SCIENCE CHINA
Information Sciences

• LETTER •

November 2016, Vol. 59 119102:1–119102:3
doi: 10.1007/s11432-016-0062-7

Traceable and revocable CP-ABE with shorter ciphertexts

Jianting NING[1], Zhenfu CAO[2*], Xiaolei DONG[2] & Lifei WEI[3]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*Shanghai Key Lab for Trustworthy Computing, East China Normal University, Shanghai* 200062*, China;*
[3]*College of Information Technology, Shanghai Ocean University, Shanghai* 201306*, China*

Received January 21, 2016; accepted March 14, 2016; published online September 5, 2016

Citation Ning J T, Cao Z F, Dong X L, et al. Traceable and revocable CP-ABE with shorter ciphertexts. Sci China Inf Sci, 2016, 59(11): 119102, doi: 10.1007/s11432-016-0062-7

Dear editor,

As a sophisticated mechanism for secure fine-grained access control on encrypted data, Ciphertext-policy attribute-based encryption (CP-ABE) is a highly promising solution for commercial applications such as cloud computing and social networks. However, there exists an important and practical issue in current CP-ABE systems awaiting to solve. As a one-to-many encryption mechanism, the same ciphertexts will be decrypted by different users as long as the attributes they possess satisfy the ciphertexts' access policies. That is, different users who have the same attributes will share the same decryption privilege. This leaves a chance for the malicious users who may be tempted to leak their decryption keys or some decryption privilege in the form of a decryption black-box/device to others for profits. Due to the nature of CP-ABE, it is difficult to trace the malicious users who leak their decryption privilege deliberately. To address this problem, many advances have been made recently [1–4]. In particular, Liu et al. [5,6] introduced black-box traceability to current CP-ABE system to trace the malicious users who leak decryption black-box/device. They intertwine a non-traceable CP-ABE system and the traitor tracing scheme [7] together in a novel way, and get the first CP-ABE that simultaneously supports public and fully collusion-resistant black-box traceability with sub-linear overhead, full security, high expressivity. Since the underlying traitor tracing part of their system is based on the traitor trace scheme in [7], the resulting ciphertexts are $2l + 17\sqrt{\mathcal{N}}$, which is the most efficient one to date, where l is the size of an access policy and $\mathcal{N}$ is the number of users in the system. In addition, the pairing computations in decryption is $2|I| + 10$, where I is the number of attributes in a decryption key that satisfies a ciphertext's access policy. This evokes the following two questions: (1) Whether there exists a more efficient black-box traceable CP-ABE with shorter ciphertexts and less the pairing computations in decryption without sacrificing other performance? (2) How to revoke the malicious users efficiently after they are traced?

Our contribution. We propose an improved CP-ABE system with high expressiveness (i.e., supporting any monotonic access structures), black-box traceability and full security (i.e., provably secure against adaptive adversaries in the standard model) as Liu et al.'s traceable CP-ABE systems [5,6]. The system is fully collusion-resistant public traceability against key-like decryption black-

* Corresponding author (email: zfcao@sei.ecnu.edu.cn)

The authors declare that they have no conflict of interest.

Table 1 Comparison with other related work[a)]

	Ref. [1]	Ref. [2]	Ref. [4]	Ref. [5,6]	This work
Traceability	White-box	White-box	White-box	Black-box	Black-box
Fully secure	$\surd$	$\times$	$\times$	$\surd$	$\surd$
Public key size	$\lvert\mathcal{U}\rvert+4$	7	7	$\lvert\mathcal{U}\rvert+3+4\sqrt{\mathcal{N}}$	$\lvert\mathcal{U}\rvert+3+4\sqrt{\mathcal{N}}$
Private key size	$\lvert S\rvert+4$	$2\lvert S\rvert+4$	$2\lvert S\rvert+4$	$\lvert S\rvert+4$	$\lvert S\rvert+4$
Ciphertext size	$2l+3$	$3l+3$	$3l+3$	$2l+17\sqrt{\mathcal{N}}$	$2l+9\sqrt{\mathcal{N}}$
Pairing in decryption	$2\lvert I\rvert+1$	$3\lvert I\rvert+1$	$3\lvert I\rvert+1$	$2\lvert I\rvert+10$	$2\lvert I\rvert+6$

