Collusion-resistant broadcast encryption based on hidden RSA subgroups[⋆]

Sigurd Eskeland

Norsk Regnesentral, Postboks 114 Blindern, 0314 Oslo, Norway
sigurd@nr.no

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. Predominantly 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 allows a sender to securely share a message to multiple recipients using a single ciphertext, in contrast to conventional encryption where the sender needs to compute a single ciphertext for every recipient. The sender specifies a subset of recipients $T \subseteq \mathcal{U}$, and computes a ciphertext that can only be decrypted by that subset T. A significant feature of broadcast encryption are no synchronisms and no interactions between the sender and recipients, nor among the recipients. Performance goals include minimum transmission overhead, computational effort, storage size, and key management.

Stateful broadcast encryption schemes maintain a state according to changes in group membership, in which the broadcast key must be updated to maintain forward and backward secrecy. With regard to performance, only those key elements that are affected by a user change should be updated, meaning that key

[⋆] This is a postprint version of the paper presented at SECRYPT 2022 under the same title (DOI: 10.5220/0011140000003283).

updates depend on previous states in group membership. For this reason, stateful schemes tend therefore to have a better scalability than stateless broadcast encryption. An inherent disadvantage is that if a user misses an update message, he or she will be left out from subsequent sessions.

In *stateless* broadcast encryption, ciphertexts are computed for arbitrary composed groups of recipients $T \subseteq \mathcal{U}$, independently of previous broadcasts as there is no updating of key material due to changes of group memberships. Early approaches were variations on combinatorial tree-based schemes, such as the subset cover framework [23], incurring complex key management and multiple encryptions in accordance with the pertaining user subsets. From 2005 and onwards, bilinear pairs are the predominant basis for stateless broadcast encryption [3, 8, 9, 11, 13, 18–21, 25–27, 29], where usually a single ciphertext header element is computed for a group T (or a complementary "revoked" subset $R = \mathcal{U} \backslash T$), while the decryption algorithm requires application of the private key x_i of a user P_i in 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:

$$\mathrm{Dec}(x_i,\, \{y_j \mid P_j \in (T \backslash \{P_i\})\}, B)$$

where the *decryption key* is composed of $(x_i,\, \{y_j \mid P_j \in (T \backslash \{P_i\})\})$, in which the number of elements equals the size of T. This brings about the following issues:

1. *Complex decryption keys and key management.* Since decryption is only possible with a complete decryption key, all pertaining public keys *must* be accessible in order to decrypt. This necessity may be inconvenient and impractical in some settings, in particular if one or more such keys are not available at the time of decryption.
2. *Computational overhead.* The decryption key size is linear to the size of T. This increases the storage and computational overhead accordingly.
3. *Transmission overhead.* Due to the complex decryption key, the encryption header must contain a list specifying the recipients T (or the revoked recipients R) and their public keys. This increases the transmission overhead accordingly.
4. *Privacy issues.* The list of recipients discloses to both intended and non-intended recipients all intended recipients. This may be just as sensitive information as the encrypted information itself, in particular if the sensitivity of the encrypted content is high.

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.

Anonymous broadcast encryption. A variant of broadcast encryption is anonymous broadcast encryption of which there exist two subcategories: 1) Fully anonymous broadcast encryption, where the intended recipients are not identifiable by anyone, including intended and non-intended recipients [12]. 2) So-called outsider anonymous broadcast encryption, where the intended recipients are identifiable by intended recipients, but not identifiable by non-intended recipients or someone else. Anonymous broadcast encryption schemes are inflicted with efficiency issues, and in some with long ciphertexts whose number of elements is linear to T (e.g., [17]).

