Wireless Personal Communications (2020) 115:961–969
https://doi.org/10.1007/s11277-020-07606-6

Identity Based Broadcast Encryption Scheme with Shorter Decryption Keys for Open Networks

Pragya Mishra[1] · **Renuka**[1] · **Vandani Verma**[1]

Published online: 17 June 2020

Abstract
In Broadcast Encryption schemes, a sender can broadcast the encrypted message securely in a threatening network to a set of legitimate system users only. In IBE scheme any sender can encrypt the desired message using his/her identity without attaining the public key certificate. Here, we have presented an efficient ID-based broadcast encryption scheme (IBBE) for open networks. In this scheme, desired messages can be broadcasted to any subset of the users by any sender but only authorized receivers are capable in retrieving the encrypted messages. This scheme has shorter decryption keys in comparison with other primitive of IBBE scheme for open networks. Moreover, the proposed scheme intends to achieve the lower cost for computation as well as transmission in comparison to earlier existing IBBE schemes.

Keywords IBBE · Open networks · ABE · PKG · IBE · CBE

1 Introduction

This era is period of communication technology and internet. Everyone is now dependent on these technologies to accomplish their various day-to-day tasks like personal, official, financial etc. Increasing demand and daily use of these techniques requires security measures in tight and vigilant mode because it brings security breach issues by leakage of private information. To eliminate such risks, various cryptographic techniques were studied in past years. Broadcast encryption schemes were studied a lot in early years. Broadcast encryption scheme allows a user to broadcast the information in a secret manner to set of authorized users so that encrypted message may be only received by authorized uses. Fiat and Naor [1] was the first who established the concept of collusion-resistant broadcast encryption. Boneh et al. [2] constructed a

✉ Pragya Mishra
pragya.login@gmail.com

Renuka
renuka4293@gmail.com

Vandani Verma
vandaniverma@yahoo.com

[1] Amity Institute of Applied Sciences, Amity University Uttar Pradesh, Noida, India

collusion-resistant broadcast encryption scheme having short cipher texts and private keys. Broadcast encryption scheme with constant size ciphertexts or decryption keys which is fully collusion secure was proposed by Delerablée et al. [3]. Boneh et al. presented a Traitor-Tracing scheme with Short Ciphertexts and Private Keys which was fully Collusion Resistant. Their scheme [4] enhances the security features of public-key Broadcast Encryption schemes.

ID based encryption scheme was established by Shamir [5] in which public key of each user is an arbitrary string. However, Boneh and Franklin [6] proposed the first IBE scheme using Weil pairing. The first completely secure Identity Based Encryption in random oracle model was proposed by Gentry [7].

An Identity based broadcast encryption scheme is the well-accepted primitive which has been studied in early years. Sakai and Furukawa [8] and Delereblee [9] explored the IBE scheme with constant size cipher texts and private keys. The later scheme was based on Key Encapsulation Mechanism (KEM) for encryption of large messages using a short symmetric key and was more efficient. Lately, using an O(log n)-way multi-linear map for n users, Boneh et al. [10] proposed an IBBE scheme. Li and Yanli, constructed an efficient IBBE scheme without random oracle model. The scheme relies on the asymmetric decisional bilinear Diffie-Hellman Exponent (DBDHE) assumption [11]. Kim et al. [12] constructed an ID based Broadcast Encryption system for stateless receivers with constant size ciphertext in the standard model which is fully collusion-resistant and an adaptively secure. In addition, the size of the private keys and public key of the system both are linear in respect of the maximum number of receivers.

Wu et al. [13] proposed the primitive of Contributory Broadcast Encryption (CBE) scheme in which a common public encryption key is shared among group of users while each user owns a distinct decryption key. The building block of this CBE scheme was Aggregatable Broadcast Encryption (ABE) which was originally based on Aggregatable Signature based broadcast offered in [14]. Up to that time, aggregatability was mostly taken in consideration under the signature setting [15] and subjected to trim down the storage overhead and the signature verification time for huge numbers of signatures to be stored and verified.

