General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps

by

Pratish Datta

joint work with

Ratna Dutta and **Sourav Mukhopadhyay**

Department of Mathematics
Indian Institute of Technology Kharagpur
Kharagpur-721302
India

ISC 2015
9–11th September, 2015

Outline

1. Introduction
2. Preliminaries
3. Our RABE Constructions
4. Security
5. Efficiency
6. Conclusion

Motivation

- *Attribute-based encryption* (ABE) has been extensively deployed to realize complex access control functionalities in cloud environment.
- Two crucial requirements of ABE systems are:
  - (i) Expressiveness of the supported decryption policies
  - (ii) User revocation

Motivation

- While [GGH+13b], [BGG+14] presented ABE for arbitrary *polynomial-size* Boolean circuits of *unbounded* fan-out, they do not support revocation.
- In all the existing *revocable* ABE (RABE) systems the decryption policies were restricted to circuits of fan-out one, paving the way for a "back-tracking" attack.

[BGG+14]: Dan Boneh et al. In Advances in Cryptology–EUROCRYPT 2014.

[GGH+13b]: Sanjam Garg et al. In Advances in Cryptology–CRYPTO 2013.

Advantage of Direct Revocation in ABE

- The *direct* revocation technique controls revocation by specifying a revocation list directly during encryption.
- This method does not involve any additional proxy server or key update phase.
- Consequently, the non-revoked users remain unaffected and revocation can take effect instantly without requiring to wait for the expiration of the current time period.

Drawback of the Tree-Based Revocation Technique of Naor et al.

- All currently available standard model RABE constructions supporting direct revocation mode follow the tree-based revocation mechanism of Naor et al. [NNL01].
- Consequently, the number of *revocation controlling components* in ciphertexts and decryption keys are $O(\widehat{r}\log\frac{N_{\max}}{\widehat{r}})$ and $O(\log N_{\max})$ respectively.
- $N_{\max}$ is the maximum number of users supported by the system and $\widehat{r}$ is the number of revoked users.

[NNL01]: Dalit Naor et al. In Advances in Cryptology–CRYPTO 2001.

Highlights of Our Work

- We apply the revocation technique introduced in [BGW05] and its improved variant [BWZ14] in the ABE setting.
- We propose two *direct* RABE schemes:
  - RABE-I: *first* to support *general circuits* and to feature *constant* number of revocation enforcing components in ciphertexts and decryption keys but public parameter size is *linear* to $N_{\max}$.
  - RABE-II: achieves similar properties with public parameter size *logarithmic* to $N_{\max}$.

[BGW05]: Dan Boneh et al. In Advances in Cryptology–CRYPTO 2005.

[BWZ14]: Dan Boneh et al. In Advances in Cryptology–CRYPTO 2014.

Multilinear Map

A (leveled) multilinear map consists of the following two algorithms:

1. $\mathcal{G}^{\mathsf{MLM}}(1^\lambda, \kappa) \rightarrow \mathsf{PP}_{\mathsf{MLM}} = (\vec{\mathbb{G}} = (\mathbb{G}_1, \ldots, \mathbb{G}_\kappa), g_1, \ldots, g_\kappa)$ where $\mathbb{G}_i$'s are groups each of prime order $p > 2^\lambda$, $g_i \in \mathbb{G}_i$ are canonical generators.
2. $e_{i,j}(g \in \mathbb{G}_i, h \in \mathbb{G}_j) \rightarrow v \in \mathbb{G}_{i+j}$ (for $i, j \in \{1, \ldots, \kappa\}, i + j \leq \kappa$) such that
$$e_{i,j}(g_i^a, g_j^b) = g_{i+j}^{ab}$$
for $a, b \in \mathbb{Z}_p$. We can also generalize e to multiple inputs as
$$e(\chi^{(1)}, \ldots, \chi^{(t)}) = e(\chi^{(1)}, e(\chi^{(2)}, \ldots, \chi^{(t)})).$$

