Correlated Pseudorandomness from Expand-Accumulate Codes

Crypto 2022 · `https://ia.cr/2022/1014`

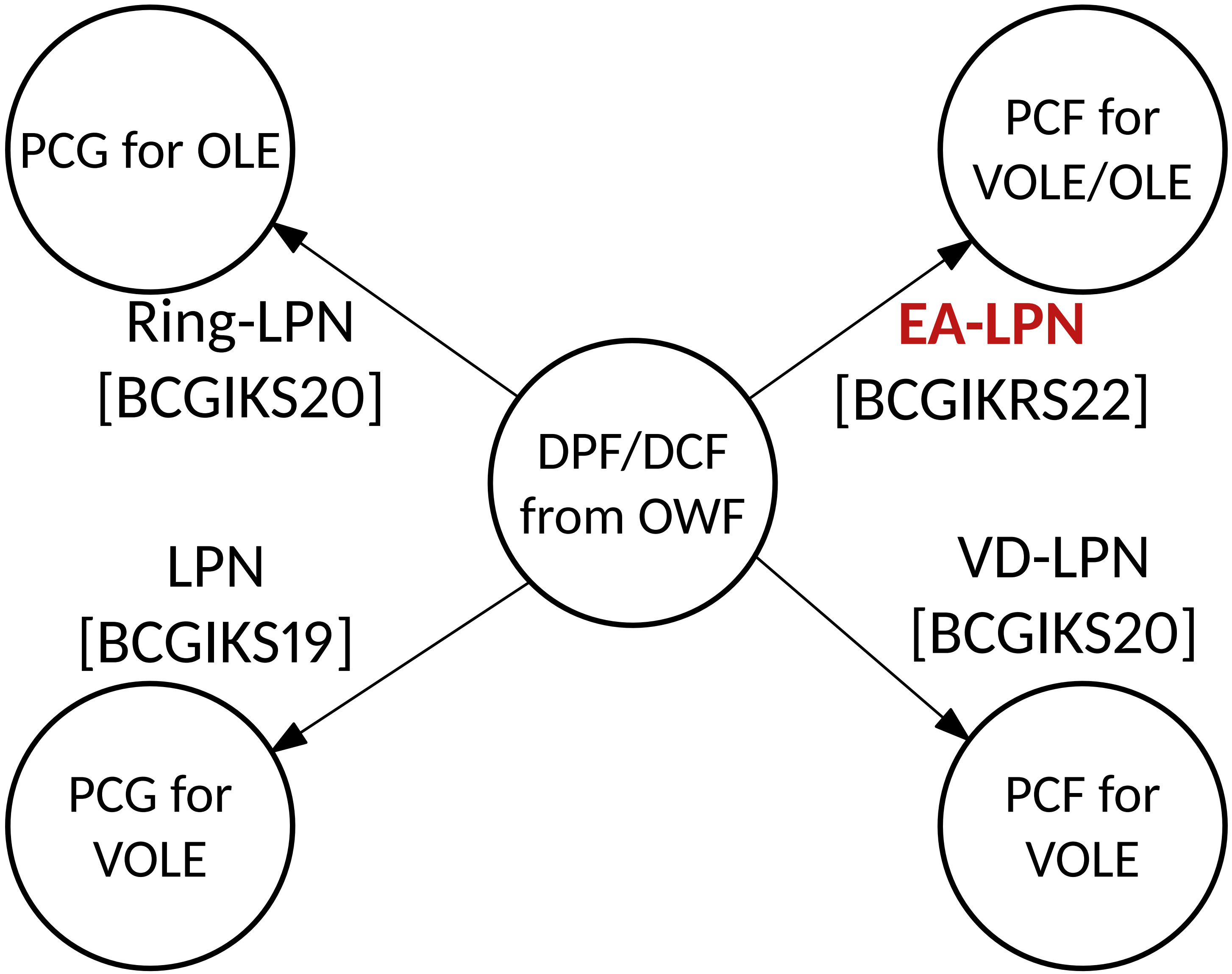
Elette Boyle · Geoffroy Couteau · Niv Gilboa ·
Yuval Ishai · Lisa Kohl · Nicolas Resch · Peter Scholl

December 4, 2022· Presented by Hongrui Cui

* Some acknowledgments?

