POSTER: Attribute Based Broadcast Encryption with Permanent Revocation*

Shlomi Dolev
Dept. of Computer Science
Ben-Gurion University of the Negev
Beer-Sheva, 84105, Israel
dolev@cs.bgu.ac.il

Niv Gilboa
Dept. of Communication Systems Eng. and Deutsche Telekom Labs at BGU
Ben-Gurion University of the Negev
Beer-Sheva, 84105, Israel
niv.gilboa@gmail.com

Marina Kopeetsky
Dept. of Software Engineering
Sami-Shamoon College of Engineering
Beer-Sheva, 84100, Israel
marinako@sce.ac.il

ABSTRACT

We propose a new and efficient scheme for broadcast encryption. A broadcast encryption system allows a broadcaster to send an encrypted message to a dynamically chosen subset RS, $|RS| = n$ of a given set of users, such that only users in this subset can decrypt the message. An important component of broadcast encryption schemes is revocation of users by the broadcaster, thereby updating the subset RS. Revocation may be either temporary, for a specific ciphertext, or permanent.

We present the first public key broadcast encryption scheme that support permanent revocation of users. Our scheme is fully collusion-resistant. In other words, even if all the users in the network collude with a revoked user, the revoked user cannot encrypt messages without receiving new keys from the broadcaster. The procedure is based on Cipher-text Policy Attribute-Based Encryption (CP-ABE).

The overhead of our system is $O(\log n)$ in all major performance measures including length of private and public keys, computational complexity, user's storage space, and computational complexity of encryption and decryption.

Categories and Subject Descriptors

C.2.0 [**COMPUTER-COMMUNICATION NETWORKS**]: General—*Security and protection*

General Terms

Security

Keywords

Attribute Based Encryption, Broadcast Encryption

1. INTRODUCTION

The concept of broadcast encryption was first introduced in [7] and further developed in many works including [13], [10], [2], [8], [6] and [11]. Broadcast encryption systems allow a broadcaster to send encrypted data to a set of users such that only a subset RS of *authorized* users can decrypt the data. A main challenge in constructing broadcast systems is ensuring that even when the users that are not in RS collude, it is computationally infeasible to decrypt a message.

Broadcast encryption systems support *temporary* revocation of users if revoked users are excluded from the set RS for a single ciphertext. Typically, in such systems, the identities of the revoked users are parameters in the encryption mechanism. Broadcast encryption systems support *permanent* revocation of users if revoked users cannot decrypt any ciphertext after the revocation. Permanent user revocation is efficiently implemented in symmetric encryption schemes (e.g. the third scheme of [6]). Temporary revocation is achieved by various schemes including [5] and the first two schemes of [6].

Broadcast encryption systems are either stateful or stateless. A stateful scheme requires receivers to store a state and update it based on the ciphertexts they receive. Stateless receivers do not necessarily update a state. Stateless schemes are preferable in the sense that receivers do not have to be continuously online to update a state. However, stateful schemes open new avenues to achieve permanent revocation by basing decryption on the state and not enabling revoked users to correctly update a state. Furthermore, broadcast models in which the receivers can open a two-way channel to the broadcaster are becoming more prevalent, e.g. IPTV and Over-The-Top broadcasting. Given such two-way channels, receivers can update their state even if they go offline for a time.

A trivial solution for constructing collusion resistant broadcast system works as follows. The broadcaster maintains n independent encryption keys, while each user is granted its personal decryption key. The broadcaster encrypts each message with all the encryption keys. Since the keys are independent, collusion resistance is satisfied for any number of revoked colluding users. Obviously, this scheme is not efficient in the number of encryption/decryption keys, size of broadcaster storage, and cost of encryption/decryption procedure.

Stateful symmetric encryption schemes.
Most of the stateful symmetric encryption schemes are based on graph theoretical constructions, and support permanent revocation of a single user or a group of users. The drawback of symmetric encryption is that only users that have the secret key, can receive and decrypt the broadcast messages.

*Rita Altura Trust Chair in Computer Science and the internal research program of Sami Shamoon College.

