Research on RSA-based Broadcast Encryption Scheme in Web Multimedia

Liang Xue  
College of Computer Science  
Sichuan University  
Chengdu, China  
13541243587  
liangxue_scu@163.com

Du Zhongjun  
College of Computer Science  
Sichuan University  
Chengdu, Sichuan  
13618066736  
duzhongjun@scu.edu.cn

Abstract—With the development of web multimedia technology, broadcast encryption schemes play an important role in multimedia services copyright protection. In this paper, we propose a new broadcast encryption scheme based on RSA, besides, we give out two algorithms—smallest power exponent algorithm and improved modular exponential algorithm, to simplify the repeated squaring in RSA. This scheme could reduce the encryption and decryption calculated amount greatly, improve the communication bandwidth and deter the forcible attack effectively. Moreover, in the course of distributing keys, we adopt the different module remainder strategy, thus realizing that when new members join in, keys needn’t be updated, and this could enhance the practicality and security of broadcast encryption scheme.

Keywords—web multimedia; RSA; broadcast encryption

I. INTRODUCTION

Web multimedia, the development of traditional multimedia services on web, is one of the hotspot of computer application technique researches now. With the development of web multimedia technology, broadcast encryption schemes play an important role in multimedia services copyright protection. The broadcast encryption[1], which provides a safe way to distribute digital information for authorized users over the broadcast channel, has a broad application prospect in the pay-TV, video conference and other occasions. In this paper, we propose a new broadcast encryption scheme based on RSA, besides, we give out two algorithms—smallest power exponent algorithm and improved modular exponential algorithm, to simplify the repeated squaring in RSA. Our scheme could reduce the encryption and decryption calculated amount greatly, improve the communication bandwidth and deter the forcible attack effectively. Moreover, in the course of distributing keys, we adopt the different module remainder strategy, thus realizing that when new members join in, keys needn’t be updated, in addition, the storage amount of keys is greatly increased.

II. RELATED WORK

The notion of broadcast encryption was first put forward by Berkovits[2] in 1991. Later, Fiat and Noar[3] gave a formal study of broadcast encryption and proposed a mechanism to prevent collusion. Since then, Broadcast encryption received extensive attention, many broadcast encryption schemes were proposed to enhance the development of this field. Naor and Pinkas[4] performed a public key broadcast encryption scheme which used a threshold secret sharing method. Tan Zuowen et al.[5] introduced a fully public key tracing and revocation scheme, and the salient feature of the scheme was that the secret keys of the users were chosen by the users themselves. Li Xiaofeng et al.[6] according to the protocol of RSA and the enlarging the small public key technology presented a new broadcast encryption scheme of RSA oriented multi-recipient. At the same time, in order to simplify the key management, some scholars put forward the identity based broadcast encryption scheme, for example, Sun Jin et al.[7] performed a novel identity-based broadcast encryption scheme by combining with Waters dual system encryption and the orthogonality property of composite-order bilinear groups.

III. RSA-BASED BROADCAST ENCRYPTION SCHEME

In our scheme, there are three entities:

Data Provider(DP): A data provider in our scheme is responsible for providing and encrypting multimedia content.

Key Generation Center(KGC): In this scheme, it is in charge of achieving system initialization, key generation, key distribution and user management.

Authorized User(AU): An authorized user is a subscriber who could receive the multimedia content.

A. Initialization

We assume that all the data transmit through security authentication channel. The procedure works as follows.

DP chooses two distinct prime numbers p and q randomly, computes \( n = pq \) and \( \phi(n) = (p - 1)(q - 1) \), where \( \phi \) is Euler's totient function, and chooses an integer \( e \) such that \( 1 < e < \phi(n) \) and greatest common divisor of \( (e, \phi(n)) = 1 \). So the public key for DP is \((e, n)\).

For all authorized users \( au_i \), \( i=1, 2, 3, \ldots, s \) (s is the number of AUs), they all send their own identity information \( ID_i \) to KGC, and KGC adds \((ID_i, d_i, R_i)\) to the storage list, where \( d_i \cdot e \equiv 1 \mod (R_i, \phi(n)) \), and \( R_i \) is a random prime number.

In the end, KGC sends the private key \((d_i, n)\) to \( au_i \) safely and accurately.
B. Encryption

In the light of RSA algorithm, we assume that the plaintext \( m=(m_1, m_2, m_3, \ldots, m_k) \) and the ciphertext \( c=(c_1, c_2, c_3, \ldots, c_k) \), so the encryption algorithm \( E \) is thus:

\[
c_j = m_j^e (mod \ n), j=1, 2, 3, \ldots, k.
\]

Note that the encryption procedure need \( k \) times modular exponential operations, obviously, the encryption speed is slow and need a significant amount of bandwidth.

While in our paper, we propose a new encryption algorithm, where the process is:

\[
c_j = (m_j \mod m_\text{id}) (mod \ n), i=\text{id}, \text{id}-1, \ldots, 3, 2
\]

and

\[
c_1 = m_1^e (mod \ n).
\]

So we only use one time modular exponential operation and \( k-1 \) times modular add operations, which considerably reduces the time of encryption.

Moreover, for the modular exponential operation, we convert exponent \( m \) to binary number for repeated squaring operation traditionally. However, in practical applications, exponent \( m \) is required to be large to enhance security, so the computation speed is still slow for encryption procedure. In our paper, we give out two algorithms—smallest power exponent algorithm and improved modular exponential algorithm, to simplify the repeated squaring in RSA. This scheme could reduce the encryption and decryption calculated amount effectively and greatly improve the communication bandwidth.

1. smallest power exponent algorithm

Judge whether \( n \) is a prime in the formula \( m^\phi(n) \) firstly.

