Threshold Broadcast Encryption With Reduced Complexity

Kerem Kaşkaloğlu
Institute of Applied Mathematics
Middle East Technical University, Ankara
Email: e110893@metu.edu.tr

Kamer Kaya
Department of Computer Engineering
Bilkent University, Ankara
Email: kamer@cs.bilkent.edu.tr

Ali Aydın Selçuk
Department of Computer Engineering
Bilkent University, Ankara
Email: selcuk@cs.bilkent.edu.tr

Abstract— **Threshold Broadcast Encryption (TBE) is a promising extension of threshold cryptography with its advantages over traditional threshold cryptosystems, such as eliminating the need of a trusted party, the ability of setting up the system by individual users independently and the ability of choosing the threshold parameter and the group of privileged receivers at the time of encryption. An ElGamal-based solution for TBE was proposed by Ghodosi et al. In this paper, we propose an improved ElGamal-based TBE scheme with reduced transmission cost.**

Keywords: Threshold broadcast encryption, ElGamal, Shamir's SSS

I. Introduction

While one sender or receiver is capable of executing the private key operations in traditional public key cryptography, in *threshold cryptography*, the number of users required to sign or decrypt a message must be as high as a specified threshold value of the system. Threshold cryptography has numerous applications. It offers a convenient way of private communication between an individual and an organization which might be a company, an association, a council or a governmental agency. There are several papers and surveys [1], [2], [3], [6], [7], [10], [11], [12] discussing applications and research aspects of threshold cryptography. A usual scenario of threshold encryption is that a message is encrypted with a public key encryption scheme and the corresponding ciphertext is sent to a group of receivers. In this scenario, a coalition containing t out of n receivers is eligible to decrypt the ciphertext whereas any smaller coalitions are not. Such a scheme is called a (t, n)-threshold encryption scheme.

Every threshold cryptosystem depends on an underlying *secret sharing scheme* (SSS). In a SSS, the aim of a coalition is to obtain the shared secret. The secret sharing problem and a solution were independently proposed by Shamir [2] and Blakey [3] in 1979. Shamir's SSS is highly practical and is based on a simple polynomial interpolation. This scheme has been widely used to obtain threshold encryption/signature schemes for various applications. Several extensions of this scheme can also be found in the literature[14], [13].

Broadcast encryption (BE) deals with the problem of securely transmitting data to a dynamically changing group of privileged users. Any user outside the privileged set should not be able to recover the message. BE was first proposed by Fiat and Naor [4] and now it is widely used in digital rights management applications such as pay-TV, multicast communication, private streaming and distribution of copyright protected material such as music and movies. The popular Content Protection for Recordable Media (CPRM) [5] technology is also based on BE techniques [15].

The threshold broadcast encryption (TBE) problem was first introduced by Ghodosi et al. [7]. In their setting, there is a set of N receivers and a subset of n privileged receivers. The sender encrypts a message and broadcasts the corresponding ciphertext to all receivers. To decrypt the ciphertext, a coalition needs at least t users from the privileged set. TBE has some advantages over traditional threshold cryptosystems. First, the need for a trusted party is eliminated and the system can be set up by individual users independently. Secondly, and perhaps the most importantly, the sender can choose the privileged set and the threshold value at the time of encryption which allows a certain dynamism in the system. Ghodosi et al. proposed a TBE scheme using ElGamal public key encryption with $O(n)$ ciphertext size.

In this work, we propose an efficient ElGamal-based TBE scheme which reduces the transmission cost to $O(n-t)$.

The rest of the paper is organized as follows: In Section II, we give an overview of the background material which will be used in our solution. In Section III, we propose our ElGamal-based TBE scheme. Section IV concludes the paper.

II. Background

A. The ElGamal Cryptosystem

ElGamal cryptosystem together with its signature scheme [8] is one of the main public key cryptosystems today which has yielded many variations. The security of the ElGamal cryptosystem depends on the hardness of the discrete logarithm problem. An overview of this scheme is given below:

- **Key Generation:** The public and private keys of a user are generated as follows:
  1) Let p be a large prime and g be a generator of $\mathbb{Z}_p^*$.
  2) Randomly choose the secret key $\alpha \in_R \mathbb{Z}_p^*$, and compute $\beta = g^\alpha \bmod p$.

