

Collusion-resistant Broadcast Encryption based on Hidden RSA Subgroups

Sigurd Eskeland^a

Norwegian Computing Center, Postboks 114 Blindern, 0314 Oslo, Norway

Keywords: Broadcast Encryption, Public Key Cryptography, RSA Subgroups.

Abstract: Public key broadcast encryption enables computations of ciphertexts, in which a single ciphertext is encrypted with regard to a set of recipients, and only the intended recipients can decrypt that ciphertext independently of each other and without interactions. A significant shortcoming of existing broadcast encryption schemes are long decryption keys comprising the public keys of pertaining recipients. Decryption therefore necessitates access to public keys, which requires key management and impacts computational and transmission overhead, accessibility, and storage. Moreover, a user description list referencing the pertaining recipients and their public keys must be appended to each ciphertext, which leads to the privacy implication of disclosing user/content-relations. Curiously, virtually all broadcast encryption schemes are based on bilinear pairings. In this paper, we propose a collusion-resistant broadcast encryption scheme that is the first broadcast encryption scheme based on the factorization problem and hidden RSA subgroups. A novel feature is that the decryption key consists of a single element only, which leads to significantly reduced key management, improved computational efficiency, and elimination of the mentioned privacy issue.

1 INTRODUCTION

Broadcast encryption is a category of cryptographic systems that allows a sender to compute ciphertexts that can only be decrypted by an arbitrary subset of recipients $T \subseteq \mathcal{U}$ specified by the sender. Broadcast encryption is characterized by having no synchronisms and no two-way interactions between the sender and recipients, nor among the recipients. The main goal of broadcast encryption is to minimize the transmission overhead, computation cost, storage size, and key management. All key establishment communication in broadcast encryption is unidirectional from the sender to the recipients, and there are no interactions between the sender and the groups of recipients, nor among the recipients.

Stateful broadcast encryption schemes maintain a state according to group membership, in which the broadcast key must be updated by the event of a change in group membership to maintain forward and backward secrecy. To meet efficiency goals, the general idea is to update only those key elements that are affected by a user change. An inherent disadvantage of statefulness is that if a user misses an update mes-


sage, he or she will be left out from subsequent sessions.

In *stateless* broadcast encryption, decryptions are conducted independently of previous sessions as there is no updating of key material due to changes of group memberships. In existing stateless broadcast encryption schemes, the decryption algorithm requires application of the private key x_i of user P_i of the target subset $T \subseteq \mathcal{U}$, the public key y_j of each of the other users P_j in T , and some system parameters B :

$$\text{Dec}(x_i, \{y_j \mid \forall P_j \in (T \setminus \{P_i\})\}, B)$$

Thus, the *decryption key* is $(x_i, \{y_j \mid \forall P_j \in (T \setminus \{P_i\})\})$, whose number of elements equals the size of T . For efficiency reasons, most broadcast encryption schemes assume the “revoked” complementary subset $R = \mathcal{U} \setminus T$ instead of T , since this set is presumed to be smaller than T . In any regard, this brings about the following issues:

1. All relevant public keys *must* be accessible, since decryption is only possible with a complete decryption key. This may be inconvenient and impractical in some settings.
2. The decryption key size is linear to the size of T . This increases the storage and computational overhead accordingly.

^a  <https://orcid.org/0000-0003-0045-3387>

3. The encryption header must contain a user description list that references each user in T (and their public keys). This increases the transmission overhead accordingly.
4. The user description list leads to a potential privacy issue.

To illustrate the last point; suppose a secure TV broadcasting scenario where each customer has access to a certain channel using his private key. The problem is that in order to decrypt the customers would have to know who else has paid for the specific subscription, which conflicts with the privacy of the individual subscribers. This privacy issue is addressed by *anonymous broadcast encryption* whose goal is that no identifying information is “leaked” about the privileged set T (Libert et al., 2012). However, these schemes are still inflicted with the same efficiency issues, and in some cases with long ciphertexts whose number of elements is linear to T (He et al., 2016).

Cryptographic Primitives. Broadcast encryption is predominantly based on bilinear pairings and elliptic curve cryptography. However, pairing based cryptography (PBC) has some disadvantages that are often overlooked. Cao and Liu (2015) note that bilinear pairings require working parameters in the order of 1024 bits to offer 80 bits security, in contrast to pure elliptic curve-based cryptographic schemes, where such parameters are typically 160 bits. They point out that there are very few industrial products being integrated with pairing-based cryptosystems, for reasons such that “pairing computation is hard to understand for most engineers” and “heavy group operation of PBC really lowers the advantages that gained from smaller key size.”

