{x_i \in \Omega} \frac{(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) - \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i))^2}{\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i)}$

Theorem ([Dai et al., 2017])

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

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

Our Technique: χ^2-method

- $\mathsf{X}^q := (\mathsf{X}_1, \ldots, \mathsf{X}_q) \sim \mathrm{Pr}_{\mathsf{X}}$, and $\mathsf{Z}^q := (\mathsf{Z}_1, \ldots, \mathsf{Z}_q) \sim \mathrm{Pr}_{\mathsf{Z}}$ over $\Omega \times \cdots \times \Omega$.
- $\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \mathsf{X}_1 = \mathsf{x}_1, \ldots, \mathsf{X}_{i-1} = \mathsf{x}_{i-1}]$,
  $\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i) := \mathbf{Pr}[\mathsf{Z}_i = \mathsf{x}_i \mid \mathsf{Z}_1 = \mathsf{x}_1, \ldots, \mathsf{Z}_{i-1} = \mathsf{x}_{i-1}]$.
- $\chi^2(\mathsf{x}_i) := \chi^2(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}, \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}) = \sum_{x_i \in \Omega} \frac{(\mathbf{Pr}_{\mathsf{X}|\mathsf{x}^{i-1}}(\mathsf{x}_i) - \mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i))^2}{\mathbf{Pr}_{\mathsf{Z}|\mathsf{x}^{i-1}}(\mathsf{x}_i)}$

Theorem ([Dai et al., 2017])

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

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

Effectively applied in [Bhattacharya and Nandi, 2018b, Bhattacharya and Nandi, 2018a, Choi et al., 2019, Mennink, 2019, Gunsing and Mennink, 2020].

Presentation Outline

Applying the χ^2-method: Problem Due to Adaptive Choice

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathscr{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$$

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \quad \leq \quad ?$$

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \ \leq \ ?$$

Can we apply the χ^2-method to upper bound $\|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$?

$$\mathsf{Adv}^{\text{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \leq \; ?$$

Can we apply the χ^2-method to upper bound $\|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$?

User of the i-th query

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

Can not apply the χ^2-method directly

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \leq \ ?$$

Can we apply the χ^2-method to upper bound $\|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$?

User of the i-th query

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

Can not apply the χ^2-method directly

Is there a way round?

$$\mathsf{Adv}^{\mathrm{mu\_prf}}_{\mathsf{XORP}[3]}(\mathcal{A}) \leq \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \leq \; ?$$

Can we apply the χ^2-method to upper bound $\|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\|$?

User of the i-th query

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

Can not apply the χ^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 ...

A Solution: Reordering the Transcript

Random Experiment for U

$\mathsf{U} := (\mathsf{U}_i : i \in [q]) \xleftarrow{\text{wr}} \mathcal{G}$
return U

Random Experiment for S

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

A Solution: Reordering the Transcript

Random Experiment for U

$\mathsf{U} := (\mathsf{U}_i : i \in [q]) \xleftarrow{\text{wr}} \mathcal{G}$

return U

Random Experiment for S

for $1 \leq i \leq u$

$\quad \widehat{\mathsf{T}}_i := (\mathsf{T}_{j,k} : j \in [\mathrm{I}_i], k \in [3]) \xleftarrow{\text{wor}} \mathcal{G}$

/ $\widehat{\mathsf{T}}_i$ is sampled independent of $\widehat{\mathsf{T}}_j,\ 1 \leq j \leq i-1$

for $1 \leq \ell \leq q$

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

return $\mathsf{S} := (\mathsf{S}_\ell : \ell \in [q])$

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

Random Experiment for U

$\mathsf{U} := (\mathsf{U}_i : i \in [q]) \xleftarrow{\text{wr}} \mathcal{G}$

return U

Random Experiment for S

for $1 \le i \le u$

$\quad \widehat{\mathsf{T}}_i := (\mathsf{T}_{j,k} : j \in [\mathrm{I}_i], k \in [3]) \xleftarrow{\text{wor}} \mathcal{G}$

