Revisiting Variable Output Length XOR Pseudorandom Function

Srimanta Bhattacharya and Mridul Nandi

Indian Statistical Institute, Kolkata.

Fast Software Encryption 2018
Bruges, Belgium
March, 2018

Outline

Basic Problem:

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$
- Goal is to generate a pseudorandom sample of size σ.

Total variation distance from a truly random WR sample is negligible

Basic Problem:

- Let $\mathcal{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathcal{G}$
- Goal is to generate a pseudorandom sample of size σ.

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$
- Goal is to generate a pseudorandom sample of size σ.
  - The original sample (with $\sigma = \bar{\sigma}$) ?

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$
- Goal is to generate a pseudorandom sample of size σ.
  - The original sample (with $\sigma = \bar{\sigma}$) ?
    - Distance between a random WOR sample and a random WR sample $\approx \frac{\sigma(\sigma-1)}{2N}$.

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$
- Goal is to generate a pseudorandom sample of size σ.
  - The original sample (with $\sigma = \bar{\sigma}$) ?
    - Distance between a random WOR sample and a random WR sample $\approx \frac{\sigma(\sigma-1)}{2N}$.

Negligible only when $\sigma << \sqrt{N}$

Basic Problem:

- Let $\mathscr{G}$ be a set of size N.
- Given a without replacement (WOR) random sample of size $\bar{\sigma}$ from $\mathscr{G}$
- Goal is to generate a pseudorandom sample of size σ.
  - The original sample (with $\sigma = \bar{\sigma}$) ?
    - Distance between a random WOR sample and a random WR sample $\approx \frac{\sigma(\sigma-1)}{2N}$.

Can we generate a pseudorandom sample for which the total variation distance becomes negligible even for $\sigma > \sqrt{N}$?

"Luby-Rackoff backwards" (PRFs from PRPs) Bellare et al., 2000.

"Luby-Rackoff backwards" (PRFs from PRPs) Bellare et al., 2000.

- Block cipher based PRFs.
  Bellare et al., 2000, Nandi, 2009, Iwata and Kurosawa, 2003, Black and Rogaway, 2002, Luykx et al., 2016.

"Luby-Rackoff backwards" (PRFs from PRPs) Bellare et al., 2000.

- Block cipher based PRFs.
  Bellare et al., 2000, Nandi, 2009, Iwata and Kurosawa, 2003, Black and Rogaway, 2002, Luykx et al., 2016.
- PMAC_Plus Yasuda, 2011, Datta et al., 2017, LightMAC+ Naito, 2017 and 3kf9 Zhang et al., 2012.

Birthday bound security

"Luby-Rackoff backwards" (PRFs from PRPs) Bellare et al., 2000.

- Block cipher based PRFs.
  Bellare et al., 2000, Nandi, 2009, Iwata and Kurosawa, 2003, Black and Rogaway, 2002, Luykx et al., 2016.
- PMAC_Plus Yasuda, 2011, Datta et al., 2017, LightMAC+ Naito, 2017 and 3kf9 Zhang et al., 2012.

"Luby-Rackoff backwards" (PRFs from PRPs) Bellare et al., 2000.

- Block cipher based PRFs.
  Bellare et al., 2000, Nandi, 2009, Iwata and Kurosawa, 2003, Black and Rogaway, 2002, Luykx et al., 2016.
- PMAC_Plus Yasuda, 2011, Datta et al., 2017, LightMAC+ Naito, 2017 and 3kf9 Zhang et al., 2012.

Beyond birthday bound security

Differences of WOR Samples:

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathcal{G}.$$

Differences of WOR Samples:

Abelian group under the group operation "+"("−" inverse)

$\bar{\sigma} = qw$ *with* $w \geq 2$

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathcal{G}.$$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathcal{G}.$$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathcal{G}.$$

$\sigma = q(w-1)$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\mathrm{wor}} \mathscr{G}.$$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathscr{G}.$$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

$S_{1,1} = T_{1,1} - T_{1,w}$

$S_{1,w-1} = T_{1,w-1} - T_{1,w}$

$S_{q,w-1} = T_{q,w-1} - T_{q,w}$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\text{wor}} \mathcal{G}.$$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

$$R^{\sigma} := (R_{1,1}, \ldots, R_{1,w-1}, \ldots, R_{i,1}, \ldots, R_{i,w-1}, \ldots, R_{q,1}, \ldots, R_{q,w-1}) \leftarrow_{\text{wr}} \mathcal{G}.$$

Differences of WOR Samples:

$$T^{\bar{\sigma}} := (T_{1,1}, \ldots, T_{1,w}, \ldots, T_{i,1}, \ldots, T_{i,w}, \ldots, T_{q,1}, \ldots, T_{q,w}) \leftarrow_{\mathrm{wor}} \mathcal{G}.$$

$$S^{\sigma} := (S_{1,1}, \ldots, S_{1,w-1}, \ldots, S_{i,1}, \ldots, S_{i,w-1}, \ldots, S_{q,1}, \ldots, S_{q,w-1}).$$

$$R^{\sigma} := (R_{1,1}, \ldots, R_{1,w-1}, \ldots, R_{i,1}, \ldots, R_{i,w-1}, \ldots, R_{q,1}, \ldots, R_{q,w-1}) \leftarrow_{\mathrm{wr}} \mathcal{G}.$$

What is $\|S^{\sigma} - R^{\sigma}\|$??

