Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 176085, 9 pages
http://dx.doi.org/10.1155/2014/176085

Research Article

A Rational Threshold Signature Model and Protocol Based on Different Permissions

Bojun Wang,[1] Cheng Cai,[1] and Quan Zhou[2]

[1] *School of Electronic and Computer Engineering, Peking University, Shenzhen 518055, China*
[2] *College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*

Correspondence should be addressed to Cheng Cai; frankgt40@gmail.com

Received 3 April 2014; Revised 1 July 2014; Accepted 4 July 2014; Published 23 July 2014

Academic Editor: Young-Sik Jeong

This paper develops a novel model and protocol used in some specific scenarios, in which the participants of multiple groups with different permissions can finish the signature together. We apply the secret sharing scheme based on difference equation to the private key distribution phase and secret reconstruction phrase of our threshold signature scheme. In addition, our scheme can achieve the signature success because of the punishment strategy of the repeated rational secret sharing. Besides, the bit commitment and verification method used to detect players' cheating behavior acts as a contributing factor to prevent the internal fraud. Using bit commitments, verifiable parameters, and time sequences, this paper constructs a dynamic game model, which has the features of threshold signature management with different permissions, cheat proof, and forward security.

1. Introduction

Secret sharing (SS) scheme, first proposed by Shamir [1] in the paper "How to share a secret," is a significant method used for the important information management. There are other SS schemes presented by Blakeley [2] and Asmuth and Bloom [3]. These (t, n)-threshold schemes above split the secret to n shares and distribute these shares to n legal players, meaning that all the players in the secret sharing system have the same permissions. However, in some specific situations, like in a company, managers and employees are supposed to have different authority in the confidential secret management. As a result, all the SS schemes are not suitable to be applied to such scenario. Later, many scholars devoted themselves to the weighted threshold SS schemes, which can solve the above problem. Shamir was concerned with weighted threshold SS in his paper "How to share a secret"—the president of a company has three shares, the vice presidents have two shares, and others have one share. Later, Morillo et al. [4] developed some main properties related to the information ratio, which measures a secret sharing system's security. After that, many researchers used their work to develop weight SS schemes, and some are with bipartite [5–7]. Chan and Chang [8] developed a new (t, n)-threshold scheme based on differential equations, which was completely different from the mechanism of weighted SS scheme and shared the same notion with Li [9]. Instead of the traditional weighted threshold SS schemes, which have the symmetrical permissions limitation, they proposed $(t_1 + t_2, n_1 + n_2)$-threshold SS scheme that is based on homogeneous constant coefficient linear difference equation. In the scheme, all players are divided into two groups (denoted by A, B) with the different secret management authority; just t_1 players from A and t_2 players from B can recover the original secret information. For example, a company divides its business secret into $(n_1 + n_2)$ shares, in which n_1 shares are possessed by n_1 specific employees and n_2 shares are distributed to n_2 managers. Any t_1 employees and t_2 managers can retrieve the business secret.

Threshold signature is based on SS, which was first proposed by Desmedt and Frankel [10] and based on RSA signature mechanism. Shamir [11] introduced the concept of signature authentication based on identity. Paterson and Schuldt [12] presented efficient identity-based signatures in the standard model. In this paper, to illustrate our model, we

adopt Okamoto's signature method [13], which is based on the identification scheme and is provably secure.

Another important issue about the traditional SS scheme is that they are all based on the assumption that every player is either honest or malicious. However, in practice, players are more likely to be selfish, trying to maximize their own utility. Halpern and Teague [14] introduced the notion of rational secret sharing (RSS) in 2004 and presented a randomized protocol for a $t \geq 3, n > 3$ SS scheme, which can achieve Nash equilibrium after repeated elimination of weakly dominated strategy. Gordon and Katz [15] improved Halpern's protocol to $t \geq 2, n > 2$ conditions. The mechanism proposed by Maleka et al. [16] is called repeated rational secret sharing (RRSS), in which the distributor needs to do second-time segmentation of the secret shares and made the players share the subshares repeatedly. Maleka's method uses punishment strategies to prevent players from finking, which is different from Halpern and Teague's RSS protocol, in which some rounds of secret sharing are meaningless.

In this paper, we present a rational threshold signature model, in which the participants are divided into two sets with the different permissions. We adopt the SS scheme based on the difference equations to distribute shares and recover the original secrets. In the recover phrase, players exchange their subshares repeatedly based on Maleka's RRSS scheme. In our model, we use several modules to manage the functions, respectively. The parameter sequence generator is used to generate the parameters of the difference equations and parameter distributor is used to distribute the parameters to the participants as their shares. Rounds controller is used to generate the random number of rounds so that the players cannot know when the repeated games will end. Bit commitment module is utilized for the players to commit their own subshares and verify others'. Besides, when a player cheats in a specific round by sending the wrong subshare, the verifiable module can detect it and the protocol will be stopped so that nobody can acquire the secret.