Hajny et al. (2018) note that there are very few libraries available supporting pairing-based cryptography, and that papers addressing implementation aspects of pairing-based cryptography are very rare. In addition to bilinear mappings, lattices have been proposed as a cryptographic primitive for broadcast encryption (Wang and Bi, 2010; Georgescu, 2013). However, these schemes produce non-constant size ciphertexts and may not be practical. It is thus of great interest to explore the applicability of alternative cryptographic primitives for broadcast encryption, in particular well-known number-theoretic primitives. However, number-theoretic primitives such as discrete logarithms and RSA assumptions have so far been considered inapplicable to broadcast encryption. *Contributions.* In this paper, we propose a fully collusion-resistant public key broadcast encryption scheme with the following novel features:

- Decryption requires a single private key-element

only. This eliminates the necessity for key management and availability of other users’ public keys.

- Decryption requires just a single exponential modular operation.
- There is no explicit need for a user description list, and thus an implicit feature is *user anonymity*.

This is an improvement compared to other broadcast encryption schemes, in which the *decryption key* is linear to the size of target group T (or the revoked group \mathcal{R}). Another novel and attractive feature is that it is based on the factorization problem and hidden RSA subgroups. To the best of our knowledge, our construction is the first collusion-resistant broadcast encryption scheme that is based on this security assumption.

The broadcast encryption header consists of a single element whose size is linear to the maximum number of recipients N . For example, the header size is 3072 bits for $N = 11$ at 128 bits security level, which for comparison is equal to the RSA ciphertext size of the same security level, and therefore a significant improvement considering the factorization assumption.

2 RELATED WORK

Earlier approaches to stateless broadcast encryption assume tree-based structures. This includes the “subset-cover” framework proposed by Naor et al. (2001) utilizing symmetric user keys, in which keys of user subsets are derived from a virtual tree structure. Building on Naor et al. (2001), Dodis and Fazio (2003) proposed a public key broadcast encryption (PKBE) scheme.

Boneh et al. (2005) proposed a stateless and fully collusion resistant PKBE scheme that was the first of many subsequent PKBE schemes to rely on bilinear pairings, in which computations are in cyclic groups of fixed order that determines the ciphertext (header) size. The authors proposed a “basic” scheme BGW_1 having a decryption key size linear to the number of recipients N and constant-size ciphertext of two elements, and a generalized variant BGW_2 consisting of parallel instances of BGW_1 achieving a tradeoff of $O(\sqrt{N})$ decryption key size and $O(\sqrt{N})$ ciphertext size. Identity-based variants of (BGW_1) , having user identities as public keys, were proposed by Delerablée (2007) and Sakai and Furukawa (2007) with the same performance properties as (BGW_1) , except shorter public key length due to the identity-orientation. Delerablée et al. (2007) proposed a dynamic PKBE scheme that allows joining of new users

without updating the group keys. The first adaptively secure PKBE scheme was proposed by Gentry and Waters (2009), and later schemes are found in (Malek and Miri, 2012; Zhang et al., 2012; Phan et al., 2013; Kim et al., 2015; Lee and Lee, 2015). Some other PKBE schemes are found in (Park et al., 2008; Dubois et al., 2013; Kim et al., 2013).

All the stateless broadcast encryption schemes are based on bilinear pairings. In addition to bilinear pairings, lattices is another cryptographic primitive that has been proposed for realizing PKBE (Wang and Bi, 2010; Georgescu, 2013).

As a sidenote, multi-receiver encryption (MRE) is different from Broadcast encryption, in which the sender encrypts N individual plaintexts, one for each recipient, resulting in N ciphertexts. MRE is probabilistic and its motivation is computational efficiency by reusing the same element of randomness for all ciphertexts (Bellare et al., 2007) instead of generating unique random integers for each ciphertext.

3 PRELIMINARIES

The proposed scheme assumes cyclic subgroups, which are realized by the following parameters.

- Let $n = pq$ be the product of two large secret primes

$$p = 2p_0 \prod_{j=1}^{\lfloor N/2 \rfloor} p_j r_p + 1 \quad (1a)$$

and

$$q = 2q_0 \prod_{j=\lfloor N/2 \rfloor + 1}^N p_j r_q + 1 \quad (1b)$$

where N is the number of recipients, $\mathcal{P} = \{p_0, q_0, p_j \mid 1 \leq j \leq N\}$ are distinct large secret primes of approximately the same size, and (r_p, r_q) are optional arbitrary integers. The security level λ is determined by $\lambda = \|\|p_0\|\| = \|\|q_0\|\| = \|\|p_j\|\|$.