This work is supported in part by the Turkish Scientific and Technological Research Agency (TÜBİTAK), under grant number EEEAG-105E065.

3) $SK = \alpha$ and $PK = (p, g, \beta)$ are the private and public keys of the user, respectively.

- **Encryption:** To encrypt a message $m \in \mathbb{Z}_p$ for the user with public key β
  1) Choose a random integer $k \in_R \mathbb{Z}_p^*$.
  2) Compute $b = \beta^k \bmod p$
  3) Compute the ciphertext $c = (c_1, c_2)$ where $c_1 = g^k \bmod p$ and $c_2 = mb \bmod p$.

- **Decryption:** Given a ciphertext $c = (c_1, c_2)$
  1) Compute $b^{-1} = {c_1}^{-\alpha} \bmod p$.
  2) Compute the message $m = b^{-1} c_2 \bmod p$.

Here, the factor b is sometimes referred as the *masking factor* since it is used to hide the original message m.

B. Shamir's Secret Sharing Scheme

Suppose the secret d is shared among n users where only a coalition of size at least t can recover the secret. Such a scheme is called a (t, n)-secret sharing scheme. In a *perfect* SSS, a coalition of size less than t cannot obtain any information about the secret.

Shamir's SSS [2] is the first and the best-known SSS in the literature. Several threshold cryptosystems have been proposed based on Shamir's SSS. The scheme works as follows: Let q be a large prime and $d \in \mathbb{Z}_q$ be the secret to be shared. The dealer chooses a random polynomial

$$f(x) = d + \sum_{i=1}^{t-1} a_i x^i$$

of degree $t-1$ from $\mathbb{Z}_q[x]$ where the constant term is set to d. The dealer then distributes the secret shares $y_i = f(i), 1 \leq i \leq n$, to the ith user.

The reconstruction process is a simple polynomial interpolation to compute $f(0) = d$. Suppose a coalition $\mathcal{S}$ wants to reconstruct the secret. They can compute the secret polynomial $f(x)$ and the secret by Lagrange's polynomial interpolation: Let

$$\lambda_{ij}^{\mathcal{S}} = \prod_{j' \in \mathcal{S} \setminus \{i\}} \frac{j - j'}{i - j'}$$

be the Lagrange coefficient for user i to compute $f(j)$. Then $f(j)$ can be computed as

$$f(j) = \sum_{i \in \mathcal{S}} y_i \lambda_{ij}^{\mathcal{S}}.$$

In particular, the secret $f(0)$ can be computed as

$$f(0) = \sum_{i \in \mathcal{S}} y_i \lambda_{i0}.$$

III. An ElGamal Based Threshold Broadcast Encryption Scheme

In broadcast encryption, there is a universal receiver set $\mathcal{U}$. Before encrypting a message m, certain receivers are designated as privileged and the ciphertext C is constructed in a way that only the receivers in the privileged set $\mathcal{P} \subseteq \mathcal{U}$ can decrypt C and obtain m. In our setting, we will denote the cardinalities of the universal and privileged sets ($\mathcal{U}$ and $\mathcal{P}$) by N and n, respectively. Without loss of generality, we assume that $\mathcal{U} = \{1, \cdots, N\}$.

In a TBE scheme with threshold t, only a coalition $\mathcal{S} \subseteq \mathcal{P}$ with size at least t is allowed to decrypt C and obtain m. This problem was introduced by Ghodosi et al. [7] who also proposed the following solution: Let each receiver $i \in \mathcal{U}$ have a public-private ElGamal key pair α_i and β_i where g and p are common public parameters. By using a combination of ElGamal encryption and Shamir's SSS, a ciphertext C is constructed as follows:

1) For $\alpha = \sum_{i \in \mathcal{P}} \alpha_i$, compute $g^\alpha = \prod_{i \in \mathcal{P}} \beta_i \bmod p$.
2) Choose a random ephemeral key $k \in_R \mathbb{Z}_p^*$ and apply Shamir's SSS to generate the shares $y_i = f(i)$ for each $i \in \mathcal{P}$ in a (t, n)-secret sharing where $f(0) = k$.
3) The ciphertext is computed as $C = (g^k \bmod p, mg^{k\alpha} \bmod p, \{y_i {\beta_i}^k \bmod p : i \in \mathcal{P}\})$.