Cryptographic primitives. Broadcast encryption is predominantly based on bilinear pairings and elliptic curve cryptography due to that bilinear pairings have computational properties consistent with multi-party computations. Bilinear pairings has some disadvantages that are often overlooked. Cao et al. [5] 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. Bilinear pairings also have a high computational load that reduces the advantages gained from the smaller key sizes. There are furthermore some practical difficulties. Pairing-based cryptography is considered hard to understand for most engineers and difficult to implement. Hajny et al. [16] 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 [14, 28]. However, these schemes produce variable header sizes and may not be practical. It is thus of great interest to explore the applicability of other 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 attractive features:

- Simplified key management. Decryption requires a single fixed-size private key-element only. This eliminates complex key management, since there is no need for other recipients' public keys in order to decrypt, as is the case for previous stateless broadcast encryption schemes.
- Transmission efficiency. Since decryption requires only a single private key-element and no complex decryption key, the need for ciphertexts having an accompanying recipient list specifying the pertaining recipients and their public keys is eliminated. This reduces the transmission overhead accordingly. Compared to the RSA cryptosystem by having multiple encryptions for N recipients, the reduced transmission overhead is in the order of 10-25 times (Table 1).
- Anonymity. Since there is no explicit need for recipient lists, the proposed scheme provides user anonymity.

- Well-understood security assumption. The proposed broadcast encryption scheme is the first to be based on the factorization problem and hidden RSA subgroups.
- Computational efficiency. Decryption requires just a single exponential modular operation.

To the best of our knowledge, our construction is the first collusion-resistant broadcast encryption scheme that is based on RSA subgroup security assumption. This cryptographic primitive is simpler and easier to implement than those based on bilinear pairings. Furthermore, the single-element decryption key is a great improvement compared to other broadcast encryption schemes, avoiding complex key management.

2 Related work

Earlier approaches to stateless broadcast encryption assume tree-based structures. Such an approach utilizing secret user keys is the "subset-cover" framework proposed by Naor et al. [23] in 2001, in which keys of user subsets are derived from a virtual tree structure. In 2002 Dodis et al. [10] proposed a public key broadcast encryption (PKBE) scheme building on [23]. Such solutions have complex key management and requires multiple encryptions for a single message, with one encryption for each relevant user subset.

Boneh, Gentry and Waters [3] proposed the first 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 one header element, and a generalized variant BGW_2 consisting of parallel instances of BGW_1 achieving a tradeoff of $\mathcal{O}(\sqrt{n})$ decryption key size and $\mathcal{O}(\sqrt{n})$ ciphertext size. Identity-based variants of (BGW_1), having user identities as public keys, were proposed by Delerablée et al. [8] and Sakai [27] with the same performance properties as (BGW_1), except shorter public key length due to the identity-orientation. In 2007, Delerablée et al. [9] 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 [13], and later schemes are found in [18,20,21,26,29]. Some other PKBE schemes are found in [11, 19, 25].

All the mentioned schemes (other than tree subset-cover type schemes) are based on bilinear pairings. In addition to bilinear pairings, lattices is another cryptographic primitive that has been proposed for realizing PKBE [14, 28].

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 [2] instead of generating unique random integers for each ciphertext.

3 Preliminaries

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

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

  $$p = 2p_0 \prod_{j=1}^{\lceil N/2 \rceil} p_j + 1 \quad \text{and} \quad q = 2q_0 \prod_{j=\lceil N/2 \rceil + 1}^{N} p_j + 1 \tag{1}$$

  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 $g = \alpha^2 \bmod n$, 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

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

  The order of $\mathbb{G}_i$ is hidden, since $\mathcal{P}$ are secret.
- Select a large random secret integer γ, whose bitsize is at least that of n.

Next we present the relevant computational hardness assumptions.

3.1 Security assumptions

Background on subgroups on hidden orders. Groth [15] proposed using small subgroups in $\mathbb{Z}_n^*$ of *hidden* orders. The purported motivation was efficiency purposes provided by the smaller subgroups for signature-, commitment- and encryption cryptosystems. In this regard, Groth proposed the decisional RSA 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. [4]. These assumptions are similar to high-residuosity assumptions, such as [22], and the composite residuosity assumption of the Paillier cryptosystem [24].

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 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., $(r^n)^\lambda \bmod n^2 = 1$. In our cryptosystem, subgroups of hidden orders are used for preventing disclosure of the secret integer γ, as discussed below.

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 $\big(g, g^a, g^b, z_b\big)$, 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 $\frac{1}{2} + \varepsilon$ 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.

