Information Processing Letters 116 (2016) 492–495

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Cryptanalysis of a CP-ABE scheme with policy in normal forms

Syh-Yuan Tan [a,*], Wun-She Yap [b]

[a] FIST, Multimedia University, Melaka, Malaysia
[b] LKCFES, Universiti Tunku Abdul Rahman, Sungai Long, Malaysia

ARTICLE INFO

Article history:
Received 26 September 2015
Received in revised form 22 January 2016
Accepted 22 February 2016
Available online 2 March 2016
Communicated by S.M. Yiu

Keywords:
Cryptography
Analysis of algorithms
Safety/security in digital systems
Interconnection networks

ABSTRACT

In 2013, Rao and Dutta constructed an efficient attribute based access control mechanism for vehicular ad hoc network (VANET) based on a newly proposed ciphertext-policy attribute-based encryption (CP-ABE) scheme. As the CP-ABE scheme views access policy in normal forms, the length of ciphertext is independent against the number of attributes in the policy besides having constant number of pairing operations for both encryption and decryption functions. In this paper, we cryptanalyze Rao and Dutta's CP-ABE scheme by mounting a chosen plaintext attack to demonstrate that a registered node in VANET can (eavesdrop the conversation to) decrypt a ciphertext with unsatisfied disjunctive normal form policy. Since the security of Rao and Dutta's proposed attribute based access control mechanism for VANET relies on the proposed CP-ABE scheme, our attack indicates that the proposed access control mechanism is insecure. Subsequently, the root cause of the attack and possible solutions are presented to serve as important remarks in designing a secure CP-ABE scheme.

1. Introduction

Sahai and Waters [16] were the first to introduce the concept of attribute-based encryption (ABE) before it was formalized by Goyal et al. [10] into key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). KP-ABE has an access policy attached to the user secret key, while CP-ABE has an access policy attached to the ciphertext. CP-ABE gains more focus than KP-ABE because it can provide finer flexibility and controlling during the creation of a ciphertext. The core engine of ABE is the linear secret sharing scheme (LSSS) which can be extended into an access tree (or the policy). In brief, LSSS splits a secret random value $s \in \mathbb{Z}_p$ into n elements where $\mathbb{Z}_p$ is a finite field with prime modulus p. A user can set a threshold t such that s can be reconstructed if t out of n elements are presented. When $t = 1$, LSSS resembles a disjunction (i.e., OR logical function); when $t = n$, LSSS resembles a conjunction (i.e., AND logical function) and the combination of these two can be used to construct an access tree.

Despite the flexibility LSSS brings to KP-ABE and CP-ABE, the computation complexity and ciphertext size increased significantly. Some works [11,9,1,6] proposed to limit the access tree to only one layer and view the access policy as a threshold gate. Another approach [7,13, 12,14,8,18] is to represent an access tree in disjunctive normal form (DNF) and conjunctive normal form (CNF) to reduce the computation complexity. In short, one can view DNF and CNF as a simplified version of access tree, where by only the elements needed to satisfy the access tree are listed while the redundant hierarchical information of the elements are discarded. For instance, an access tree OR(AND (a, OR(d, AND(c, e)), AND(b, e))) can be simplified into the combination of CNF and DNF as {a, d} OR {a, c, e} OR {b, e} by removing the hierarchical information. In the worse case scenario where each CNF set under the DNF contains only one attribute, the ciphertext size is the

* Corresponding author.
E-mail addresses: sytan@mmu.edu.my (S.-Y. Tan), yapws@utar.edu.my (W.-S. Yap).

http://dx.doi.org/10.1016/j.ipl.2016.02.006
0020-0190/

Table 1
Differences on access policy formats.

Properties	Tree	CNF	DNF	CNF+DNF
Hierarchy	✓	×	×	×
AND	✓	✓	×	✓
OR	✓	×	✓	✓
Threshold	✓	×	×	✓
Ciphertext Size	n	1	$\leq n$	$\leq n$

same as that of the tree structure. The differences among these access policy formats are shown in Table 1.

In 2013, inspired by [13], Rao and Dutta proposed an efficient CP-ABE [15] which supports DNF policy for applications in VANET. Their work utilized a Certificate Authority (CA) to assign random pseudonyms to the vehicle's On-Board Unit (OBU) and take into consideration the existence of the Road Side Units (RSUs). The proposed CP-ABE scheme can achieve constant ciphertext size and only two pairing operations are needed for decryption. The authors claimed the security of their proposed scheme under generic group model and showed that their scheme is secure against corrupted RSUs besides withstanding the user collusion attack.

