



BETTER.

SESSION ID: CRYP-T07

Large Universe Subset Predicate Encryption Based on Static Assumption (without Random Oracle)

Sanjit Chatterjee

Associate Professor,
Indian Institute of Science, Bangalore,
India

Sayantan Mukherjee

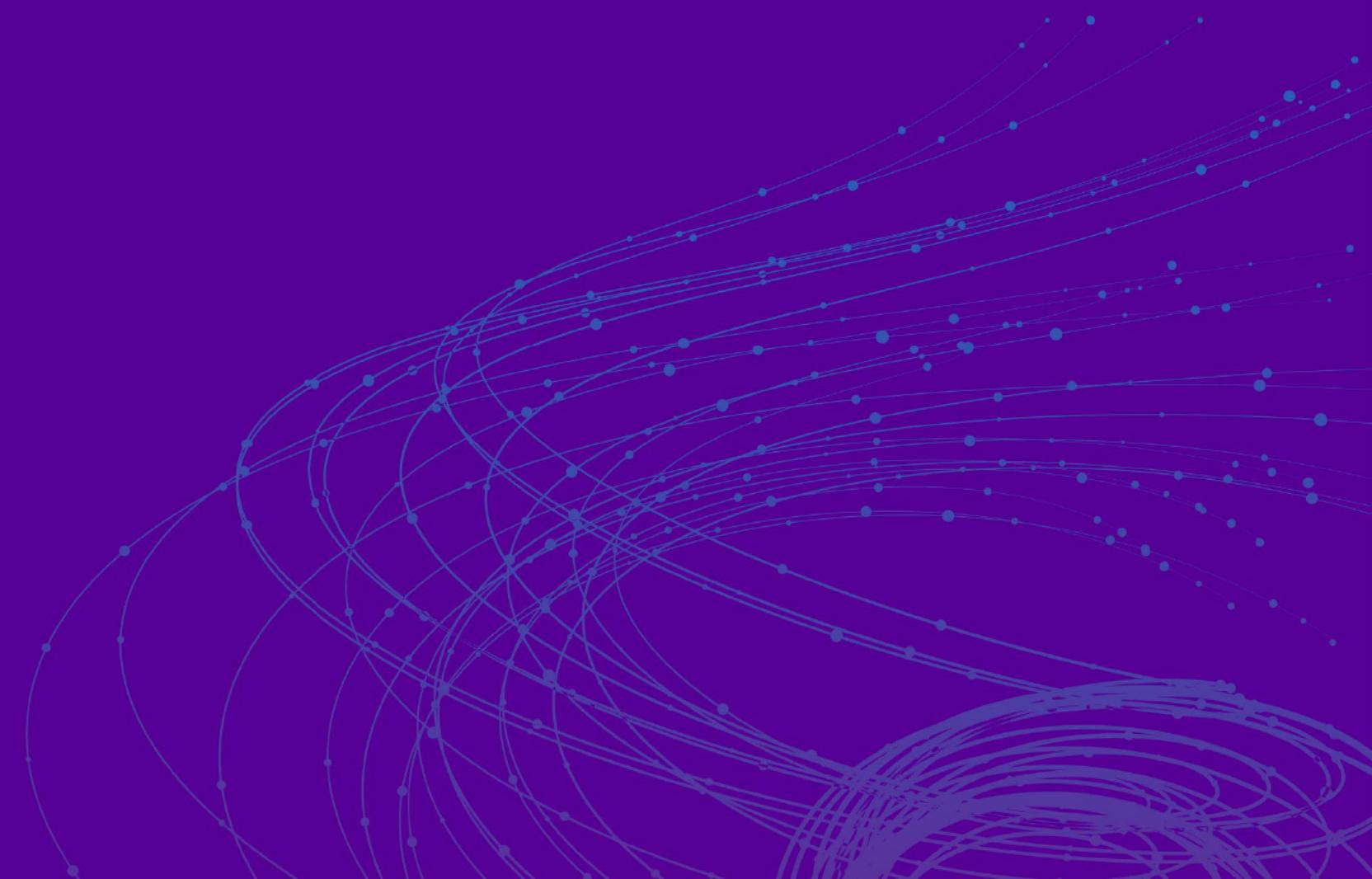
PhD Student,
Indian Institute of Science, Bangalore,
India

Agenda

- Background
- Our constructions
- Applications
- Conclusion



Background



Predicate Encryption

$R : X \times Y \rightarrow \{0, 1\}$ s.t. $R(x, y) = 1$ if $x \in X$ and $y \in Y$ satisfy R .

