IEICE TRANS. INF. & SYST., VOL.E95–D, NO.2 FEBRUARY 2012

LETTER

Analysis and Improvement of a Secret Broadcast with Binding Encryption in Broadcasting Networks

Mingwu ZHANG[†,††a)], ***Nonmember***, **Fagen LI**[††], ***and*** **Tsuyoshi TAKAGI**[††], ***Members***

SUMMARY A secret broadcasting scheme deals with secure transmission of a message so that more than one privileged receiver can decrypt it. Jeong et al. proposed an efficient secret broadcast scheme using binding encryption to obtain the security properties of IND-CPA semantic security and decryption consistency. Thereafter, Wu et al. showed that the Jeong et al.'s scheme just achieves consistency in relatively weak condition and is also inefficient, and they constructed a more efficient scheme to improve the security. In this letter, we demonstrate that the Wu et al.'s scheme is also a weak decryption consistency and cannot achieve the decryption consistency if an adversary has the ability to tamper with the ciphertext. We also present an improved and more efficient secret broadcast scheme to remedy the weakness. The proposed scheme achieves decryption consistency and IND-CCA security, which can protect against stronger adversary's attacks and allows us to broadcast a digital message securely.

key words: *secret broadcast, binding encryption, public key, decryption consistency*

1. Introduction

Broadcast encryption is an interesting application of cryptography which allows one to broadcast a secret to a changing group of intended recipients in such a way that no one outside this group can view the secret, which is a cryptographic problem of encrypting broadcast content (e.g. TV programs) in such a way that only authorized users can decrypt the content. It allows to broadcast a digital message to multiple users secretly. That is to say, broadcasting a secret to a dynamically changing set of intended recipients in such a way that no one outside this set can recover the secret.

In a public broadcasting network, it is very important to broadcast a message to multiple receivers with the security requirements of secrecy and consistency. Secrecy means that only the designated receivers can extract the original message. Consistency means that the receivers can assure that all of the receivers have exactly the same message. However, it is not easy to guarantee both consistency and secrecy at the same time in a broadcasting network.

Verheul and Tilborg [1] proposed a binding encryption scheme achieves provable security in the random oracle model. Gentry and Waters [2] designed a fully collusion-resistant broadcast scheme and proposed a security model to obtain adaptive security, where the adversary can corrupt all the users, except the target users. Jeong et al. [3] constructed a binding encryption scheme with security proof in the standard model. However, Wu et al. [4] showed that the Jeong et al.'s scheme just achieves consistency in a relatively secure model but not in a stronger model. Furthermore, they pointed out the Jeong et al.'s scheme is inefficient in communication load and computation cost even when their model is accepted. Thereafter, they proposed a simple and more efficient scheme.

In this letter, we first indicate that the Wu et al.'s scheme [4] (WZP scheme) can not achieve the security requirement of decryption consistency. Furthermore, we also propose an improved version that attains the IND-CCA semantic security and decryption consistency, simultaneously.

2. Review and Analysis of the WZP Secret Broadcast Scheme

Let θ be a security parameter, and $\{0,1\}^\theta$ be the set of θ-bit strings. We denote $x \xleftarrow{\$} Z_q$ as x is randomly selected from Z_q. It also uses a public encryption scheme PE that is a triple of polynomial algorithms $PE = (PE.key, PE.enc, PE.dec)$, where $PE.key(1^\theta)$ generates a key (pk, sk); $PE.enc_{pk}(m)$ encrypts the message m with public key pk; and $PE.dec_{sk}(c)$ decrypts the ciphertext c with private key sk. In the WZP scheme, it assumes that the public-key encryption scheme PE in use has an additional property that the public/private key pair can be easily verified.