Circuit Notation

- We consider *monotone* and *layered* circuits with OR and AND gates having fan-in two.
- A circuit $f = (\ell, q, d, \mathbb{A}, \mathbb{B}, \mathsf{GateType})$.
- Here, ℓ, q, and d respectively denote the length of the input, the number of gates, and depth of the circuit.
- Input $= \{1, \ldots, \ell\}$, Gates $= \{\ell+1, \ldots, \ell+q\}$, $W =$ Input $\cup$ Gates, and $\ell + q =$ the output wire.
- $\mathbb{A}, \mathbb{B}$: gates $\rightarrow W \backslash \{\ell + q\}$ are functions such that for all $w \in$ Gates, $\mathbb{A}(w)$ and $\mathbb{B}(w)$ respectively identify w's first and second incoming wires. We consider $w > \mathbb{B}(w) > \mathbb{A}(w)$.

Circuit Notation

- $\mathsf{GateType} : \mathsf{Gates} \to \{\mathsf{AND}, \mathsf{OR}\}$ defines a functions that identifies a gate as either an AND or an OR gate.
- $\mathsf{depth} : W \to \{1, \ldots, d\}$ is a function such that $\mathsf{depth}(w) = 1$, if $w \in \mathsf{Input}$, and $\mathsf{depth}(w) =$ one plus the length of the shortest path from w to an input wire, otherwise. Since our circuit is layered, for all $w \in \mathsf{Gates}$,

$$\mathsf{depth}(\mathbb{A}(w)) = \mathsf{depth}(\mathbb{B}(w)) = \mathsf{depth}(w) - 1.$$

- $f(x) =$ evaluation of the circuit f on input $x \in \{0,1\}^\ell$, and $f_w(x) =$ value of wire w of f on x.

RABE-I

RABE.Setup$(1^\lambda, \ell, d, N_{\max})$

1. $\mathcal{G}^{\mathsf{MLM}}(1^\lambda, \kappa = \ell + d + 1) \rightarrow \mathsf{PP}_{\mathsf{MLM}} = (\vec{\mathbb{G}} = (\mathbb{G}_1, \ldots, \mathbb{G}_\kappa), g_1, \ldots, g_\kappa)$.
2. $A_{i,\beta} = g_1^{a_{i,\beta}}$ for $i = 1, \ldots, \ell;\ \beta \in \{0, 1\}$, where $(a_{1,0}, a_{1,1}), \ldots, (a_{\ell,0}, a_{\ell,1}) \in_\$ \mathbb{Z}_p^2$.
3. $\vartheta_j = g_1^{\alpha^{(j)}}$ for $j = 1, \ldots, N_{\max}, N_{\max} + 2, \ldots, 2N_{\max}, Y = g_1^{\gamma}$, $Z = g_{d-1}^{\theta},\ \Omega = g_{d+1}^{\alpha^{(N_{\max}+1)}\theta}$, where $\alpha, \gamma, \theta \in_\$ \mathbb{Z}_p$.
4. Publish $\mathsf{PP} = (\mathsf{PP}_{\mathsf{MLM}}, \{A_{i,\beta}\}_{i=1,\ldots,\ell;\beta\in\{0,1\}}, \{\vartheta_j\}_{j=1,\ldots,N_{\max},N_{\max}+2,\ldots,2N_{\max}}, Y, Z, \Omega)$ along with $\mathsf{UL} = \varnothing$ while keep $\mathsf{MK} = (\alpha, \gamma, \theta)$.

RABE-I

RABE.KeyGen(PP, MK, UL, ID, $f = (\ell, q, d, \mathbb{A}, \mathbb{B}$, GateType))

1. Assign $u \in \mathcal{N} = \{1, \ldots, N_{\max}\}$ such that $(\cdot, u) \notin$ UL to ID, update UL = UL $\cup$ $\{(\text{ID}, u)\}$.
2. $r_1, \ldots, r_{\ell+q} \in_{\$} \mathbb{Z}_p$.
3. $\mathcal{K} = g_d^{\alpha^{(u)}\theta\gamma - r_{\ell+q}}$.