- $\text{Setup}(1^\lambda)$ outputs mpk, msk
- $\text{KeyGen}(\text{msk}, x)$ outputs secret key SK_x
- $\text{Encrypt}(\text{mpk}, y)$ outputs encapsulation key \mathcal{K} and ciphertext CT_y
- $\text{Decrypt}((\text{SK}_x, x), (\text{CT}_y, y))$ outputs \mathcal{K} if $R(x, y) = 1$

Procedure Initialize(1^λ)

$(\text{mpk}, \text{msk}) \leftarrow \text{Setup}(1^\lambda)$

Return mpk

Procedure KeyExtract(msk, x)

$Q \leftarrow Q \cup \{x\}$

Return $\text{SK}_x \leftarrow \text{KeyGen}(\text{msk}, x)$

Procedure Challenge(mpk, y)

$(\mathcal{K}, \text{CT}_y) \leftarrow \text{Encrypt}(\text{mpk}, y)$

Choose $\mathcal{K} \leftarrow \mathcal{K}$

Return $(\mathcal{K}, \text{CT}_y)$

Procedure Finalize(b)

Return $\left\{ R(x, y) \stackrel{?}{=} 0 \right\}_{x \in Q} \wedge b$



Predicate Functions

- Equality Predicate (IBE): If $x = y$, then $R(x,y)=1$
- Membership Predicate (BE): If $x \in y$, then $R(x,y)=1$
- Zero Inner-Product (IPE): If $\langle x, y \rangle = 0$, then $R(x,y)=1$
- ...

Predicate Functions

- Equality Predicate (IBE): If $x = y$, then $R(x,y)=1$
- Membership Predicate (BE): If $x \in y$, then $R(x,y)=1$
- Zero Inner-Product (IPE): If $\langle x, y \rangle = 0$, then $R(x,y)=1$
- ...
- Subset Predicate (SPE): if $x \subseteq y$, then $R(x,y)=1$



Subset Predicate Encryption

Subset Predicate $R(\Omega, \Theta) = 1$ if $\Omega, \Theta \in U$ and $\Omega \subseteq \Theta$.

- $\text{Setup}(1^\lambda)$ outputs mpk, msk
- $\text{KeyGen}(\text{msk}, \Omega)$ outputs secret key SK_Ω
- $\text{Encrypt}(\text{mpk}, \Theta)$ outputs encapsulation key κ and ciphertext CT_Θ
- $\text{Decrypt}((\text{SK}_x, x), (\text{Ct}_y, y))$ outputs κ if $R(x, y) = 1$

Subset Predicate Encryption

- Subset Predicate \equiv multiple Membership Predicate
 - $\Omega \subseteq \Theta \Leftrightarrow$ for any $i \in \Omega$, check if $i \in \Theta$
 - Katz. et al [KMM17]:
 - Trivial lifting of membership predicate is insecure
 - SPE must have “un-downgradable” SK
- Katz et al. presented two constructions
 - small universe constructions
 - $O(n)$ CT and $O(1)$ SK
 - selective secure



Our Constructions

Two standard model large-universe constructions



SPE-I

O(1) secret key, O(1) ciphertext, selective*security

SPE-I Intuition

- Set $S \equiv$ Characteristic polynomial $P_S(z) = \prod_{i \in S} (z + i)$
- Set $\Omega \subseteq$ Set $\Theta \Leftrightarrow P_\Omega(z)$ divides $P_\Theta(z)$
- If $\Theta = \Omega \cup \Phi$ then $P_\Theta(z) = P_\Omega(z) \cdot P_\Phi(z) \Leftrightarrow P_\Phi(z) = P_{\Theta \setminus \Omega}(z)$
- Encodings
 - Ciphertext encodes Θ as $g^{sP_\Theta(\alpha)}$
 - Secret key encodes Ω as $u^{1/P_\Omega(\alpha)}$
 - Requires canceling of $P_\Phi(\alpha)$: mpk keeps various powers of α
 - The constant i.e. $P_\Phi(0)$ gives out $e(g, u)^s \equiv \mathcal{K}$



SPE-I Construction

Setup($1^\lambda, m$)

