IEICE TRANS. INF. & SYST., VOL.E93–D, NO.12 DECEMBER 2010

LETTER

Improvement of the Efficient Secret Broadcast Scheme

Eun-Jun YOON[†a)], **Muhammad KHURRAM KHAN**[††b)], ***and*** **Kee-Young YOO**[†c)], ***Members***

SUMMARY In 2009, Jeong et al. proposed a secure binding encryption scheme and an efficient secret broadcast scheme. This paper points out that the schemes have some errors and cannot operate correctly, contrary to their claims. In addition, this paper also proposes improvements of Jeong et al.'s scheme that can withstand the proposed attacks.

key words: *broadcasting network, secret broadcast, binding encryption, message consistency, security*

1. Introduction

An efficient secret broadcast problem is one of the basic problems in the broadcasting networks. In order to perform secret broadcast, a sender must broadcast a message secretly and consistently to the receivers. And also, a receiver must assure that all of the other receivers have also received the exact same message. However, it is not easy work to develop such a broadcast scheme [1], [2].

Quite recently, Jeong et al. [3] proposed a secure binding encryption scheme against chosen plaintext attacks in the standard model [4]. They also proposed an efficient secret broadcast scheme based on the binding encryption scheme. However, Jeong et al. schemes cannot perform correctly. This paper shows that there are two serious mistakes in Jeong et al.'s schemes as follows: (1) The encryption/decryption algorithms of their schemes do not perform correctly; (2) The schemes do not meet the requirement of message consistency unlike their claims. As a result, Jeong et al.'s schemes are impractical. To eliminate the security problems, this paper also proposes improvements of Jeong et al.'s scheme. Compared with Jeong et al.'s scheme, the proposed scheme can be used for the broadcasting networks because it is more secure and efficient.

2. Review of Jeong et al.'s Scheme

This section reviews Jeong et al.'s [3] binding encryption scheme and efficient secret broadcast scheme, respectively.

Manuscript received June 1, 2010.
Manuscript revised August 11, 2010.

[†]The authors are with the School of Electrical Engineering and Computer Science, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702–701, South Korea.
[††]The author is with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Kingdom of Saudi Arabia.
a) E-mail: ejyoon@knu.ac.kr
b) E-mail: mkhurram@ksu.edu.sa
c) E-mail: yook@knu.ac.kr
DOI: 10.1587/transinf.E93.D.3396

2.1 Binding Encryption Scheme in Standard Model

Let $\mathsf{SE} = (\mathsf{SE.key}, \mathsf{SE.enc}, \mathsf{SE.dec})$ be a symmetric encryption scheme. $\mathsf{SE.key}(1^\theta)$ generates a key k. $\mathsf{SE.enc}_k(m)$ encrypts the message m with the key k. $\mathsf{SE.dec}_k(c)$ decrypts the ciphertext c with the key k. The public-key encryption scheme $\mathsf{PE} = (\mathsf{PE.key}, \mathsf{PE.enc}, \mathsf{PE.dec})$ should satisfy completeness as follows: If $(pk, sk) \leftarrow \mathsf{PE.key}(1^\theta)$, $c = \mathsf{PE.enc}_{pk}(m)$, and $m' = \mathsf{PE.dec}_{sk}(c)$, then the equation $m = m'$ always holds for any m. To make probabilistic public-key encryption scheme, the scheme uses the notation $c = \mathsf{PE.enc}_{pk,r}(m)$ to explicitly denote that a random string r is used to make the ciphertext c. This means that a ciphertext c should be generated using an independently and randomly selected string r. Let $\mathsf{F}_K : \{0,1\}^\theta \rightarrow \{0,1\}^\theta$ be a function selected from a function family F, where $\mathsf{F} = \{\mathsf{F}_K | K$ is in the space of θ-bit strings$\}$.

Let $\mathsf{BE} = (\mathsf{BE.key}, \mathsf{BE.enc}, \mathsf{BE.dec})$ be a binding encryption scheme. $\mathsf{BE.key}$ generates a pair of public-/private-keys for a party. $\mathsf{BE.enc}$ encrypts a plaintext using the public keys of a set of receivers. $\mathsf{BE.dec}$ decrypts a ciphertext using one of the secret keys of the receivers and outputs a plaintext if the ciphertext is valid or $\perp$ otherwise.

