SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

November 2018, Vol. 61 118101:1–118101:3
https://doi.org/10.1007/s11432-017-9287-6

Dual-mode broadcast encryption

Yan ZHU[1*], Ruyun YU[1], E CHEN[1] & Dijiang HUANG[2]

[1]*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing* 100083*, China;*
[2]*School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe* 85287*, USA*

Received 25 June 2017/Revised 4 September 2017/Accepted 27 October 2017/Published online 21 May 2018

Citation Zhu Y, Yu R Y, Chen E, et al. Dual-mode broadcast encryption. Sci China Inf Sci, 2018, 61(11): 118101, https://doi.org/10.1007/s11432-017-9287-6

Broadcast encryption (BE) is a technique to implement secure group-oriented communication. The concept of broadcast encryption was firstly introduced by Fiat and Naor [1]. In a BE system, a broadcaster firstly chooses a receiver set and encrypts messages, and then broadcasts the ciphertext to all the users in the system while only the users in the chosen set can decrypt the ciphertext.

Motivation. The existing broadcast encryption system can be divided into two categories:

• BE with designation mechanism. A small set of designated users in system can decrypt the ciphertext, called select-mode broadcast;

• BE with revocation mechanism. All but a small set of revoked users in system can decrypt the ciphertext, called cut-mode broadcast.

A large number of BE constructions have been proposed during the past two decades, and they support either designation mechanism or revocation mechanism. However, we find that the construction supporting dual modes, select-mode and cut-mode, is scarcely discussed in literature. Moreover, there seems to be no evidence that such two mechanisms cannot coexist in one cryptosystem. Hence, it remains a fascinating problem to achieve dual modes while keeping fewer construction discrepancy.

In this article, we call broadcast encryption supporting designation and revocation mechanisms as dual-mode broadcast encryption (DMBE). It is intuitively plausible that the advantage of DMBE is the decreasing of computational overheads on encryption and decryption. For example, the user group is $U = S \cup R$, where S and R denote the designated set and the revoked set, respectively. In a DMBE system, one can determine an optimized encryption mode according to the relationship between the authorized users S and the unauthorized users R in the system. Namely, the designation mechanism is more efficient if $|S| < |R|$; otherwise, the revocation mechanism is better.

Exactly, the mode choice is determined:

• Select-mode. A minority of users in U can decrypt the ciphertext, i.e., $|S| < \frac{|U|}{2}$;

• Cut-mode. A majority of users in U can decrypt the ciphertext, i.e., $|R| \leqslant \frac{|U|}{2}$.

According to this choice, the computational overhead can be optimized to $O(\min\{|S|, |R|\})$. However, in a single-mode BE system, the computational complexity of encryption and decryption is generally either $O(|S|)$ or $O(|R|)$. Therefore, the DMBE system has a considerable computational advantage to improve the performance of large-size group-oriented communication.

In this article, we put forward the concept of DMBE and present a new scheme of revocation-based broadcast encryption (RBBE). This scheme can be also combined with Boneh et al.'s scheme [2] over designation mechanism to achieve a complete DMBE system.

* Corresponding author (email: zhuyan@ustb.edu.cn)

Related work. There has already existed various researches for BE with respect to designation mechanism. The scheme proposed by Boneh et al. [2] in 2005 has been noted as one of the most significant works because they first presented a new method for achieving fully collusion resistant by using groups with bilinear maps. Moreover, both ciphertexts and private keys are of constant size (i.e., $O(1)$) for any subset of receivers, and the public key size is directly proportional to the total number of users in the system (i.e., $O(N)$, where N is the total number of users). In 2009, Gentry et al. [3] improved Boneh et al.'s BE scheme in the aspect of security and presented the first adaptively secure BE scheme with sublinear ciphertexts (i.e., $O(\sqrt{\lambda \cdot |S|})$, where λ is the security parameter and $|S|$ denotes the number of users in a designated set S).

Another important research direction about BE is to realize revocation mechanism. In 2000, Naor et al. [4] presented a public-key revocation scheme based on t-threshold secret sharing, such that it can remove up to t parties and is secure against a coalition of the t revoked users. The advantage of this scheme is constant-size private key, but the computational overheads of a new key, encryption, and decryption are linear in t (i.e., $O(t)$).

In 2007, Delerablée et al. [5] put forward two public-key revocation schemes which can permanently revoke any subgroup of users. Their schemes are provably resist full collusions of users under the (t, n)-GDDHE (general decisional Diffie-Hellman exponent) assumption without any dependency on random Oracles. Recently, Lai et al. [6] addressed the problem of removing target designated receivers from the ciphertext. They constructed an anonymous IBBE scheme with full anonymity, in which only the sender knows the receivers' identities and the revocation process does not reveal any information of the plaintext and receiver identity. However, their scheme is proved to be semantically secure in the random Oracle model.