Theorem (Pseudorandomness of S)

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

Theorem (Pseudorandomness of S)

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

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

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

Theorem (Pseudorandomness of S)

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

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

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

Theorem (Variable width case)

Let $w_1, w_2, \ldots, w_q \geq 2$, $\bar{\sigma} = \sum_i w_i$, *and* $w_{max} = \max_i w_i$. *Then,*

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

Theorem (Pseudorandomness of S)

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

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

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

Theorem (Variable width case)

Let $w_1, w_2, \ldots, w_q \geq 2$, $\bar{\sigma} = \sum_i w_i$, *and* $w_{max} = \max_i w_i$. *Then,*

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

Theorem (Pseudorandomness of S)

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

Bound is tight.

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

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

Improves the result of Dai et al., 2017

Theorem (Variable width case)

Let $w_1, w_2, \ldots, w_q \geq 2$, $\bar{\sigma} = \sum_i w_i$, and $w_{max} = \max_i w_i$. Then,

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

$\mathsf{XORP}^{e_K}[w]$ Construction

$\mathsf{XORP}^{e_K}[w]$ Construction

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

where $s \le \lceil \log_2 w\rceil$, $x \in \{0,1\}^{n-s}$ and $\langle i\rangle_s$ is the s-bit representation of i.

$\mathsf{XORP}^{e_K}[w]$ Construction

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

where $s \leq \lceil \log_2 w \rceil$, $x \in \{0,1\}^{n-s}$ and $\langle i\rangle_s$ is the s-bit representation of i.

$T_{i,w}$ $T_{i,1}$ $T_{i,w}$ $T_{i,w-1}$

$\mathsf{XORP}^{e_K}[w]$ Construction

$$\mathsf{XORP}[w](x) = \underbrace{\Big(e_K(x\|\langle 0\rangle_s)\oplus e_K(x\|\langle 1\rangle_s)\Big)}_{S_{i,1}}\|\cdots\|\underbrace{\Big(e_K(x\|\langle 0\rangle_s)\oplus e_K(x\|\langle w-1\rangle_s)\Big)}_{S_{i,w-1}}$$

where $s \le \lceil \log_2 w \rceil$, $x \in \{0,1\}^{n-s}$ and $\langle i \rangle_s$ is the s-bit representation of i.

- $\mathsf{RF}_{m \to p} \leftarrow_{\text{wr}} \mathsf{Func}_{m \to p}$.

Set of all functions from $\{0,1\}^m$ to $\{0,1\}^p$

- $\mathsf{RF}_{m\to p} \leftarrow_{\mathrm{wr}} \mathsf{Func}_{m\to p}$.

- $\mathsf{RF}_{m\to p} \leftarrow_{\mathrm{wr}} \mathsf{Func}_{m\to p}$. $\mathsf{RP}_p \leftarrow_{\mathrm{wr}} \mathsf{Perm}_p$.

Set of all permutations of $\{0,1\}^p$

- $\mathsf{RF}_{m\to p} \leftarrow_{\mathrm{wr}} \mathsf{Func}_{m\to p}$. $\mathsf{RP}_p \leftarrow_{\mathrm{wr}} \mathsf{Perm}_p$.

- $\mathsf{RF}_{m\to p} \leftarrow_{\text{wr}} \mathsf{Func}_{m\to p}$. $\mathsf{RP}_p \leftarrow_{\text{wr}} \mathsf{Perm}_p$.
- Let $\mathscr{A}$ be a distinguisher,

- $\mathsf{RF}_{m \to p} \leftarrow_{\mathrm{wr}} \mathsf{Func}_{m \to p}$. $\mathsf{RP}_p \leftarrow_{\mathrm{wr}} \mathsf{Perm}_p$.
- Let $\mathscr{A}$ be a distinguisher,
- $f : \mathscr{K} \times \{0,1\}^m \to \{0,1\}^p$ be a keyed function.

- $\mathsf{RF}_{m\to p} \leftarrow_{\text{wr}} \mathsf{Func}_{m\to p}$. $\mathsf{RP}_p \leftarrow_{\text{wr}} \mathsf{Perm}_p$.
- Let $\mathscr{A}$ be a distinguisher,
- $f : \mathscr{K} \times \{0,1\}^m \to \{0,1\}^p$ be a keyed function.

PRF-advantage of $\mathscr{A}$ against f

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

- $\mathsf{RF}_{m\to p} \leftarrow_{\mathrm{wr}} \mathsf{Func}_{m\to p}$. $\mathsf{RP}_p \leftarrow_{\mathrm{wr}} \mathsf{Perm}_p$.
- Let $\mathscr{A}$ be a distinguisher,
- $f : \mathscr{K} \times \{0,1\}^m \to \{0,1\}^p$ be a keyed function.

PRF-advantage of $\mathscr{A}$ against f

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

PRP-advantage of $\mathscr{A}$ against a keyed permutation f (in this case $m = p$)

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

We assume (w.l.o.g.)

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.

After the random choices are made everything is deterministic.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

Information theoretic security.
$\mathscr{A}$ is computationally unbounded.
Runs with best random coins.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.
- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.
- Gets $X^q := (X_1, \ldots, X_q)$ if the it is f_K oracle.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.
- Gets $X^q := (X_1, \ldots, X_q)$ if the it is f_K oracle. $R^q := (R_1, \ldots, R_q)$ if the it is $\mathsf{RF}_{m \to p}$ oracle.

