Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 637458, 8 pages
http://dx.doi.org/10.1155/2015/637458

Research Article

Fair Secure Computation with Reputation Assumptions in the Mobile Social Networks

Yilei Wang,[1,2] Chuan Zhao,[1] Qiuliang Xu,[1] Zhihua Zheng,[3] Zhenhua Chen,[4] and Zhe Liu[5]

[1]*School of Computer Science and Technology, Shandong University, Jinan 250101, China*
[2]*School of Information and Electrical Engineering, Ludong University, Yantai 264025, China*
[3]*School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China*
[4]*School of Computer Science, Shaanxi Normal University, Xi'an 710062, China*
[5]*Laboratory of Algorithmics, Cryptology and Security (LACS), 1359 Luxembourg, Luxembourg*

Correspondence should be addressed to Qiuliang Xu; xql@sdu.edu.cn

Received 29 August 2014; Accepted 1 September 2014

Academic Editor: David Taniar

With the rapid development of mobile devices and wireless technologies, mobile social networks become increasingly available. People can implement many applications on the basis of mobile social networks. Secure computation, like exchanging information and file sharing, is one of such applications. Fairness in secure computation, which means that either all parties implement the application or none of them does, is deemed as an impossible task in traditional secure computation without mobile social networks. Here we regard the applications in mobile social networks as specific functions and stress on the achievement of fairness on these functions within mobile social networks in the presence of two rational parties. Rational parties value their utilities when they participate in secure computation protocol in mobile social networks. Therefore, we introduce reputation derived from mobile social networks into the utility definition such that rational parties have incentives to implement the applications for a higher utility. To the best of our knowledge, the protocol is the first fair secure computation in mobile social networks. Furthermore, it finishes within constant rounds and allows both parties to know the terminal round.

1. Introduction

Mobile computing and telecommunications are areas of rapid growth. A mobile social network connects individuals or organizations using off-the-shelf, sensor-enabled mobile phones with sharing of information through social networking applications such as Facebook, MySpace, and scientific collaboration networks [1]. A mobile social network plays an important role as the spread of information and influence in the form of "word of mouth" [2]. The advantages of wireless communications are that they can provide many new services that will revolutionize the way that society handles information [3]. The most significant property for mobile users in the mobile social network lies in the fact that they have reputation when they interact in the network [4–6], which can be utilized to boost cooperation in secure two-party computation. Secure two-party computation [7] means that two distributed parties wish to correctly compute some functionality using their private inputs while disclosing nothing except for the output. The computation should suffice three basic requirements: (i) privacy: nothing is learned from the protocol other than the output, (ii) correctness: the output is distributed according to the prescribed functionality, and (iii) independence: parties cannot make their inputs depending on other parties' inputs. Another requirement is fairness which means that either all parties learn the results or none of them does. Plenty of researchers delve into implementing fairness among parties. Unfortunately, Cleve [8] shows that fairness cannot be achieved in two-party settings. So, the accepted folklore is that nothing nontrivial can be computed with fairness. The usual treatment of secure two-party computation [9] wakens the ideal world to the one where fairness is not guaranteed at all.

In the setting of two-party games under incomplete information, two selfish parties wish to maximize their utilities with their private information. Each party has

a set of strategies and certain private information-like types. Both parties take their strategies simultaneously or alternately in each round (maybe just in one shot) and the last round leads to an outcome which assigns each party a utility. Cryptography and game theory are both concerned with understanding interactions among mutually distrusted parties with conflicting interests. Cryptographic protocols are designed to protect the private inputs of each party against arbitrary behaviors, while game theory protocols are designed to reach various Nash equilibria against rational deviations.

1.1. Related Works. Research shows great increases in communications through mobile phone call, text messages, and the spatial reach of social networks [10–12]. People frequently have ties at a distance and they socialize with these ties through mobile phones and so forth. Larsen et al. [13] consider how mobile phones are used to coordinate face-to-face meetings between distanced friends and family members. Wang et al. [14] deal with the problem of influence maximization in a mobile social network where users in the network communicate through mobile phones. A mobile social network can be extracted from call logs and is modeled as a weighted directed graph. A mobile phone user corresponds to a node. The weight of one node is its reputation and is established when it interacts with other nodes in the network. Miluzzo et al. [15] discuss the design, implementation, and evaluation of the cenceme application on the basis of mobile social networks. González et al. [16] represent a model of mobile agents to construct social networks on the basis of a system of moving particles by keeping track of the collisions during their permanence in the system. Beach et al. [17] discuss the security and privacy issues in mobile social network when users in the network share their IDs or handles.