a) Let $\mathcal{U}$ be the size of the attribute universe, $|S|$ the size of the attribute set of a private key, l the size of an access policy, $|I|$ the number of attributes in a decryption key that satisfies a ciphertext's access policy, and $\mathcal{N}$ the number of users in the system.

box, that is, the tracing algorithm can track at least one of the malicious users even if there are an arbitrary number of malicious users colluding by pulling all of their decryption keys together when building a key-like decryption black-box, and it is public in the sense that the tracing algorithm needs no secrets and can be run by anyone. Furthermore, the system is more efficient than the best cases of black-box traceable CP-ABE systems (i.e., Liu et al.'s traceable CP-ABE systems [5,6]), that is, the ciphertext size is shorter and the decryption is faster, without sacrificing the sizes of public keys and private keys, which is the most efficient to date. We note that, the ciphertext size and the pairing computations in decryption both have a great impact on practicality, and traceable CP-ABE systems with shorter ciphertexts and less pairing computations in decryption are desirable. In addition, the system can revoke the traced malicious users efficiently, which is quite suitable for real-life applications. We introduce a new and simpler "cancellation technique" than [5, 6] to build our system, which may be of independent interests. Table 1 gives the comparison between our work and some other related work.

Our construction.

(1) $\texttt{Setup}_E(\lambda,\mathcal{U},\mathcal{N}=m^2)\rightarrow(\text{pp},\text{msk})$: It runs the group generator algorithm $\mathcal{G}$, and gets the groups and the bilinear mapping description $\text{GD}=(N,G,G_T,e)$, where (G,G_T) are groups of order $N=p_1p_2p_3$ (3 distinct primes) and e is the bilinear mapping. Let G_{p_i} denote the subgroup of order p_i in G. It randomly chooses $g,u,v\in G_{p_1},g_3\in G_{p_3},\{\alpha_i,r_i,f_i\}_{i\in[m]}\in\mathbb{Z}_N,\{b_j\}_{j\in[m]},\{h_k\}_{k\in\mathcal{U}}\in\mathbb{Z}_N$. It sets $(\text{GD},g,u,v,\{E_i=e(g,g)^{\alpha_i},G_i=g^{r_i},F_i=g^{f_i}\}_{i\in[m]},\{B_j=g^{b_j}\}_{j\in[m]},\{H_k=g^{h_k}\}_{k\in\mathcal{U}})$ as pp and $(\{\alpha_i,r_i\}_{i\in[m]},\{b_j\}_{j\in[m]},g_3)$ as msk. In addition, a counter cout = 0 is included in msk implicitly.

(2) $\texttt{KeyGen}_E(\text{pp},\text{msk},S)\rightarrow\text{sk}_{(i,j),S}$: The algorithm first sets cout = cout + 1 and computes the corresponding index in the form of (i,j), where $i,j\in[m]$ and $(i-1)\times m+j=\text{cout}$. It then randomly chooses $t_{i,j},s_{i,j}\in\mathbb{Z}_N$ and $R,R',R'',R'''\{R_k\}_{k\in S}\in G_{p_3}$. The private key $\text{sk}_{(i,j),S}$ is set as follows:

$$\langle K_{i,j}=g^{\alpha_i}g^{r_ib_j}u^{t_{i,j}}v^{s_{i,j}}R,K'_{i,j}=g^{s_{i,j}}R',$$
$$K''_{i,j}=g^{t_{i,j}}R'',K'''_{i,j}=F_i^{t_{i,j}}R''',$$
$$\{K_{i,j,k}=H_k^{t_{i,j}}R_k\}_{k\in S}\rangle$$

