COMMENTS

Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme

Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang

Abstract—In a decentralized attribute-based encryption (ABE) system, any party can act as an authority by creating a public key and issuing private keys to different users that reflect their attributes without any collaboration. Such an ABE scheme can eliminate the burden of heavy communication and collaborative computation in the setup phase of multiauthority ABE schemes, thus is considered more preferable. Recently in IEEE Transactions Parallel Distributed Systems, Han et al. [3] proposed an interesting privacy-preserving decentralized key-policy ABE scheme, which was claimed to achieve better privacy for users and to be provably secure in the standard model. However, after carefully revisiting the scheme, we conclude that their scheme cannot resist the collusion attacks, hence fails to meet the basic security definitions of the ABE system.

Index Terms—Cryptanalysis, attribute-based encryption, privacy, access control

1 Introduction

As attribute-based encryption (ABE) can simultaneously provide flexible access control and data confidentiality functionalities, it has become a promising technique for building secure access in practical distributed systems [5]. Very recently, Han et al. [3] proposed a decentralized key-policy ABE scheme in the standard model, based on which, they proposed a privacy-preserving key extraction protocol to protect the user's identifier. They also claimed that they solved the challenging open problem left by Chase and Chow [2] by constructing a privacy-preserving multi-authority ABE scheme without interactions among the authorities. However, after carefully analyzing their scheme, we have found that this scheme is vulnerable to the collusion attack, which is a basic security requirements for ABE systems.

Basically, Han et al. [3] tried to use a global identifier (GID) to bind a user's access ability at all authorities (that is why they use such an identifier in the key extraction at each authority). Furthermore, a user can decrypt a ciphertext only if his attributes simultaneously satisfy all the access structures at all the authorities (implicitly) involved in the ciphertext (also because of the GID). However, such a binding guaranteed by the GID seems too weak to prevent users' collusion. As we will show, two users with the same attribute sets S at some authorities can easily remove the GID and generate a new secret keys associated with S for any other GID. As a result, for N authorities system, if there are at most $2N$ users among those at least two users have all the attributes at each authority, then they can collude to generate a new secret keys with any identifier that it can be used to decrypt any ciphertext in the system. Therefore, the scheme in [3] has been totally broken.

2 Review of Han et al.'s ABE Scheme

We briefly review Han et al.'s ABE scheme [3] here:

- *Global setup*. Let $\mathbb{G}$ and $\mathbb{G}_T$ be bilinear groups of prime order p, where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. Let g, h and h_1 be the generators of $\mathbb{G}$. Suppose there are N authorities $A_1, \ldots, A_N$ in the system. A_i monitors a set of attributes $\widetilde{A}_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,n_i}\}$ for $i = 1, 2, \ldots, N$. Let the universal set of attributes $\mathcal{U} = \cup_{i=1}^{N} \widetilde{A}_i$.
- *Authorities setup*. Each authority A_i selects random $\alpha_i, \beta_i \in \mathbb{Z}_p$, and sets $Y_i = e(g, g)^{\alpha_i}, Z_i = g^{\beta_i}$. For each attribute $a_{i,j} \in \widetilde{A}_i$, it randomly chooses $t_{i,j} \in \mathbb{Z}_p$, and computes $T_{i,j} = g^{t_{i,j}}$. The public keys and secret keys of A_i are $PK_i = \{Y_i, Z_i, T_{i,1}, \ldots, T_{i,n_i}\}$ and $SK_i = \{\alpha_i, \beta_i, t_{i,1}, \ldots, t_{i,n_i}\}$. Each authority A_i also specifies a (k_i, n_i)—threshold access structure $\mathbb{A}_i$ with $k_i \leq n_i$.
- *KeyGen*. Suppose that a user U has the global identifier $u \in \mathbb{Z}_p$ and a set of attributes A_U. To generate a key for U for the attribute $a_{i,j} \in \widetilde{A}_i$, A_i chooses $r_i \in \mathbb{Z}_p$ and a random $k_i - 1$ degree polynomial $p_i(x) \in \mathbb{Z}_p[x]$ with $p_i(0) = r_i$, and computes $D_i = g^{\alpha_i} h^{r_i} h_1^{u\beta_i}$,
$$D_{i,j} = h^{\frac{p_i(a_{i,j})}{t_{i,j}}},$$
for $a_{i,j} \in A_U^i$ with $A_U^i = A_U \cap \widetilde{A}_i$.
- *Encryption*. Taking as inputs a message $M \in \mathbb{G}_T$, the system parameters *params* and a set of attributes $A_C = \{A_C^1, A_C^2, \ldots, A_C^N\}$, the encrypter randomly chooses $s \in \mathbb{Z}_p$, and outputs the ciphertext as follows: $C_1 = M \cdot \prod_{i \in I_C} e(g, g)^{\alpha_i s}, C_2 = g^s, C_3 = \prod_{i \in I_C} g^{\beta_i s}$,$\{C_{i,j} = T_{i,j}^s\}_{a_{i,j} \in A_C}$, where $A_C^i = A_C \cap \widetilde{A}_i$, and I_C is the index set of the authority A_i such that $A_C^i \neq \{\emptyset\}$, for $i = 1, \ldots, N$.
- *Decryption*. To decrypt the ciphertext $C = (C_1, C_2, C_3, \{C_{i,j}\}_{a_{i,j} \in A_C})$, the user computes
$$E = \prod_{i \in I_C} e(D_i, C_2), V = e(C_3, h_1^u),$$
$$F_i = \prod_{a_{i,j} \in A_C^i} e(D_{i,j}, C_{i,j})^{\triangle_{a_{i,j}, A_C^i}(0)}$$
for each $i \in I_C$, and $M = C_1 V E^{-1} \prod_{i \in I_C} F_i$. Here, the Lagrange coefficient for i in S is $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} (x - j) \ / \ (i - j)$.

