International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

An Adaptively Secure Identity-Based Broadcast Encryption using CAST Algorithm

Asha Prasad G†* and Deepthy Mathews†

†Dept. of CSE Christ Knowledge City, Mannor, Ernakulam, India

Accepted 28 Nov 2015, Available online 03 Dec 2015, **Vol.5, No.6 (Dec 2015)**

Abstract

An adaptively secure identity-based broadcast encryption system featuring constant sized ciphertext is introduced. The size of public key and private keys of the system are both linear in the maximum number of receivers. The system is fully collusion-resistant and has stateless receivers. Here, in the system CAST algorithm is used for encryption of the broadcast message. The scheme is well optimized for broadcast encryption. The computational complexity of decryption depends only on the number of receivers and not on the maximum number of receivers of the system. A dual system encryption technique is used and adaptive security under general subgroup decisional assumption is proposed.

Keywords: *Broadcast, Encryption, Constant cipher text, Identity based broadcast encryption*

1. Introduction

In telecommunication and information theory, broadcasting refers to a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface, or it may be a low level networking operation, for example broadcasting on Ethernet.
Broadcast encryption is the cryptographic problem of delivering encrypted content (e.g. TV programs or data on DVDs) over a broadcast channel in such a way that only qualified users (e.g. subscribers who have paid their fees or DVD players conforming to a specification) can decrypt the content. The challenge arises from the requirement that the set of qualified users can change in each broadcast emission, and therefore revocation of individual users or user groups should be possible using broadcast transmissions, only, and without affecting any remaining users. As efficient revocation is the primary objective of broadcast encryption, solutions are also referred to as revocation schemes (A. B. Lewko *et al*, 2010). Rather than directly encrypting the content for qualified users, broadcast encryption schemes distribute keying information that allows qualified users to reconstruct the content encryption key whereas revoked users find insufficient information to recover the key. The typical setting considered is that of a unidirectional broadcaster and stateless users (i.e., users do not keep bookmarking of previous messages by the broadcaster), which is especially challenging. In contrast, the scenario where users are supported with a bidirectional communication link with the broadcaster and thus can more easily maintain their state, and where users are not only dynamically revoked but also added (joined), is often referred to as multicast encryption.

The security of BE is defined by the security model it follows. A BE scheme is adaptive secure if it allows the adversary to declare the set that he/she wants to attack by using the public parameters and private keys compromised under the restriction that the adversary cannot possess any decryption key of the users in the target set. The selective security, by comparison, requires that the adversary to decide the target set before the system parameters are chosen. Selective security is a weaker notion but it is relatively easier to achieve.

An identity-based broadcast encryption (IBBE) is a broadcast encryption scheme in which each receiver is identified by his/her unique identity. As identities are arbitrary bit-strings, an IBBE should support exponentially many users as potential receivers. This implies that for an IBBE to be practical, the size of parameters such as public parameters, private keys and cipher texts must not be related to the total number of users in the system. IBBE is often simplified to mID-KEM (multiple identity based key encryption scheme) which is the cryptographic primitive combining identity-based encryption and mKEM (multiple-receiver key encapsulation Mechanism). In mID-KEM and mKEM, multiple parties share a secret

*Corresponding author **Asha Prasad G** is a PG Scholar **and Deepthy Mathews** is working as Assistant Professor

key for their future secure communications to be protected by symmetric cryptographic algorithms.

A trivial solution to broadcast is to encrypt the same message under each receiver's public key. However, this trivial solution possesses a cipher text size linear with the number of receivers. Thus, the goal of broadcast encryption is to reduce the size. Although there are several realizations in broadcast encryption allowing polynomial users in the system of the cipher text, achieving an IBBE scheme having efficient sized parameters remains a difficult problem because it has to support exponentially many users in the system using the limited entropy provided in public parameters. An IBBE should satisfy several important properties. First, an IBBE scheme should be fully collusion resistant. This property requires that even if all the users collude, they should not be able to learn anything about the message if none of the colluding users is included in the set of receivers for the broadcast. The stateless receiver's property is also important for the efficiency of the system. If an IBBE scheme does not have stateless receivers, it must distribute private keys again whenever there is a change in the set of receivers.

2. Existing System

Several existing broadcast encryption schemes achieve constant-sized cipher text. While they are secure in the standard model, these schemes support only polynomially many users because they have parameters, such as public keys or private keys, which increase linearly with the number of total users in the system. In these systems, the users are normally labelled from 1 to n. Gentry and Waters suggested the first adaptively secure identity-based scheme having sub-linear sized cipher text (B. Malek *et al*, 2012). First, they introduced an IBBE scheme in which a linear sized Tag is included in the cipher text to allow exponentially many users in the system. Subsequently, they suggested a way to achieve sublinear sized cipher text by reusing Tag in the original scheme and increasing the size of other components in a cipher text from constant to sublinear.