CCS'11, October 17–21, 2011, Chicago, Illinois, USA.
ACM 978-1-4503-0948-6/11/10.

Stateless schemes. The stateless broadcast encryption schemes may be based on symmetric-key or public-key approach. The use of symmetric key cryptosystems restricts the solutions presented in e.g. [13] and [6] in the sense that only the server (or central module) may broadcast the sensitive data.

A powerful technique for public-key, broadcast encryption systems, is Attribute Based Encryption (ABE) (e.g., [5], [12]). The purpose of ABE is to establish access policy for decrypted data among users of a given set. Unfortunately, all the ABE based schemes support only temporary revocation of users. The best public-key, broadcast encryption scheme in terms of performance is [11], which can also be used to construct improved ABE schemes.

Efficiency of the broadcast encryption scheme. Efficiency is measured in server/user storage space, computational complexity of key update procedure and a number of messages sent upon join or revocation event.

Optimal efficiency is achieved for public key with temporary revocation by [11] and for symmetric key with permanent revocation by [6]. In both works, the encryption/decryption keys are of constant size, ciphertext size is of $O(r)$, where r is the number of revoked users, and the computational complexity of a key update procedure is $O(r)$.

The permanent revocation achieved in our scheme requires a public key of length $O(1)$, private keys of length $O(\log n)$ and the ciphertext length to revoke r users is $O(r \log n)$. The computational complexity of a key update is also $O(r \log n)$.

Our contributions. We propose the first efficient public-key encryption scheme that supports permanent user revocation. We use Ciphertext Policy ABE (CP-ABE) techniques introduced and analyzed in [1] as a building block and extend it to support permanent revocation. Any user in [1] is assigned a set of attributes and can decrypt any ciphertext that embeds a policy, which satisfies the user's attributes. Furthermore, any coalition of users cannot decrypt a ciphertext if none of the user's attributes satisfies the policy.

A previous broadcast encryption work [5] bases broadcast encryption on CP-ABE. However, each revocation is temporary since sequentially revoked users (identified with different sets of attributes) can share their attribute keys and reconstruct the keys updated after their revocation. We eliminate this problem in such a way that any revoked user/users cannot decrypt any ciphertext broadcast after the revocation. Moreover, the collusion of all users from the new set of broadcast receivers, cannot help in this attempt.

The main advantages of our schemes are:

• We propose the first efficient public-key encryption scheme that supports permanent users' revocation. The identities of the revoked users are permanently excluded (upon key update procedure) from the encryption mechanism. Previous schemes that enabled permanent revocation were all based on symmetric keys: e.g, scheme 3 of [6] and [13]. The use of public encryption systems allows any user to encrypt and broadcast a message.

• By providing permanent users' revocation, we treat the more complex notion of collusion when a previously revoked user U_i can get private information (including secret keys) from a later revoked user U_j (or set of such revoked users). Hence, our schemes cope with stronger adversary, compared with the previous public key schemes e.g., [2], [5]. The penalty we pay is that our scheme is stateful and hence all the participating users must be permanently on-line (or updated about the sessions they missed).

• There is no change in the public key upon executing the *Join* procedure, and *Join* may be efficiently implemented in $O(\log n)$ time complexity (it should be noted that the best implementation is introduced in [6] that requires $O(1)$ time complexity). We use an efficient key update based on the CP-ABE techniques, that is executed by the server (broadcaster).

• The efficiency of our scheme is worse by at most a factor of $O(\log n)$ from the most efficient public key scheme [11], which only achieves temporary revocation. Efficiency is measured in the length of private and public keys, length of a ciphertext and computational complexity of a decryption/key update procedure.

• It may be possible to to integrate our technique into other schemes e.g., [11].

2. BROADCAST ENCRYPTION WITH PERMANENT REVOCATION

Our scheme uses CP-ABE [1] in a way that support users' permanent revocation. The main idea is to change the state of each non revoked user by updating the master key MK and the secret key SK_i of each user in a way that all the users except the revoked user U_j can decrypt the ciphertext and no coalition of users (that record the messages after the exclusion of U_j) can assist in updating SK_j and computing the new secret master key.