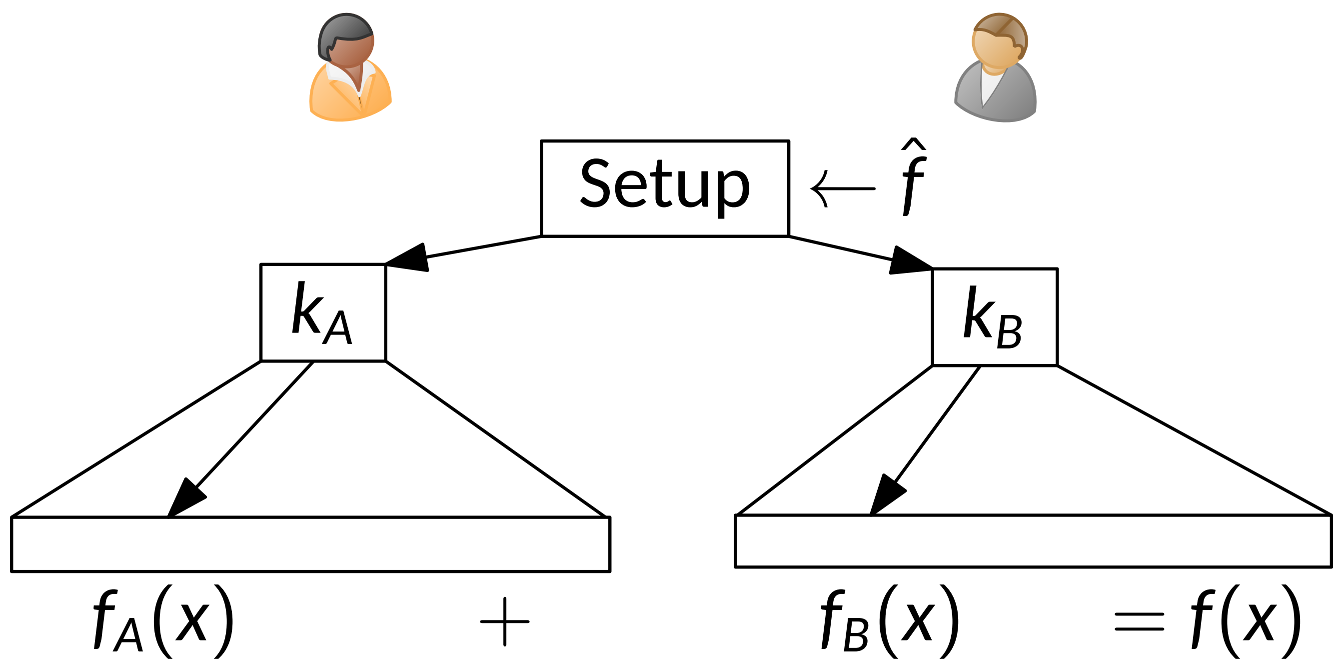
Introduction

- PCG/PCF paradigm = FSS + LPN
- The main contribution is a new LPN variant and FSS optimization



