Efficient Pseudorandom Correlation Generators for Any Finite Field

Zhe Li, Chaoping Xing, Yizhou Yao, and Chen Yuan

Shanghai Jiao Tong University

05/05/2025 – EuroCrypt2025

饮 水 思 源 • 爱 国 荣 校

MPC with Preprocessing [Beaver' 91]

Bob

$[a_i]_0, [b_i]_0, [c_i]_0$

Setup Protocol

Cryptographic, dominates overall cost

$[a_i], [b_i], [c_i = a_i \cdot b_i]$
$a_i, b_i \leftarrow \$$

Alice

$[a_i]_1, [b_i]_1, [c_i]_1$

Offline Phase

Online Phase

$\boldsymbol{x}$

$\boldsymbol{y}$

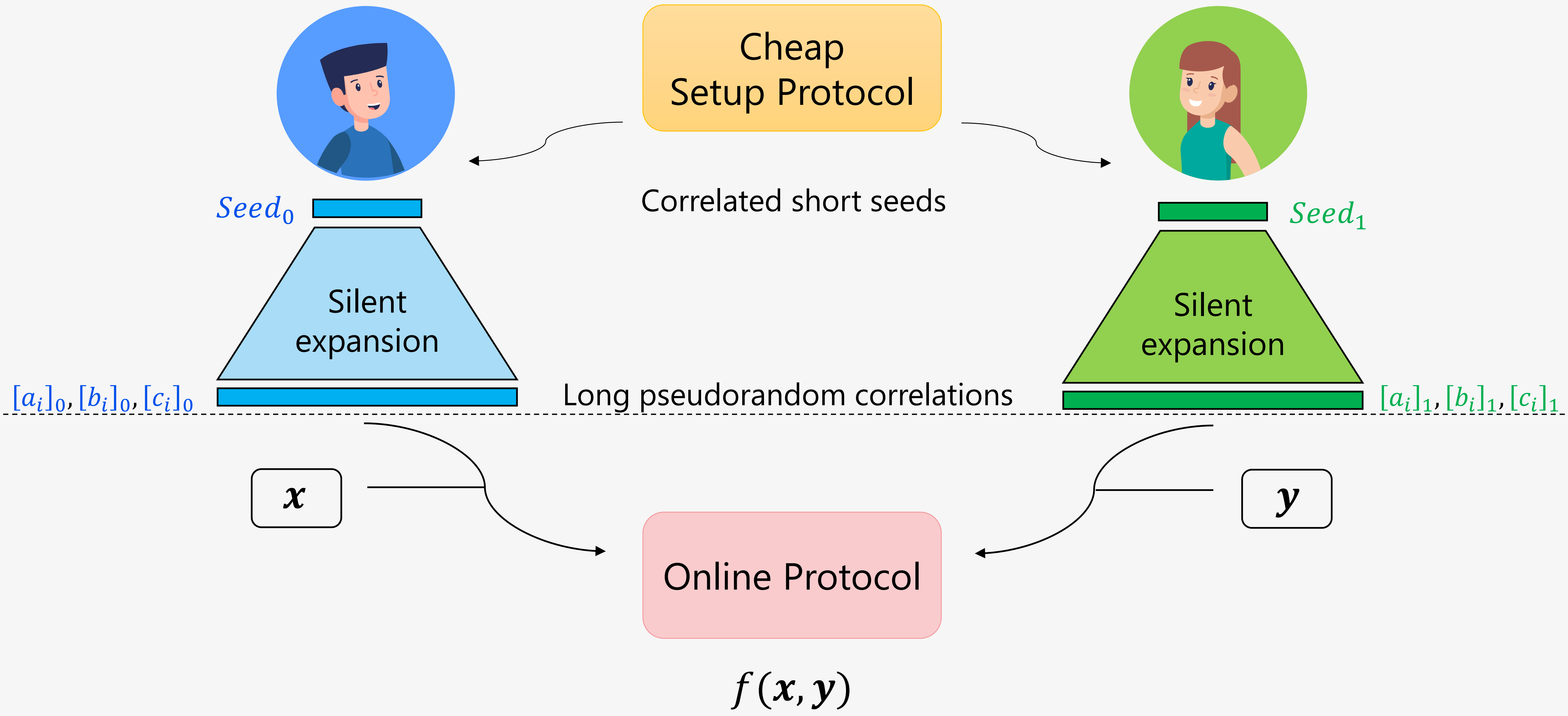
Online Protocol

Information-theoretic, fast

$f(\boldsymbol{x}, \boldsymbol{y})$

Goal: make preprocessing <u>cheaper</u>

Silent Preprocessing via PCG [BCGIKS 19]



