개선된 Identity 기반의 브로드캐스트 암호화 기법[1]

Improved Identity-Based Broadcast Encryption

김 기 탁*, 박 종 환, 이 동 훈
(Ki Tak Kim, Jong Hwan Park and Dong Hoon Lee)

Abstract : The primitive of Identity-Based Broadcast Encryption allows a sender to distribute session keys or messages for a dynamically changing set of receivers using the receiver's identity as a public key. We already know that the trade-off exists the efficiency between the public parameter size and the ciphertext size. So, if the ciphertext size is $O(1)$, then the public parameter size may be $O(n)$. Some of IBBE scheme take the public parameters as input in decryption phase. Thus, a decryption device (or client) has to store the public parameters or receive it. This means that a decryption device (or client) has to have the proper size storage. Recently, delerabl□e proposed an IBBE which have the $O(1)$ size ciphertexts and the $O(n)$ size public parameters. In this paper, we present an IBBE scheme. In our construction the ciphertext size and the public parameter size are sub-linear in the total number of receivers, and the private key size is constant.

Keywords: Identity-Based Cryptography, Broadcast Encryption

I. Introduction

Broadcast encryption allows a sender to securely distribute messages to a dynamically changing set of users over an insecure channel. Generally, broadcast encryption schemes are considered as a Key Encapsulation Mechanism (KEM) for a specified session key. In an Identity-Based Broadcast Encryption (IBBE) scheme, this is done in the identity-based setting [19,5], where a Key Generation Center (KGC) issues a private key for a user identity and public parameters for the IBBE scheme are shared with all users. When a sender wants to broadcast a message to certain set of receivers, he generates a ciphertext, called "header", with the public parameters and the identity set of receivers. A legitimate user who belongs to the set decrypts the header, and obtains a message encryption key which can be used to recover the original message. Since revoked users (i.e., illegitimate users) can collude, the IBBE schemes must be secure against any number of colluders. We refer to this requirement as "full collusion-security". A Public Key Broadcast Encryption (PKBE) scheme has a similar property to the IBBE scheme in a sense that anyone can encrypt a message to arbitrary set of receivers. In PKBE schemes [14,7,9,2], an individual user is assigned to one of linearly ordered numbers, say {1, …, n}, as an identity. To our knowledge, most of the PKBE schemes [7,9,2] have a performance of $O(\sqrt{n})$ ciphertext size and $O(\sqrt{n})$ private key size (or $O(n)$) ciphertext size and $O(1)$ private key size when the public key is transmitted together with ciphertext. Though the PKBE schemes [7,9,2] have advantages in applications where identities of users are linearly ordered, the schemes are not desirable in applications where user may select its own identity at will. To deal with an arbitrary selected identity, one can attempt to consider a large value of n, for example, $n = 2^{64}$ at system initialization. However, this value results in too much ciphertext and private key size. We can also (informally) see that IBBE schemes can be applied to the PKBE schemes, by replacing the identity set {ID_1, …, ID_n} with the ordered set {1, …, n}.

As a trivial solution of the IBBE scheme, one can easily consider multi-receiver IBE schemes by simply generating |S| different ciphertexts for a multi-receiver set $S \in \{ID_1,...,ID_n\}$. Until now, there are two practical IBE schemes [23,15] secure (and practical) without random oracles. First, for the Waters IBE [23] scheme the trivial IBBE construction still suffers from the exponential security degradation of the number of "target" identities. Second, for the Gentry IBE scheme [16] the resulting scheme has a tight security reduction, but the ciphertexts consist of |S| group elements in $\mathbb{G}$ plus 2|S| group elements in $\mathbb{G}_1$, where the group $\mathbb{G}$ and $\mathbb{G}_1$ are published by the KGC. Furthermore, using the Gentry's scheme the IBBE construction as the KEM is not possible. Although the trivial IBBE schemes with O(|S|) ciphertexts are derived from the existing IBE schemes, the resulting schemes are less attractive because they are not appropriate to use in environments with large number of receivers.

