Fully threshold broadcast encryption

Sigurd Eskeland
Norwegian Computing Center
0314 Oslo, Norway
sigurd.eskeland@nr.no

ABSTRACT

Threshold broadcast encryption (TBE) is a class of threshold cryptographic schemes that allow a sender to compute ciphertexts to ad hoc user groups. Plaintexts can only be recovered if t of the pertaining recipients collaborate by each producing a partial decryption share. Existing TBE schemes require that the partial decryptions are transferred through secure channels to a single combiner that restores the plaintext. Thus, the single combiner becomes the eventual target for the deciphered plaintext, and not the addressed group. As such, a single combiner and explicit secure channels are inconsistent with the concept of broadcasting.

In this paper, we propose a fully TBE scheme that does not require a combiner and secure channels. In this scheme, the partial decryptions are broadcasted, and only the intended recipients that are defined ad hoc by the sender are able to decrypt.

ACM Reference format:
Sigurd Eskeland. 2017. Fully threshold broadcast encryption. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017,* 5 pages.
https://doi.org/10.1145/3098954.3103159

1 INTRODUCTION

Threshold-oriented cryptography provisions distributed computations of cryptographic operations for the purpose to avoid single points of trust. A typical motivation is to prevent the risk of having a system compromised even if a single entity is compromised. Generally speaking, a threshold-oriented system of a threshold value t would tolerate compromises of $t - 1$ or less entities. Relevant types of threshold-oriented applications include threshold encryption, threshold signatures, distributed user certification and distributed user key computation.

Threshold encryption schemes allow a sender to compute ciphertexts that can be decrypted only by means of collaboration of t out of n recipients. In *static* threshold encryption schemes, user group memberships and the threshold t are predefined by a trusted authority (TA) during the setup phase [1, 3, 4, 8, 15–17]. The TA computes a public key representing the group, and a corresponding private key share for each user. Using the pertaining encryption algorithm, an arbitrary sender can compute a ciphertext by means of the public key. At least t partial user decryptions must be transmitted to a *combiner* that restores the plaintext. To preserve the confidentiality of the plaintext, the partial decryptions must be transferred through *secure channels* to the combiner. It could be noted that some authors use the term *threshold decryption* due to that minimum t users are required to decrypt.

In threshold broadcast encryption schemes (TBE) [2, 5–7, 12, 19, 20, 20, 23, 24], group memberships are not predefined. Instead, coalitions of recipients $\mathcal{V}$ and the threshold t are defined ad hoc by the sender. Ciphertexts are computed by using the public keys of the recipients $\mathcal{V}$. As with static threshold encryption, the partial user decryptions must be transmitted to a combiner through secure channels.

Accordingly, it could be argued that the term "broadcast" in threshold broadcast encryption is misleading:

(1) The group members that provide partial decryption do not obtain the plaintexts.
(2) A designated combiner is required to compute the plaintext given t partial decryptions.
(3) Secure channels are required between each group member and the combiner for secure transmissions of the partial decryptions.

These characteristics conform not well with broadcast-oriented environments. For many broadcast applications, it could be desirable avoid the constraint of a single combiner. Moreover, it may be desirable that each group member can securely restore the plaintexts individually.

Lastly, establishing secure channels between each group member and the combiner add additional and undesired computational and transmission overhead. If each participant is to obtain the plaintext by individually combining the partial decryptions, this would result in $t(t - 1)$ additional encryption/decryption operations and transmissions. Clearly, this does not scale with broadcast-oriented environments.

Our contribution. In this paper, we present a TBE scheme that provisions broadcasting of partial user decryptions, without need for secure channels, and the inherit constraint of a single combiner. All messages are broadcasted, including partial decryptions. It is therefore denoted a *fully* threshold broadcast encryption scheme.

2 RELATED WORK

In static threshold encryption schemes, a set of n recipients $\mathcal{V}$ and a threshold value t are predefined. In dynamic threshold encryption schemes, a set of n recipients $\mathcal{U}$ and the threshold t are defined arbitrarily by the sender.

