Multiparty DPF

Based on ePrint 2025/1074

Hongrui Cui

Shanghai Jiao Tong University

June 18, 2025

Syntax of Multiparty DPF

Point Functions

Given domain $\mathcal{D}$ and range $\mathcal{R}$, a *point function* $f_{\alpha,\beta}$ for $\alpha \in \mathcal{D}, \beta \in \mathcal{R}$ is defined as:

$$f_{\alpha,\beta}(x) = \begin{cases} \beta & x = \alpha \\ 0 & x \neq \alpha \end{cases}$$

Distributed Point Functions

A p-party DPF scheme is defined by two algorithms:

- $\mathrm{Gen}(\alpha, \beta) \mapsto (k_0, \ldots, k_{p-1})$
- $\mathrm{Eval}(i, k_i, x) \mapsto y_i \in \mathcal{R}$

They should satisfy two properties:

- **Correctness:** $y_0 + \ldots + y_{p-1} = f_{\alpha,\beta}(x)$
- **Security:** $\{k_j\}_{j \neq i^*}$ do not leak α, β

Contributions

Prior art in **Minicrypt**: (Let $O(S) = O(S \cdot (\lambda + \log(|\mathcal{R}|)))$)

Lemma ([BGI15])

Assuming OWF, there is a p-party DPF scheme with key size

$$O(2^{p-1} \cdot |\mathcal{D}|^{1/2})$$

New Result

A p-party DPF scheme with key size

$$O(p^3 \cdot |\mathcal{D}|^{1/2+\epsilon})$$

Multiparty DPF Framework

Consider a 3-party DPF with $\mathcal{D} = \{0,1\}^n = [0, N)$, $\mathcal{R} = \{0,1\}$.

- A trivial scheme:
  - Let $T := (f_{\alpha,\beta}(0...00), f_{\alpha,\beta}(0...01), ..., f_{\alpha,\beta}(1...11))$
  - For $i \in \{0,1,2\}$, $k_i = [\![T]\!]_i$
  - $\mathsf{Eval}(i, k_i, x) = k_i[x]$
- Quadratic improvement from PRG: Decompose $\alpha = \alpha_r \cdot \sqrt{N} + \alpha_c$

$$T = \sqrt{N}\left\{\overbrace{\begin{matrix} 0 \cdots 0 \cdots 0 \\ \vdots \quad \vdots \quad \vdots \\ 0 \cdots 0 \cdots 0 \\ 0 \cdots 1 \cdots 0 \\ 0 \cdots 0 \cdots 0 \\ \vdots \quad \vdots \quad \vdots \\ 0 \cdots \underset{\substack{\uparrow \\ \alpha_c}}{0} \cdots 0 \end{matrix}}^{\sqrt{N}}\right. \begin{matrix} \\ \\ \\ \leftarrow \alpha_r \\ \\ \\ \\ \end{matrix}$$

- For $i \in [0, \sqrt{N})$:
  - If $i \neq \alpha_r$, Sample $s_0, s_1, s_2 \in \{0,1\}^\lambda$, $k_0[i] = (s_0, s_1)$, $k_1[i] = (s_1, s_2)$, $k_2[i] = (s_2, s_0)$
  - If $i = \alpha_r$, Sample $s_0, s_1, s_2, s' \in \{0,1\}^\lambda$, $k_0[i] = (s_0, s')$, $k_1[i] = (s_1, s')$, $k_2[i] = (s_2, s')$
- $\widetilde{\mathsf{Eval}}(i, k_i, x)$: Let $x = x_r \cdot \sqrt{N} + x_c$.
  - Parse $k_i[x_r] := (s, s')$
  - Output $\mathsf{PRG}(s) \oplus \mathsf{PRG}(s') \in \{0,1\}^{n/2}$

Multiparty DPF Framework

Row Recovery

- $x_r \neq \alpha_r$:

$$\begin{pmatrix} \mathrm{PRG}(s_0) \\ \oplus \\ \mathrm{PRG}(s_1) \end{pmatrix} \oplus \begin{pmatrix} \mathrm{PRG}(s_1) \\ \oplus \\ \mathrm{PRG}(s_2) \end{pmatrix} \oplus \begin{pmatrix} \mathrm{PRG}(s_2) \\ \oplus \\ \mathrm{PRG}(s_0) \end{pmatrix} = 0^{\sqrt{N}}$$