RABE-I

RABE.KeyGen$(\mathsf{PP}, \mathsf{MK}, \mathsf{UL}, \mathsf{ID}, f = (\ell, q, d, \mathbb{A}, \mathbb{B}, \mathsf{GateType}))$

4. Generate key components for every wire w as follows:
   - *Input wire*: $\mathcal{K}_w = e(A_{w,1}, g_1)^{r_w} = g_2^{r_w a_{w,1}}$.
   - *OR gate*: Let $t = \mathsf{depth}(w)$. $\mu_w, \nu_w \in_{\$} \mathbb{Z}_p$,

     $$\mathcal{K}_w = \left(K_{w,1} = g_1^{\mu_w}, K_{w,2} = g_1^{\nu_w}, K_{w,3} = g_t^{r_w - \mu_w r_{\mathbb{A}(w)}}, K_{w,4} = g_t^{r_w - \nu_w r_{\mathbb{B}(w)}}\right).$$
   - *AND gate*: Let $t = \mathsf{depth}(w)$. $\mu_w, \nu_w \in_{\$} \mathbb{Z}_p$,

     $$\mathcal{K}_w = \left(K_{w,1} = g_1^{\mu_w}, K_{w,2} = g_1^{\nu_w}, K_{w,3} = g_t^{r_w - \mu_w r_{\mathbb{A}(w)} - \nu_w r_{\mathbb{B}(w)}}\right).$$
5. Give $\mathsf{SK}_{f,\mathsf{ID}} = \left(f, \mathsf{ID}, \mathcal{K}, \{\mathcal{K}_w\}_{w \in \{1,\ldots,\ell+q\}}\right)$ to the user.

RABE-I

RABE.Encrypt(PP, UL, $x = x_1 \ldots x_\ell \in \{0,1\}^\ell$, RL, $M \in \mathbb{G}_\kappa$)

1. Define RI $\subseteq \mathcal{N}$ corresponding to RL using UL, i.e., if ID $\in$ RL and (ID, j) $\in$ UL include j in RI. Determine SI $= \mathcal{N} \backslash$RI.
2. $s \in_\$ \mathbb{Z}_p$,

$$C_M = e(\Omega, A_{1,x_1}, \ldots, A_{\ell,x_\ell})^s M = g_\kappa^{\alpha^{(N_{\max}+1)}\theta s \delta(x)} M,$$
$$C = g_1^s,\ C' = \Big(Y \prod_{j \in \mathsf{SI}} \vartheta_{N_{\max}+1-j}\Big)^s = \Big(g_1^\gamma \prod_{j \in \mathsf{SI}} g_1^{\alpha^{(N_{\max}+1-j)}}\Big)^s,$$

where $\delta(x) = \prod_{i=1}^{\ell} a_{i,x_i}$.

3. Output $\mathsf{CT}_{x,\mathsf{RL}} = (x, \mathsf{RL}, C_M, C, C')$.

RABE-I

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

1. Output $\perp$, if $[f(x) = 0] \ \vee \ [\mathsf{ID} \in \mathsf{RL}]$; otherwise, proceed to the next step.
2. $D = \ e(A_{1,x_1}, \ldots, A_{\ell,x_\ell}) = g_\ell^{\delta(x)}$,
   $\widehat{E} = \ e(\mathcal{K}, D, C) = g_\kappa^{(\alpha^{(u)}\theta\gamma - r_{\ell+q})s\delta(x)}$.