- $\mathsf{BE.key}(1^\theta)$: A party P_i runs this algorithm to generate a pair of public-/private-keys (pk_i, sk_i).
  1. The algorithm uses the key generation algorithm of a public-key encryption scheme.
  2. The algorithm gets $(pk_i, sk_i) \leftarrow \mathsf{PE.key}(1^\theta)$ and outputs (pk_i, sk_i).
- $\mathsf{BE.enc}_{pk_1,\ldots,pk_n}(m)$: This algorithm produces a ciphertext for a message m.
  1. The algorithm randomly selects $k_e, k_f \leftarrow \{0,1\}^\theta$ and calculates $c_0 \leftarrow \mathsf{SE.enc}_{k_e}(m)$
  2. For $1 \le i \le n$, the algorithm calculates the followings:
  $$\begin{aligned} r_i &\leftarrow \mathsf{F}_{k_f}(i) \\ c_i &\leftarrow \mathsf{PE.enc}_{pk_i,r_i}(k_e) \\ d_i &\leftarrow \mathsf{PE.enc}_{pk_i}(k_f) \end{aligned} \quad (1)$$
  3. The algorithm outputs a ciphertext (Γ, σ), where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (c_0, c_1, \ldots, c_n, d_1, \ldots, d_n)$.

- $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$: This algorithm extracts a plaintext from the ciphertext (Γ, σ) using the private key sk_i.
  1. The algorithm first extracts the followings:
  $$k'_e \leftarrow \mathsf{PE.dec}_{sk_i}(c_i) \quad (2)$$
  $$k'_f \leftarrow \mathsf{PE.dec}_{sk_i}(d_i)$$
  2. For $1 \le i \le n$, the algorithm extracts and tests the followings:
  $$r'_i \leftarrow \mathsf{F}_{k'_f}(i) \quad (3)$$
  $$c_i \stackrel{?}{=} \mathsf{PE.enc}_{pk_i, r'_i}(k'_e) \quad (4)$$
  3. If the test is not successful, the algorithm outputs $\perp$. Otherwise, the algorithm extracts the followings:
  $$m' \leftarrow \mathsf{SE.dec}_{k'_e}(c_0) \quad (5)$$
  and outputs m'.

2.2 Efficient Secret Broadcast Scheme

Let BE = (BE.key, BE.enc, BE.dec) be a binding encryption scheme which is described in the above Sect. 2.1. Figure 1 illustrates Jeong et al.'s efficient 1-round secret broadcast scheme and runs as follows:

1. Assume that a sender wants to send a secret message m to the receivers $(P_1, \ldots, P_n)$ in the broadcasting networks. We also assume that P_i has a pair of public-/private-keys (pk_i, sk_i) for the binding encryption scheme BE.
2. Sender $\rightarrow$ Each Receiver P_i: (Γ, σ)
   a. The sender first makes the followings:
   $$(\Gamma, \sigma) \leftarrow \mathsf{BE.enc}_{pk_1, \ldots, pk_n}(m) \quad (6)$$
   where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (c_0, c_1, \ldots, c_n, d_1, \ldots, d_n)$.

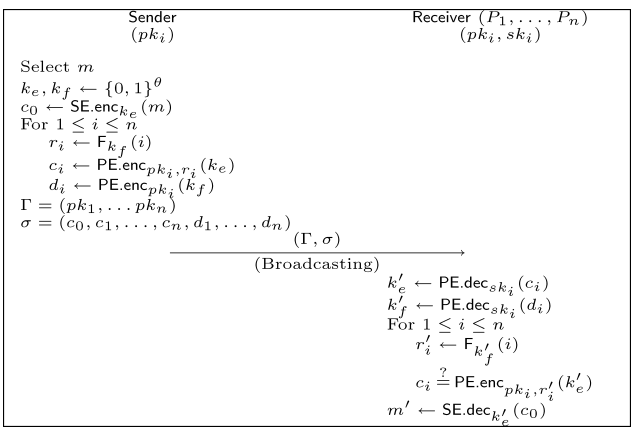

Fig. 1 Jeong et al.'s efficient secret broadcast scheme.

   b. The sender broadcasts (Γ, σ) to the receivers in the broadcasting networks.
3. Each receiver P_i extracts $m' \leftarrow \mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ from the ciphertext (Γ, σ).