The shortcoming of CBE scheme is that it doesn't support the system where users changes dynamically. In recent years many IBBE schemes were studied but a little attention was paid to recruit new system users in IBBE scheme. Li et al. [16] proposed an IBBE scheme with constant cipher text using KEM without multilinear maps to recruit new users. Their scheme was combination of IBE scheme and ABE scheme and was secure for open networks. Our scheme also support the system where users dynamically changes and have lower set up cost while maintaining security in open networks. Its more efficient than IBBE scheme in [16].

In this paper firstly we will discuss preliminaries which are the basis of our scheme. Then in next section, we will explain our proposed scheme. This section will include all the steps involved in this scheme. The next section will cover the scheme analysis of our scheme which includes cost analysis, performance analysis, security analysis and storage analysis of our scheme. This section also contains a table which flaunts our scheme performance over other existing scheme in terms of cost of transmission and computation for system setup, transmission cost and computation cost to add new user. In last, we will conclude our results under the title "Conclusion".

2 Preliminaries

2.1 Bilinear Maps

Let G be an additive cyclic group of order p and G′ be a multiplicative cyclic group of same order p, where p is a prime number. A bilinear mapping e:G×G→G′ holds the following properties:

Bilinearity: ∀u,v∈G, ∀a,b∈ Z, $e(u^a,v^b)=e(u,v)^{ab}$
Non-degeneracy: ∃ generator g ∈ G where (g, g) ≠ 1.
Computability: ∀u,v∈G, e(u,v) can be computed effectively.

2.2 Assumption for Computation

The basis of computational assumption of our scheme is Decision n-Bilinear Deffie-Hellman Exponent (n-BDHE) problem. For a given $g_i = g^{\alpha_i} \in G_1$ for $1 \le i, i \ne n+1 \le 2n$ where $\alpha \in Z_q$ is unknown and G_1 and G_2 are same as discussed above; to choose if $Z = e(g,h)^{n+1} \in G_2$ where Z is not known and chosen randomly from G_2. The assumption of Decision n-BDHE holds the belief that it is not possible to solve the Decision n-BDHE problem using any algorithm within polynomial-time.

3 Our Proposal

3.1 SD Para Gen (λ,n)

It takes security parameter λ and total no. of system users n as input, the PKG chooses two cyclic multiplicative group U and V with large prime of order p where a is generator of U. There is also an efficient bilinear map e:UXU → V. The PKG arbitrarily chooses master secret key $MSK = s' \in Zp*$ and computes $a_0 = a^{s'} \in U$. Then PKG chooses hash function $H : \{0,1\}* \rightarrow U$ and a symmetric-key encryption scheme $\varepsilon k(.)/Dk(.)$ where K is session key for encryption of the sending message. Now Private Key Generator (PKG) holds master secret key s' and publish the following tuple of parameters:

$$\Pi = \left\{p, U, V, e, a, a_0, H, \varepsilon_k(.)/\, D_k(.)\right\}$$

SD extract (s', ID_i): On using input s' and user N_i's identity $ID_i \in \{0,1\}*$, it computes $id_i = H(ID_i)$ and $k_i = id_i^{s'}$, where k_i is N_i's private key.

3.2 SD Setup (s′, Π, N)

On using input s', the system users $N = \left\{N_1, N_2 \ldots N_n\right\}$, the PKG computes the following actions:

1) Setting up of public broadcast encryption: For $0 \le i \le n$, randomly chooses $A_i \in U/\{i\}$, $r_i \in Z_p^* s.t.$ if $m_1 \ne m_2$ then $A_{m_1} \ne A_{m_2}$ and $r_{m_1} \ne r_{m_2}$ and computes $R_i = a^{-r_i}, B_i = e(A_i, a)$. It publishes the public broadcast encryption key as $K_{pub} = ((R_0, B_0) \ldots (R_n, B_n))$ and keep $K_{\text{sec}} = ((r_0, A_0) \ldots (r_n, A_n))$ secret.