Current Landscape of PCG

Oblivious linear evaluation (OLE): $a, [ab]_0, b, [ab]_1$, with $a, b \in \mathbb{F}_p$, $[ab]_0 + [ab]_1 = ab$

	N OLE	Communication	Computation	Programmability	Assumption
[BCGIKS 19]	Any $\mathbb{F}_p$	$O(\lambda^3 \log N)$	$O(N^2 \log N)$	YES	Dual-LPN
[BCGIKS 20]	$\mathbb{F}_p, p > N$	$O(\lambda^3 \log N)$	$O(N \log N)$	YES	Ring-LPN
[BCCD 23]	$\mathbb{F}_p, p > 2$	$O(\lambda^3 \log N)$	$O(N \log N)$	YES	QA-SD
[BCGIKRS 23]	$\mathbb{F}_2$	$O(\lambda^2 \log N)$	$O(N)$	NO	Dual-LPN
This work	Any $\mathbb{F}_p$	$O(\lambda^3 \log N)$	$O(N \log N)$	YES	QA-SD/Ring-LPN

Key Fact: OLE + Programmability $\Longrightarrow$ multi-party Beaver triple

Our Contribution:

Break the *field size barrier* of previous works, while maintaining *fast computation* and offering *programmability*

Performance Evaluation

On multi-party Binary triple

	Party Number	Triple Number	Communication Point-to-Point	Communication Broadcast	Seed Expansion Time (s)
SoftSpokenOT [Roy 22]	2	10^9	3.7 GB	0	211
	10	10^9	34 GB	0	1900
F4OLEAGE [BBCCDS 24]	2	10^9	33.5 MB	0	83
	10	10^9	0.6 GB	0.12 GB linear term	1511
This work	2	10^9	33.6 MB	0	162
	10	10^9	0.6 GB	0	2932

On authenticated Binary triple

	Field	Communication	Triple Generation
Overdrive [KPR 18]	128-bit prime field	2 GB	30,000/s
PCG [BCGIKS 20]	128−bit prime field	4.2 MB	50,000/s
This work	Boolean with 128−bit MAC key	47.54 MB	43,000/s

Technical Details

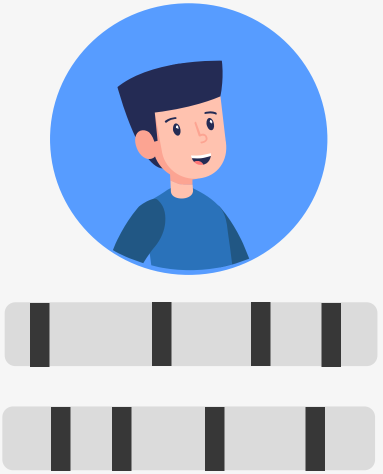
Overview: PCG from Ring-LPN [BCGIKS 20]

$\boxed{\mathrm{PCG.GEN}}$

$s_0, e_0, Seed_0$ ← PCG.GEN → $s_1, e_1, Seed_1$

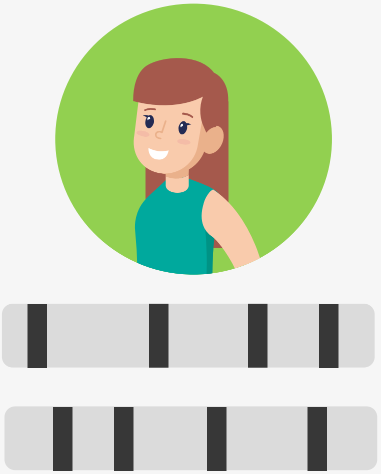
Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$



$s_0, e_0 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$



$s_1, e_1 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

Requirements:
(1) Ring-LPN assumption

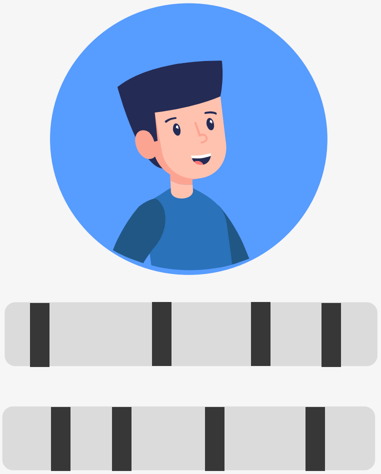
Overview: PCG from Ring-LPN [BCGIKS 20]