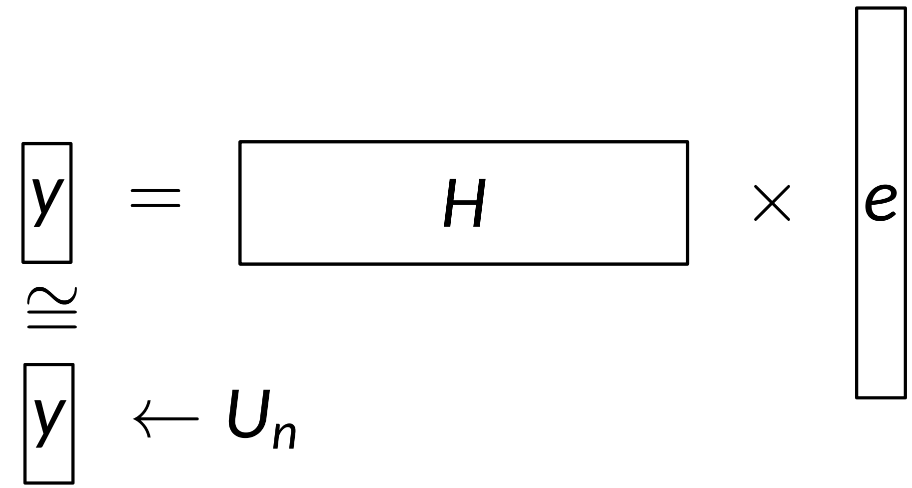
Preliminaries on PCG/PCF

Function Secret Sharing



- Succinctness: $|k_A|, |k_B| \ll 2^{|x|}$
- Efficient FSS exists for point/comparison functions

dual-LPN



- View e as seed, H is a linear PRG
- PCG idea: generate sparse correlations as seed and expand them using dual-LPN

Example: PCG for VOLE

- KeyGen:

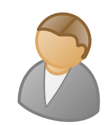
Step 1: $e \leftarrow \chi^N$ $\quad e = \begin{array}{|cccc|}\hline \beta_1 & \beta_2 & \dots & \beta_\ell \\ \hline \end{array}$

$$\begin{array}{cccc} \alpha_1 & \alpha_2 & \dots & \alpha_\ell \end{array}$$

Step 2: $(k_0^1, k_1^1) \leftarrow FSS.KeyGen(\alpha_1, \beta_1 \cdot \Delta)$

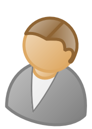
$\dots$

$(k_0^\ell, k_1^\ell) \leftarrow FSS.KeyGen(\alpha_\ell, \beta_\ell \cdot \Delta)$

 $key_0 := \{k_0^1, ..., k_0^\ell\}, \Delta$  $key_1 := \{k_1^1, ..., k_1^\ell\}, e$

- Expand:

 $w := H \cdot (FullEval(k_0^1) + ... + FullEval(k_0^\ell))$

 $v := H \cdot (FullEval(k_1^1) + ... + FullEval(k_1^\ell)), u := H \cdot e$

$$w + v = \begin{array}{c} \begin{array}{|c|}\hline \beta_1 \cdot \Delta \qquad\qquad\qquad \\ \hline \end{array} \\ + ... + \\ \begin{array}{|c|}\hline \qquad\qquad\qquad \beta_\ell \cdot \Delta \\ \hline \end{array} \end{array} = H \cdot e \cdot \Delta = u \cdot \Delta$$

From PCG to PCF

- Analogous to the extension from PRG to PRF
- Main problem: N is super-polynomial
- If H has no structure, then evaluating the inner-product is infeasible

$$N > n$$

$$n = \kappa^{\omega(1)} \quad \boxed{y} = \boxed{H} \times \boxed{e}$$

Expand-Accumulate LPN

- Structure:

$$\boxed{\quad H \quad} = \underset{c_1\, c_2\ \cdots\ c_N}{\boxed{\quad Ber \quad}} \times \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix}$$

  - $h_N = c_N$
  - $h_{N-1} = h_N + c_{N-1}$
  - $h_1 = h_2 + c_1$

- Proof strategy: Prove that one row in H is high-weight whp.