Here the secret share y_i for each receiver $i \in \mathcal{P}$ is encrypted with the corresponding ElGamal public key β_i. Each receiver in the privileged set obtains a share for k. Since p and g^α are publicly known, after reconstructing k with t shares the inverse of the mask $g^{k\alpha}$ can be computed hence the message m can be unmasked. In this TBE scheme, the ciphertext has size $O(n)$.

A. An Improved ElGamal Based TBE Scheme

Here we propose an improved TBE scheme with a lower transmission cost than the scheme of Ghodosi et al. [7] described above. The proposed scheme works along the same lines as the ID-based scheme of Daza et al. [12]. Our scheme consists of the following phases:

- **Setup:** The public parameters of the system are determined in this phase:
  1) Choose a large safe prime $p = 2q + 1$ where q is also a large prime. Let g be an element in $\mathbb{Z}_p^*$ with order q.
  2) Let $\mathcal{X} = \{N+1, N+2, \cdots, N+(n-t)\}$ be a set of $n - t$ integers.

- **Key generation:** Each receiver $i \in \mathcal{U}$ generates a public-private key pair β_i and α_i as described in Section II-A and publishes his public key.

- **Encryption:** Let m be the message to be encrypted for a privileged set $\mathcal{P}$ of n users with a threshold value t.

  1) Choose a random ephemeral key $k \in_R \mathbb{Z}_q$.

2) Define $y_i = k\alpha_i \bmod q$ and compute

$$c_i = {\beta_i}^k \bmod p = g^{y_i} \bmod p$$

for all $i \in \mathcal{P}$.

3) Compute

$$r = g^{f(0)} = g^{\sum_{i \in \mathcal{P}} y_i \lambda_{i0}^{\mathcal{P}}} = \prod_{i \in \mathcal{P}} {c_i}^{\lambda_{i0}^{\mathcal{P}}} \bmod p$$

4) Set $c' = rm \bmod p$

5) Construct the set $\mathcal{Y}$ corresponding to the x-coordinates in $\mathcal{X}$ as follows:

$$\mathcal{Y} = \{\prod_{i \in \mathcal{P}} {c_i}^{\lambda_{ij}^{\mathcal{P}}} \bmod p : j \in \mathcal{X}\}$$

6) Broadcast the ciphertext $C = (g^k \bmod p, c', \mathcal{Y})$.

The encryption process uses Shamir's SSS in a slightly different way. Instead of choosing a random secret polynomial $f(x)$, the sender chooses a random ephemeral key k and takes $f(i) = k\alpha_i$ for all $i \in \mathcal{P}$. Unlike the conventional applications of Shamir's SSS, the degree of $f(x)$ is assumed to be n hence the $f(i)$ values for all $i \in \mathcal{P}$ determine the polynomial uniquely. Note that, the sender does not know any $f(i)$ but he can compute $c_i = g^{f(i)} = {\beta_i}^k \bmod p$ since β_i is public. Hence the sender can compute $g^{f(0)} \bmod p$ without knowing $f(0)$. To compute the inverse of the mask r, a coalition will need at least n points on the polynomial. The receivers are given $g^{f(j)} \bmod p$ for all x-coordinates $j \in \mathcal{X}$ with the ciphertext C. So a coalition containing t privileged users (i.e. a privileged coalition) can obtain m as follows:

- **Decryption:** Let C be the ciphertext and $\mathcal{S}$ be a privileged coalition.

1) Each user $i \in \mathcal{S}$ computes

$$g^{y_i} = (g^k)^{\alpha_i} \bmod p$$

2) The coalition computes

$$r = g^{f(0)} = \prod_{j \in \mathcal{S} \cup \mathcal{X}} (g^{y_j})^{\lambda_{j0}^{\mathcal{S} \cup \mathcal{X}}} \bmod p$$

3) Compute r^{-1} and obtain $m = r^{-1}c' \bmod p$

After receiving the ciphertext, a privileged receiver i computes $g^{f(i)} = (g^k)^{\alpha_i} \bmod p$. Since $\mathcal{U} \cap \mathcal{X} = \emptyset$ we also know that $\mathcal{S} \cap \mathcal{X} = \emptyset$ hence any privileged coalition $\mathcal{S}$ has n distinct $g^{f(j)} \bmod p$ values for all $j \in \mathcal{S} \cup \mathcal{X}$. So $r = g^{f(0)} \bmod p$ can be computed by Lagrange interpolation.