Ghodosi et al. [10] presented the first dynamic threshold scheme, where the sender defines a set of recipients and the threshold value. In this scheme, the sender generates a polynomial, and

ARES '17, August 29-September 01, 2017, Reggio Calabria, Italy
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5257-4/17/08…$15.00
https://doi.org/10.1145/3098954.3103159

encrypts a polynomial value individually for each recipient. At least t recipients are required to decrypt their value in order for a combiner restore the encryption key. Hence, the ciphertext comprises $O(n)$ elements, one for each recipient, and it could be argued that this scheme is a "individual-oriented" threshold scheme. Other individual-oriented dynamic threshold schemes are found in [2, 9, 11, 18, 19].

Threshold broadcast encryption (TBE) schemes are characterized by ciphertexts less than $O(n)$ elements [5, 6, 12, 20, 23, 24]. Some authors refer to TBE schemes by the more general term dynamic threshold schemes [7, 20]. In TBE, the long term keys of the recipients constitute implicitly a secret polynomial, whereof a secret encryption key is deduced. The lowered number of elements of the ciphertext is obtained by sender computation of $n-t$ dummy shares that are computed by means of the public user keys. Some TBE schemes are identity-oriented, and are based on bilinear maps of elliptic curves [1, 2, 7, 20, 24]. The scheme presented in [7] replaces the mentioned dummy shares with dummy identities, and has thus constant size ciphertexts. The scheme presented in [20] has neither dummy shares nor dummy identities.

A dynamic threshold decryption scheme *without* a combiner was proposed in [18]. It is individual-oriented, i.e., the sender computes a ciphertext for each recipient, and decryption must be carried out by collaboration. The scheme was shown to be insecure [22]. A revised scheme was presented [11] that was followed by new attacks [14, 21].

As noted, a single combiner in conjunction with end-to-end-oriented secure channels do not comply with broadcast-oriented environments, where assumably all messages are to be broadcasted. Also all participants should be eligible to perform the combining function. To our best knowledge, this is the case for all existing TBE schemes.

2.1 Preliminaries

The threshold mechanism in TBE schemes is commonly based on Lagrange interpolation, and as such the well-known Shamir secret scheme. In this scheme, a predefined secret polynomial constitutes the basis for a shared secret.

TBE schemes are dynamic in the sense that there is no predefined secret polynomial. The basis for the threshold mechanism are randomly generated long-term user keys of each user $P_i \in \mathcal{V}$, associated to an arbitrarily-defined user coalition $\mathcal{V}$. The idea is that any set of user keys (denoted by $\mathcal{Y}$) implicitly constitute a polynomial $f_{\mathcal{Y}}$ in such a way that $m = |\mathcal{Y}|$ long-term user keys define points on the polynomial $f_{\mathcal{Y}}$. The polynomial is thus of order $m-1$.

The interpolation polynomial $f_{\mathcal{Y}}$ is computed as the sum of basis polynomials. A Lagrange basis polynomial is given by

$$\lambda_i^{\mathcal{Y}}(x) = \prod_{\substack{j\in\mathcal{Y}\\ i\neq j}} \frac{x-j}{i-j} = \sum_{j=0}^{m-1} c_{i,j}\, x^j \tag{1}$$

where each $c_{i,j}$ constitutes a polynomial coefficient in the expanded representation, and $j \in \mathcal{Y}$ denotes $(j \mid y_j \in \mathcal{Y})$. The interpolation polynomial is given by

$$\begin{aligned} f_{\mathcal{Y}}(z) &= \sum_{i\in\mathcal{Y}} x_i\, \lambda_i^{\mathcal{Y}}(z) = \sum_{i\in\mathcal{Y}} x_i \prod_{\substack{j\in\mathcal{Y}\\ i\neq j}} \frac{z-j}{i-j} \\ &= \sum_{i\in\mathcal{Y}} x_i \sum_{\substack{j=0\\ i\neq j}}^{m-1} c_{i,j}\, z^j \\ &= \sum_{i\in\mathcal{Y}} \Big(\sum_{\substack{j=0\\ i\neq j}}^{m-1} x_i\, c_{i,j} \Big)\, z^j \\ &= \sum_{j=0}^{m-1} \Big(\sum_{\substack{i\in\mathcal{Y}\\ i\neq j}} x_i\, c_{i,j} \Big) z^j = \sum_{j=0}^{m-1} a_j\, z^j \end{aligned} \tag{2}$$

Hence, the polynomial coefficients of $f_{\mathcal{Y}}$ are $a_j = \sum_{i\in\mathcal{Y}} x_i\, c_{i,j}$.