(3) $\texttt{Encrypt}_E(\text{pp},(A,\rho),(x,y),M,\text{RL})\rightarrow\text{ct}$: For A an $l\times n$ matrix and ρ a map from each row A_k of A to an attribute $\rho(k)$, the algorithm randomly chooses $\boldsymbol{\vartheta}=(s,\vartheta_2,\ldots,\vartheta_n)$. For $\text{RL}\subseteq[m,m]$ an revocation list which stores the indexes of revoked users, let $\text{RL}_{i'}$ be the set of revoked row index and $\text{RL}_{j'}$ be the set of revoked column index. The algorithm then randomly chooses $\{\sigma_d\}_{d\in[2]},\{\gamma_d\}_{d\in[6]},\{\delta_i\}_{i\in[m]},\{\eta_i\}_{i\in[m]},\{\mu_j\}_{j\in[y-1]},\{\theta_k\}_{k\in[l]},\{\tau_{i,d}\}_{i\in[x-1],d\in[4]}\in\mathbb{Z}_N$ under constraints that $\gamma_2\gamma_3-\gamma_1\gamma_4\neq0$, $\gamma_1\gamma_6-\gamma_2\gamma_5=0$ and $(\gamma_1+\gamma_5)\gamma_4-(\gamma_2+\gamma_6)\gamma_3=0$. To encrypt a message M to the recipients whose (index, attribute set) tuples $((i,j),S_{i,j})$ satisfy $(i,j)\geqslant(x,y)\ \wedge\ (S_{i,j}\text{ satisfies }(A,\rho))\ \wedge\ ((i,j)\in[m,m]\backslash\text{RL})$, the ciphertext ct is set as follows.

For each row $i\in[m]$, the algorithm creates row ciphertexts $(C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6},C_{i,7})$:

- if $i<x$:
$C_{i,1}=g^{\tau_{i,1}},C_{i,2}=g^{\tau_{i,2}},C_{i,3}=g^{\tau_{i,3}},$
$C_{i,4}=u^{\tau_{i,3}}F_i^{\eta_i}u^s,C_{i,5}=v^{\tau_{i,3}},$
$C_{i,6}=g^{\eta_i},C_{i,7}=E_i^{\tau_{i,4}}.$
- if $(i=x)\wedge(i\in\text{RL}_{i'})$:
$C_{i,1}=G_i^{\gamma_3\delta_i}G_i^{\gamma_5\delta_i},C_{i,2}=G_i^{\gamma_4\delta_i}G_i^{\gamma_6\delta_i},$
$C_{i,3}=g^{((\gamma_3+\gamma_5)\sigma_1+(\gamma_4+\gamma_6)\sigma_2)\delta_i},$
$C_{i,4}=u^{((\gamma_3+\gamma_5)\sigma_1+(\gamma_4+\gamma_6)\sigma_2)\delta_i}F_i^{\eta_i}u^s,$
$C_{i,5}=v^{((\gamma_3+\gamma_5)\sigma_1+(\gamma_4+\gamma_6)\sigma_2)\delta_i},C_{i,6}=g^{\eta_i},$
$C_{i,7}=M\cdot E_i^{((\gamma_3+\gamma_5)\sigma_1+(\gamma_4+\gamma_6)\sigma_2)\delta_i}.$
- if $(i=x)\wedge(i\notin\text{RL}_{i'})$:
$C_{i,1}=G_i^{\gamma_1\delta_i},C_{i,2}=G_i^{\gamma_2\delta_i},$
$C_{i,3}=g^{(\gamma_1\sigma_1+\gamma_2\sigma_2)\delta_i},$
$C_{i,4}=u^{(\gamma_1\sigma_1+\gamma_2\sigma_2)\delta_i}F_i^{\eta_i}u^s,$
$C_{i,5}=v^{(\gamma_1\sigma_1+\gamma_2\sigma_2)\delta_i},$
$C_{i,6}=g^{\eta_i},C_{i,7}=M\cdot E_i^{(\gamma_1\sigma_1+\gamma_2\sigma_2)\delta_i}.$
- if $(i>x)\wedge(i\in\text{RL}_{i'})$:
$C_{i,1}=G_i^{\gamma_3\delta_i},C_{i,2}=G_i^{\gamma_4\delta_i},$
$C_{i,3}=g^{(\gamma_3\sigma_1+\gamma_4\sigma_2)\delta_i},$
$C_{i,4}=u^{(\gamma_3\sigma_1+\gamma_4\sigma_2)\delta_i}F_i^{\eta_i}u^s,$