This TBE scheme reduces the transmission cost to $O(n-t)$ from the $O(n)$ cost of the scheme of Ghodosi et al. [7].

B. Security Analysis

The security of the proposed scheme depends on the security of Shamir's SSS and ElGamal encryption. First of all, an attacker cannot decrypt the ciphertext since the ephemeral key k remains secret even though $g^k \bmod p$ is known. In the proposed scheme, the ciphertext contains $n - t$ distinct $g^{f(i)} \bmod p$ values for a polynomial $f(x)$ of degree n. In addition to these values, we need at least t extra points to compute $r = g^{f(0)} \bmod p$ using Lagrange interpolation. These t points are obtained by the secret α_i values of the receivers in a privileged coalition, and given that the discrete logarithm problem is hard in $\mathbb{Z}_p^*$, i.e., an adversary cannot obtain an α_i from a β_i, our extra points on the polynomial remain secret. Also, no information can be obtained about $g^{f(0)} \bmod p$ by a coalition of size $t - 1$ because Shamir's SSS is perfectly secure.

IV. Conclusion

In this paper, we proposed a threshold broadcast encryption scheme with a lower transmission complexity than the previous work by Ghodosi et al. [7]. The security of our system is based on a threshold ElGamal encryption scheme using Shamir's sharing scheme as the underlying SSS.

The ideas used here to construct the TBE scheme can also be used to propose other TBE schemes based on different public key cryptosystems. In particular obtaining a similar system with RSA encryption is an interesting open problem.

References

[1] Y. Desmedt. Some recent research aspects of threshold cryptography. In E. Okamoto, G. I. Davida, and M. Mambo, editors, ISW '97: *Proceedings of the First International Workshop on Information Security*, volume 1396 of Lecture Notes in Computer Science, pages 158–173. Springer-Verlag, 1998.

[2] A. Shamir, How to Share a Secret, *Comm. ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[3] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, 1979, American Federation of Information Processing Societies Proceedings 48 (1979), 313-317.

[4] A. Fiat, M. Naor, Broadcast Encryption, *Proceedings of CRYPTO'93*, Lecture Notes in Computer Science, 773, Springer-Verlag, pp. 148-154, 1994.

[5] http://www.4centity.com/tech/cprm/

[6] Z. Chai, Z. Cao and Y. Zhou. Efficient ID-based broadcast threshold decryption in ad hoc network. *Proceedings of IMSCCS06, Volume 2, IEEE Computer Society*, pp. 148154 (2006).

[7] H. Ghodosi, J. Pieprzyk and R. Safavi-Naini. Dynamic threshold cryptosystems: a new scheme in group oriented cryptography. *Proceedings of Pragocrypt96, CTU Publishing House*, pp. 370-379, 1996.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logartihms. *IEEE Transactions on Information Theory*, IT-31:469-472, 1985.

[9] W. Diffie, M. E. Hellman, New Directions in Cryptography, *IEEE Transactions on Information Theory*, 1976

[10] C. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29(2):208-210,1983.

[11] Y. Desmedt. Threshold cryptosystems. *Advances in Cryptology, Proceedings of CRYPTO'89, Ed G. Brassard, Lecture Notes in Computer Science, Vol. 435*, pages 307-315, Springer-Verlag, 1990.

[12] V. Daza, J. Herranz, P. Morillo and C. Ráfols, CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts, *http://eprint.iacr.org/2007/127.*

[13] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, Proactive secret sharing or: How to cope with perpetual Leakage, *Proceedings of CRYPTO'95*, Lecture Notes in Computer Science, 963, Springer-Verlag, pp. 339-352, 1995.

[14] P. Feldman, A practical scheme for non-interactive verifiable secret sharing, *IEEE Symposium on Foundations of Computer Science*, pp. 427-437, IEEE, 1987.

[15] D. Naor, M. Naor, J. Lotspiech, Revocation and Tracing Schemes for Stateless Receivers, *Proceedings of CRYPTO'01*, Lecture Notes in Computer Science, 2139, Springer-Verlag, pp. 41-62, 2001.