3. Cryptanalysis of Jeong et al.'s Scheme

This section proves that there are two mistakes in Jeong et al.'s scheme: (1) The encryption/decryption algorithms do not perform correctly; (2) The scheme does not meet the requirement of message consistency unlike their claims.

3.1 Incorrect Binding Encryption Scheme

Jeong et al.'s binding encryption scheme has a serious problem. That is, the encryption/decryption algorithms of their scheme cannot be correctly performed for secret broadcast. In $\mathsf{BE.enc}_{pk_1, \ldots, pk_n}(m)$ algorithm, the algorithm calculates c_i (for $1 \le i \le n$) as follows (see above Eq. (1)):

$$c_i \leftarrow \mathsf{PE.enc}_{pk_i, r_i}(k_e)$$

In $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm, the algorithm extracts k'_e by using the private key sk_i as follows (see above Eq. (2)):

$$k'_e \leftarrow \mathsf{PE.dec}_{sk_i}(c_i)$$

From the above Eqs. (1) and (2), we can easily see that the $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm cannot extract a correct k'_e by using the private key sk_i. From Eq. (1), k_e is encrypted by using the private key sk_i and r_i, where $r_i \leftarrow \mathsf{F}_{k_f}(i)$ and $k_f \leftarrow \{0,1\}^\theta$ is randomly selected value. From Eq. (2), $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm just uses its private key sk_i to extract k'_e from c_i. However, without knowing r_i, it is impossible to obtain the correct k'_e form c_i. So, the above Eq. (2) must be changed to correctly extract the k'_e from c_i as follows:

$$k'_e \leftarrow \mathsf{PE.dec}_{sk_i, r_i}(c_i) \quad (7)$$

However, r_i is computed by $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm after extract k'_e as follows (see above Eq. (3)):

$$r'_i \leftarrow \mathsf{F}_{k'_f}(i)$$

for $1 \le i \le n$. So, $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm cannot compute Eq. (7) because r'_i cannot be computed in advance easily. As a result, although $\mathsf{BE.enc}_{pk_1, \ldots, pk_n}(m)$ algorithm sends a valid ciphertext (Γ, σ), $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm will always output $\perp$ because the ciphertext (Γ, σ) cannot pass the following verification equation (see above Eq. (4)):

$$c_i \stackrel{?}{=} \mathsf{PE.enc}_{pk_i, r'_i}(k'_e)$$

Obviously, Jeong et al.'s binding encryption scheme is incorrectly designed. Since Jeong et al.'s efficient secret broadcast scheme as shown in Fig. 1 is basically operated by their binding encryption scheme, it automatically inherits the same design flaws as described above.

3.2 Message Consistency Problem

Jeong et al. insisted that their proposed schemes provide message consistency. Message consistency means that each receiver can assure that all of the receivers have received the same message. However, Jeong et al.'s schemes do not meet the requirement of message consistency unlike their claims. In the binding encryption scheme, an adversary $\mathcal{A}$ can compute a forged c_0^* as follows:

$$c_0^* \leftarrow \mathsf{SE.enc}_{k_e^*}(m^*) \tag{8}$$

to break the message consistency, where $k_e^* \leftarrow \{0,1\}^\theta$ and m^* are a random value and a fake message chosen by $\mathcal{A}$, respectively. $\mathcal{A}$ can intercept a ciphertext (Γ, σ), where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (c_0, c_1, \ldots, c_n, d_1, \ldots, d_n)$. It is easy to obtain the information since these values are readily available over the open network. Upon intercepting (Γ, σ), $\mathcal{A}$ replaces the intercepted c_0 with its computed c_0^*. $\mathcal{A}$ then broadcasts (Γ, σ^*), where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma^* = (c_0^*, c_1, \ldots, c_n, d_1, \ldots, d_n)$. In here, we assume that Jeong et al.'s binding encryption scheme is performed correctly without the design flaws as described above.

Upon receiving (Γ, σ^*), $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma^*)$ algorithm will extract m^{**} by decrypting c_0^* as follows (see above Eq. (5)):

$$m^{**} \leftarrow \mathsf{SE.dec}_{k_e'}(c_0^*) \tag{9}$$

From the above Eqs. (8) and (9), we can easily see that $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma^*)$ algorithm cannot obtain the original message m despite the satisfaction of the verification equation (4) for the decryption key k_e' because the algorithm does not check the integrity of the forged fake message m^*.

