Analysis on Hu et al.'s Identity-based Broadcast Encryption

Xingwen Zhao and Fangguo Zhang
(Corresponding author: Fangguo Zhang)

School of Information Science and Technology, Sun Yat-Sen University
Guangdong Key Laboratory of Information Security Technology
No. 135, XinGang West Road, Guangzhou 510275, P.R. China (Email: isszhfg@mail.sysu.edu.cn)
(Received June 10, 2010; revised and accepted Aug. 16, 2010)

Abstract

Analysis is given on Hu et al.'s efficient identity-based broadcast encryption (IBBE) scheme published in Journal of Computers, Vol. 5, No. 3, March 2010. Two major flaws are described. One is that valid group members outside the receiver set can still decrypt the ciphertext, which contradicts the authors' definition for IBBE. The other is that, given a valid private key, it is easy to generate private keys for other people without interacting with Private Key Generator (PKG).

Keywords: Broadcast encryption, identity-based broadcast encryption, private key generator

1 Introduction

Broadcast encryption (BE) [2] provides a convenient method to distribute digital content to subscribers over an insecure broadcast channel so that only the qualified users can recover the data. Broadcast encryption is quite useful and enjoys many applications including pay-TV systems, distribution of copyrighted material, streaming audio/video, secure ad hoc routing [5] and many others.

An ID-based Encryption (IBE) [8] system is a public key system where the public key can be an arbitrary string such as an email address, IP address or telephone numbers, which will be used as a receiver's identities.

Hu et al. [4] proposed an efficient identity-based broadcast encryption (IBBE) scheme in the Journal of Computers, Vol. 5, No. 3, March 2010. They claim to achieve constant size public key, private key and ciphertext.

We make an analysis on Hu et al.'s scheme, and describe two major flaws in it. One is that valid group members outside the receiver set can still decrypt the ciphertext, which contradicts the authors' definition for IBBE scheme. The other is that, given a valid private key, it is easy to generate private keys for other people without interacting with Private Key Generator (PKG). That is to say, any member with valid private key can act as PKG to issue private keys to others, which contradicts IBE architecture and makes PKG obsolete. If a malicious user holds such ability, the system will be in danger.

2 Hu et al.'s Identity-based Broadcast Encryption

We first review Hu et al.'s identity-based broadcast encryption scheme [4] in brief.

Let $\mathcal{G}_1, \mathcal{G}_2$ be a bilinear group of prime order p. We also assume the K is an element in $\mathcal{G}_2$, where $K \in \mathcal{K}$ and $\mathcal{K}$ is the set of keys for the symmetric encryption scheme.

Setup(λ, m): Given the security parameter λ and a total number of possible receivers m, a bilinear map $e : \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ is constructed. Then a random generator $g \in \mathcal{G}_1$, two random elements $x, y \in Z_p^*$ is selected, and $X = g^x$ and $Y = g^y$ are computed. The public key PK and the master secret key MSK are defined as follows:

$$\begin{aligned} PK &= (g, X, Y), \\ MSK &= (x, y). \end{aligned}$$

Extract(MSK, ID_i): PKG creates a private key for the public key identity $ID_i \in Z_p^*$ with $MSK = (x, y)$:

1) pick a random element $r \in Z_p$, and and compute $R = g^{\frac{1}{(r+ID_i)\cdot y + x}}$,

2) output the private key $sk_{ID_i} = (r, R)$.

Encrypt(PK, $\mathcal{N}$, K): Assume the notation $\mathcal{N} = \{ID_j\}_{j=1}^n$ represents the set of the receivers, with $n \leq m$. To encrypt a symmetric key $K \in \mathcal{K}$, the broadcaster needs to randomly pick $s \in Z_p^*$, and computes the $Hdr = (A, B, C, D)$ using PK and s to encapsulate the

symmetric key K, where

$$\begin{aligned} A &= Y^{\prod_{j=1}^{n} ID_j \cdot s}, \\ B &= X^s, \\ C &= Y^s, \\ D &= e(g,g)^s \cdot K. \end{aligned}$$

Note that $e(g,g)$ can be pre-computed.

Decrypt(PK, $\mathcal{N}$, ID_i, sk_{ID_i}, Hdr): any receiver in the set $\mathcal{N} = \{ID_j\}_{j=1}^{n}$ with identity $ID_i \in \mathcal{N}$ and the private key $sk_{ID_i} = (r, R)$ should compute as follows:

$$\begin{aligned} K &= \frac{D}{e(A^{\frac{1}{\prod_{j=1, j\neq i}^{n} ID_j}} \cdot B \cdot C^r, R)} \\ &= \frac{D}{e(g^{y \cdot ID_i \cdot s} \cdot g^{x \cdot s} \cdot g^{y \cdot s \cdot r}, g^{\frac{1}{(r+ID_i)\cdot y + x}})} \\ &= \frac{e(g,g)^s \cdot K}{e(g,g)^s}. \end{aligned} \quad (1)$$

Then the symmetric key K is used for encrypting the data.