2) Generating the decryption key of users: For $0 \le i \le n$, it computes decryption key for user N_i as $d_i = (\psi_{0,i}, \psi_{1,i} \ldots \psi_{n,i})$ where $\psi_{k,i} = null$ under the following restrictions:

a. $K = 2$ and $i = 1$
b. $K = i$ where $1 \le i \le n$
c. $K = 2i$ & $k = [(n+2) - ((2i+n) \bmod (n+1))]$ where $2 \le i \le \lceil n/2 \rceil$
d. $K = 2(n-i)$ & $k = 2i \bmod (n+1)$ where $\lceil n/2 \rceil < i \le n$

Here, $\lceil x \rceil$ denotes least integer not less than x.

3.3 SD Encrypt (Π, S, K_{pub}, m)

Message M can be broadcasted by any sender who knows the public broadcast encryption key K_{pub} to the receiver set S by following actions:

1. Set $\bar{S} = \{0 \ldots n\} \backslash S$ and choose q randomly from Z_p to get the session key $\xi = (\Pi_{i \in \bar{S}} B_i)^q$ p
2. It gives the ciphertext $C = (C_1, C_2, C_3)$ as output where $C_1 = a^q$, $C_2 = (\Pi_{i \in \bar{S}} R_i)^q)$, $C_3 = \varepsilon_{\xi}(M)$
3. Finally broadcast (S,C) to receivers.

3.4 SD Decrypt (Π, S, N_i, d_i, K_i, C)

Take $i \in S$. For decryption of the cipher text C with the use of decryption key d_i and private key K_i, user N_i can proceed as given below:

Computation of session key: $\xi = e(\Pi_{i \in \bar{R}} \psi_{j,i}, c_1) \cdot e(k_i, c_2)$
Decryption using session key: i.e. $M = D_{\xi}(c_3)$

The correctness of the IBBE-scheme can be confirmed as-

$$
\begin{aligned}
&= e(\Pi_{j \in \bar{s}} \psi_{j,i}, c_1) \cdot e(k_i, c_2) \\
&= e(\Pi_{j \in \bar{s}} \psi_{j,i}, a^q) \cdot e(k_i, (\Pi_{i \in \bar{s}} R_i)^q) \\
&= e(\Pi_{j \in \bar{s}} A_j H(ID_i)^{r_j \cdot s'}, a^q) \cdot e(H(ID_i)^{s'}, (\Pi_{i \in \bar{s}} a^{-r_i})^q) \\
&= e(\Pi_{j \in \bar{s}} A_j, a^q) \cdot e(\Pi_{j \in \bar{s}} H(ID_i)^{r_j \cdot s'}, a^q) e(H(ID_i)^{s'}, (\Pi_{i \in \bar{s}} a^{-r_i})^q) \\
&= e(\Pi_{j \in \bar{s}} A_j, a^q) \cdot e(H(ID_i)^{s' \Sigma_{j \in \bar{s}} r_j}, a^q) e(H(ID_i)^{s'}, a^{q[\Sigma_{i \in \bar{s}}(-r_i)]}) \\
&= e(\Pi_{j \in \bar{s}} A_j, a^q) \cdot e(H(ID_i, a)^{s' q \Sigma_{j \in \bar{s}} r_j}) e(H(ID_i, a)^{s' q \Sigma_{i \in \bar{s}}(-r_i)}) \\
&= e(\Pi_{j \in \bar{s}} A_j, a^q) \\
&= \Pi_{j \in \bar{s}} e(A_j, a)^q = (\Pi_{i \in \bar{S}} B_i)^q = \xi \\
&\text{Therefore, } D_{\xi}(C_{\xi}) = D_{\xi}(\varepsilon_{\xi}(M)) = M
\end{aligned}
$$

4 Scheme Analysis

4.1 Cost Analysis

The transmission cost and computation cost for the proposed scheme is $O((n-1)^2)$ which is $O(n^2)$ for the already mentioned IBBE Scheme.