$s_0, e_0, Seed_0$ ⟵ $\mathrm{PCG.GEN}$ ⟶ $s_1, e_1, Seed_1$

Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$



$s_0, e_0 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$Seed_0$

$\mathrm{PCG.EXPAND}$ ⬇

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

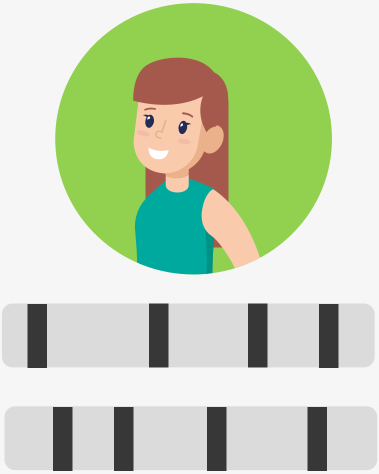
⬇

$z_0 = [b_0 \cdot b_1]_0$

Requirements:

(1) Ring-LPN assumption

(2) Sparse s_0, s_1, e_0, e_1, so that the cross-terms can be succinctly shared via DPF



$s_1, e_1 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

$Seed_1$

$\mathrm{PCG.EXPAND}$ ⬇

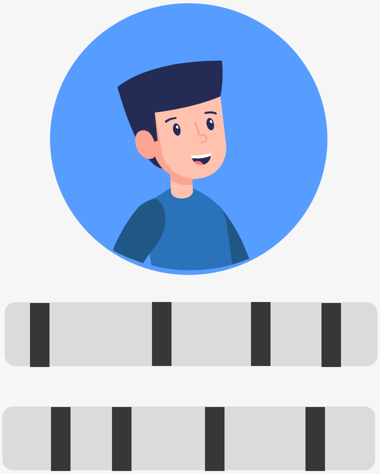
$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

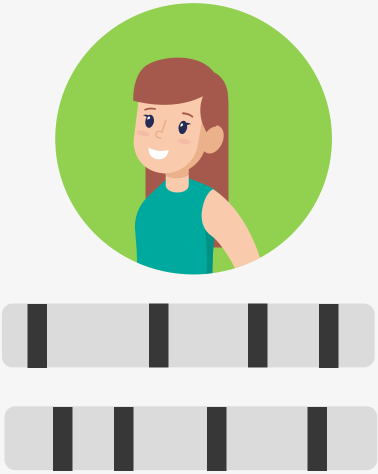
⬇

$z_1 = [b_0 \cdot b_1]_1$

Overview: PCG from Ring-LPN [BCGIKS 20]

$s_0, e_0, Seed_0$ ← **PCG. GEN** → $s_1, e_1, Seed_1$





Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$

$s_0, e_0 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$s_1, e_1 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

Requirements:
1. Ring-LPN assumption
2. Sparse s_0, s_1, e_0, e_1, so that the cross-terms can be succinctly shared via DPF
3. Fully reducible $X^N - 1$, so that $\mathbb{F}_p[X]/(X^N - 1) \cong \mathbb{F}_p^N$ via CRT

$Seed_0$

PCG. EXPAND ⬇

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

⬇

$z_0 = [b_0 \cdot b_1]_0$

$Seed_1$

PCG. EXPAND ⬇

$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

⬇

$z_1 = [b_0 \cdot b_1]_1$

$$\vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$$

Overview: PCG from Ring-LPN [BCGIKS 20]

$s_0, e_0, Seed_0$ ← PCG.GEN → $s_1, e_1, Seed_1$

Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$

$s_0, e_0 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$s_1, e_1 \in \mathbb{F}_p[X]/(X^N - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

Requirements:

(1) Ri

(2

(3) Fully reducible $X^N - 1$, so that $\mathbb{F}_p[X]/(X^N - 1) \cong \mathbb{F}_p^N$ via CRT

Limitation: $p > N$

$Seed_0$

PCG.EXPAND ⬇

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

⬇

$z_0 = [b_0 \cdot b_1]_0$

$Seed_1$

PCG.EXPAND ⬇

$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

⬇

$z_1 = [b_0 \cdot b_1]_1$

$$\vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$$

Overview: PCG from QA-SD [BCCD 23]

$\mathrm{PCG.GEN}$

$s_0, e_0, Seed_0$

$s_1, e_1, Seed_1$

Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$

$s_0, e_0 \in \mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$Seed_0$

$\mathrm{PCG.EXPAND}$ ⬇

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

⬇

$z_0 = [b_0 \cdot b_1]_0$

(1) Syndrome decoding of quasi-abelian codes
(2) Sparse s_0, s_1, e_0, e_1, so that the cross-terms can be succinctly shared via DPF

$s_1, e_1 \in \mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

$Seed_1$

$\mathrm{PCG.EXPAND}$ ⬇

$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

⬇

$z_1 = [b_0 \cdot b_1]_1$

Overview: PCG from QA-SD [BCCD 23]

PCG.GEN

$s_0, e_0, Seed_0$ $\quad$ $s_1, e_1, Seed_1$

Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$

$s_0, e_0 \in \mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1)$

$s_1, e_1 \in \mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$b_1 = a \cdot s_1 + e_1 \approx \$$

