Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 462345, 7 pages
http://dx.doi.org/10.1155/2015/462345

Research Article

Verifiable Rational Secret Sharing Scheme in Mobile Networks

En Zhang,[1,2,3] Peiyan Yuan,[1,3] and Jiao Du[4]

[1]*College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[3]*Engineering Lab of Intelligence Business & Internet of Things, Xinxiang, Henan 453007, China*
[4]*College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China*

Correspondence should be addressed to En Zhang; zhangenzdrj@163.com

Received 30 January 2015; Revised 18 May 2015; Accepted 27 May 2015

Academic Editor: Francesco Gringoli

With the development of mobile network, lots of people now have access to mobile phones and the mobile networks give users ubiquitous connectivity. However, smart phones and tablets are poor in computational resources such as memory size, processor speed, and disk capacity. So far, all existing rational secret sharing schemes cannot be suitable for mobile networks. In this paper, we propose a verifiable rational secret sharing scheme in mobile networks. The scheme provides a noninteractively verifiable proof for the correctness of participants' share and handshake protocol is not necessary; there is no need for certificate generation, propagation, and storage in the scheme, which is more suitable for devices with limited size and processing power; in the scheme, every participant uses her encryption on number of each round as the secret share and the dealer does not have to distribute any secret share; every participant cannot gain more by deviating the protocol, so rational participant has an incentive to abide by the protocol; finally, every participant can obtain the secret fairly (means that either everyone receives the secret, or else no one does) in mobile networks. The scheme is coalition-resilient and the security of our scheme relies on a computational assumption.

1. Introduction

1.1. Background. Secret sharing is playing a more and more important role in modern cryptography. In classical (t, n) secret sharing schemes [1, 2], a secret can be shared among n participants. At least t or more participants can reconstruct the secret, but $t - 1$ or fewer participants cannot obtain anything about the secret. Recently, a series of secret sharing schemes were proposed in [3–6]. However, the works in [1–6] cannot prevent the dealer or players from cheating. For example, in Shamir's scheme, we assume that one party does not broadcast his share, while exactly $t-1$ other players reveal their shares. He can still reconstruct the secret although his cheating can be detected by the scheme [7–9].

Motivated by the desire to develop more realistic models, the cryptographic community has significant interest in exploring protocols for rational secret sharing. Halpern and Teague [10] firstly introduced the notion of rational secret sharing. They pointed out that there exist many Nash equilibriums which, in some sense, are unreasonable. Therefore, they focus on one particular refinement of Nash equilibrium that is determined by iterated deletion of weakly dominated strategies. However, their protocols cannot work for 2 out of 2 secret sharing and require the online dealer. Later, a series of rational secret sharing schemes [11–20] were proposed. However, none of them are fully satisfactory. The works in [11–13] rely on secure multiparty computation which is strong. Kol and Naor's scheme [14] has information theoretic security. However, their scheme fails to resist against coalitions. The works in [15, 16] require the involvement of some trusted external parties during the reconstruction phase which is difficult to find. The solution in [17] constructs a rational scheme based on repeated games. However, every player has high probability to learn the secret in his last round. The works of Lepinski et al. [19, 20] and Izmalkov et al. [15, 18] can guarantee fairness, prevent coalitions, and eliminate side information. However, their solutions rely on physical assumption such as secure envelopes and ballot

boxes. The works in [10–14, 17, 21–25] assume the existence of broadcast channel which is not realistic. The works in [11–13, 19–27] need to exchange public keys associated with certificate management, including revocation, storage and distribution, and the computational cost of certificate verification. Nowadays, with the development of mobile network, a large percent of the world's population now has access to mobile phones and incredibly fast mobile networks give users ubiquitous connectivity. New devices like smart phones and tablets are providing users with a lot of applications and services and have fundamentally changed our lives. However, smart phones and tablets are poor in computational resources such as processor speed, memory size, and disk capacity. A drawback of public key infrastructure (PKI) is that they are computationally very intensive, which makes them less suitable mobile phones. From the discussion above, it seems clear that all of above schemes cannot work in a mobile system.

1.2. Our Results. In this paper, we propose a verifiable rational secret sharing scheme in mobile networks. The major contribution of this work is as follows. We present a new verifiable random function for multiparty case, which provides a noninteractively verifiable proof for the correctness of participants' share and handshake protocol is not necessary; there is no need for certificate generation, propagation, and storage in the scheme, which is more suitable for devices with limited size and processing power; the public key in our approach is based on each participant's identity (e.g., telephone number or email address), which can be very much shorter as compared to the 1024 bits public key in RSA cryptosystem; in the scheme, every participant uses her/his encryption on number of each round as the secret share and the dealer does not have to distribute any secret share, which reduce the computational consumption and communicational overhead; the participants do not know whether the current round is a test round or not, and every participant cannot gain more by cheating. Finally, every player can obtain the secret fairly (means that either everyone receives the secret, or else no one does) in mobile networks. To the best of our knowledge, we propose the first rational secret sharing scheme over mobile networks.

1.3. Overview. The rest of this paper is organized as follows. In Section 2, the preliminary of game theory and cryptography for rational secret sharing are introduced. Section 3 introduces the rational secret scheme in mobile networks. In Section 4, we analyze the new scheme. Finally, we present our conclusions in Section 5.

2. Preliminaries

2.1. Basics of Game Theory. We begin by introducing some basic terminology of game theory in this section. For more details, please refer to [28].