3 FULLY THRESHOLD BROADCAST ENCRYPTION

In this section, we present a threshold broadcast encryption scheme that does not require any secure channels, including in particular the combining phase. It is based on the TBE scheme proposed by Daza et al. [5], which, however, requires secure channels for a combiner in the combining step. Our scheme resolves the restriction of a single combiner and secure channels, and provides full broadcast-orientation that allows each legitimate recipient to decrypt.

3.1 FTBE algorithms

Let $\mathcal{U} = \{P_1, P_2, \ldots\}$ denote all registered users that each is assigned a long-term public/private key pair. The scheme proposed in this section consists of the following algorithms:

Initialization. The TA generates the public parameters $PP = (p, q, \alpha) = \mathrm{Init}(k)$, where k is a security parameter indicating the size of q.

Long-term user keys computation. Each user $P_i \in \mathcal{U}$ uses a randomized key generation algorithm, $(x_j, y_j) \leftarrow \mathrm{KeyGen}$ (p, q, α, i), $j \in \{2i, 2i+1\}$, to compute two key pairs, where x_j denotes the private key and y_j the public key.

Encryption. A sender selects ad hoc a set of recipients $\mathcal{V} \subseteq \mathcal{U}$, and a threshold value t, where $t \leq |\mathcal{V}|$.
Let $\mathcal{Y} = \{y_{2i}, y_{2i+1} \mid P_i \in \mathcal{V}\}$. The encryption algorithm $(\mathcal{Z}_D, s, k_{\mathcal{Y}}) \leftarrow \mathrm{Enc}(\mathcal{Y}, t, \alpha, p)$ is probabilistic, and produces a set of $2n-t-1$ ephemeral dummy shares $\mathcal{Z}_D$ for decryption.

Partial decryption. Exactly t recipients $P_i \in T \subseteq \mathcal{V}$, $t = |T|$, computes and broadcasts an ephemeral decryption share $z_{2i} \in \mathcal{Z}_T$ using the algorithm $z_{2i} \leftarrow \mathrm{PartDec}(x_{2i}, s, p)$.

Decryption. Each receiver $P_i \in \mathcal{V}$ uses the decryption algorithm $k_{\mathcal{Y}} \leftarrow \mathrm{Dec}(x_{2j+1}, s, \mathcal{Z}_D, \mathcal{Z}_T, p)$ for restoring the plaintext.

3.2 Security assumptions

Definition 1. Two computational problems related to the Discrete Logarithm Problem (DLP) are the Computational Diffie-Hellman (CDH) problem and the Decisional Diffie-Hellman (DDH) problem. It is considered that DDH problem is hard, and that the hardness of CDH and DLP is equivalent or harder than the DDH problem. The

DDH problem states that given the tuple $(\alpha^x, \alpha^y, \alpha^{xy})$ is computationally indistinguishable from $(\alpha^x, \alpha^y, \alpha^R)$, where $R \in Z_q$ is a random value.

Let z_1 be randomly assigned either α^{xy} or α^R, so that $z_1 \in \{\alpha^{xy}, \alpha^R\}$ and $z_2 \in \{\alpha^{xy}, \alpha^R\}\backslash\{z_1\}$. The DDH problem is the difficulty of selecting which number $z \in \{z_1, z_2\}$ that is associated with (α^x, α^y), so that $z = \alpha^{xy}$. The probability of selecting the correct value is $\frac{1}{2}$. Formally,

$$\left| Pr[\mathcal{A}(\alpha, \alpha^x, \alpha^y, z_1) = 1] - Pr[\mathcal{A}(\alpha, \alpha^x, \alpha^y, z_2) = 1] \right| \leq \epsilon(n)$$

where $\mathcal{A}$ is a polynomial-time adversary and $\epsilon(k)$ is a negligible function in the security parameter k. See e.g., [13, ch.7]. If it is secure against a single query, it is secure against q^* queries.

