RSAConference2019
San Francisco | March 4–8 | Moscone Center

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

RSA Conference 2019

Background

Predicate Encryption

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

- Setup: Outputs mpk, msk
- KeyGen: Gets x and outputs secret key SK_x
- Encrypt: Gets y and outputs encapsulation key $\mathfrak{K}$ and ciphertext CT_y
- Decrypt((SK_x, x), (Ct_y, y)): Outputs $\mathfrak{K}$ if $R(x,y)=1$

<u>Procedure $\mathsf{Initialize}(1^\lambda)$</u>

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

<u>Procedure $\mathsf{KeyExtract}(\mathsf{msk}, \mathsf{x})$</u>

$Q \leftarrow Q \cup \{\mathsf{x}\}$
Return $\mathsf{SK_x} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathsf{x})$

<u>Procedure $\mathsf{Challenge}(\mathsf{mpk}, \mathsf{y})$</u>

$(\mathfrak{K}, \mathsf{CT_y}) \leftarrow \mathsf{Encrypt}(\mathsf{mpk}, \mathsf{y})$
$\boxed{\text{Choose } \mathfrak{K} \hookleftarrow \mathcal{K}}$
Return $(\mathfrak{K}, \mathsf{CT_y})$

<u>Procedure $\mathsf{Finalize}(\mathfrak{b})$</u>

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

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 ϵ y, then R(x,y)=1
- Zero Inner-Product (IPE): If <x,y> = 0, then R(x,y)=1
- ...
- Subset Predicate (SPE): if $x \subseteq y$, then R(x,y)=1

Subset Predicate Encryption

- Subset Predicate $\equiv$ multiple Membership Predicate
  - $\Omega \subseteq \Theta \Leftrightarrow$ for any $i \in \Omega$, $i \in \Theta$
  - Trivial implementation is insecure [KMM17]
- 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

RSAConference2019

SPE_1

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 Θ $\Leftrightarrow$ $P_\Omega(z)$ 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 $P_\Phi(\alpha)$ encoded in mpk
  - The constant i.e. $P_\Phi(0)$ gives out $e(g,u)^s$

SPE-I Construction

Setup$(1^\lambda, m)$

1: $(p_1, p_2, p_3, \mathsf{G}, \mathsf{G_T}, e) \leftarrow \mathcal{G}_{\text{sbg}}(1^\lambda, 3)$
2: $|\mathsf{G}| = |\mathsf{G_T}| = N = p_1 p_2 p_3$
3: Let G_i subgroup of G of order p_i
4: $g_1, u \hookleftarrow \mathsf{G}_1,\ g_3, R_{3,1}, \ldots, R_{3,m} \hookleftarrow \mathsf{G}_3$
5: $\alpha, \beta \hookleftarrow N$, H
6: $\mathsf{msk} = (\alpha, \beta, u, g_3)$
7: $\mathsf{mpk} = \left(g_1, g_1^\beta, \left(G_i = g_1^{\alpha^i}\right)_{i\in[m]}, \left(U_i = u^{\alpha^i} \cdot R_{3,i}\right)_{i\in[m]}, e(g_1, u)^\beta, \mathsf{H}\right)$

KeyGen(msk, Ω)

1: $X_3 \hookleftarrow \mathsf{G}_3$
2: $P_\Omega(z) = \prod_{x\in\Omega}(z + x)$
3: $\mathsf{SK}_\Omega = u^{\frac{\beta}{P_\Omega(\alpha)}} \cdot X_3 = u^{\frac{\beta}{\prod_{x\in\Omega}(\alpha+x)}} \cdot X_3$

Encrypt(mpk, Θ)

1: $s \hookleftarrow \mathbb{Z}_N$
2: $P_\Theta(z) = \prod_{y\in\Theta}(z + y) = \sum_{i\in[0,l]} c_i z^i$
3: $\mathfrak{K} = \mathsf{H}(e(g_1, u)^{s\beta}), \mathsf{C}_0 = g_1^{s\beta}$

$\mathsf{C}_1 = g_1^{sP_\Theta(\alpha)} = \left(g_1^{c_0} \prod_{i\in[l]} G_i^{c_i}\right)^s$