This can be easily seen with the help of Table 1. All the system users in the proposed scheme can be accessed information delivered by the PKG. In Table 1, note that $1 \leq i \leq \lceil n/2 \rceil, \lceil n/2 \rceil < j \leq n$ and "a" represents the value $[n+2-((2i+n) \bmod (n+1))]$.The symbol "⇓" shows that the values below it constitute the key above it.

In Table 1, the value of each $\psi_{k,i}$ is null for:

(i) $k = i; 1 \leq i \leq n$
(ii) $k = 2 \& i = 1$
(iii) $k = 2i \& k = [(n+2) - ((2i+n) \bmod (n+1))]; 2 \leq i \leq \lceil n/2 \rceil$
(iv) $k = 2(n-i) \&\quad k = 2i \bmod (n+1); \lceil n/2 \rceil < i \leq n$

Otherwise, $\psi_{k,i} = A_k H(ID_i)^{r_k s'}; 0 \leq k \leq n, 1 \leq i \leq n$, where s′ denotes master secret key which is known to PKG only.

As for the transmission cost and computation cost, in the algorithm SD Setup(), the PKG computes all the values mentioned in Table 1. This Table 1 represents a matrix of order (n + 1, n) i.e. each column has n + 1 rows. In each column (except the first one) PKG have to compute n-2 value (i.e. 2nd onwards each column has 3 null values) and column first has only 2 null values (i.e. PKG have to compute n-1 values for the first column) whatever be the value of n. Hence the total no. of values which must be computed by PKG is $(n-1)^2$.We can attain lesser costs by employing some other trades-off.

Our scheme also renders advantage over performance for newcomers. Just as the IBBE scheme, PKG only wants to compute as well as publish the rows corresponding to

Table 1 Information published by the PKG

K_{Pub}	d_1	⋯	d_i	⋯	d_j	⋯	d_n
⇓	⇓	⋯	⇓	⋯	⇓	⋯	⇓
(R_0, B_0)	$\psi_{0,1}$	⋯	$\psi_{0,i}$	⋯	$\psi_{0,j}$	⋯	*null*
(R_1, B_1)	*null*	⋯	$\psi_{1,i}$	⋯	$\psi_{1,j}$	⋯	$\psi_{1,n}$
(R_2, B_2)	*null*	⋯	$\psi_{2,i}$	⋯	$\psi_{2,j}$	⋯	$\psi_{2,n}$
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
$(R_{2(n-j)}, B_{2(n-j)})$	$\psi_{2(n-j),1}$	⋯	$\psi_{2(n-j),i}$	⋯	*null*	⋯	$\psi_{2(n-j),n}$
⋮	⋮	⋱		⋱		⋱	⋮
(R_i, B_i)	$\psi_{i,1}$	⋯	*null*	⋯	$\psi_{i,j}$	⋯	$\psi_{i,n}$
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
$(R_{2j \bmod (n+1)}, B_{2j \bmod (n+1)})$	$\psi_{2j \bmod (n+1),1}$	⋯	$\psi_{2j \bmod (n+1),i}$	⋯	*null*	⋯	$\psi_{2j \bmod (n+1),n}$
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
(R_j, B_j)	$\psi_{j,1}$	⋯	$\psi_{j,i}$	⋯	*null*	⋯	$\psi_{j,n}$
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
(R_{2i}, B_{2i})	$\psi_{2i,1}$	⋯	*null*	⋯	$\psi_{2i,j}$	⋯	$\psi_{2i,n}$
⋮	⋮	⋱		⋱		⋱	⋮
(R_a, B_a)	$\psi_{a,1}$	⋯	*null*	⋯	$\psi_{a,j}$	⋯	$\psi_{a,n}$
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
$(R_{2n \bmod (n+1)}, B_{2n \bmod (n+1)})$	$\psi_{2n \bmod (n+1),1}$	⋯	$\psi_{2n \bmod (n+1),i}$	⋯	$\psi_{2n \bmod (n+1),j}$	⋯	*null*
⋮	⋮	⋱	⋮	⋱	⋮	⋱	⋮
(R_n, B_n)	$\psi_{n,1}$	⋯	$\psi_{n,i}$	⋯	$\psi_{n,j}$	⋯	*null*