2. Relative Works

2.1. The Model of Li Bin Scholar. The model is outlined as follows.

Maker constructs homogeneous constant coefficient linear differential equation:

$$a_n + \sum_{i=1}^{t_1} b_i a_{n-i} = 0 \quad \left(b_i \in Z_q\right), \tag{1}$$

Master key: $k = a_N$ $(N > n_1)$,

Shadow keys of participants in set A are (a_i, b_1) $(i = 0, 1, \ldots, n_1 - 1)$,

Shadow keys of participants in set B are $(N, b_2, \ldots, b_{t_1})$.

The general term formula of homogeneous constant coefficient linear differential equation is

$$a_n = \sum_{i=1}^{t_1} c_i f_i(n). \tag{2}$$

Because coefficient determinant is nondegenerate second-order tensor,

$$\Delta_{t\times t} = \begin{vmatrix} f_1(0) & f_2(0) & \cdots & f_t(0) \\ f_1(1) & f_2(1) & \cdots & f_t(1) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(t-1) & f_2(t-1) & \cdots & f_t(t-1) \end{vmatrix}_{t\times t} \neq 0. \tag{3}$$

Participants in set A calculate constant vector:

$$c = \left(c_1, c_2, \ldots, c_{t_1}\right)^T. \tag{4}$$

Any participant in set B makes $n = N$ can obtain the system master key:

$$a_N = \sum_{i=1}^{t_1} c_i f_i(N) \quad \left(N > n_1\right). \tag{5}$$

2.2. Problems. The model mentioned above is a big innovation in the field of threshold structure; however, if applied directly to the threshold signature, while in practical use, some problems may exist as follows.

(1) The permissions in this model have limitations. The second component of $(n_1 + n_2, t_1 + 1)$-threshold shared structure on behalf of the second category participants with special privileges; these participants have excessive permissions, because anyone of them can represent the group. Thus, weexpand the second component into $(n_1 + n_2, t_1 + t_2)$ structure. Wei et al.'s scholars [17, 18] at Shandong University have proposed the definition of such structure. However, when this scheme is implemented, its two groups both use the polynomial ring, which possesses the symmetrical nature, thus it will break the different privileges characteristic of the homogeneousconstant coefficient linear differential equation. This paper promotes $(n_1 + n_2, t_1 + 1)$ structure based on homogeneous constant coefficient linear differential equation, extends permissions, in the meantime, and improves the original proposal.

(2) This model cannot resist conspiracy attacks, because of that when greater than or equal to the $(t_1,0)$ threshold number of participants work out the constant vector group of equation (4), at the same time, the equation (2) is determined. Conspires can get the the private key of the participants of the first set, using the general term formula, and one copy of the private key of the second set's participant can be used to conjecture the others' private keys in the second set.

(3) The model cannot resist internal fraud. When put into practical use, the model does not have a verifiable,

and the participants' fraud is undetectable. If there are no validation measures, the participants may run this protocol arbitrarily, or send their false shares, and these cannot be tolerated.

(4) The model has the dealer, who is the trusted third party. In the distributed network environment, the parameters is generated by a machine or by the secure multiparty computation.

(5) This model does not have the rational characteristics. When the signature private keys are generated, and when the first set's participants compute the equation (2)—after computing the general term formula, the participants in the second set have no motive to expose their private key to the participants in the first set, after they generate their private keys. This loses fairness.

3. Protocol Model

3.1. The Structure of Model. The structure of the model is shown in Figure 1.

(1) Parameter Sequence Generator. Each time while in the signature step, the registers in parameters sequence generator dynamically generate the next state parameters according to the last state parameters. Each signature call the module once; the use of time series technology makes the model have forward security.

The initial vector in parameter sequence generator is

$$\begin{aligned} a^{T_0} &= \left(a_n^{T_0}, a_{n-1}^{T_0}, \ldots, a_{n-t_1}^{T_0}\right)^T, \\ b^{T_0} &= \left(b_1^{T_0}, b_2^{T_0}, \ldots, b_{t_1}^{T_0}\right)^T. \end{aligned} \tag{6}$$

The iterative formulas of parameter sequence generator are as follows:

$$\begin{aligned} a^{T_{i+1}} &= \left(a_n^{\rho T_i}, a_{n-1}^{\rho T_i}, \ldots, a_{n-t_1}^{\rho T_i}\right)^T \bmod q \\ &\quad \left(i \geq 0 \wedge i \in Z^+, \rho \in_R GF(q)^*\right), \\ b^{T_{i+1}} &= \left(b_1^{\rho T_i}, b_2^{\rho T_i}, \ldots, b_{t_1}^{\rho T_i}\right)^T \bmod q \\ &\quad \left(i \geq 0 \wedge i \in Z^+, \rho \in_R GF(q)^*\right). \end{aligned} \tag{7}$$

Other parameters are generated like this way.