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.
- Gets $X^q := (X_1, \ldots, X_q)$ if the it is f_K oracle. $R^q := (R_1, \ldots, R_q)$ if the it is $\mathsf{RF}_{m \to p}$ oracle.

$\Pr_X$

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.
- Gets $X^q := (X_1, \ldots, X_q)$ if the it is f_K oracle. $R^q := (R_1, \ldots, R_q)$ if the it is $\mathsf{RF}_{m \to p}$ oracle.

$(R_1, \ldots, R_q) \leftarrow_{\text{wr}} \{0,1\}^p$
$\Pr_R$

$$\mathbf{Adv}_f^{\text{prf}}(\mathscr{A}) = |\Pr_R(\mathscr{E}) - \Pr_X(\mathscr{E})| \leq \|\Pr_R - \Pr_X\|.$$

We assume (w.l.o.g.)

- $\mathscr{A}$ does not repeat its queries.
- $\mathscr{A}$ deterministic.

- $\mathscr{A}$ sends q queries $Q_1, \ldots, Q_q$.
- Gets $X^q := (X_1, \ldots, X_q)$ if the it is f_K oracle. $R^q := (R_1, \ldots, R_q)$ if the it is $\mathsf{RF}_{m \to p}$ oracle.

$$\mathbf{Adv}_f^{\mathrm{prf}}(\mathscr{A}) = |\Pr_R(\mathscr{E}) - \Pr_X(\mathscr{E})| \leq \|\Pr_R - \Pr_X\|.$$

$\mathscr{E} = \{x^q \in \{0,1\}^p : \mathscr{A}(x^q) = 1\}$

Corollary

- *e_K is a blockcipher over $\{0,1\}^n$ with a randomly chosen key K.*

Corollary

- *e_K is a blockcipher over $\{0,1\}^n$ with a randomly chosen key K.*
- *Adversary $\mathscr{A}$ makes at most q queries to $\mathsf{XORP}^{e_K}[w]$ or to $\mathsf{RF}_{(n-s)\to n(w-1)}$.*

Corollary

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

Corollary

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

Corollary

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

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

<u>Variable width</u>

Nonce respecting

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

Corollary

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

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

Variable width

$\max_i w_i$

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

- Fix the parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$.

- Fix the parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$.
- $M = M_1 \| \cdots \| M_\ell \in (\{0,1\}^n)^\ell$, $P \in \{0,1\}^m$, $\ell = w\ell' \leq \ell_{max}$, $m = n - (r+s) > 0$.

- Fix the parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$.
- $M = M_1 \| \cdots \| M_\ell \in (\{0,1\}^n)^\ell$, $P \in \{0,1\}^m$, $\ell = w\ell' \leq \ell_{max}$, $m = n - (r+s) > 0$.

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

- Fix the parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$.
- $M = M_1 \| \cdots \| M_\ell \in (\{0,1\}^n)^\ell$, $P \in \{0,1\}^m$, $\ell = w\ell' \leq \ell_{max}$, $m = n - (r+s) > 0$.

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

Theorem (PRF-security of CENC)

For every nonce-respecting distinguisher $\mathscr{A}$ making at most $\bar{\sigma}$ many queries there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ many queries such that

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

- Fix the parameters: width w, $s = \lceil \log_2 w \rceil$, maximum number of blocks ℓ_{max}, and $r = \lceil \log_2 \ell_{max}/w \rceil$.
- $M = M_1 \| \cdots \| M_\ell \in (\{0,1\}^n)^\ell$, $P \in \{0,1\}^m$, $\ell = w\ell' \le \ell_{max}$, $m = n - (r+s) > 0$.

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

Theorem (PRF-security of CENC)

For every nonce-respecting distinguisher $\mathscr{A}$ making at most $\bar{\sigma}$ many queries there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ many queries such that

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

Improvement over the query range $w\bar{\sigma} \le \frac{N}{67}$ in Iwata et al., 2016

- Nonce based authenticated encryption.

- Nonce based authenticated encryption.
- Provides birthday bound security.

- Nonce based authenticated encryption.
- Provides birthday bound security.

Due to PRP-PRF switching lemma

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction:

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.
- $M = (m_1, \ldots, m_\ell)$ an ℓ-block message.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.
- $M = (m_1, \ldots, m_\ell)$ an ℓ-block message.
- Nonce $P \in \{0,1\}^{n-s}$.

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.
- $M = (m_1, \ldots, m_\ell)$ an ℓ-block message.
- Nonce $P \in \{0,1\}^{n-s}$.

s is such that $\ell < 2^s - 1$ for longest message

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.
- $M = (m_1, \ldots, m_\ell)$ an ℓ-block message.
- Nonce $P \in \{0,1\}^{n-s}$.

1. Compute ciphertext $C = (c_1, \ldots, c_\ell)$

$$c_i = m_i \oplus e_K(P \| \langle i \rangle_s) \oplus e_K(P \| \langle s-1 \rangle_s).$$

- Nonce based authenticated encryption.
- Provides birthday bound security.
- CAESER aims to get better constructions.

Modified GCM (mGCM):

The construction: Let

- e_K - underlying random permutation.
- H - *hash key* chosen uniformly at random from $\{0,1\}^n$.
- $M = (m_1, \ldots, m_\ell)$ an ℓ-block message.
- Nonce $P \in \{0,1\}^{n-s}$.