Congruences and subgroups of hidden orders. Consider the modular residue $\gamma_i = \gamma \bmod p_0 q_0 \bar{p}_i$, where $\bar{p}_i$ is defined in Eq. (2). The prime p_k divides $\bar{p}_i$ if $i \neq k$. This implies the congruences $\gamma_i \equiv \gamma_j \pmod{p_k}$, $1 \leq i, j, k \leq N$, $i \neq j \neq k$, since

$$\begin{aligned} \gamma_i \bmod p_k &= (\gamma \bmod p_0 q_1 \bar{p}_i) \bmod p_k \\ = \gamma_j \bmod p_k &= (\gamma \bmod p_0 q_1 \bar{p}_j) \bmod p_k = \gamma \bmod p_k \end{aligned}$$

For the group $\mathbb{G}_k$ of order p_k generated by g_k, we have likewise

$$g_k^{\gamma_i} \equiv g_k^{\gamma_j} \equiv g_k^{\gamma} \pmod{n} \quad \text{for} \quad 1 \leq i, j, k \leq N, i \neq j \neq k \tag{3}$$

where g_k generates a RSA subgroup $\mathbb{G}_k$. The congruences hold since the order of $\mathbb{G}_k$ is $p_0 q_0 p_k$, which divides the moduli of γ_i and γ_j, $i \neq j \neq k$.

In the proposed scheme γ is a secret integer. This means that for any two residues $\gamma_i = \gamma \bmod p_0 q_0 \bar{p}_i$ and $\gamma_j = \gamma \bmod p_0 q_0 \bar{p}_j$, γ can be disclosed by means of the Chinese remainder theorem:

$$\gamma \equiv \begin{cases} \gamma_i & \pmod{p_0 q_0 \bar{p}_i} \\ \gamma_j & \pmod{p_i} \end{cases} \tag{4}$$

if and only if $(p_0, q_0, \bar{p}_i, p_i)$ are known. To prevent disclosure of γ, we use subgroups of hidden orders, in which all primes in $\mathcal{P}$ are secret. This ensures *collusion resistance*, preventing any subset of colluding users $\mathcal{R}$ from establishing γ.

On the special RSA moduli and 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 $\mathbb{G}_i < \mathbb{Z}_n^*$ in conjunction with g_i than by factoring methods such as general number field sieves [7]. The secret primes (p_0, q_0), cf. Eq. (1), are necessary to prevent factorization of n in conjunction with g_i, since the absence of these primes would allow trivial factorization.

Euler's theorem states that $a^{\phi(n)} \equiv 1 \pmod{n}$, where a is an arbitrary integer. Recall that g_i is a generator of $\mathbb{G}_i$ of order $p_0 q_0 p_i$. Accordingly, $g_i^{p_0 q_0 p_i} \equiv \alpha^{\phi(n)} \equiv 1 \pmod{n}$, and $g_i^{p_0 q_0 p_i} = kn + 1$, where k is a positive integer. Because of the composition of the RSA factor p, cf. Eq. (1), none of the primes composing q, i.e., $(q_0, \{, p_i \mid \lceil \frac{N}{2} \rceil + 1 \leq i \leq N\})$, divide $p - 1$. Thus

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

Table 1: Parameter and header sizes

λ	N	$\|\|c\|\|$	δ
80	10	1120	9,1
80	20	1920	10,7
80	50	4320	11,9
80	100	4320	12,3
112	10	2048^*	13,1
112	20	2688	15,2
112	50	6048	16,9
112	100	6048	17,6
128	10	3072^*	17,1
128	20	3072	20,0
128	50	6912	22,2
128	100	6912	23,1

and k' is a positive integer. Using this fact, p can be found if p_0 is known by

$$p = \gcd\left((g_i^{p_0} \bmod n) - 1, n\right)$$

The RSA security strength λ (in number of bits) is therefore essentially equivalent to the size of (p_0, q_0), i.e., $\lambda = ||p_0|| = ||q_0||$. However, consideration has to be taken when selecting an RSA modulus whose prime factors have a unusual composition. For example, the attack of Coron et al. [6] has a computational time *and* space complexity of $\mathcal{O}(\sqrt{p_0})$, 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 the order of $2^{50} \approx 1,125 \cdot 10^{15}$, which is insurmountable for any practical realizations of the attack.