- Let $g = \alpha^2 \pmod n$, where α is a generator (i.e., primitive element) for a cyclic group in \mathbb{Z}_p^* and in \mathbb{Z}_q^* .
- Let g_i , $1 \leq i \leq N$, denote a generator for the subgroup \mathbb{G}_i of order $p_0 q_0 p_i$, where

$$g_i = g^{\bar{p}_i} \pmod n \quad \text{and} \quad \bar{p}_i = \prod_{j=1, j \neq i}^N p_j \quad (2)$$

The order of \mathbb{G}_i is hidden, since \mathcal{P} are secret.

- Select a large random secret integer γ , whose bit-size is at least that of n .

Next we present the relevant computational hardness assumptions.

3.1 Security Assumptions

Background on subgroups on Hidden Orders. For efficiency purposes for public key signature, commitment, and encryption cryptosystems, Groth (2005) proposed using small subgroups in \mathbb{Z}_n^* of secret orders. For this purpose, Groth proposed a pertaining decisional RSA subgroup security assumption, whose hardness is the difficulty to determine if an element pertains to a subgroup $\mathbb{G} < \mathbb{Z}_n^*$ or to \mathbb{Z}_n^* . A similar decisional RSA subgroup assumption is formulated by Bourse et al. (2020). These assumptions are similar to high-residuosity assumptions, such as (Naccache and Stern, 1998), and the composite residuosity assumption of the Paillier cryptosystem (Paillier, 1999).

Secret subgroups can for instance be useful and convenient when designing cryptosystems and cryptographic protocols that are using secret encryption factors (or blinding factors), since knowing the subgroup order (represented by the private key) allows elimination of those encryption factors. This is seen in the mentioned Paillier cryptosystem, in which using the private key λ as an exponent to the ciphertext eliminates the encryption factor r^n , due to that its subgroup order is λ , i.e., $(r^n)^\lambda \pmod{n^2} = 1$. In our cryptosystem, subgroups of hidden orders are used for preventing disclosure of the secret integer γ , as discussed below.

Congruences. Consider the modular residue

$$\gamma_i = \gamma \pmod{p_0 q_0 \bar{p}_i} \quad (3)$$

which in the proposed scheme is the private key for user P_i . The prime p_k divides \bar{p}_i if $i \neq k$ in agreement with Eq. (2). This implies the congruence $\gamma_i \pmod{p_k} \equiv \gamma_j \pmod{p_k}$ for any two residues γ_i and γ_j , $i \neq j$. In general, this is

$$\gamma \equiv \gamma_i \equiv \gamma_j \pmod{p_k}$$

for $1 \leq i, j, k \leq N$, $i \neq j \neq k$. Taking a generator g_i and the composite modulus n into consideration, the mentioned congruences agree with

$$g_k^\gamma \equiv g_k^{\gamma_i} \pmod{n} \quad (4)$$

where g_k generates a cyclic subgroup \mathbb{G}_k . The congruence holds since the order of \mathbb{G}_k is $p_0 q_0 p_k$, which divides the modulus $p_0 q_0 \bar{p}_i$ of γ_i for $i \neq k$.

In agreement with Eq. (3), the secret integer γ is congruent to each residue γ_j , $1 \leq j \leq N$:

$$\gamma \equiv \begin{cases} \gamma_1 & \pmod{p_0 q_0 \bar{p}_1} \\ \vdots & \\ \gamma_N & \pmod{p_0 q_0 \bar{p}_N} \end{cases}$$

In the proposed scheme γ is a secret integer. This means that for any two residues $\gamma_i = \gamma \pmod{p_0 q_0 \bar{p}_i}$

and $\gamma_j = \gamma \bmod p_0 q_0 \bar{p}_j$, γ can be disclosed in agreement with the Chinese remainder theorem:

$$\gamma \equiv \begin{cases} \gamma_i & (\bmod p_0 q_0 \bar{p}_i) \\ \gamma_j & (\bmod p_i) \end{cases} \quad (5)$$

if and only if $(p_0, q_0, \bar{p}_i, p_i)$ are known. For this reason, to prevent disclosure of γ , we use subgroups of hidden order, in which all primes in \mathcal{P} are kept secret. Due to the secrecy of these primes, it is not possible to restore γ . This ensures *collusion resistance*, which prevents any subset of colluding users \mathcal{R} from establishing γ .