Game theory aims to help us understand situations in which decision-makers interact. A strategic game consists of three components: (a) a set of players; (b) a set of actions for each player; (c) for each player, preferences over the set of action profiles.

Let $a = (a_1, \ldots, a_n)$ be profile of players, a_i denote the strategy employed by player P_i, a_{-i} be a strategy profile of all players except for the player P_i, and $(a_i', a_{-i}) = (a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$ denote the strategy vector a with P_i's strategy changed to a_i'; $u_i(a)$ represents P_i's preferences, which rational players wish to maximize.

Definition 1 (Nash equilibrium). Let $\Gamma = (\{A_i\}, \{u_i\}_{i=1}^n)$ be a game presented in normal form. A strategy profile $a = (a_1, \ldots, a_n) \in A$ is Nash equilibrium if, for all i and every $a_i' \in A_i$, it holds that

$$u_i\left(a_i', a_{-i}\right) \leq u_i\left(a\right). \tag{1}$$

Generally speaking, Nash equilibrium holds the idea that no rational party has an incentive to deviate from the protocol. Everyone is playing a best response to everyone else and no individual can do strictly better by moving away. The definition of Nash equilibrium is designed to model a steady state among experienced players. In a steady state, no player wishes to change her behavior, considering the other players' behavior.

In a traditional secret sharing scheme, a player is thought as either honest or malicious. However, in a rational secret sharing scheme, it may make more sense to view the players, not as good or bad, but as rational individuals trying to maximize their own utility [10]. For any player P_i, assume that any rational player prefers to get the secret rather than miss it. And secondarily, prefer that as few as possible of the other players get it.

Now, let we introduce the definition of computational C-immune [13] in which utility functions take the security parameter k as input.

Definition 2 (computational C-immune). Let σ be an efficient protocol for a computing game and $\mathbb{C}$ be a set of coalitions (subsets of players). Let R^t be the set of sequences of random tapes for the first t iterations that do not cause σ to end. A sequence $r \in R^t$ is of the form $r = (r^1, \ldots, r^t)$ where $r^s = (r_1^s, \ldots, r_n^s)$ and r_j^s is the random tape used by player j in iteration s.

The protocol σ is computational C-immune if, for every coalition $C \in \mathbb{C}$ and every sequence of tapes $r_0 = (r_0^1, \ldots, r_0^t) \in R^t$ used by the players in the first t round, there exists a negligible function $\varepsilon(k)$ such that, for every player $i \in C$, every efficient (deviating) joint strategy σ_C' for players in C, and every efficient joint strategy τ_{-C} for players in N/C implementing σ_{-C}, it holds that

$$\begin{aligned} &E\left[u_i\left(\tau_{-C}\left(k\right), \sigma_C\left(k\right)\right)\right] + \varepsilon\left(k\right) \\ &\quad \geq E\left[u_i\left(\tau_{-C}\left(k\right), \sigma_C'\left(k\right)\right)\right]. \end{aligned} \tag{2}$$

2.2. Cryptographic Terminology

Definition 3 (bilinear pairing). Let G_1 and G_2 be multiplicative groups of prime order p. g is the generator of G_1.

A bilinear pairings is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties.

(1) Bilinear: for all $u, v \in G_1$ and all $a, b \in Z$, one has $e(u^a, v^b) = e(u, v)^{ab}$.

(2) Nondegenerate: $e(g, g) \neq 1$.

(3) Computable: there is an efficient algorithm to compute $e(u, v)$ for all u and $v \in G_1$.

We describe decisional bilinear Diffie-Hellman inversion assumption below.

Given $(g, g^x, \ldots, g^{(x^q)})$ as input, to distinguish $e(g, g)^{1/x}$ from random. An algorithm A has advantage ε in solving the q-DBDHI problem if

$$\left|\Pr\left[A\left(g, g^x, \ldots, g^{(x^q)}, e\left(g, g\right)^{1/x}\right) = 1\right] - \Pr\left[A\left(g^x, \ldots, g^{(x^q)}, \Gamma\right) = 1\right]\right| \leq \varepsilon, \tag{3}$$

where $x \in Z_p^*$ and $\Gamma \in G_2$.

We say that the (t, q, ε)-DBDHI assumption holds in G_1, if no t-time algorithm A has advantage at least ε in solving the q-DBDHI problem in G_1.

2.3. Verifiable Random Function from Identity-Based Key Encapsulation (IB-KEM). Verifiable random function (VRF) was firstly introduced by Micali et al. [29]. A VRF is a pseudorandom function that provides a noninteractively verifiable proof for the correctness of its output, and the VRF has many useful applications. References [29–32], respectively, constructed a VRF. Next we briefly recall the VRF from a VRF-suitable IB-KEM [32].

The IB-KEM Scheme. An identity-based key encapsulation mechanism (IB-KEM) scheme allows a sender and a receiver to agree on a random session key K. And it is defined by four algorithms: Setup(1^k) takes a security parameter as input and outputs a master key pairs (mpk, msk); KeyDer(msk, ID) uses the master secret key to compute $\mathrm{sk}_{\mathrm{ID}}$ for identity ID; Encap(mpk, ID) computes a random session key K and a ciphertext C; Decap(C, $\mathrm{sk}_{\mathrm{ID}}$) allows the receiver to decapsulate C to get back a session key K. An VRF-suitable IB-KEM scheme [33] is defined by the following algorithms.