Moreover, for each receiver $(P_1, \ldots, P_n)$, $\mathcal{A}$ can send different fake messages m_i^* (for $1 \le i \le n$) to break the message consistency which receive different messages to all of the receivers. Obviously, Jeong et al.'s binding encryption scheme does not meet the requirement of message consistency. Jeong et al.'s efficient secret broadcast scheme automatically inherits the same problem as described above because it is basically operated by their binding encryption scheme.

4. Proposed Scheme

This section proposes an improvement of Jeong et al.'s [3] binding encryption scheme and efficient secret broadcast scheme, respectively.

4.1 Proposed Binding Encryption Scheme

In the proposed binding encryption scheme, the system setup environments are same as Jeong et al.'s schemes. The proposed binding encryption scheme performs as follows:

- $\mathsf{BE.key}(1^\theta)$: A party P_i runs this algorithm to generate a pair of public-/private-keys (pk_i, sk_i).
  1. The algorithm uses the key generation algorithm of a public-key encryption scheme.
  2. The algorithm gets $(pk_i, sk_i) \leftarrow \mathsf{PE.key}(1^\theta)$ and outputs (pk_i, sk_i).
- $\mathsf{BE.enc}_{pk_1,\ldots,pk_n}(m)$: This algorithm produces a ciphertext for a message m.
  1. The algorithm randomly selects $k_e \leftarrow \{0,1\}^\theta$.
  2. The algorithm calculates the followings:
  $$c_0 \leftarrow \mathsf{SE.enc}_{k_e}(m) \tag{10}$$
  3. For $1 \le i \le n$, the algorithm calculates the followings:
  $$c_i \leftarrow \mathsf{PE.enc}_{pk_i}(k_e, m) \tag{11}$$
  4. The algorithm outputs a ciphertext (Γ, σ), where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (c_0, c_1, \ldots, c_n)$.
- $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$: This algorithm extracts a plaintext from the ciphertext (Γ, σ) using the private key sk_i.
  1. The algorithm first extracts the followings:
  $$k_e' \leftarrow \mathsf{PE.dec}_{sk_i}(c_i) \tag{12}$$
  2. The algorithm extracts the message m' as follow:
  $$m' \leftarrow \mathsf{SE.dec}_{k_e'}(c_0) \tag{13}$$
  3. For $1 \le i \le n$, the algorithm extracts and tests the followings:
  $$c_i \stackrel{?}{=} \mathsf{PE.enc}_{pk_i, r_i'}(k_e', m') \tag{14}$$
  4. If the test is not successful, the algorithm outputs $\perp$. Otherwise, the algorithm accepts the message m'.

4.2 Proposed Efficient Secret Broadcast Scheme

Let BE = (BE.key, BE.enc, BE.dec) be a binding encryption scheme which is described in the above Sect. A. Figure 2 illustrates the proposed efficient 1-round secret broadcast scheme and runs as follows:

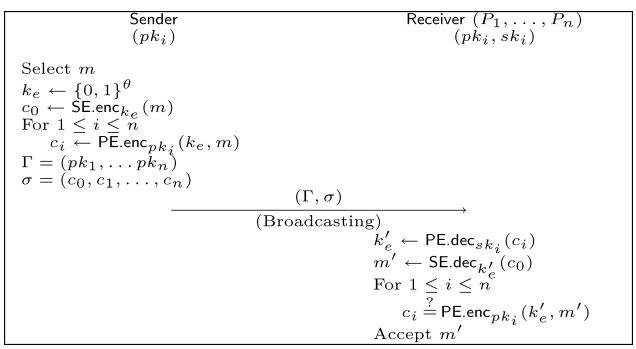

Fig. 2 Proposed efficient secret broadcast scheme.

1. Assume that a sender wants to send a secret message m to the receivers $(P_1, \ldots, P_n)$ in the broadcasting networks. We also assume that P_i has a pair of public-/private-keys (pk_i, sk_i) for the binding encryption scheme BE.
2. Sender $\rightarrow$ Each Receiver P_i: (Γ, σ)
   a. The sender first makes the followings:
   $$(\Gamma, \sigma) \leftarrow \mathsf{BE.enc}_{pk_1,\ldots,pk_n}(m) \quad (15)$$
   where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (c_0, c_1, \ldots, c_n)$.
   b. The sender broadcasts (Γ, σ) to the receivers in the broadcasting networks.
3. Each receiver P_i extracts and verifies m' from the ciphertext (Γ, σ) by using $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ as follows:
   $$m' \leftarrow \mathsf{BE.dec}_{sk_i}(\Gamma, \sigma) \quad (16)$$

5. Security and Efficiency Analysis

5.1 Security Analysis

This subsection will only discuss the enhanced security features of the proposed scheme. The other features are the same as original Jeong et al.'s scheme.