- $x_r = \alpha_r$:

$$\begin{pmatrix} \mathrm{PRG}(s_0) \\ \oplus \\ \mathrm{PRG}(s') \end{pmatrix} \oplus \begin{pmatrix} \mathrm{PRG}(s_1) \\ \oplus \\ \mathrm{PRG}(s') \end{pmatrix} \oplus \begin{pmatrix} \mathrm{PRG}(s_2) \\ \oplus \\ \mathrm{PRG}(s') \end{pmatrix} = \underbrace{\begin{pmatrix} \mathrm{PRG}(s') \oplus \mathrm{PRG}(s_0) \\ \oplus \\ \mathrm{PRG}(s_1) \oplus \mathrm{PRG}(s_2) \end{pmatrix}}_{\mathbf{r}}$$

We need to fix $\mathbf{r}$ to $\mathbf{e}_{\alpha_c}$

Multiparty DPF Framework

Column Fixing

During Gen($\alpha = \alpha_r \cdot \sqrt{N} + \alpha_c, \beta$), generate

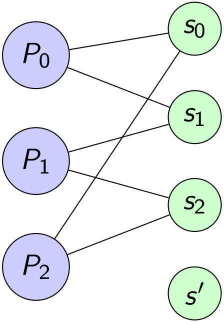
- $\sqrt{N}$ set of PRG seeds
- $[\![\mathbf{e}_{\alpha_r}]\!]$
- $\mathsf{cw} := \mathbf{r} \oplus \beta \cdot \mathbf{e}_{\alpha_c}$
- $k_i := (\mathsf{seeds}, \mathsf{cw}, [\![\mathbf{e}_{\alpha_r}]\!]_i)$

During Eval($i, k_i, x = x_r \cdot \sqrt{N} + x_c$):

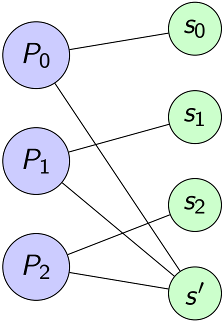
- Recover the x_r-th row $\tilde{\mathbf{y}} \in \{0,1\}^{\sqrt{N}}$ from PRG
- Compute $\mathbf{y} = \tilde{\mathbf{y}} \oplus [\![\mathbf{e}_{\alpha_r}]\!]_i[x_r] \cdot \mathsf{cw}$
- Output $\mathbf{y}[x_c]$

Using a bipartite graph to model this process

G_0: **Sharing Zero Row**



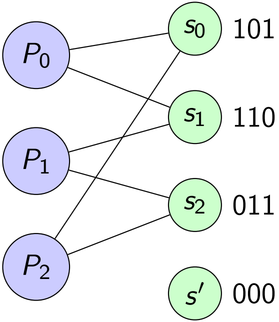
G_1: **Sharing Non-Zero Row**

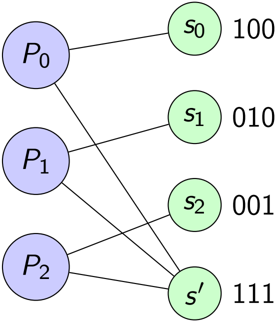


- **Correctness**: Right nodes in G_0 has even degrees
- **Pseudorandom**: Every left node in G_1 has an exclusive right node
- **Privacy**: For $i \in \{0, 1, 2\}$, the subgraph of removing P_i in G_0 and G_1 should be identical

From 3-party to p-parties

We can describe the bipartite graph G_0, G_1 using a series of vectors:





p-party DPF [BGI15]

- G_0: Set of even Hamming weights
- G_1: Set of odd Hamming weights

Negative Result

A lower bound on deterministic bipartite graphs

The total number of seeds in G_0 or $G_1 \geq 2^{p-1}$

Proof.

We prove by induction that G_0 has all even-weight vectors and G_1 has all odd-weight vectors.

- **Base**: $i = 1$: Pseudorandomness
- **Hypothesis**: Result holds for $\mathbf{hw} \leq i$
- **Induction** (odd i):
  - By **Hypothesis**, $\forall \mathbf{v} \in \{0,1\}^p$ s.t. $\mathrm{HW}(\mathbf{v}) = i$, $\mathbf{v} \in G_1$
  - By **Privacy**, $\forall j \in [0,p)$, $\mathbf{v}[j] = 0$, $\mathbf{v}^* \in G_0$ s.t. $\mathbf{v}[i] = \mathbf{v}^*[i]$, $i \neq j$
  - By **Correctness**, $\mathrm{HW}(\mathbf{v}^*)$ is even, so $\mathbf{HW}(\mathbf{v}^*) = i + 1$
  - Therefore, $\forall \mathbf{v}^*$ s.t. $\mathrm{HW}(\mathbf{v}^*) = i + 1$, $\mathbf{v}^* \in G_0$

$\square$

Negative Result

Proof.