Lewko, Sahai and Waters introduced a revocation scheme based on a revocation system which achieves broadcast encryption not by including users but by revoking users (A. B. Lewko *et al*, 2010). The size of the parameters does not depend on the total number of users in the system. However, the size of the cipher text linearly increases with the number of revoked users in their scheme. In addition, while its parameters do not depend on the total number of users in the system, adaptive security has been proved when it allows a polynomial number of users. The system can only be proven selective secure if exponentially many users are to be supported. Similarly, an adaptively secure Key Policy Attribute Based Encryption (KP-ABE) scheme featuring constant-sized cipher text and supporting exponentially-many attributes was introduced by Attrapadung (N. Attrapadung *et al*, 2014).

There are three IBBE systems using multilinear map (D. Boneh *et al*, 2014). Due to the properties of multi-linear map, they can be very efficient. However, although the number of the group elements of a cipher text is constant, the size of the group elements is O ($\log_2$N). Also, the security of these systems depends on some q-type assumptions, which is undesirable. Attrapadung and Libert introduced the first IBBE scheme having a constant sized cipher text as an application of Inner Product Encryption (IPE). Since broadcast encryption can be interpreted as a special case having only OR-gates between recipients, broadcast encryption can be also achieved by IPE. Their scheme is constructed in a prime order group and has a constant sized cipher text although the sizes of a private key and a public parameter of their scheme linearly increase with the size of maximum number of receivers in the system. To achieve this, they used the dual system encryption (N. Attrapadung *et al*, 2014). Their scheme depends on standard assumptions (hardness of the Decision Linear Problem (DLIN) and the Decision Bilinear Diffie-Hellman Problem (DBDH)). However, their scheme is designed for IPE and is not well adapted for an IBBE system. Some important features are missing in their construction arising from this matter. The security of their system fails if only one receiver is included in a cipher text because their n-wise independence argument does not hold. Also, their computational complexity can be reduced if IPE is used to construct IBBE. They also achieved an adaptively secure broadcast encryption. However, this scheme requires a subgroup decisional assumption, which cannot be reduced as General Subgroup Decision (GSD) Assumption.

3. Proposed System

Traditional way to prove the security of broadcast encryption is using q-type assumptions and partitioning the key space by the set of identities of receivers and others. The dual system encryption, introduced by Waters (N. Attrapadung *et al*, 2014), gives a break-through in security proof methodology by introducing the concept of semi-functional keys and cipher text which are only used in the security proof. However, proving the invariance between a semi-functional key and a normal key is still challenging because the simulator can detect this correlation by generating a semi-functional cipher text which can be decrypted only by a normal key to distinguish whether the key is a semi-functional key or a normal key.

Dual system encryption is used widely to provide security protocols including BE. Lewko and Waters suggested a way to solve this problem. In their suggestion, when the algorithm generates a semi-functional cipher text, the cipher text is correlated with semi-functional keys. This means if a valid semi-functional key is used to decrypt a semi-functional

cipher text, the semi functional key does not hinder decryption and works like a normal key, but this correlation between the semi-functional key and cipher text is hidden to the adversary who cannot query a valid key for the challenge cipher text. Although the nominally semi-functionality is very helpful to prove the security, hiding the correlation is not trivial if the system has to support exponentially many users with limited entropy.