(R_{n+1}, B_{n+1}) and the columns corresponding to d_{n+1}, where $R_{n+1}=a^{-r_{n+1}}, B_{n+1}=e(A_{n+1}, a)$. However, transmission cost as well as computation cost for employing a fresh user is O(n − 2), which serves O(n) in favour of the IBBE scheme.

4.2 Security Analysis

Since our scheme IBBE-SDK is an optimization (up to some extent) of IBBE scheme which is based on the ABE scheme. Therefore it has same security features as the ABE scheme, which relies on the Decision n-BDHE assumption.

4.3 Storage Analysis

In Table 1, K_{pub} consists of (n + 1) pairs and each pair has one element in U and another in V. To encrypt messages, a sender needs to store the column of K_{pub} and therefore the storage required for K_{pub} is $(n + 1) \cdot (l_U + l_V)$, where l_U, l_V denote the bit-length of element in U and V respectively. On the other hand, a receiver needs to hold (n + 1) components in U for decryption key in addition of one component in U for her/his private key.

4.4 Performance Analysis

For encryption of a message, user has to compute one symmetric encryption operation and two exponentiations in U.Therefore with the difference of only two elements in U, the final cipher-text almost depends on the cipher-text given by symmetric encryption scheme. For decryption, the computation cost is one symmetric decryption and about two bilinear pairing operations. Therefore, the online cost for our proposed scheme is also lower in comparison of the IBBE scheme [16].

5 Result

Table 2 shows the comparison among our scheme, the IBBE scheme [16] and the ABE scheme. To make clear the comparison among the schemes, values given in Table 2 are in form of their overall magnitude not as per their definite values.

Table 2 shows that our proposed scheme has equivalent performance as the IBBE scheme [16]. However the length of decryption keys in our SD-IBBE scheme is smaller than the length in IBBE scheme (as it consists n-2 tuples on an average, whereas in earlier IBBE scheme it consist n tuples) which will in turn affect storage, transmission and computation costs. Thus, (from Table 2) we can easily conclude that our proposed scheme covers a great lead over the IBBE scheme.

Table 2 Achievement of our scheme over the existing schemes

	Schemes		
	Ours	IBBE	ABE
Based on Identity	Yes	Yes	No
Provides open network security	Yes	Yes	No
Support new users recruitment	Yes	Yes	No
Cost of transmission for system setup	$o((n-1)^2)$	$O(n^2)$	$O(n)$
Cost of computation for system setup	$o((n-1)^2)$	$O(n^2)$	$O(n)$
Transmission cost to add new user	$O(n-2)$	$O(n)$	$O(n)$
Computation cost to add new user	$O(n-2)$	$O(n)$	$O(n)$

6 Conclusion

Our scheme is extension of IBBE scheme [16] in an efficient way which supports security for open networks using computation cost of O(n) for addition of new user. Our scheme has lesser length for decryption key i.e. n-2 tuples as compared to earlier IBBE scheme which is of n tuples. However, Our scheme's performance is comparatively effective if we go through the computation cost of a fresh user which is O(n-2), in addition of transmission cost and storage cost without any compromise with security concerns taken in IBBE scheme [16]. Our scheme serves lower cost for addition of new user when compared with other IBBE schemes.