On the Necessity of (p_0, q_0) . The composite modulus n can be factorized more efficiently by utilizing the smaller search space of the subgroup $\mathbb{G}_i < \mathbb{Z}_n^*$ provided by g_i than by factoring methods such as general number field sieves. This situation was also pointed out by Damgård et al. (2008). The secret primes (p_0, q_0) , cf. Eq. (1), are necessary to prevent factorization of n in conjunction with g_i .

According to Fermat's little theorem, then $g^p = kp + 1$, where $g, k > 0$ and p is a prime. Thus, $g^{xp} = (kp + 1)^x = k'p + 1$, where $x, k' > 0$. Recall that g_i generates a subgroup of order $p_0 q_0 p_i$. According to the composition of p , cf. Eq. (1), then $\{q_0, p_i \mid \lceil \frac{N}{2} \rceil + 1 \leq i \leq N\}$, do not divide $p - 1$. In agreement with Fermat's theorem then

$$g_i^{p_0 p_i} = \alpha^{2 p_0 p_i \bar{p}_i} = k'' p + 1 \quad \text{for} \quad \left\lceil \frac{N}{2} \right\rceil + 1 \leq i \leq N$$

where (g_i, \bar{p}_i, p) are defined in Eqs. (1, 2). This means that p can be found by an exhaustive search w.r.t. the unknown integer p_0 , where $p' = \gcd((g_i^x \bmod n) - 1, n)$. If $x = p_0$ then $p' = p$. The security strength λ w.r.t. this attack is therefore equivalent to $\lambda = ||p_0|| = ||q_0||$.

The DDH Assumption. In addition to the factorization problem, the security also relies on the decisional Diffie-Hellmann assumption. Let g be a generator for a sufficiently large subgroup \mathbb{G} of order q . Let (a, b, c) be randomly selected large integers in $[1, \dots, q]$. Given the triplet (g, g^a, g^b, z_b) , where b is a uniform random bit. Let $z_b = g^{ab}$ and $z_{1-b} = g^c$. The probability that b is correctly determined is at least $\frac{1}{2} + \epsilon$ for some value ϵ . If g^{ab} and g^c are indistinguishable, so that b cannot be determined w.r.t. $z_b = g^{ab}$, then ϵ is negligible, meaning that the DDH assumption holds.

3.2 Broadcast Encryption Algorithms

A trusted authority is necessary for setting up an instance of the proposed scheme by computing long-term user keys. Let $\mathcal{U} = \{P_1, \dots, P_N\}$ denote a set of

N users. The scheme proposed consists of the following algorithms:

Setup. The algorithm $(pk, sk) \leftarrow \text{Setup}(N, \lambda)$ inputs a security parameter λ and the number of users N , and outputs $pk = (\{g_i, y_i \mid 0 \leq i \leq N\}, n)$ and $sk = \{\gamma_i \mid 1 \leq i \leq N\}$.

Encryption. For any subset $T \subseteq \mathcal{U}$, where $\mathcal{R} = \mathcal{U} \setminus T$ is the corresponding set of excluded (or revoked) users, the encryption algorithm $(k_T, z) \leftarrow \text{Enc}(\{g_j, y_j \mid P_j \in \mathcal{R}\}, n)$ takes the public keys of the revoked users as input, and outputs a broadcast key k_T and an encryption header z .

Decryption. The decryption algorithm $k_T \leftarrow \text{Dec}(\gamma_i, z, n)$ takes the private key γ_i (of which $P_i \in T$) and the encryption header z as input, and outputs the broadcast key k_T .

The correctness property is met if for any subset $T \subseteq \mathcal{U}$ the broadcast keys $(k'_T, z) \leftarrow \text{Enc}(\{g_j, y_j \mid P_j \in \mathcal{R}\}, n)$ and $k''_T \leftarrow \text{Dec}(\gamma_i, z, n)$ match, i.e., $k'_T = k''_T$.

3.3 Security Model

The security of the proposed scheme can be defined using a game between an adversary \mathcal{A} and a challenger \mathcal{C} . The adversary defines an arbitrary set of compromised users S^* in which the adversary is permitted to obtain the private keys. This is consistent with a revoked set of colluding users $\mathcal{R} = \mathcal{U} \setminus T$.

Setup. The challenger computes $(pk, sk) \leftarrow \text{Setup}(N, \lambda)$ and obtains N user keys. It then submits PK to the adversary \mathcal{A} .