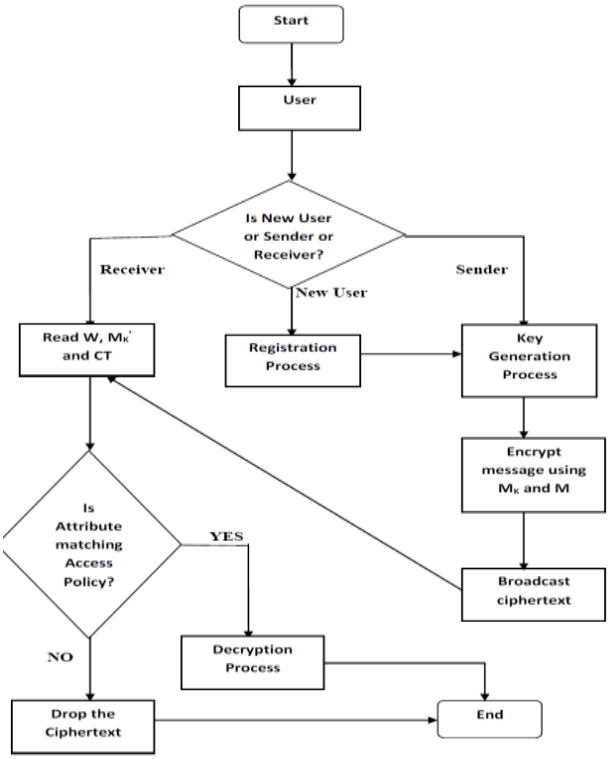

Fig 1: Flow Chart of Broadcast System

Lewko and Waters introduced the technique to overcome the shortage of randomness. To amplify the entropy, they localize semi-functional spaces by introducing ephemeral semi-functional space which is only used to prove the key invariance between a normal key and a semi-functional key. The random values, hiding the correlation between the key and the cipher text, are only used in ephemeral semi-functional space. Then, the semi-functional spaces share only random values which do not interrupt to hide this correlation in ephemeral semi-functional space. We prove the security of our scheme. However, we prove the adaptive security of our system using General Subgroup Decision (GSD) Assumption only. Specifically, when they proved the semi-functional invariance of their scheme, they used an assumption which cannot be reduced to GSD.

In contrast, prove semi functional invariance without this assumption. Hence, the security of our scheme relies on fewer assumptions than Lewko and Waters' scheme (N. Attrapadung *et a*l, 2014). Our IBBE scheme achieves adaptive security by combining dual system encryption with n-wise pairwise independence argument. However, the n-wise independence argument does not hold if only one receiver is included in the system. Hence, first we restrict our scheme so that the number of receivers is larger than 1. Then, we provide a practical way to overcome this restriction. The computational complexity of the decryption algorithm of our scheme only depends on the number of receivers.

4. IBBE

Our broadcast encryption scheme consists of four algorithms, namely, setup (Setup), private key generation (KeyGen), encryption (Enc) and decryption (Dec) as defined below.

- **Setup (λ, n, ℓ)** - takes as input the number of receivers (n) and the maximal size of a broadcast recipient group (ℓ ($\leq$ n)). It outputs a public/master secret key pair (PK, MSK).
- **KeyGen (i, MSK)** - takes as input an index i $\in$ {1, n} and the secret key MSK. It outputs a private key d_i.
- **Enc(S, M, PK)** - takes as input a subset S C {1... n}, a message M and a public key PK. If $|S| \leq \ell$, it outputs a CT.
- **Dec(S, i, d_i, CT, PK)** - takes as input a subset S C {1... n} an index i $\in$ {1... n}, a private key di for i, a cipher text CT, and the public key PK. If $|S| \leq \ell$ and i $\in$ S, then the algorithm outputs the message M.

I. IMPLEMENTATION

Let i be an identity of a user in the system, and S be a set of identities of recipients for a broadcast. Also we define the maximum number of receivers' ℓ. We restricted the number of receivers to be greater than 1.

Setup (λ, n, ℓ)

//Input: λ - a random number generated as security parameter, n – no of receivers, ℓ - maximum no of receivers

//Output: (PK, MSK) a public/master secret key pair

1. Generate a set of three distinct primes, p_1,p_2,p_3
2. Choose a bilinear group G of order N, where N = $p_1p_2p_3$
3. Generate a subgroup of order p_1 : {g, u , w, v, h} $\in$ G_{pi}
4. Generate a Master Key MSK = {δ} from Z_N, which is a non-empty subset of N integers and public key PK = {g, u, w, v^{α_j}, h^{α_j}, e(g, h) $^{\delta}$: j $\in$ [1, ℓ]}, where $\alpha \in Z_N$

KeyGen (i, MSK)

//Input: i – array of identities of users, MSK – Set of Master Key for each user

//Output: d_i - array of private key

1. Generate y_i, $r_i \in Z_N$ for each identity i

2. Assign $(x^{\ell}, \ldots, x^1, x^0) = (i_{\ell}, \ldots i_1, i_0)$
3. Generate set of private keys

$d_i = (K_0, K_1, K_2, K_{3,j} : j \in [1, \ell])$

$= (g^{\delta} wy_i, hy_i, vy_i \cdot ur_i, h(-\alpha_0 x_j / x_0 + \alpha_j)^{r_i} : j \in [1, \ell])$

Enc(S, M, PK) - CAST Algorithm can be used to provide encryption of the broadcast message.

//Input: S – subset of users, M – Message, PK – Public Key

//Output: CT - cipher text

1. Compute 16 pairs of sub keys $\{K_{mi}, K_{ri}\}$ from K
2. (L_0, R_0) <-- $(m_1 \ldots m_{64})$. (Split the plaintext into left and right 32-bit halves $L_0 = m_1 \ldots m_{32}$ and $R_0 = m_{33} \ldots m_{64}$.)
3. For i =1 to 16, compute L_i and R_i as follows:
   a. $L_i = R_{i-1}$;
   b. $Ri = L_{i-1} \wedge f(R_{i-1}, K_{mi}, K_{ri})$, f is of Type 1, Type 2, or Type 3, depending on i
4. $c_1 \ldots c_{64}$ <-- (R_{16}, L_{16}) - Exchange final blocks L_{16}, R_{16} and concatenate to form the cipher text