1. Our Contribution

In Asiacrypt 2007, Delerabl□e proposed the first IBBE with constant size ciphertext. However, this scheme takes the public parameters, which is a linear size of n, as input in decryption algorithm. We improve this fact. Our IBBE also takes the public parameters, which is a sub-linear size of n. This improvement give that the decryption devices does not need a large storage.

2. Organization

In section 2, we describe a formal definition of IBBE and bilinear pairing. In section 3, we propose an improved IBBE. Finally, in section 4, we conclude the paper.

II. Preliminaries

We briefly review the formal definition of Identity-Based Broadcast Encryption (IBBE) scheme and its security model. We also summarize the bilinear pairing.

1. Identity-Based Broadcast Encryption

[1] "This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-(C1090-0801-0025))

An IBBE scheme consists of the four algorithms: Setup, KeyGen, Encrypt, Decrypt.

Setup(1^k, n): takes as input a security parameter 1k and the number of users n. It outputs public parameters PP and secret master key msk.

KeyGen(msk, ID): takes as input the secret master key msk and an identity $\mathrm{ID} \in \mathrm{I\ D}$. It outputs a private key d_{ID} for ID.

Encrypt(S, PP): takes as input an identity set S and the public parameters PP. It outputs a pair (Hdr;K) where Hdr is called the header and $\mathrm{K} \in \mathrm{K}$ is a message encryption key. The broadcast to users in S consists of (S, Hdr, C_M), where C_M is an encrypted message under the K using a symmetric key cipher.

Decrypt(d_{ID}, S, Hdr, PP): takes as input the private key d_{ID} for ID, an identity set S, a header Hdr, and the public parameters PP. If ID $\in$ S, then the algorithm outputs the message encryption key $\mathrm{K} \in \mathrm{K}$, which is used to decrypt C_M and obtain the message M.

2. Bilinear Pairing

We briefly review the bilinear pairing.

Bilinear Pairing: We follow the notation in [5,3]. Let G and G_T be two (multiplicative) cyclic groups of prime order p. We assume that g is a generator of G . Let $e : \mathrm{G} \times \mathrm{G} \to \mathrm{G}_T$ be a function that has the following properties:

1. Bilinear: for all $u, v \in \mathrm{G}$ and $a, b \in \mathrm{Z}$, we have $e(u^a, v^b) = e(u,v)^{ab}$.

2. Non-degenerate: $e(g,g) \neq 1$.

3. Computable: there is an efficient algorithm to compute the map e.

Then, we say that G is a bilinear group and the map e is a bilinear pairing in G .

III. Improved Identity-Based Broadcast Encryption

In this section, we present our IBBE construction, which is motivated by the recent work of Delerabl□e [13]. Let G and G_T be groups of prime order p, and let $e : \mathrm{G} \times \mathrm{G} \to \mathrm{G}_T$ be the bilinear map. We often use h_0 to denote h.

1. Scheme

Setup(1^k, n, a, b): To generate IBBE parameters, the KGC picks two random generators $g, h \in \mathrm{G}$. It selects random $\alpha, \beta_1, \ldots, \beta_a \in \mathrm{Z}_p^*$, and $u_1, \ldots, u_a \in \mathrm{G}$. It sets $h_i = h^{\alpha^i} \in \mathrm{G}$ for $i = 1, \ldots, b$ and $v_j = u_j^{\beta_j} \in \mathrm{G}$ for $j = 1, \ldots, a$, and $w = g^\alpha, v = e(g,h)$. Choose a cryptographic hash function $\mathrm{H} : \{0,1\}^* \to \mathrm{Z}_p^*$. H constitutes a system public parameter. The public parameters PP (with the description of $(\mathrm{G}, \mathrm{G}_T, e, p)$) and the secret master key msk are given by

$$PP = (w, v, h, h_1, \ldots, h_b, u_1, \ldots, u_a, v_1, \ldots, v_a), \quad msk = (g, \alpha, \beta_1, \ldots, \beta_a) .$$

The security analysis will view H as a random oracle.