1. *The proposed encryption/decryption algorithms can be perform correctly.* The random value r_i is not used in the proposed binding encryption scheme unlike Jeong et al.'s scheme. The proposed binding encryption scheme uses only one random value k_e to provide the message freshness. Since Eq. (10) in the proposed $\mathsf{BE.enc}_{pk_1,\ldots,pk_n}(m)$ algorithm and (12) in the proposed $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm are always identical, the message m' can be correctly verified by each receiver by using the verification equation (14). As a result, the proposed encryption/decryption algorithms can be perform correctly and secure. Since the proposed efficient secret broadcast scheme as shown in Fig. 2 is basically operated by the proposed binding encryption scheme, it automatically can be perform correctly and secure.
2. *The proposed schemes meet the requirement of message consistency.* In the proposed binding encryption scheme, an adversary $\mathcal{A}$ can compute a forged $c_0^* \leftarrow \mathsf{SE.enc}_{k_e^*}(m^*)$ to break the message consistency, where $k_e^* \leftarrow \{0,1\}^\theta$ and m^* are a random value and a fake message chosen by $\mathcal{A}$, respectively. Suppose that $\mathcal{A}$ replaces the intercepted c_0 with its computed c_0^* upon intercepting (Γ, σ) and then broadcasts (Γ, σ^*), where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma^* = (c_0^*, c_1, \ldots, c_n)$. However, in the proposed $\mathsf{BE.dec}_{sk_i}(\Gamma, \sigma)$ algorithm, each receiver always verifies the integrity of the decrypted message m' by performing the verification process $c_i \stackrel{?}{=} \mathsf{PE.enc}_{pk_i}(k'_e, m')$ (see above Eq. (14)). Therefore, the faked message m^* is always rejected by each receiver $(P_1, \ldots, P_n)$. Thus, the proposed schemes meet the requirement of message consistency.

Table 1 Comparison results of the computational costs.

	DC	Security Model	Computation
K [1]	X	Random Oracle	enc.: nPE.enc
			dec.: 1PE.dec
VT [2]	O	Random Oracle	enc.: $(2n+1)$Exp.
			dec.: $2n$Exp.
JKL [3]	X	Standard	enc.: $2n$PE.enc
			dec.: nPE.enc + 2PE.dec
Proposed	O	Standard	enc.: nPE.enc
			dec.: nPE.enc + 1PE.dec

DC: Decryption Consistency.
enc.: Computational costs for encryption by a sender.
dec.: Computational costs for decryption by a receiver.
Exp.: Modular exponentiation.

5.2 Efficiency Analysis

Table 1 shows the comparison results of the computational costs of the proposed scheme and of various multi-receiver encryption schemes [1]–[3]. As shown in Table 1, we can see that the proposed scheme has the smallest computational workloads compare with Jeong et al.'s multi-receiver encryption scheme.

6. Conclusions

This paper pointed out two serious mistakes in Jeong et al.'s schemes: (1) An incorrect design of the secret broadcast scheme; (2) A message consistency problem. To eliminate the security problems of Jeong et al.'s schemes, this paper also proposed improvements of the scheme. As a result, compared with Jeong et al.'s scheme, the proposed scheme can be used for the broadcasting networks because it is more secure and efficient.

References

[1] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," Proc. PKC'02, LNCS 2274, pp.48–63, 2002.
[2] E.R. Verheul and H.C.A. van Tilborg, "Binding ElGamal: A fraud-detectable alternative to key-escrow proposals," Proc. EUROCRYPT 1997, LNCS 1233, pp.119–133, 1997.
[3] I.R. Jeong, J.O. Kwon, and D.H. Lee, "Efficient secret broadcast in the broadcasting networks," IEEE Commun. Lett., vol.13, no.12, pp.1001–1003, 2009.
[4] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable random-oracle-model scheme for a hybrid-encryption problem," Proc. EUROCRYPT'04, LNCS 3027, pp.171–188, 2004.