The security of the proposed scheme complies to indistinguishability under chosen plaintext attack (IND-CPA) for thresholds $t^* < t$, in agreement with the probabilistic ElGamal public key encryption scheme. An analysis is shown in Section 4. This can be modelled as interactions between a challenger C and a PPT adversary $\mathcal{A}$:

Setup. The challenger C runs KeyGen and submits the public keys $\{y_{2i}, y_{2i+1} \mid P_i \in \mathcal{U}\}$ and the private keys $\{x_{2i}, x_{2i+1} \mid P_i \in T^*\}$ to $\mathcal{A}$, where $t^* = |T^*|$ and $T^* \subset \mathcal{V}$.

Challenge. The challenger C computes a ciphertext $(\mathcal{Z}_D, s, k_{\mathcal{Y}}) \leftarrow \text{Enc}(\{y_{2i}, y_{2i+1} \mid P_i \in T\}, t, p)$, and generates a random secret integer w. C randomly selects a bit $b \in \{0, 1\}$, and selects $k_V^* = \{\alpha^w, k_{\mathcal{Y}}\}$ according to the random bit. C submits k_V^* to $\mathcal{A}$.

Guess. $\mathcal{A}$ outputs a bit b', where $\mathcal{A}$ correctly identifies that encipherment if $b' = b$.

The attack is said to be $\epsilon(n)$-distinguishable if the probability for it to succeed is negligible according to the mentioned DDH problem. It is assumed that the adversary $\mathcal{A}$ has access to the following sets of private and public user keys: $\{x_{2i}, x_{2i+1} \mid P_i \in T^*\}$, $\{y_{2i}, y_{2i+1} \mid P_i \in \mathcal{V}\}$.

3.3 A fully threshold broadcast encryption scheme

A sender wants to encrypt a message to an ad-hoc group of recipients $\mathcal{V} \subseteq \mathcal{U}$. The sender sets a threshold value t, where $n = |\mathcal{V}|$ and $t \leq n$. Decryption requires that exactly t users in $T \subseteq \mathcal{V}$ broadcast a partial decryption share, where $t = |T|$.

Encryption is realized by means of an encryption key that is computed using the public keys for each user in $\mathcal{V}$. Each user is represented by two public key pairs. The $2n$ public keys (denoted $\mathcal{Y}$) of the users in $\mathcal{V}$ define a polynomial $f_{\mathcal{Y}}$. The sender computes $2n{-}t{-}1$ ephemeral dummy shares and the encryption key given $f_{\mathcal{Y}}$. Exactly t recipients $T \subseteq \mathcal{V}$ broadcast each an ephemeral decryption share using the first private key. Hence, in total $2n{-}1$ shares are publicized, which is insufficient for outsiders to interpolate $f_{\mathcal{V}}$. Finally, each user in $\mathcal{V}$ computes privately another ephemeral decryption share using the second private key, sufficient to restore the encryption key.

Initialization. Let $\mathcal{U} = \{P_1, \ldots, P_n\}$ denote a group of n participants. A trusted authority (TA) selects two large public primes p and q so that $q \mid p - 1$, for instance, $p = 2q + 1$, and a generator α to $\mathbb{Z}_q$. Let k be the number of bits of q.

Key Setup. Each user $P_i \in \mathcal{U}$ is represented by two long-term key pairs $(x_j, y_j = \alpha^{x_j} \bmod p)$, $j = \{2i, 2i + 1\}$, where the private keys $x_j \in \mathbb{Z}_q$ are selected randomly.

Encryption. To encrypt a message to an ad-hoc group of recipients $\mathcal{V} \subseteq \mathcal{U}$, the sender carries out the following steps:

(1) The sender generates a random secret number $r \in \mathbb{Z}_q$.