$Seed_0$

$\text{PCG.EXPAND} \Downarrow$

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

$\Downarrow$

$z_0 = [b_0 \cdot b_1]_0$

(1) Syndrome decoding of quasi-abelian codes

(2) Sparse s_0, s_1, e_0, e_1, so that the cross-terms can be succinctly shared via DPF

(3) Fully reducible $X_i^d - 1$, i.e., $d \mid p - 1$, so that $\mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \cong \mathbb{F}_p^N$ via CRT, where $N = d^n$

$Seed_1$

$\text{PCG.EXPAND} \Downarrow$

$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

$\Downarrow$

$z_1 = [b_0 \cdot b_1]_1$

$$\vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$$

Overview: PCG from QA-SD [BCCD 23]

$\mathrm{PCG.GEN}$

$s_0, e_0, Seed_0$

$s_1, e_1, Seed_1$

Goal: N OLE correlations over $\mathbb{F}_p$

$$b_0 \cdot b_1 = (a \cdot s_0 + e_0) \cdot (a \cdot s_1 + e_1)$$
$$= a^2 \cdot s_0 s_1 + a \cdot (s_0 e_1 + s_1 e_0) + e_0 e_1$$

$$\boxed{[b_0 \cdot b_1] = a^2 \cdot [s_0 s_1] + a \cdot ([s_0 e_1] + [s_1 e_0]) + [e_0 e_1]}$$

$s_0, e_0 \in \mathbb{F}_p[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$Seed_0$

$\mathrm{PCG.EXPAND}$

$[s_0 s_1]_0, [s_0 e_1]_0, [s_1 e_0]_0, [e_0 e_1]_0$

$z_0 = [b_0 \cdot b_1]_0$

$s_1, e_1 \in \mathbb{F}_p[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1)$

$b_1 = a \cdot s_1 + e_1 \approx \$$

$Seed_1$

$\mathrm{PCG.EXPAND}$

$[s_0 s_1]_1, [s_0 e_1]_1, [s_1 e_0]_1, [e_0 e_1]_1$

$z_1 = [b_0 \cdot b_1]_1$

(1) Synd ... codes
(2) Spars ... erms
can b ... d DFT
(3) Fully reducible $X_i^d - 1$, i.e., $d \mid p - 1$, so that $\mathbb{F}_p[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1) \cong \mathbb{F}_p^N$ via CRT, where $N = d^n$

Limitation: $p > 2$

$$\vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$$

Overview: Our Approach

$\mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_p^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

This leads to $p > 2$

Ideally, we hope:

Here $p^k > 2$ suffices.

$\mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_{p^k}^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

Overview: Our Approach

$\mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_p^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

This leads to $p > 2$

Ideally, we hope:

Here $p^k > 2$ suffices,
but NO ring isomorphism!

$\mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \ncong \quad \mathbb{F}_p^{kN}$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1 \quad \not\Longleftrightarrow \quad \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$

Overview: Our Approach

$\mathbb{F}_p[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1) \quad \cong \quad \mathbb{F}_p^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

This leads to $p > 2$

Ideally, we hope:

Here $p^k > 2$ suffices, but NO ring isomorphism!

$\mathbb{F}_{p^k}[X_1, \ldots, X_n]/(X_1^d - 1, \ldots, X_n^d - 1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \ncong \quad \mathbb{F}_p^{kN}$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1 \quad \not\Longleftrightarrow \quad \vec{b}'_0 * \vec{b}'_1 = \vec{z}'_0 + \vec{z}'_1$

Trace to the rescue: $\quad Tr_{\mathbb{F}}: \mathbb{F}_{p^k} \to \mathbb{F}_p, \quad x \longmapsto x + x^{p^1} + \cdots + x^{p^{k-1}}$

$\mathbb{F}_{p^k}^N \quad \longrightarrow \quad \mathbb{F}_p^N$

$Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0) + Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \quad \vec{b}'_0 * \vec{b}'_1 = \vec{z}'_0 + \vec{z}'_1$

Overview: Our Approach

$\mathbb{F}_p[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \quad \cong \quad \mathbb{F}_p^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

This leads to $p > 2$

Ideally, we hope:

Here $p^k > 2$ suffices,
but NO ring isomorphism!