(i) Setup(1^k) is a probabilistic algorithm that takes in input a security parameter k and outputs a master public key mpk and a master secret key msk. Let G_1, G_2 be bilinear groups of prime order q. Additionally, let e: $G_1 \times G_1 \rightarrow G_2$ denote the bilinear map. The description of G_1 contains a generator $g \in G_1$. Then the algorithm picks a random $s \leftarrow Z_p^*$, sets $h = g^s$, and outputs a master key pairs (mpk = (g, h), msk = s).

(ii) KeyDer(msk, ID): the key derivation algorithm uses the master secret key to compute a secret key $\mathrm{sk}_{\mathrm{ID}} = g^{1/(s+\mathrm{ID})}$ for identity ID.

(iii) Encap(mpk, ID): the encapsulation algorithm picks a random $t \leftarrow Z_q$ and computes a random session key $K = e(g, g)^t$ using (mpk, ID). Moreover it uses (mpk, ID) to computes a ciphertext $C = (g^s g^{\mathrm{ID}})^t$ encrypted under the identity ID.

(iv) Decap(C, $\mathrm{sk}_{\mathrm{ID}}$) allows the possessor of $\mathrm{sk}_{\mathrm{ID}}$ to compute a session key K from a ciphertext C as follows: $K = e(C, \mathrm{sk}_{\mathrm{ID}})$.

The VRF (Gen, Func, and Ver) Construction Is as follows

(i) Gen(1^k) runs (mpk, msk) $\leftarrow$ Setup(1^k), chooses an arbitrary identity $\mathrm{ID}_0 \in$ ID, where ID is the identity space, and computes $C_0 \leftarrow$ Encap(mpk, ID_0). Then it sets vpk = (mpk, C_0) and vsk = msk.

(ii) $\mathrm{Func}_{\mathrm{vsk}}(x)$ computes $\pi_x = (\mathrm{sk}_x, \mathrm{aux}_x) =$ KeyDer(msk, x) and $y =$ Decap(C_0, π_x). It returns (y, π_x) where y is the output and π_x is the proof.

(iii) Ver(vpk, x, y, π_x) first checks if π_x is a valid proof for x by computing $(C, K) =$ Encap(mpk, x, aux_x) and checking if $K =$ Decap(C, π_x). Then it checks the validity of y by testing if Decap(C_0, π_x) = y. If both the tests are true, then the algorithm returns 1, otherwise it returns 0.

With a modification, we extend the VRF from a VRF-suitable IB-KEM [32] to multiparty case, and this can be used in our rational secret sharing schemes. Let $p_1, \ldots, p_n$ be n participants, $\mathrm{ID}_i \in$ ID ($i = 1, \ldots, n$) be the identity of p_i, where ID is the identity space, and d_i be the private key of p_i.

(i) Gen(1^k) takes a security parameter k, returns mpk_i, msk_i and computes $C_0^i \leftarrow$ Encap($\mathrm{mpk}_i, \mathrm{ID}_i$). Then it sets $\mathrm{vpk}_i = (\mathrm{mpk}_i, C_0^i)$ and $d_i = \mathrm{msk}_i$.

(ii) $\mathrm{Func}_{d_i}(x)$ computes $\pi_{d_i}(x) = (\mathrm{sk}_x^i, \mathrm{aux}_x^i) =$ KeyDer(msk_i, x) and $E_{d_i}(x) =$ Decap(C_i, π_x). It returns $(E_{d_i}(x), \pi_{d_i}(x))$ where the VRF output is $E_{d_i}(x)$ and $\pi_{d_i}(x)$ is the proof.

(iii) VER($\mathrm{vpk}_i, x, E_{d_i}(x), \pi_{d_i}(x)$) checks if $\pi_{d_i}(x)$ is a valid proof by computing $(C_i, K_i) =$ Encap($\mathrm{mpk}_i, x, \mathrm{aux}_x^i$) and checking if $K_i =$ Decap($C_i, \pi_{d_i}(x)$). Then it checks the validity of y by testing if Decap(C_0^i, $\pi_{d_i}(x)$) = $E_{d_i}(x)$. If both the tests are true, then the algorithm returns 1, otherwise it returns 0.

2.4. The Model of Security

Init. The adversary declares the identity set $\varphi = (\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n)$ that he wants to be challenged.

Setup. The challenger runs the setup phase of the algorithm and tells the adversary the public parameter.

Phase 1. The adversary is allowed to issue queries for private keys for many identities χ_i, where $|\chi_i \cap \varphi| < t$.

Challenge. The adversary output a message x^*. The challenger flips a random coin b and obtains a session key K_b. If $b = 0$,

then K_b is a correct form, otherwise K_b is random. Finally, it sends K_b to the adversary.

Phase 2. This goes exactly as phase 1.

Guess. The adversary outputs a guess b' of b. The adversary wins if $b' = b$.

We define the advantage of an adversary in this game as $\Pr[b' = b] - 1/2$.

3. The Rational Secret Sharing Scheme

3.1. System Parameters. Let $p_1, \ldots, p_n$ be n participants and l be the secret. Assume $\mathrm{ID}_i \in \mathrm{ID}$ $(i = 1, \ldots, n)$ is the identity of p_i, where $\mathrm{ID} \in Z_p^*$ is the identity space and $h : \{0,1\}^* \to Z_p^*$ is a collision resistance hash function. Let d_i be the private key of p_i.