- Intuition1: Bernoulli noise accumulates to uniform due to pilling up lemma
- Intuition2: Columns of H corresponds to random walk

Tools: Random Walk and Markov Chain

Theorem 3.6 (Expander Hoeffding Bound) *Let $(\mathcal{V}, P)$ denote a finite, irreducible and reversible Markov chain with stationary distribution $\vec{\pi}$ and second largest eigenvalue λ. Let $f : \mathcal{V} \to [0,1]$ with $\mu = \mathbb{E}_{V\sim\vec{\pi}}[f(V)]$. For any integer $N \geq 1$, consider the random variable $S_N = \sum_{i=1}^{N} f(V_i)$, where V_0 is sampled uniformly at random from V and then $V_1, \ldots, V_N$ is a random walk starting at V_0.*

Then, for $\lambda_0 = \max(0, \lambda)$ and any $\varepsilon > 0$ with $\mu + \varepsilon < 1$, the following bound holds:

$$\Pr[S_N \geq N(\mu + \varepsilon)] \leq \exp\left(-2\frac{1-\lambda_0}{1+\lambda_0}N\varepsilon^2\right) .$$

- Applying Markov bound

Corollary 3.7 *Let $(\mathcal{V}, P)$ denote a finite, irreducible and reversible Markov chain with $\mathcal{V} = \{v_0, v_1\}$, stationary distribution $\vec{\pi} = (1/2, 1/2)$ and second largest eigenvalue λ. Let $f : \mathcal{V} \to [0,1]$ with $1/2 = \mathbb{E}_{V\sim\vec{\pi}}[f(V)]$. For any integer $N \geq 1$, consider the random variable $\tilde{S}_N = \sum_{i=1}^{N} f(V_i)$, where $V_0 = v_0$ with probability 1 and then $V_1, \ldots, V_N$ is a random walk starting at v_0.*

Then, for $\lambda_0 = \max(0, \lambda)$ and any $\varepsilon > 0$ with $1/2 + \varepsilon < 1$, the following bound holds:

$$\Pr\left[\tilde{S}_N \geq N(1/2 + \varepsilon)\right] \leq 2\exp\left(-2\frac{1-\lambda_0}{1+\lambda_0}N\varepsilon^2\right) .$$

Security of EA-LPN against Linear Attack

Theorem 3.10 *Let $n, N \in \mathbb{N}$ with $n \leq N$ and put $R = \frac{n}{N}$, which we assume to be a constant. Let $C > 0$ and set $p = \frac{C \ln N}{N} \in (0, 1/2)$. Fix $\delta \in (0, 1/2)$ and put $\beta = 1/2 - \delta$. Assume the following relation holds:*

$$R < \min\left\{\frac{2}{\ln 2} \cdot \frac{1 - e^{-1}}{1 + e^{-1}} \cdot \boxed{\beta^2}, \frac{2}{e}\right\} \tag{2}$$

Then, assuming N is sufficiently large we have

$$\begin{aligned}\Pr\left[\mathsf{d}(H) \geq \delta N \mid H \xleftarrow{\$} \mathsf{EAGen}(n, N, p)\right] &\geq 1 - 2\sum_{r=1}^{n} \binom{n}{r} \exp\left(-2\frac{1 - \xi_r}{1 + \xi_r} N\beta^2\right) \\ &\geq 1 - 2RN^{-2\beta^2 C + 2}.\end{aligned} \tag{3}$$

- (ϵ, η)-security: $\Pr[\mathsf{d}(H) \geq d] > \eta$ and $\max_{|v| \geq d} \mathsf{bias}_v(\chi^N) \leq \epsilon$
- $\mathsf{d}(H) \geq \delta N \to$ bias $\leq \frac{1}{2} \cdot (1 - 2 \cdot \frac{t}{N})^{\delta N} \approx \frac{1}{2} \cdot 2^{-2t\delta}$
- For $C = O(1)$, $\eta = 1 - \frac{1}{\mathsf{poly}}$; for $C = \log(N)$, $\eta = 1 - \mathsf{negl}$