Theorem 1. *The model has forward security.*

Proof. On the completion of the last signature, in next signature step, the parameter sequence generator precompiled the iteration values in registers. After iteration, according to recurrence relations (7), the last data in registers will not exist. That is to say, this time's signature data in registers will cover the last data in them. According to the recurrence relations (7), if an attacker wants to get last data in registers, he or she must calculate mode square root:

$$\begin{aligned} a_k^{T_i} &= \sqrt[\rho]{a_k^{T_{i+1}}} \bmod q, \\ &\left(i \geq 0 \wedge i \in Z^+, k = n, \ldots, n - t_1 \wedge \rho \in_R GF(q)^*\right), \\ b_k^{T_i} &= \sqrt[\rho]{b_k^{T_{i+1}}} \bmod q, \\ &\left(i \geq 0 \wedge i \in Z^+, k = 1, \ldots, t_1 \wedge \rho \in_R GF(q)^*\right). \end{aligned} \tag{8}$$

The mode square root in polynomial time is computationally infeasible, and the mode indices are random; attacker cannot predict. So the model has forward security. □

(2) Rounds Controller. This model, which runs multiple rounds in the signature process, is a limited time repetitions dynamic game. It is vital in the model and controls the operation of the entire process. Here we use the idea of stochastic process [19] to construct model.

Theorem 2. *The distribution of round obeys Poisson distribution with parameter λ.*

Proof. In the condition of time limited game process, note that the number of deceptions in each round is k, with the probability satisfying the following formula:

$$\Pr_k(r_0, r) = \Pr\{N(r_0, r) = k\} \quad (k \in Z). \tag{9}$$

Participants' behavior is independent in each round.

Assuming the number of rounds has continuity, that is to say, the process of game is taken as continuous function with time,

$$\begin{aligned} \Pr_1(r, r + \Delta r) &= \Pr\{N(r, r + \Delta r) = 1\} \\ &= \lambda \Delta r + o(\Delta r) \quad (\lambda > 0 \wedge \forall \Delta r \longrightarrow 0), \\ \sum_{i=2}^{\infty} \Pr_i(r, r + \Delta r) &= \sum_{i=2}^{\infty} \Pr\{N(r, r + \Delta r) = i\} \\ &= o(\Delta r) \quad (\lambda > 0 \wedge \forall \Delta r \longrightarrow 0), \end{aligned} \tag{10}$$

and it satisfies that

$$N(0) = 0 + o(\varepsilon). \tag{11}$$

□

This means that, the probability of cracking the system with ε computational advantages can be negligible, when the threshold signature process is not performed. The model satisfies the four conditions mentioned above and meets the definition of Poisson process with λ intensity. That is,

$$N(r) - N(r_0) \sim \pi(\lambda(r - r_0)). \tag{12}$$

Theorem 3. *The expectations rounds of this model are λ, each time the model convergence time complexity is $O(\lambda)$.*