2.1 The WZP Scheme

The WZP secret broadcast encryption scheme [4] is described as follows:

- BE.key(1^θ): A party $P_i (1 \le i \le n)$ runs this algorithm to generate a pair of public-/private-keys $[pk_i, sk_i]$. This algorithm uses the key generation algorithm of a public-key encryption scheme PE. The algorithm gets $[pk_i, sk_i] \leftarrow PE.key(1^\theta)$ and outputs $[pk_i, sk_i]$.
- BE.enc$_{pk_1,\ldots,pk_n}(m)$: It first uses $PE.key$ to get another pair of PE's public-/private-keys $[pk_0, sk_0]$. Then the algorithm calculates $c_0 \leftarrow PE.enc_{pk_0}(m)$. For $i = 1, \ldots, n$, it also computes $c_i \leftarrow PE.enc_{pk_i}(sk_0)$, and outputs a ciphertext $C = [\Gamma, \sigma]$ where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (pk_0, c_0, c_1, \ldots, c_n)$.
- BE.dec$_{sk_i}(\Gamma, \sigma)$: It first extracts $sk'_0 \leftarrow PE.dec_{sk_i}(c_i)$ and check if (pk_0, sk'_0) is a correct pair of PE's

Manuscript received September 15, 2011.
Manuscript revised October 27, 2011.

[†]The author is with College of Information, South China Agri University, China.
[††]The authors are with Institute of Mathematics for Industry, Kyushu University, Fukuoka-shi, 819–0395 Japan.
a) E-mail: mwzhang@imi.kyushu-u.ac.jp

DOI: 10.1587/transinf.E95.D.686

public-/private-keys. It outputs the extracted message by $m' \leftarrow PE.dec_{sk'_0}(c_0)$ if the test is successful, and outputs $\perp$ as failure otherwise.

2.2 Security Model

In [4], the authors declared that their scheme has the security requirement of a binding encryption: semantic secure (IND-CPA/CCA) and decryption consistency (DC). Informally, IND-CPA/CCA means that any adversary cannot get any information of the plaintext from a ciphertext, and DC intends that any adversary cannot make a ciphertext such that the receivers extract different messages from this same ciphertext.

Definition 1: COMPLETENESS If $(pk, sk) \leftarrow PE.key(1^\theta)$, $C = PE.enc_{pk}(m)$, and $m' = PE.dec_{sk}(C)$, then the equation $m' = m$ always holds for any m.

Definition 2: IND-CCA A secret broadcast public-key encryption BE is secure against adaptive chosen-ciphertext attacks (IND-CCA) if the advantage of any ppt adversary $\mathcal{A}$ is negligible in the following game:

1. $BE.key(1^\theta)$ outputs (pk, sk), and adversary $\mathcal{A}$ is given 1^θ and pk.
2. $\mathcal{A}$ may make polynomially-many queries to a decryption oracle $BE.dec(\cdot)$.
3. At some point, $\mathcal{A}$ outputs two messages m_0, m_1 with $|m_0| = |m_1|$. A bit b is randomly chosen and the adversary is given a challenge ciphertext $C \leftarrow BE.enc(m_b)$.
4. $\mathcal{A}$ may continue to query its decryption oracle $BE.dec(\cdot)$ except that it may not request the decryption of C.
5. Finally, $\mathcal{A}$ outputs a guess b.

We say that $\mathcal{A}$ succeeds the guess, and denote the probability of this event by $Pr_{A,PKE}[Succ]$. The adversary's advantage is defined as $|Pr^{\text{IND-CCA}}_{\mathcal{A},PE}[Succ] - \frac{1}{2}|$.

Definition 3: IND-CPA A secret broadcast public-key encryption scheme BE is secure against chosen-plaintext attacks (IND-CPA) if an adversary $\mathcal{A}$ is unable to make query to the decryption oracle in steps (2) and (4) in the game of definition 2, and the advantage of $\mathcal{A}$ is negligible.

Definition 4: DECRYPTION CONSISTENCY Decryption consistency requires that no adversary can produce a ciphertext such that all receivers get the different messages from the same ciphertext. Formally, a secret broadcast scheme is DC-secure if the advantage of an adversary in the following experiment is negligible.