4: $\mathsf{CT}_\Theta = (\mathsf{C}_0, \mathsf{C}_1)$

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

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: $A = e(\mathsf{C}_0, \prod_{i\in[t]} U_i^{a_i})$

$= e(g_1^{s\beta}, u^{P_{\Theta\setminus\Omega}(\alpha) - a_0} \cdot R_3)$

4: $B = e(\mathsf{C}_1, \mathsf{SK}_\Omega) = e(g_1^{sP_\Theta(\alpha)}, u^{\frac{\beta}{P_\Omega(\alpha)}})$
5: Output $\mathfrak{K} = \mathsf{H}((B/A)^{1/a_0})$

SPE-I Correctness

$$B = e(\mathsf{C}_1, \mathsf{SK}_\Omega) = e(g_1^{sP_\Theta(\alpha)}, u^{\frac{\beta}{P_\Omega(\alpha)}} \cdot X_3) = e(g_1, u)^{s\beta P_{\Theta\setminus\Omega}(\alpha)}$$

$$A = e(\mathsf{C}_0, \prod_{i\in[t]} U_i^{a_i}) = e(g_1^{s\beta}, u^{P_{\Theta\setminus\Omega}(\alpha)-a_0}) = e(g_1, u)^{s\beta\left(P_{\Theta\setminus\Omega}(\alpha)-a_0\right)}$$

$$\text{Then, } \mathsf{H}((B/A)^{1/a_0}) = \mathsf{H}(e(g_1, u)^{s\beta a_0 \cdot a_0{}^{-1}})$$

$$= \mathsf{H}(e(g_1, u)^{s\beta})$$

$$= \mathfrak{K}$$

Security Proof

- Under Sub-Group Decision Problem
- Deja Q framework
- Selective security
  - 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 SK_{Ω_1}, SK_{Ω_2} and SK_{Ω_3},

$$\left(\frac{\mathsf{SK}_{\Omega_1}}{\mathsf{SK}_{\Omega_2}}\right)^{(x_3-x_1)^{-1}} = \left(\frac{\mathsf{SK}_{\Omega_1}}{\mathsf{SK}_{\Omega_3}}\right)^{(x_3-x_2)^{-1}} = u^{\frac{1}{(\alpha+x_1)(\alpha+x_2)(\alpha+x_3)}} = \mathsf{SK}_{\Omega}$$

    where $\Omega=\{x_1,x_2,x_3\}$
  - Restriction: Key queries needs to be on cover-free sets

RSAConference2019

SPE_2

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

$\underline{\mathsf{Setup}(1^\lambda, m)}$

1: $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \leftarrow \mathcal{G}_{\mathrm{abg}}(1^\lambda)$
2: $(g_1, g_2) \hookleftarrow \mathbb{G}_1 \times \mathbb{G}_2,\ g_T \leftarrow \mathbb{G}_T$
3: $\alpha_1, \alpha_2, c, d, (u_i, v_i)_{i\in[m]} \hookleftarrow \mathbb{Z}_p$
4: $b \hookleftarrow \mathbb{Z}_p^\times,\ g_T^\alpha = e(g_1, g_2)^{(\alpha_1 + b\alpha_2)}$
5: $\left(g_1^{w_i} = g_1^{u_i + bv_i}\right)_{i\in[m]},\ g_1^w = g_1^{c+bd}$
6: $\mathsf{msk} = (g_2, g_2^c, \alpha_1, \alpha_2, d, (u_i, v_i)_{i\in[m]})$
7: $\mathsf{mpk} = \left(g_1, g_1^b, (g_1^{w_i})_{i\in[m]}, g_1^w, g_T^\alpha\right)$

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \Omega)}$

1: $r \hookleftarrow \mathbb{Z}_p$
2: $\mathsf{K}_1 = g_2^r, \mathsf{K}_2 = g_2^{cr}, \mathsf{K}_4 = g_2^{dr}$

$$\mathsf{K}_3 = g_2^{\alpha_1 + r \sum_{x\in\Omega} \sum_{j\in[m]} u_j x^j}$$

$$\mathsf{K}_5 = g_2^{\alpha_2 + r \sum_{x\in\Omega} \sum_{j\in[m]} v_j x^j}$$

3: $\mathsf{SK}_\Omega = (\mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3, \mathsf{K}_4, \mathsf{K}_5)$