3.2. Protocol for Sharing Phase

Step 1. The dealer chooses an integer $r^{\mathrm{real}} \in Z_p^*$ according to a geometric distribution with parameter λ. We discuss how to set λ below. The dealer computes $\mathrm{Gen}(1^k)$ and obtains d_i.

Step 2. Choose a prime p and construct two $(n-1)$ degree polynomials. One is $W(x)$ with the knowledge of n pairs of $(\mathrm{ID}_1 \parallel r^{\mathrm{real}}, E_{d_1}(r^{\mathrm{real}})), \ldots, (\mathrm{ID}_n \parallel r^{\mathrm{real}}, E_{d_n}(r^{\mathrm{real}}))$ as (4). The other is $W'(x)$ with the knowledge of n pairs of $(\mathrm{ID}_1 \parallel (r^{\mathrm{real}} + 1), E_{d_1}(r^{\mathrm{real}} + 1)), \ldots, (\mathrm{ID}_n \parallel (r^{\mathrm{real}} + 1), E_{d_n}(r^{\mathrm{real}} + 1))$ as (5):

$$W(x) = \sum_{i=1}^{n} E_{d_i}\left(r^{\mathrm{real}}\right) \cdot \prod_{j=1, j\neq i}^{n} \frac{x - h\left(\mathrm{ID}_j \parallel r^{\mathrm{real}}\right)}{h\left(\mathrm{ID}_i \parallel r^{\mathrm{real}}\right) - h\left(\mathrm{ID}_j \parallel r^{\mathrm{real}}\right)} \bmod p, \tag{4}$$

$$W'(x) = \sum_{i=1}^{n} E_{d_i}\left(r^{\mathrm{real}} + 1\right) \cdot \prod_{j=1, j\neq i}^{n} \frac{x - h\left(\mathrm{ID}_j \parallel \left(r^{\mathrm{real}} + 1\right)\right)}{h\left(\mathrm{ID}_i \parallel \left(r^{\mathrm{real}} + 1\right)\right) - h\left(\mathrm{ID}_j \parallel \left(r^{\mathrm{real}} + 1\right)\right)} \bmod p \tag{5}$$

$$= a_0^{r^{\mathrm{real}}+1} + a_1^{r^{\mathrm{real}}+1} x + a_2^{r^{\mathrm{real}}+1} x^2 + \cdots + a_{n-1}^{r^{\mathrm{real}}+1} x^{n-1},$$

$$\text{let } M^{r^{\mathrm{real}}} = W(0), \tag{6}$$

$$\text{value} = l \oplus M^{r^{\mathrm{real}}}. \tag{7}$$

Step 3. The dealer chooses the $n - t$ minimum integers $m_1, \ldots, m_{n-t}$ from $[p, q-1] - (\mathrm{ID}_i \parallel r)$ for $r = 1, 2, \ldots, r^{\mathrm{real}}$ and computes $W(m_k)$ and $W'(m_k)$ for $k = 1, 2, \ldots, n - t$.

Step 4. The dealer publishes the values $((m_k, W(m_k)), (m_k, W'(m_k)))$ for $k = 1, 2, \ldots, n - t$, value and $h(a_j^{r^{\mathrm{real}}+1})$ for $j = 0, 1, \ldots, n-1)$, and sends d_i to p_i.

3.3. Protocols for Reconstruction Phase. Let $T = \{p_{a_1}, p_{a_2}, \ldots, p_{a_t}\}$ be the set of the t active participants and $(E_{d_{a_i}}(r), \pi_{d_{a_i}}(r))$ be the share of p_{a_i} $(1 \le i \le t)$. In each iteration $(r = 0, 1, \ldots)$ the players execute the following steps.

Step 1. When $r \equiv i (\mathrm{mod}\, t)$, each of the t active participants sends her share in the order $p_{a_{i+1}}, p_{a_{i+2}}, \ldots, p_{a_t}, p_{a_1}, p_{a_2}, \ldots, p_{a_i}$ for $0 \le i \le t-1$.

Step 2. $p_{a_j} \in T$ receives the share from $p_{a_i} \in T$. If $\mathrm{VER}(\mathrm{vpk}_i, r, E_{d_{a_i}}(r), \pi_{d_{a_i}}(r)) = 0$, $\pi_{d_{a_i}}(r)$ is an invalid proof of $E_{d_{a_i}}(r)$, then, with the knowledge of t pairs of $(\mathrm{ID}_{a_1} \parallel (r-1), E_{d_{a_1}}(r-1)), \ldots, (\mathrm{ID}_{a_t} \parallel (r-1), E_{d_{a_t}}(r-1))$ and $n - t$ pairs of $(m_1, W(m_1)), \ldots, (m_{n-t}, W(m_{n-t}))$, the $(n-1)$ degree polynomial $B(x)$ can be uniquely determined as follows:

$$B(x) = \sum_{i=1}^{t} E_{d_{a_i}}(r-1) \cdot \prod_{j=1, j\neq i}^{t} \frac{x - h\left(\mathrm{ID}_{a_j} \parallel (r-1)\right)}{h\left(\mathrm{ID}_{a_i} \parallel (r-1)\right) - h\left(\mathrm{ID}_{a_j} \parallel (r-1)\right)} \cdot \prod_{j=1}^{n-t} \frac{x - m_i}{h\left(\mathrm{ID}_{a_i} \parallel (r-1)\right) - m_i} + \sum_{i=1}^{n-t} W(m_i) \cdot \prod_{j=1, j\neq i}^{n-t} \frac{x - m_j}{m_i - m_j} \prod_{j=1}^{t} \frac{x - h\left(\mathrm{ID}_{a_j} \parallel (r-1)\right)}{m_i - h\left(\mathrm{ID}_{a_j} \parallel (r-1)\right)} \bmod p. \tag{8}$$