(2) The exponents (i.e., the private keys) of the $2n$ public keys $\mathcal{Y} = \{y_{2i}, y_{2i+1} \mid P_i \in \mathcal{V}\}$ of the recipients of $\mathcal{V}$ constitute a polynomial f_Y. Using Lagrange interpolation (Eq. 2), the sender computes a secret encryption key

$$k_{\mathcal{Y}} = \alpha^{rf_{\mathcal{Y}}(0)} = \prod_{j \in \mathcal{Y}} y_j^{r\lambda_j^{\mathcal{Y}}(0)} \bmod p \tag{3}$$

where $\lambda_i^{\mathcal{Y}}(x)$ is defined in Eq. 1, and $f_{\mathcal{Y}}$ is of order $2n{-}1$. The notation $j \in \mathcal{Y}$ denotes indices $(j \mid y_j \in \mathcal{Y})$.

(3) The threshold security property is realized by a set of $2n{-}t{-}1$ ephemeral dummy shares

$$\mathcal{Z}_D = \Big\{z_i = \prod_{j \in \mathcal{Y}} y_j^{r\lambda_j^{\mathcal{Y}}(i)} \bmod p \mid i \notin \{j \in \mathcal{U}\}\Big\} \tag{4}$$

in agreement with Eq. 2, and where $z_i = \alpha^{rf_{\mathcal{Y}}(i)}$. The dummy shares must be unique, so that $\mathcal{Z}_D \cap \{y_j^r \mid j \in \mathcal{U}\} = \emptyset$, to assure that decryption is confined to the users in $\mathcal{V}$ only.

(4) The sender computes $s = \alpha^r \bmod p$, and encrypts the plaintext by means of $k_{\mathcal{Y}}$.

(5) The sender broadcasts the ciphertext and $(s, \mathcal{Z}_D)$.

Partial decryption. This phase requires the computations of exactly t recipients $T \subseteq \mathcal{V}$, where $t = |T|$. Each recipient $P_i \in T$ computes and broadcasts a partial decryption share $z_{2i} = s^{x_{2i}} \bmod p$. Let $\mathcal{Z}_T = \{z_{2j} \mid j \in T\}$ denote all t user shares.

Decryption. After having received each other's partial decryption shares, each user $P_i \in \mathcal{V}$ has $2n{-}1$ publicized ephemeral shares. He or she then computes a private decryption share $z_{2i+1} = s^{x_{2i+1}} \bmod p$. Possessing in total $2n$ ephemeral shares $\mathcal{Z}_i = \mathcal{Z}_D \cup \mathcal{Z}_T \cup \{z_{2i+1}\}$, he or she restores the encryption key

$$k_{\mathcal{Y}} = \prod_{j \in \mathcal{Z}_i} z_j^{\lambda_j^{\mathcal{Z}_i}(0)} = \alpha^{rf_{\mathcal{Y}}(0)} \bmod p \tag{5}$$

Lastly, the plaintext is recovered by means of the restored key.

Given $2n{-}1{-}t$ ephemeral dummy shares $\mathcal{Z}_D$ and t user shares $\mathcal{Z}_T$, in total $2n - 1$ publicized shares, is insufficient for outsiders $\mathcal{A} \notin \mathcal{V}$ to interpolate $f_{\mathcal{Y}}$, and hence to restore $k_{\mathcal{Y}}$.

3.4 Computational work

The number of modular exponentiations carried out for encryption by the sender is $2n(2n{-}t{-}1){+}2n{+}1 = 2n(2n{-}t){+}1$. Each recipient $P_j \in T$ carries out one modular exponentiation to compute a partial decryption share, and $2n$ modular exponentiations to compute $k_{\mathcal{Y}}$.

4 SECURITY ANALYSIS

The security of the presented scheme is based on the Shamir secret sharing and the ElGamal public key cryptosystem, which is based on the difficulty of the Decicional DH Problem.

Theorem 1. The proposed scheme is secure under an indistinguishable chosen plaintext attack (IND-CPA) in agreement with the DDH problem.