$\mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \cancel{\cong} \quad \mathbb{F}_p^{kN}$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1 \quad \cancel{\Longleftrightarrow} \quad \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$

Trace to the rescue: $\quad Tr_{\mathbb{F}}: \mathbb{F}_{p^k} \to \mathbb{F}_p, \qquad x \mapsto x + x^{p^1} + \cdots + x^{p^{k-1}}$

Define trace maps over $\mathcal{R}_k := \mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1)$, $\boxed{Tr_{\mathcal{R}}: \mathcal{R}_k \to \mathcal{R}_k, \qquad x \mapsto x + x^{p^1} + \cdots + x^{p^{k-1}}}$

$\mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \to \quad \mathbb{F}_p^N$

$Tr_{\mathcal{R}}(b_0) \cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(z_0) + Tr_{\mathcal{R}}(z_1) \Longleftrightarrow Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0) + Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$

Overview: Our Approach

$\mathbb{F}_p[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_p^N$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1$

This leads to $p > 2$

Ideally, we hope:

Here $p^k > 2$ suffices, but NO ring isomorphism!

$\mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \not\cong \quad \mathbb{F}_p^{kN}$

$b_0 \cdot b_1 = z_0 + z_1 \quad \Longleftrightarrow \quad \vec{b}_0 * \vec{b}_1 = \vec{z}_0 + \vec{z}_1 \quad \not\Longleftrightarrow \quad \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$

Trace to the rescue: $Tr_{\mathbb{F}}\colon \mathbb{F}_{p^k} \to \mathbb{F}_p, \quad x \mapsto x + x^{p^1} + \cdots + x^{p^{k-1}}$

Define trace maps over $\mathcal{R}_k := \mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1)$, $\boxed{Tr_{\mathcal{R}}\colon \mathcal{R}_k \to \mathcal{R}_k, \quad x \mapsto x + x^{p^1} + \cdots + x^{p^{k-1}}}$

$\mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \quad \cong \quad \mathbb{F}_{p^k}^N \quad \rightarrow \quad \mathbb{F}_p^N$

$Tr_{\mathcal{R}}(b_0) \cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(z_0) + Tr_{\mathcal{R}}(z_1) \overset{?}{\Longleftrightarrow} Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0) + Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$

Missing pieces: <u>*correctness*</u> and <u>*efficiency*</u> when plugged into PCG paradigm.

More Details of Trace Functions

Let $\phi: \mathcal{R}_k = \mathbb{F}_{p^k}[X_1, \dots, X_n]/(X_1^d - 1, \dots, X_n^d - 1) \to \mathbb{F}_{p^k}^N$ be a ring isomorphism.

Recall that $Tr_{\mathcal{R}}: \mathcal{R}_k \to \mathcal{R}_k,\ x \mapsto x + x^{p^1} + \cdots + x^{p^{k-1}}$

Proposition 1 (Commutative)

$$\begin{tikzcd} \mathcal{R}_k \arrow[r, "\phi"] \arrow[d, "Tr_{\mathcal{R}}"'] & \mathbb{F}_{p^k}^N \arrow[d, "Tr_{\mathbb{F}}"] \\ Im(Tr_{\mathcal{R}}) \arrow[r, "\phi"] & \mathbb{F}_p^N \end{tikzcd}$$

I.e., $Tr_{\mathbb{F}}\big(\phi(x)\big) = \phi(Tr_{\mathcal{R}}(x))$, for any $x \in \mathcal{R}_k$.

Proposition 2 (Additive Hom)

$Tr_{\mathcal{R}}(x) + Tr_{\mathcal{R}}(y) = Tr_{\mathcal{R}}(x + y)$, for any $x, y \in \mathcal{R}_k$.

Correctness

Proposition 3 ($\mathbb{F}_p$-Linearity)

$Tr_{\mathcal{R}}(b_0) \cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}\big(b_0 \cdot Tr_{\mathcal{R}}(b_1)\big)$, by Proposition 1 and $\mathbb{F}_p$-Linearity of $Tr_{\mathbb{F}}$.

Proposition 4 (Sparsity)

Assume s_0 is t-sparse, then $s_0^{p^i}$ is t-sparse for any integer i, since p is the characteristic of $\mathcal{R}_k$

Proposition 5 (Extraction)

Assume b_0 is random, and $(1, \zeta, \dots, \zeta^{k-1})$ is a basis of $\mathbb{F}_{p^k} = \mathbb{F}_p(\zeta)$ over $\mathbb{F}_p$.

Then $\big(Tr(b_0), Tr(\zeta \cdot b_0), \dots, Tr\big(\zeta^{k-1} \cdot b_0\big)\big)$ is random in $\mathbb{F}_p^{kN}$

Efficiency

Attempts

$$\mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \cong \mathbb{F}_{p^k}^N \rightarrow \mathbb{F}_p^N$$

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(z_0) + Tr_{\mathcal{R}}(z_1) \Longleftrightarrow Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0) + Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$$

Prop 4

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(a\cdot s_0 + e_0)\cdot Tr_{\mathcal{R}}(a\cdot s_1 + e_0)$$
$$= \left((as_0+e_0)^{p^0} + \cdots + (as_0+e_0)^{p^{i-1}}\right)\cdot\left((as_1+e_1)^{p^0} + \cdots + (as_1+e_1)^{p^{i-1}}\right)$$