- 1: $(p_1, p_2, p_3, G, G_T, e) \leftarrow \mathcal{G}_{\text{sbg}}(1^\lambda, 3)$
- 2: $|G| = |G_T| = N = p_1 p_2 p_3$
- 3: Let G_i subgroup of G of order p_i
- 4: $g_1, u \leftarrow G_1, g_3, R_{3,1}, \dots, R_{3,m} \leftarrow G_3$
- 5: $\alpha, \beta \leftarrow N, H$
- 6: $\text{msk} = (\alpha, \beta, u, g_3)$
- 7: $\text{mpk} = (g_1, g_1^\beta, (G_i = g_1^{\alpha^i})_{i \in [m]}, (U_i = u^{\alpha^i} \cdot R_{3,i})_{i \in [m]}, e(g_1, u)^\beta, H)$

KeyGen(msk, Ω)

- 1: $X_3 \leftarrow G_3$
- 2: $P_\Omega(z) = \prod_{x \in \Omega} (z + x)$
- 3: $\text{SK}_\Omega = u^{\frac{\beta}{P_\Omega(\alpha)}} \cdot X_3$

Encrypt(mpk, Θ)

- 1: $s \leftarrow \mathbb{Z}_N$
- 2: $P_\Theta(z) = \prod_{y \in \Theta} (z + y) = \sum_{i \in [0, l]} c_i z^i$
- 3: $\mathfrak{K} = H(e(g_1, u)^{s\beta}), C_0 = g_1^{s\beta}$
 $C_1 = g_1^{\textcolor{blue}{sP_\Theta(\alpha)}} = \left(g_1^{c_0} \prod_{i \in [l]} G_i^{c_i} \right)^s$
- 4: $\text{CT}_\Theta = (C_0, C_1)$

Decrypt((SK_Ω, Ω), (CT_Θ, Θ))

- 1: Here $\Omega \subseteq \Theta$, Let $t = |\Theta \setminus \Omega|$
- 2: $P_{\Theta \setminus \Omega}(\alpha) = \prod_{z \in \Theta \setminus \Omega} (\alpha + z) = \sum_{i \in [0, t]} a_i \alpha^i$
- 3: $A = e(C_0, \prod_{i \in [t]} U_i^{a_i})$
 $= e(g_1^{s\beta}, u^{P_{\Theta \setminus \Omega}(\alpha) - a_0} \cdot R_3)$
- 4: $B = e(C_1, \text{SK}_\Omega) = e(g_1^{sP_\Theta(\alpha)}, u^{\frac{\beta}{P_\Omega(\alpha)}})$
- 5: Output $\mathfrak{K} = H((B/A)^{1/a_0})$



SPE-I Correctness

$$B = e(C_1, SK_{\Omega}) = e(g_1^{sP_{\Theta}(\alpha)}, u^{\frac{\beta}{P_{\Omega}(\alpha)}} \cdot X_3) = e(g_1, u)^{s\beta P_{\Theta \setminus \Omega}(\alpha)}$$

$$A = e(C_0, \prod_{i \in [t]} U_i^{a_i}) = e(g_1^{s\beta}, u^{P_{\Theta \setminus \Omega}(\alpha) - a_0}) = e(g_1, u)^{s\beta(P_{\Theta \setminus \Omega}(\alpha) - a_0)}$$

$$\begin{aligned} \text{Then, } H((B/A)^{1/a_0}) &= H(e(g_1, u)^{s\beta a_0 \cdot a_0^{-1}}) \\ &= H(e(g_1, u)^{s\beta}) \\ &= \mathfrak{K} \end{aligned}$$

Security Proof

- Deja-Q framework under Sub-Group Decision Problem
- Selective security
 - Let $\Omega = \{x_1, x_2, x_3\}$
 - Key queries are made on sets $\Omega_1 = \{x_1, x_2\}$, $\Omega_2 = \{x_2, x_3\}$ and $\Omega_3 = \{x_1, x_3\}$
 - Given $\text{SK}_{\Omega_1}, \text{SK}_{\Omega_2}$ and SK_{Ω_3} ,
$$\left(\frac{\text{SK}_{\Omega_1}}{\text{SK}_{\Omega_2}}\right)^{(x_3-x_1)^{-1}} = \left(\frac{\text{SK}_{\Omega_1}}{\text{SK}_{\Omega_3}}\right)^{(x_3-x_2)^{-1}} = u^{\frac{1}{(\alpha+x_1)(\alpha+x_2)(\alpha+x_3)}} = \text{SK}_{\Omega}$$
- **Problem:** Semi-functional key components might become dependent
- **Restriction:** Key queries must be on cover-free sets $\Omega_i \setminus (\bigcup_{j \in [1, i-1]} \Omega_j) \neq \emptyset$