- **Induction** (even i):
  - By **Hypothesis**, $\forall \mathbf{v} \in \{0,1\}^p$ s.t. $\mathrm{HW}(\mathbf{v}) = i$, $\mathbf{v} \in G_0$
  - By **Privacy**, $\forall j \in [0,p)$, $\mathbf{v}[j] = 0$, $\mathbf{v}^* \in G_0$ s.t. $\mathbf{v}[i] = \mathbf{v}^*[i]$, $i \neq j$
  - No parity constraint in G_1. Instead we prove by contradiction.
    - Let $m = \#\{\mathbf{v}\}$
    - By **Privacy**, $\#\{\mathbf{v}^*\} = m$.
    - Suppose $\forall \mathbf{v}^*, \mathrm{HW}(\mathbf{v}^*) = i$
    - Consider $j^* \in [0,p)$ s.t. $\mathbf{v}[j^*] = 1$
    - By **Hypothesis**, $\exists \tilde{\mathbf{v}} \in G_1$ s.t. $\tilde{\mathbf{v}}[\neq j^*] = \mathbf{v}[\neq j^*] \wedge \tilde{\mathbf{v}}[j^*] = 0$
    - Consider the marginal view $G_0[\text{left} \neq j^*]$ and $G_1[\text{left} \neq j^*]$
    - In G_0, $\#\{\mathbf{v}' \in \{0,1\}^p \mid \mathbf{v}'[\neq j^*] = \mathbf{v}[\neq j^*]\} = m$
    - In G_1, $\#\{\mathbf{v}' \in \{0,1\}^p \mid \mathbf{v}'[\neq j^*] = \mathbf{v}[\neq j^*]\} \geq m+1$
  - Therefore, $\exists \mathbf{v}^* \in G_1$ s.t. $\mathrm{HW}(\mathbf{v}^*) = i+1$

$\square$

Negative Result

Proof.

Note that

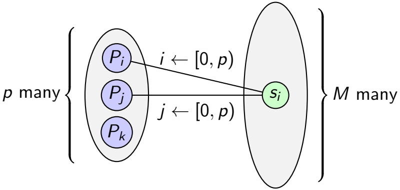
- $\#\{\mathbf{v} \in \{0,1\}^p \mid \mathrm{HW}(\mathbf{v}) \text{ is odd } \} = 2^{p-1}$
- $\#\{\mathbf{v} \in \{0,1\}^p \mid \mathrm{HW}(\mathbf{v}) \text{ is even } \} = 2^{p-1}$

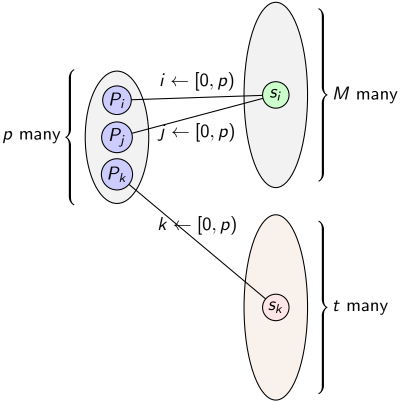
Therefore, the right nodes in G_0 and $G_1 \geq 2^{p-1}$ $\square$

Randomized Graphs

Consider the following design:

- Let $M, t = \mathrm{poly}(p)$ be two parameters





Security of the Randomized Design

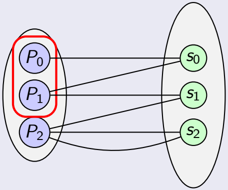
- **Correctness:** Counting duplicate edges, G_0's every right node has degree 2
- **Pseudorandomness:** For $i \in [0, p)$, let $\mathrm{Bad}_i :=$ No red nodes connect to P_i
  - $\Pr[\mathrm{Bad}_i] = \left(\frac{p-1}{p}\right)^t$
  - $\Pr\left[\bigcup_i \mathrm{Bad}_i\right] \leq p \cdot \left(\frac{p-1}{p}\right)^t = p \cdot \left(1 - \frac{1}{p}\right)^{(-p)\cdot(-\frac{t}{p})} = p \cdot O(\exp(-\frac{t}{p})) = O(\exp(-\frac{t}{p}))$