KeyGen(msk, ID): For a user $ID \in \mathrm{Z}_p^*$, if ID is a member of the i-th user set S_i , then the KGC outputs the private key

$$d_{ID} = (g^{1/(\alpha + \mathrm{H}(ID))}, g^{\beta_i/(\alpha + \mathrm{H}(ID))}) .$$

If $\mathrm{H}(ID)$ is an inverse element of α in Z_p^* , the KGC aborts.

Encrypt(S, PP): A sender chooses random $r \in \mathrm{Z}_p$ and sets $K = v^r \in \mathrm{G}_T$. Without loss of generality, assume the receiver set S is divided into subsets $S_1, \ldots, S_a$.

Let $F_{S_i}(x) = \prod_{ID \in S_i} (x + \mathrm{H}(ID)) \in \mathrm{Z}_p[x]$ for the recipient set S_i . A header (Hdr) is generated with the public parameters PP as follows:

$$Hdr = (w^{-r}, \left\{(v_i \square h^{F_{S_i}(\alpha)})^r\right\}_{i=1}^{a}, \left\{u_i^r\right\}_{i=1}^{a}) .$$

The algorithm outputs the pair (Hdr,K). Then, the sender broadcasts (S, Hdr,C_M), where C_M is an encrypted message under the K using a symmetric key cipher. Note that the values $F_{S_i}(\alpha)$ can be computed, using the public parameters PP, since we can always compute all coe_cients of $F_{S_i}(x)$.

Decrypt(d_{ID}, S, Hdr, PP): Assume a user with identity ID belongs to S_i for some $i \in \{1, \ldots, a\}$. The user ID decrypts the Hdr using his private key $d_{ID} = (d_{ID,0}, d_{ID,1})$, where $d_{ID,0} = g^{1/(\alpha + \mathrm{H}(ID))}$ and $d_{ID,1} = g^{\beta_i/(\alpha + \mathrm{H}(ID))}$. Let $Hdr = (A, B_1, \ldots, B_a, C_1, \ldots, C_a)$, and $F_{S_i\text{₩D}}(x) = \frac{1}{x}\left(\prod_{ID' \in S_i\text{₩}D} (x + \mathrm{H}(ID')) - \prod_{ID' \in S_i\text{₩}D} \mathrm{H}(ID')\right)$ for the recipient set S_i . Then, it outputs

$$K = \left(\frac{e(A, h^{F_{S_i\text{₩}D}(\alpha)}) \square e(d_{ID,0}, B_i)}{e(C_i, d_{ID,1})} \right)^{1/\prod_{ID' \in S_i\text{₩}D} \mathrm{H}(ID')} .$$

2. Correctness

We first show that the sender can compute the value $h^{F_{S_i}(\alpha)}$ for the receiver subset S_i. Let $F_{S_i}(x) = \prod_{ID \in S_i} (x + \mathrm{H}(ID))$ be expended as $F_{S_i}(x) = \sum_{j=1}^{|S_i|} c_j x^j$ for some $c_j \in \mathrm{Z}_p$ .. Note that $c_{|S_i|} = 1 \in \mathrm{Z}_p$. Then, $h^{F_{S_i}(\alpha)}$ can be computed as $\prod_{j=1}^{|S_i|} h_j^{c_j}$, where $h_0 = h$. Then, for random $r \in \mathrm{Z}_p$, we have that $B_i = (v_i \cdot h^{F_{S_i}(\alpha)})^r = (v_i \cdot h^{\prod_{ID \in S_i} (\alpha + \mathrm{H}(ID))})^r$.