SPE-II

$O(1)$ secret key, $O(n)$ ciphertext, adaptive security

SPE-II Intuition

| | small universe | large universe |
|---|---------------------------|--|
| identity z | h_z | $\sum_{j \in m} w_j z^j$ |
| Encoding of set Ω (constant size) | $\sum_{z \in \Omega} h_z$ | $\sum_{z \in \Omega} \sum_{j \in m} w_j z^j$ |
| Encoding of set Θ | $\{h_z\}_{z \in \Theta}$ | $\left\{ \sum_{j \in m} w_j z^j \right\}_{z \in \Theta}$ |



SPE-II Construction

Setup($1^\lambda, m$)

- 1: $(p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}_{\text{abg}}(1^\lambda)$
- 2: $(g_1, g_2) \leftarrow G_1 \times G_2, g_T \leftarrow G_T$
- 3: $\alpha_1, \alpha_2, c, d, (u_i, v_i)_{i \in [m]} \leftarrow \mathbb{Z}_p$
- 4: $b \leftarrow \mathbb{Z}_p^\times, g_T^\alpha = e(g_1, g_2)^{(\alpha_1 + b\alpha_2)}$
- 5: $(g_1^{w_i} = g_1^{u_i + bv_i})_{i \in [m]}, g_1^w = g_1^{c+bd}$
- 6: $\text{msk} = (g_2, g_2^c, \alpha_1, \alpha_2, d, (u_i, v_i)_{i \in [m]})$
- 7: $\text{mpk} = (g_1, g_1^b, (g_1^{w_i})_{i \in [m]}, g_1^w, g_T^\alpha)$

Encrypt(mpk, Θ)

- 1: $s, (t_i)_{i \in [m]} \leftarrow \mathbb{Z}_p$
- 2: $\mathfrak{K} = e(g_1, g_2)^{\alpha s}, C_0 = g_1^s, C_1 = g_1^{bs}$
 $C_{2,y} = g_1^{s \left(\sum_{j \in [m]} w_j y^j + wt_i \right)}$
- 3: $\text{CT}_\Theta = (C_0, C_1, (C_{2,y}, t_y)_{y \in \Theta})$

KeyGen(msk, Ω)

- 1: $r \leftarrow \mathbb{Z}_p$
- 2: $K_1 = g_2^r, K_2 = g_2^{cr}, K_4 = g_2^{dr}$
 $K_3 = g_2^{\alpha_1+r \sum_{x \in \Omega} \sum_{j \in [m]} u_j x^j}$
 $K_5 = g_2^{\alpha_2+r \sum_{x \in \Omega} \sum_{j \in [m]} v_j x^j}$
- 3: $\text{SK}_\Omega = (K_1, K_2, K_3, K_4, K_5)$

Decrypt($(\text{SK}_\Omega, \Omega), (\text{CT}_\Theta, \Theta)$)

- 1: $A = e \left(\prod_{y_i \in \Omega} C_{2,i}, K_1 \right)$
- 2: $B = e \left(C_0, K_3 \prod_{y_i \in \Omega} K_2^{t_i} \right) e \left(C_1, K_5 \prod_{y_i \in \Omega} K_4^{t_i} \right)$
- 3: Output $\mathfrak{K} = B/A$



SPE-II Correctness

$$B = e \left(C_0, K_3 \prod_{y_i \in \Omega} K_2^{t_i} \right) e \left(C_1, K_5 \prod_{y_i \in \Omega} K_4^{t_i} \right),$$

$$= e \left(C_0, g_2^{\sum_{y_i \in \Omega} ((u_0 + bv_0) + (u_1 + bv_1)y_i + \dots + (u_m + bv_m)y_i^m)} \cdot \prod_{y_i \in \Omega} g_2^{r(c+bd)t_i} \right)$$

$$= e \left(g_1^s, g_2^{\sum_{y_i \in \Omega} (w_0 + w_1y_i + w_2y_i^2 + \dots + w_my_i^m + wt_i)} \right)$$

$$A = e \left(\prod_{y_i \in \Omega} C_{2,i}, K_1 \right)$$

$$= e \left(g_1^{\sum_{y_i \in \Omega} (w_0 + w_1y_i + w_2y_i^2 + \dots + w_my_i^m + wt_i)}, g_2^r \right)$$

Then $B/A = e(g_1^s, g_2^\alpha) = \kappa$.