$4k^2$ t^2-sparse cross-terms to be shared

Attempts

$$\mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \cong \mathbb{F}_{p^k}^N \to \mathbb{F}_p^N$$

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(z_0)+Tr_{\mathcal{R}}(z_1) \Longleftrightarrow Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0)+Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$$

Prop 4

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(a\cdot s_0+e_0)\cdot Tr_{\mathcal{R}}(a\cdot s_1+e_0)$$
$$= \left((as_0+e_0)^{p^0}+\cdots+(as_0+e_0)^{p^{i-1}}\right)\cdot\left((as_1+e_1)^{p^0}+\cdots+(as_1+e_1)^{p^{i-1}}\right)$$

$4k^2$ t^2-sparse cross-terms to be shared

Prop 3

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}\big((a\cdot s_0+e_0)\cdot Tr_{\mathcal{R}}(a\cdot s_1+e_0)\big)$$
$$= Tr_{\mathcal{R}}\left((a\cdot s_0+e_0)\cdot\left(\boxed{(as_1+e_1)^{p^0}}+\cdots+(as_1+e_1)^{p^{k-1}}\right)\right)$$

Prop 4

$$= Tr_{\mathcal{R}}\left((a\cdot s_0+e_0)\cdot\left(\boxed{a^{p^0}s_1^{p^0}+e_1^{p^0}}+\cdots+a^{p^{i-1}}s_1^{p^{k-1}}+e_1^{p^{k-1}}\right)\right)$$

$4k$ cross-terms to be shared, i.e.,
$s_0s_1^{p^i}, e_0s_1^{p^i}, s_0e_1^{p^i}, e_0e_1^{p^i}$, for $i\in[0,k-1]$.
They are t^2-sparse by Prop 4

We get N OLEs over $\mathbb{F}_p$

Attempts

$$\mathbb{F}_{p^k}[X_1,\dots,X_n]/(X_1^d-1,\dots,X_n^d-1) \cong \mathbb{F}_{p^k}^N \to \mathbb{F}_p^N$$

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(z_0)+Tr_{\mathcal{R}}(z_1) \Longleftrightarrow Tr_{\mathbb{F}}(\vec{b}_0) * Tr_{\mathbb{F}}(\vec{b}_1) = Tr_{\mathbb{F}}(\vec{z}_0)+Tr_{\mathbb{F}}(\vec{z}_1) \Longrightarrow \vec{b}_0' * \vec{b}_1' = \vec{z}_0' + \vec{z}_1'$$

Prop 4

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}(a\cdot s_0+e_0)\cdot Tr_{\mathcal{R}}(a\cdot s_1+e_1)$$
$$=\left((as_0+e_0)^{p^0}+\cdots+(as_0+e_0)^{p^{i-1}}\right)\cdot\left((as_1+e_1)^{p^0}+\cdots+(as_1+e_1)^{p^{i-1}}\right)$$

$4k^2$ t^2-sparse cross-terms to be shared

Prop 3

$$Tr_{\mathcal{R}}(b_0)\cdot Tr_{\mathcal{R}}(b_1) = Tr_{\mathcal{R}}\big((a\cdot s_0+e_0)\cdot Tr_{\mathcal{R}}(a\cdot s_1+e_1)\big)$$
$$=Tr_{\mathcal{R}}\left((a\cdot s_0+e_0)\cdot\left(\boxed{(as_1+e_1)^{p^0}}+\cdots+(as_1+e_1)^{p^{k-1}}\right)\right)$$

Prop 4

$$=Tr_{\mathcal{R}}\left((a\cdot s_0+e_0)\cdot\left(\boxed{a^{p^0}s_1^{p^0}+e_1^{p^0}}+\cdots+a^{p^{i-1}}s_1^{p^{k-1}}+e_1^{p^{k-1}}\right)\right)$$

$4k$ cross-terms to be shared, i.e.,
$s_0s_1^{p^i}, e_0s_1^{p^i}, s_0e_1^{p^i}, e_0e_1^{p^i}$, for $i\in[0,k-1]$.
They are t^2-sparse by Prop 4

We get N OLEs over $\mathbb{F}_p$

Prop 5

$$Tr_{\mathcal{R}}(\zeta^j b_0)\cdot Tr_{\mathcal{R}}(\zeta^j b_1) = Tr_{\mathcal{R}}\left(\zeta^j(a\cdot s_0+e_0)\cdot Tr_{\mathcal{R}}\left(\zeta^j(a\cdot s_1+e_1)\right)\right)$$
$$=Tr_{\mathcal{R}}\left(\zeta^j(a\cdot s_0+e_0)\cdot\left(\boxed{\zeta^{jp^0}(as_1+e_1)^{p^0}}+\cdots+\zeta^{jp^{k-1}}(as_1+e_1)^{p^{k-1}}\right)\right)$$