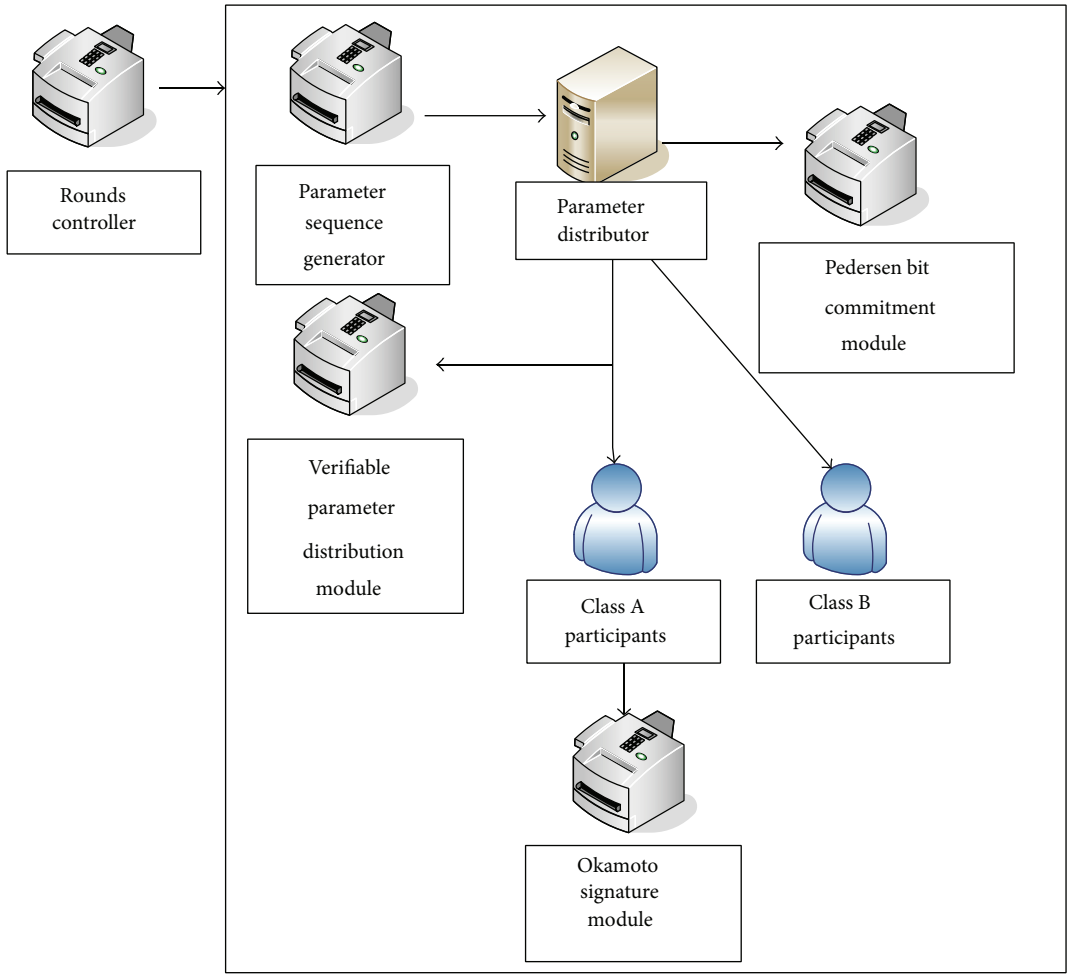

FIGURE 1: The structure diagram of model.

Proof. Differential equations are established for the rounds $(r_0, r_1, \ldots, r^*)$ respectively, based on the four conditions mentioned above

$$\begin{aligned} \Pr_k(r_0, r) &= \Pr\{N(r_0, r) = k\} \\ &= \frac{[\lambda(r - r_0)]^k}{k!} e^{-\lambda(r-r_0)} \quad (r, k \in Z). \end{aligned} \tag{13}$$

The mathematical expectation is

$$E[N(r) - N(r_0)] = \lambda(r - r_0). \tag{14}$$

So the expectations rounds of this model are λ, each time the model convergence time complexity is $O(\lambda)$. □

(3) Parameter Distributor. A machine can analog the behavior of distributor (maker) and can be a trusted server in the distributed network.

(4) Pedersen Bit Commitment Module. Pedersen bit commitment protocol [20] is a security protocol taken as commitment to the bit stream information. In each time of signature, the system generates coefficients of homogeneous constant coefficients differential equations, and the coefficients of algebraic curved $F(x)$ with order $n_2 - 1$, which correspond to the participants in set B. After storing the coefficients in the binary bits formation, we note them as form of m_i $(i \in Z \wedge m_i \in \{0, 1\})$, in the form of bits stream. The parameter distributor is also attached with the bit commitment model to prevent it from attacks.

Theorem 4. *The model can detect whether the parameter distributor is under attack or not.*

Proof. The model adapts the Pedersen's bit stream commitment protocol.

Parameter distributor selects a random number $\rho \in_R GF(p^{\max\{n_1, n_2\}})^*$, timestamp information t, and secure hash function $H(m_i, t)$ $(i \in Z \wedge m_i \in \{0, 1\})$.

To make bit stream and timestamp above hash process. The primitive element of group $GF(p^{\max\{n_1, n_2\}})$ is g; publish

$$\delta = g^{\rho} y^{H(m_i, t)} \bmod p^{\max\{n_1, n_2\}} \quad (i \in Z \wedge m_i \in \{0, 1\}). \tag{15}$$

The triple (ρ, m_i, t) will be publish to the public, right after the end of the signature process. Set A and set B participants

can verify commitment to make sure whether parameter distributor is being attacked or not. □

(5) Verifiable Parameter Distribution Module. Using the idea of Feldman's [21] verification. First, publicize bivariate one-way function $H(x, y)$. In each threshold signature process, parameter distributor generates polynomial with $n_1 - 1$ orders which corresponds to set A participants:

$$G(x) = \sum_{i=1}^{n_1-1} u_i x \bmod p^{n_1}. \tag{16}$$

Our model uses the primitive element in the finite fields $GF(p^{n_1})$, which is g_1, to compute the number of the operation rounds, which is r^*, according to the Poisson distribution with parameter λ, and then distribute the points sequence:

$$(x_{1i}, y_{1i}) = \left(H\left(s_{1i}, g_1^{r^*}\right), G(x_{1i})\right) \quad (i = 0, 1, \ldots, n_1 - 1). \tag{17}$$

Then it arbitrarily selects $n_1 - t_1$ points in the field of $F_{p^{n_1}}(x, y)$ except the ones in the equation (17), and publish them to the public.

Then it saves the vector

$$s_{1i} \quad (i = 0, 1, \ldots, 2n_1 - t_1 - 1), \tag{18}$$

and calls Pedersen's bit commitment module.

After that, it broadcasts:

$$V_i = g_1^{u_i} \bmod p^{n_1} \quad (i = 0, 1, \ldots, n_1 - 1). \tag{19}$$

Send each participant in set A:

$$\mathrm{TPK}_i = [a_i + G(0)] \bmod p^{n_1},$$
$$\left(i = 1, 2, \ldots, n_1, a_i \in GF(q)^*, G(0) \in GF\left(p^{n_1}\right)^* > \sup a_i\right). \tag{20}$$

In the set B, the parameter distributor generates the primitive element, which is g_2, in the infinite field $GF(p^{n2})$, according to this polynomial with $n_2 - 1$ orders:

$$L(x) = \sum_{i=1}^{n_2-1} l_i x \bmod p^{n_2}. \tag{21}$$

And then, with the rounds number r^* noted before, the system distributes publish the points sequence:

$$(x_{2i}, y_{2i}) = \left(H\left(s_{2i}, g_2^{r^*}\right), L(x_{2i})\right) \quad (i = 0, 1, \ldots, n_2 - 1). \tag{22}$$

We adopt (n_2, t_2) threshold structure constructed by matrix method. t_2 players in set B participate in the repeated games and recover the secret S using the published $n_2 - t_2$ points. As a result, the players in set A can input S after they get the general term formula of homogeneous constant coefficient linear differential equation.