Proving Theorem 3.10 Using Random Walk

- Differentiate between different hamming weight of x

$$\boxed{x^T} \times \boxed{H} = \boxed{x^T} \times \boxed{Ber(p)} \times \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix}$$

$$= \boxed{Ber'(p')} \times A$$

- Pilling-up lemma: $2 \cdot Bias' = (2 \cdot Bias)^{|x|} \iff \xi_r = \xi^r$ s.t. $|x| = r$
- Applying the Hoeffding bound:

$$\Pr[\mathrm{wt}(Ber') \leq (\tfrac{1}{2} - \beta) \cdot N] \leq 2 \cdot \exp(-2 \cdot \tfrac{1-2\cdot Bias'}{1+2\cdot Bias'} \cdot N \cdot \beta^2)$$

- This gives the first inequality in Theorem 3.10

$$\Pr\left[\mathsf{d}(H) \geq \delta N \mid H \xleftarrow{\$} \mathsf{EAGen}(n, N, p)\right] \geq 1 - 2\sum_{r=1}^{n} \binom{n}{r} \exp\left(-2\frac{1-\xi_r}{1+\xi_r} N\beta^2\right)$$

Bounding the Failure Probability

- $r = 1$

$$\binom{n}{1} \exp(-2 \cdot \frac{1-\xi}{1+\xi} \cdot N \cdot \beta^2) \leq RN \cdot \exp(-2pN\beta^2)$$

$$= RN \cdot \exp(-2\frac{C \ln N}{N} N\beta^2)$$

$$\leq N^{-2C\beta^2+1}$$

- $2 \leq r \leq \frac{N}{2C \ln N}$: Equivalent to prove

$$\ln\left(\binom{n}{r} \exp(-2 \cdot \tfrac{1-\xi_r}{1+\xi_r} N\beta^2)\right) = -\Omega(\log N)$$

$$-1 \cdot \ln\left(\binom{n}{r} \exp(-2 \cdot \frac{1-\xi_r}{1+\xi_r} N\beta^2)\right) = 2 \cdot \frac{1-\xi_r}{1+\xi_r} N\beta^2 - \ln\binom{n}{r}$$

$$\geq (1-\xi_r)N\beta^2 - r\ln(\frac{eRN}{r}) \geq \ln(N^{2C\beta^2-1})$$

$$R \leq \frac{e}{2}$$

Bounding Failure Probability (Continued)

- $r \geq \frac{N}{2C \ln N}$

$$\xi_r = (1 - \tfrac{2C \ln N}{N})^r \leq e^{-1}$$
$$\ln \tbinom{n}{r} \leq \ln(2^{RN}) = RN \ln(2)$$