1.1. Contribution

In this paper, we falsify the security claim of Rao and Dutta's CP-ABE [15] scheme by mounting a chosen plaintext attack to break its one-way encryption property, in which anyone in the system either RSU or OBU can eavesdrop conversation between other parties and decrypt a ciphertext alone without satisfying the DNF policy set by encryptor. More precisely, we demonstrate the OWE-CPA attack where an (insider) attacker can manipulate a ciphertext with unsatisfiable DNF policy into one with satisfiable DNF policy. However, we note that Rao and Dutta's CP-ABE scheme is secure if the ciphertext policy is limited to CNF only, as done in some of the CP-ABE schemes [7,8,18] with constant ciphertext size. For the ease of understanding, we describe Rao and Dutta's scheme and the attack in the context of conventional CP-ABE without using the jargon in VANET throughout the paper.

1.2. Organization

The rest of the paper is organized as follows. In Section 2, we present the preliminaries of CP-ABE and access policy, followed by the description of Rao and Dutta's CP-ABE scheme in Section 3. We then present the cryptanalysis of Rao and Dutta's CP-ABE scheme in Section 4. In Section 5, we discuss the root cause of the attack and suggest a solution. Finally, we conclude the paper in Section 6.

2. Preliminaries

2.1. Access structure

We adopt the definition of access structure from [3] as follows.

Definition 1. Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}}$ is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$ then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P_1, P_2, \ldots, P_n\}} \setminus \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets and the sets not in $\mathbb{A}$ are called the unauthorized sets.

In the context of CP-ABE, the role of the parties is taken by the attributes. Thus, the access structure $\mathbb{A}$ will contain the authorized sets of attributes.

2.1.1. Normal form policy

Definition 2. A normal form policy is the compressed version of an access structure $\mathcal{T}$ with the corresponding attribute set S. The compression eliminates the hierarchical structure as well as transforms the OR gate into disjunctive normal form (DNF) and the AND gate into conjunctive normal form (CNF). The expression in DNF is written as $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} w_{i,j}$ while the expression in CNF is written as $\bigwedge_{i=1}^{n} \bigvee_{j=1}^{m} w_{i,j}$ where $w_{i,j} \in S$.

2.2. Security model

We briefly describe the security against indistinguishability under chosen plaintext (IND-CPA) attack as follows. IND-CPA attack environment is setup by a challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ is given access to the key extraction oracle $\mathcal{O}_k$.

Setup. $\mathcal{C}$ runs the setup algorithm of CP-ABE and gives the master public key to $\mathcal{A}$.

Phase 1. $\mathcal{A}$ can query $\mathcal{O}_k$ for user private keys corresponding to the sets of attributes $S_1, \ldots, S_n$.

Challenge. $\mathcal{A}$ submits two equal length messages M_0, M_1 together with an access structure $\mathbb{A}^*$ to $\mathcal{C}$, such that none of the sets $S_1, \ldots, S_2$ queried previously satisfy $\mathbb{A}^*$. $\mathcal{C}$ encrypts M_b under $\mathbb{A}^*$ for a random bit $b \in \{0, 1\}$. The ciphertext CT* is returned to $\mathcal{A}$.

Phase 2. Phase 1 is repeated with the restriction that the sets of attributes $S_{n+1}, \ldots, S_q$ in the new queries cannot satisfy $\mathbb{A}^*$.

Guess. $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins if $b' = b$.

In the security game of one-way encryption under chosen plaintext attack (OWE-CPA), $\mathcal{A}$ will be given a ciphertext CT* during Challenge phase. $\mathcal{A}$ wins if it can recover the plaintext M^* correctly during Guess phase such that $M^* = \mathbf{Dec}(\text{CT}^*)$.