The scheme proceeds as follows:

• Each user is defined by a unique combination of attributes, e.g. the bits in a binary representation of the user's ID. Each user receives attribute keys that enable sending a public-key encrypted message to be decrypted by any subset of users, see [5] for details. The broadcaster authorizes a subset of receivers RS by broadcasting the global secret decryption key K_{global}. This key is encrypted by the appropriate attribute keys for RS (according to the ABE system). The broadcaster may then encrypt bulk data using K_{global}.

• Each user from the receiver set RS maintains the state $State_i$ that is defined as a value of a certain function over a secret counter variable CTR: $State_i = f_i(CTR)$.

• When a user U_j is revoked from the receivers set RS, the broadcaster updates the counter variable CTR to a new secret value $\widetilde{CTR}$, and broadcasts its encrypted value to all non revoked users. As a result, the state of each user U_i, $U_i \in RS - \{U_j\}$ is updated to $State_i = f_i(\widetilde{CTR})$. Thus, the encryption key and ciphertext generated by the broadcaster, and appropriate secret encryption key K_{global} are updated. This update is performed in such a way that even a coalition of all users from the new set of receivers RS cannot collude in order to reveal the updates after U_j's revocation $State_j = f_j(\widetilde{CTR})$.

Consider the basic CP-ABE system construction in [1]. Let G_0 be a bilinear group of prime order p, and let g be a random generator of G_0. Let $e : G_0 \times G_0 \rightarrow G_1$ be a proper bilinear map. The security parameter k denotes the size of the groups. Let M be a secret message that should be encrypted and sent by the broadcaster to the users from the set $RS - \{U_j\}$.

Our modifications of the basic scheme of [1] are as follows:

Setup. Choose G_0, g, and two random elements $\alpha, \beta \in Z_p$. The public key is published exactly as in [1]: $PK = G_0,\ g,\ h = g^{\beta}, e(g,g)^{\alpha}$. The master key MK includes our new random component $CTR \in Z_p$: $MK = \beta,\ g^{\alpha}, CTR$.

Key generation (MK, S). The input of the algorithm is a set of attributes S, and the output is a secret key that identifies the set. Two random numbers r and r_j are chosen from Z_p for each attribute $j \in S$. The component E encodes the state, which is a function of CTR. The private key is:

$$\left\{ D = g^{\frac{\alpha + r}{\beta}},\ E = e(g,g)^{r \cdot CTR}, \forall\, j \in S : D_j = g^r H(j)^{r_j},\ D'_j = g^{r_j} \right\}.$$

Encrypt. The encryption procedure encrypts a message M under the access structure (AS) $T = RS - \{U_j\}$ (see [1] and [5] for a simplification of AS). For each node x (including the leaves) a

polynomial q_x is properly defined (see [1] for the encryption details). Starting with the root node R, a random secret for sharing $s \in Z_p$ is chosen and the root polynomial is defined in 0 as $q_R(0) = s$. It should be noted that the secret s and its corresponding shares are changed (decremented by CTR) in our modification. Set $s_2 = -s - CTR \bmod p$ and construct the ciphertext CT is as:

$$CT = \left(T = RS - \{U_j\},\ \widetilde{C} = Me(g,g)^{\alpha s_2}\right)$$

$$C = h^{s_2}, \forall\, y \in Y : C_y = g^{q(0)},\ C'_y = H(att(y))^{q_y(0)}.$$

Here Y denotes the set of leaf nodes in T and H is a cryptographic proper hash function.

Decryption. The decryption procedure performed by each user that possess a set of attributes corresponding to T is as follows: First, the user computes $A = e(g,g)^{rs}$, by using the DecryptNode procedure of [1]. Then,

$$M = \widetilde{C}/(e(C,D) \cdot A \cdot E)$$

since

$$e(C,D) = e\left(g^{\beta s_2}, g^{\frac{\alpha+r}{\beta}}\right) = e(g,g)^{(\alpha+r)s_2} = e(g,g)^{\alpha s_2} \cdot e(g,g)^{rs_2} = e(g,g)^{\alpha s_2} \cdot e(g,g)^{r(-s-CTR)}.$$