RABE-I

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

3. Perform the bottom-up evaluation of the circuit. For every wire w with corresponding depth$(w) = t$, if $f_w(x) = 0$, compute nothing, otherwise, compute $E_w = g_{\ell+t+1}^{r_w s\delta(x)}$ as follows:
   - *Input wire*:
   $$E_w = e(\mathcal{K}_w, A_{1,x_1}, \ldots, A_{w-1,x_{w-1}}, A_{w+1,x_{w+1}}, \ldots, A_{\ell,x_\ell}, C) = g_{\ell+1+1}^{r_w s\delta(x)}.$$
   - *OR gate*: If $f_{\mathbb{A}(w)}(x) = 1$,
   $$E_w = e(E_{\mathbb{A}(w)}, K_{w,1})e(K_{w,3}, D, C) = g_{\ell+t+1}^{r_w s\delta(x)}.$$
   Alternatively, if $f_{\mathbb{A}(w)}(x) = 0$ and hence $f_{\mathbb{B}(w)}(x) = 1$,
   $$E_w = e(E_{\mathbb{B}(w)}, K_{w,2})e(K_{w,4}, D, C) = g_{\ell+t+1}^{r_w s\delta(x)}.$$
   - *AND gate*: Certainly $f_{\mathbb{A}(w)}(x) = f_{\mathbb{B}(w)}(x) = 1$.
   $$E_w = e(E_{\mathbb{A}(w)}, K_{w,1})e(E_{\mathbb{B}(w)}, K_{w,2})e(K_{w,3}, D, C) = g_{\ell+t+1}^{r_w s\delta(x)}.$$

   Finally, $E_{\ell+q} = g_\kappa^{r_{\ell+q} s\delta(x)}$, as $f(x) = f_{\ell+q}(x) = 1$.

RABE-I

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

4. Determine $\mathsf{RI} \subseteq \mathcal{N}$ corresponding to RL using UL and obtain $\mathsf{SI} = \mathcal{N} \backslash \mathsf{RI}$. Since $\mathsf{ID} \notin \mathsf{RL}$, $u \in \mathsf{SI}$.
5. Retrieve the message by the following computation:

$$
\begin{aligned}
& C_M \widehat{E} E_{\ell+q} e\big(\prod_{j \in \mathsf{SI}\backslash\{u\}} \vartheta_{N_{\max}+1-j+u}, Z, D, C\big) e\big(\vartheta_u, Z, D, C'\big)^{-1} \\
& = g_\kappa^{\alpha^{(N_{\max}+1)}\theta s \delta(x)} M \cdot g_\kappa^{(\alpha^{(u)}\theta\gamma - r_{\ell+q}) s \delta(x)} \cdot g_\kappa^{r_{\ell+q} s \delta(x)} \cdot \\
& \quad \prod_{j \in \mathsf{SI}\backslash\{u\}} g_\kappa^{\alpha^{(N_{\max}+1-j+u)}\theta s \delta(x)} \cdot \big[g_\kappa^{\alpha^{(u)}\theta\gamma s \delta(x)} \cdot \\
& \quad g_\kappa^{\alpha^{(N_{\max}+1)}\theta s \delta(x)} \cdot \prod_{j \in \mathsf{SI}\backslash\{u\}} g_\kappa^{\alpha^{(N_{\max}+1-j+u)}\theta s \delta(x)} \big]^{-1} \\
& = M.
\end{aligned}
$$

RABE-II

RABE.Setup$(1^\lambda, \ell, d, N_{\max})$

1. Choose two positive integers n, m suitably such that $N_{\max} \leq \binom{n}{m}$. $\mathcal{N} = \{j \in \{1, \ldots, 2^n - 2\} \mid \mathsf{HW}(j) = m\}$.
2. $\mathcal{G}^{\mathsf{MLM}}(1^\lambda, \kappa = n+d+m-1) \rightarrow \mathsf{PP}_{\mathsf{MLM}} = (\vec{\mathbb{G}} = (\mathbb{G}_1, \ldots, \mathbb{G}_\kappa), g_1, \ldots, g_\kappa)$.
3. $A_i = g_m^{a_i}$ for $i = 1, \ldots, \ell$ where $a_1, \ldots, a_\ell \in_\$ \mathbb{Z}_p$.
4. $\xi_\iota = g_1^{\alpha^{(2^\iota)}}$ for $\iota = 0, \ldots, n$, $Y = g_{n-1}^\gamma$, $Z = g_d^\theta$, $\Omega = g_\kappa^{\alpha^{(2^n-1)}\theta}$, where $\alpha, \gamma, \theta \in_\$ \mathbb{Z}_p$.
5. Keep $\mathsf{MK} = (\alpha, \gamma, \theta)$ while publish $\mathsf{PP} = (\mathsf{PP}_{\mathsf{MLM}}, n, m, \{A_i\}_{i=1,\ldots,\ell}, \{\xi_\iota\}_{\iota=0,\ldots,n}, Y, Z, \Omega)$ along with $\mathsf{UL} = \varnothing$.