3. The Rao and Dutta's CP-ABE scheme

For ease of understanding, we describe the Rao and Dutta's CP-ABE [15] scheme in the context of conventional CP-ABE scheme where the specific terms used for VANET will be ignored here. Generally, Rao and Dutta's CP-ABE scheme consists of four fundamental algorithms: Setup, Encrypt, KeyGen and Decrypt as follows:

Setup. The CA works as follows:

- Chooses a prime number p, a bilinear group $\mathbb{G}$, a generator $g \in \mathbb{G}$ and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ where $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative groups of same prime order p.
- Selects a random point $Q \in \mathbb{G}$ and a random exponent $y \in \mathbb{Z}_p$.
- Computes g^y and $Y = e(g, g)^y$.
- Defines the universe of static attributes S.
- Selects a random key K.
- For each static attribute $s \in S$, chooses a random exponent $t_s \in \mathbb{Z}_p$ and computes $P_s = g^{t_s}$.
- Return the public parameters $params = (p, \mathbb{G}, \mathbb{G}_T, e, g, Q, Y, \{P_s : s \in S\})$ and the master secret key $mk = y, K, \{t_s : s \in S\}$.

KeyGen(mk, S). The CA equipped with mk takes as input a set of attributes S and output a key that identifies with that set as follows:

- For a node i with an identity ID_i, computes $SK_{ID_i} = g^y \cdot Q^{H_K(ID_i)}$ where $H_K(\cdot) : \{0, 1\} \to \mathbb{Z}_p$ is a keyed hash function. At the same time, $PK_{ID_i} = g^{H_K(ID_i)}$ is made public.
- For a node i with an identity ID_i and a set of attributes S_i, computes a set of secret attribute-keys $\{\text{AttrSK}_{s,ID_i} = g^{t_s \cdot H_K(ID_i)} : s \in S_i\}$.

Both SK_{ID_i} and $\{\text{AttrSK}_{s,ID_i}\}$ are returned to the node i.

Encrypt(params, M, W). Given the access policy in DNF is W and a message M, the encryption algorithm works as follows:

- Note that $W = \bigvee_{l=1}^{k} (\bigwedge_{w \in W_l} w)$ where W_l denotes the set of attributes in the l-th conjunction of W for $1 \leq l \leq k$.
- Chooses a random exponent $r \in \mathbb{Z}_p$.
- Computes $C = M.Y^r$ and $C_0 = g^r$.
- For each $1 \leq l \leq k$, computes $C_l = (Q \cdot \Pi_{w \in W_l} P_w)^r$.
- Returns the ciphertext CT as $(W, C, C_0, \ldots, C_l)$.

Decrypt(params, CT). Suppose the attribute set A_{ID_i} of the node with ID_i satisfies the l-th conjunction of W, i.e., $W_l \subset A_{ID_i}$, then node with ID_i works as follows:

- Computes $K_l = SK_{ID_i} \cdot \Pi_{a \in W_l}(\text{AttrSK}_{ID_i})$.
- Recovers $M = C \cdot \dfrac{e(g^{H_K(ID_i)}, C_l)}{e(K_l, C_0)}$.

4. Cryptanalysis of Rao and Dutta's CP-ABE scheme

We now mount the chosen plaintext attack to break the OWE-CPA security of Rao and Dutta's CP-ABE scheme. To ease the explanation, we let a malicious user Bob who holds a valid set of secret attribute key to represent the adversary $\mathcal{A}$ which has access to the key extraction oracle $\mathcal{O}_k$.

- Let $S = \{a, b, c, d, e\}$, a police man Alex's car has attributes $\{a, c, e\}$, a resident Bob's car has attributes $\{b, c, d\}$.
- A patrol car encrypts a ciphertext C with the policy OR(AND(b, e), AND(a, OR(AND(c, e), d))). The policy can be represented in DNF as: $\{a, c, e\}$ OR $\{a, d\}$ OR $\{b, e\}$.
- The resulted ciphertext is $C = MY^r$, $C_0 = g^r$, $C_1 = (Q \prod_{w \in W_{a,c,e}} P_w)^r$, $C_2 = (Q \prod_{w \in W_{a,d}} P_w)^r$, $C_3 = (Q \prod_{w \in W_{b,e}} P_w)^r$.
- Alex can decrypt since he has AttrSK_a, AttrSK_c, AttrSK_e corresponding to the attributes $\{a, c, e\}$.
- Bob can't decrypt as he has only AttrSK_b, AttrSK_c, AttrSK_d but he can manipulate the ciphertext as follows:

$$\begin{aligned} C^* &= \frac{C_2 \cdot C_3}{C_1} \\ &= \frac{(Q \prod_{w \in W_{a,d}} P_w)^r (Q \prod_{w \in W_{b,e}} P_w)^r}{(Q \prod_{w \in W_{a,c,e}} P_w)^r} \\ &= (QP_b P_c^{-1} P_d)^r \end{aligned}$$