Key Query. The adversary queries the private keys for a subset $S^* \subset S$, where $S = \{1, \dots, N\}$. The challenger submits $\{\gamma_i \mid i \in S^*\}$ to \mathcal{A} .

Challenge. The challenger invokes $(k_S, z) \leftarrow \text{Enc}(g_j, y_j \mid j \in S^*, n)$. The challenger randomly pick a bit $b \in \{0, 1\}$, and sets $k_b = k_S$ and randomly sets k_{1-b} in the space of possible session keys. It then submits the triplet (z, k_0, k_1) to the adversary.

Output. The adversary outputs a bit b' . The adversary succeeds if $b = b'$.

The game can be conducted for any subset $S^* \subseteq S$. Let $\Pr(b' = b) - \frac{1}{2}$ be the probability that the adversary correctly outputs $b = b'$ after the game. We say that the broadcast encryption scheme is key indistinguishable if $|\Pr(b' = b) - \frac{1}{2}| \leq \epsilon$, where ϵ is negligible due to the difficulty of correctly distinguishing keys.

4 PUBLIC KEY BROADCAST ENCRYPTION

A trusted authority (TA) is necessary for setting up system parameters and long-term user keys.

Setup. The TA conducts the following tasks to set up an instance of the system.

1. Compute $n = pq$, where p and q are two large random secret primes selected in agreement with Eq. (1).
2. Select a large random secret integer γ whose size is larger than n .
3. The private keys for $P_i \in \mathcal{U}$ are computed as

$$\gamma_i = \gamma \bmod p_0 q_0 \bar{p}_i, \quad \text{where} \quad \bar{p}_i = \prod_{j=1, i \neq j}^N p_j$$

4. Let g be a generator of the multiplicative groups modulo p and q . The corresponding public keys are computed as

$$g_i = g^{\bar{p}_i} \bmod n, \quad y_i = g_i^\gamma \bmod n, \quad 0 \leq j \leq N$$

Each user $P_i \in \mathcal{U}$ is assigned the key tuple (γ_i, g_i, y_i) . Note that (g_0, y_0) are generic and to be applied for the case $\mathcal{R} = \emptyset$.

Encryption. Select a set of recipients $T \subseteq \mathcal{U}$ that is the target for a secure broadcast, in which $\mathcal{R} = \mathcal{U} \setminus T$ denotes a set of so-called revoked users. Generate a random secret integer $r \in \mathbb{Z}_n^*$, and compute the encryption key

$$k_T = \left(\prod_{j \in \mathcal{R}} y_j \right)^r \bmod n$$

and the encryption header

$$z = \left(\prod_{j \in \mathcal{R}} g_j \right)^r \bmod n$$

If $\mathcal{R} = \emptyset$ then $k_T = k_{\mathcal{U}} = y_0^r$ and $z = g_0^r$. Then the plaintext is encrypted using k_T .

Decryption. At the receipt of z , each user $P_i \in T$ is able to restore k_T by the modular exponentiation

$$k_T = z^{\gamma_i} \bmod n$$

Note that there is only one public key element and private key element (for each user), and the header is only element.

4.1 Correctness

The following shows that the output of the decryption algorithm (Eq. (6a)) is consistent with the output of

the encryption algorithm (Eq. (6d)):

$$k_{T,i} \equiv z^{\gamma_i} \equiv \left(\left(\prod_{k \in \mathcal{R}} g_k \right)^r \right)^{\gamma_i} \pmod{n} \quad (6a)$$

$$\equiv \prod_{k \in \mathcal{R}} g_k^{r \bar{p}_k (\gamma \bmod p_0 q_0 p_k)} \pmod{n} \quad (6b)$$

$$\equiv \left(\prod_{k \in \mathcal{R}} g_k \right)^{r \gamma} \pmod{n} \quad (6c)$$

$$\equiv \left(\prod_{k \in \mathcal{R}} y_k \right)^r \pmod{n} = k_T \quad (6d)$$

for $\gamma_i, i \notin \mathcal{R}$, in agreement with Eq. (4). The congruence holds since the order of the subgroup \mathbb{G}_k generated by g_k is $p_0 q_0 p_k$, and $p_0 q_0 p_k$ divides the modulus $p_0 q_0 \bar{p}_i$ of γ_i , if $i \neq k$. Therefore, two users $P_i, P_j \in T$, holding two distinct private keys (γ_i, γ_j) , will compute the same key k_T .