RABE-II

RABE.KeyGen(PP, MK, UL, ID, $f = (\ell, q, d, \mathbb{A}, \mathbb{B}, \text{GateType})$)

1. Assign to ID $u \in \mathcal{N}$ such that $(\cdot, u) \notin \text{UL}$, update $\text{UL} = \text{UL} \cup \{(\text{ID}, u)\}$.
2. $r_1, \ldots, r_{\ell+q} \in_{\$} \mathbb{Z}_p$.
3. $\mathcal{K} = g_{n+d-1}^{\alpha^{(u)}\theta\gamma - r_{\ell+q}}$.

RABE-II

RABE.KeyGen(PP, MK, UL, ID, $f = (\ell, q, d, \mathbb{A}, \mathbb{B}, \text{GateType})$)

4. Form key components for every wire w as follows:
   - *Input wire*: $z_w \in_\$ \mathbb{Z}_p$,
   $$\mathcal{K}_w = \big(K_{w,1} = g_n^{r_w} e(A_w, g_{n-m})^{z_w} = g_n^{r_w} g_n^{a_w z_w},\ K_{w,2} = g_n^{-z_w}\big).$$
   - *OR gate*: Let $t = \text{depth}(w)$. $\mu_w, \nu_w \in_\$ \mathbb{Z}_p$,
   $$\mathcal{K}_w = \big(K_{w,1} = g_1^{\mu_w}, K_{w,2} = g_1^{\nu_w}, K_{w,3} = g_{n+t-1}^{r_w - \mu_w r_{\mathbb{A}(w)}}, K_{w,4} = g_{n+t-1}^{r_w - \nu_w r_{\mathbb{B}(w)}}\big).$$
   - *AND gate*: Let $t = \text{depth}(w)$. $\mu_w, \nu_w \in_\$ \mathbb{Z}_p$,
   $$\mathcal{K}_w = \big(K_{w,1} = g_1^{\mu_w}, K_{w,2} = g_1^{\nu_w}, K_{w,3} = g_{n+t-1}^{r_w - \mu_w r_{\mathbb{A}(w)} - \nu_w r_{\mathbb{B}(w)}}\big).$$
5. Hand $\text{SK}_{f,\text{ID}} = \big(f, \text{ID}, \mathcal{K}, \{\mathcal{K}_w\}_{w \in \{1,\ldots,\ell+q\}}\big)$ to the user.

RABE-II

RABE.Encrypt(PP, UL, $x = x_1 \dots x_\ell \in \{0,1\}^\ell$, RL, $M \in \mathbb{G}_\kappa$)

1. Define RI $\subseteq \mathcal{N}$ corresponding to RL using UL and set SI $= \mathcal{N} \setminus$ RI.
2. Compute ϑ_{2^n-1-j} for all $j \in$ SI as follows, where $\vartheta_\varpi = g_{n-1}^{\alpha^{(\varpi)}}$ for positive integer ϖ. For any $j \in$ SI $\subseteq \mathcal{N}$, $j = \sum_{\iota \in J} 2^\iota$ where $J \subseteq \{0, \dots, n-1\}$, $|J| = m$. Thus, $2^n - 1 - j = \sum_{\iota \in \overline{J}} 2^\iota$ where $\overline{J} = \{0, \dots, n-1\} \setminus J = \{\iota_1, \dots, \iota_{n-m}\}$ (say). So,

$$\vartheta_{2^n-1-j} = e(\xi_{\iota_1}, \dots, \xi_{\iota_{n-m}}, g_{m-1}) = g_{n-1}^{\alpha^{(2^n-1-j)}}.$$

RABE-II

RABE.Encrypt(PP, UL, $x = x_1 \dots x_\ell \in \{0,1\}^\ell$, RL, $M \in \mathbb{G}_\kappa$)