Save vector

$$s_{2i} \quad (i = 0, 1, \ldots, 2n_2 - t_2 - 1). \tag{23}$$

And call Pedersen's bit commitment module.

After that, it broadcasts:

$$W_i = g_2^{l_i} \bmod p^{n_2} \quad (i = 0, 1, \ldots, n_2 - 1). \tag{24}$$

Send each participant in set B:

$$\mathrm{TPK}_j = [S + L(0)] \bmod p^{n_2},$$
$$\left(j = 1, 2, \ldots, n_2, S \in GF(p)^*, L(0) \in GF\left(p^{n_2}\right)^* > S\right). \tag{25}$$

Theorem 5. *The model is verifiable.*

Proof. When distributing point's sequence and broadcasting corresponding authentication information, participants can simultaneously verify the information.

Set A participants verify

$$g_1^{G(x_{1i})} = \prod_{j=0}^{n_1-1} V_i^{x_{1i}^j} \bmod p^{n_1} \quad (i = 0, 1, \ldots, n_1 - 1). \tag{26}$$

Set B participants verify

$$g_2^{L(x_{2i})} = \prod_{j=0}^{n_2-1} W_i^{x_{2i}^j} \bmod p^{n_2} \quad (i = 0, 1, \ldots, n_2 - 1). \tag{27}$$

If the verification succeeds, participants can trust the information sent by others. □

(6) Participants. Participants in two different permissions together constitute the threshold structure $(n_1 + n_2, t_1 + t_2)$. In addition, $|A| = n_1 |B| = n_2$, and the threshold values are $|A|_{\text{threshold}} = t_1$ and $|B|_{\text{threshold}} = t_2$.

(7) Okamoto Signature Module. After calculating the threshold signature private key, take $\mathrm{TSK} = a_S$ as the first private key component of the signature module, while the second private key component is generated by public key signature method; select private keys; and publicize public keys, respectively. The model adopts Okamoto signature algorithm to signature finally.

Theorem 6. *The model can resist conspiracy attack.*

Proof. The second component of the private key in Okamoto signature algorithm can avoid conspiracy attacks which are performed by using general term formula to get other participants' private keys when meeting the threshold condition to calculate homogeneous linear differential equations with constant coefficients general term formula in original model. The second component of everyone's private key has to be kept privately by each individual. On condition that the second component of the private key ensures the privacy, the threshold signature cannot be forged. Furthermore, we can establish a mechanism, that is when there is a dispute, the system will check every participant involving the process of signature arise disputes. □

3.2. Improved Threshold Model. We adopt (n_2, t_2) threshold structure constructed by matrix method. t_2 players in set B participate in the repeated games and recover the secret S using the published $n_2 - t_2$ points. As a result, the players in set A can input S after they get the general term formula of homogeneous constant coefficient linear differential equation.

Make two field extensions:

$$\begin{aligned}[GF(p^{n_1}) : GF(q)] &= [GF(p^{n_1}) : GF(p)]\,[GF(p) : GF(q)],\\ [GF(p^{n_2}) : GF(q)] &= [GF(p^{n_2}) : GF(p)]\,[GF(p) : GF(q)].\end{aligned} \tag{28}$$

Expansion order of algebraic number field $GF(q)$ is

$$\begin{aligned}Q_1 &= [GF(p^{n_1}) : GF(q)] = n_1 * \left[\frac{p-1}{q}\right],\\ Q_2 &= [GF(p^{n_2}) : GF(q)] = n_2 * \left[\frac{p-1}{q}\right].\end{aligned} \tag{29}$$

Remove the noise terms $L(0)$ and $G(0)$ to get coefficients information of homogeneous constant coefficient linear differential equation.

3.3. Dynamic Game Model

Definition 7. The Computable complete and perfect information dynamic game $\tau = [P, T, A, S, R, H, I, O, U]$ satisfies:

Participants are noted as $P = \{\text{Simulator}, P_i\}$ (Simulator represents the nature and parameter distributor).

The set of Types is $T = \{T_i\}$ $(T_i \in \{\text{honesty}, \text{fraud}\})$.

Actions set is $A = \{A_i\}$ $(A_i \in \{\text{honesty}, \text{fraud}\})$.

Strategy set is $S = \{S_i\}\varphi : (T_i, H_i, I_i, A_i) \to S_i$.

Rounds set is $R < O(\lambda) \wedge R \in Z^+$.

Full history set $H = \{h \mid h = \bigoplus_{i=1}^{k} A_i\}$ $(i \in R \wedge 0 \le k \le R)$ is depicted as game tree, whose root is empty history node $\emptyset$.