3.2 Parameter selection and header size

Taking into account the mentioned attack of Coron et al. [6], we suggest that $||p_0|| = ||q_0|| = 2\lambda$, and similarly $||p_j|| = \lambda$, $1 \leq j \leq N$, to ensure a sufficiently large distribution of subgroups and private keys. The header size $||c||$ is confined by the RSA modulus size $||n||$ and proportional the number of recipients N and the security level λ, so that $||c|| = ||n|| = 4\lambda + N\lambda$. Table 1 shows header size as a function of n and λ, where $\delta = \frac{N||c^*||}{||c||}$ is the transmission efficiency compared to the RSA cryptosystem, i.e., the ratio between the size of N RSA encryptions $||c^*||$ and the header size $||c||$ w.r.t. N recipients for the same λ.

The number of recipients for an broadcast encryption and an RSA ciphertext for the same security level NIST suggests RSA modulus sizes of 1024 bits for 80 bits security level, 2048 bits for 112 bits security level, and 3072 bits for 128 bits security [1]. The asterisk indicates that the RSA modulus is incremented to match the NIST recommendations for those cases.

3.3 Broadcast encryption algorithms

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

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

Encryption For any subset $T \subseteq \mathcal{U}$, where $\mathcal{R} = \mathcal{U} \backslash T$ is the corresponding set of excluded (or revoked) users, the encryption algorithm $(k_T, z) \leftarrow \mathrm{Enc}(\{g_j, y_j \mid P_j \in \mathcal{R}\}, n)$ 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 $k_T \leftarrow \mathrm{Dec}(\gamma_i, z, n)$ 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 $(k'_T, z) \leftarrow \mathrm{Enc}(\{g_j, y_j \mid P_j {\in} \mathcal{R}\}, n)$ and $k''_T \leftarrow \mathrm{Dec}(\gamma_i, z, n)$ match, i.e., $k'_T = k''_T$.

3.4 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 security model model lets the adversary define an arbitrary set of compromised users S^* that is consistent with a set of revoked users $\mathcal{R} = \mathcal{U} \backslash T$, in which the adversary is permitted to obtain the private keys of a S^*, thus modelling a colluding set of user $\mathcal{R}$.

Setup. The challenger computes $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{Setup}(N, \lambda)$ 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 $S = \{1, \ldots, N\}$. The challenger submits $\{\gamma_i \mid i \in S^*\}$ to $\mathcal{A}$.

Challenge. The challenger invokes $(k_S, z) \leftarrow \mathrm{Enc}(g_j, y_j \mid j \in S^*, n)$. 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 $|\Pr(b' = b) - \frac{1}{2}| \leq \varepsilon$, 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). The security parameter λ determines the minimum subgroup order $\lambda = \min(p \in \mathcal{P})$.
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

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

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

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

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 special case $\mathcal{R} = \emptyset$.

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

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

and the encryption header

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

For the special case $\mathcal{R} = \emptyset$ 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 decryption algorithm (Eq. (5a)) is consistent with the output of the encryption algorithm (Eq. (5d)):

$$\begin{aligned}
k_{T,i} \equiv z^{\gamma_i} &\equiv \big((\prod_{k\in\mathcal{R}} g_k)^r\big)^{\gamma_i} \pmod{n} && \text{(5a)}\\
&\equiv \prod_{k\in\mathcal{R}} g^{r\bar{p}_k(\gamma \bmod p_0q_0p_k)} \pmod{n} && \text{(5b)}\\
&\equiv \big(\prod_{k\in\mathcal{R}} g_k\big)^{r\gamma} \pmod{n} && \text{(5c)}\\
&\equiv \big(\prod_{k\in\mathcal{R}} y_k\big)^{r} \pmod{n} = k_T && \text{(5d)}
\end{aligned}$$

for γ_i, $i \notin \mathcal{R}$, in agreement with Eq. (3). The congruences hold since the order of the subgroup $\mathbb{G}_k$ generated by g_k is $p_0q_0p_k$, and $p_0q_0p_k$ divides the modulus $p_0q_0\bar{p}_i$ of γ_i for $i \neq k$. 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 $n = (2p_0p_1+1)(2q_0p_2p_3+1)$. Then $\gamma_1 = \gamma \bmod p_0q_0p_2p_3$ and $\gamma_2 = \gamma \bmod p_0q_0p_1p_3$. 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