3. $s \in_{\$} \mathbb{Z}_p$,

$$C_M = \Omega^s M = g_\kappa^{\alpha^{(2^n-1)}\theta s} M,\ C = g_m^s,$$
$$C_i' = A_i^s = g_m^{a_i s} \text{ for } i \in \mathcal{S}_x = \{i | i \in \{1,\dots,\ell\} \ \wedge\ x_i = 1\},$$
$$C'' = \Big(Y \prod_{j \in \mathsf{SI}} \vartheta_{2^n-1-j}\Big)^s = \Big(g_{n-1}^{\gamma} \prod_{j \in \mathsf{SI}} g_{n-1}^{\alpha^{(2^n-1-j)}}\Big)^s.$$

4. Output $\mathsf{CT}_{x,\mathsf{RL}} = (x, \mathsf{RL}, C_M, C, \{C_i'\}_{i \in \mathcal{S}_x}, C'')$.

RABE-II

RABE.Decrypt(PP, UL, CT$_{x,\mathsf{RL}}$, SK$_{f,\mathsf{ID}}$)

1. Output $\perp$, if $[f(x) = 0] \vee [\mathsf{ID} \in \mathsf{RL}]$; otherwise, proceed to the next step.
2. $\widehat{E} = e(\mathcal{K}, C) = e(g_{n+d-1}^{\alpha^{(u)}\theta\gamma - r_{\ell+q}}, g_m^s) = g_\kappa^{(\alpha^{(u)}\theta\gamma - r_{\ell+q})s}$.

RABE-II

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

3. Perform the bottom-up evaluation of the circuit. For every wire w with corresponding depth$(w) = t$, if $f_w(x) = 0$, compute nothing, otherwise, compute $E_w = g_{n+t+m-1}^{r_w s}$ as follows:
   - *Input wire*:
   $$E_w = e(K_{w,1}, C)e(K_{w,2}, C'_w) = g_{n+m}^{r_w s} = g_{n+1+m-1}^{r_w s}.$$
   - *OR gate*: If $f_{\mathbb{A}(w)}(x) = 1$,
   $$E_w = e(E_{\mathbb{A}(w)}, K_{w,1})e(K_{w,3}, C) = g_{n+t+m-1}^{r_w s}.$$
   Alternatively, if $f_{\mathbb{A}(w)}(x) = 0$ and hence $f_{\mathbb{B}(w)}(x) = 1$,
   $$E_w = e(E_{\mathbb{B}(w)}, K_{w,2})e(K_{w,4}, C) = g_{n+t+m-1}^{r_w s}.$$
   - *AND gate*: Certainly $f_{\mathbb{A}(w)}(x) = f_{\mathbb{B}(w)}(x) = 1$.
   $$E_w = e(E_{\mathbb{A}(w)}, K_{w,1})e(E_{\mathbb{B}(w)}, K_{w,2})e(K_{w,3}, C) = g_{n+t+m-1}^{r_w s}.$$

Finally, $E_{\ell+q} = g_{\kappa}^{r_{\ell+q} s}$, as $f(x) = f_{\ell+q}(x) = 1$.

