Proceedings of the 2nd International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/114/2024.18213

# A Multi-Authority RSA Broadcast Encryption Scheme Based on Modulus $N_i$

**Liyin Hu**

School of International Business, Chengdu Institute Sichuan International Studies University, Chengdu, 611844, China

2195546449huliyin@gmail.com

**Abstract.** With the development of network technology, multicast and broadcast communications have gradually replaced unicast communication. Traditional RSA encryption is no longer suitable for many network applications, such as scenarios where multiple users with different privilege levels access paid content. This paper demonstrates the limitations of the key management protocol proposed by Lin in 2004 under a multi-privilege user system and redefines the algorithm for generating the modulus $N_i$, achieving a hierarchical division of privilege levels. Based on this key management protocol, a new multi-privilege RSA broadcast encryption scheme is proposed, addressing the limitations of traditional RSA encryption in one-to-many communication scenarios and taking into account the different privilege levels of users. This scheme allows high-privilege users to decrypt more information, while low-privilege users decrypt less information, adapting to the needs of practical applications. By dynamically dividing user privilege levels and distributing private keys of different decryption levels accordingly, the system enables dynamic user addition and removal, enhancing the scalability and flexibility of the system. This expands the application scenarios of RSA encryption while increasing its security and practicality.

**Keywords:** Privilege level division, broadcast encryption, key management protocol.

## 1. Introduction

The concept of broadcast encryption, introduced by Berkovits, allows a sender to efficiently broadcast encrypted messages to selected recipients while preventing others from decrypt them [1]. Traditionally, RSA encryption, a public-key cryptosystem proposed by Rivest, Shamir, and Adleman in 1977, is designed for one-to-one communication [2]. However, with the rapid growth of networks, most applications now operate in one-to-many communication scenarios, making traditional RSA cryptosystems less suitable. Consequently, research on multi-user cryptosystems leveraging broadcast encryption.has expanded. Sigurd proposed a collusion-resistant scheme based on hidden RSA subgroups, while Baee et al. introduced a broadcast authentication scheme to enhance vehicle-to-vehicle (V2V) communication security improvement [3-4]. Balakrishna conducted a systematic review on broadcast encryption and Srivastava et al. proposed a multivariate polynomial-based identity-based broadcast encryption (MulIB-BE) scheme [5-6]. Further, Rabaninejad et al. developed an attribute-based anonymous broadcast encryption scheme (Improved-YRL), Dupin et al. introduced a symmetric cryptography-based broadcast encryption model, and Lin Guoqing et al. proposed a key management

DOI: 10.54254/2755-2721/114/2024.18213

protocol suitable for RSA broadcast encryption [7-9]. Li Xiaofeng et al. designsed a multi-user RSA encryption scheme for targeted receivers [10]. Collectively, these contributions have significantly advanced broadcast encryption technology, particularly in improving the efficiency, security, and practicality. Based on the research of Lin Guoqing and Li Xiaofeng, this paper proposes a new multi-privilege RSA broadcast encryption scheme, which implements the division of multiple privilege levels.

## 2. Related works

This section introduces the key generation algorithm for generating multiple private keys from a single public key and reviews Lin's 2004 RSA-based broadcast encryption protocol. It also defines the public key modulus $N_i$ and the secret key $S_i$ generation algorithm used for privilege level division, forming the theoretical foundation of this paper.

Key generation algorithm: Assume that a broadcast center intends to broadcast messages to $n$ users. The broadcast center selects a public key $e$ and generates a private key $d_i$ for each user $u_i$. For each user $u_i$, different moduli $n_i$ are selected for key generation, generating a different private key $d_i$. This can be viewed as a function $d_i = f(n_i)$ where the input is the modulus $n_i$ and the output is the private key $d_i$, with $n_i = p_i * q_i$, and $\varphi(n_i) = (p_i - 1) * (q_i - 1)$, ensuring that $\gcd(\varphi(n_i), e) = 1$, and thus $ed_i \equiv 1 \bmod \phi(n_i)$. For example, with $e = 7$, let $n_1 = 7 \times 11 = 77$, so $\varphi(n_1) = 60$, and $7d_1 \equiv 1 \bmod 60$, yielding $d_1 = 43$, Similarly, let $n_2 = 2 * 11 = 22$, so $\varphi(n_2) = 10$, and $7d_2 \equiv 1 \bmod 10$, yielding $d_2 = 3$. This proves that for each user $u_i$, a different private key $d_i$ corresponding to $u_i$ can be generated. This key generation algorithm improves the computational efficiency of the key management center and reduces storage requirements.