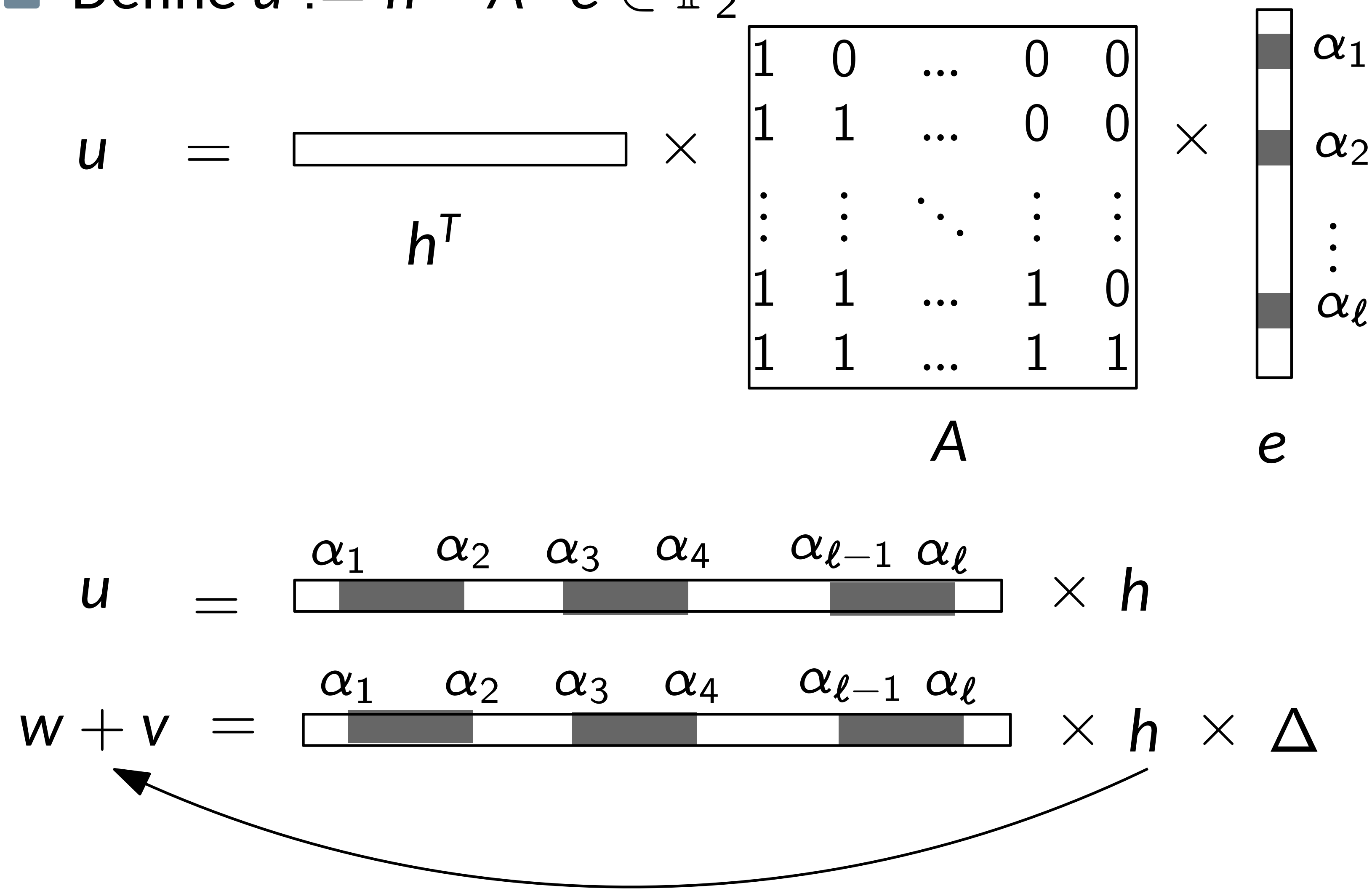
$$-1 \cdot \ln \left(\binom{n}{r} \exp(-2 \cdot \frac{1-\xi_r}{1+\xi_r} N\beta^2) \right) = 2 \cdot \frac{1-\xi_r}{1+\xi_r} N\beta^2 - \ln \binom{n}{r}$$
$$\geq 2 \cdot \frac{1-e^{-1}}{1+e^{-1}} N\beta^2 - RN \ln(2) > 0 \qquad R < 2 \cdot \tfrac{1-e^{-1}}{1+e^{-1}} \cdot \tfrac{\beta^2}{\ln(2)}$$

- Summing over $1 \leq r \leq n$:

$$\Pr[\text{Fail}] \leq 2 \cdot n \cdot N^{-2C\beta^2+1} = 2 \cdot R \cdot N^{-2C\beta^2+2}$$