Proof (sketch). An attack is modelled as interactions between a challenger C and a PPT adversary $\mathcal{A}$. For the sake of simplicity, let the threshold t=n. In the setup phase, C runs KeyGen for $i \in \mathcal{V}=\{1 \ldots n\}$ for an imaginary group. C submits to $\mathcal{A}$ the public keys $\mathcal{Y} = \{y_{2i}, y_{2i+1} \mid i \in \mathcal{V}\}$, and n private keys $\mathcal{X} = \{x_{2i} \mid i \in \mathcal{V}\}$.

C computes a challenge $(\mathcal{Z}_D, s, c) \leftarrow \text{Enc}(\mathcal{Y}, n, \alpha, p)$. C randomly selects a bit b, and selects $k^*_{\mathcal{Y}} \in \{k_{\mathcal{Y}}, \alpha^w\}$ according to b, where $w \in \mathbb{Z}_q$ is a random value. C sends $(\alpha^{f_{\mathcal{Y}}(0)}, k^*_{\mathcal{Y}}, \mathcal{Z}_D, s = \alpha^r)$ to $\mathcal{A}$, whereof $f_{\mathcal{Y}}(0)$ and r are secret. Since $\mathcal{A}$ possesses $\mathcal{X}$, it can compute the corresponding decryption shares $\mathcal{Z}_{\mathcal{V}} = \{z_{2j} \mid j \in \mathcal{V}\}$ using PartDec. $\mathcal{A}$ possesses then $|\mathcal{Z}_D \cup \mathcal{Z}_{\mathcal{V}}| = 2n - 1 < 2n$ ephemeral shares.

Given the public keys $\{y_{2j+1} \mid j \in \mathcal{V}\}$ and $s = \alpha^r$, $\mathcal{A}$ is prevented from computing the corresponding ephemeral shares $\{\alpha^{rx_{2j+1}} \mid j \in \mathcal{V}\}$ due to the Computational Diffie-Hellman problem, which is equivalent in hardness to the DDH problem.

The number of ephemeral shares $\mathcal{Z}_{\mathcal{V}} \cup \mathcal{Z}_D$ possessed by $\mathcal{A}$ is less than the $2n$ coefficients of $f_{\mathcal{Y}}$, that is implicitly defined by $2n$ user keys. The algebraic equation system that the exponents of $\mathcal{Z}_{\mathcal{V}} \cup \mathcal{Z}_D$ constitute is underdefined (cp. Shamir secret sharing). $\mathcal{A}$ is thus prevented from interpolating $\alpha^{rf_{\mathcal{Y}}(0)}$.

Given that $\mathcal{A}$ can compute $Pr[\mathcal{A}(\alpha, \alpha^{f_{\mathcal{Y}}(0)}, \alpha^r, \alpha^{rf_{\mathcal{Y}}(0)}) = 1]$ if $k^*_{\mathcal{Y}} = \alpha^{rf_{\mathcal{Y}}(0)}$, and $Pr[\mathcal{A}(\alpha, \alpha^{f_{\mathcal{Y}}(0)}, \alpha^r, \alpha^w) = 0]$ if $k^*_{\mathcal{Y}} = \alpha^w$, this is equivalent to that $\mathcal{A}$ can solve the DDH problem. Since the DDH problem is known to be hard, the scheme is secure according to Theorem 1. □

Daza et al. [5] showed that their ElGamal-based TBE scheme scheme is secure concerning chosen plaintext attacks (CPA) and non-adaptive chosen ciphertext attacks (CCA1). Our scheme is equivalent with the Daza scheme concerning construction and security, where the principal difference between the two schemes is reflected by the respective $(n, 2n - t)$ and $(2n, 3n - t)$ threshold mechanisms, which is due to the doubled number of key pairs in our scheme.