The information set $I = \{I_i\}$ can be tested and is perfect.

Outcome set is $O = \{O_i\}\gamma : (A_i, S_i) \to O_i$.

Utility function set is $U = \{U_i\}$ $\gamma \circ \varphi : (T_i, H_i, I_i, A_i, S_i, O_i) \to U_i$ and satisfies $\partial^2 U_i < 0$.

The above game τ can be calculated in polynomial time.

Definition 8. Computable complete and perfect information dynamic game with $t_1 + t_2$ elastic equilibrium will reach the equilibrium results, under the conditions that it satisfies the Definition 7 and that each participants is rational. That is, $U(\sigma_i, \sigma_{-i}) < U(\sigma_i^*, \sigma_{-i})$, σ is multiple real variable function $\sigma : (T_i, H_i, I_i, A_i, S_i, O_i, U_i) \to U(\sigma_i, \sigma_{-i})$.

Theorem 9. *The model converges to computable complete and perfect information dynamic game with $t_1 + t_2$ elastic equilibrium.*

Proof. Participants who accord with threshold signature conditions possess superiority of $\Pr = \varepsilon$ $(0 < \varepsilon < 1)$. They can get threshold signature private key without the normal operation of the model. Definitions of utility functions are as follows:

$U^{++}_{(0,i)}$: participants' ideal utility without the normal operation of the model to obtain the threshold signature private key;

$U^{+}_{(r,i)}$ $(0 \le r \le r^*)$: the utility that participant i gets signature private key and others do not get it in r round;

$U^{-}_{(r,i)}$ $(0 \le r \le r^*)$: utility that participant i does not comply with the normal execution of the model when model run r round;

$U_{(r,i)}$ $(0 \le r \le r^*)$: utility that participant i complies with the normal execution of the model when model run r round;

$U_{(r^*,i)}$: normal utility that participant i always complies with the operation of the model obtains threshold signature private key when model reaches the last one round;

$U^{-}_{(r,\text{all})}$ $(0 \le r \le r^*)$: utility that all participants do not obtain the threshold signature private key. Illustrate that there are some participants had deceived cause model abnormal termination.

Utility function satisfies the strong partial: $U^{++}_{(0,i)} > U^{+}_{(r,i)} > U_{(r^*,i)} > U^{-}_{(r,\text{all})}$.

Define events as follows.

A: participant uses the advantage of $\Pr = \varepsilon$ $(0 < \varepsilon < 1)$ to crack threshold signature private key.

B: participant implements protocol.

C: participant takes honesty policy in round r.

D: participant takes fraud policy in round r.

We denote the utility of departing from the protocol as $U_{\text{exception}}$ and denote the expected utility as $E(U_{\text{exception}})$. We can get the equation as follows.

$$\begin{aligned}U_{\text{exception}} &= \varepsilon U(\Pr(A)) + (1-\varepsilon)\,U(\Pr(B)),\\ U(\Pr(B)) &= U(\Pr(B \mid C)\Pr(C) + \Pr(B \mid D)\Pr(D))\\ &= \lambda U_{(r^*,i)} + (1-\lambda)\sum_{i=1}^{r} U^{-}_{(r,i)}\\ &= \lambda U_{(r^*,i)} + (1-\lambda)\end{aligned}$$

$$\times \sum_{i=1}^{r} \left[\frac{1}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,i)}^{+} + \frac{\left(GF(p)^* - 1\right)^2}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,\mathrm{all})}^{-} \right],$$

$$U_{\mathrm{exception}} = \varepsilon U_{(0,i)}^{++} + (1-\varepsilon) \times \left[U_{(r^*,i)} + (1-\lambda) \times \sum_{i=1}^{r} \left(\frac{1}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,i)}^{+} + \frac{\left(GF(p)^* - 1\right)^2}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,\mathrm{all})}^{-} \right) \right], \tag{30}$$

$$[GF(p) : GF(q)] = \frac{p-1}{q}.$$

In our protocol,

$$U_{\mathrm{exception}} < U_{(r^*,i)}. \tag{31}$$

Distribution function satisfies

$$r^* = \psi(\lambda). \tag{32}$$

The following formulas are met:

$$\lambda < \Phi * \left[\frac{U_{(r^*,i)} - \varepsilon U_{(0,i)}^{++}}{1-\varepsilon} - \sum_{i=1}^{r} \left(\frac{1}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,i)}^{+} + \frac{\left(GF(p)^* - 1\right)^2}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,\mathrm{all})}^{-} \right) \right], \tag{33}$$

in which

$$\Phi = 1 \times \left(U_{(r^*,i)} - \sum_{i=1}^{r} \left(\frac{1}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,i)}^{+} + \frac{\left(GF(p)^* - 1\right)^2}{\left|GF(p)^*\right|\left|GF(p)^*\right|} U_{(r,\mathrm{all})}^{-} \right) \right)^{-1}. \tag{34}$$

The above equation can determine the range of parameters selection, so that the model converges to computable complete and perfect information dynamic game with $t_1 + t_2$ elastic equilibrium. □