/ $\widehat{\mathsf{T}}_i$ is sampled independent of $\widehat{\mathsf{T}}_j$, $1 \le j \le i-1$

for $1 \le \ell \le q$

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

return $\mathsf{S} := (\mathsf{S}_\ell : \ell \in [q])$

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

Reordering P to S:

$$\mathsf{S} = \overbrace{\mathsf{S}_1, \mathsf{S}_2, \ldots, \mathsf{S}_{q_{max}}}^{U_1}, \underbrace{\mathsf{S}_{q_{max}+1} \ldots, \mathsf{S}_{2q_{max}}}_{U_2}, \ldots, \overbrace{\mathsf{S}_{(u-1)q_{max}+1} \ldots, \mathsf{S}_{q=uq_{max}}}^{U_u}$$

Two Observations

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

Reordering (Contd.)

Two Observations

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

Makes reordering possible

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

(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.
- $\mathscr{A}$ makes same number ($= q_{max}$) of queries to each user.

Makes reordering possible

(In S) U_i is uniquely determined by i

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

So, in particular

$$\mathbf{Pr}\{\overbrace{\mathsf{S}_{i=(j-1)q_{max}+k}}^{U=j}|\overbrace{\mathsf{S}_1,\ldots,\mathsf{S}_{q_{max}}}^{U=1},\underbrace{\mathsf{S}_{q_{max}+1}\ldots,\mathsf{S}_{2q_{max}}}_{U=2},\ldots,\overbrace{\mathsf{S}_{(j-1)q_{max}+1}\ldots,\mathsf{S}_{i-1}}^{U=j}\}$$

$$= \mathbf{Pr}\{\overbrace{\mathsf{S}_i}^{U=j}|\overbrace{\mathsf{S}_{(j-1)q_{max}+1}\ldots,\mathsf{S}_{i-1}}^{U=j}\}$$ (RP_j is independent of RP_1, $\mathsf{RP}_2, \ldots$)

Two Observations

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

Makes reordering possible

(In S) U_i is uniquely determined by i

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

So, in particular

$$\mathbf{Pr}\{\overbrace{\mathsf{S}_{i=(j-1)q_{max}+k}}^{U=j} | \overbrace{\mathsf{S}_1, \ldots, \mathsf{S}_{q_{max}}}^{U=1}, \underbrace{\mathsf{S}_{q_{max}+1} \ldots, \mathsf{S}_{2q_{max}}}_{U=2}, \ldots, \overbrace{\mathsf{S}_{(j-1)q_{max}+1} \ldots, \mathsf{S}_{i-1}}^{U=j}\}$$

$$= \mathbf{Pr}\{\overbrace{\ \mathsf{S}_i\ }^{U=j} | \overbrace{\mathsf{S}_{(j-1)q_{max}+1} \ldots, \mathsf{S}_{i-1}}^{U=j}\} \quad (\mathsf{RP}_j \text{ is independent of } \mathsf{RP}_1, \mathsf{RP}_2, \ldots)$$

This is needed for the application of the χ^2-method

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

(In S) 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

$$\mathbf{Pr}\{\overbrace{\mathsf{S}_{i=(j-1)q_{max}+k}}^{U=j} | \overbrace{\mathsf{S}_1, \ldots, \mathsf{S}_{q_{max}}}^{U=1}, \underbrace{\mathsf{S}_{q_{max}+1} \ldots, \mathsf{S}_{2q_{max}}}_{U=2}, \ldots, \overbrace{\mathsf{S}_{(j-1)q_{max}+1} \ldots, \mathsf{S}_{i-1}}^{U=j}\}$$

$$= \mathbf{Pr}\{\overbrace{\mathsf{S}_i}^{U=j} | \overbrace{\mathsf{S}_{(j-1)q_{max}+1} \ldots, \mathsf{S}_{i-1}}^{U=j}\}$$ (RP_j is independent of RP_1, $\mathsf{RP}_2, \ldots$)

This is needed for the application of the χ^2-method

Reordering preserves statistical distance: $\|\mathbf{Pr}_\mathsf{S} - \mathbf{Pr}_\mathsf{U}\| = \|\mathbf{Pr}_\mathsf{P} - \mathbf{Pr}_\mathsf{R}\|$

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

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 $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

S and U are marginals of X and Y resp.