$\mathbf{Exp}^{DC}_{BE,\mathcal{A}}(\theta)$
$For\ i = 1, \ldots, n,\ \ (pk_i, sk_i) \leftarrow BE.key(\theta)$
$\Gamma \leftarrow (pk_1, \ldots, pk_n);\ \sigma \leftarrow \mathcal{A}(pk_1, \ldots, pk_n)$
$\exists \alpha, \beta \in [1, n]$, if $BE.dec_{sk_\alpha}(\Gamma, \sigma) \neq BE.dec_{sk_\beta}(\Gamma, \sigma)$
$output\ b = 1$
$output\ b = 0$

2.3 Drawbacks

In this section, we show that the WZP scheme in [4] cannot resist on the decryption consistency.

First, we consider a simple case with $n = 3$. If an attacker got a broadcasting ciphertext $[\Gamma, \sigma]$ to P_1, P_2, P_3, where $\Gamma = (pk_1, pk_2, pk_3)$ and $\sigma = (pk_0, c_0, c_1, c_2, c_3)$ (Here Γ is the public keys list and σ is the ciphertext), he can simply modify and update the component Γ with $\Gamma' = (pk_1, pk_3, pk_2)$. It is easily to see that P_1 can decrypt the message successfully from $[\Gamma', \sigma]$ but P_2, P_3 can not because they will detect that (pk_0, sk'_0) is not a valid key pair by extracting the sk'_0 from c_2 $(resp.\ c_3)$ with secret key sk_3 $(resp.\ sk_2)$, that is, $sk'_0 = PE.dec_{sk_3}(c_2)$ $(resp.\ sk'_0 = PE.dec_{sk_2}(c_3))$. This will violate the definition of *decryption consistency*.

Moreover, we give another attack and indicate that the broadcasting receivers may get different invalid message from the ciphertext even though the test of (pk_0, sk'_0) is successfully in the decryption procedure. In [4], authors introduce the ElGamal key as verifiable public/private key pair. We also take ElGamal encryption as the instance of PE. To encrypt a message $m \in \mathbb{G}$, the ElGamal encryption is presented as follows.

$PE.key$:	Receiver generates description of a multiplicative cyclic group $\mathbb{G}$ of order q with generator g; chooses a random $x \in Z_q^*$ and computes $y = g^x$; publishes $< y, \mathbb{G}, q, g >$ as the public key and retains x as the private key.
$PE.enc$:	Sender computes $\hat{c}_1 = g^r$, $s = y^r$, $\hat{c}_2 = m \cdot s$ where r is a randomly picked/input from Z_q^*; outputs ciphertext $C = (\hat{c}_1, \hat{c}_2) = (g^r, m \cdot g^{xr})$.
$PE.dec$:	Receiver computes $s = \hat{c}_1^{q-x}$ using his private key x and gets message $m' = \hat{c}_2 \cdot s$.

In WZP broadcast encryption algorithm $BE.enc$, we consider the process as follows: at first use ElGamal scheme to get PE a key pair $(sk_0 = \tilde{x}, pk_0 = g^{\tilde{x}})$, then we calculate $c_0 = PE.enc_{pk_0}(m) = (g^r, m \cdot g^{\tilde{x}r})$. For $i = 1, \ldots, n$, it computes $c_i = PE.enc_{pk_i}(sk_0) = (\hat{c}_{i,1}, \hat{c}_{i,2}) = (g^{r_i}, \tilde{x} g^{x_i r_i})$ where x_i is the private key of user P_i and $r_i \overset{\$}{\leftarrow} Z_q^*$. It outputs a ciphertext $[\Gamma, \sigma]$ such that $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (pk'_0 = pk_0^t, c_0, c'_1 = (\hat{c}_{1,1}, t \cdot \hat{c}_{1,2}), \ldots, c'_n = (\hat{c}_{n,1}, t \cdot \hat{c}_{n,2}))$ where t is randomly picked from Z_q ($t \neq 0$ and $t \neq 1$).