Theorem 10. *The model can resist inner fraud.*

Proof. According to Theorem 9, a rational participant will not depart from the protocol execution in any round. The model overcomes the sensitivity of backward induction and adopts mixed strategy equilibrium. If participants adopted a deceptive strategy in the model execution of any round, this caused the decrease in revenue of participants to $U_{(r,\mathrm{all})}^{-}$. When the protocol terminates, punishment strategies can be used, thus putting an end to deceiving behavior effectively. So the model can prevent inner fraud. □

4. Protocol Procedure

4.1. Parameters Generation Process. Determine the order of set A and set B; determine the threshold value according to the requirements, respectively. Select big prime q, p meets $q \mid (p-1)$. Select primitive element g_1 in finite field $GF(p^{n_1})$ and g_2 in finite field $GF(p^{n_2})$. The participants in set A and set B select signature private key as the second component of the Okamoto signature, respectively.

Parameter sequence generator generates coefficient constants vector of homogeneous constant coefficient linear differential equation:

$$a^0 = \left(a_1^0, a_2^0, \ldots, a_{n-t_1}^0\right) \quad \left(a_i^0 \in Z_q\right),$$
$$b^0 = \left(b_1^0, b_2^0, \ldots, b_{n-t_1}^0\right) \quad \left(b_i^0 \in Z_q\right). \tag{35}$$

Superscript represents signature number of times; 0 represents the first signature.

4.2. Dynamic Games Process. Rounds controller according to Poisson distribution with parameter λ secret generates threshold signature round r^*. According to the number of participants in set A and set B, the threshold value generates coefficient constants vector of polynomial $G(x)$ and $L(x)$, respectively:

$$u^0 = \left(u_1^0, u_2^0, \ldots, u_{n_1}^0\right) \quad \left(u_i^0 \in Z_{q^{n_1}}\right),$$
$$l^0 = \left(l_1^0, l_2^0, \ldots, l_{n_2}^0\right) \quad \left(l_i^0 \in Z_{q^{n_2}}\right). \tag{36}$$

Superscript signature represents the number of rounds; 0 represents the first round.

Parameter distributor according to (17) and (22) distributes and publicizes points. Participants in set A and set B can use the verifiable parameter distribution module for verification. If there is no cheating behavior, the protocol continues to execute. Otherwise, the verifiable parameter distribution module goes to the interrupt processing. In every round of the games, the players in set A and set B use the published points sequence and generate $G(0)^r$ and $L(0)^r$, respectively.

Table 1: Several models comparison.

Model	Verifiable	Bit commitment	Resist conspiracy attack	Forward security	permission	Convergence time	Range of parameters
Halpern and Teague	No	No	No	No	different	$O(\frac{5}{\alpha^3})(0<\alpha<1)$	$\frac{\alpha^2}{\alpha^2+(1-\alpha)^2}U^+(\sigma_i,\sigma_{-i}) + \frac{(1-\alpha)^2}{\alpha^2+(1-\alpha)^2}U^-(\sigma_i,\sigma_{-i}) > U(\sigma_i^*,\sigma_{-i})$
Gordon and Katz	No	No	No	No	different	$O(\frac{1}{\beta})(0<\beta<1)$	$\beta \le \frac{U(\sigma_i^*,\sigma_{-i})-U^-(\sigma_i,\sigma_{-i})}{U^+(\sigma_i,\sigma_{-i})-U^-(\sigma_i,\sigma_{-i})}$
Computable complete and perfect information dynamic game	Yes	Yes	Yes	Yes	different	$O(\lambda)(\lambda>0)$	$\lambda < \frac{U_{(r^*,i)}-\varepsilon U_{(0,i)}^{++}}{(1-\varepsilon)*U_{(r^*,i)}}$

Parameter distributor verifies, respectively,

$$\begin{aligned}&\left[\mathrm{TPK}_i - G^r(0)\right] \bmod p^{n_1} \stackrel{?}{=} a_i,\\ &\left(G^r(0) \in GF\left(p^{n_1}\right)^* > \sup a_i, i = 1,2,\ldots,n_1\right),\\ &\left[\mathrm{TPK}_j - L^r(0)\right] \bmod p^{n_2} \stackrel{?}{=} S,\\ &\left(S \in GF(p)^* \wedge L^r(0) \in GF\left(p^{n_2}\right)^* > S, j = 1,2,\ldots,n_2\right).\end{aligned} \tag{37}$$

If $r = r^*$ and (37) holds, calculate (2), and then

$$\mathrm{TSK} = a_S \quad (S > n_1 + n_2). \tag{38}$$

If $r \neq r^*$ and (37) does not hold, $G(0)^r$ and $L^r(0)$ equal the expected value and the protocol enters into the next round.

If $r \neq r^*$ and (37) does not hold, meanwhile, $G(0)^r$ and $L^r(0)$ do not equal the expected value, someone of the players have cheated. At this time, the parameter distributor can perceive the cheating behavior so that the player cannot obtain the signature private key. According to Theorem 10, the rational participants will not deceive.

