Qiang FAN, Mingjian ZHANG, Yue ZHANG

Department of Computer Science and Technology, Hunan Police Academy

Key Escrow Scheme with the Cooperation Mechanism of Multiple Escrow Agents

Abstract. *To combat crime and terrorist organizations, government expects to monitor the suspicious communication but the leak of personal privacy is a common problem. Assuming that there are two Escrow Agent groups (Escrow party), one is designated by the government, while the other is unofficial. The two groups can achieve mutual supervision and dependence, thus implementing monitoring for users by the cooperation rather than by only a single one. If the number of the mutual participation is less than the required threshold number, the monitoring cannot be achieved. Therefore, an equation set corresponding to the specific program can be constructed, for example, multiply i^{th} equation and j^{th} equation to get an $(i+j)^{th}$ equation. As long as this kind of equation set is established, various key escrow schemes involved by several Escrow Agent groups can be constructed. Nowadays, the increasing political, economic, and cultural exchanges all over the world will lead to more and more transnational crime and terrorist attacks, so this program can be adapted to the multinational (or multi-organization) key escrow cooperation.*

Streszczenie. *Analizuje się możliwości monitorowania transakcji w przypadku wielu escrow agents – depozytariuszy. Metoda ma na celu ochronę rynku przed atakami terrorystycznymi. (**Schematy depozytowe (escrow) w mechanizmach kooperacyjnych przy wielu depozytariuszach**)*

Keywords: key escrow, multi-group escrow agent, cooperation mechanism, advanced threshold scheme.
Słowa kluczowe: escrow agent, transakcje depozytowe

1. Introduction

In Ordinary key escrow threshold scheme, the private key fragments with different numbers are distributed based on the differences of the privilege of escrow in which escrow with the greater privilege can access to more fragments. However, general threshold scheme does not take into account the cooperation mechanism of the multi-group Escrow Agent [1-3].

1) Cooperation mechanism of two groups. For the escrow party designated by government and the unofficial one, if there are Q official escrow agents out of P ($Q \le P$) as well as S nonofficial escrow agents out of R ($S \le R$), the cooperation of the two groups can implement the monitoring for users.

2) Multiple-group cooperation mechanism. With the increasing multinational cooperation and exchange, the police cooperation against transnational crime or terrorist attacks is necessary. That is, the communication key of suspicious criminals can be authorized to be extracted by the multinational (or multi-organization) cooperation to protect the privacy and normal communication. Then it is possible to specify a set of Escrow Agent for each country (or region), which will result in the multi-group cooperation.

According to the actual situation of each group, the number of Escrow Agents even the threshold value can be set as variable. When necessary, if the number of Escrow Agent of each group reaches its threshold quantity, the escrow key can be obtained. This escrow scheme is conductive for users to set the weight of escrow agent flexibly, which is not only in line with the actual situation but also beneficial for the application of key escrow in real life.

In this paper, restoring the user's key by the cooperation of two sets of Escrow Agent is taken as an example to describe the design of this escrow scheme. If being expanded, this design can be used for the multi-group cooperation.

2. The description of system

Assuming that there is a Key Management Center(*KMC*) in the cryptosystem that is responsible for issuing the public key certificate of the communication users. The escrow user (trustee) is represented by A. Assume that $P = \{P_1, P_2, ..., P_i\}$ ($i \le n-1$) is the collection of official Escrow Agent, and $Q = \{Q_1, Q_2, ..., Q_j\}$ ($j \le n-1$) is the collection of unofficia Escrow Agent. E refers to the monitoring of law enforcement agencies for the communications of users. a is the private key hosted by the user A. Ks is the session key which is used to encrypt the communication information among users. At the same time, the private key a can be divided into $n=i+j$ parts, which are respectively entrusted to $P_1, P_2, ..., P_i$ and $Q_1, Q_2, ..., Q_j$.

If the number of official Escrow Agent is t ($t \le i$) or more than t, and the number of unofficial Escrow Agent is s ($s \le j$) or more than s, the cooperation of two groups is conductive to implement the monitoring for user A. If the actual number of P_i is less than t, or the number of Q_j is less than s, the monitoring cannot be achieved. In addition, the cooperation of the entire P_i or Q_j is useless for the monitoring, thus it is impossible to obtain any information of a.

3. The generation and the escrow of key

3.1 The generation of key

The *KMC* should select a large prime P and a primitive element g of $GF(P)$. The private key of users can be generated through the following methods.

The user A should randomly select $a' \in Z_p$, calculate

$Y' \equiv g^{a'} \bmod p$

and send Y' to *KMC*.

Then *KMC* will randomly choose k, $a'' \in Z_p$ so as to make

$Y \equiv g^{a''} Y' \neq 1 \bmod p$,

$Y_1 \equiv g^k \bmod p$, $Y_2 \equiv a'' Y^k \bmod p$

should be calculated and (p,g,Y) should be public. Then (Y_1, Y_2) should be sent to user A.