On the other hand, users in mobile social networks are assumed as rational parties who care about their utilities as those in game theory. Wang et al. [18] propose social rational secure multiparty computation protocol when rational parties belong to a social network. Rational parties, introduced by Halpern and Teague [19], behave neither like honest parties who always follow the protocol nor like malicious parties who arbitrarily violate the protocol. Rational parties only adopt the strategies which maximize their utilities. Halpern and Teague [19] prove the impossible result with rational parties and then give a random solution for rational multiparty computation. However, given at least three malicious parties, their protocol cannot achieve fairness at all.

1.2. Motivations and Contributions. Rational parties in secure computations are expected to cooperate with each other. However, they have no incentives to cooperate according to traditional utility definition. Therefore new utility definition must be considered assigning incentives to rational parties. With the motivation that reputation derived from mobile social networks can boost cooperation among users, we consider rational secure computation in mobile social works such that rational parties can utilize the reputation in the networks. In particular, users in the mobile social networks are willing to cooperate with those who have good reputation of cooperation. Furthermore, the good reputation can be transmitted among friends in the networks. For example, if Alice cooperated with Bob once, then Bob's friends are willing to cooperate with Alice or Bob will cooperate with Alice when they meet again. Therefore, reputation is a useful tool to encourage mutual cooperation.

In this paper, we only consider two rational parties to securely compute a function. The parties come from a mobile social network, where they both have reputation value and use Tit-for-Tat (TFT) strategies to boost cooperation. Note that reputation affects the way parties achieve their utilities. The rational computation protocol in the presence of such rational parties is divided into several iterations. At the end of each iteration both parties gain some utilities and update their reputations. This process is similar to repeated games with stage games. Maleka et al. [20] first introduce repeated games into secret sharing scheme and get positive/negative results in infinitely/finitely repeated games. They discuss repeated games under complete information scenarios and conclude that parties cannot reconstruct secret when they know the terminal iteration. In this paper, we introduce the TFT strategy, reputation assumption, and incomplete information in order to facilitate mutual cooperation between both parties. Thus, it is possible for parties to achieve fairness in constant rounds.

Our settings are approximately similar to those of Groce and Katz [21] with the exception of the TFT strategy [22], the reputation assumption, and incomplete information scenarios. The main contributions of this paper are the introduction of the TFT strategy and reputation assumptions.

(i) The main target of rational two-party computation in the mobile social networks is how to facilitate cooperation among parties in order to complete the protocol (like the prisoners' dilemma game). In game theory scenario (especially in repeated games), TFT is an efficient strategy to promote cooperation. In fact, this seemingly simple and quite natural strategy defeats other strategies in Axelrod's prisoners' dilemma tournament [23]. The main intuition of the TFT strategy is that parties implement cooperation at the first round to make an attempt to elicit mutual cooperation from their opponents and copy the opponent's last action in the next round. In other words, a TFT party (who adopts the TFT strategy) cooperates with parties who cooperate and finks with parties who fink. Nowak and Sigmund [24] design experiments based on Axelrod's tournament to simulate the role of reciprocity in societies. In rational secure two-party computation, parties participate in the computation using the TFT strategy.

(ii) In previous works, parties in rational multiparty computation have no private types. Namely, the fact that parties are rational is common knowledge (common knowledge about an event between two parties means that one party knows the event and he knows the

other party knows the event too, and vice versa [25]) and parties run the protocol under complete information scenario. Consequently, parties execute the protocol according to the Nash equilibrium. However, feasibility condition is that parties may have their own private type. For example, some people are kind, some others are vicious, and still others may be revengeful. Everybody knows exactly his own type and only has a priori probability on the private type of other parties. We call this incomplete information scenario.

Under this scenario, parties adopt their strategies consulting the preceding actions when executing the protocol. The preceding actions form a reputation for a certain type. For example, in the mobile social networks people who often help others have a good reputation, while people who often deceive others have a bad reputation.

In rational computation under incomplete information scenario, parties need to build a good reputation if they want to obtain the computation results. On the other hand, parties should show their private type to others through their actions. Otherwise, other parties may always adopt their dominating strategies which may lead to lower utilities.

(iii) Traditional utility assumptions in rational multiparty computation include two sides: (i) *correctness*, parties wish to compute the functionality correctly and (ii) *exclusivity*, parties wish that other parties do not obtain the correct result. Following the results of [19], parties have no incentives to participate in the protocol, not to mention how to realize fairness among them. Therefore, new assumptions should be introduced such that parties are willing to participate in the protocol. Other than the above utility assumptions, we introduce a new reputation assumption when parties come from a mobile social network. Namely, parties value and form their reputation in the network. We note that parties with a good reputation can inspire other parties to cooperate with them and boost their ultimate utilities. Reputation exists in many business-related, financial, political, and diplomatic settings and a good reputation is of great concern. Sometimes, companies, institutions, and individuals involved cannot afford the embarrassment, loss of reputation.