1. Compute ciphertext $C = (c_1, \ldots, c_\ell)$

$$c_i = m_i \oplus e_K(P \| \langle i \rangle_s) \oplus e_K(P \| \langle s-1 \rangle_s).$$

2. Compute tag T

$$T = (H^\ell c_1 \oplus \cdots \oplus H c_\ell) \oplus e_K(P \| \langle 0 \rangle_s) \oplus e_K(P \| \langle s-1 \rangle_s).$$

Theorem (PRF-security of mGCM)

For every nonce-respecting distinguisher $\mathscr{A}$ making at most $\bar{\sigma}$ many queries, where the longest query has block length ℓ_{max}, there is an adversary $\mathscr{B}$ making at most $\bar{\sigma}$ many queries such that

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

Mirror Theory:

Mirror Theory:

- Fix σ.

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i, j) : 1 \leq i < j \leq \sigma\}$. Fix $c_{i,j}$ for $(i, j) \in \mathscr{C}$

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \le i < j \le \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \ldots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j} \text{ for } (i,j) \in \mathscr{C}\}$

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \leq i < j \leq \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \ldots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j} \text{ for } (i,j) \in \mathscr{C}\}$

What is $|\mathcal{S}|$?

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \le i < j \le \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \ldots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j}$ for $(i,j) \in \mathscr{C}\}$

What is $|\mathcal{S}|$?

- Mirror theory provides a lower bound on $|\mathcal{S}|$.

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \leq i < j \leq \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \ldots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j} \text{ for } (i,j) \in \mathscr{C}\}$

What is $|\mathcal{S}|$?

- Mirror theory provides a lower bound on $|\mathcal{S}|$.
  - Implies an upper bound on $\|S^\sigma - R^\sigma\|$. (Patarin, 2010)

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \le i < j \le \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \dots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j} \text{ for } (i,j) \in \mathscr{C}\}$

What is $|\mathcal{S}|$?

- Mirror theory provides a lower bound on $|\mathcal{S}|$.
  - Implies an upper bound on $\|S^\sigma - R^\sigma\|$. (Patarin, 2010)
- Powerful in terms of implications. Optimum security for many constructions such as EDM, EWCDM etc. (Mennink and Neves, 2017)

Mirror Theory:

- Fix σ.
- Let $\mathscr{C} \subseteq \{(i,j) : 1 \leq i < j \leq \sigma\}$. Fix $c_{i,j}$ for $(i,j) \in \mathscr{C}$
- $\mathcal{S} = \{(P_1, \ldots P_\sigma) \in \{0,1\}^n \times \cdots \times \{0,1\}^n \mid P_i \oplus P_j = c_{i,j} \text{ for } (i,j) \in \mathscr{C}\}$

What is $|\mathcal{S}|$?

- Mirror theory provides a lower bound on $|\mathcal{S}|$.
  - Implies an upper bound on $\|S^\sigma - R^\sigma\|$. (Patarin, 2010)
- Powerful in terms of implications. Optimum security for many constructions such as EDM, EWCDM etc. (Mennink and Neves, 2017)
- Quite complex. Some of the steps lack necessary details.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of $\mathsf{XORP}[2]$.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of $\mathsf{XORP}[2]$.
  - Improved security of EDM.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of XORP[2].
  - Improved security of EDM.
- Stam (Stam, 1978) used it to show pseudorandomness of trucation of WOR samples (in statistical context).

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of XORP[2].
  - Improved security of EDM.
- Stam (Stam, 1978) used it to show pseudorandomness of trucation of WOR samples (in statistical context).
- Much transparent than the mirror theory.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of XORP[2].
  - Improved security of EDM.
- Stam (Stam, 1978) used it to show pseudorandomness of trucation of WOR samples (in statistical context).
- Much transparent than the mirror theory.
- Seems to have potential.

χ^2 Method

- Recently (in Crypto 2017) introduced by Dai, Hoang, and Tessaro in cryptographic context.
  - Full security of XORP[2].
  - Improved security of EDM.
- Stam (Stam, 1978) used it to show pseudorandomness of trucation of WOR samples (in statistical context).
- Much transparent than the mirror theory.
- Seems to have potential.
  - Full indifferentiability of the sum of multiple random permutations.(Bhattacharya and Nandi, 2018)

Notation:

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i | x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$.

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i | x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$.

$\Pr_{\mathsf{X}}(x_1 | x^0) := \Pr[X_1 = x_1]$

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i | x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$. Similarly for $\Pr_{\mathsf{Y}}(x_i | x^{i-1})$.