Example. Let $N = 3$ and $n = (2p_0 p_1 + 1)(2q_0 p_2 p_3 + 1)$. Then $\gamma_1 = \gamma \bmod p_0 q_0 p_2 p_3$ and $\gamma_2 = \gamma \bmod p_0 q_0 p_1 p_3$. Let $P_3 \in \mathcal{R}$ be a revoked user realized by means of g_3 in the encryption step. The following expressions are in \mathbb{Z}_n^* , and show that

$$\begin{aligned} g_3^{\gamma_1} &= g^{\bar{p}_3 \gamma_1} = g^{p_1 p_2 \gamma_1} = g^{p_1 p_2 (\gamma \bmod p_0 q_0 p_2 p_3)} \\ &\equiv g^{p_1 p_2 \gamma \bmod p_0 q_0 p_1 p_2 p_3} \equiv g^{\bar{p}_3 \gamma} \end{aligned}$$

and

$$\begin{aligned} g_3^{\gamma_2} &= g^{\bar{p}_3 \gamma_2} = g^{p_1 p_2 \gamma_2} = g^{p_1 p_2 (\gamma \bmod p_0 q_0 p_1 p_3)} \\ &\equiv g^{p_1 p_2 \gamma \bmod p_0 q_0 p_1 p_2 p_3} \equiv g^{\bar{p}_3 \gamma} \end{aligned}$$

are hence equivalent. However, $g_3^{\gamma_3}$ results in the incongruency

$$g_3^{\gamma_3} = g^{p_1 p_2 \gamma_3} = g^{p_1 p_2 (\gamma \bmod p_0 q_0 p_1 p_2)} \not\equiv g^{\bar{p}_3 \gamma}$$

This prevents $P_3 \in \mathcal{R}$ from computing the broadcast key.

4.2 Parameter Sizes

In agreement with the discussion in Section 3.1, we suggest that $\lambda = \|p_0\| = \|q_0\|$. We also suggest that $\lambda = \|p_j\|$, $1 \leq j \leq N$, to ensure a sufficiently large distribution of the private keys γ_j , $1 \leq j \leq N$. Table 1 shows the sizes of modulus primes $\ell = \|p\| = \|q\|$ and n as a function of λ and N . This is in agreement with the recommendations of NIST (Barker, 2016), which suggests RSA modulus should be 1024 bits for 80 bits security level, 2048 bits for 112 bits security level, and 3072 bits for 128 bits security. Note that for $(\lambda = 128, N = 10)$, n should be increased to 3072 bits to meet the current recommendations for $\lambda = 128$.

Consideration has to be taken when selecting a RSA modulus whose prime factors have a unusual composition. For example, the attack of Coron et al.

Table 1: Parameters.

λ	N	ℓ	$\ n\ $
80	10	880	1760
80	20	1688	2260
112	10	1232	2464
112	20	2352	4704
128	10	1408	2816*
128	20	2688	5376

(2011) has a computational time *and* space complexity of $O(\sqrt{p_0})$, which gives the bound $\|p_0\| = \|q_0\| \geq 2\lambda$. However, this attack imposes a vast space complexity for moderate security levels. For $\lambda = 100$ bits, the memory requirements amounts to $\|n\| \times 1,125,899$ GB, which is insurmountable for any practical realizations of the attack.

5 SECURITY ANALYSIS

In this section, we provide a security proof in the standard model.

Theorem 1 *The proposed scheme is secure assuming that λ is sufficiently large.*

Proof. The proof models interaction between an adversary \mathcal{A} and a challenger \mathcal{C} , and proves collusion resistance concerning revoked users $\mathcal{R} = \mathcal{U} \setminus T$.

Setup. A challenger \mathcal{C} sets up an instance of the cryptosystem, and computes the public keys $PK = (\{g_i, y_i \mid 0 \leq i \leq N\}, n)$ and private keys $\{\gamma_i \mid 0 \leq i \leq N\}$ by invoking $\text{Setup}(N, \lambda)$. Since the random values (γ, \mathcal{P}) are chosen uniformly, the keys have a distribution to that of an actual construction. \mathcal{C} submits PK to \mathcal{A} .

Key Query. \mathcal{A} queries private user keys for a subset $S^* \subset \{1, \dots, N\}$. \mathcal{C} submits $\{\gamma_i \mid i \in S^*\}$ to \mathcal{A} .

Challenge. Let $\hat{g} = \prod_{j \in S^*} g_j$. The challenger invokes $(k_S, z) \leftarrow \text{Enc}(g_j, y_j \mid j \in S^*, n)$, where $k_S = \hat{g}^{\gamma^r}$ and $z = \hat{g}^r$.