In the Daza scheme, a set of n arbitrary public keys constitute a polynomial $f^*_{\mathcal{Y}}$ whereof $n - t$ dummy shares are interpolated. Hence, it agrees to a $(n, n+n-t) = (n, 2n-t)$ threshold mechanism. Our scheme uses a $(2n, 3n - t)$ threshold mechanism due to that the number of public keys are twice, i.e., $2n$. Hence, the polynomial $f_{\mathcal{Y}}$ that corresponds to the public keys has an order of $2n-1$, and not $n-1$. In our scheme are $2n-t-1$ ephemeral dummy shares and t partial decryption shares publicized, in total $2n - 1$, which is insufficient to interpolate on $f_{\mathcal{Y}}$, in agreement with Shamir secret sharing. Thus, $\mathcal{A} \notin \mathcal{V}$ is prevented from restoring the secret encryption key $k_{\mathcal{Y}}$. Each recipient $P_j \in \mathcal{V}$ is able to compute a private ephemeral share z_{2j+1}, and having in total $2n$ ephemeral shares, i.e., $\mathcal{Z}_D \cup \mathcal{Z}_T \cup \{z_{2j+1}\}$, computes $k_{\mathcal{Y}}$. Hence, a single combiner and secure channels are avoided.

In the Daza scheme, in contrast, $n - t$ ephemeral dummy shares are publicized, and t partial decryption shares are submitted to a combiner protected by secure channels. Only the combiner having the n shares that agrees with the pertaining polynomial $f^*_{\mathcal{Y}}$ can then decrypt.

Given that our scheme is equivalent with the Daza scheme except the respective $(n, 2n - t)$ and $(2n, 3n - t)$ threshold mechanisms, our scheme is therefore as secure as the Daza scheme, which is shown to be as secure as the ElGamal public key cryptosystem.

5 CONCLUSION

Threshold broadcast encryption (TBE) allows a sender to compute ciphertexts to ad hoc user groups. Existing TBE schemes require that partial decryptions from each user are transferred to a single combiner through secure channels. We have pointed out that a single combiner that requires secure channels, and that becomes the eventual target for the restored plaintext, and not the addressed group, are properties of TBE that are inconsistent with broadcast-orientation.

In this paper, we have proposed a fully TBE scheme, where no single combiner and secure channels are required. Exactly t of the sender-addressed recipients broadcast their partial decryptions, and only the sender-addressed users are able to securely decrypt the ciphertext subsequently.

The scheme is equivalent with [5] concerning construction and security, where the difference is that [5] uses a $(n, 2n - t)$ threshold mechanism, and our scheme uses a $(2n, 3n-t)$ threshold mechanism in order to achieve fully TBE.

REFERENCES

[1] Joonsang Baek and Yuliang Zheng. 2004. *Identity-Based Threshold Decryption.* Springer Berlin Heidelberg, Berlin, Heidelberg, 262–276.

[2] Zhenchuan Chai, Zhenfu Cao, and Yuan Zhou. 2006. Efficient ID-based Broadcast Threshold Decryption in Ad Hoc Network. In *Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences - Volume 2 (IMSCCS'06) - Volume 02 (IMSCCS '06).* IEEE Computer Society, Washington, DC, USA, 148–154.

[3] Ivan Damgård and Mats Jurik. 2001. A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography (PKC '01).* Springer-Verlag, London, UK, UK, 119–136.

[4] Ivan Damgård and Mads Jurik. 2003. *A Length-Flexible Threshold Cryptosystem with Applications.* Springer Berlin Heidelberg, Berlin, Heidelberg, 350–364.

[5] Vanesa Daza, Javier Herranz, R. Molva, Paz Morillo, and Carla RÃăfols. 2008. Ad-Hoc Threshold Broadcast Encryption with Shorter Ciphertexts. *Electronic Notes in Theoretical Computer Science. Proceedings of theThird Workshop on Cryptography for Ad-hoc Networks (WCAN 2007)* 192, 2 (2008), 3 – 15.

[6] Vanesa Daza, Javier Herranz, Paz Morillo, and Carla Ràfols. 2007. *CCA2-Secure Threshold Broadcast Encryption with Shorter Ciphertexts.* Springer Berlin Heidelberg, Berlin, Heidelberg, 35–50.

[7] Cécile Delerablée and David Pointcheval. 2008. *Dynamic Threshold Public-Key Encryption.* Springer Berlin Heidelberg, Berlin, Heidelberg, 317–334.