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

Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of $\mathsf{S} \subseteq$ Support of U?

How to ensure?

S and U are marginals of X and Y resp.

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

How to extend?

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

S and U are marginals of X and Y resp.

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

How to extend?

$$\left.\begin{aligned} \mathsf{X}_i &= (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i) \\ \mathsf{Y}_i &= (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_i) \end{aligned}\right\} \text{ for all } i \in [q]$$

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

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.*

How to extend?

$\mathsf{S}_i = \mathsf{T}_{i,1} + \mathsf{T}_{i,2} + \mathsf{T}_{i,3}$

$$\left.\begin{aligned} \mathsf{X}_i &= (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i) \\ \mathsf{Y}_i &= (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_i) \end{aligned}\right\} \text{for all } i \in [q]$$

Extending the Transcripts: Ensuring the Support Condition

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

S and U are marginals of X and Y resp.

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

How to extend?

$\mathsf{S}_i = \mathsf{T}_{i,1} + \mathsf{T}_{i,2} + \mathsf{T}_{i,3}$

$$\left.\begin{aligned} \mathsf{X}_i &= (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i) \\ \mathsf{Y}_i &= (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_i) \end{aligned}\right\} \text{ for all } i \in [q]$$

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

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

S *and* U *are marginals of* X *and* Y *resp.*

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

How to extend?

$\mathsf{S}_i = \mathsf{T}_{i,1} + \mathsf{T}_{i,2} + \mathsf{T}_{i,3}$

$$\left.\begin{aligned} \mathsf{X}_i &= (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i) \\ \mathsf{Y}_i &= (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_i) \end{aligned}\right\} \text{ for all } i \in [q]$$

$\mathsf{V}_{i,3} = \mathsf{V}_{i,1} + \mathsf{V}_{i,2} + \mathsf{U}_i$

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

Enough to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$

Can χ^2-method be applied to upper bound $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\|$?

Support of S $\subseteq$ Support of U?

How to ensure?

S *and* U *are marginals of* X *and* Y *resp.*

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

How to extend?

$\mathsf{S}_i = \mathsf{T}_{i,1} + \mathsf{T}_{i,2} + \mathsf{T}_{i,3}$

$$\left.\begin{aligned} \mathsf{X}_i &= (\mathsf{T}_{i,1}, \mathsf{T}_{i,2}, \mathsf{S}_i) \\ \mathsf{Y}_i &= (\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{U}_i) \end{aligned}\right\} \text{ for all } i \in [q]$$

$\mathsf{V}_{i,3} = \mathsf{V}_{i,1} + \mathsf{V}_{i,2} + \mathsf{U}_i$

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

What are $\mathsf{V}_{i,1}, \mathsf{V}_{i,2}$?

Extending the Transcripts: Details

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

$U_i = j$

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

$U_i = j$

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

$$n_i = \Bigg\{ (\mathsf{v}_1, \mathsf{v}_2) \Bigg| \; \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \; \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \Bigg\}$$

$U_i = j$

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

All previous samples of the j-th user

$$\mathcal{n}_i = \left\{ (\mathsf{v}_1, \mathsf{v}_2) \;\middle|\; \begin{array}{l} \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup\limits_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \\ \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \end{array} \right\}$$

$U_i = j$

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

All previous samples of the j-th user

$$\mathcal{N}_i = \Bigg\{ (\mathsf{v}_1, \mathsf{v}_2) \Bigg| \; \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \; \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \Bigg\}$$

$$(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) \leftarrow_{\$} \mathcal{N}_i$$

$U_i = j$

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

$$\mathcal{n}_i = \left\{ (\mathsf{v}_1, \mathsf{v}_2) \middle| \begin{array}{l} \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \\ \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \end{array} \right\}$$

All previous samples of the j-th user

$$(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) \leftarrow_{\$} \mathcal{n}_i$$

After Extension

- Support of X $=$ Support of Y

$U_i = j$

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

All previous samples of the j-th user

$$\mathcal{N}_i = \left\{ (\mathsf{v}_1, \mathsf{v}_2) \;\middle|\; \begin{array}{l} \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \\ \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \end{array} \right\}$$

$$(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) \leftarrow_{\$} \mathcal{N}_i$$