The user A will calculate

$a'' \equiv Y_2 (Y_1^{a'})^{-1} \bmod p$, $a \equiv a' \oplus a'' \bmod (p-1)$.

If $a=0$, A will reapply the public key certificate. Otherwise, a will be considered as the private key of user A.

3.2 The partition of key

1) The user A is required to select $i-1$ random number b_w ($0 < b_w < p$), $w=1,2,...,i-1$ to construct the polynomial:

$$f(x) = c_{i-1}x^{i-1} + c_{i-2}x^{i-2} + ... + c_1 x + a' \in Z_p[x],$$

in which $f(0) = a'$.

2) The user A should randomly select t_1. t_1 is a primitive element in $GF(P)$. Meanwhile, it is required to calculate i key pieces:

$a_w = f(t_1^w) \bmod p$, $w=1,2,...,i$.

3) The *KMC* is required to select $j-1$ random number c_z ($0 < c_z < p$), $z=1,2,...,j-1$ to construct the polynomial:

$f(x)=c_{j-1}x^{j-1}+c_{j-2}x^{j-2}+...+c_1x+a'' \in Z_p[x]$,

in which $f(0)=a''$.

4) The *KMC* transmits secretly *a''* to user *A*. The user *A* should randomly select t_2. t_2 is a primitive element in *GF*(*P*). Meanwhile, it is required to calculate *j* key pieces:

$a_z=f(t_2^z) \bmod p$, $z=1,2,...,j$.

5) The user *A* should calculate

$Y_i \equiv g^{ai} \bmod p$

and Y_i,*t* should be public.

3.3 The recovery of private key

1) Firstly, it is required to construct the polynomial $f(x)$ so as to get *a'*:

$$f(x)=\sum_{i=1}^{t_1} d_i \prod_{\substack{j=1 \\ j\neq i}}^{t_1} \frac{x-c^i}{c^j-c^i} \bmod p,$$

Then

$$a'=f(0)=\sum_{i=1}^{t_1} d_i \prod_{\substack{j=1 \\ j\neq i}}^{t_1} \frac{-c^i}{c^j-c^i} \bmod p.$$

2) Similarly, construct the polynomial $f(x)$, *a''* will be obtained.

3) Afterwards, we can calculate $a=a' \oplus a''$.

3.4 The key escrow

1) The user *A* should apply to *KMC* for escrow business and obtain ID_A.

2) The user *A* will encrypt (a_i,ID_A) by the public key of escrow parties and then send it to the escrow agent P_w(*w=1,2,...,i*).

3) The escrow agent P_w uses its own private key for decryption so as to obtain a_i. At the same time, it is also necessary to verify whether

$a_i \in Z_p$ and $Y_i \equiv g^{ai} \bmod p$

are tenable.

If they are tenable, it will be required to calculate the signature

$s_i=Sig_i(h(ID_A,Y_i,Y))$,

in which *h*(.) is the secure one-way hash function. What's more, it is also necessary to send (ID_A,Y_i,*Y*,s_i) to *KMC*. Otherwise, the signature will be refused.

4) The user *A* will encrypt (a_z,ID_A) by the public key of escrow parties and then send it to the escrow agent Q_z(*z=1,2,...,j*).

5) The escrow agent Q_z uses its own private key for decryption so as to obtain a_z. At the same time, it is also necessary to verify whethter

$a_z \in Z_p$ and $Y_z \equiv g^{az} \bmod p$

are tenable.

If they are tenable, it will be required to calculate the signature

$S_z=Sig_z(h(ID_A,Y_z,Y))$.

What's more, it is also necessary to send (ID_A,Y_i,*Y*,s_z) to *KMC*. Otherwise, the signature will be refused.

6) When *KMC* receives (ID_A,Y_i,*Y*,*s*) of each escrow agent P_w(*w=1,2,...,i*) and Q_z(*i=1,2,...,j*), it will judge whether

$$Y \equiv \prod_{i=1}^{n} Y_i \bmod p$$

is tenable through verifying the signature.

If it is tenable, *KMC* will calculate the signature

$s=Sig_{KMC}(h(ID_A, p,g,Y))$

and issue the public key certificate $C(A)=(ID_A,p,g,Y,s)$ of user *A*. Otherwise, the registration of user *A* will be refused.

4. The communications between users

Assuming that *A* prefers to communicate with *B*. Firstly, *A* will check the public key certificate *C*(*B*) of user *B* from the public key manual. *A* will randomly select K_s and $t \in Z_p$. K_s is the session key of encrypted message *M* and *t* is the timestamp. Calculating:

$Y_1 \equiv g^t \bmod p$, $Y_2 \equiv K_s Y^t \bmod p$, $s=Sig_A(h(Y_1,Y_2,t,ID_A,ID_B)$.