Constructing PCF from EA-LPN

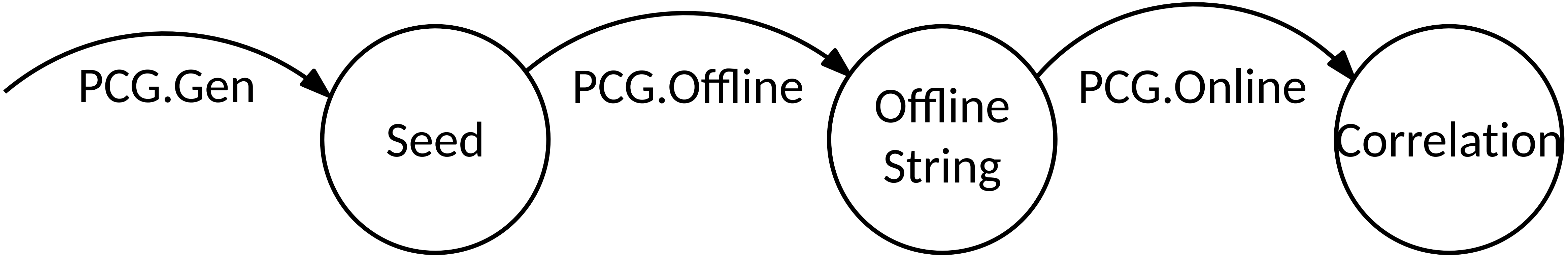
- Sample one row of H: $\mathsf{Samp}(x) \mapsto h^T$
- Define $u := h^T \cdot A \cdot e \in \mathbb{F}_2$



Run DCF on every (public) non-zero coordinate of h

Generalizations

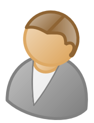
- Offline/Online PCG



- Motivation: Utilize online idle time to mitigate offline burden

- Expand:

$$w := H \cdot (FullEval(k_0^1) + ... + FullEval(k_0^\ell))$$

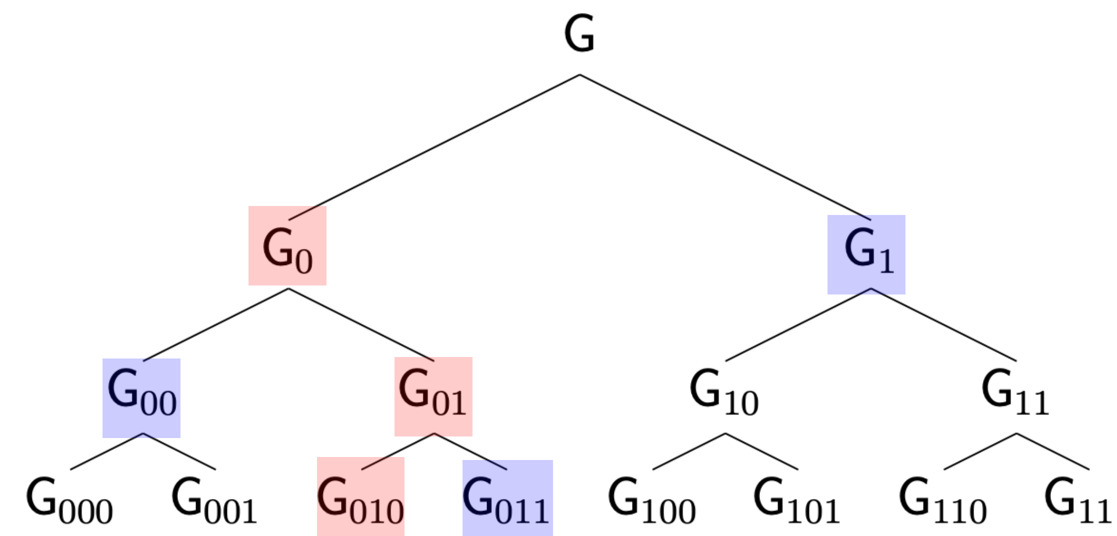


$$v := H \cdot (FullEval(k_1^1) + ... + FullEval(k_1^\ell)), u := H \cdot e$$

$$\boxed{H \leftarrow Ber} \times \boxed{}$$ offline string

Relaxed Distributed Comparison Function

- RDCF: $f(x) = \begin{cases} 0 & x \leq \alpha \\ \beta & x > \alpha \end{cases}$ $\quad \mathrm{Expand}(k^0) \mapsto \alpha, y^0 \quad \mathrm{Expand}(k^0) \mapsto y^1$
- Example: $\alpha = 010$