In Lin Guoqing and Li Xiaofeng's research on RSA broadcast encryption schemes, both adopted similar key generation algorithms. However, in their schemes, the public key modulus $N$ is defined as $N = n_1 * n_2 * ... * n_i$, and encryption is performed using $N$ as the modulus. Since $N$ is a multiple of each $n_i$, any user $u_i$ can use their corresponding private key $d_i$ to decrypt all broadcast messages. The proof of this point is as follows:

Assume a broadcast system has two users $u_1$ and $u_2$. The broadcast center needs to send two messages: $M_1$(the message intended for user $u_1$) and $M_2$(the message intended for user $u_2$). The public key is $e$, and $N = n_1 * n_2$, where $n_1 = p_1 * q_1$, and $n_2 = p_2 * q_2$. During decryption, user $u_1$ uses their private key $(d_1, n_1)$ to decrypt message $M_1$, where:

$$M_1 = C_1^{d_1} \bmod n_1 = (M_1^{ed_1} \bmod N) \bmod n_1$$

Since $N = n_1 * n_2$, $N$ is a multiple of $n_1$, thus:

$$M_1 = (M_1^{ed_1} \bmod N) \bmod n_1 = M_1^{ed_1} \bmod n_1$$

However, if user $u_2$, acting as an attacker, attempts to decrypt both messages, they will derive:

$$M_1 = (M_1^{ed_2} \bmod N) \bmod n_2 = M_1^{ed_2} \bmod n_2$$

By Euler's theorem, since $\gcd(M_1, n_1) = 1$ and $\gcd(M_2, n_2) = 1$, it follows that:

$$M_1^{\varphi(n_1)} \equiv 1 \bmod n_1, M_1^{\varphi(n_2)} \equiv 1 \bmod n_2$$

Thus:

$$M_1^{ed_1} \equiv M_1^{k\varphi(n_1)+1} \equiv M[M^{\varphi(n_1)}]^k \bmod n_1 \equiv M[1]^k \bmod n_1 \equiv M \bmod n_1 = M$$

Similarly:

$$M_1^{ed_2} \equiv M \bmod n_2 = M$$

Therefore, user $u_2$, using their private key $(d_2, n_2)$, can also decrypt message $M_1$, which is unreasonable for a broadcast system with privilege division.

DOI: 10.54254/2755-2721/114/2024.18213

It is worth noting that Lin's scheme proposed a key management protocol that divides plaintext into groups and encrypts them using a randomly generated secret key $S$, which is then broadcasted after RSA encryption. However, their scheme did not explicitly define how the random secret key $S$ is generated. Moreover, to prevent users from decrypting others' messages, $m$ different secret keys $S_i$ should be used to encrypt each of the $m$ messages, and the secret key $S_i$ used for encrypting each plaintext $M_i$ must differ.

*2.1. Public key modulus $N_i$ and secret key $S$ definition for privilege division*

To avoid a scenario where one user can decrypt messages intended for other users, this paper builds upon Lin's scheme and proposes an RSA encryption scheme suitable for a multi-privilege broadcast system. This scheme redefines the public key modulus $N_i$ and the secret key $S$ generation suitable for a privilege division system.

*2.1.1. Definition of public key modulus $N_i$.* To distinguish between users' privilege levels, assume a broadcast center needs to broadcast $m$ messages. It should generate $m$ different $N_i$. The user with the highest privilege level should be able to decrypt all messages, and the private key distributed to this user by the key management center is denoted as $(d_m, n_m)$. Each $N_i$ should be a multiple of $n_m$ to ensure that this user can decrypt all messages. Therefore, the formula for the public key modulus $N_i$ is:

$$N_i = r_i * \prod_{i=1}^{m} n_i$$

$$N_1 = r_1 * n_1 * n_2 ... * n_m$$

$$N_2 = r_2 * n_2 * ... * n_m$$

…

$$N_m = r_m * n_m$$

where $r_i$ is a confusion factor. During encryption, the secret key $S_i$ is encrypted using $N_i$. For user $u_1$, if they attempt to use their private key $d_1$ to decrypt any message other than $M_1$, they will fail because $N_i (2 \leq i \leq m)$ is not a multiple of $n_1$, preventing the correct decryption of the secret key $K_i$. This will be proven in Section 4.