Prop 4

$$=Tr_{\mathcal{R}}\left(\zeta^j(a\cdot s_0+e_0)\cdot\left(\boxed{\zeta^{jp^0}a^{p^0}s_1^{p^0}+\zeta^{jp^0}e_1^{p^0}}+\cdots+\zeta^{jp^{k-1}}a^{p^{i-1}}s_1^{p^{k-1}}+\zeta^{jp^{k-1}}e_1^{p^{k-1}}\right)\right)$$

Hence, $\left[s_0s_1^{p^i}\right], \left[e_0s_1^{p^i}\right], \left[s_0e_1^{p^i}\right], \left[e_0e_1^{p^i}\right]$, can be reused among k extractions

We get kN OLEs over $\mathbb{F}_p$

Concrete Instantiation: $\mathbb{F}_4$ to $\mathbb{F}_2$ via *Trace*

$s_0, e_0, Seed_0$ ← PCG. GEN → $s_1, e_1, Seed_1$

Goal: $2N$ OLE correlations over $\mathbb{F}_2$

$$[Tr(b_0)\cdot Tr(b_1)] = Tr\left(a^2[s_0 s_1]\right) + Tr\left([s_0 s_1^2]\right)$$
$$+Tr(a[s_0 e_1]) + Tr\left(a\left[s_0 e_1^2\right]\right) + Tr(a[s_1 e_0]) + Tr\left(a\left[s_1 e_0^2\right]\right)$$
$$+ Tr([e_0 e_1]) + Tr\left([e_0 e_1^2]\right)$$

$s_0, e_0 \in \mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1)$

$s_1, e_1 \in \mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

$b_1 = a \cdot s_1 + e_1 \approx \$$

(1) QA-SD (or Ring-LPN for large $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$)

(2) 8 t^2-sparse cross-terms for $2 \cdot 3^n$ OLEs

(3) $\mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1) \cong \mathbb{F}_4^{3^n}$

$Seed_0$

PCG. EXPAND ↓

$[s_0 s_1]_0, [s_0 s_1^2]_0, [s_0 e_1]_0, [s_0 e_1^2]_0,$
$[s_1 e_0]_0, [s_1 e_0^2]_0, [e_0 e_1]_0, [e_0 e_1^2]_0$

↓

$z_0^{(j)} = [Tr(\zeta^j b_0) \cdot Tr(\zeta^j b_1)]_0$

$Seed_1$

PCG. EXPAND ↓

$[s_0 s_1]_0, [s_0 s_1^2]_0, [s_0 e_1]_0, [s_0 e_1^2]_0,$
$[s_1 e_0]_0, [s_1 e_0^2]_0, [e_0 e_1]_0, [e_0 e_1^2]_0$

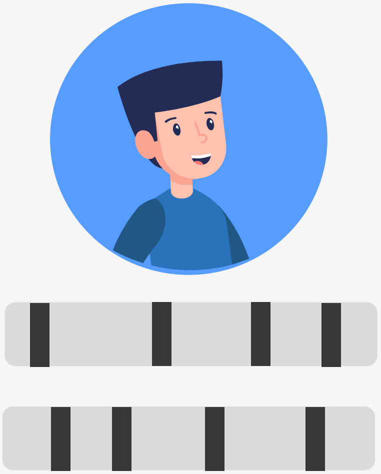
↓

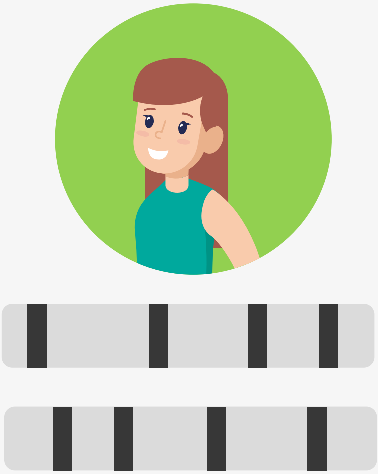
$z_0^{(j)} = [Tr(\zeta^j b_0) \cdot Tr(\zeta^j b_1)]_0$