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i | x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$. Similarly for $\Pr_{\mathsf{Y}}(x_i | x^{i-1})$.
-

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

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i | x^{i-1}) := \Pr[X_i = x_i | X^{i-1} = x^{i-1}]$. Similarly for $\Pr_{\mathsf{Y}}(x_i | x^{i-1})$.
-

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

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

Notation:

- Let $\mathsf{X} := X^q := (X_1, \ldots, X_q)$ and $\mathsf{Y} := Y^q := (Y_1, \ldots, Y_q)$ be two random vectors distributed over Ω^q.
- $\Pr_{\mathsf{X}}(x_i|x^{i-1}) := \Pr[X_i = x_i|X^{i-1} = x^{i-1}]$. Similarly for $\Pr_{\mathsf{Y}}(x_i|x^{i-1})$.
-

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

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

$\forall i$, Support of Y^i should contain support of $X^i (= \Omega_i)$

Theorem (Dai et al., 2017)

Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then

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

Theorem (Dai et al., 2017)

Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then

$$\|\Pr_X - \Pr_Y\| \leq \left(\frac{1}{2} \sum_{i=1}^{q} \mathbf{Ex}[\chi^2(X^{i-1})] \right)^{\frac{1}{2}}$$

Ingradients:

Theorem (Dai et al., 2017)

Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then

$$\|\mathrm{Pr}_X - \mathrm{Pr}_Y\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}}$$

Ingradients:

1. Pinsker's inequality.

Theorem (Dai et al., 2017)

Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then

$$\|\mathrm{Pr}_X - \mathrm{Pr}_Y\| \leq \left(\frac{1}{2}\sum_{i=1}^{q} \mathbf{Ex}[\chi^2(X^{i-1})]\right)^{\frac{1}{2}}$$

Ingradients:

1. Pinsker's inequality.
2. chain rule of *Kullback-Leibler divergence* (KL divergence).

Theorem (Dai et al., 2017)

Following the notation as above and assuming that the support of X^i is contained in the support of Y^i for every i, then

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

Ingradients:

1. Pinsker's inequality.
2. chain rule of *Kullback-Leibler divergence* (KL divergence).
3. Jensen's inequality.

Random Experiment for R

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

Random Experiment for R

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

Random Experiment for S

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

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathscr{G}^{q(w-1)}$.

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathscr{G}^{q(w-1)}$.
- They don't have same support.

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathcal{G}^{q(w-1)}$.
- They don't have same support.
  - The support of R is $\mathcal{G}^{q(w-1)}$.

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathcal{G}^{q(w-1)}$.
- They don't have same support.
  - The support of R is $\mathcal{G}^{q(w-1)}$.
  - $T_{i,j}$'s are distinct implies

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathscr{G}^{q(w-1)}$.
- They don't have same support.
  - The support of R is $\mathscr{G}^{q(w-1)}$.
  - $T_{i,j}$'s are distinct implies
    1. $S_{i,j} \neq 0$ for all i, j,

Random Experiment for R

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

Random Experiment for S

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

- Both R and S have same sample space $\mathcal{G}^{q(w-1)}$.
- They don't have same support.
  - The support of R is $\mathcal{G}^{q(w-1)}$.
  - $T_{i,j}$'s are distinct implies
    1. $S_{i,j} \neq 0$ for all i, j, and
    2. for any i and for all $j \neq j' \le w-1$, $S_{i,j} \neq S_{i,j'}$.

- Consider an intermediate distribution U

- Consider an intermediate distribution U

Random Experiment for U

$$
\begin{aligned}
&\textbf{for } 1 \le i \le q \\
&\quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\} \\
&\textbf{return } \mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])
\end{aligned}
$$

- Consider an intermediate distribution U

Random Experiment for U

---

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

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

- Consider an intermediate distribution U

Random Experiment for U

$$\begin{array}{l}\textbf{for } 1 \leq i \leq q \\ \quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\text{wor}} \mathcal{G} \setminus \{0\} \\ \textbf{return } \mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])\end{array}$$

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \leq \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\leq \frac{w(w-1)q}{2N}$

- Consider an intermediate distribution U

Random Experiment for U

---

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

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$$\le \frac{w(w-1)q}{2N}$$

  - U is identical with R until

- Consider an intermediate distribution U

Random Experiment for U

---

for $1 \leq i \leq q$
$\quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
return $\mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])$

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \leq \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\leq \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$.

- Consider an intermediate distribution U

Random Experiment for U

---

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

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\le \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$.
    2. for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$.

- Consider an intermediate distribution U

Random Experiment for U

$$\begin{aligned}
&\textbf{for } 1 \le i \le q \\
&\quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\} \\
&\textbf{return } \mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])
\end{aligned}$$

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\le \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$. Probability $\le \frac{q(w-1)}{N}$.
    2. for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$.

- Consider an intermediate distribution U

Random Experiment for U

$$\begin{aligned}&\textbf{for } 1 \le i \le q\\ &\quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\text{wor}} \mathcal{G} \setminus \{0\}\\ &\textbf{return } \mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1])\end{aligned}$$

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\le \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$. Probability $\le \frac{q(w-1)}{N}$.
    2. for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$. Probability $\le q \times \frac{(w-1)(w-2)}{2N}$.

- Consider an intermediate distribution U

Random Experiment for U

$$\begin{array}{l} \textbf{for } 1 \le i \le q \\ \quad U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\text{wor}} \mathcal{G} \setminus \{0\} \\ \textbf{return } \mathsf{U} := (U_{i,j} : i \in [q], j \in [w-1]) \end{array}$$

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\le \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$. Probability $\le \frac{q(w-1)}{N}$.
    2. for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$. Probability $\le q \times \frac{(w-1)(w-2)}{2N}$.
- $\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\|$?