After Extension

- Support of X $=$ Support of Y
- S and U are marginals of X and Y (resp.) $\Rightarrow$ $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| \leq \|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\|$

Extending the Transcripts: Details

$U_i = j$

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

$$\mathcal{N}_i = \left\{ (\mathsf{v}_1, \mathsf{v}_2) \middle| \begin{array}{l} \mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\}, \\ \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \end{array} \right\}$$

All previous samples of the j-th user

$$(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) \leftarrow_{\$} \mathcal{N}_i$$

After Extension

- Support of X $=$ Support of Y
- S and U are marginals of X and Y (resp.) $\Rightarrow$ $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| \le \|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\|$

$U_i = j$

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

$$\mathcal{n}_i = \Big\{ (\mathsf{v}_1, \mathsf{v}_2) \mid$$

All previous samples of the j-th user

$$\mathsf{v}_1, \mathsf{v}_2, \mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2 \in \mathcal{G} \setminus \bigcup_{i=(j-1)q_{max}+1}^{(j-1)q_{max}+k-1} \{\mathsf{V}_{i,1}, \mathsf{V}_{i,2}, \mathsf{V}_{i,3}\},$$

$$\mathsf{U}_i + \mathsf{v}_1 + \mathsf{v}_2, \mathsf{v}_1, \mathsf{v}_2 \text{ distinct} \Big\}$$

$$(\mathsf{V}_{i,1}, \mathsf{V}_{i,2}) \leftarrow_{\$} \mathcal{n}_i$$

After Extension

- Support of X $=$ Support of Y
- S and U are marginals of X and Y (resp.) $\Rightarrow$ $\|\mathbf{Pr}_{\mathsf{S}} - \mathbf{Pr}_{\mathsf{U}}\| \leq \|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\|$

Apply χ^2-method to upper bound $\|\mathbf{Pr}_{\mathsf{X}} - \mathbf{Pr}_{\mathsf{Y}}\|$

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$

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

$\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}$, $\widehat{\mathsf{X}}_j$ = block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1}$ = block of first $k-1$ X_i's for the j-th user.

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$

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

$\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}$, $\widehat{\mathsf{X}}_j =$ block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1} =$ block of first $k-1$ X_i's for the j-th user.

Conditional Probabilities Under $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\stackrel{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\
&= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}], \\
&\quad \text{since } (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) \text{ is independent of } \widehat{\mathsf{X}}_j^{k-1} \text{ and } \widehat{\mathsf{X}}_{j,k} \\
&= \frac{1}{(N - 3(k-1))^3}
\end{aligned}$$

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$

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

$\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}$, $\widehat{\mathsf{X}}_j =$ block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1} =$ block of first $k-1$ X_i's for the j-th user.

Conditional Probabilities Under $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$

$$\begin{aligned}\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\stackrel{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\ &= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}],\end{aligned}$$

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

Due to reordering.

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

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$ $\qquad$ $i = (j-1)q_{max} + k \Rightarrow$ i-th query $=$ j-th user's k-th query

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$ $\qquad$ $\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}$, $\quad \widehat{\mathsf{X}}_j =$ block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1} =$ block of first $k-1$ X_i's for the j-th user.

Conditional Probabilities Under $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\stackrel{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\
&= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}],
\end{aligned}$$

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

Due to reordering.

$$= \frac{1}{(N - 3(k-1))^{\underline{3}}}$$

Falling factorial

χ^2-Method: Steps

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$ $\qquad i = (j-1)q_{max} + k \Rightarrow$ i-th query $= j$-th user's k-th query

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$ $\qquad \mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}, \quad \widehat{\mathsf{X}}_j =$ block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1} =$ block of first $k-1$ X_i's for the j-th user.