The challenger randomly picks a bit $b \in \{0, 1\}$, and sets $k_b = k_S$ and $k_{1-b} = \hat{g}^c$, where c is a large secret integer. It then submits the triplet (z, k_0, k_1) to the adversary. This agree with the DDH challenge

$$(\hat{g}, \hat{g}^\gamma, \hat{g}^r, \hat{g}^{\gamma^r}, \hat{g}^c)$$

where $\hat{g}^\gamma = \prod_{j \in S^*} y_j$, and \hat{g}^{γ^r} is a valid encryption key and \hat{g}^r is a valid header.

Output. The challenge corresponds with two cases:

Case 1. The computational problem of \mathcal{A} is to determine if k_S is k_0 or k_1 with more than $\frac{1}{2} + \epsilon$ probability, where ϵ is a negligible probability. If the adversary succeeds at this, it is equivalent to that the adversary

can solve the DDH problem in polynomial time. If the subgroup is sufficiently large, this is known to be a computationally intractable problem.

Case 2. Since γ is secret and not known by the adversary, he can compute γ using the private keys/residues $(y_i, y_j \mid i, j \in S)$ according to

$$\gamma \equiv \begin{cases} \gamma_i & (\text{mod } p_0 q_0 \bar{p}_i) \\ \gamma_j & (\text{mod } p_i) \end{cases}$$

in agreement with Eq. (5) and the Chinese remainder theorem. Since this requires $(p_0, q_0, \bar{p}_i, p_i)$, which are secret and unknown to the adversary. This requires that the adversary finds the exact subgroup orders and/or decomposes the secret primes (p, q) , which means that the adversary will be able to solve the factorization problem. Assuming that λ and n are sufficiently large, this is known to be a computationally intractable problem. The adversary outputs a bit b' , where the probability that $b = b'$ is $\frac{1}{2} + \epsilon$. Thus, the proposed scheme is secure assuming that λ is sufficiently large. \square

6 CONCLUSION

Predominantly all existing stateless broadcast encryption schemes are based on bilinear pairings, with a couple of exceptions that are based on lattices. However, such schemes have in common some shortcomings, such as long decryption keys comprising the public keys of pertaining recipients. Decryption therefore necessitates access to public keys, which requires key management and impacts computational and transmission overhead, accessibility, and storage.

In this paper, we have proposed a novel broadcast encryption scheme that is based on the factorization problem and hidden RSA subgroups. It has some unique features. The encryption header is relatively short, and the decryption key consists only one key element, which is the private user key only. This eliminates the need for recipients to access public keys of other recipients and thus key management. An implication is anonymity, in which there is no longer any need that a user description list referencing the pertaining recipients and their public keys is attached to the ciphertexts. Future work based on the proposed approach includes anonymous attribute-based broadcast encryption.

ACKNOWLEDGEMENTS

Parts of this research has been supported by the NORCICS project, RCN grant number 310105.