- $\gamma_1 = H(G), \gamma_2 = H(G_0), \gamma_3 = H(G_{01})$
- $c_1 = \bar{\alpha}_1 \cdot \gamma_1, c_2 = \bar{\alpha}_2 \cdot \gamma_2, c_3 = \bar{\alpha}_3 \cdot \gamma_3$
- $B_i = c_1 + \ldots + c_{i-1} + \alpha_i \cdot \gamma_i + \alpha_i \cdot \beta$

$k^1 := G$

$k^0 := \langle \alpha, \{B_i\}, y = G_{010} + \sum c_i, G_1, G_{00}, G_{011} \rangle$

- Eval (x): Define $c_1^1 = \bar{x}_1 \cdot H(G), c_2^1 = \bar{x}_2 \cdot H(G_{x_1}), c_3^1 = \bar{x}_3 \cdot H(G_{x_1 x_2})$

$f^1(x) = G_{x_1 x_2 x_3} + \sum c_i^1$

$$f^0(x) = \begin{cases} y & x = \alpha \\ G_{x_1 x_2 x_3} + B_j + c_{j+1}^1 + \ldots + c_m^1 & x \neq \alpha \end{cases}$$

Offline Optimization: UPF

- Replace pseudorandomness in PPRF by unpredictability

$\underline{\mathsf{Exp}^{\mathsf{unp}}_{\mathsf{UPF},\mathcal{A}}(\lambda)}$:

$\alpha \xleftarrow{\$} \mathcal{X}_\lambda$

$k \leftarrow \mathsf{Setup}(1^\lambda)$

$k^* \leftarrow \mathsf{Puncture}(k, \alpha)$

$y \leftarrow \mathcal{A}(k^*, \alpha)$

$\textbf{If } y = \mathsf{Eval}(k, \alpha) \textbf{ return } 1$

$\textbf{Else return } 0.$

- Step1: a UPF that takes N ROs
- Step2: a PPRF by hashing the left leaves of UPF that takes $N/2$ ROs
- Computation saving: $2N \rightarrow 1.5N$

Summary

- Contribution 1: EA-LPN
- Contribution 2: Offline Optimization (subsumed by Half-tree 2022/1431)

	Assump.	Corr.	Computation	Communication (bits)	
				$P_0 \to P_1$	$P_1 \to P_0$
[BCG+22]	ROM	sVOLE	m RO calls	$2t(\log \frac{m}{t} - 1)\lambda + 3t \log \lvert\mathbb{K}\rvert$	$t \log \lvert\mathbb{F}\rvert$
	Ad-hoc[1]	sVOLE	m RP calls + $0.5m$ RO calls		
This work	RPM	COT	m RP calls	$t(\log \frac{m}{t} - 1)\lambda + \lambda$	–
		sVOLE	m RP calls	$t(\log \frac{m}{t} - 1) \log \lvert\mathbb{K}\rvert + \lambda$	$t(\log \frac{m}{t} + 1) \log \lvert\mathbb{F}\rvert$
		sVOLE	$1.5m$ RP calls	$t(\log \frac{m}{t} - 2)\lambda + 3t \log \lvert\mathbb{K}\rvert + \lambda$	$t \log \lvert\mathbb{F}\rvert$

[1] Security relies on the conjecture that the adversary cannot evaluate the punctured result in their RPM-based UPF, where the GGM-style tree expansion uses $G(x) := \mathsf{H}_0(x) \,\|\, \mathsf{H}_1(x)$ for $\mathsf{H}_0(x) := \mathsf{H}(x) \oplus x$ and $\mathsf{H}_1(x) := \mathsf{H}(x) + x \bmod 2^\lambda$.

Table 2: **Comparison with the concurrent work.** "RO/ROM" (resp., "RP/RPM") is short for random oracle (resp., permutation) and the model. m denotes the length of sVOLE correlations. Computation is measured by the amount of symmetric-key operations. In practice, there is also some LPN-related computation cost. Assume weight-t regular LPN noises in sVOLE extension with field $\mathbb{F}$ and extension field $\mathbb{K}$.