We let $M^{r-1} = B(0)$. The secret can be obtained as $l' = \text{value} \oplus M^{r-1}$ and then output l' and terminate the protocols. If $\mathrm{VER}(\mathrm{vpk}_i, r, E_{d_{a_i}}(r), \pi_{d_{a_i}}(r)) = 1$, $\pi_{d_{a_i}}(r)$ is a valid proof of $E_{d_{a_i}}(r)$, then the protocol continues.

Step 3. With the knowledge of t pairs of $((\mathrm{ID}_{a_1} \parallel r), E_{d_{a_1}}(r)), \ldots, ((\mathrm{ID}_{a_t} \parallel r), E_{d_{a_t}}(r))$ and $n - t$ pairs of $(m_1, W'(m_1)), \ldots, (m_{n-t}, W'(m_{n-t}))$, the $(n-1)$ degree polynomial $B'(x)$ can be uniquely determined as follows:

$$B'(x) = \sum_{i=1}^{t} E_{d_{a_i}}(r) \prod_{j=1, j\neq i}^{t} \frac{x - h\left(\mathrm{ID}_{a_j} \parallel r\right)}{h\left(\mathrm{ID}_{a_i} \parallel r\right) - h\left(\mathrm{ID}_{a_j} \parallel r\right)} \cdot \prod_{j=1}^{n-t} \frac{x - m_i}{h\left(\mathrm{ID}_{a_i} \parallel r\right) - m_i} + \sum_{i=1}^{n-t} W'(m_i) \cdot \prod_{j=1, j\neq i}^{n-t} \frac{x - m_j}{m_i - m_j} \prod_{j=1}^{t} \frac{x - h\left(\mathrm{ID}_{a_j} \parallel r\right)}{d_{a_i} - h\left(\mathrm{ID}_{a_j} \parallel r\right)} \bmod p = b_0^r + b_1^r x + b_2^r x^2 + \cdots + b_{n-1}^r x^{n-1}. \tag{9}$$

Step 4. If $h(b_j^r) \neq h(a_j^{r^{\mathrm{real}}+1})$ for $j = 0, 1, \ldots, n-1$ then the protocol goes to next iteration, else if $h(b_j^r) = h(a_j^{r^{\mathrm{real}}+1})$, then $r = r^{\mathrm{real}} + 1$, with the knowledge of t pairs of $((\mathrm{ID}_{a_1} \parallel r^{\mathrm{real}}), E_{d_{a_1}}(r^{\mathrm{real}})), \ldots, ((\mathrm{ID}_{a_t} \parallel r^{\mathrm{real}}), E_{d_{a_t}}(r^{\mathrm{real}}))$ and $n - t$

pairs of $(m_1, W(m_1)), \ldots, (m_{n-t}, W(m_{n-t}))$, the $(n-1)$ degree polynomial $B^{\text{real}}(x)$ can be uniquely determined as follows:

$$\begin{aligned} B^{\text{real}}(x) = & \sum_{i=1}^{t} E_{d_{a_i}}\left(r^{\text{real}}\right) \\ & \cdot \prod_{j=1, j\neq i}^{t} \frac{x - h\left(\text{ID}_{a_j} \parallel r^{\text{real}}\right)}{h\left(\text{ID}_{a_i} \parallel r^{\text{real}}\right) - h\left(\text{ID}_{a_j} \parallel r^{\text{real}}\right)} \\ & \cdot \prod_{j=1}^{n-t} \frac{x - m_i}{h\left(\text{ID}_{a_i} \parallel r^{\text{real}}\right) - m_i} + \sum_{i=1}^{n-t} W(m_i) \\ & \cdot \prod_{j=1, j\neq i}^{n-t} \frac{x - m_j}{m_i - m_j} \prod_{j=1}^{t} \frac{x - h\left(\text{ID}_{a_j} \parallel r^{\text{real}}\right)}{d_{a_i} - h\left(\text{ID}_{a_j} \parallel r^{\text{real}}\right)} \bmod p. \end{aligned} \tag{10}$$

Let $M^{r^{\text{real}}} = B^{\text{real}}(0)$. The secret can be obtained as $l = \text{value} \oplus M^{r^{\text{real}}}$. Then output l and terminate the protocols.

4. Proof of Security

In this section, the poof of the security is discussed.

Theorem 4. *If an adversary can break our scheme, then one can build a simulator to solve the q-DBDHI assumption with a nonnegligible advantage.*

Proof. We assume there exists an adversary A that has nonnegligible advantage $\varepsilon(k)$ into breaking the protocol. Then we can build a simulator B which is able to break the q-DBDHI assumption with nonnegligible advantage.

Input to the Reduction. Algorithm B receives a tuple $(g, g^{\alpha}, \ldots, g^{(\alpha^q)}, \Gamma) \in G_1^{q+1} \times G_2$, and output 1 if $\Gamma = e(g, g)^{1/\alpha}$, or 0 otherwise.