3 Security Analysis of Han et al.'s Scheme

Before presenting our concrete attack, we first give several useful observations on Han et al.'s scheme [3]. The first two observations show some properties of Han et al.'s scheme, and are useful for our

- *A. Ge is with the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou 450002, China.*
E-mail: geaijun2011@gmail.com.
- *J. Zhang and Z. Zhang are with the Laboratory of Trusted Computing and Information Assurance, Institute of Software, Chinese Academy of Sciences, 4# South Fourth Street, Zhong Guan Cun, Beijing 100190, China. E-mail: jiangzhang09@gmail.com, zfzhang@tca.iscas.ac.cn.*
- *R. Zhang is with the State Key Lab of Information Security (SKLOIS), Institute of Information Engineering (IIE), Chinese Academy of Sciences (CAS), 89# Minzhuang Street, Haidian District, Beijing 100093, China.*
E-mail: r-zhang@iie.ac.cn
- *C. Ma is with the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou, 450002, China, and the Institute of Information Engineering, Chinese Academy of Sciences.*
E-mail: chuanguima@sina.com.

Manuscript received 28 July 2012; revised 2 Nov. 2012; accepted 6 Nov. 2012; published online 28 Nov. 2012.
Recommended for acceptance by W. Lou.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2012-07-0681.
Digital Object Identifier no. 10.1109/TPDS.2012.328.

later attack. The last observation is basically from Shamir secret share scheme, which is a building block in Han et al.'s scheme, and it guarantees the correctness of our attack:

- *Observation 1.* Each authority A_i in Han et al.'s scheme specifies a (k_i, n_i)-threshold access structure $\mathbb{A}_i$, and all the authorities are only weakly connected by a global identifier $u \in \mathbb{Z}_p$ in the secret keys.
- *Observation 2.* A ciphertext C is actually associated with a set of authorities (determined by I_C). A user can decrypt the ciphertext C if and only if his attribute set simultaneously satisfies $\mathbb{A}_i$ for all $i \in I_C$. Moreover, such a "simultaneity" highly relies on the global identifier u which is used to generate the user's secret keys by all involved authorities.
- *Observation 3.* For two secret values r_1, r_2, if we use two polynomials $p_1(x)$, $p_2(x)$ with the same degree k to share r_1 and r_2 (i.e., $p_1(0) = r_1, p_2(0) = r_2$), and compute the secret shares on the same $n \geq k+1$ different point $X = \{x_1, \ldots, x_n\}$, then we finally obtain a share set $Y_j = \{y_{j,i} = p_j(x_i)\}_{i \in \{1,\ldots,n\}}$ for each r_j with $j \in \{1,2\}$. Then, it is not hard to see that for any constant a, b, the set $Y' = \{y'_i = ay_{1,i} + by_{2,i}\}_{i \in \{1,\ldots,n\}}$ is a valid share set for $ar_1 + br_2$ with the polynomial $p'(x) = ap_1(x) + bp_2(x)$.