*2.1.2. Secret key $K_i$ generation.* The secret key $K_i$ is used for symmetric encryption of plaintext messages. To ensure that users with different privilege levels can decrypt different messages, $m$ secret keys $K_i$ are generated for $m$ plaintext messages $M_i$. The key management center selects $m$ large numbers $t_i$ as modulus confusion factors, which should be slightly smaller than the corresponding $M_i$. The secret key $K_i$ is then generated by performing a modulus operation on $M_i$:

$$K_i = M_i \bmod t_i$$

## 3. RSA broadcast encryption

The scheme proposed consists of three stages: in the stage of system initializagtion, the key management center generates the public key $(e, N_i)$ and private keys $d_i$ for each level $L = i, 0 \leq i \leq m$. The private keys are distributed to users based on their assigned privilege levels $L = i$, where $0 \leq i \leq m$. Each user receives the corresponding private key $d_i$ according to their privilege level. Second, in the encryption stage, the broadcast center generates a secret key $K_i$ for each plaintext message $M_i$, where $0 \leq i \leq m$. The secret key $K_i$ is used to symmetrically encrypt the plaintext message $M_i$, producing the information ciphertext $C_i$. The secret key $K_i$ is then encrypted using the RSA algorithm, resulting in the secret key ciphertext $S_i$. Both the secret key ciphertext $S_i$ and the information ciphertext $C_i$ are broadcasted. Last, when users receive the broadcast message, they use their private key $d_i$ to decrypt the corresponding secret key $K_i$. Once the secret key $K_i$ is obtained, it is used to decrypt the information ciphertext $C_i$ to retrieve the original plaintext message $M_i$.

DOI: 10.54254/2755-2721/114/2024.18213

### *3.1. System initialization*

Assume the broadcast center needs to broadcast $m$ plaintext messages $\{M_1, M_2, \dots, M_m\}$, The key management center divides the users into $m+1$ privilege levels $L = \{0,1,2, \dots, m\}$. Users are assigned a privilege level upon registration. The lowest privilege level is $L = 0$, representing unauthorized (or illegal) users who do not receive private keys and thus cannot decrypt any messages. The highest privilege level is $L = m$, where users can decrypt all messages. The relationship between privilege levels required to decrypt messages is as follows:

$$M_m > M_{m-1} > \cdots > M_2 > M_1$$

Before transmission, the key management center generates $m$ public keys and $m$ private keys. First, it selects $2m$ distinct large prime numbers $p_1, q_1, p_2, q_2, \dots, p_{m-1}, q_{m-1}, p_m, q_m$. The decryption modulus is $n_i = p_i * q_i$, and the Euler's totient function is $\varphi(n_i) = (p_i - 1) * (q_i - 1)$. A public exponent $e$ is selected such that $e$ is a positive integer smaller than and coprime with each $\varphi(n_i)$. Next, $m$ large primes $r_i$are chosen as confusion factors, ensuring that $r_i \neq e \neq p_1 \dots p_m \neq q_1 \dots q_m$. The public key modulus $N_i$ is calculated as:

$$N_i = r_i * \prod_{i=1}^{m} n_i \tag{1}$$

The broadcast center uses $(e, N_i)$ as the public key and generates $m$ private keys $d_i$, where $d_i$ satisfies the congruence:

$$e^{d_i} \equiv 1 \bmod \varphi(n_i) \tag{2}$$

The resulting private key set $\{d_1, d_2, \dots d_m\}$ is distributed to users based on their privilege levels. Users with privilege level $L = i, \text{where}(0 \leq i \leq m)$ can decrypt the set of ciphertexts is:

$$Q_i(L) = \begin{cases} \emptyset, L = 0 \\ \{M_i\}: 1 \leq i \leq m, L > 0 \end{cases} \tag{3}$$

according to the following decryption expectations:

L=0: Users do not receive private keys and thus cannot decrypt any messages.