Next, we verify that K is correctly derived from the well-formed Hdr. To easily show that, we use the following notations:

$$\mathrm{P}_{S_i,x}^1(ID) = \prod_{ID' \in S_i\text{₩}D} (x + \mathrm{H}(ID')) ,$$

$$\mathrm{P}_{S_i}^2(ID) = \prod_{ID' \in S_i\text{₩}D} \mathrm{H}(ID')$$

then,

$$F_{S_i}(x) / (x + \mathrm{H}(ID)) = \prod_{ID' \in S_i\text{₩}D} (x + \mathrm{H}(ID')) = \mathrm{P}_{S_i,x}^1(ID) .$$

As above, let $F_{S_i\text{₩}D}(x) = \frac{1}{x}\left(\sum_{j=1}^{|S_i|} e_j x^j - \prod_{ID' \in S_i \setminus ID} \mathrm{H}(ID')\right)$ for some $e_j \in \mathrm{Z}_p$. Note that $e_{S_i} = 1 \in \mathrm{Z}_p$. Assuming $ID \in S_i$, then user with identity ID decrypts as:

$$K = \left(\frac{e(A, h^{F_{S_i \setminus ID}(\alpha)}) \cdot e(d_{ID,0}, B_i)}{e(d_{ID,1}, C_i)} \right)^{1/\prod_{ID' \in S_i \setminus ID} \mathrm{H}(ID')}$$

$$=\left(\frac{e(g^{-r\alpha},h^{1/\alpha(\mathrm{P}^1_{S_i,x}(ID)-\mathrm{P}^2_{S_i}(ID))})\cdot e(g^{1/(\alpha+\mathrm{H}(ID))},u_i^{r\beta_i}\cdot h^{rF_{S_i}(\alpha)})}{e(g^{\beta_i/(\alpha+\mathrm{H}(ID))},u_i^z)}\right)^{1/\mathrm{P}^2_{S_i}(ID)}$$

$$=(e(g,h^{-r\mathrm{P}^1_{S_i,\alpha}(ID)+r\mathrm{P}^2_{S_i}(ID)})\cdot e(g,h^{r\mathrm{P}^1_{S_i,\alpha}(ID)}))^{1/\mathrm{P}^2_{S_i}(ID)}$$

$$=(e(g,h^{r\mathrm{P}^2_{S_i}(ID)}))^{1/\mathrm{P}^2_{S_i}(ID)}$$

$$=e(g,h)^r$$

as required.

IV. Conclusion

We introduced the improved identity-based broadcast encryption (IBBE) scheme with sub-linear size ciphertexts and constant size private keys.

참고문헌

[1] —. Abdalla, E. Kiltz, and G. Neven, "Generalized key delegation for hierarchical identity-based encryption." To appear in the proceedings of *Esorics'07*, Springer, 2007.

[2] N. Attrapadung, J. Furukawa, and H. Imai, "Forward-secure and searchable broadcast encryption with short ciphertexts and private keys.", In *Asiacrypt'06*, volume 4284 of *LNCS*, page 161-177, 2006.

[3] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles.", In *Eurocypt'04*, volume 3027 of *LNCS*, page 223-238, Springer, 2005.

[4] D. Boneh, X. Boyen, and E. Goh. "Hierarchical identity based encryption with constant size ciphertext.", In *Eurocrypt'05*, volume 3494, pages 440-456, Springer, 2005.

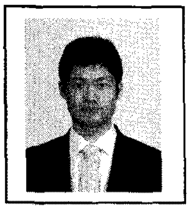
[5] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing.", In *Crypto'01*, volume 2139, of *LNCS*, pages 213-229. Springer, 2001.

[6] M. Barosa and P. Farshim. "Efficient identity-based key encapsulation to multiple parties. "In *IMA'05*, volume 3796 of *LNCS*, pages 428-441, Springer, 2005.

[7] D. Boneh, C. Gentry, and B. Waters. "Collusion resistant broadcast encryption with short ciphertexts and private keys", In *Crypto'05*, volume 3621 of *LNCS*, pages 258-275, Springer, 2005.

[8] J. Baek, R. Safavi-Naini, and W. Susilo. "Efficient multi-receiver identity-based encryption and its application to broadcast encryption." In *PKC'05*, volume 3386 of *LNCS*, pages 380-397, Springer, 2005.