$\vec{b}_0^{(j)} * \vec{b}_1^{(j)} = \vec{z}_0^{(j)} + \vec{z}_1^{(j)}$

Application: PCG for Authenticated Binary Triple

$s_0, e_0, Seed_0$ $\xleftarrow{}$ PCG. GEN $\xrightarrow{}$ $s_1, e_1, Seed_1$





Goal: 2N Authenticated Binary triple

$$
\begin{aligned}
&[\Delta \cdot Tr(b_0) \cdot Tr(b_1)] \\
&= [\Delta(a^2 s_0^2 + e_0^2 + a s_0 + e_0)(a^2 s_1^2 + e_1^2 + a s_1 + e_1)] \\
&= a^2 \cdot ([\Delta s_0^2 e_1^2] + [\Delta s_0^2 e_1] + [\Delta s_0 s_1] + [\Delta s_1^2 e_0^2] + [\Delta s_1^2 e_0]) \\
&+ a([\Delta s_0^2 s_1^2] + [\Delta s_0 e_1^2] + [\Delta s_0 e_1] + [\Delta s_1 e_0^2] + [\Delta s_1 e_0]) \\
&+ ([\Delta s_0^2 s_1] + [\Delta s_1^2 s_0] + [\Delta e_0^2 e_1^2] + [\Delta e_0^2 e_1] + [\Delta e_0 e_1^2] + [\Delta e_0 e_1])
\end{aligned}
$$

$s_0, e_0 \in \mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1)$

$s_1, e_1 \in \mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1)$

$b_0 = a \cdot s_0 + e_0 \approx \$$

Global MAC key $\Delta \in \mathbb{F}_{2^\lambda}$

$b_1 = a \cdot s_1 + e_1 \approx \$$

$\Delta_0 \in \mathbb{F}_{2^\lambda} = \mathbb{F}_4(\xi)$

$\Delta_1 \in \mathbb{F}_{2^\lambda} = \mathbb{F}_4(\xi)$

(1) QA-SD over $\mathbb{F}_4[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1)$

(2) $\mathbb{F}_{2^\lambda}[X_1, \dots, X_n]/(X_1^3 - 1, \dots, X_n^3 - 1) \cong \mathbb{F}_{2^\lambda}^{3^n} \cong \left(\mathbb{F}_4(\xi)\right)^{3^n}$

(3) Prop.3 ($\mathbb{F}_2$-linearity) is not applicable since $\Delta \in \mathbb{F}_{2^\lambda}$

(4) 16 t^2-sparse cross-terms for $2 \cdot 3^n$ triples (Prop.5 Extraction)

Summary

1. First concretely efficient PCG for many useful correlations over *ANY* finite field
   (i) OLE/Beaver triple, yielding semi-honest MPC over Boolean circuits with silent preprocessing
   (ii) Two-party authenticated binary multiplication triple
   (iii) Matrix multiplication triple, (string) OT *(Omitted)*
2. As efficient as previous PCG for large fields: same communication, $\approx 2 \times$ computation
3. Security relies on standard existing assumptions (QA-SD/Ring-LPN)

Summary

1. First concretely efficient PCG for many useful correlations over *ANY* finite field
   (i) OLE/Beaver triple, yielding semi-honest MPC over Boolean circuits with silent preprocessing
   (ii) Two-party authenticated binary multiplication triple
   (iii) Matrix multiplication triple, (string) OT *(Omitted)*
2. As efficient as previous PCG for large fields: same communication, $\approx 2\times$ computation
3. Security relies on standard existing assumptions (QA-SD/Ring-LPN)

Future work & Open problems:

1. PCG for OLE over $\mathbb{Z}_{2^k}$ and SPD$\mathbb{Z}_{2^k}$ triples. *(To appear at CRYPTO 2025)*
2. PCG for higher degree or more complex correlations. *(it is interesting to consider **Norm** map)*
3. PCG for multiparty authenticated triples.

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

Thank You

饮 水 思 源　爱 国 荣 校

Reference

[BCGIKS 19] Efficient Pseudorandom Correlation Generators: Silent OT Extension and More
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl (CRYPTO 2019)

[KPR 18] Overdrive: Making SPDZ Great Again
Marcel Keller, Valerio Pastro, and Dragos Rotaru (EUROCRYPT 2018)

[BCGIKS 20] Efficient Pseudorandom Correlation Generators from Ring-LPN
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl (CRYPTO 2020)

[BCGIKRS 23] Oblivious Transfer with Constant Computational Overhead
Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl. (EUROCRYPT 2023)

[BCCD 23] Correlated Pseudorandomness from the Hardness of Quasi-abelian Decoding
Maxime Bombar, Geoffroy Couteau, Alain Couvreur, and Clément Ducros (CRYPTO 2023)

[BBCCDS 24] FOLEAGE: F4OLE-Based MultiParty Computation for Boolean Circuits
Maxime Bombar, Dung Bui, Geoffroy Couteau, Alain Couvreur, Clément Ducros, and Sacha Servan-Schreiber (ASIACRYPT 2024)

[Roy 22] SoftSpokenOT: Quieter OT Extension from Small-field Silent VOLE in the Minicrypt Model
Lawrence Roy (CRYPTO 2022)