REFERENCES

- Barker, E. (2016). Nist special publication 800-57. recommendation for key management. Technical report, National Institute of Standards and Technology. Part 1:General (Revision 4).
- Bellare, M., Boldyreva, A., Kurosawa, K., and Staddon, J. (2007). Multi-recipient encryption schemes: Efficient constructions and their security.
- Boneh, D., Gentry, C., and Waters, B. (2005). Collusion resistant broadcast encryption with short ciphertexts and private keys. In *Proceedings of the 25th Annual International Conference on Advances in Cryptology, CRYPTO'05*, pages 258–275, Berlin, Heidelberg. Springer-Verlag.
- Bourse, F., Sanders, O., and Traoré, J. (2020). Improved secure integer comparison via homomorphic encryption. In *Topics in Cryptology – CT-RSA 2020: The Cryptographers' Track at the RSA Conference 2020, San Francisco, CA, USA, February 24–28, 2020, Proceedings*, page 391–416, Berlin, Heidelberg. Springer-Verlag.
- Cao, Z. and Liu, L. (2015). On the disadvantages of pairing-based cryptography. *IACR Cryptology ePrint Archive*, 2015:84.
- Coron, J.-S., Joux, A., Mandal, A., Naccache, D., and Tibouchi, M. (2011). Cryptanalysis of the rsa subgroup assumption from tcc 2005. In Catalano, D., Fazio, N., Gennaro, R., and Nicolosi, A., editors, *Public Key Cryptography – PKC 2011*, pages 147–155, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Damgård, I., Geisler, M., and Krøigaard, M. (2008). A correction to "efficient and secure comparison for on-line auctions". *IACR Cryptology ePrint Archive*, 2008:321.
- Delerablée, C. (2007). Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Proceedings of the Advances in Cryptology 13th International Conference on Theory and Application of Cryptology and Information Security, ASIACRYPT'07*, pages 200–215, Berlin, Heidelberg. Springer-Verlag.
- Delerablée, C., Paillier, P., and Pointcheval, D. (2007). Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In *Proceedings of the First International Conference on Pairing-Based Cryptography, Pairing'07*, pages 39–59, Berlin, Heidelberg. Springer-Verlag.
- Dodis, Y. and Fazio, N. (2003). Public key broadcast encryption for stateless receivers. In Feigenbaum, J., editor, *Digital Rights Management*, pages 61–80, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Dubois, R., Guillevic, A., and Breton, M. S. L. (2013). Improved broadcast encryption scheme with constant-size ciphertext. In *Proceedings of the 5th International Conference on Pairing-Based Cryptography, Pairing'12*, pages 196–202, Berlin, Heidelberg. Springer-Verlag.
- Gentry, C. and Waters, B. (2009). Adaptive security in broadcast encryption systems (with short ciphertexts). In *Proceedings of the 28th Annual International Conference on Advances in Cryptology: The Theory and Applications of Cryptographic Techniques, EUROCRYPT '09*, pages 171–188, Berlin, Heidelberg.
- Georgescu, A. (2013). Anonymous lattice-based broadcast encryption. In *Proceedings of ICT-EurAsia, March 25-29, 2013*, pages 353–362, Berlin, Heidelberg. Springer.
- Groth, J. (2005). Cryptography in subgroups of \mathbb{Z}_n^* . In Kilian, J., editor, *Theory of Cryptography*, pages 50–65, Berlin, Heidelberg. Springer.
- Hajny, J., Dzurenda, P., Ricci, S., Malina, L., and Vrba, K. (2018). Performance analysis of pairing-based elliptic curve cryptography on constrained devices. In *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pages 1–5.
- He, K., Weng, J., Liu, J.-N., Liu, J. K., Liu, W., and Deng, R. H. (2016). Anonymous identity-based broadcast encryption with chosen-ciphertext security. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ASIA CCS '16*, pages 247–255, New York, NY, USA. ACM.
- Kim, J., Susilo, W., Au, M. H., and Seberry, J. (2013). Efficient semi-static secure broadcast encryption scheme. In *Pairing-Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers*, pages 62–76.
- Kim, J., Susilo, W., Au, M. H., and Seberry, J. (2015). Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. *IEEE Transactions on Information Forensics and Security*, 10(3):679–693.
- Lee, K. and Lee, D. H. (2015). Adaptively secure broadcast encryption under standard assumptions with better efficiency. *IET Information Security*, 9:149–157(8).
- Libert, B., Paterson, K. G., and Quaglia, E. A. (2012). Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In Fischlin, M., Buchmann, J., and Manulis, M., editors, *Public Key Cryptography – PKC 2012*, pages 206–224, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Malek, B. and Miri, A. (2012). Adaptively secure broadcast encryption with short ciphertexts. *International Journal of Network Security*, 14(2):71–79.
- Naccache, D. and Stern, J. (1998). A new public key cryptosystem based on higher residues. In *Proceedings of the 5th ACM Conference on Computer and Communications Security, CCS '98*, page 59–66, New York, NY, USA. Association for Computing Machinery.
- Naor, D., Naor, M., and Lotspiech, J. B. (2001). Revocation and tracing schemes for stateless receivers. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '01*, pages 41–62, London, UK, UK. Springer-Verlag.
- Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceedings*, pages 223–238.

- Park, J. H., Kim, H. J., Sung, M. H., and Lee, D. H. (2008). Public key broadcast encryption schemes with shorter transmissions. *IEEE Transactions on Broadcasting*, 54(3):401–411.
- Phan, D.-H., Pointcheval, D., Shahandashti, S. F., and Strefler, M. (2013). Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4):251–265.
- Sakai, R. and Furukawa, J. (2007). Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217.
- Wang, J. and Bi, J. (2010). Lattice-based identity-based broadcast encryption scheme. *IACR Cryptology ePrint Archive*, 2010:288.
- Zhang, L., Hu, Y., and Wu, Q. (2012). Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. *Mathematical and Computer Modelling*, 55(1):12 – 18. *Advanced Theory and Practice for Cryptography and Future Security*.