Key Generation. Assume that A tries to guess the challenge message $x_0 \in Z_p^*$. Let $s = \alpha - x_0$. Using the binomial theorem, it computes $(g, g^s, \ldots, g^{(s^q)})$. Then B define $f(z) = \prod_{w\neq x_0}^{w\in z_q}(z + w) = \sum_{i=0}^{q-1} c_i z^i$ and compute the new base $g' = g^{f(s)} = \prod_{i=0}^{q-1} g^{s^i c_i}$. Finally it computes $h = (g')^s = \prod_{i=1}^{q-1} g^{s^i c_{i-1}}$, picks a random t, and sets $C_0 = (g')^t$. Then it gives g', h, C_0 as the public key to A.

Phase 1. The adversary A is allowed to issue queries for private keys for many identities χ_i, where $|\chi_i \cap \varphi| < t$ and $\varphi = (\text{ID}_1, \text{ID}_2, \ldots, \text{ID}_n)$. Consider the ith query $(1 \le i < q)$ on message x_i. If $x_i = x_0$, then B fails. Otherwise B can compute the secret key as follows. Firstly it defines $f_i(z) = f(z)/(z + x_i) = \sum_{i=0}^{q-2} z^i \nu_i$. Then it computes $\text{sk}_{x_i} = (g')^{1/(s+x_i)} = g^{f_i(s)} = \sum_{i=0}^{q-2} g^{s^i \nu_i}$ and returns it to A as the private key of χ_i. With the knowledge of t pairs of $((\text{ID}_{a_1} \parallel r), E_{d_{a_1}}(r)), \ldots, ((\text{ID}_{a_t} \parallel r), E_{d_{a_t}}(r))$ and $n - t$ pairs of $(m_1, W'(m_1)), \ldots, (m_{n-t}, W'(m_{n-t}))$, the simulator can construct the $(n-1)$ degree polynomial $B'(x)$ by using the Lagrange interpolation polynomial. However, the coefficient of the $B'(x)$ is identical to that of the original scheme.

Challenge. The adversary A output a message x^*. If $x^* \neq x_0$, then B fails. Otherwise, the challenger can compute a session key K_b in the following way. Let $f'(z) = f(z)/(z + x_0) - \gamma/(z + x_0) = \sum_{i=0}^{q-2} z^i \gamma_i$ and compute $Z_0 = (\prod_{i=0}^{q-1}\prod_{j=0}^{q-2} e(g^{s^i}, g^{s^j}))(\prod_{m=0}^{q-2} e(g, g^{s^m})^{\gamma\gamma_m}) = e(g, g)^{(f(s)-\gamma^2)/\alpha}$. The simulator flips a random coin, b, and sets a session key $K_b = (Z^{\gamma^2} \cdot Z_0)^t$, if $b = 0$, then $Z = e(g, g)^{1/\alpha}$ and $K_b = e(g', g')^{t/(s+x_i)}$ is a correct form. Otherwise Z is a random, and so is K_b. Finally, it sends K_b to the adversary.

Phase 2. This goes exactly as phase 1.

Guess. The adversary A outputs a guess b' of b. B returns b' as its guess as well.

For the sake of contradiction, suppose there exists a probabilistic polynomial time attacker A can break the protocol with probability $1/2 + \varepsilon(k)$. Then we can build a simulator B which is able to break the q-DBDHI assumption with probability $1/2 + \varepsilon(k)$. (The output of B is the same as the output of A.) Because the q-DBDHI assumption is hard to be solved, there is no any adversary A that has nonnegligible advantage $\varepsilon(k)$ into breaking the protocol. This completes the proof. □

Theorem 5. *The above rational secret sharing scheme is computational C-immune, and rational participant has an incentive to abide by the protocol.*

Proof. Given the $n - t$ public values $W(m_k), W'(m_k)$, the two $(n-1)$ degree polynomials $W(x), W'(x)$ cannot be constructed by anyone. So, an adversary can learn nothing about the secret. Any $t - 1$ or fewer participants cannot obtain the secret too. In the scheme, any rational participant can detect and determine who is cheating. Suppose that $p_{a_j} \in T$ receives the share from $p_{a_i} \in T$. If $\text{VER}(\text{vpk}_i, r, E_{d_{a_i}}(r), \pi_{d_{a_i}}(r)) = 0$, $\pi_{d_{a_i}}(r)$ is an invalid proof of $E_{d_{a_i}}(r)$, and p_{a_j} terminates the protocols. If $\text{VER}(\text{vpk}_i, r, E_{d_{a_i}}(r), \pi_{d_{a_i}}(r)) = 1$, $\pi_{d_{a_i}}(r)$ is a valid proof of $E_{d_{a_i}}(r)$, and p_{a_j} continues the protocols. Assume that P_i who is the member of the collusion C does not know which round is r^{real}. He can only guess the secret and get U_i^+ with probability β, if the collusion C does not participate in the scheme. On the contrary, he can guess a wrong secret and get U_i^- with probability $1 - \beta$. So, when the collusion C does not participate in the protocols, the expected utility of P_i is as in

$$E\left(U_i^{\text{guess}}\right) = \beta * U_i^+ + (1 - \beta) * U_i^-. \tag{11}$$