L=1: Users receive $(d_1, n_1)$ and can decrypt $\{M_1\}$

L=2: Users receive $(d_2, n_2)$ and can decrypt $\{M_1, M_2\}$

…

L=m: Users receive $(d_m, n_m)$ and can decrypt $\{M_1, M_2, \dots, M_m\}$

### *3.2. Encryption*

A large confusion modulus $t$ is selected, and the broadcast center performs a modulus operation on each plaintext $M_i$ to generate the secret key $K_i$, then RSA-encrypted to produce $m$ secret key ciphertexts $S_i$:

$$K_i = M_i \bmod t \tag{4}$$

$$S_i = K_i^e \bmod N_i \tag{5}$$

For each plaintext $M_i$, DES encryption is performed using $K_i$ as the key, resulting in $m$ information ciphertexts $C_i$:

$$C_i = E(K_i, M_i) \tag{6}$$

The broadcast center then broadcasts the set $(e, \{N_1 \dots N_m\}, \{S_1 \dots S_m\}, \{C_1 \dots C_m\})$ to all users.

### *3.3. Decryption*

Each user receives the broadcast message and uses their private key $(d_i, n_i)$ to decrypt the broadcast message and obtain the secret key set $\{K_1, \dots, K_i\}, \text{where}(1 \leq i \leq m)$. The user then uses the secret keys to decrypt the ciphertext set $\{C_1 \dots C_m\}$ to retrieve the corresponding plaintext messages:

DOI: 10.54254/2755-2721/114/2024.18213

$$K_i = S_i^{d_i} \bmod n_i \tag{7}$$

$$M_i = D(K_i, C_i) \tag{8}$$

## 4. Feasibility proof

By selecting e, p, and q, the private key $(d, n)$ and public key $(e, N)$ can be obtained using formulas (1) and (2). Let the plaintext be M. By applying formula (4), the secret key K is derived. If N is a multiple of n, then applying formula (7) will yield the correct K. If N is not a multiple of n, the correct K will not be obtained. The proof is as follows:

$$S = K^e \bmod N$$

$$K = S^d \bmod n = \left(K^{ed} \bmod N\right) \bmod n$$

Since the private key is generated such that $ed \equiv 1 \bmod \phi(n)$, it follows that:

$$K^{ed} = K^{\varphi(n)+1}$$

Thus:

$$K = \left(K^{\varphi(n)+1} \bmod N\right) \bmod n = \left(K^{\varphi(n)+1} - \alpha N\right) \bmod n = (K - \alpha N) \bmod n$$

For the proof of $\left(K^{\varphi(n)+1} - \alpha N\right) \bmod n = (K - \alpha N) \bmod n$, consider the following two cases:

When K is coprime with n:

According to Euler's theorem, if $\gcd(\alpha, n) = 1$, then $\alpha^{\varphi(n)} \equiv 1 \bmod n$. Thus:

$$K^{\varphi(n)} \equiv 1 \bmod n$$

Therefore:

$$\left(K^{\varphi(n)+1} - \alpha N\right) \bmod n = \left(K\left[K^{\varphi(n)}\right] - \alpha N\right) \bmod n = (K - \alpha N) \bmod n$$

When K is not coprime with n:

Assume $K = c * p$, and $M < n$. Since $K < n$, K cannot be a multiple of both p and q, implying that K must be coprime with q. By Euler's theorem, $K^{\varphi(q)} \equiv 1 \bmod q$,hence:

$$[K^{\varphi(p)}]^{\varphi(q)} \equiv 1 \bmod q$$

This implies:

$$K^{\varphi(n)} \equiv 1 \bmod q$$

Therefore:

$$K^{\varphi(n)} = 1 + b * q$$

Consequently:

$$K^{\varphi(n)+1} \bmod n = K + K * b * q \bmod n = K + cpbq \bmod n = K + cbn \bmod n = K$$

Thus, it follows that:

$$\left(K^{\varphi(n)+1} - \alpha N\right) \bmod n = (K - \alpha N) \bmod n$$

When N is a multiple of n, $\alpha N \bmod n = 0$. Since $K < n$, it follows that $K \bmod n = K$. Therefore:

$$(K - \alpha N) \bmod n = K - 0 = K$$

DOI: 10.54254/2755-2721/114/2024.18213

Using $M = D(K, C)$, the correct plaintext can be decrypted. When $N$ is not a multiple of n $(K - \alpha N) \bmod n = K - (\alpha N \bmod n)$, and the correct $K$ cannot be obtained, aligning with the expected decryption.