- Consider an intermediate distribution U

Random Experiment for U

---

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

- By triangle inequality

$$\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{R}}\| \le \|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\| + \|\Pr_{\mathsf{U}} - \Pr_{\mathsf{R}}\|$$

$\le \frac{w(w-1)q}{2N}$

  - U is identical with R until
    1. for some i, j, $R_{i,j} = 0$. Probability $\le \frac{q(w-1)}{N}$.
    2. for some $1 \le i \le q$, $1 \le j \ne j' \le w-1$, $R_{i,j} = R_{i,j'}$. Probability $\le q \times \frac{(w-1)(w-2)}{2N}$.
- $\|\Pr_{\mathsf{S}} - \Pr_{\mathsf{U}}\|$?
  - χ^2 method.

- Extend S to X (S is marginal random variables of X.)

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G}$
for $1 \le i \le q$
  for $1 \le j \le w - 1$
    $S_{i,j} = T_{i,j} - T_{i,w}$
  $X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w})$
  $S_i = (S_{i,1}, \ldots, S_{i,w-1})$
return $\mathsf{X} := (X_1, \ldots, X_q)$

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G}$
for $1 \le i \le q$
  for $1 \le j \le w-1$
    $S_{i,j} = T_{i,j} - T_{i,w}$
  $X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w})$
  $S_i = (S_{i,1}, \ldots, S_{i,w-1})$
return $\mathsf{X} := (X_1, \ldots, X_q)$

-
  - $\rho : \mathcal{G}^w \mapsto \mathcal{G}^w$, $\rho(z_1, \ldots, z_w) = (z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$ is a permutation.

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$$
\begin{aligned}
&\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G} \\
&\textbf{for } 1 \le i \le q \\
&\quad \textbf{for } 1 \le j \le w-1 \\
&\quad\quad S_{i,j} = T_{i,j} - T_{i,w} \\
&\quad X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w}) \\
&\quad S_i = (S_{i,1}, \ldots, S_{i,w-1}) \\
&\textbf{return } \mathsf{X} := (X_1, \ldots, X_q)
\end{aligned}
$$

-
  - $\rho : \mathcal{G}^w \mapsto \mathcal{G}^w$, $\rho(z_1, \ldots, z_w) = (z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$ is a permutation.
  - $\rho(X_i) = T_i$

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G}$
for $1 \leq i \leq q$
  for $1 \leq j \leq w-1$
    $S_{i,j} = T_{i,j} - T_{i,w}$
  $X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w})$
  $S_i = (S_{i,1}, \ldots, S_{i,w-1})$
return $\mathsf{X} := (X_1, \ldots, X_q)$

-
  - $\rho : \mathcal{G}^w \mapsto \mathcal{G}^w$, $\rho(z_1, \ldots, z_w) = (z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$ is a permutation.
  - $\rho(X_i) = T_i$, $\rho^*(X^i) := (\rho(X_1), \ldots, \rho(X_i)) = (T_1, \ldots, T_i) = T^i$
  - $\Pr_{\mathsf{X}}(x_i \mid x^{i-1}) \stackrel{\text{def}}{=} \Pr[X_i = x_i \mid X^{i-1} = x^{i-1}]$

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$$
\begin{array}{l}
\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G} \\
\textbf{for } 1 \le i \le q \\
\quad \textbf{for } 1 \le j \le w-1 \\
\quad\quad S_{i,j} = T_{i,j} - T_{i,w} \\
\quad X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w}) \\
\quad S_i = (S_{i,1}, \ldots, S_{i,w-1}) \\
\textbf{return } \mathsf{X} := (X_1, \ldots, X_q)
\end{array}
$$

-
  - $\rho : \mathcal{G}^w \mapsto \mathcal{G}^w$, $\rho(z_1, \ldots, z_w) = (z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$ is a permutation.
  - $\rho(X_i) = T_i$, $\rho^*(X^i) := (\rho(X_1), \ldots, \rho(X_i)) = (T_1, \ldots, T_i) = T^i$
  - $\Pr_{\mathsf{X}}(x_i \mid x^{i-1}) \overset{\text{def}}{=} \Pr[X_i = x_i \mid X^{i-1} = x^{i-1}] = \Pr[T_i = a_i \mid T^{i-1} = a^{i-1}] = \frac{1}{(N-(i-1)w)^{\underline{w}}}$.

- Extend S to X (S is marginal random variables of X.)

Random Experiment for X

$$
\begin{array}{l}
\mathsf{T} = (T_{i,j} : i \in [q], j \in [w]) \leftarrow_{\text{wor}} \mathcal{G} \\
\textbf{for } 1 \le i \le q \\
\quad \textbf{for } 1 \le j \le w-1 \\
\quad\quad S_{i,j} = T_{i,j} - T_{i,w} \\
\quad X_i = (S_{i,1}, \ldots, S_{i,w-1}, T_{i,w}) \\
\quad S_i = (S_{i,1}, \ldots, S_{i,w-1}) \\
\textbf{return } \mathsf{X} := (X_1, \ldots, X_q)
\end{array}
$$

-
  - $\rho : \mathcal{G}^w \mapsto \mathcal{G}^w$, $\rho(z_1, \ldots, z_w) = (z_1 + z_w, \ldots, z_{w-1} + z_w, z_w)$ is a permutation.
  - $\rho(X_i) = T_i$, $\rho^*(X^i) := (\rho(X_1), \ldots, \rho(X_i)) = (T_1, \ldots, T_i) = T^i$
  - $\Pr_{\mathsf{X}}(x_i \mid x^{i-1}) \stackrel{\text{def}}{=} \Pr[X_i = x_i \mid X^{i-1} = x^{i-1}] = \Pr[T_i = a_i \mid T^{i-1} = a^{i-1}] = \frac{1}{(N-(i-1)w)^{\underline{w}}}$.