$C_{i,5} = v^{(\gamma_3\sigma_1+\gamma_4\sigma_2)\delta_i}$,
$C_{i,6} = g^{\eta_i}, C_{i,7} = M \cdot E_i^{(\gamma_3\sigma_1+\gamma_4\sigma_2)\delta_i}$.

- if $(i > x) \wedge (i \notin \mathrm{RL}_{i'})$:

$C_{i,1} = G_i^{(\gamma_1+\gamma_5)\delta_i}, C_{i,2} = G_i^{(\gamma_2+\gamma_6)\delta_i}$,
$C_{i,3} = g^{((\gamma_1+\gamma_5)\sigma_1+(\gamma_2+\gamma_6)\sigma_2)\delta_i}$,
$C_{i,4} = u^{((\gamma_1+\gamma_5)\sigma_1+(\gamma_2+\gamma_6)\sigma_2)\delta_i} F_i^{\eta_i} u^s$,
$C_{i,5} = v^{((\gamma_1+\gamma_5)\sigma_1+(\gamma_2+\gamma_6)\sigma_2)\delta_i}$,
$C_{i,6} = g^{\eta_i}, C_{i,7} = M \cdot E_i^{((\gamma_1+\gamma_5)\sigma_1+(\gamma_2+\gamma_6)\sigma_2)\delta_i}$.

For each column $j \in [m]$, the algorithm creates column ciphertexts $(C_{j,1}, C_{j,2})$:

- if $(j < y) \wedge (j \in \mathrm{RL}_{j'})$:

$C_{j,1} = B_j^{\sigma_1} g^{\gamma_4\mu_j} g^{\gamma_2\mu_j}, C_{j,2} = B_j^{\sigma_2} g^{-\gamma_3\mu_j} g^{-\gamma_1\mu_j}$.

- if $(j < y) \wedge (j \notin \mathrm{RL}_{j'})$:

$C_{j,1} = B_j^{\sigma_1} g^{\gamma_4\mu_j}, C_{j,2} = B_j^{\sigma_2} g^{-\gamma_3\mu_j}$.

- if $(j \geqslant y) \wedge (j \in \mathrm{RL}_{j'})$:

$C_{j,1} = B_j^{\sigma_1} g^{\gamma_2\mu_j}, C_{j,2} = B_j^{\sigma_2} g^{-\gamma_1\mu_j}$.

- if $(j \geqslant y) \wedge (j \notin \mathrm{RL}_{j'})$:

$C_{j,1} = B_j^{\sigma_1}, C_{j,2} = B_j^{\sigma_2}$.

For each $k \in [l]$, it sets policy ciphertexts (D_k, D'_k): $D_k = u^{A_k \cdot \vartheta} H_{\rho(k)}^{-\theta_k}, D'_k = g^{\theta_k}$.

It outputs ciphertext $\mathrm{ct} = \langle \{C_{i,1}, C_{i,2}, C_{i,3}, C_{i,4}, C_{i,5}, C_{i,6}, C_{i,7}\}_{i\in[m]}, \{C_{j,1}, C_{j,2}\}_{j\in[m]}, \{D_k, D'_k\}_{k\in[l]}, (A, \rho)\rangle$.