Conditional Probabilities Under $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\stackrel{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\
&= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}],
\end{aligned}$$

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

Due to reordering.

$$= \frac{1}{(N-3(k-1))^{\underline{3}}}$$

Falling factorial

Similarly for $\mathbf{Pr}_{\mathsf{Y}}$

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

Setting

$\mathsf{X}_1, \ldots, \mathsf{X}_q \sim \mathbf{Pr}_{\mathsf{X}}$

$\mathsf{Y}_1, \ldots, \mathsf{Y}_q \sim \mathbf{Pr}_{\mathsf{Y}}$

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

$\mathsf{X}_i = \widehat{\mathsf{X}}_{j,k}$, $\widehat{\mathsf{X}}_j =$ block of X_i's for the j-th user

$\widehat{\mathsf{X}}_j^{k-1} =$ block of first $k-1$ X_i's for the j-th user.

Conditional Probabilities Under $\mathbf{Pr}_{\mathsf{X}}$ and $\mathbf{Pr}_{\mathsf{Y}}$

$$\begin{aligned}
\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) &\stackrel{\text{def}}{=} \mathbf{Pr}[\mathsf{X}_i = \mathsf{x}_i \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}, (\mathsf{X}^{i-1} \setminus \widehat{\mathsf{X}}_j) = (\mathsf{x}^{i-1} \setminus \widehat{\mathsf{x}}_j^{k-1})] \\
&= \mathbf{Pr}[\widehat{\mathsf{X}}_{j,k} = \widehat{\mathsf{x}}_{j,k} \mid \widehat{\mathsf{X}}_j^{k-1} = \widehat{\mathsf{x}}_j^{k-1}],
\end{aligned}$$

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

Due to reordering.

$$= \frac{1}{(N - 3(k-1))_3}$$

Falling factorial

Similarly for $\mathbf{Pr}_{\mathsf{Y}}$

$$\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i \mid \mathsf{x}^{i-1}) = \frac{1}{N} \times \frac{1}{|\eta^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})|}$$

Same as η_i

χ^2 distance and its expectation

$$\chi^2(\mathsf{x}^{i-1}) := \sum_{\mathsf{x}_i=(\mathsf{v}_{i,1},\mathsf{v}_{i,2},\mathsf{u}_i)} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1})} = C \times \sum_{\mathsf{u}_i\in\{0,1\}^n} (|n^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D)$$

χ^2 distance and its expectation

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

$$\chi^2(\mathsf{x}^{i-1}) := \sum_{\mathsf{x}_i=(\mathsf{v}_{i,1},\mathsf{v}_{i,2},\mathsf{u}_i)} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1})} = C \times \sum_{\mathsf{u}_i\in\{0,1\}^n} (|n^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D)$$

χ^2 distance and its expectation

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

$$\chi^2(\mathsf{x}^{i-1}) := \sum_{\mathsf{x}_i=(\mathsf{v}_{i,1},\mathsf{v}_{i,2},\mathsf{u}_i)} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1})} = C \times \sum_{\mathsf{u}_i\in\{0,1\}^n} (|n^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D)$$

$$\Downarrow$$

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \;=\; C \times \sum_{\mathsf{u}_i} \mathbf{Ex}[(|n^{\mathsf{u}_i}(\widehat{\mathsf{X}}_j^{k-1})| - D)^2].$$

χ^2 distance and its expectation

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

$$\chi^2(\mathsf{x}^{i-1}) := \sum_{\mathsf{x}_i=(\mathsf{v}_{i,1},\mathsf{v}_{i,2},\mathsf{u}_i)} \frac{(\mathbf{Pr}_{\mathsf{X}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}) - \mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1}))^2}{\mathbf{Pr}_{\mathsf{Y}}(\mathsf{x}_i|\widehat{\mathsf{x}}_j^{k-1})} = C \times \sum_{\mathsf{u}_i\in\{0,1\}^n} (|n^{\mathsf{u}_i}(\widehat{\mathsf{x}}_j^{k-1})| - D)$$

$$\Downarrow$$

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] = C \times \sum_{\mathsf{u}_i} \mathbf{Ex}[(|n^{\mathsf{u}_i}(\widehat{\mathsf{X}}_j^{k-1})| - D)^2].$$

Goal is to compute $\mathbf{Ex}[(|n^{\mathsf{u}_i}(\widehat{\mathsf{X}}_j^{k-1})| - D)^2]$