RABE-II

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

4. Determine $\mathsf{RI} \subseteq \mathcal{N}$ corresponding to RL using UL and obtain $\mathsf{SI} = \mathcal{N} \backslash \mathsf{RI}$. As $\mathsf{ID} \notin \mathsf{RL}$, $u \in \mathsf{SI}$.
5. Compute $\vartheta'_u = g_m^{\alpha^{(u)}}$ and $\vartheta_{2^n-1-j+u} = g_{n-1}^{\alpha^{(2^n-1-j+u)}}$ for all $j \in \mathsf{SI}\backslash\{u\}$ as follows:
   (a) (Computing ϑ'_u) As $u \in \mathsf{SI} \subseteq \mathcal{N}$, $u = \sum_{\iota \in U} 2^\iota$ where $U = \{\iota'_1, \ldots, \iota'_m\} \subseteq \{0, \ldots, n-1\}$ (say). So, $\vartheta'_u = e(\xi_{\iota'_1}, \ldots, \xi_{\iota'_m}) = g_m^{\alpha^{(u)}}$.
   (b) (Computing $\vartheta_{2^n-1-j+u}$ for $j \in \mathsf{SI}\backslash\{u\}$) $2^n - 1 - j = \sum_{\iota \in \overline{J}} 2^\iota$ where $\overline{J} = \{\iota_1, \ldots, \iota_{n-m}\} \subseteq \{0, \ldots, n-1\}$. $U \cap \overline{J} = \varnothing$ only if $j = u$. Since $j \neq u$, $\exists \widehat{\iota} \in \overline{J} \cap U$. $\widehat{\iota} = \iota_{n-m} = \iota'_m$ (say). Then, $2^n - 1 - j + u = \sum_{\iota \in \overline{J} \backslash \{\widehat{\iota}\}} 2^\iota + \sum_{\iota \in U \backslash \{\widehat{\iota}\}} 2^\iota + 2^{\widehat{\iota}+1}$. So,
   $$\vartheta_{2^n-1-j+u} = e(\xi_{\iota_1}, \ldots, \xi_{\iota_{n-m-1}}, \xi_{\iota'_1}, \ldots, \xi_{\iota'_{m-1}}, \xi_{\widehat{\iota}+1}) = g_{n-1}^{\alpha^{(2^n-1-j+u)}}.$$

RABE-II

RABE.Decrypt$(\mathsf{PP}, \mathsf{UL}, \mathsf{CT}_{x,\mathsf{RL}}, \mathsf{SK}_{f,\mathsf{ID}})$

6. Retrieve the message by the following computation:

$$C_M \widehat{E} E_{\ell+q} e\Big(\prod_{j \in \mathsf{SI} \setminus \{u\}} \vartheta_{2^n-1-j+u}, Z, C\Big) e\big(\vartheta'_u, Z, C''\big)^{-1}$$

$$= g_\kappa^{\alpha^{(2^n-1)}\theta s} M \cdot g_\kappa^{(\alpha^{(u)}\theta\gamma - r_{\ell+q})s} \cdot g_\kappa^{r_{\ell+q}s} \cdot \prod_{j \in \mathsf{SI} \setminus \{u\}} g_\kappa^{\alpha^{(2^n-1-j+u)}\theta s} \cdot$$

$$\Big[g_\kappa^{\alpha^{(u)}\theta\gamma s} \cdot g_\kappa^{\alpha^{(2^n-1)}\theta s} \cdot \prod_{j \in \mathsf{SI} \setminus \{u\}} g_\kappa^{\alpha^{(2^n-1-j+u)}\theta s} \Big]^{-1}$$

$$= M.$$

Security Statements

Theorem (RABE-I)

- RABE-I *is secure in the selective revocation list model against* CPA *if the* $(\ell + d + 1, N_{\max})$-MDHE *assumption holds for the underlying multilinear group generator* $\mathcal{G}^{\mathsf{MLM}}$.
- $\ell, d,$ *and* $N_{\max}$ *denote respectively the input length of decryption circuits, depth of the decryption circuits, and the maximum number of users supported by the system.*

Theorem (RABE-II)

- RABE-II *is secure in the selective revocation list model against* CPA *if the* (n, d, m)-cMDHE *assumption holds for the underlying multilinear group generator* $\mathcal{G}^{\mathsf{MLM}}$.
- n, m *are two integers for which* $N_{\max} \leq \binom{n}{m}$.