## 5. Security analysis

If an attacker (an unauthorized user) attempts to access all broadcast messages directed to $m$ users, they must break either the RSA encryption or symmetric encryption. Since each broadcast round varies in message and key sets, private and secret keys also differ per round. Therefore, even if an attacker obtains keys from one round, they are invalid for previous and the subsequent rounds, ensuring both forward and backward security. If an attacker intercepts the secret key ciphertext $S_i$ and the information ciphertext $C_i$ they must attack the RSA encryption, that is, obtain the secret key KKK of the user with the highest privilege. Since the secret key $K$ is encrypted using the RSA algorithm, its security is based on the difficulty of factoring large integers, consistent with the security of the standard RSA algorithm. If the attacker intercepts only the information ciphertext $C_i$, they must conduct an attack on DES encryption $m$ times. Because each plaintext $M_i$ is encrypted with a different secret key $S_i$, the attacker cannot ascertain the privilege level of the user and thus cannot determine the set of secret keys accessible to the user. In this scenario, the user remains anonymous to the attacker. Even if one secret key is cracked, the attacker cannot identify the corresponding user.

## 6. Conclusion

This paper presents an RSA broadcast encryption scheme suitable for a privilege division system. By differentiating user privilege levels, high-privilege users can decrypt more information, while low-privilege users can decrypt less, improving applicability and usability. By constructing different public key moduli $N_i$, the scheme implements user privilege division and provides a relatively secure RSA encryption scheme for network applications with a privilege hierarchy or for paid content access scenarios, thus expanding the use cases for RSA encryption and increasing its security and practicality. In this scheme, users do not need to possess multiple private keys; a single private key enables users to decrypt one or multiple plaintext messages. Additionally, unauthorized low-privilege users cannot correctly decrypt the secret keys of other users. During any given round of broadcasting, as users dynamically join or leave, the remaining users do not need to update their keys. Although the scheme proposes a multi-privilege public key broadcast encryption system for paid content access, limitations still exist in scenarios involving privilege division. For instance, if a user $u_x$ only needs to obtain the x-th message, this scheme currently allows the user to access the message set $\{M_1, M_2, \ldots, M_x\}$. To address such cases, further optimization of this scheme can be considered, such as enabling users to hold multiple private keys to satisfy specific user message retrieval needs, thereby providing broader applications for public key cryptography and the development of broadcast encryption technologies.

## References

[1] Sakai, R., & Furukawa, J. (2007). Identity-based broadcast encryption. Cryptology ePrint Archive.
[2] Berkovits, S. (1991, April). How to broadcast a secret. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 535-541). Berlin, Heidelberg: Springer Berlin Heidelberg.
[3] Eskeland, S. (2022). Collusion-resistant broadcast encryption based on hidden RSA subgroups. In Proceedings of the 19th International Conference on Security and Cryptography.
[4] Baee, M. A. R., Simpson, L., Boyen, X., Foo, E., & Pieprzyk, J. (2022). ALI: Anonymous lightweight inter-vehicle broadcast authentication with encryption. IEEE Transactions on Dependable and Secure Computing, 20(3), 1799-1817.
[5] Chinnala Balakrishna, D. T. H. (2020). CONTRIBUTORY BROADCAST ENCRYPTION WITH EFFICIENT ENCRYPTION AND SHORT CIPHER TEXTS.

DOI: 10.54254/2755-2721/114/2024.18213

[6] Srivastava, V., Debnath, S. K., Stanica, P., & Pal, S. K. (2023). A multivariate identity-based broadcast encryption with applications to the internet of things. Adv. Math. Commun., 17(6), 1302-1313.
[7] Rabaninejad, R., Ameri, M. H., Delavar, M., & Mohajeri, J. (2019). An attribute-based anonymous broadcast encryption scheme with adaptive security in the standard model. Scientia Iranica, 26(3), 1700-1713.
[8] Dupin, A., & Abelard, S. (2024). Broadcast Encryption using Sum-Product decomposition of Boolean functions. Cryptology ePrint Archive.
[9] Lin Guoqing, Li Ying & Wang Xinmei. (2008). RSA-based broadcast encryption scheme. Journal of Southeast University(Natural Science Edition) (S1), 86-89.
[10] Li Xiaofeng, Lu Jianzhu & Wang Meng. (2006). A new scheme for broadcast encryption based on RSA. Microcomputer Information (09), 59-60.