Finishing the Proof: An Important Lemma

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

For $\mathsf{u} \in \mathcal{G}$

$$\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}$$

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 $\mathsf{u} \in \mathcal{G}$

$$\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}|$$

Finishing the Proof: An Important Lemma

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

For $\mathsf{u} \in \mathcal{G}$

Same as $\mathcal{N}^{\mathsf{u}_i}(\widehat{\mathsf{X}}_j^{k-1})$

$$\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}|$$

Finishing the Proof: An Important Lemma

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

For $\mathsf{u} \in \mathcal{G}$

$$\mathbf{N}_r^{\mathsf{u}} := |\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}|$$

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 $\mathsf{u} \in \mathcal{G}$

$$\mathbf{N}_r^{\mathsf{u}} := |\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}|$$

To compute $\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2]$

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

For $\mathsf{u} \in \mathcal{G}$

$$\mathbf{N}_r^{\mathsf{u}} := |\{(\mathsf{g}_1, \mathsf{g}_2) \in \mathcal{V}_r \times \mathcal{V}_r : \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2 \in \mathcal{V}_r; \mathsf{u}, \mathsf{g}_1, \mathsf{g}_2 \text{ distinct}\}|$$

To compute $\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2]$

Computation of $\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}]$:

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

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

$$\mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}] = \mathbf{Ex}[\sum_{\mathsf{g} \in \mathcal{G}_{\mathsf{u}}} \mathrm{I}_{\mathsf{g}}] = \sum_{\mathsf{g} \in \mathcal{G}_{\mathsf{u}}} \mathbf{Ex}[\mathrm{I}_{\mathsf{g}}] = \mathbf{Pr}[\{\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2\} \subseteq \mathcal{V}_r] = \frac{r^{\underline{3}}}{N} = D.$$

From expectation to variance:

$$\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2] = \mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - \mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}])^2] = \mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$$

From expectation to variance:

$$\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2] = \mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - \mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}])^2] = \mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$$

To compute $\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2] \quad \Rightarrow \quad$ To compute $\mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$

How to compute $\mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$?

From expectation to variance:

$$\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2] = \mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - \mathbf{Ex}[\mathbf{N}_r^{\mathsf{u}}])^2] = \mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$$

To compute $\mathbf{Ex}[(\mathbf{N}_r^{\mathsf{u}} - D)^2] \quad \Rightarrow \quad$ To compute $\mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$

How to compute $\mathbf{Var}[\mathbf{N}_r^{\mathsf{u}}]$?

Setting:

$$\text{For } \mathsf{g} = (\mathsf{g}_1, \mathsf{g}_2), \qquad \mathcal{S}_{\mathsf{u}}^{\mathsf{g}} = \{\mathsf{g}_1, \mathsf{g}_2, \mathsf{u} + \mathsf{g}_1 + \mathsf{g}_2\}$$

Observation:

$$w = |\mathcal{S}_{\mathsf{u}}^{\mathsf{g}} \cup \mathcal{S}_{\mathsf{u}}^{\mathsf{g}'}| \in \{3, 5, 6\}$$

Technicalities:

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

$$\mathbf{Var}[\mathrm{I}_{\mathsf{g}}] = \mathbf{Ex}[\mathrm{I}_{\mathsf{g}}](1 - \mathbf{Ex}[\mathrm{I}_{\mathsf{g}}])$$

$$\mathbf{Cov}(\mathrm{I}_{\mathsf{g}}, \mathrm{I}_{\mathsf{g}'}) = \mathbf{Ex}[\mathrm{I}_{\mathsf{g}}\mathrm{I}_{\mathsf{g}'}] - \mathbf{Ex}[\mathrm{I}_{\mathsf{g}}]\mathbf{Ex}[\mathrm{I}_{\mathsf{g}'}]$$

$$\boxed{\leq \frac{6r^2(r-1)(r-2)}{N^2}}$$

$w = 3$

$$\boxed{\leq \frac{30r^2(r-1)(r-2)}{N^2}}$$

$w \in \{5, 6\}$

$$\boxed{\leq \frac{4^8(r')^3}{27CN^6}}$$

$$+$$

$$\mathbf{Var}[\mathrm{N}_r^{\mathsf{u}}] \leq \frac{576}{N^3} + \frac{4^8(r')^3}{27CN^6}$$