According to the law enforcement field $LEAF=(Y_1,Y_2,t,ID_A,ID_B,s)$, the message *M* should be encrypted into the cipher text $c=E_{ks}(M)$ and (*LEAF*,*c*) should be sent to *B*. When the user *B* receives (*LEAF*,*c*), it is required to calculate $K_s \equiv Y_2(Y_1^a)^{-1}$ and use *Ks* to decrypt the cipher text *c* so as to obtain the plaintext $M=D(c,k)$.

5. The electronic monitoring

It is required to employ the once monitoring method within the validity period and the perpetual off-line monitoring method to monitor the users.[4-6]

5.1 The one-off online monitoring within the validity period

1) Firstly, the government monitoring agency should apply for the monitoring certificate from the court. The monitoring time is provided in the certificate.

2) The government will monitor and intercept the cipher text *c* and *LEAF*. And the monitoring certificate will be also presented to each escrow agent P_w(*w=1,2,...,i*), and Q_z(*z=1,2,...,j*).

3) When the escrow agent verifies that the validity of certificate is the same as *t*, it is required to calculate

$Z_w \equiv (Y_1)^{aw} \bmod p$, $Z_z \equiv (Y_1)^{az} \bmod p$

and send Z_w, Z_z to the government monitoring agencies.

4) When the government monitoring agency receives morn than *t* (*t*≤*i*) Z_w and moren than *s* (*s*≤*j*) Z_z, it is required to calculate

$$Z \equiv \prod_{i=1}^{n-1,P^*} Z_i \equiv \prod_{i=1}^{n-1,P^*} Y_i^{ai} \equiv \prod_{i=1}^{n-1,P^*} g^{tai} \equiv g^t \sum_{i=1}^{n-1,p} a_i \equiv Y^t$$

mod *p*, $Ks \equiv Y_2 z^{-1} \bmod p$.

5) The government monitoring agency can adopt *Ks* to decrypt *c* so as to get the plaintext *M*. Then the monitoring can be achieved.

5.2 The perpetual off-line monitoring

1) Firstly, the government monitoring agency should apply for the monitoring certificate from the court. The monitoring time is provided in the certificate.

2) The government will monitor and intercept the cipher text *c* and *LEAF*.

3) The monitoring certificate will be also presented to each escrow agent P_w(*w=1,2,...,i*), and Q_z(*z=1,2,...,j*).

4) When the escrow agent verifies that the validity of certificate is the same as *t*, it is required to secretly send a_w(*w=1,2,...,i*) and a_z(*z=1,2,...,j*) to the government monitoring agencies.

5) When the government monitoring agency receives morn than *t*(*t*≤*i*) a_w and morn than *s*(*s*≤*j*) a_z, it is required to calculate

$$a' = \sum_{i=1}^{w} d_{wi} \prod_{\substack{j=1 \\ j\neq i}}^{w} \frac{-c^i}{c^j-c^i} \bmod p$$

$$a'' = \sum_{i=1}^{z} d_{zi} \prod_{\substack{j=1 \\ j\neq i}}^{z} \frac{-c^i}{c^j-c^i} \bmod p$$

$a=a' \oplus a''$

6) The government monitoring agency can use *a* to get the session key *Ks*. And *Ks* is also employed to decrypt *c*

so as to get the plaintext *M*. Then the monitoring can be achieved.

6. The safety performance analysis

1) The safety of the scheme (the generation, the partition, the escrow, the communication and the monitoring of key in scheme) is based on the following two points which have the unconditional security.[7,8]

The difficulty of solving the discrete logarithm in ElGamal cryptosystem is equivalent to the solution of discrete logarithm, which belongs to the NP problem.

Any *k-1* or less than *k-1* sub-keys in Shamir(*k, n*) threshold scheme can't reconstruct the security of the threshold theory of system key.

This program is the threshold key escrow scheme. For each set of government-designated escrow agent or unofficial escrow agent, when one or several of them are unwilling to cooperate or cannot cooperate (but it is necessary to reach the threshold amount), part of the escrowed keys still can be restored.

2) The key sharing scheme of escrow agents can be flexibly established due to the employment of the advanced threshold scheme idea. The system will have greater flexibility and adaptability, but the security will not be reduced. According to the specific circumstances of escrow agents, the design can be appropriately made.[9,10]

In this scheme, k^{th} equation is constructed, which is the product of *a* i^{th} equation (ie, threshold sharing equation of key *a'*) and *a* j^{th} equation (ie, threshold sharing equation of key *a''*). For the official escrow agency, each person will get a key fragment, which is the solution of the i^{th} equation. For the unofficial escrow agency, per person will get a key fragment, which is the value of the j^{th} equation. The former can use *i+1* key fragments to reconstruct the i^{th} equation, but no matter how many other key fragments they own, they cannot get any information about the private key *a*. For the latter one, *j+1* keys can be used to construct j^{th} equation, but they cannot get any information of the private key *a*. Only if the two groups to share their equations, the private key *a* can be reconstructed by multiplying the two equations.