Multilinear Diffie-Hellman Exponent Assumption: (κ, N)-MDHE

- It is hard to guess $\widetilde{b} \in \{0,1\}$ given $\varrho_{\widetilde{b}} \leftarrow \mathcal{G}_{\widetilde{b}}^{(\kappa,N)\text{-MDHE}}(1^{\lambda})$.
- $\underline{\mathcal{G}_{\widetilde{b}}^{(\kappa,N)\text{-MDHE}}(1^{\lambda})}$:
  - $\mathcal{G}^{\mathsf{MLM}}(1^{\lambda}, \kappa) \rightarrow \mathsf{PP}_{\mathsf{MLM}}$;
  - $\alpha, \varsigma, \psi_1, \ldots, \psi_{\kappa-2} \in_{\$} \mathbb{Z}_p$;
  - $\vartheta_j = g_1^{\alpha^{(j)}}$ for $j = 1, \ldots, N, N+2, \ldots, 2N, \Upsilon = g_1^{\varsigma}, \tau_i = g_1^{\psi_i}$ for $i = 1, \ldots, \kappa - 2$;
  - $\Re_0 = g_{\kappa}^{\alpha^{(N+1)}\varsigma \prod_{i=1}^{\kappa-2} \psi_i}$, $\Re_1 =$ some random element in $\mathbb{G}_{\kappa}$;
  - $\varrho_{\widetilde{b}} = (\mathsf{PP}_{\mathsf{MLM}}, \vartheta_1, \ldots, \vartheta_N, \vartheta_{N+2}, \ldots, \vartheta_{2N}, \Upsilon, \tau_1, \ldots, \tau_{\kappa-2}, \Re_{\widetilde{b}})$.

Compressed Multilinear Diffie-Hellman Exponent Assumption: (n,k,l)-cMDHE

- It is hard to guess $\widetilde{b} \in \{0,1\}$ given $\varrho_{\widetilde{b}} \leftarrow \mathcal{G}_{\widetilde{b}}^{(n,k,l)\text{-cMDHE}}(1^\lambda)$.
- $\underline{\mathcal{G}_{\widetilde{b}}^{(n,k,l)\text{-cMDHE}}(1^\lambda)}$:
  - $\mathcal{G}^{\mathsf{MLM}}(1^\lambda, \kappa = n+k+l-1) \rightarrow \mathsf{PP}_{\mathsf{MLM}}$;
  - $\alpha, \varsigma, \psi_1, \ldots, \psi_k \in_{\$} \mathbb{Z}_p$;
  - $\xi_\iota = g_1^{\alpha^{(2^\iota)}}$ for $\iota = 0, \ldots, n, \tau_h = g_1^{\psi_h}$ for $h = 1, \ldots, k,\ \Upsilon = g_l^{\varsigma}$;
  - $\mathfrak{R}_0 = g_\kappa^{\alpha^{(2^n-1)}\varsigma\prod_{h=1}^{k}\psi_h}$, $\mathfrak{R}_1 =$ some random element of $\mathbb{G}_\kappa$;
  - $\varrho_{\widetilde{b}} = (\mathsf{PP}_{\mathsf{MLM}}, \xi_0, \ldots, \xi_n, \tau_1, \ldots, \tau_k, \Upsilon, \mathfrak{R}_{\widetilde{b}})$.

Complexity Analysis

Communication and Storage

- RABE-I:
  - only 3 group elements in the ciphertexts.
  - number of decryption key components $\ell + 4q + 1$ in the worst case.
  - the number of PP components linear to $N_{\max}$.
- RABE-II:
  - the number of PP components linear to n, where $N_{\max} \leq \binom{n}{m}$, i.e., $\log N_{\max}$ approximately for a judicious choice of n and m.
  - number of ciphertext and decryption key components meant for revocation do not grow with $N_{\max}$.
- No previous RABE scheme with direct revocation could achieve such parameters.

Complexity Analysis
Computation

Table: Count of Multilinear Operation

RABE	RABE.Setup	RABE.KeyGen	RABE.Encrypt	RABE.Decrypt
RABE-I	$2\ell + 2N_{\max} + 2$	$2\ell + 4q + 2$	4	$\ell + 3q + 4$
RABE-II	$\ell + 2n + 5$	$4\ell + 4q + 3$	$\ell + 3$	$2\ell + 3q + 3$

Future Scope

- Designing an *adaptively* secure RABE scheme with *polynomial* security reduction under *standard* assumption while attaining the efficiency level of our constructions.
- Building a *revocable storage* ABE (RSABE) scheme with those parameters achieved by our work.

Thanking Note