$\underline{\mathsf{Encrypt}(\mathsf{mpk}, \Theta)}$

1: $s, (t_i)_{i\in[m]} \hookleftarrow \mathbb{Z}_p$
2: $\mathfrak{K} = e(g_1, g_2)^{\alpha s}, \mathsf{C}_0 = g_1^s, \mathsf{C}_1 = g_1^{bs}$

$$\mathsf{C}_{2,y} = g_1^{s\left(\sum_{j\in[m]} w_j y^j + w t_i\right)}$$

3: $\mathsf{CT}_\Theta = (\mathsf{C}_0, \mathsf{C}_1, (\mathsf{C}_{2,y}, t_y)_{y\in\Theta})$

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

1: $A = e\left(\prod_{y_i\in\Omega} \mathsf{C}_{2,i}, \mathsf{K}_1\right)$
2: $B = e\left(\mathsf{C}_0, \mathsf{K}_3 \prod_{y_i\in\Omega} \mathsf{K}_2^{t_i}\right) e\left(\mathsf{C}_1, \mathsf{K}_5 \prod_{y_i\in\Omega} \mathsf{K}_4^{t_i}\right)$
3: Output $\mathfrak{K} = B/A$

SPE-II Correctness

$$B = e\left(\mathsf{C}_0, \mathsf{K}_3 \prod_{y_i \in \Omega} \mathsf{K}_2^{t_i}\right) e\left(\mathsf{C}_1, \mathsf{K}_5 \prod_{y_i \in \Omega} \mathsf{K}_4^{t_i}\right),$$

$$= e\left(\mathsf{C}_0, g_2^{(\alpha_1 + b\alpha_2) + r \sum_{y_i \in \Omega} ((u_0 + bv_0) + (u_1 + bv_1) y_i + \ldots + (u_m + bv_m) y_i^m)} \cdot \prod_{y_i \in \Omega} g_2^{r(c+bd)t_i}\right)$$

$$= e\left(g_1^s, g_2^{\alpha + r \sum_{y_i \in \Omega} (w_0 + w_1 y_i + w_2 y_i^2 + \ldots + w_m y_i^m + w t_i)}\right)$$

$$A = e\left(\prod_{y_i \in \Omega} \mathsf{C}_{2,i}, \mathsf{K}_1\right)$$

$$= e\left(g_1^{s \sum_{y_i \in \Omega} (w_0 + w_1 y_i + w_2 y_i^2 + \ldots + w_m y_i^m + w t_i)}, g_2^r\right)$$

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

SPE-II Security

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

and

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

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

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	$\lvert mpk \rvert$	$\lvert SK \rvert$	$\lvert CT \rvert$	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_2 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 $C_1 \vee C_2 \vee \cdots C_t$ where $C_j \subseteq \mathcal{U}$.
  - Key-index is attribute set $\mathsf{A} \subseteq \mathcal{U}$.
  - Satisfies if $\exists j \in [t]$ such that $C_j \subseteq \mathsf{A} \iff \mathcal{U} \setminus \mathsf{A} \subseteq \mathcal{U} \setminus C_j$.
  - For $id \in \{C_1, C_2, \cdots C_t, \mathsf{A}\}$, $S_{id}[i] = \begin{cases} 0 & \text{if } i \in id \\ 1 & \text{if } i \notin id \end{cases}$

DNF Schemes	|mpk|	|SK|	|CT|	pairing	Security	Assumption
SPE-1 [KMMS17]	$(n+2)\mathbb{G}_1$	$\mathbb{G}_2 + \mathbb{Z}_p$	$\gamma((n+1)\mathbb{G}_1)$	1	selective	q-BDHI
SPE-2 [KMMS17]	$(n+1)\mathbb{G}_1 + 2\mathbb{G}_2$	$\mathbb{G}_1 + \mathbb{G}_2$	$\gamma(2n\mathbb{G}_1 + \mathbb{G}_2)$	2	selective	DBDH
SPE_2 based	$(n+3)\mathbb{G}_1$	$5\mathbb{G}_2$	$\gamma((n+2)\mathbb{G}_1 + n\mathbb{Z}_p)$	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_1
  - SPE_2 with smaller ciphertext size

RSAConference2019

Thank you

Questions?