$$g_3^{\gamma_1} = g^{\bar{p}_3\gamma_1} = g^{p_1p_2\gamma_1} = g^{p_1p_2(\gamma \bmod p_0q_0p_2p_3)} \equiv g^{p_1p_2\gamma \bmod p_0q_0p_1p_2p_3} \equiv g^{\bar{p}_3\gamma}$$

and

$$g_3^{\gamma_2} = g^{\bar{p}_3\gamma_2} = g^{p_1p_2\gamma_2} = g^{p_1p_2(\gamma \bmod p_0q_0p_1p_3)} \equiv g^{p_1p_2\gamma \bmod p_0q_0p_1p_2p_3} \equiv g^{\bar{p}_3\gamma}$$

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

$$g_3^{\gamma_3} = g^{p_1p_2\gamma_3} = g^{p_1p_2(\gamma \bmod p_0q_0p_1p_2)} \not\equiv g^{\bar{p}_3\gamma}$$

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

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 $\mathcal{R} = \mathcal{U}\backslash T$.

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 Setup(N, λ). Since the random values $(\gamma, \mathcal{P})$ 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 $S^* \subset \{1, \ldots, N\}$. $\mathcal{C}$ submits $\{\gamma_i \mid i \in S^*\}$ to $\mathcal{A}$.

Challenge. Let $\hat{g} = \prod_{\forall j \in \mathcal{S}^*} g_j$. The challenger invokes $(k_S, z) \leftarrow \mathrm{Enc}(g_j, y_j \mid j \in S^*, n)$, 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

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

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

Output. Given

$$\left(\hat{g},\ \hat{g}^{\gamma},\ z = \hat{g}^{r},\ k_b = \hat{g}^{\gamma r},\ k_{b-1} = \hat{g}^{c}\right)$$

where $\hat{g}^{\gamma} = \prod_{\forall j \in \mathcal{S}^*} y_j$. The computational problem of $\mathcal{A}$ is to determine if k_S is k_0 or k_1 with more than $\frac{1}{1} + \epsilon$ 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 subgroups is sufficiently, this is known to be a computationally intractable problem.

Otherwise, given $(\hat{g}, \gamma)$ the adversary can compute $\hat{g}^{\gamma}$. But 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

$$\gamma \equiv \begin{cases} \gamma_i & \pmod{p_0 q_0 \bar{p}_i} \\ \gamma_j & \pmod{p_i} \end{cases}$$

in agreement with Eq. (4) 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 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 output a bit b', where the probability that $b = b'$ is $\frac{1}{1} + \epsilon$. Thus, the proposed scheme is secure assuming that λ is sufficiently large. □

6 Conclusion

Existing stateless broadcast encryption schemes have some shortcomings, such as complex decryption keys, privacy issues, key management, and some transmission overhead. In this paper, we have proposed a novel broadcast encryption scheme that is based on the factorization problem and hidden RSA subgroups. The proposed scheme has some unique features. The decryption key consists only of a single-private key element, and no public keys of other recipients are needed for decryption. An implication of the single-element decryption key is anonymity, since there is no need to attach a recipient list referencing their public keys to the ciphertexts, as is the case for schemes based on bilinear pairings. Hence, key management is utterly simplified, and transmission overhead is in this regard reduced. Future work includes to consider how other privacy-preserving group-oriented security applications can be built on hidden RSA subgroups, such as attribute-based broadcast encryption and group authentication.

Acknowledgements

Parts of this research has been supported by basic institute funding at Norsk Regnesentral, RCN grant number 194067, and the NORCICS project, RCN grant number 310105.