The participant P_i will get utility U_i^+, if the collusion C participates in the protocols and aborts in real round with probability λ. Otherwise, the participant P_i's utility is $E(U_i^{\text{guess}})$. Therefore, when the collusion C deviates, the expected utility of P_i is at most

$$\lambda * U_i^+ + (1 - \lambda) * E\left(U_i^{\text{guess}}\right). \tag{12}$$

When the collusion C abides by the protocol, the utility of the participant P_i is U_i. So, rational collusion C has an inventive not to deviate from the protocol if the protocol satisfies

$$U_i > \lambda * U_i^+ + (1-\lambda) * E\left(U_i^{\text{guess}}\right). \tag{13}$$

We denote λ' the probability that players in C can only have a negligible advantage over λ. There exists a negligible function $\xi(k)$ such that for every k it holds that

$$\lambda' \leq \lambda + \xi(k). \tag{14}$$

We let $U^{*'}$ denote the utility when allowing for the computationally secure. Then

$$\begin{aligned} U^{*'} &= \lambda' U_i^+ + \left(1-\lambda'\right) * E\left(U_i^{\text{guess}}\right) \\ &= \lambda'\left(U_i^+ - E\left(U_i^{\text{guess}}\right)\right) + E\left(U_i^{\text{guess}}\right) \\ &\leq (\lambda + \xi(k))\left(U_i^+ - E\left(U_i^{\text{guess}}\right)\right) + E\left(U_i^{\text{guess}}\right) \\ &\leq \lambda * U_i^+ + (1-\lambda) * E\left(U_i^{\text{guess}}\right) \\ &\quad + \xi(k)\left(U_i^+ - E\left(U_i^{\text{guess}}\right)\right) < U_i + \varepsilon(k). \end{aligned} \tag{15}$$

That is for every iteration and for all $C \subset [n]$ with $|C| \leq t-1$, all $i \in C$, and any $a'_C \in \Delta(A_C)$, no information about the secret is revealed. So, the scheme is computational C-immune and rational player has an incentive to abide by the protocol. □

5. Comparison

We compare the efficiency and security with previous rational secret sharing scheme as follows.

The work of Halpern and Teague [10] assumes the existence of simultaneous broadcast channels (SBC). Their schemes fail to resist against coalitions and have expected round complexity $O(5/\alpha^3)$. The works in [11–13] rely on secure multiparty computation which are inefficient. The works of Kol and Naor [14] have shown how to avoid simultaneous broadcast, at the cost of increasing the round complexity. In addition, the scheme is not collusion-free, and the round complexity is $O(n/\beta)$ and the works in [15, 16] require the involvement of some trusted external parties during the reconstruction phase which is difficult to find. The round complexity of Maleka et al. [17] is $O(n^2)$. The works of Izmalkov et al. [18] and Lepinski et al. [19, 20] rely on a physical assumption such as secure envelopes and ballot boxes. The works in [10–14, 17, 21–25] assume the existence of broadcast channel which is not realistic. The works in [11–13, 19–27] need handshake protocol and exchange public keys associated with certificate management, including distribution, storage, revocation, and the computational cost of certificate verification, which are relatively expensive and limit their practical application to mobile networks. In contrast with prior schemes, the round complexity is $O(1/\lambda)$ (the value of α, β, and λ is roughly the same) in our scheme, and we do not assume multiparty computations, physical assumption, or trust party, which is more practical; the scheme provides a noninteractively verifiable proof for the correctness of participants' share and handshake protocol is not necessary; there is no need for certificate generation, propagation, and storage in the scheme, which is more suitable for devices with limited size and processing power; the public key in our approach is based on each participant's identity which can be very much shorter as compared to the 1024 bits public key in RSA cryptosystem; in the scheme, every participant uses her encryption on number of each round as the secret share and the dealer does not have to distribute any secret share, which reduce the computational consumption and communicational overhead; the scheme can withstand the conspiracy attack and no player of the coalition C can do better, even if the whole coalition C cheats.

6. Conclusions

We propose a rational secret sharing scheme in mobile networks. The scheme, without needing to resort to broadcast channel, eliminates the online certificate authority and simplifies key management, which is more practical for devices of limited size and processing power, such as mobile phones. In addition, the scheme assumes neither the availability of a trusted party nor multiparty computations in the reconstruction phase. Moreover, the scheme can withstand the conspiracy attack and no player of the coalition C can do better, even if the whole coalition C cheats. So, rational players have no incentive to cheat in the scheme, and, finally, every player can obtain the secret fairly in mobile networks.

Conflict of Interests

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

Acknowledgments

The authors would like to thank the anonymous referees for their suggestions. This work was supported by the National Natural Science Foundation of China (nos. 61170221, 11471104, U1204606, U1404601, and U1404602) and the Key Project of Education Department of Henan Province (no. 14A520032).

References

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

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

[3] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai, and A.-Y. Tseng, "Block-based progressive visual secret sharing," *Information Sciences*, vol. 233, no. 4, pp. 290–304, 2013.

[4] J. Herranz, A. Ruiz, and G. Sáez, "New results and applications for multi-secret sharing schemes," *Designs, Codes, and Cryptography*, vol. 73, no. 3, pp. 841–864, 2014.

[5] J. Shao, "Efficient verifiable multi-secret sharing scheme based on hash function," *Information Sciences*, vol. 278, pp. 104–109, 2014.

[6] M. Fatemi, R. Ghasemi, and T. Eghlidos, "Efficient multistage secret sharing scheme using bilinear map," *IET Information Security*, vol. 8, no. 4, pp. 224–229, 2014.