3) The ElGamal private key *a* of the users in this scheme is generated by the cooperation between the random number *a'* selected by users and the random number *a''* selected by *KMC*. The random number *a'* is hosted by official escrow agent after partition, and the random number *a''* is hosted by private escrow agent after partition.

The shortcomings which include the subliminal attack and the shadow public key attack caused by the independent selection of *a* can be effectively prevented. At the same time, the phenomenon that the security of the private key is lower as the *KMC* or the user doesn't have a good random number generator can be also avoided.

4) This scheme can effectively prevent the conspiracy of some escrow agents or the illegal recovery of private key *a* due to the leakage of the keys of some escrow agents.

According to the several aspects discussed above, it is proved that this scheme is feasible and safe.

7. Conclusion

Based on the threshold thought and advanced threshold scheme, in this paper, the author utilizes the ElGamal cryptosystem to design the key escrow program with the participation of multi-escrow agents. The main achievements and innovation are shown as follows:

1) Based on the threshold thought and advanced threshold scheme, the author designs the key escrow program with the multi-group cooperation mechanism, which should be implemented by the cooperation of government-designated escrow agent as well as the unofficial escrow agent. Besides, this program is also applicable to the cooperation mechanism with more groups. It has also effectively solved the flexible setting problem of the weight of escrow agents, which enables the system to possess more flexibilities and adaptabilities.

2) Considered the difficulty of solving the discrete logarithm in ElGamal cryptosystem, a proposal is made that user's public key certificate can be issued when the validities of all escrow key fragments have been tested by KMC, which ensures effective implementation of lawful monitoring.

3) Once-monitoring in term of validity and perpetual offline monitoring can confine the privilege of monitoring agency and ensure the effective implementation of monitoring. Once-monitoring in terms of validity can aid the monitoring agency to access decoding key fragments between users' conversations, which make it impossible for monitoring agency to "once monitoring, perpetual monitoring." The possibility for monitoring agencies to decode the user's private key is based on their rights of perpetual offline monitoring.

Acknowledgments

Foundation Item: Projects of Science and Technology of Hunan Province(No.2011FJ3011),

Application Innovation Project of Ministry of Public Security (No.2009YYCXHNST002).

REFERENCES

[1] Nechvatal J., A public-key-based key escrow system, *Journal of Systems Software*, 35 (1996), nr 1, 73-83

[2] Fan Q., Xie D.Q., Key Escrow Scheme for Flexible Placing of Escrow Agent, *Computer Engineering and Applications*, 41 (2005), nr 10, 122-123

[3] Micali S., Fair Cryptosystems and Methods for Use, *MIT/LCS/TR-579.b* (1993)

[4] Shamir A., Partial key escrow: A new approach to software key escrow, *Proceedings of the Key Escrow Conference*, Washington (1995)

[5] Płonkowski M.,Urbanowicz P.,Lisica E., The use of quaternions in the cryptographic key agreement protocol based on the architectures of the TPQM neural networks, *Przegląd Elektrotechniczny*, 91 (2010), nr 7, 90-91

[6] Liu L., Zhang Q., Wei X.P., Zhou C. J., Image Encryption Algorithm Based on Chaotic Modulation of Arnold Dual Scrambling and DNA Computing, *Adv. Sci. Lett.*, 4 (2011), nr 11, 3537-3542

[7] Xie D.Q., Zhang D.F., A Key Escrow Sche me for Escrow Agency of Arbitrary Number, *Chinese Journal of Electronics*, 29(2001), nr 2, 172-174

[8] Duan S.S., Certificateless undeniable signature scheme, *Information Sciences：An International Journal*, 178 (2008), nr 3, 742-755

[9] Esnaashari M., Meybodi M.R., A Cellular Learning Automata Based Clustering Algorithm for Wireless Sensor Networks, *Sensors Lett.*, 6 (2008), nr 5, 723-735

[10] You L., Zhang G.W., Zhang F., A Cryptographic Key Binding Method Based on Fingerprint Features and the Threshold Scheme, *International Journal of Advancements in Computing Technology*, 3 (2011), nr 4, 21-31

***Authors**: Fan Qiang, senior engineer, associate professor, No.9 of the 3rd Yuanda Street, Changsha, 410138, China, E-mail: Fqabc@tom.com; Zhang Mingjian, associate professor; Zhang Yue, lecturer.*