References

1. Elaine Barker. Nist special publication 800-57. recommendation for key management. Technical report, National Institute of Standards and Technology, 01 2016. Part 1:General (Revision 4).
2. M. Bellare, A. Boldyreva, K. Kurosawa, and J. Staddon. Multi-recipient encryption schemes: Efficient constructions and their security. 2007.
3. Dan Boneh, Craig Gentry, and Brent Waters. 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, 2005. Springer-Verlag.
4. Florian Bourse, Olivier Sanders, and Jacques Traoré. 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, 2020. Springer-Verlag.
5. Zhengjun Cao and Lihua Liu. On the disadvantages of pairing-based cryptography. *IACR Cryptology ePrint Archive*, 2015:84, 2015.
6. Jean-Sébastien Coron, Antoine Joux, Avradip Mandal, David Naccache, and Mehdi Tibouchi. Cryptanalysis of the RSA subgroup assumption from TCC 2005. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *Public Key Cryptography – PKC 2011*, pages 147–155, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.
7. Ivan Damgård, Martin Geisler, and Mikkel Krøigaard. A correction to "efficient and secure comparison for on-line auctions". *IACR Cryptology ePrint Archive*, 2008:321, 01 2008.
8. Cécile Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'07, pages 200–215, Berlin, Heidelberg, 2007. Springer-Verlag.
9. Cécile Delerablée, Pascal Paillier, and David Pointcheval. 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, 2007. Springer-Verlag.

10. Yevgeniy Dodis and Nelly Fazio. Public key broadcast encryption for stateless receivers. In Joan Feigenbaum, editor, *Digital Rights Management*, pages 61–80, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

11. Renaud Dubois, Aurore Guillevic, and Marine Sengelin Le Breton. 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, 2013. Springer-Verlag.

12. Nelly Fazio and Irippuge Milinda Perera. Outsider-anonymous broadcast encryption with sublinear ciphertexts. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 225–242, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

13. Craig Gentry and Brent Waters. 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, 2009.

14. Adela Georgescu. Anonymous lattice-based broadcast encryption. In *Proceedings of ICT-EurAsia, March 25-29, 2013*, pages 353–362, Berlin, Heidelberg, 2013. Springer.

15. Jens Groth. Cryptography in subgroups of $\mathbb{Z}_n^*$. In Joe Kilian, editor, *Theory of Cryptography*, pages 50–65, Berlin, Heidelberg, 2005. Springer.

16. Jan Hajny, Petr Dzurenda, Sara Ricci, Lukas Malina, and Kamil Vrba. 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, 2018.

17. Kai He, Jian Weng, Jia-Nan Liu, Joseph K. Liu, Wei Liu, and Robert H. Deng. 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, 2016. ACM.

18. J. Kim, W. Susilo, M. H. Au, and J. Seberry. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. *IEEE Transactions on Information Forensics and Security*, 10(3):679–693, March 2015.

19. Jongkil Kim, Willy Susilo, Man Ho Au, and Jennifer Seberry. 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, 2013.

20. Kwangsu Lee and Dong Hoon Lee. Adaptively secure broadcast encryption under standard assumptions with better efficiency. *IET Information Security*, 9:149–157(8), May 2015.

21. Behzad Malek and Ali Miri. Adaptively secure broadcast encryption with short ciphertexts. *International Journal of Network Security*, 14(2):71–79, 2012.

22. David Naccache and Jacques Stern. 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, 1998. Association for Computing Machinery.

23. Dalit Naor, Moni Naor, and Jeffrey B. Lotspiech. 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, 2001. Springer-Verlag.

24. Pascal Paillier. 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, Proceeding*, pages 223–238, 1999.
25. J. H. Park, H. J. Kim, M. H. Sung, and D. H. Lee. Public key broadcast encryption schemes with shorter transmissions. *IEEE Transactions on Broadcasting*, 54(3):401–411, Sept 2008.
26. Duong-Hieu Phan, David Pointcheval, Siamak F. Shahandashti, and Mario Strefler. Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts. *International Journal of Information Security*, 12(4):251–265, 2013.
27. Ryuichi Sakai and Jun Furukawa. Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217, 2007.
28. Jin Wang and Jingguo Bi. Lattice-based identity-based broadcast encryption scheme. *IACR Cryptology ePrint Archive*, 2010:288, 2010.
29. Leyou Zhang, Yupu Hu, and Qing Wu. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. *Mathematical and Computer Modelling*, 55(1):12 – 18, 2012. Advanced Theory and Practice for Cryptography and Future Security.