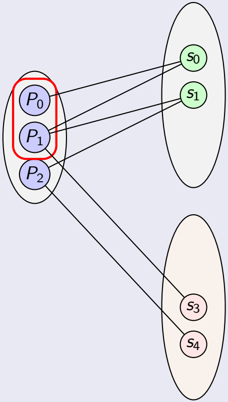
Security of the Randomized Design

- **Privacy:** For any $i \in [0, p)$, consider the subgraph of removing P_i in G_0 and G_1.

Structure of Adversary's View

A series of right nodes, with $\{0, 1, 2\}$ edges (counting duplicates).





- M-sd: $\begin{pmatrix} 2 & 1 & 0 \\ \frac{(p-1)^2}{p^2} & \frac{2(p-1)}{p^2} & \frac{1}{p^2} \end{pmatrix}$
- t-seeds: $\begin{pmatrix} 1 & 0 \\ \frac{p-1}{p} & \frac{1}{p} \end{pmatrix}$

Security of Randomized Design

Adversary's View

View = (#1-edge nodes, #2-edge nodes) = $(\mathcal{S}, \mathcal{D})$

- Let $(\mathcal{S}_0, \mathcal{D}_0)$ be the distribution in G_0, $(\mathcal{S}_1, \mathcal{D}_1)$ be the distribution in G_1
- $\mathsf{SD}((\mathcal{S}_0, \mathcal{D}_0), (\mathcal{S}_1, \mathcal{D}_1)) = \mathbb{E}_{\mathcal{D}}\left[\mathsf{SD}(\mathcal{S}_0, \mathcal{S}_1 \mid \mathcal{D})\right]$

Security of Randomized Design

Since $0 \leq \mathcal{D} \leq M$, consider $d \in [0, M]$:

$\mathcal{S}_0 \mid (\mathcal{D}_0 = d)$

- $\mathcal{S}_0 \mid (\mathcal{D}_0 = d) = I_0 + \ldots + I_{M-d-1}$
- $I_i = \text{Ber}_{\frac{2(p-1)}{2p-1}}$

$\mathcal{S}_1 \mid (\mathcal{D}_1 = d)$

- $\mathcal{S}_1 \mid (\mathcal{D}_1 = d) = I_0 + \ldots + I_{M-d-1} + I'_0 + \ldots + I'_{t-1}$
- $I_i = \text{Ber}_{\frac{2(p-1)}{2p-1}}$
- $I'_i = \text{Ber}_{\frac{p-1}{p}}$

Security of Randomized Design

Sum of Independent Bernoulli's [Rö07]

Let $J_0, \ldots, J_{n-1}$ be independent Bernoulli distributions with parameters $p_0, \ldots, p_{n-1}$. Let $\mu = \sum p_i$, $\sigma^2 = \sum p_i(1-p_i)$. We have

$$\mathrm{SD}(\sum J_i, \mathrm{TP}(\mu, \sigma^2)) \leq \frac{\sqrt{\sum p_i^3(1-p_i)} + 2}{\sigma^2}$$

Corollary of [Rö07]

Conditioned on $\mathcal{D} = d$:

- $\mathrm{SD}(\mathcal{S}_0, \mathrm{TP}(\mu_0, \sigma_0^2)) \leq \frac{\frac{2(p-1)}{2p-1} \cdot \sigma_0 + 2}{\sigma_0^2} = O(\sqrt{\frac{p}{M-d}})$
- $\mathrm{SD}(\mathcal{S}_1, \mathrm{TP}(\mu_1, \sigma_1^2)) \leq \frac{\sqrt{(M-d) \cdot \frac{(2(p-1))^2}{(2p-1)^2} + t \cdot \frac{(p-1)^3}{p^4}} + 2}{\sigma_1^2} = O(\sqrt{\frac{p}{M-d}})$

Security of Randomized Design

Distance of Translated Possion [BLU06]

$$\mathsf{SD}(\mathsf{TP}(\mu_0, \sigma_0^2), \mathsf{TP}(\mu_1, \sigma_1^2)) \le \frac{|\mu_0 - \mu_1|}{\sigma_0} + \frac{\left|\sigma_0^2 - \sigma_1^2\right| + 1}{\sigma_0^2}$$

