A Threshold Decryption Scheme without Session Keys *

Min-Shiang Hwang[†] Chin-Chen Chang[‡] Kuo-Feng Hwang[‡]

Department of Information Management [†]
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng
Taichung County, TAIWAN, R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-3742337

Department of Computer Science and Information Engineering [‡]
National Chung Cheng University,
Chaiyi, TAIWAN, R.O.C.
Email: ccc@cs.ccu.edu.tw

October 31, 2012

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-001.

A Threshold Decryption Scheme without Session Keys

Abstract

In the present study, a new threshold decryption scheme is proposed which allows confidential messages to be encrypted in t-out-of-n shared secret schemes. Whenever the number of participants from the group is larger than or equal to a predetermined threshold value t, the confidential message can be obtained. There are three advantages of the present scheme. The first advantage is that both the key distribution and generation is not required in the present scheme, secondly the scheme can efficiently encrypt large secret files or messages and the third advantage is other cryptosystems for enciphering/deciphering confidential messages is not needed.

Key Words: Threshold Scheme, Secret Sharing, Cryptography.

1 Introduction

The concept of secret sharing was developed independently in 1979 by Blakely [**?**] and Shamir [**?**]. A t-out-of-n secret sharing scheme allows t or more users of the group to share the secret key which is used to decrypt a confidential message.

The general shared secret schemes are useful for robusting key management [**?**]. The schemes are used to solve two problems. One is that the legitimate users are locked out of the system since the cryptographic key is lost for some reasons. While the other is that unauthorized users are able to get into the system without a secret key.

However, there are two disadvantages of the general shared secret scheme. The first disadvantage is that the system must carefully distribute shares to the participants.

While the other is that the scheme needs another cryptosystem to encrypt/decrypt confidential messages.

In the present study, a threshold decryption scheme is proposed which does not have the disadvantages of the general shared secret scheme. The present scheme allows confidential messages to be encrypted in t-out-of-n shared secret schemes. Whenever the number of participants from the group is larger than or equal to a predetermined threshold value t, the confidential messages can be obtained.

The purpose of this article is to solve a performance problem in threshold decryption [?]. We propose a threshold decryption scheme which does not use session keys but relies on public-key infrastructure. This is different from conventional schemes where each message is encrypted with the corresponding session key and the session key is the object to be shared by using threshold mechanism, To achieve efficiency, the proposed scheme uses one-way compression/expansion functions.

We outline the goals of the this work as follows.

1. Both the generation and the distribution of shared secret for the member of the group is not required.
2. The large confidential files or messages can be encrypted efficiently.
3. The proposed scheme does not require other cryptosystems for enciphering/deciphering the large confidential messages.

2 The Secret Sharing and Information Dispersal Scheme

The secret sharing scheme proposed by Shamir [?] is called a t-out-of-n threshold scheme. It allows a secret key, k, to be shared in a group of n participants u_i's, for $1 \leq i \leq n$. When the number of participants is greater than or equal to a predetermined value t, the secret key can be thus derived. We briefly introduce the t-out-of-n threshold scheme as follows. The system randomly creates a polynomial $f(x)$ with degree $t-1$ as follows.

$$f(x) = A_{t-1}x^{t-1} + A_{t-2}x^{t-2} + \cdots + A_1 x + k \bmod P, \tag{1}$$

where P is a large prime number, and k is used as a cryptographic key. All the coefficients A_i's, for $i = 1, 2, \cdots, t-1$, of Equation (1) is selected arbitrarily. The value of $f(u_i)$, for i=1 to n, are distributed to the participants u_i's by a privacy channel.