In the $BE.dec$ phase, the extracted sk'_0 is a valid component to public key pk'_0. i.e.,

$$
\begin{aligned}
sk'_0 &= PE.dec_{sk_i}(c'_i) = (t \cdot \hat{c}_{i,2}) \cdot \hat{c}_{i,1}^{q-x_i} \\
&= (t\tilde{x} g^{x_i r_i}) \cdot (g^{r_i})^{q-x_i} \\
&= t\tilde{x} g^{x_i r_i} \cdot g^{r_i q - r_i x_i} \\
&= t\tilde{x} g^{x_i r_i - x_i r_i} (g^q)^{r_i} = t\tilde{x} \\
g^{sk'_0} &= g^{t\tilde{x}} = (g^{\tilde{x}})^t = pk_0^t = pk'_0
\end{aligned}
$$

Thus (pk'_0, sk'_0) can pass through the *test* check and consider as a valid *PE* public-/private-key pair. It can extract the message m' by $m' \leftarrow PE.dec_{sk'_0}(c_0)$ and claims that m' is a valid message from the original message m of the sender, i.e. $m' = m$. However, we indicate that the decrypted message m' is not equal to the original m.

$$\begin{aligned} m' &= PE.dec_{sk'_0}(c_0) = m \cdot g^{\tilde{x}r} \cdot (g^r)^{q-t\tilde{x}} \\ &= m \cdot g^{r\tilde{x}-rq-rt\tilde{x}} = m \cdot g^{r(1-t)\tilde{x}} \neq m \end{aligned}$$

As $r, \tilde{x} \in Z_q^*$ and $t \neq 1$, it holds that $g^{r(1-t)\tilde{x}} \neq 1$. Then $m \cdot g^{r(1-t)\tilde{x}} \neq m$. In this case, all receivers can get the same message m' but it is not the original message m, this holds the *decryption consistency* but contradicts the *correctness* of an encryption scheme.

3. Improved Scheme

3.1 Proposed Scheme

We introduce a pseudo-random function $\pi_\kappa : \{0,1\}^\theta \rightarrow \{0,1\}^\theta$ that is selected from a function family $\pi = \{\pi_\kappa | \kappa$ *is in the space of* θ*-bit strings*$\}$. Like in [4], we also use a public key encryption *PE* that the key pair is verifiable. i.e., $test(pk, sk) = 1$ if (pk, sk) is a valid key pair. For instance, in the well-known ElGamal scheme, the equation $pk = g^{sk}$ always holds between a valid public key *pk* a private key *sk*. The improved scheme is presented as follows.

- $(pk, sk) \leftarrow$BE.key(1^θ): This algorithm generates and outputs a key pair of public-/private-key (pk, sk) by calling the public key generation algorithm *PE.key*. Private key holder can verify the key consistency by checking $test(pk, sk) = 1$.
- $(\Gamma, \sigma) \leftarrow$BE.enc$_{pk_1,\ldots,pk_n}(m)$: The algorithm first calls *PE.key* to get a key pair $[ek, dk]$. For $1 \leq i \leq n$, it computes $c_i = PE.enc_{pk_i}(dk)$. It computes $c_0 \leftarrow m \oplus dk$, $h = \pi_{dk}(c_0, c_1, \ldots, c_n)$, $w = PE.enc_{ek}(ek \oplus h)$, and outputs a ciphertext $[\Gamma, \sigma]$ where $\Gamma = (pk_1, \ldots, pk_n)$ and $\sigma = (w, c_0, c_1, \ldots, c_n)$.
- $m|\perp \leftarrow$BE.dec$_{sk_i}(\Gamma, \sigma)$: Taken as the input ciphertext $[\Gamma, \sigma]$ and a broadcast receiver's private key sk_i, this algorithm first computes $\widetilde{dk} \leftarrow PE.dec_{sk_i}(c_i)$, $\tilde{h} = \pi_{\widetilde{dk}}(c_0, c_1, \ldots, c_n)$, and $\widetilde{ek} = \tilde{h} \oplus PE.dec_{\widetilde{dk}}(w)$; Checks equation $test(\widetilde{ek}, \widetilde{sk}) = 1$ holds and outputs $m \leftarrow c_0 \oplus \widetilde{dk}$; Otherwise outputs $\perp$ as decryption failure.