Corollary of [BLU06]

Conditioned on $\mathcal{D} = d$:

$$\begin{aligned}
\mathsf{SD}(\mathcal{S}_0, \mathcal{S}_1) &\le \begin{array}{c} \mathsf{SD}(\mathcal{S}_0, \mathsf{TP}(\mu_0, \sigma_0^2)) \\ +\mathsf{SD}(\mathsf{TP}(\mu_0, \sigma_0^2), \mathsf{TP}(\mu_1, \sigma_1^2)) \\ +\mathsf{SD}(\mathcal{S}_1, \mathsf{TP}(\mu_1, \sigma_1^2)) \end{array} \\
&\le O\left(\sqrt{\frac{p}{M-d}}\right) + \frac{|\mu_0 - \mu_1|}{\sigma_0} + \frac{\left|\sigma_0^2 - \sigma_1^2\right| + 1}{\sigma_0^2} \\
&= O\left(t \cdot \sqrt{\frac{p}{M-d}}\right)
\end{aligned}$$

Security of Randomized Design

Finally, apply tail bound on $\mathcal{D}$:

Chernoff

- Since $\mathcal{D} = I_0^* + \ldots + I_{M-1}^*$, $I_i^* = \mathrm{Ber}_{\frac{(p-1)^2}{p^2}}$
- Apply Chernoff bound

$$\begin{aligned}
&\Pr\left[\mathcal{D} \geq \left(1 + \frac{1}{p-1}\right) \cdot \left(M \cdot \frac{(p-1)^2}{p^2}\right)\right] \\
&\leq \exp\left(-\frac{\left(\frac{1}{p-1}\right)^2 \cdot \left(M \cdot \frac{(p-1)^2}{p^2}\right)}{2 + \frac{1}{p-1}}\right) \\
&= \exp\left(-\frac{M}{2p^2 + \frac{p^2}{p-1}}\right)
\end{aligned}$$

Security of Randomized Design

Putting everything together.

Privacy

$$
\begin{aligned}
\mathsf{SD}((\mathcal{S}_0, \mathcal{D}_0), (\mathcal{S}_1, \mathcal{D}_1)) &= \mathbb{E}_{\mathcal{D}}\left[\mathsf{SD}(\mathcal{S}_0, \mathcal{S}_1)\right] \\
&= \sum_d \Pr[\mathcal{D} = d] \cdot \mathsf{SD}(\mathcal{S}_0, \mathcal{S}_1 \mid \mathcal{D} = d) \\
&\leq \Pr[\mathcal{D} \geq M \cdot \frac{p-1}{p}] + \mathsf{SD}(\mathcal{S}_0, \mathcal{S}_1 \mid \mathcal{D} = M \cdot \frac{p-1}{p}) \\
&\leq \exp\left(-\frac{M}{2p^2 + \frac{p^2}{p-1}}\right) + O\left(t \cdot \sqrt{\frac{p}{M - M \cdot \frac{p-1}{p}}}\right) \\
&\leq O\left(\frac{tp}{\sqrt{M}}\right)
\end{aligned}
$$

Privacy Amplification

Privacy Bound

- The above scheme only achieves inverse polynomial privacy $\left(O\left(\frac{tp}{\sqrt{M}}\right), M, t = \mathrm{poly}(p, \lambda)\right)$
- We need negligible privacy error
- Apply the technique in [BGIK22] using Locally Decodable Codes to boost privacy.

Locally Decodable Codes

Consider alphabet $\mathbb{Z}_p$ and parameter $q, \sigma \in \mathbb{N}$, a $[L, N]$-code is q-query locally decodable if

- Deterministic Encoding: $C : \mathbb{Z}_p^N \to \mathbb{Z}_p^L$
- Probabilistic Decoding: $d : [N] \to [L]^q$
- Correctness: $\forall \mathbf{z} \in \mathbb{Z}_p^N, \alpha \in [N]$, $\sum_{\ell=0}^{q-1} (C(\mathbf{z}))_{d(\alpha)_\ell} = z_\alpha$

Privacy Amplification

Reed-Muller code (w-variable, r-degree multivariate polynomials) is a LDC.