Now, we give a generic attack on the scheme [3]. Our attack employs the above three observations, and breaks the weak ties between authorities. Our idea is to remove such a connection by changing the identifier associated with particular secret keys. Assume we have two different users U_1, U_2 with the identifier u_1 and u_2, respectively. In addition, we also assume both users U_1 and U_2 satisfy the (k_i, n_i)-threshold access structure with the same attribute set (namely $A^i_{U_1} = A^i_{U_2}$) at the authority A_i. We will show how to produce secret keys associated with attribute set $A^i_{\tilde{U}} = A^i_{U_1}$ for any unauthorized user $\tilde{U}$ with the identifier $\tilde{u}$. The secret keys issued by A_i associated with u_1 and u_2 are as follows:

$$D_i = g^{\alpha_i} h^{r_i} h_1^{u_1\beta_i}, D_{i,j} = h^{\frac{p_i(a_{i,j})}{t_{i,j}}}, for\ a_{i,j} \in A^i_{U_1},$$
$$D'_i = g^{\alpha_i} h^{r'_i} h_1^{u_2\beta_i}, D'_{i,j} = h^{\frac{p'_i(a_{i,j})}{t_{i,j}}}, for\ a_{i,j} \in A^i_{U_2}.$$

We first compute

$$D''_i = \left(\frac{D_i}{D'_i}\right)^{\frac{1}{u_1-u_2}} = h^{\frac{r_i-r'_i}{u_1-u_2}} h_1^{\beta_i} = h^{r''_i} h_1^{\beta_i},$$
$$D''_{i,j} = \left(\frac{D_{i,j}}{D'_{i,j}}\right)^{\frac{1}{u_1-u_2}} = h^{\frac{p_i(a_{i,j})-p'_i(a_{i,j})}{(u_1-u_2)t_{i,j}}} = h^{\frac{p''_i(a_{i,j})}{t_{i,j}}},$$

where $r''_i = \frac{r_i - r'_i}{u_1-u_2}$ and $p''_i(x) = \frac{p_i(x)-p'_i(x)}{u_1-u_2}$. Note that $p''_i(0) = r''_i$, and $\{p''_i(a_{i,j})\}_{a_{i,j} \in A^i_{U_1} = A^i_{U_2}}$ also consist of valid interpolation points of $p''_i(0)$ according to Observation 3. Now, we use D''_i and $D''_{i,j}$ to generate secret keys associated with attribute sets $A^i_{\tilde{U}} = A^i_{U_1} = A^i_{U_2}$ in respect to the authority A_i for any unauthorized user $\tilde{U}$ with the identifier $\tilde{u}$. Concretely,

$$\begin{aligned}\tilde{D}_i &= D_i \cdot (D''_i)^{\tilde{u}-u_1} = g^{\alpha_i} h^{r_i} h_1^{u_1\beta_i} \cdot h^{(\tilde{u}-u_1)r''_i} h_1^{(\tilde{u}-u_1)\beta_i}\\ &= g^{\alpha_i} h^{r_i+(\tilde{u}-u_1)r''_i} h_1^{\tilde{u}\beta_i} = g^{\alpha_i} h^{\tilde{r}_i} h_1^{\tilde{u}\beta_i},\end{aligned}$$
$$\begin{aligned}\tilde{D}''_{i,j} &= D_{i,j} \cdot (D''_{i,j})^{\tilde{u}-u_1} = h^{\frac{p_i(a_{i,j})}{t_{i,j}}} \cdot h^{\frac{(\tilde{u}-u_1)p''_i(a_{i,j})}{t_{i,j}}}\\ &= h^{\frac{\tilde{p}_i(a_{i,j})}{t_{i,j}}}, for\ a_{i,j} \in A^i_{\tilde{U}},\end{aligned}$$

where $\tilde{r}_i = r_i + (\tilde{u} - u_1)r''_i$ and $\tilde{p}_i(x) = p_i(x) + (\tilde{u} - u_1)p''_i(x)$. It is easy to check that $(\tilde{D}_i, \{\tilde{D}''_{i,j}\}_{a_{i,j} \in A^i_{\tilde{U}}})$ are valid secret keys for the user $\tilde{U}$ (the identifier $\tilde{u}$) with random $\tilde{r}_i$ and polynomial $\tilde{p}_i(x)$ for the attribute set $A^i_{\tilde{U}}$.