[8] Yvo Desmedt. 1993. *Threshold cryptosystems.* Springer Berlin Heidelberg, Berlin, Heidelberg, 1–14.

[9] Yevgeniy Dodis and Jonathan Katz. 2005. *Chosen-Ciphertext Security of Multiple Encryption.* Springer Berlin Heidelberg, Berlin, Heidelberg, 188–209.

[10] H. Ghodosi, Josef Pieprzyk, and Rei Safavi-naini. 1996. Dynamic Threshold Cryptosystems. In *in Proceedings of PRAGOCRYPT '96 –International Conference on the Theory and Applications of Cryptology.* 370–379.

[11] Hossein Ghodosi and Shahrokh Saeednia. 2001. Modification to self-certified group-oriented cryptosystem without combiner. *Electronics Letters* 37 (2001), 86–87.

[12] Kerem Kaskaloglu, Kamer Kaya, and Ali Aydin Selcuk. 2007. Threshold broadcast encryption with reduced complexity. In *Computer and information sciences, 2007. iscis 2007. 22nd international symposium on.* IEEE, 1–4.

[13] Jonathan Katz and Yehuda Lindell. 2008. *Introduction to Modern Cryptography.* Chapman & Hall/CRC. Hardcover.

[14] Wei-Bin Lee and Kuan-Chieh Liao. 2006. Improved Self-certified Group-oriented Cryptosystem Without a Combiner. *J. Syst. Softw.* 79, 4 (April 2006), 502–506.

[15] Roel Peeters, Svetla Nikova, and Bart Preneel. 2008. Practical RSA Threshold Decryption for Things That Think. In *3rd Benelux Workshop on Information and System Security (WISSec 2008)*. Eindhoven,NL, 16.

[16] Bo Qin, Qianhong Wu, Lei Zhang, and Josep Domingo-Ferrer. 2010. *Threshold Public-Key Encryption with Adaptive Security and Short Ciphertexts*. Springer Berlin Heidelberg, Berlin, Heidelberg, 62–76.

[17] Bo Qin, Qianhong Wu, Lei Zhang, Oriol FarrÃăs, and Josep Domingo-Ferrer. 2012. Provably secure threshold public-key encryption with adaptive security and short ciphertexts. *Information Sciences* 210 (2012), 67 – 80.

[18] Shahrokh Saeednia and Hossein Ghodosi. 1999. *A Self-Certified Group-Oriented Cryptosystem without a Combiner*. Springer, Berlin, Heidelberg, 192–201.

[19] Yusuke Sakai, Keita Emura, Jacob C.N. Schuldt, Goichiro Hanaoka, and Kazuo Ohta. 2015. *Dynamic Threshold Public-Key Encryption with Decryption Consistency from Static Assumptions*. Springer International Publishing, Cham, 77–92.

[20] Willy Susilo, Fuchun Guo, and Yi Mu. 2016. Efficient dynamic threshold identity-based encryption with constant-size ciphertext. *Theor. Comput. Sci.* 609 (2016), 49–59. https://doi.org/10.1016/j.tcs.2015.09.006

[21] Willy Susilo and Hiroaki Kikuchi. 2007. Cryptanalysis of Modification to Self-Certified Group-Oriented Cryptosystem without A Combiner. *I. J. Network Security* 4, 3 (2007), 288–291. http://ijns.femto.com.tw/contents/ijns-v4-n3/ijns-2007-v4-n3-p288-291.pdf

[22] W. Susilo and R. Safavi-Naini. 1999. Remark on self-certified group-oriented cryptosystem without a combiner. *Electronics Letters* 35 (1999), 1539–1540.

[23] P. Yang, Z. Cao, and X. Dong. 2009. A Dependable Threshold Broadcast Encryption System for Key Distribution in Mobile Ad Hoc Network. In *Dependability, 2009. DEPEND '09. Second International Conference on*. 1–6.

[24] Leyou Zhang, Yupu Hu, and Qing Wu. 2010. Identity-based Threshold Broadcast Encryption in the Standard Model. *KSII Transactions on Internet & Information Systems* 4, 3 (2010).