Lemma ([BIPW17])

Let $\sigma, w, r, N \in \mathbb{N}^+$ s.t. $N \leq \binom{r+w}{w}$ and p be a prime. RM code is a LDC and

- $q = O(\sigma^2 r)$, $L = O(p^{w+1} r^{w+1} \sigma^{w+1})$
- *For every $\alpha \in [N]$, $d(\alpha) \in [L]^q$ is σ-wise independent*

Privacy Amplification

- Basic idea: consider evaluating DPF on point $x \in [N]$
- Let $(\Delta_0, ..., \Delta_{q-1}) \leftarrow d(\alpha)$

$$\begin{aligned} f_{\alpha,\beta}(x) &= \langle \mathbf{e}_x, \mathsf{TT}(f_{\alpha,\beta}) \rangle \\ &= \beta \cdot (\mathbf{e}_x)_\alpha \\ &= \beta \cdot \sum_{\ell=0}^{q-1} C(\mathbf{e}_x)_{\Delta_\ell} \\ &= \sum_{\ell=0}^{q-1} \langle C(\mathbf{e}_x), \mathsf{TT}(f_{\Delta_\ell,\beta}) \rangle \end{aligned}$$

Intuition

- Simultaneously breaking $> \sigma$ DPF keys is hard
- $\leq \sigma$ DPF keys follows the same distribution

Privacy Amplification

Lemma ([BGIK22])

Let $\widetilde{DPF}$ be a DPF scheme with $^1/_q$-privacy, then using RM code with previous parameters, we get a DPF scheme such that

- *has $O\left(2^{-\Omega(\sigma)} + negl(\lambda)\right)$-privacy*
- *has $q \times \widetilde{DPF}$ cost*

Theorem ([GWW25])

Assuming OWF, for any $\epsilon \in (0, 1)$, there is a DPF scheme with $negl(\lambda)$-privacy and $O(p^3 \cdot N^{1/2+\epsilon})$ key size.

Privacy Amplification

Formally arguing privacy amplification requires some interesting techniques.

Lemma (Leaky secret [BGIK22])

Let $\rho_1 : [L] \to \{0,1\}^*$ *be a randomized function such that*

$$\forall \alpha, \alpha' \in [L], Adv(\rho_1(\alpha), \rho_1(\alpha')) \leq \delta$$

Then there exists a randomized mapping $\tau_\delta : [L] \to [L] \cup \{\perp\}$ *and* $\rho_2 : [L] \cup \{\perp\} \to \{0,1\}^*$ *such that*

$$\forall \alpha \in [L], Adv(\rho_1(\alpha), \rho_2(\tau_\delta(\alpha))) = negl$$

and

$$\forall \alpha \in [L], \Pr[\tau_\delta(\alpha) = \alpha] \leq \delta, \quad \Pr[\tau_\delta(\alpha) = \perp] = 1 - \Pr[\tau_\delta(\alpha) = \alpha]$$

Privacy Amplification

Leaky secret lemma says that we can change $\rho_1(\alpha)$ to $\rho_2(\tau_\delta(\alpha))$, and $\tau_\delta(\alpha)$ is likely to be $\perp$.

Lemma (Hardcore [MT10])

Let $F_1, F_2 : \mathcal{R} \to \{0,1\}^*$, $\epsilon, \delta \in (0,1)$. *If for all dist. of size* T *we have*

$$r \leftarrow \mathcal{R}, Adv(F_1(r), F_2(r)) \leq \delta$$

then there exists a set $\mathcal{Q} \subseteq \mathcal{R}$ *s.t.* $|\mathcal{Q}| \geq (1-\delta)|\mathcal{R}|$ *such that*

$$r' \leftarrow \mathcal{Q}, Adv(F_1(r'), F_2(r')) \leq \epsilon$$

for all dist. of size $T' = \frac{T\epsilon^2}{256\log(|\mathcal{R}|)+1}$

Proof of Leaky Secret Lemma

- Let $\mathcal{R}$ be the set of random tape for ρ_1.
- By the **hardcore lemma**, there exists $\mathcal{Q} \subseteq \mathcal{R}$ s.t. $\forall \epsilon \in (0,1)$,

$$\forall \alpha, \alpha' \in [L], r' \leftarrow \mathcal{Q}, Adv(\rho_1(\alpha, r'), \rho_1(\alpha', r')) \leq \epsilon$$

- Now define

$$\rho_2(\alpha) = \begin{cases} \rho_1(\alpha) & \alpha \neq \perp \\ \rho_1(0) & \alpha = \perp \end{cases} \quad \tau_\delta(\alpha; r) = \begin{cases} \perp & r \in \mathcal{Q} \\ \alpha & r \notin \mathcal{Q} \end{cases}$$