3 Analysis

In this section, we make an analysis on Hu et al.'s scheme, and describe two major flaws in it. The Encrypt algorithm in Hu et al.'s IBBE scheme aims to encrypt symmetric key K to the specified receiver set, but we show that any valid group members outside the receiver set can obtain the symmetric key K. In IBE architecture, PKG is the trusted party who controls the issuing of private keys to all the members. However, we show that any member with valid private key can act as PKG to issue private keys to others.

3.1 Decrypt Outside the Receiver Set

Suppose the receiver set is $\mathcal{N} = \{ID_j\}_{j=1}^{n}$, and a Hdr $= (A, B, C, D)$ is sent to $\mathcal{N}$ where

$$\begin{aligned} A &= Y^{\prod_{j=1}^{n} ID_j \cdot s}, \\ B &= X^s, \\ C &= Y^s, \\ D &= e(g,g)^s \cdot K, \end{aligned}$$

as described in Section 2. We can notice that, a valid user $ID_i \notin \mathcal{N}$, with private key $sk_{ID_i} = (r, R = g^{\frac{1}{(r+ID_i)\cdot y + x}})$, can decrypt the symmetric key K as follows.

$$\begin{aligned} \frac{D}{e(C^{(r+ID_i)} \cdot B, R)} &= \frac{e(g,g)^s \cdot K}{e(g^{s \cdot y \cdot (r+ID_i)} \cdot g^{s \cdot x}, g^{\frac{1}{(r+ID_i)\cdot y + x}})} \\ &= \frac{e(g,g)^s \cdot K}{e(g^{s((r+ID_i)\cdot y + x)}, g^{\frac{1}{(r+ID_i)\cdot y + x}})} \\ &= \frac{e(g,g)^s \cdot K}{e(g^s, g)} \\ &= K. \end{aligned} \quad (2)$$

User $ID_i \notin \mathcal{N}$ can fetch K with only (B, C, D) from the Hdr. It means that messages sent to receiver set $\mathcal{N}$ can be recovered by any other members in the system, so Hu et al.'s scheme is broken.

3.2 Extract Other Valid Keys Without PKG

Suppose there exists a valid user ID_i with private key $sk_{ID_i} = (r_i, R = g^{\frac{1}{(r_i+ID_i)\cdot y + x}})$. We show that user ID_i can generate private keys for others without interacting with PKG. When user ID_i wants to issue private key for user ID_j, user ID_i computes

$$r_j = r_i + ID_i - ID_j (\mathrm{mod} p).$$

Then $(r_j,\ R = g^{\frac{1}{(r_j+ID_j)\cdot y + x}})$ is the valid private key for ID_j. The validity is straightforward if we try it in Formulas (1) and (2), because it has the same structure as those keys generated by PKG. This flaw is also unacceptable, for the system will be in danger if a valid key is held by malicious person.

We notice that user ID_i fails when $r_i + ID_i = ID_j (\mathrm{mod} p)$, but the probability is negligible.

4 Conclusion

In this paper, we point out two flaws of Hu et al.'s identity-based broadcast encryption scheme [4]. The Encrypt algorithm in Hu et al.'s IBBE scheme aims to encrypt symmetric key K to specified receiver set, but we show that any valid group members outside the receiver set can obtain the symmetric key K. In IBE architecture, PKG is the trusted party who controls the issuing of private keys to all the members. However, we show that any member with valid private key can act as PKG to issue private keys to others.

For secure identity-based broadcast encryption schemes, we refer our readers to [1, 3, 6, 7].

References

[1] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," *Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 200-215, Malaysia, 2-6 Dec., 2007.

[2] A. Fiat and M. Naor, "Broadcast encryption," *Advances in Cryptology (CRYPTO'93)*, pp. 480-491, California, 22-26 Aug., 1993.

[3] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," *Advances in Cryptology (EUROCRYPT'2009)*, pp. 171-188, Cologne, Germany, 26-30 Apr., 2009.

[4] L. Hu, Z. Liu, and X. Cheng, "Efficient identity-based broadcast encryption without random oracles", *Journal of Computers*, vol. 5, no. 3, pp. 331-336, 2010.
[5] M. Ramkumar, "Broadcast authentication with preferred verifiers," *International Journal of Network Security*, vol. 4, no. 2, pp. 166-178, 2007.
[6] Y. Ren and D. Gu, "Fully CCA2 secure identity based broadcast encryption without random oracles", *Information Processing Letters*, vol. 109, no. 11, pp. 527-533, 2009.
[7] R. Sakai and J. Furukawa, "Identity-based broadcast encryption", *Technical Report*, Cryptology ePrint Archive, Report 2007/217. (http://eprint.iacr.org/2007/217).
[8] A. Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology (CRYPTO'84)*, pp. 47-53, California, 19-22 Aug., 1984.

Xingwen Zhao is a doctor candidate in the School of Information Science and Technology at Sun Yat-sen University in Guangzhou, China. He was born in 1977, Guangxi, China. He received the B.S degree and M.S. degree from School of Communication Engineering, Xidian University in 1999 and 2004. His main research interests include broadcast encryption, signatures and key management.

Fangguo Zhang is a professor in the School of Information Science and Technology, at Sun Yat-sen University in Guangzhou, China. He obtained his Ph.D. degree in Cryptography from School of Communication Engineering, Xidian University in 2001. His main research interests include elliptic curve cryptography, pairing-based cryptosystem and its applications.