3.2 Efficiency Analysis

We compare the performance between JKL [3], WZP [4] and ours. Our proposed scheme attains stronger decryption consistency and achieves more stronger security of IND-CCA. Moreover, WZP [4] and ours scheme have the similar computing complex and communicating cost in secret broadcast networks, which is more efficient than JKL scheme.

	JKL [3]	WZP [4]	ours
# of CT	$(2n+1)\|C\|$	$(n+1)\|C\| + \|\mathbb{G}\|$	$n\|C\| + \|\mathbb{G}\|$
# of enc	$2n \cdot \mathcal{E}$	$(n+1)\mathcal{E} + \mathcal{K}_1$	$(n+1)\mathcal{E} + \mathcal{K}_1$
# of dec	$n \cdot \mathcal{E} + 2\mathcal{D}$	$2\mathcal{D} + \mathcal{K}_2$	$2\mathcal{D} + \mathcal{K}_2$
semantic security	IND-CPA	IND-CPA	IND-CCA
DC	weak	weak	strong

n: number of broadcast user
$|\mathbb{G}|$: element size of group $\mathbb{G}$
$\mathcal{K}_1$: computation cost for generating a public-/private-pair
$\mathcal{K}_2$: verification cost for (pk, sk) of PE
$\mathcal{E}$: computation cost for encryption of PE
$\mathcal{D}$: computation cost for decryption of PE
$\mathcal{C}$: ciphertext size of public encryption PE

3.3 Security

In [3], [4], the schemes are only IND-CPA secure in semantic security. Our proposed scheme achieves IND-CCA security that the adversary can make query to decryption oracles. Semantic security, roughly speaking, requires that observation of a ciphertext does not enable an adversary to compute anything about the underlying plaintext message that it could not have computed on its own (i.e., prior to observing the ciphertext); this should hold even if the adversary has some a priori information about the message.

Security against IND-CCA is a strong and very useful notion of security for public-key encryption schemes. This notion is known to suffice for many applications of encryption in the presence of active attackers, including secure broadcast communications, and electronic voting schemes, etc. Our proposed scheme is proved to achieve IND-CCA security.

Definition 5: PRF-SECURE A pseudorandom function $\pi_\kappa : \{0,1\}^\theta \rightarrow \{0,1\}^\theta$ is PRF-secure if the advantage of any adversary $\mathcal{A}$ is negligible in distinguishing $b_i (i \in \{0,1\})$ for the following two experiments, where $Rand(\cdot)$ is a set of all functions from domain $\{0,1\}^\theta$ to range $\{0,1\}^\theta$.

$\mathbf{Exp}^{PRF_0}_{\pi,\mathcal{A}}(1^\theta)$	$\mathbf{Exp}^{PRF_1}_{\pi,\mathcal{A}}(1^\theta)$
$\kappa \leftarrow \{0,1\}^\theta$	$h \leftarrow Rand^{\{0,1\}^\theta \rightarrow \{0,1\}^\theta}$
$b_0 \leftarrow \mathcal{A}^{\pi_\kappa(\cdot)}(1^\theta)$	$b_1 \leftarrow \mathcal{A}^{h(\cdot)}(1^\theta)$
output b_0	output b_1

Lemma 1: An encryption scheme can achieve the adaptive chosen-ciphertext security that derives from a building blocks any CPA-secure public-key encryption scheme and a one-time signature.