Construction of RBBE. Our revocation-based BE scheme is constructed on the designation-based BE scheme proposed by Boneh et al. [2]. In our construction, the user group is defined as $U = \{1, 2, \ldots, n-1\}$, where $n \in \mathbb{N}$. The construction of RBBE is composed of four algorithms: Setup, KeyGen, Encrypt and Decrypt, which are described as follows.

Setup$(1^\kappa, U)$**.** Given the security parameter κ and the user group U, this algorithm firstly generates the bilinear map group system $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e(\cdot,\cdot))$. Secondly, it randomly chooses two elements μ, r in $\mathbb{Z}_p^*$, picks a generator g of $\mathbb{G}$, and chooses $h \in_R \mathbb{G}$. Thirdly, it computes $w = g^r \cdot h$. Finally, it computes g_i for $i = 1, 2, \ldots, n-1, n+1, \ldots, 2n$ as $g_i = g^{\mu^i}$. The master key is outputted as $\mathrm{MK} = (\mu, r, h)$ and the public key is $\mathrm{PK} = (g, w, \{g_i\}_{i=1, i\neq n}^{2n})$.

KeyGen$(\mathrm{PK}, \mathrm{MK}, i)$**.** For each user $i \in U$, this algorithm computes the corresponding secret key as $\mathrm{sk}_i = g_i^r \cdot \frac{h^{\mu^i}}{g_n}$.

Encrypt(PK, R)**.** Given the public key PK and the revoked set R, this algorithm randomly chooses $t \in \mathbb{Z}_p^*$. The ciphertext $C_R = (C_0, C_1)$ can be computed as follows:

$$\begin{cases} C_0 = g^t, \\ C_1 = (w/\prod_{j\in R} g_{n-j})^t. \end{cases} \tag{1}$$

And then, this algorithm sets the session key $\mathrm{ek} = e(g_n, g)^t$.

Decrypt$(\mathrm{PK}, R, C_R, i, \mathrm{sk}_i)$**.** On receiving the ciphertext C_R, with the knowledge of PK and the revoked set R, each user $i \notin R$ can use his secret key sk_i to recover the session key as follows:

$$\mathrm{ek}' = \frac{e(C_1, g_i)}{e(\mathrm{sk}_i/\prod_{j\in R} g_{n-j+i}, C_0)}. \tag{2}$$

It is easy to verify the correctness of our construction, i.e., for a given set $R \subseteq U$ of revoked users, the Decrypt algorithm works correctly for each user $i \notin R$ by using

$$\begin{aligned} \mathrm{ek}' &= \frac{e(C_1, g_i)}{e(\mathrm{sk}_i/\prod_{j\in R} g_{n-j+i}, C_0)} \\ &= \frac{e((w/\prod_{j\in R} g_{n-j})^t, g_i)}{e(g_i^r \cdot h^{\mu^i}/(g_n \cdot \prod_{j\in R} g_{n-j+i}), g^t)} \\ &= \frac{e(g^r \cdot h/\prod_{j\in R} g_{n-j}, g_i)^t}{e([g^r \cdot h/(g_{n-i} \cdot \prod_{j\in R} g_{n-j})]^{\mu^i}, g)^t} \\ &= e(g_{n-i}, g_i)^t = e(g_n, g)^t = \mathrm{ek}. \end{aligned} \tag{3}$$

• Security analysis. The security of our RBBE scheme is based on a complexity assumption called bilinear Diffie-Hellman exponent (BDHE) problem which is defined as follows.

Definition 1 (DBDHE problem)**.** Given a $(2n+1)$-tuple $(g, g^t, \{g^{\mu^i}\}_{i=1, i\neq n}^{2n}) \in \mathbb{G}^{2n+1}$ and a random element $W \xleftarrow{R} \mathbb{G}_T$ as input, output 1 if $W = e(g^{\mu^n}, g)^t$ and 0 otherwise.

The DBDHE assumption is defined as follows.

Definition 2 ((ϵ, n)-DBDHE assumption)**.** We say that the DBDHE assumption is (ϵ, n)-secure, if for all probabilistic polynomial-time algorithms $\mathcal{B}$, the advantage of solving the DBDHE problem is at most ϵ, i.e., $\mathrm{Adv}_{\mathrm{DBDHE}}^{\mathrm{IND}}(\mathcal{B}) < \epsilon$.