When t or more participants want to determine the cryptographic key k, each participant submits his share $(u_i, f(u_i))$ to the central authority (CA for short). CA is responsible for generating the cryptographic key k. The secret polynomial can be thus reconstructed by applying Lagrange interpolation formula with t or more shares. An important application of secret sharing is reported for information dispersal [?, ?]. The method is to break a file or message M of length L into t pieces M_i's, for $i = 1, \cdots, t$. Each length is of L/t bits. Wherein t or more pieces suffice for reconstructing M. Let $M = M_1 M_2 \cdots M_t$, where $|M_i| = L/t$ bits, $1 \leq i \leq t$. Here $|x|$ denotes the length of the message x. The scheme constructs a polynomial with degree $t-1$, $F(x) = M_1 x^{t-1} + M_2 x^{t-2} + \cdots + M_{t-1}x + M_t$. By using the polynomial, n pieces are generated by computing $F(j), j = 1, 2, \cdots, n$. Whereas any t or more pieces can be used to reconstruct the polynomial $F(x)$ by applying Lagrange interpolation. There is one disadvantage of this scheme. Since the size of M_i, $i = 1, 2, \cdots, t$, is dependent on the message M, it is time consuming to reconstruct a polynomial with a large M_i. In the present study, an efficient threshold scheme is proposed which has three advantages. The first advantage is that both the key distribution and generation is not required in the present scheme, secondly the scheme can efficiently encrypt large secret files or messages, and the third advantage is that other cryptosystems for enciphering/deciphering confidential messages is not needed.

3 Our Scheme

In this section, an efficient threshold decryption scheme is proposed. Our scheme is based on Diffie-Hellman key distribution scheme [**?**] and general shared secret scheme [**?**, **?**].

The Diffie-Hellman key distribution scheme is used to generate the key pair of public key and secret key. Each participant with identity u_i, for $i = 1, 2 \cdots, n$, randomly selects a secret key $k_i \in Z_p$ and computes the corresponding public key $p_i = g^{k_i} \bmod P$. Here P is a large prime number (let $|P| = 513$ bits) and g is a primitive element of $GF(P)$.

On the other hand, the shared secret scheme is used to hide plaintext but not the session key. However, to send a plaintext M to a group G of n participants $u_1, u_2, \cdots$, and u_n, the plaintext is encrypted by t-out-of-n threshold scheme. Wherein the sender performs the following steps:

Enciphering Algorithm:

1. Generate a random integer r, $1 \le r \le P - 1$, and $\gcd(r, P - 1) = 1$. Next, compute $e_i = p_i^r \bmod P$ for $i = 1, 2, \cdots, n$. Here, p_i is a public key of u_i, which is in the group of n participants. e_i is used to compute coefficients of the polynomial

with degree $n-1$.

2. Construct a polynomial with degree n-1 , $f(x) = A_{n-1}x^{n-1} + A_{n-2}x^{n-2} + A_{n-3}x^{n-3} + \cdots + A_1x + A_0 \bmod P$, such that $f(u_i) = e_i$ for $i = 1, 2, \cdots, n$. The coefficients A_i's, for $i = 0, 1, \cdots, n-1$, can be found by solving n simultaneous equations. Here the length of each A_i is of 512 bits. Thereafter A is obtained by concatenating all coefficients. That is, $A = A_{n-1}A_{n-2}A_{n-3}\cdots A_1A_0$.

3. Modify A to the same length of M. There are now three cases to be considered.

   - Case 1: if $|A| = |M|$, then nothing to be done for A.
   - Case 2: if $|A| > |M|$, compute $g(A_i)$, for $i = 0, 1, \cdots, n-1$, where $g(\cdot)$ is a one-way function which compresses the length of A_i. The length of $g(A_i)$ is $\lceil \frac{|M|}{n} \rceil$.
   - Case 3: if $|A| < |M|$, compute $h(A_i)$, $i = 0, 1, \cdots, n-1$, where $h(\cdot)$ is a one-way function which expands the length of A_i. The length of $h(A_i)$ is $\lceil \frac{|M|}{n} \rceil$.

4. Compute $C = A \oplus M$, $R = g^r \bmod P$, and $f(j)$ for $j = 1, 2, \cdots, (n-t)$. Here, $\oplus$ denotes an exclusive operator, and we assume that $(n-t) < u_i$, $i = 1, 2, \cdots, n$.