(4) $\mathtt{Decrypt}_E(\mathrm{pp}, \mathrm{sk}_{(i,j),S}, \mathrm{ct}) \to M$ or $\perp$: For a secret key corresponding to an authorized set S, the algorithm first computes constants $\omega_k \in \mathbb{Z}_N$ such that $\sum_{\rho(k)\in S} \omega_k A_k = (1, 0, \ldots, 0)$. It then computes

$$P_1 = \frac{e(C_{i,1}, C_{j,1}) e(C_{i,2}, C_{j,2}) e(K''_{i,j}, C_{i,4}) e(K'_{i,j}, C_{i,5})}{e(K_{i,j}, C_{i,3}) e(K'''_{i,j}, C_{i,6})},$$

$$P_2 = \prod_{\rho(k)\in S} (e(D_k, K''_{i,j}) e(D'_k, K_{i,j,\rho(k)}))^{\omega_k} = e(g, u)^{st_{i,j}}.$$

The algorithm then computes and outputs $\bar{M} = \frac{P_1 \cdot C_{i,7}}{P_2}$. Note that it can be verified that only when $((i > x)$ or $(i = x) \wedge (j \geqslant y)) \wedge ((i, j) \in [m, m] \backslash \mathrm{RL})$, $\bar{M} = M$ will hold, where (x, y) is the encryption index and M is the encrypted message.

We refer the interested reader to the supplementary file for the formal definitions of assumptions and security games ($\mathrm{Game}_{\mathrm{MH}_1}$, $\mathrm{Game}_{\mathrm{MH}_{\mathcal{N}+1}}$ and $\mathrm{Game}_{\mathrm{IH}}$) used in the following theorems.

(1) Message-hiding security.

Theorem 1. If Assumption 1, the general subgroup decision assumption, the 3-party Diffie-Hellman assumption in a subgroup, and the source group q-parallel BDHE assumption in a subgroup hold, no polynomial time adversary can achieve a non-negligible advantage in winning $\mathrm{Game}_{\mathrm{MH}_1}$.

Theorem 2. No polynomial-time adversary can achieve a non-negligible advantage in winning $\mathrm{Game}_{\mathrm{MH}_{\mathcal{N}+1}}$.

(2) Index-hiding security.

Theorem 3. If the 3-party Diffie-Hellman assumption and the XDH assumption in a subgroup hold, no polynomial-time adversary can achieve a non-negligible advantage in winning $\mathrm{Game}_{\mathrm{IH}}$.

Theorem 4. If the construction presented above is message-hiding and index-hiding secure against key-like decryption black-box, it can be transformed to a black-box traceable and revocable CP-ABE against key-like decryption black-box.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Grant Nos. 61371083, 61373154, 61411146001, 61402282), Prioritized Development Projects of the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130073130004) and Shanghai Yang-Fan Plan (Grant No. 14YF1410400).

Supporting information The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Liu Z, Cao Z F, Wong D C S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures. IEEE Trans Inf Foren Secur, 2013, 8: 76–88
2 Ning J T, Cao Z F, Dong X L, et al. Large universe ciphertext-policy attribute-based encryption with white-box traceability. In: Computer Security-ESORICS 2014. Berlin: Springer, 2014. 55–72
3 Ning J T, Dong X L, Cao Z F, et al. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Computer Security–ESORICS 2015. Berlin: Springer, 2015. 270–289
4 Ning J T, Dong X L, Cao Z F, et al. White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans Inf Foren Secur, 2015, 10: 1274–1288
5 Liu Z, Cao Z F, Wong D C S. Traceable cp-abe: how to trace decryption devices found in the wild. IEEE Trans Inf Foren Secur, 2015, 10: 55–68
6 Liu Z, Cao Z F, Wong D C S. Blackbox traceable cp-abe: how to catch people leaking their keys by selling decryption devices on ebay. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013. 475–486
7 Garg S, Kumarasubramanian A, Sahai A, et al. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 121–130