Then if it is, compute \( \phi(n) \) and \( r \), where \( r \) is remainder of deviding \( \phi(n) \) by \( e \), thus \( r \) is final smallest power exponent.

Then if not, factorize integer \( n=p_1^{v_1}p_2^{v_2}p_3^{v_3}\ldots p_k^{v_k} \), and figure out \( \phi(p_1^{v_1}), \phi(p_2^{v_2}), \phi(p_3^{v_3}), \ldots, \phi(p_k^{v_k}) \) respectively, let \( \lambda=[\phi(p_1^{v_1}), \phi(p_2^{v_2}), \phi(p_3^{v_3}), \ldots, \phi(p_k^{v_k})] \), and compute \( e=\phi(\mod \lambda) \), thus \( r \) is final smallest power exponent.

2. improved modular exponential algorithm

First, we let \( m_0=m \) and \( e_0=e \), compute \( m_0^{v_1}, m_0^{v_2}, \ldots, \) until finding out a \( q_0 \), satisfying \( m_0^{q_0}>n \) and \( m_0^{q_0-1}<n \). If no \( q_0 \) meet this condition, then compute \( m^e=x (mod \ n) \) directly; if having an appropriate \( q_0 \), compute \( m_0^{q_0}=m_1 (mod \ n) \), \( e_0=q_0e_1+r_1 \), where \( 1\leq r_1<q_0\leq e_0 \), \( m_0^{q_1}=b_1 \), so we could transform \( m^e (mod \ n) \) to \( m_0^{e_1}b_1 (mod \ n) \);

Similarly, make a calculation of \( m_1^{v_1}, m_1^{v_2}, \ldots, \) until finding out a \( q_1 \), satisfying \( m_1^{q_1}>n \) and \( m_1^{q_1-1}<n \). If no \( q_1 \) meet this condition, then compute \( m_1^{q_1}b_1=x_1 (mod \ n) \) directly; if having an appropriate \( q_1 \), compute \( m_1^{q_1}=m_2 (mod \ n) \),

\[
e_1=q_1e_2+r_2, \text{where } 1\leq r_2<q_1\leq e_1, m_1^{q_1}=b_2, \text{so we could transform } m^e (mod \ n) \text{ to } m_2^{e_1}b_2 (mod \ n);
\]

In the encryption process, \( e \) is a definite number, so by the finite-step calculation, \( m^e (mod \ n) \) is transformed to the following formula:

\[
m_k^{e_k}b_k b_{k-1} \ldots b_1 (mod \ n).
\]

As can be seen from above, we could get the final answer only by \( k \) times multiplication and \( mod \ n \) operations. This could reduce the calculation amount of modular exponential operation effectively.

C. Decryption

Assume that the plaintext \( m=(m_1, m_2, m_3, \ldots, m_k) \), correspondingly, the ciphertext \( c=(c_1, c_2, c_3, \ldots, c_k) \), so the decryption algorithm for traditional RSA is thus:

\[
m_j = c_j^{d_j} (mod \ n), j=1, 2, 3, \ldots, k.
\]

Similarly, in our scheme, we use a new RSA decryption algorithm:

\[
m_1 = c_j^{d_j} (mod \ n)
\]

and

\[
m_j = (c_j \cdot m_j) (mod \ n), j=2, 3, 4, \ldots k-1, k.
\]

So we only use one time modular exponential operation and \( k-1 \) times modular add operations, which considerably reduces the time of decryption.

Besides, we also use smallest power exponent algorithm and improved modular exponential algorithm to reduce the decryption calculation.

IV. SECURITY ANALYSIS

In the RSA-based broadcast encryption scheme, public key \((e,n)\) is open to all, i.e., eavesdroppers could get the value of \( e \) and \( n \). If a eavesdropper attempts to crack the ciphertext, he need know the private key \((d,n)\), where \( d=\phi(n) \mod \phi(n) \), \( e \) and \( n \) are known. The crucial point to get \( d \) is from the value of \( p \times q \) to get the value of \( p-1 \) and \( (q-1) \), but it is a recognized mathematical problem to divide the product of two large prime numbers, moreover, when the product of \( p \) and \( q \) is as large as 1024 bits, it is out of the question to complete the factorization so far. For this reason, RSA is considered to be one of the best public key algorithms. In our paper, we apply RSA algorithm to our broadcast encryption scheme, unauthorized users will not get the private key \((d,n)\), the KGC sends to AU, and they could not get it by collusion.

In RSA applications, \( p \) and \( q \) must be large enough prime numbers to ensure the safety of RSA and avoid being forcibly attacked, only in this way, can we make attackers not divide the product of two large prime numbers in polynomial time. However, as the bit of private key increases, the time-consuming modulo exponentiation computation in encryption and decryption procedures, which has always been the bottle-
neck of RSA, restricts its wider development. In our paper, the new scheme significantly lowers the computational complexity, and greatly reduces the burden of larges keys in RSA, thus we could deter the forcible attack effectively.

V. CONCLUSION

We propose a new RSA-based broadcast encryption in web multimedia. In the course of KGC distributing keys, we adopt the different module remainder strategy, thus realizing that when new members jion in, keys needn’t be updated, and this could enhance the practicality and security of broadcast encryption scheme. In the process of encryption and decryption, we use one time modular exponential operation and k-1 times modular add operations instead of traditional k times modular exponential operations to reduce the time of encryption and decryption. Besides, we use two new algorithms—smallest power exponent algorithm and improved modular exponential algorithm to simplify the repeated squaring in RSA. With the acceleration of computation, the scheme could greatly reduces the burden of larges keys in RSA, thus we could deter the forcible attack effectively.

REFERENCES