[7] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pp. 383–395, IEEE Computer Society, Portland, Ore, USA, October 1985.

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

[9] T. P. Pedersen, "Distributed provers with applications to undeniable signatures," in *Advances in Cryptology—EUROCRYPT '91*, vol. 547 of *Lecture Notes in Computer Science*, pp. 221–242, Springer, Berlin, Germany, 1991.

[10] 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*, pp. 623–632, ACM Press, New York, NY, USA, June 2004.

[11] 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.

[12] E. Zhang and Y. Q. Cai, "A new rational secret sharing scheme," *China Communications*, vol. 7, no. 40, pp. 18–22, 2010.

[13] G. Kol and M. Naor, "Cryptography and game theory: designing protocols for exchanging information," in *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19–21, 2008. Proceedings*, vol. 4948 of *Lecture Notes in Computer Science*, pp. 320–339, Springer, Berlin, Germany, 2008.

[14] G. Kol and M. Naor, "Games for exchanging information," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 423–432, ACM Press, May 2008.

[15] S. Izmalkov, M. Lepinski, and S. Micali, "Verifiably secure devices," in *Theory of Cryptography: Proceedings of the 5th Theory of Cryptography Conference, TCC 2008, New York, USA, March 19–21, 2008*, vol. 4948 of *Lecture Notes in Computer Science*, pp. 273–301, Springer, Berlin, Germany, 2008.

[16] S. Micali and A. Shelat, "Purely rational secret sharing (extended abstract)," in *Theory of Cryptography: 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15–17, 2009. Proceedings*, vol. 5444, pp. 54–71, Springer, Berlin, Germany, 2009.

[17] 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, Miami, Fla, USA, April 2008.

[18] S. Izmalkov, M. Lepinski, and S. Micali, "Rational secure computation and ideal mechanism design," in *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05)*, pp. 623–632, IEEE Press, New York, NY, USA, October 2005.

[19] M. Lepinski, S. Micali, and A. Shelat, "Collusion-free protocols," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC '05)*, pp. 543–552, ACM, Baltimore, Md, USA, May 2005.

[20] M. Lepinski, S. Micali, C. Peikert, and A. Shelat, "Completely fair SFE and coalition-safe cheap talk," in *Proceedings of the 23rd ACM Symposium on Principles of Distributed Computing (PODC '04)*, pp. 1–10, July 2004.

[21] T. Isshiki, K. Wada, and K. Tanaka, "A rational secret-sharing scheme based on RSA-OAEP," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 93, no. 1, pp. 42–49, 2010.

[22] Z. Zhang and M. Liu, "Rational secret sharing as extensive games," *Science China Information Sciences*, vol. 56, no. 3, pp. 1–13, 2013.

[23] E. Zhang and Y. Q. Cai, "Collusion-free rational secure sum protocol," *Chinese Journal of Electronics*, vol. 22, no. 3, pp. 563–566, 2013.

[24] Y. Yang and Z. F. Zhou, "An efficient rational secret sharing protocol resisting against malicious adversaries over synchronous channels," in *Information Security and Cryptology*, vol. 7763 of *Lecture Notes in Computer Science*, pp. 69–89, Springer, Berlin, Germany, 2013.

[25] Y. Tian, J. Ma, C. Peng, and Q. Jiang, "Fair (t, n) threshold secret sharing scheme," *IET Information Security*, vol. 7, no. 2, pp. 106–112, 2013.

[26] G. Fuchsbauer, J. Katz, and D. Naccache, "Efficient rational secret sharing in standard communication networks," in *Theory of Cryptography: 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9–11, 2010. Proceedings*, vol. 5978 of *Lecture Notes in Computer Science*, pp. 419–436, Springer, Berlin, Germany, 2010.

[27] E. Zhang and Y. Q. Cai, "Rational multi-secret sharing scheme in standard point-to-point communication networks," *International Journal of Foundations of Computer Science*, vol. 24, no. 6, pp. 879–897, 2013.

[28] J. Katz, "Bridging game theory and cryptography: recent results and future directions," in *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19–21, 2008. Proceedings*, vol. 4948 of *Lecture Notes in Computer Science*, pp. 251–272, Springer, Berlin, Germany, 2008.

[29] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, pp. 120–130, IEEE Press, New York, NY, USA, 1999.

[30] Y. Dodis, "Efficient construction of (distributed) verifiable random functions," in *Public Key Cryptography—PKC 2003*, Y. G. Desmedt, Ed., vol. 2567 of *Lecture Notes in Computer Science*, pp. 1–17, Springer, Berlin, Germany, 2002.

[31] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proof and keys," in *Public Key Cryptography—PKC 2005*, vol. 3386 of *Lecture Notes in Computer Science*, pp. 416–431, Springer, Berlin, Germany, 2005.

[32] M. Abdalla, D. Catalano, and D. Fiore, "Verifiable random functions from identity-based key encapsulation," in *Advances in Cryptology—EUROCRYPT 2009*, vol. 5479 of *Lecture Notes in Computer Science*, pp. 554–571, Springer, Berlin, Germany, 2009.

[33] R. Sakai and M. Kasahara, "ID based cryptosystems with pairing on elliptic curve," in *Proceedings of the Symposium on Cryptography and Information Security*, Report 2003/054, Cryptology ePrint Archive, 2003.