5. Send $\{t, R, f(1), f(2), ..., f(n-t), C, g(\cdot)\ or\ h(\cdot)\}$ to the group G in the public network.

When t or more participants, $u_{i_1}, u_{i_2}, \cdots$, and u_{i_t}, decide to recover the confidential message M. They can decrypt the message by performing the following steps:

Deciphering Algorithm:

1. Compute individual secret shared. Each u_{i_j} computes his secret share $e_{i_j} = R^{k_{i_j}} \bmod P$. Here k_{i_j} is the secret key of u_{i_j}.

2. Apply Lagrange interpolation formula to reconstruct a polynomial $f(x) = A_{n-1}x^{n-1} + A_{n-2}x^{n-2} + \cdots + A_1 x + A_0 \bmod P$. Since we know $f(i)$, $i = 1, 2, \cdots, n-t$, and t participants' secret shares $f(u_{i_j})$'s, for $j = 1, 2, \cdots, t$. The coefficients A_i's, for $i = 0, 1, \cdots, n-1$, can be found by solving n simultaneous equations. Let $A = A_{n-1}A_{n-2}A_{n-3} \cdots A_0$.

3. Modify A to A' with the same length as C by the one-way function $g(\cdot)$ or $h(\cdot)$ or none, if $|A| = |C|$.

4. Recover message M by computing $A' \oplus C$.

4 Security Analysis

Since the present scheme is based on the Diffie-Hellman distribution scheme [**?**], it is very difficult for an illegal user to compute the secret key k_i of the user u_i from the equation $p_i = g^{k_i} \bmod P$. Moreover, it is not easy for an intruder to obtain the system-generated random number r directly from the equation $e_i = p_i^r \bmod P$ and $R = g^r \bmod P$ in Steps 1 and 4 of the Enciphering Algorithm in Section 3, respectively. Besides, it is difficult for an intruder to obtain the secret key k_{i_j} of user u_{i_j} directly from the equation $e_{i_j} = R^{k_{i_j}} \bmod P$ in Step 1 of the Deciphering Algorithm in Section 3. The difficulty is due to the complexity of computing discrete logarithms over finite fields [**?**].

Since the random integer r is a variable in every run of the Enciphering Algorithm in Section 3, our scheme is thus secure against the replaying attacks.

Since the present scheme is based on the general shared secret scheme [**?**], it is very difficult for the illegal user to get the polynomial $f(x)$ without enough knowledge about the secret shares. In other words, with knowledge of any $t-1$ or fewer secret shares, it is not possible to reconstruct the polynomial with degree $t-1$. The coefficients thus cannot be obtained. Therefore, $t-1$ or fewer users in the group cannot obtain the confidential message by computing $A \oplus C$.

5 Conclusions

A new threshold decryption scheme is proposed, which allows a confidential message to be encrypted in t-out-of-n shared secret schemes. Whenever the number of participants from the group is larger than or equal to a predetermined threshold value t, the confidential message can be obtained. However, with knowledge of any $t-1$ or fewer users in the group, the intruder cannot obtain the confidential message. There are three advantages of the present scheme they are as follows.

1. The general shared secret scheme [**?**], needs to generate the shared secret pair $(u_i, f(u_i))$, and deliver these secret pair to each participant in a privacy channel. Since the present scheme is based on the Diffie-Hellman key distribution scheme, both the generation and the distribution of shared secret for the member of the group is not required in our scheme.

2. Irrespective of the length of the confidential messages, the degree of polynomial is always $n-1$, and the length of coefficients is always 512 bits. Therefore, large confidential files or messages can be encrypted efficiently in the present scheme. Althought the degree of polynomial is $t-1$ of the Rabin's information dispersal scheme [**?**], the length of the coefficients is dependent on the message. Hence, it is time consuming to reconstruct a polynomial with a large confidential message.

3. The confidential messages are broken into n pieces and hidden in the coefficients

of the polynomial $f(x)$ in the present scheme. The scheme thus does not require other cryptosystems for enciphering/deciphering confidential messages.

ACKNOWLEDGEMENTS

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC88-2213-E-324-021.