$$\Downarrow$$

$$\mathbf{Ex}[\chi^2(\mathsf{X}^{i-1})] \leq \frac{576}{N^2} + \frac{4^8(r')^3}{27CN^5} \Rightarrow \|\mathbf{Pr}_{\mathsf{P}} - \mathbf{Pr}_{\mathsf{R}}\| \leq \frac{20\sqrt{uq_{max}}}{N}$$

- 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 $O(\frac{1}{\sqrt{2^n}})$ 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 $O(\frac{1}{\sqrt{2^n}})$ 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 $O(\frac{1}{\sqrt{2^n}})$ 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

Bellare, M., Goldreich, O., and Krawczyk, H. (1999).
Stateless evaluation of pseudorandom functions: Security beyond the birthday barrier.
In Wiener, M. J., editor, *Advances in Cryptology - CRYPTO '99*, volume 1666 of *LNCS*, pages 270–287. Springer.

Bellare, M. and Impagliazzo, R. (1999).
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.

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

Bhattacharya, S. and Nandi, M. (2018a).
Full indifferentiable security of the xor of two or more random permutations using the χ^2-method.
In Nielsen, J. B. and Rijmen, V., editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 387–412, Cham. Springer International Publishing.

Bhattacharya, S. and Nandi, M. (2018b).
Revisiting variable output length XOR pseudorandom function.
IACR Transactions on Symmetric Cryptology, 2018(1):314–335.

Choi, W., Lee, B., and Lee, J. (2019).
Indifferentiability of truncated random permutations.
In Galbraith, S. D. and Moriai, S., editors, *Advances in Cryptology - ASIACRYPT 2019*, volume 11921 of *LNCS*, pages 175–195.

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

COGLIATI, B., LAMPE, R., AND PATARIN, J. (2014).
THE INDISTINGUISHABILITY OF THE XOR OF K PERMUTATIONS.
In Cid, C. and Rechberger, C., editors, *FSE 2014*, volume 8540 of *LNCS*, pages 285–302. Springer.

DAI, W., HOANG, V. T., AND TESSARO, S. (2017).
INFORMATION-THEORETIC INDISTINGUISHABILITY VIA THE CHI-SQUARED METHOD.
In Katz, J. and Shacham, H., editors, *Advances in Cryptology - CRYPTO 2017*, volume 10403 of *LNCS*, pages 497–523. Springer.

GUNSING, A. AND MENNINK, B. (2020).
THE SUMMATION-TRUNCATION HYBRID: REUSING DISCARDED BITS FOR FREE.
In Micciancio, D. and Ristenpart, T., editors, *Advances in Cryptology - CRYPTO 2020*, volume 12170 of *LNCS*, pages 187–217. Springer.

HOANG, V. T. AND SHEN, Y. (2020).
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.

Iwata, T. (2006).
New blockcipher modes of operation with beyond the birthday bound security.
In Robshaw, M. J. B., editor, *FSE 2006*, volume 4047 of *LNCS*, pages 310–327. Springer.

Iwata, T., Minematsu, K., Peyrin, T., and Seurin, Y. (2017).
ZMAC: A fast tweakable block cipher mode for highly secure message authentication.
IACR Cryptology ePrint Archive, 2017:535.

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

Lucks, S. (2000).
The sum of PRPs is a secure PRF.
In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 470–484. Springer.

Mennink, B. (2019).
Linking Stam's bounds with generalized truncation.
In Matsui, M., editor, *Topics in Cryptology - CT-RSA 2019*, volume 11405 of *LNCS*, pages 313–329. Springer.

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

Patarin, J. (2008).
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.

Patarin, J. (2010).
Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography.
Cryptology ePrint Archive, Report 2017/287.
http://eprint.iacr.org/2010/287.

YASUDA, K. (2011).
A new variant of PMAC: beyond the birthday bound.
In *CRYPTO 2011*, pages 596–609.