Hence,

$$e(C,D) \cdot E = e(g,g)^{\alpha s_2} \cdot e(g,g)^{-rs}.$$

As a result,

$$e(C,D) \cdot E \cdot A = e(g,g)^{\alpha s_2}.$$

Finally,

$$M = \widetilde{C}/(e(C,D) \cdot A \cdot E).$$

The broadcaster updates CTR in MK by $CTR \leftarrow CTR + s \bmod p$. The user updates E in its private key by

$$E \leftarrow E \cdot A = e(g,g)^{rCTR} e(g,g)^{rs} = e(g,g)^{r(CTR+s)}.$$

Unlike previous CP-ABE based schemes (e.g. [5]), the users' attribute keys in our scheme remain constant regardless of the possible revocations, whereas only a global state CTR and corresponding functions of CTR are updated.

Once a user U_j is revoked, it cannot compute its function of CTR, $e(g,g)^{r \cdot CTR}$ even with the collusion of every other user. Thus, the revocation is permanent.

3. REFERENCES

[1] J. Bethencourt, A. Sahai, B. Waters,"Ciphertext-Policy Attribute Based Encryption", *IEEE Symposium on Security and Privacy* (SP '07), pp. 321-334, 2007.

[2] D. Boneh, C. Gentry, B. Waters, "Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys", *25-th Annual International Cryptology Conference CRYPTO 2005*, USA, 2005. In *Lecture Notes in Computer Science*, volume 3621, pp. 258-275.

[3] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions", *INFOCOM'99*, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Proceedings, volume 2, pp. 708-716, 1999.

[4] R. Canetti, T. Malkin, K. Nissim, "Efficient Communication-Storage Tradeoffs for Multicast Encryption", *EUROCRYPT'99, LNCS1592*, pp. 459-474, 1999.

[5] L. Cheung, J. A. Cooley, R. Khazan, C. Newport, "Collusion Resistant Group Key Management Using Attribute Based Encryption", *Cryptology ePrint Archive*, Report 2007/161, 2007. Presented at GOCP Æ07.

[6] C. Delerablee, P. Paillier, D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys", *Proceedings of the first International Conference on Pairing-based Cryptography*, LNCS 4575, pp. 39-59, Springer-Verlag, July 2007, Tokyo, Japan.

[7] A. Fiat, M. Naor, "Broadcast Encryption". In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pp. 480-491, CA, USA, 1994. Springer-Verlag, Berlin, Germany.

[8] C. Gentry, B. Waters, "Adaptive Security in Broadcast Encryption Systems", In *Eurocrypt*, 2009.

[9] H. Harney, E. Harder, "Logical Tree Hierarchy Protocol", *Internet Draft, Internet Engineering Task Force*, April, 1999.

[10] D. Halevy, A. Shamir, "The LSD Broadcast Encryption Scheme", *CRYPTO 2002*, LNCS 2442, pp. 47-60, 2002.

[11] A. Lewko, A. Sahai, B. Waters, "Revocation Systems with Very Small Private Keys", In *Security and Privacy*, 2010.

[12] D. Lubicz, T. Sirvent, "Attribute-Based Broadcast Encryption Scheme Made Efficient", In *AFRICACRYPT*, LNCS, volume 5023, pp. 342-325, 2008.

[13] D. Naor, M. Naor, J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", *CRYPTO 2001*, LNCS, vol. 2139, pp.41-62, 2001.

[14] A. Perrig, D. Song, J. D. Tygar, "ELK, a New protocol for Efficient Large-Group Key Distribution", *IEEE Symposium on Security and Privacy 2001*, Proceedings, pp. 247-262, 2001.

[15] A. T. Sherman, D. A. McGrew, "Key Establishment in Large Dynamic Groups using One-Way Function Trees", *IEEE Transactions on Software Engineering*, no. 29, volume 5, pp. 444-458, 2003.

[16] C. K. Wong, M. Gouda, S. Lam, "Secure Group Communications Using Key Graphs", *IEEE/ACM Transactions on Networking*, volume 8, no. 1, February, 2000.