Thus, by using this new key, two authorized users U_1, U_2 at A_i with (k_i, n_i)-threshold access ability (but not authorized by A_j), and a user U_3 who is authorized to have (k_j, n_j)-threshold access ability at A_j (but not authorized by A_i) can collude to decrypt a ciphertext intended for users who simultaneously have (k_i, n_i)-threshold access ability at A_i and (k_j, n_j)-threshold access ability at A_j. This is very dangerous, because none of the users U_1, U_2, U_3 satisfies the requirements alone, which also shows our collusion attack can be launched successfully.

Moreover, at most $2N$ users are needed, among which there are at least two different users have all the attributes at each authority A_i (thus, we can transfer their access ability to any other unauthorized user, e.g., $\tilde{U}$), to create a super user $\tilde{U}$ such that it can decrypt all the ciphertexts in the system.

4 Conclusion

Recently, in IEEE Transactions Parallel Distributed Systems, Han et al. [3] proposed an interesting privacy-preserving decentralized key-policy ABE scheme, which was claimed to achieve better privacy for users and to be provably secure in the standard model. In this comment, we demonstrate that unfortunately, their scheme is vulnerable to collusion attacks. At present, it is still a challenging open problem to construct a decentralized privacy-preserving multiauthority ABE scheme in the standard model.

Acknowledgments

The authors would like to thank the editor and anonymous referees for valuable comments. This work was partially supported by the National Basic Research Program of China (No. 2013CB338003, 2012CB315804), National Natural Science Foundation of China (No. 61379150, 61100225, and No. 61170278), Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDA06010701), and the National High Technology Research and Development Program of China (No. 2011AA010803).

References

[1] M. Chase, "Multi-Authority Attribute Based Encryption," *Proc. Fourth Conf. Theory of Cryptography (TCC '07),* S. Vadhan, ed., pp. 515-534, Feb. 2007.

[2] M. Chase and S. Chow, "Improving Privacy and Security in Multi-Authority Attribute Based Encryption," *Proc. ACM Conf. Computer and Comm. Security (CCS '09),* E. Al-Shaer, S. Jha, and A. Keromytis, eds., pp. 121-130, Nov. 2009.

[3] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption ," *IEEE Trans. Parallel and Distributed Systems,* vol. 23, no. 11, pp. 2150-2162, Nov. 2012.

[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Proc. 24th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05),* R. Cramer, ed., pp. 457-473, May 2005.

[5] S. Yu, K. Ren, and W. Lou, "FDAC: Toward Fine-Grained Data Access Control in Wireless Sensor Networks," *IEEE Trans. Parallel and Distributed Systems,* vol. 22, no. 4, pp. 673-686, Apr. 2011.

Aijun Ge received the MS degree from Zhengzhou Information Science and Technology Institute, China, in 2010, and is currently working toward the PhD degree at Zhengzhou Information Science and Technology Institute. His research fields include attribute-based cryptography and digital signatures.

Jiang Zhang received the BE degree in information and computational science from Sun Yat-sen University, China, in 2009, and is currently working toward the PhD degree at the Institute of Software, Chinese Academy of Sciences. He is interested in public-key encryption, attribute-based encryption, and lattice-based cryptographic systems.

Rui Zhang received the BE degree in 1999 from Tsinghua University, and the MS and PhD degrees from the University of Tokyo in 2002 and 2005, respectively. From 2005 to 2006, he was a JSPS research fellow. From 2006 to 2010, he was a research scientist at National Institute of Advanced Industrial Science and Technology (AIST), Japan. Since 2011, he has been a research professor in Chinese Academy of Sciences (CAS). His research interest includes applied cryptography and information theory..

Chuangui Ma received the BE degree in mathematics in 1982 from Zhengzhou University of China, the MS degree in mathematics in 1985 from Liaocheng University of China, and the PhD degree in mathematics in 1998 from Zhejiang University of China. Since December 2002, he has been a professor with the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.

Zhenfeng Zhang received the PhD degree from Academy of mathematics and Systems Science, Chinese Academy of Sciences at 2001. He is currently a professor and the PhD supervisor at the Laboratory of Trusted Computing and Information Assurance, Institute of Software, Chinese Academy of Sciences. His research interests include cryptography and information security.