- Bob continues to compute K^*:

$$\begin{aligned} K^* &= SK_{ID_{Bob}} \cdot \text{AttrSK}_b \cdot \text{AttrSK}_c^{-1} \cdot \text{AttrSK}_d \\ &= g^y Q^{H_K(ID_{Bob})} \\ &\quad \cdot g^{t_b H_K(ID_{Bob})} g^{-t_c H_K(ID_{Bob})} g^{t_d H_K(ID_{Bob})} \end{aligned}$$

- Bob can recover M:

$$\begin{aligned} M &= \frac{C \cdot e(PK_{ID_{Bob}}, C^*)}{e(K^*, C_0)} \\ &= \frac{MY^r e(g^{H_K(ID_{Bob})}, (QP_b P_c^{-1} P_d)^r)}{e(g^y Q^{H_K(ID_{Bob})} \cdot g^{t_b H_K(ID_{Bob})} g^{-t_c H_K(ID_{Bob})} g^{t_d H_K(ID_{Bob})}, g^r)} \\ &= \frac{Me(g, g)^{yr} e(g^{H_K(ID_{Bob})}, (Q g^{t_b} g^{-t_c} g^{t_d})^r)}{e(g^y, g^r) e(Q^{H_K(ID_{Bob})} g^{t_b H_K(ID_{Bob})} g^{-t_c H_K(ID_{Bob})} g^{t_d H_K(ID_{Bob})}, g^r)} \\ &= \frac{Me(g, g)^{yr} e(g, Q g^{t_b - t_c + t_d})^{r H_K(ID_{Bob})}}{e(g, g)^{yr} e(Q g^{t_b - t_c + t_d}, g)^{r H_K(ID_{Bob})}} \\ &= M \end{aligned}$$

5. Discussion

One can view the chosen plaintext attack as a ciphertext collusion attack. This attack indicates that extra care is needed when we represent the ciphertext in DNF form as the hierarchical information which distinguishes the same attribute in different position of an access tree is now removed. To be exact, as long as the ciphertext structure in a CP-ABE scheme is the same as that of [15], the scheme can only support CNF policy such as [7,8,18].

A trivial fix for the problem is to randomize each ciphertext element using independent secret exponents. Referring the same example given in Section 4, the fixed ciphertext structure is:

$$C^{(1)} = MY^{r_1}, C^{(2)} = MY^{r_2}, C^{(3)} = MY^{r_3},$$
$$C_0^{(1)} = g^{r_1}, C_0^{(2)} = g^{r_1}, C_0^{(3)} = g^{r_3},$$
$$C_1 = (Q \prod_{w \in W_{a,c,e}} P_w)^{r_1}, C_2 = (Q \prod_{w \in W_{a,d}} P_w)^{r_2},$$
$$C_3 = (Q \prod_{w \in W_{b,e}} P_w)^{r_3}$$

which can be viewed as the multiple encryptions of M under the DNF policies each having a single conjunction. So, the original decryption algorithm can be used to decrypt any of the $C^{(i)}$. Notice that a DNF policy with a single conjunction is in fact a CNF policy and one can view the output of the fixed encryption as a bundle of M's ciphertexts under different CNF policies.

We do not provide the fixed Rao and Dutta's CP-ABE scheme using this solution as such construction is very similar to the authors' second remark [15] on the CP-ABE scheme which allows the encryption to pack messages $M_1, \ldots, M_n$ under a single ciphertext policy W where the messages may or may not be distinct. The difference is that all messages must be the same in the fixed Rao and Dutta's scheme. Besides, the solution also resembles to the schemes proposed in [13,12,14]. Anyway, we note that the trivial fix is not practical as it will increase the ciphertext size for n times where n is the number of repeated encryptions. Such ciphertext structure has significantly larger size compared to that of access tree policy as in [4,2,5,17] because the ciphertext elements C which contains M is also repeated for n times. For instance, if M is a MBytes GPS file, the ciphertext size of the trivially fixed Rao and Dutta's CP-ABE and [13,12,14] is of approximately n MBytes.