Theorem 1: If the public encryption PE is $(O(t_1), \varepsilon)$-semantic secure (i.e., IND-CPA/CCA) and the pseudorandom function π_κ is $(O(t_2), \epsilon)$-PRF-secure, the proposed BE scheme is $(O(t_1 + t_2), \varepsilon + 2\epsilon)$- DC-secure.

Proof of Theorem 1. In *PE.dec* phase, it is easy to see that the pair $(\widetilde{ek}, \widetilde{dk})$ is a valid key pair if and only if $BE.dec_{sk_i}(\Gamma, \sigma)$ outputs a valid message instead of $\perp$. Under this circumstances, $\widetilde{ek} = \tilde{h} \oplus PE.dec_{\widetilde{dk}}(w) = \tilde{h} \oplus$

$PE.dec_{\widetilde{dk}}(ek \oplus h)$. If $\widetilde{dk} = dk$, it has $ek \oplus h \leftarrow PE.dec_{\widetilde{dk}}(dk \oplus h)$. When $\tilde{h} = \pi_{\widetilde{dk}}(c_0, \ldots, c_n) = \pi_{dk}(c_0, \ldots, c_n) = h$, it then $\widetilde{ek} = ek$.

The pseudorandom permutation π_{dk} will retain the integrity and verification of the ciphertext (Γ, σ). Therefore, any tamper of the ciphertext will produce distinct $\widetilde{ek}$ that will not pass through the test of public-/private-key pair. By deploying a $(O(t_1), \varepsilon)$-secure pseudorandom function and a $(O(t_2), \epsilon)$-secure public encryption, the advantage of an adversary in attacking the decryption consistency is $(\varepsilon + 2\epsilon)$.

Theorem 2: If the public encryption PE is IND-CPA secure, the proposed BE is IND-CPA secure.

Proof of Theorem 2. If an adversary $\mathcal{A}$ can attack the proposed scheme with advantage ϵ, we can attack the public encryption scheme PE with the same advantage by deploying $\mathcal{A}$ as a subroutine. After given a challenged ciphertext $C^* = [\Gamma^*, \sigma^* = (w^*, c_0^*, \ldots, c_n^*)]$ to $\mathcal{A}$ that $\mathcal{A}$ does not carry any private key of broadcast users in Γ^*. If $\mathcal{A}$ succeeds in guessing the plaintext m^* in ciphertext C^*, we can attack the IND-CPA for PE scheme. Note that w^* is encrypted by PE under a secret key dk, and we cannot decrypt it if we do not hold dk. First, we compute $d = c_0^* \oplus m^*$. Then we can recover the plaintext $v = ek \oplus h$ in w^* such that $v = PE.dec_d(w^*)$.

Theorem 3: If the public-key encryption scheme PE is IND-CPA secure and pseudorandom function π_κ is PRF-secure, the proposed BE is IND-CCA secure.

Proof of Theorem 3. In the proposed scheme, we use $\widetilde{dk}$ as the one-time signature key to sign the ciphertext, i.e., $\tilde{h} = \pi_{\widetilde{dk}}(c_0, \ldots, c_n)$. Thus, any modification of the ciphertext (Γ, σ) will cause the failure of the key test of $(\widetilde{ek}, \widetilde{dk})$, and any decryption query of adversary must be valid ciphertext components. In Theorem 2, we have proved that the scheme is IND-CPA-secure. According to Lemma 1, the proposed scheme achieves IND-CCA security that combines a CPA-secure PE to encrypt the message with a one-time signature scheme to sign the ciphertext.

Acknowledgement

This work is supported by NSFC under Grant 60973134 and 61173164, National Science Foundation of Guangdong Under Grant 10151064201000028, and Grant-in-Aid for JSPS Fellows of Japan under Grant 22·00045.

References

[1] 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.
[2] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," Proc. Eurocrypt 2009, LNCS 5479, pp.171–188, 2009.
[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] S. Wu, Y. Zhu, and Q. Pu, "Comments on an efficient secret broadcast in the broadcasting networks," IEEE Commun. Lett., vol.14, no.7, pp.685–687, 2010.