$\rho(x_i) = a_i$

$\rho^*(x^{i-1}) = a^{i-1}$

- Extend U to Y (U is marginal random variable of Y.)

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

---

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

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$.

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$.

Support of X^i.

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$.

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$. $x_i = (u_i, x_{i,w})$.

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \neq \varnothing$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$. $x_i = (u_i, x_{i,w})$.
- $\forall i \in [q]$, and $\forall x^i \in \Omega_i$,

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

---

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
  $U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
  $\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
  if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
  $Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
  $\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$. $x_i = (u_i, x_{i,w})$.
- $\forall i \in [q]$, and $\forall x^i \in \Omega_i$,

$$\Pr_{\mathsf{Y}}(x_i \mid x^{i-1}) \stackrel{\text{def}}{=} \Pr[Y_i = x_i \mid Y^{i-1} = x^{i-1}]$$

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

---

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
  $U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \xleftarrow{\text{wor}} \mathcal{G} \setminus \{0\}$
  $\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
  if $\mathcal{N}_i \neq \emptyset$ **then** $V_{i,w} \xleftarrow{\text{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
  $Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
  $\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$. $x_i = (u_i, x_{i,w})$.
- $\forall i \in [q]$, and $\forall x^i \in \Omega_i$,

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

- Extend U to Y (U is marginal random variable of Y.)

Random Experiment for Y

---

initialize $\mathcal{S}_0 = \mathcal{G}$
for $1 \le i \le q$
$U_i := (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}) \leftarrow_{\mathrm{wor}} \mathcal{G} \setminus \{0\}$
$\mathcal{N}_i = \{v \in \mathcal{S}_{i-1} : v + U_{i,j} \in \mathcal{S}_{i-1}, \forall j \in [w-1]\}$
if $\mathcal{N}_i \ne \varnothing$ **then** $V_{i,w} \leftarrow_{\mathrm{wr}} \mathcal{N}_i$ **else** $V_{i,w} = 0$
$Y_i = (U_{i,1}, U_{i,2}, \ldots, U_{i,w-1}, V_{i,w})$
$\mathcal{S}_i = \mathcal{G} \setminus \left(\{V_{i',j} := U_{i',j} + V_{i',w} : i' \in [i], j \in [w-1]\} \cup \{V_{1,w}, \ldots, V_{i,w}\}\right)$
return $\mathsf{Y} := (Y_1, \ldots, Y_q)$

- $x^i := (x_1, \ldots, x_i) \in \Omega_i$. $u_i := (x_{i,1}, \ldots, x_{i,w-1})$. $x_i = (u_i, x_{i,w})$.
- $\forall i \in [q]$, and $\forall x^i \in \Omega_i$,

$$\Pr_{\mathsf{Y}}(x_i \mid x^{i-1}) \stackrel{\mathrm{def}}{=} \Pr[Y_i = x_i \mid Y^{i-1} = x^{i-1}]$$
$$= \frac{1}{(N-1)^{\underline{w-1}}} \times \frac{1}{|\mathcal{N}^{u_i}(x^{i-1})|} \quad > 0$$

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

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

$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

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

$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

$\mathsf{C} = \frac{(N-1)\underline{w-1}}{((N-(i-1)w)\underline{w})^2}$

$\mathsf{D} = \frac{(N-(i-1)w)\underline{w}}{(N-1)\underline{w-1}}$

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \Big(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D} \Big)^2.$$

$$\mathbf{Ex}[\chi^2(X^{i-1})] = \mathsf{C} \times \sum_{u_i} \mathbf{Ex}\Big[\Big(|\mathcal{N}^{u_i}(X^{i-1})| - \mathsf{D} \Big)^2\Big]$$

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

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

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

$\mathsf{D} = \mathbf{Ex}[|\mathcal{N}^{u_i}(X^{i-1})|]$

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

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \Big(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\Big)^2.$$

$$\mathbf{Ex}[\chi^2(X^{i-1})] = \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\Big(|\mathcal{N}^{u_i}(X^{i-1})| - \mathsf{D}\Big)^2]$$
$$= \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\Big(|\mathcal{N}^{u_i}(X^{i-1})| - \mathbf{Ex}[|\mathcal{N}^{u_i}(X^{i-1})|]\Big)^2]$$
$$= \mathsf{C} \times \sum_{u_i} \mathbf{Var}[|\mathcal{N}^{u_i}(X^{i-1})|]$$

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

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

$$w^2 \times \frac{(N-r)^{\underline{w}}}{(N-1)^{\underline{w-1}}} \times \left(1 - \frac{(N-r)^{\underline{w}}}{N^{\underline{w}}}\right)$$
$$r = w(i-1)$$