Table 1 Performance evaluation of the RBBE scheme[a)]

	Computational complexity	Communication/storage complexity
Setup	$(2n) \cdot E(\mathbb{G}) + 1 \cdot M(\mathbb{G})$	$(2n+1) \cdot l_{\mathbb{G}}$(PK), $2 \cdot l_{\mathbb{Z}_p^*} + 1 \cdot l_{\mathbb{G}}$(MK)
KeyGen	$\lvert U\rvert \cdot (3 \cdot E(\mathbb{G}) + 1 \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}))$ (for $\lvert U\rvert$ users)	$\lvert U\rvert \cdot l_{\mathbb{G}}$ (sk_i, for $\lvert U\rvert$ users)
Encrypt	$2 \cdot E(\mathbb{G}) + 1 \cdot E(\mathbb{G}_T) + (\lvert R\rvert - 1) \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}) + 1 \cdot B$	$2 \cdot l_{\mathbb{G}}$ (C_R)
Decrypt	$(\lvert R\rvert - 1) \cdot M(\mathbb{G}) + 1 \cdot D(\mathbb{G}) + 2 \cdot B + 1 \cdot D(\mathbb{G}_T)$	$1 \cdot l_{\mathbb{G}_T}$ (ek)

a) $E(\cdot)$, $M(\cdot)$ and $D(\cdot)$ denote the exponentiation operation, multiplication operation and division operation in cyclic group, respectively. B denotes the bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. $|U|$ and $|R|$ denote the number of users in set U and R, respectively. $l_{\mathbb{Z}_p^*}$, $l_{\mathbb{G}}$ and $l_{\mathbb{G}_T}$ denote the length of elements in $\mathbb{Z}_p^*$, $\mathbb{G}$ and $\mathbb{G}_T$, respectively.

Our RBBE scheme is semantically secure against chosen plaintext attack with full collusion, such that we have Theorem 1.

Theorem 1 (Semantic security)**.** Our RBBE scheme for group with $n-1$ users is (ϵ, n)-semantically secure against chosen plaintext attack with full collusion under the (ϵ, n)-DBDHE assumption, and the advantage of the adversary $\mathcal{A}$ is $\mathrm{Adv}^{\mathrm{IND}}_{\mathrm{RBBE}}(\mathcal{A}) < \epsilon$.

• Performance evaluation. The performance evaluation of our RBBE scheme is presented in Table 1. From Table 1, we can see that the computational overheads of Setup and KeyGen are directly proportional to the number of users in U, i.e., $|U|$. However, the storage overheads of each user's secret key and ciphertext are constant, just one group element and two group elements, respectively. The computational costs of Encrypt and Decrypt are directly proportional to the number of users in revoked set R, such that the smaller the size of the set R, the better the performance. Hence, our RBBE scheme is more efficient for the case that almost all users in group are authorized to decrypt the ciphertext.

Dual-mode broadcast encryption. According to complementarity between designation and revocation mechanisms, we have an attractive idea to present a new scheme, called DMBE, which is a mixture of Boneh et al.'s scheme and our RBBE scheme. With the help of such a mixture, the DMBE system supports dual modes: select-mode and cut-mode, where the Boneh et al.'s scheme is used to achieve select-mode while the cut-mode is realized by our RBBE scheme.

By integrating such two modes, the DMBE scheme can help us to improve the performance of secure group-oriented communication. For example, in an E-mail system there are usually two kinds of messages: one is the regular emails that are sent only to a few friends; another is the announcement emails (such as official document, bulletin, meeting announcement) used to broadcast messages to all users. Our DMBE scheme is directly applicable to such a practical scenario.

Conclusion and future work. We propose the concept of DMBE and its embodiment. Our study shows that it is feasible to construct a BE cryptosystem which supports designation and revocation mechanisms, simultaneously. However, considering that these two mechanisms are opposite (or complementary) in functionality, one must deal carefully with the security impact caused by integrating them into one cryptosystem. Therefore, we will give an efficient and provably secure DMBE scheme in future work.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61472032), NSFC-Genertec Joint Fund for Basic Research (Grant No. U1636104), and Joint Research Fund for Overseas Chinese Scholars and Scholars in Hong Kong and Macao (Grant No. 61628201).

References

1 Fiat A, Naor M. Broadcast encryption. In: Proceedings of the 13th Annual International Cryptology Conference, Santa Barbara, 1993. 480–491
2 Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Proceedings of the 25th Annual International Cryptology Conference, Santa Barbara, 2005. 258–275
3 Gentry C, Waters B. Adaptive security in broadcast encryption systems (with short ciphertexts). In: Proceedings of the 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques, Cologne, 2009. 171–188
4 Naor M, Pinkas B. Efficient trace and revoke schemes. In: Proceedings of the 4th International Conference on Financial Cryptography, Anguilla, 2000. 1–20
5 Delerablée C, Paillier P, Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: Proceedings of the 1st International Conference on Pairing-Based Cryptography, Tokyo, 2007. 39–59
6 Lai J C, Mu Y, Guo F C, et al. Anonymous identity-based broadcast encryption with revocation for file sharing. In: Proceedings of the 21st Australasian Conference on Information Security and Privacy, Melbourne, 2016. 223–239