[9] D. Boneh and B. Waters. "A collusion resistant broadcast, trace and revoke system.", In *ACM Conference on Computer and Communications Security – CCS'06*, pages 211-220. New-York: ACM Press, 2006.



김 기 탁

2006년 고려대학교 수학과 학사 졸업.
2006년~현재 고려대학교 정보경영공학 전문대학원 석사과정 재학중.
관심분야는 암호프로토콜, 암호이론.

이 동 훈

1983년 고려대학교 경제학과 학사 졸업.
1987년 Oklahoma Univ. 전산학과 석사 졸업.
1992년 Oklahoma Univ. 전산학과 박사 졸업.
1993년 고려대학교 전산학과 조교수
1997년 고려대학교 전산학과 부교수
2001년~현재 고려대학교 정보경영공학전문대학원 교수
관심분야는 암호프로토콜, 암호이론.

[10] C. Cocks. "An identity based encryption scheme based on quadratic residues.", In 8^{th} *IMA International Conference on Cryptography and Coding'01*, pages 26-28, 2001.

[11] S. Chatterjee and P. Sarkar. "Generalization of the selective-ID security model for HIBE protocols.", In *PKC'06*, volume 3958 of *LNCS*, pages 241-256, Springer, 2006.

[12] S. Chatterjee and P. Sarkar. "Multi-receiver identity-based encapsulation with shortened ciphertext.", In *Indocrypt'06*, volume 4329 of *LNCS*, pages 394-408, Springer, 2006.

[13] Cecile Delerablee. "Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys", In *Asiacrypt'07*, volume 4833 of *LNCS*, pages 200-215. Springer, 2007.

[14] Y. Dodis and N. Fazio. "Public key broadcast encryption secure against adaptive chosen ciphertext attack.", In *PKC'03*, volume 2567 of *LNCS*, pages 100-115. Springer, 2003.

[15] X. Du, Y. Wang, J. Ge, and Y. Wang. "An id-based broadcast encryption scheme for key distribution.", In *IEEE Transaction on Broadcasting*, volume 51, No. 2, pp.264-266. 2005.

[16] C. Gentry. Practical Identity-Based Encryption Without Random Oracles.", In *Eurocrypt'06*, volume 4004 of *LNCS*, pages 445-464. Springer, 2006.

[17] C. Gentry and A. Silverberg. "Hierarchical ID-based cryptography.", In *Asiacrypt'02*, volume 2501 of *LNCS*, pages 548-566. Springer, 2002.

[18] J. Horwitz and B. Lynn. "Toward hierarchical identity-based encryption.", In *Eurocrypt'02*, volume 2332 of *LNCS*, pages 466-481. Springer, 2002.

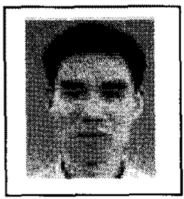
[19] A. Shamir. "Identity-based cryptosystems and signature schemes.", In *Crypto'84*, volume 196 of *LNCS*, pages 47-53. Springer, 1984.

[20] M. Scott. "Implementing cryptographic pairings.", In *Pairing'07*, volume 4575 of *LNCS*, pages 177-196. Springer, 2007.

[21] R. Sakai and J. Furukawa. "Identity-based Broadcast Encryption.", Cryptology ePrint Archive, Report 2007/217, 2007. http://eprint.iacr.org/2007/217.

[22] R. Sakai, K. Ohgishi, and M. Kasahara. "Cryptosystem based on pairing.", In SCIS'00, Okinawa, Japan, 2000.

[23] B. Waters. "Efficient identity-based encryption without random oracles.", In Eurocrypt'05, volume 3494 of LNCS, pages 114-127. Springer, 2005.



박 종 환

1997년 고려대학교 수학과 학사 졸업
2003년 고려대학교 정보보호대학원 석사 졸업.
2003년~현재 고려대학교 정보경영공학 전문대학원 박사과정 수료.
관심분야는 암호프로토콜, 암호이론.