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \Big(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\Big)^2.$$

$$\begin{aligned}\mathbf{Ex}[\chi^2(X^{i-1})] &= \mathsf{C} \times \sum_{u_i} \mathbf{Ex}\Big[\Big(|\mathcal{N}^{u_i}(X^{i-1})| - \mathsf{D}\Big)^2\Big] \\ &= \mathsf{C} \times \sum_{u_i} \mathbf{Ex}\Big[\Big(|\mathcal{N}^{u_i}(X^{i-1})| - \mathbf{Ex}[|\mathcal{N}^{u_i}(X^{i-1})|]\Big)^2\Big] \\ &= \mathsf{C} \times \sum_{u_i} \mathbf{Var}[|\mathcal{N}^{u_i}(X^{i-1})|] \leq \frac{8rw^3}{N^2}.\end{aligned}$$

$$\chi^2(x^{i-1}) := \sum_{x_i} \frac{(\Pr_{\mathsf{X}}(x_i|x^{i-1}) - \Pr_{\mathsf{Y}}(x_i|x^{i-1}))^2}{\Pr_{\mathsf{Y}}(x_i|x^{i-1})}$$
$$= \mathsf{C} \times \sum_{u_i} \left(|\mathcal{N}^{u_i}(x^{i-1})| - \mathsf{D}\right)^2.$$

$$\mathbf{Ex}[\chi^2(X^{i-1})] = \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\left(|\mathcal{N}^{u_i}(X^{i-1})| - \mathsf{D}\right)^2]$$
$$= \mathsf{C} \times \sum_{u_i} \mathbf{Ex}[\left(|\mathcal{N}^{u_i}(X^{i-1})| - \mathbf{Ex}[|\mathcal{N}^{u_i}(X^{i-1})|]\right)^2]$$
$$= \mathsf{C} \times \sum_{u_i} \mathbf{Var}[|\mathcal{N}^{u_i}(X^{i-1})|] \leq \frac{8rw^3}{N^2}.$$

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

For $w = 2$ and $\mathscr{G} = \{\{0,1\}^n, \oplus\}$,

$$\mathbf{Ex}[\chi^2(X^{i-1})] \leq \frac{2(N-1)r^2}{(N-2q)^4}$$

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

Random Experiment for R'

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

Random Experiment for U'

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

Random Experiment for S'

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

Random Experiment for R'

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

Random Experiment for U'

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

Random Experiment for S'

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

Theorem

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

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

Questions?

Thank You!

References I

Bellare, M., Kilian, J., and Rogaway, P. (2000).
The security of the cipher block chaining message authentication code.
J. Comput. Syst. Sci., 61(3):362–399.

Bhattacharya, S. and Nandi, M.
A note on the chi-square method : A tool for proving cryptographic security.
Cryptography and Communications, in Press.

Bhattacharya, S. and Nandi, M. (2018).
Full indifferentiable security of the xor of two or more random permutations using the χ^2 method.
In *Eurocrypt 2018*. Springer International Publishing.

References II

Black, J. and Rogaway, P. (2002).
A block-cipher mode of operation for parallelizable message authentication.
In *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 384–397. Springer.

Dai, W., Hoang, V. T., and Tessaro, S. (2017).
Information-theoretic indistinguishability via the chi-squared method.
In Katz and Shacham, 2017, pages 497–523.

Datta, N., Dutta, A., Nandi, M., Paul, G., and Zhang, L. (2017).
Single key variant of pmac_plus.
To appear in IACR Transaction on Symmetric Key Cryptology, (4).

References III

Gilboa, S. and Gueron, S. (2016).
The advantage of truncated permutations.
CoRR, abs/1610.02518.

Gilboa, S., Gueron, S., and Morris, B. (2017).
How many queries are needed to distinguish a truncated random permutation from a random function?
Journal of Cryptology.

Gueron, S., Langley, A., and Lindell, Y. (2017).
AES-GCM-SIV: specification and analysis.
IACR Cryptology ePrint Archive, 2017:168.

References IV

Gueron, S. and Lindell, Y. (2017).
Better bounds for block cipher modes of operation via nonce-based key derivation.
In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 1019–1036, New York, NY, USA. ACM.

Iwata, T. and Kurosawa, K. (2003).
OMAC: one-key CBC MAC.
In *Fast Software Encryption, 2003*, volume 2887 of *LNCS*, pages 129–153. Springer.

References V

Iwata, T., Mennink, B., and Vizár, D. (2016).
CENC is optimally secure.
IACR Cryptology ePrint Archive, 2016:1087.

Iwata, T. and Seurin, Y. (2017).
Reconsidering the security bound of aes-gcm-siv.
IACR Transactions on Symmetric Cryptology, 2017(4):240–267.

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

References VI

Luykx, A., Preneel, B., Tischhauser, E., and Yasuda, K. (2016).
A MAC mode for lightweight block ciphers.
In Peyrin, T., editor, *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, volume 9783 of *Lecture Notes in Computer Science*, pages 43–59. Springer.

Mennink, B. and Neves, S. (2017).
Encrypted davies-meyer and its dual: Towards optimal security using mirror theory.
In Katz and Shacham, 2017, pages 556–583.

References VII

Naito, Y. (2017).
Blockcipher-based macs: Beyond the birthday bound without message length.
In Takagi, T. and Peyrin, T., editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 446–470, Cham. Springer International Publishing.

Nandi, M. (2009).
Fast and secure cbc-type mac algorithms.
In Dunkelman, O., editor, *Fast Software Encryption*, pages 375–393, Berlin, Heidelberg. Springer Berlin Heidelberg.

References VIII

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.

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

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

References IX

Zhang, L., Wu, W., Sui, H., and Wang, P. (2012).
3kf9: Enhancing 3gpp-mac beyond the birthday bound.
In *ASIACRYPT 2012*, pages 296–312.