Therefore, Rao and Dutta's as well as other CP-ABE schemes [7,13,12,14,8,18] which view policy in normal forms are suitable for the scenario where the ciphertext policy only needs AND gates or CNF policy. If OR gates are needed in a policy, one have to use the CP-ABE schemes [4,2,5,17] which view policy as an access tree structure. In the case where only a threshold gate is needed, we may use the access tree structured CP-ABE schemes with single level or the schemes [11,9,1,6] which support threshold access structure. We leave the possibility of constructing an efficient CP-ABE which supports access tree structure with constant-size ciphertext as an open problem.

6. Conclusion

We cryptanalyzed Rao and Dutta's CP-ABE scheme and showed that it is not secure against one-way encryption under chosen plaintext attack. A fix is proposed by treating the DNF ciphertext as a bundle of CNF ciphertexts of the same plaintext. We suggest to use CP-ABE schemes with CNF policy when only AND gates are needed, and use CP-ABE schemes with access tree policy when OR gates are needed as well.

Acknowledgement

The authors would like to thank the Malaysia government's Fundamental Research Grant Scheme (FRGS/2/2014/ICT04/MMU/03/1) for supporting this work.

References

[1] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E.d. Panafieue, C. Ràfols, Attribute-based encryption schemes with constant-size ciphertexts, Theor. Comput. Sci. 422 (2012) 15–38.
[2] J. Baek, W. Susilo, J. Zhou, New constructions of fuzzy identity-based encryption, in: ACM-CCS '07, 2007, pp. 368–370.
[3] A. Beimel, Secure schemes for secret sharing and key distribution, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[4] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[5] L. Cheung, C. Newport, Provably secure ciphertext policy ABE, in: ACM-CCS '07, 2007, pp. 456–465.
[6] N. Doshi, D.C. Jinwala, Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption, J. Secur. Commun. Netw. 7 (11) (2014) 1988–2002.
[7] K. Emura, A. Miyaji, A. Nomura, K. Omote, M. Soshi, A ciphertext-policy attribute-based encryption scheme with constant ciphertext length, in: Information Security Practice and Experience, in: LNCS, vol. 5451, Springer-Verlag, 2009, pp. 13–23.
[8] K.G. Figueroa, S. Pancho-Festin, An access control framework for semi-trusted storage using attribute-based encryption with short ciphertext and mediated revocation, in: Second International Symposium on Computing and Networking '14, 2014, pp. 507–512.
[9] A. Ge, R. Zhang, C. Chen, C. Ma, Z. Zhang, Threshold ciphertext policy attribute-based encryption with constant size ciphertexts, in: ACISP '12, in: LNCS, vol. 7372, Springer-Verlag, 2012, pp. 336–349.
[10] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: ACM-CCS '06, 2006, pp. 89–98.
[11] J. Herranz, F. Laguillaumie, C. Ràfols, Constant size ciphertexts in threshold attribute-based encryption, in: PKC '10, in: LNCS, vol. 6056, Springer-Verlag, 2010, pp. 19–34.
[12] P. Junod, A. Karlov, An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies, in: ACM-DRM '10, 2010, pp. 13–24.
[13] S. Müller, S. Katzenbeisser, C. Eckert, Distributed attribute-based encryption, in: ICISC '08, in: LNCS, vol. 5461, Springer-Verlag, 2009, pp. 20–36.
[14] Y.S. Rao, R. Dutta, Computationally efficient secure access control for vehicular ad hoc networks, in: ICISS '12, in: LNCS, vol. 7671, Springer-Verlag, 2012, pp. 294–309.
[15] Y.S. Rao, R. Dutta, Efficient attribute based access control mechanism for vehicular ad hoc network, in: NSS '13, in: LNCS, vol. 7873, Springer-Verlag, 2013, pp. 26–39.
[16] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Advances in Cryptology — EUROCRYPT '05, in: LNCS, vol. 3494, Springer-Verlag, 2005, pp. 457–473.
[17] B. Waters, Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, Available from http://eprint.iacr.org/2008/290.pdf.
[18] Y. Zhang, D. Zheng, X. Chen, J. Li, H. Li, Attribute-based encryption with constant-size ciphertexts, in: ProvSec '14, in: LNCS, vol. 8782, Springer-Verlag, 2014, pp. 259–273.