SPE-II Security

$$\Omega \rightarrow \sum_{z \in \Omega} \sum_{j \in [m]} u_j z^j$$

and

$$\Theta^* \rightarrow \left\{ \sum_{j \in [m]} u_j z^j \right\}_{z \in \Theta^*}$$

Security ($\Omega \not\subseteq \Theta^*$): Note that $\exists x \in \Omega \setminus \Theta^*$.

- $\sum_{z \in \Omega} \sum_{j \in [m]} u_j z^j = \sum_{z \in \Omega \setminus \{x\}} \sum_{j \in [m]} u_j z^j + \sum_{j \in [m]} u_j x^j.$

- Argument for independence.

- $x \notin \Theta^*$ $\Rightarrow \sum_{j \in [m]} u_j x^j \perp \left\{ \sum_{j \in [m]} u_j z^j \right\}_{z \in \Theta^*}$.

- $x \notin \Omega \setminus \{x\}$ $\Rightarrow \sum_{j \in [m]} u_j x^j \perp \sum_{z \in \Omega \setminus \{x\}} \sum_{j \in [m]} u_j z^j.$

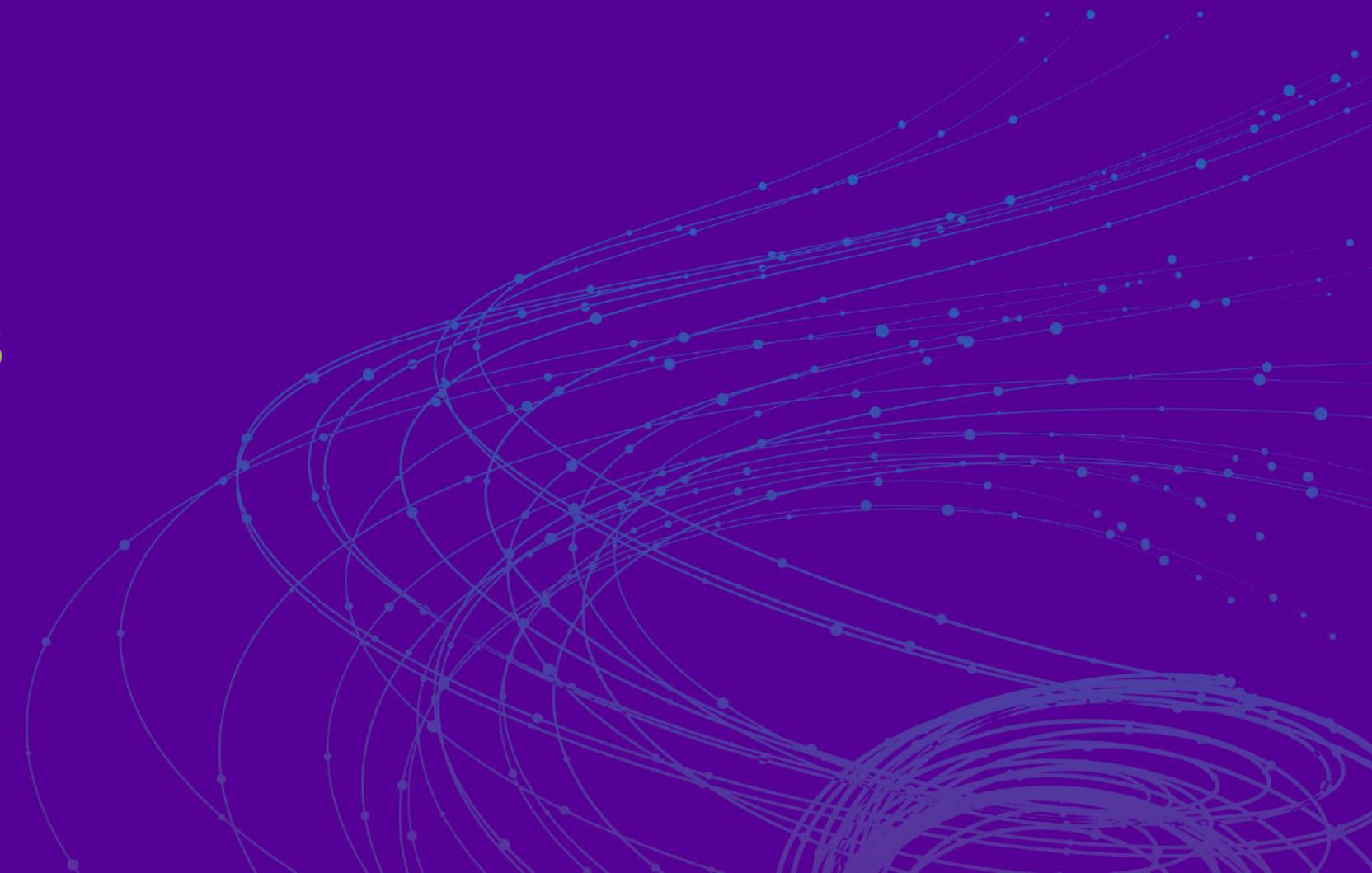
- $\sum_{j \in [m]} u_j x^j$ supplies entropy.