References

1. Fiat, A., & Naor, M. (1993). Broadcast encryption. In *Proceedings of Crypto'93*, volume 773 of LNCS (pp 480–491). Springer.
2. Boneh, D., Gentry, C., & Waters, B. (2005). Collusion resistant Broadcast Encryption with short cipher texts and private keys. In *Proceedings of Crypto'05*, volume 3621 of LNCS (pp. 258–275).
3. Delerablée, C., Paillier, P., & Pointcheval, D. (2007). Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In *Pairing-based cryptography–pairing 2007* (pp. 39–59), Springer.
4. Boneh, D., Sahai, A., & Waters, B. (2006). Fully collusion resistant traitor tracing with short ciphertexts and private keys. In *EUROCRYPT 2006* (vol. 4004, pp. 573–592). Heidelberg: LNCS, Springer.
5. Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *Advances in cryptology* (pp. 47–53).
6. Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. *SIAM Journal on Computing, 32,* 586–615.
7. Gentry, C. (2006). Practical identity-based encryption without random oracles. In *Advances in Cryptology-EUROCRYPT 2006* (pp. 445–464). Springer.
8. Sakai, R., & Furukawa, J. (2007). Identity-based broadcast encryption. *IACR Cryptology ePrint Archive, 2007,* 217.
9. Delerablée, C. (2007). Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Advances in cryptology—ASIACRYPT 2007* (pp. 200–215). Springer.
10. Boneh, D., Waters, B., & Zhandry, M. (2014). Low overhead broadcast encryption from multilinear maps. In *Advances in cryptology—CRYPTO 2014* (pp. 206–223). Springer.
11. Li, X., & Yanli, R. (2014). Efficient anonymous identity-based broadcast encryption without random oracles. *International Journal of Digital Crime and Forensics (IJDCF), 6,* 40–51.

12. Kim, J., Susilo, W., Au, M. H., & Seberry, J. (2015). Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. *IEEE Transactions on Information Forensics and Security, 10,* 679–693.
13. Wu, Q., Qin, B., Zhang, L., Domingo-Ferrer, J. & Farras, O. (2011). Bridging broadcast encryption and group key agreement. In *Advances in cryptology–ASIACRYPT 2011* (pp. 143–160), Springer.
14. Wu, Q., Mu, Y., Susilo, W., Qinand, B., & Domingo-Ferrer, J. (2009). Asymmetric group key agreement. In *Advances in cryptology—EUROCRYPT 2009* (pp. 153–170). Springer.
15. Boneh, D., Gentry, C., Lynn, B., & Shacham, H. (2003). Aggregate and verifiably encrypted signatures from bilinear maps. In *EUROCRYPT 2003* (Vol. 2656, pp. 416–432). Heidelberg: LNCS, Springer.
16. Li, M. C., Xu, X., Zhuang, R., Guo, C., & Tan, X. (2015). Identity based broadcast encryption schemes for open networks. In *9th international conference on frontier of computer science & technology*. https://doi.org/10.1109/fcsc.2015.20.

Ms. Pragya Mishra has done Masters in Pure Mathematics. She is pursuing Ph.D. in Mathematical Cryptography from the Department of Mathematics, Amity Institute of Applied Sciences, Amity University, Noida. Ms. Mishra has published research papers related to encryption schemes and signature schemes.

Ms. Renuka has done M.Sc. Mathematics, Specialization in Algebra from Kurukshetra University Kurukshetra (India). Presently she is doing research in area of Cryptography.

Dr. Vandani Verma (M.Sc., M.Phil., Ph.D.) working as assistant professor in the Department of Mathematics, Amity Institute of Applied Sciences, Noida. She has 15 years of teaching experience of B.Tech., B.Sc., M.Sc. students. She has published several research papers in international and national journals and also guided the B.Sc., M.Sc., Ph.D. students for their research projects.