4.3. Threshold Signature Process. The Okamoto signature module is used to complete the feature of signature.

Okamoto signature algorithm contains two private keys: the first is threshold signature private key just generated, and the second is each participator's signature private key in set A and set B. Only after verification, parameter distributor can call Okamoto signature module. Two private key generation equations are as follows:

$$\begin{aligned}&\mathrm{TSK}_1 = a_S \quad (s > n_1 + n_2),\\ &\mathrm{TSK}_2 = \prod_{i=0}^{t_1+t_2-1} \mathrm{SHA}(m)^{SK_i}.\end{aligned} \tag{39}$$

Verify equation

$$\prod_{i=0}^{t_1+t_2-1} \mathrm{TSK}_2^{PK_i} \stackrel{?}{=} \mathrm{SHA}(m). \tag{40}$$

m is message sequence, and SHA is secure hash function. We use the equation (41) to complete signature.

$$\left(\sigma_1,\sigma_2,\sigma_3\right) = \mathrm{Okamoto}\left(\mathrm{TSK}_1, \mathrm{TSK}_2\right). \tag{41}$$

Validation process can use standard Okamoto algorithm.

4.4. Several Models Comparison. Table 1 is several models comparison. The parameters range of this model uses the limiting form of (31), (32), (33), and (34).

5. Conclusion

This paper proposed computable complete and perfect information dynamic game with $t_1 + t_2$ elastic equilibrium, based on the homogeneous constant coefficient linear differential equation. We constructs a dynamic game model and protocol using time sequences, bit commitments, Feldman's verification menthod, and Okamoto's signature permissions. The model achieves two different threshold signature permissions. We proved that, during the game, no participant has the tendency of departing from normal operation, so that the model achieves the purpose of preventing fraud. Our method expands the idea of permission and overcomes five inherent problems in homogeneous constant coefficient linear differential equation.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No.61170221). The authors appreciate the help as well as the hard work of the editor.

References

[1] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. Blakeley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, pp. 313–317, AFIPS Press, New York, NY, USA, 1979.

[3] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 208–210, 1983.

[4] P. Morillo, C. Padró, G. Sáez, and J. L. Villar, "Weighted threshold secret sharing schemes," *Information Processing Letters*, vol. 70, no. 5, pp. 211–216, 1999.

[5] C. Padró and G. Sáez, "Secret sharing schemes with bipartite access structure," *IEEE Transactions on Information Theory*, vol. 46, no. 7, pp. 2596–2604, 2000.

[6] T. Tassa and N. Dyn, "Multipartite secret sharing by bivariate interpolation," *Journal of Cryptology*, vol. 22, no. 2, pp. 227–258, 2009.

[7] O. Farràs, J. R. Metcalf-Burton, C. Padró, and L. Vázquez, "On the optimization of bipartite secret sharing schemes," *Designs, Codes and Cryptography*, vol. 63, no. 2, pp. 255–271, 2012.

[8] C.-W. Chan and C.-C. Chang, "A new (t, n)-threshold scheme based on difference equations," in *Combinatorics, Algorithms, Probabilistic and Experimental Methodologies*, pp. 94–106, Springer, Berlin, Germany, 2007.

[9] B. Li, "Differential secret sharing scheme based on special access secret sharing scheme," *Journal of Sichuan University (Natural Science)*, vol. 43, no. 1, pp. 78–83, 2006.

[10] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Proceedings of Advances in Cryptology-CRYPTO '91, Santa Barbara, Calif, USA, 1991*, pp. 457–469, Springer, Berlin, Germany, 1992.

[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, vol. 196 of *Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1985.

[12] K. G. Paterson and J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Information Security and Privacy*, vol. 4058 of *Lecture Notes in Computer Science*, pp. 207–222, Springer, Berlin, Germany, 2006.

[13] T. Okamoto, "Provable secure and practical identification schemes and corresponding signature schemes," in *Advances in Cryptology-CRYPTO '92*, vol. 740 of *Lecture Notes in Computer Science*, pp. 31–53, Springer, Berlin, Germany, 1992.

[14] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation: extended abstract," in *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC '04)*, pp. 623–632, New York, NY, USA, 2004.

[15] S. D. Gordon and J. Katz, "Rational secret sharing, revisited," in *Security and Cryptography for Networks*, vol. 4116 of *Lecture Notes in Computer Science*, pp. 229–241, Springer, Berlin, Germany, 2006.

[16] S. Maleka, A. Shareef, and C. P. Rangan, "The deterministic protocol for rational secret sharing," in *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS '08)*, pp. 1–7, IEEE, April 2008.

[17] D. Wei and X. Qiuliang, "Special permission-based rational secret sharing scheme," *China Electronic Business: Communications Market*, no. 2, pp. 180–184, 2009.

[18] W. Dong, *Secret sharing based on game theory and application of the theory [M.S. thesis]*, Shandong University, 2011.

[19] F. Z. Ben, *Stochastic Process*, Science Press, Beijing, China, 2011.

[20] Q. Weidong, *Crypto Graphic Protocols Foundation*, Higher Education Press, Beijing, China, 2009.

[21] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pp. 427–437, 1987.