RSA® Conference 2019

Applications

WIBE, CP-DNF



WIBE

- SPE to WIBE (* in data-index):

$$- S_{id}[2i, 2i+1] = \begin{cases} 10 & \text{if } id[i] = 1 \\ 01 & \text{if } id[i] = 0 \\ 11 & \text{if } id[i] = * \end{cases}$$

- Example: (1010 satisfies $1 * * 0$) $\equiv S_{1010} \subseteq S_{1***0}$.
 $S_{1***0} = 10111101 = \{1, 3, 4, 5, 6, 8\}$
 $S_{1010} = 10011001 = \{1, 4, 5, 8\}$

| WIBE Schemes | mpk | SK | CT | pairing | Security | Assumption |
|-----------------------------------|----------------------|-----------------------|------------------------------|-----------|-----------|------------|
| BBG-WIBE [ACD ⁺ 06] | $(n + 4)G$ | $(n + 2)G$ | $(n + 2)G$ | 2 | adaptive | n -BDHI |
| Wa-WIBE [ACD ⁺ 06] | $((\ell + 1)n + 3)G$ | $(n + 1)G$ | $((\ell + 1)n + 2)G$ | $(n + 1)$ | adaptive | DBDH |
| SPE-1 [KMMS17] | $(2n + 2)G_1$ | $1G_2 + \mathbb{Z}_p$ | $(2n + 1)G_1$ | 1 | selective | q -BDHI |
| SPE-2 [KMMS17] | $(2n + 1)G_1 + 2G_2$ | $1G_1 + 1G_2$ | $2nG_1 + 1G_2$ | 2 | selective | DBDH |
| SPE-II based | $(2n + 6)G_1$ | $5G_2$ | $(n + 2)G_1 + n\mathbb{Z}_p$ | 3 | adaptive | SXDH |

CP-DNF

- SPE to CP-DNF:

- Data-index is a DNF formula $C_1 \vee C_2 \vee \dots \vee C_t$ where $C_j \subseteq \mathcal{U}$.
- Key-index is attribute set $A \subseteq \mathcal{U}$.
- Satisfies if $\exists j \in [t]$ such that $C_j \subseteq A \iff \mathcal{U} \setminus A \subseteq \mathcal{U} \setminus C_j$.
- For $id \in \{C_1, C_2, \dots, C_t, A\}$, $S_{id}[i] = \begin{cases} 0 & \text{if } i \in id \\ 1 & \text{if } i \notin id \end{cases}$

| DNF Schemes | $ \text{mpk} $ | $ \text{SK} $ | $ \text{CT} $ | pairing | Security | Assumption |
|-------------------|-------------------|----------------------|------------------------------------|---------|-----------|------------|
| SPE-1 [KMMS17] | $(n+2)G_1$ | $G_2 + \mathbb{Z}_p$ | $\gamma((n+1)G_1)$ | 1 | selective | q -BDHI |
| SPE-2 [KMMS17] | $(n+1)G_1 + 2G_2$ | $G_1 + G_2$ | $\gamma(2nG_1 + G_2)$ | 2 | selective | DBDH |
| SPE-II based | $(n+3)G_1$ | $5G_2$ | $\gamma((n+2)G_1 + n\mathbb{Z}_p)$ | 3 | adaptive | SXDH |



Conclusion

- First large-universe SPE with $O(1)$ CT and $O(1)$ SK
 - Selective* secure
- First large-universe adaptive secure SPE
 - $O(n)$ CT and $O(1)$ SK
- Future works
 - Selective secure SPE-I
 - SPE-II with smaller ciphertext size



RSA® Conference 2019

Thank you

ePrint: ia.cr/2018/1190

Questions?