- $\forall \alpha \in [L]$, $Adv(\rho_1(\alpha; r), \rho_2(\tau_\delta(\alpha; r); r))$

$$\begin{aligned} &\leq \Pr[r \in \mathcal{Q}] \cdot (Adv \mid r \in \mathcal{Q}) + \Pr[r \notin \mathcal{Q}] \cdot (Adv \mid r \notin \mathcal{Q}) \\ &\leq \Pr[r \in \mathcal{Q}] \cdot \epsilon + \Pr[r \notin \mathcal{Q}] \cdot 0 \leq \epsilon \end{aligned}$$

Proof of Privacy Amplification

- Let $\alpha, \alpha' \in [N]$ and $(r_0, ..., r_{q-1}) \leftarrow d(\alpha)$, $(r'_0, ..., r'_{q-1}) \leftarrow d(\alpha')$, ρ_1 be the inv-poly-private KeyGen
- We want to argue that

$$Adv\left(\left(\rho_1(r_0), ..., \rho_1(r_{q-1})\right), \left(\rho_1(r'_0), ..., \rho_1(r'_{q-1})\right)\right) = negl \quad (1)$$

- By **leaky secret lemma**, $Adv \leq negl + Adv\left(\left(\rho_2(\tau(r_0)), ..., \rho_2(\tau(r_{q-1}))\right), \left(\rho_2(\tau(r'_0)), ..., \rho_2(\tau(r'_{q-1}))\right)\right)$
- Since $\delta = 1/q$, let X denote the number of $\perp$ in $\{\tau(r_0), ..., \tau(r_{q-1})\}$, by **Chernoff bound**, we have $\Pr[X > \sigma] = O\left(2^{-\sigma}\right)$

$$\begin{aligned} Adv &= \Pr[X > \sigma] \cdot (Adv \mid X > \sigma) + \Pr[X \leq \sigma] \cdot (Adv \mid X \leq \sigma) \\ &\leq \Pr[X > \sigma] \cdot 1 + \Pr[X \leq \sigma] \cdot 0 \\ &\leq O\left(2^{-\sigma}\right) \end{aligned}$$

Instantiating Privacy Amplification

- We need to ensure that $L = O(N^2)$
- For sufficiently small $\delta \in (0,1)$, we can set

$$\sigma = \log(\lambda)^2, \quad w = \frac{\delta \cdot \log(N)}{\log\log(N)}, \quad r = (\log(N))^{1+1/\delta}$$

- We can verify that

$$\binom{w+r}{r} \geq \frac{w^r}{w!} \geq N$$

$$L = q^{w+1} = O(p^{w+1} r^{w+1} \sigma^{w+1}) = O(N^{1+2\epsilon})$$

- So by setting $M = O(t^2 p^2)$, we get p-party DPF with key size $O(p^3 \cdot N^{1/2+\epsilon})$ and privacy $negl(\lambda)$

References I

Elette Boyle, Niv Gilboa, and Yuval Ishai.
Function secret sharing.
In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 337–367. Springer, Berlin, Heidelberg, April 2015.

Elette Boyle, Niv Gilboa, Yuval Ishai, and Victor I. Kolobov.
Programmable distributed point functions.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part IV*, volume 13510 of *LNCS*, pages 121–151. Springer, Cham, August 2022.

Elette Boyle, Yuval Ishai, Rafael Pass, and Mary Wootters.
Can we access a database both locally and privately?
In Yael Kalai and Leonid Reyzin, editors, *TCC 2017, Part II*, volume 10678 of *LNCS*, pages 662–693. Springer, Cham, November 2017.

References II

Andrew D. Barbour, Torgny Lindvall, and Göteborgs Universitet.
Translated poisson approximation for markov chains.
Journal of Theoretical Probability, 19:609–630, 2006.

Aarushi Goel, Mingyuan Wang, and Zhiheng Wang.
Multiparty distributed point functions.
Cryptology ePrint Archive, 2025.

Ueli M. Maurer and Stefano Tessaro.
A hardcore lemma for computational indistinguishability: Security amplification for arbitrarily weak PRGs with optimal stretch.
In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 237–254. Springer, Berlin, Heidelberg, February 2010.

Adrian Röllin.
Translated poisson approximation using exchangeable pair couplings.
The Annals of Applied Probability, 17(5–6), October 2007.