- Types of Rounds in CAST
  1. Type 1: $I = ((K_{mi} + D) <<< K_{ri})$; $f = ((S_1[I_a] \wedge S_2[I_b]) - S_3[I_c]) + S_4[I_d]$
  2. Type 2: $I = ((K_{mi} \wedge D) <<< K_{ri})$; $f = ((S_1[I_a] - S_2[I_b]) + S_3[I_c]) \wedge S_4[I_d]$
  3. Type 3: $I = ((K_{mi} - D) <<< K_{ri})$; $f = ((S_1[I_a] + S_2[I_b]) \wedge S_3[I_c]) - S_4[I_d]$

Where,

Rounds 1, 4, 7, 10, 13, and 16 use f function Type 1.

Rounds 2, 5, 8, 11, and 14 use f function Type 2.

Rounds 3, 6, 9, 12, and 15 use f function Type 3.

D – Data, I_a to I_d –Most Significant Byte to the Least Significant Byte

Dec(S, i, d_i, CT, PK)

//Input: S – subset of users, i – array of identity of receivers, d_i – array of Private Key, CT - Cipher text, PK – Public Key

//Output: M – message

1. Cipher text $\{c_1 \ldots c_{64}\}$ is divided into (R_{16}, L_{16})
2. Exchange R_{16}, L_{16} to obtain (L_{16}, R_{16})
3. For i =15 to 0, compute L_i and R_i as follows:
   a. $L_i = R_{i+1}$;
   b. $R_i = L_{i+1} \wedge f(R_i+1, K_{mi}, K_{ri})$, f is of Type 1, Type 2, or Type 3, depending on I

Now $L_0 = m_1 \ldots m_{32}$ and $R_0 = m_{33} \ldots m_{64}$

4. Merge $(L_0, R_0) = (m_1 \ldots m_{64})$ to obtain the plain text

5. Results

In comparison with the IBBE scheme developed using AES, CAST algorithm has achieved a constant sized cipher text in O (log n) times. CAST has been proved to be more secure than AES.

Table 1: Result Analysis

Scheme	Assumption	Public Key	Private Key	CT	Decrypt	Security	Order
AES	GSD	$O(\ell)$	$O(\ell)$	4GN	4P + kE	Adaptive	Composite
CAST	GSD, CSD	O(1)	$O(\ell)$	Constant (32-40 Bytes)	$O(\ell)$	Adaptive	Prime

Conclusion

An adaptively secure identity based broadcast encryption scheme featuring constant size cipher text was introduced. The public parameters and private keys in the scheme increase linearly with the maximum number of receivers and not with the total number of users. Also, the computational complexity of the decryption process depends only on the number of receivers. Finally, it was shown that the scheme is adaptively secure under the general decisional subgroup assumption instead of multiple subgroup decisional assumptions in the standard model through the use of the dual system encryption technique.

References

N. Attrapadung (2014), Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more, . *Springer*, vol. 8441, pp. 557577.

D. Boneh, B. Waters, and M. Zhandry (2014), Low overhead broadcast encryption from multi-linear maps, *Springer* , vol. 2014, pp. 195

M. Zhang, B. Yang, Z. Chen, and T. Takagi (2013), Efficient and adaptively secure broadcast encryption systems, *Security and Communication Networks*, vol. 6, no. 8, pp. 10441052.

L. Zhang, Y. Hu, and Q.Wu (2012), Adaptively secure identity-based broadcast encryption with constant size private keys and cipher texts from the subgroups, *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp.1218

B. Malek and A. Miri (2012), Adaptively secure broadcast encryption with short cipher texts, *Network Security*, vol. 14, no. 2, pp. 717

M. Bellare, B. Waters, and S. Yilek (2011), Identity-based encryption secure against selective opening attack, *Springer*, Ed., vol. 6597, pp. 2352

A. B. Lewko and B. Waters (2011), Unbounded hibe and attribute-based encryption, *EUROCRYPT, ser. Lecture Notes in Computer Science*, *K. G. Paterson*, *Springer*, Ed., vol. 6632, pp. 547567

A. B. Lewko and B. Waters (2010), New techniques for dual system encryption and fully secure hibe with short ciphertexts, *TCC, ser. Lecture Notes in Computer Science, D. Micciancio*, *Springer*, Ed., vol. 5978, pp. 4554

A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters (2010), Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, *EUROCRYPT, ser. Lecture Notes in Computer Science, H. Gilbert, Springer,* Ed., vol. 6110, pp. 6291

A. B. Lewko, A. Sahai, and B. Waters (2010), Revocation systems with very small private keys, *IEEE Symposium on Security and Privacy*, pp. 273285.