(iv) In this paper, there are two private types of parties: rational parties who always adopt their dominating strategies and TFTer parties who follow the TFT strategies. Each party knows his own private type and has a prior probability γ on the type of the other party. We stress that the prior probability (corresponding to their reputation) is not static, and it is updated after each round of the protocol.

Loosely speaking, we assume that there are two parties (each has his private type), say P_0 and P_1, wishing to jointly compute a function f with their private inputs x_0 and x_1, where the distributions of them are common knowledge. Following [26–28], our protocol consists of two stages, where the first stage is regarded as a "preprocessing" stage and the second stage includes several iterations.

1.3. Paper Outline. Section 2 presents some preliminaries in our protocol, such as the TFT strategy, utility assumptions, and the reputation assumption. Section 3 presents the description of our protocol in the ideal-real world paradigm. Then Section 4 proves how to construct a fair protocol with constant rounds. In the last section, we conclude this paper and anticipate some open problems.

2. Preliminaries

2.1. Utility Assumptions. We first introduce the concept of the *stage game*, a building block of repeated games and our protocol. Let $\Gamma(P, A, U)$ denote a stage game, where $P = \{P_b\}_{b\in\{0,1\}}$. In the following section, we denote by $-b$ the complementary of b. Furthermore, let $A = A_0 \times A_1$, where A_b includes the strategy *fink* (F) and *cooperate* (C). Let $U = \{u_b\}$ be the utility set of parties. Let $\mu_b(o)$ be the utility of P_b with the outcome o, and let $\delta_b(o)$ be an indicator denoting the notion whether P_b learns the output of the function, and let $\text{num}(o) = \sum_b \delta_b(o)$ denote the aggregated number of parties who learn the output of the function. According to [19], we make the utility function assumptions as follows.

(a) Correctness. If $\delta_b(o) > \delta_b(o')$, then $\mu_b(o) > \mu_b(o')$; that is, parties prefer to learn the output of the function.

(b) Exclusivity. If $\delta_b(o) = \delta_b(o')$ and $\text{num}(o) < \text{num}(o')$, then $\mu_b(o) > \mu_b(o')$; that is, P_b hopes the other party does not learn the output of the function.

For simplicity, we define the following outcomes:

(i) $u_b = a$ if P_b learns the output of the function, while P_{-b} does not;

(ii) $u_b = 1$ if both P_b and P_{-b} learn the output of the function;

(iii) $u_b = 0$ if neither P_b nor P_{-b} learns the output of the function;

(iv) $u_b = c$ if P_{-b} learns the output of the function, while P_b does not.

Here $a > 1$, $c < 0$, and $a + c < 2$ hold (if $a + c < 2$, the strategy where both parties take cooperation is Pareto-dominated by the strategy where both parties alternately take fink and cooperate); otherwise parties have no incentives to participate in the protocol (this is very much like the scenario of prisoner's dilemma game [23]).

In repeated games, parties interact in several periods and take actions simultaneously or nonsimultaneously in each stage game $(\Gamma_1, \Gamma_2, \ldots, \Gamma_T)$, where T is a finite number. The total utility of P_b in the repeated games is

$$U_b = \sum_{t=0}^{T} u_b. \tag{1}$$

Table 1: Reputation $R_i^j(t+1)$ updating rules.

$R_i^j(t)$	Cooperation by j	Fink by j
>0	$R_i^j(t) + \alpha(1 - R_i^j(t))$	$(R_i^j(t) + \beta)/(1 - \min\{\lvert R_i^j(t)\rvert, \lvert\beta\rvert\})$
<0	$(R_i^j(t) + \alpha)/(1 - \min\{\lvert R_i^j(t)\rvert, \lvert\alpha\rvert\})$	$R_i^j(t) + \beta(1 + R_i^j(t))$
=0	α	β

2.2. Reputation Assumption. Rational parties are allowed to have utilities, and then we might as well regard the rational parties as parts of a social network and endow them with an additional property like reputation. Reputation plays an important role when distrusted parties interact under incomplete information scenarios, where parties only have a prior probability on the types of other parties. The famous prisoner's dilemma game under incomplete information accounts for how reputation encourages reciprocal cooperation in multistage games. In this paper we use reputation effects for our purpose. Put differently, a rational party values his reputation, because a high reputation can attract other parties to cooperate with him and boost his total utilities. That is, reputation makes a difference to the utilities. Precisely for this reason, we introduce another assumption on utility that rational parties under incomplete information think highly of their reputations. The definition of reputation in this paper is in accordance with [29]. (Although there is an improvement in [30] on the definition of reputation, we still use the original definition in this paper. Since the reputation equals trust when there are only two parties, we do not distinguish these two notions in this paper.)

Definition 1. Let $R_i^j(t)$ denote the reputation of party P_j assigned by P_i in period t such that $R_i^j(t) \in (-1, 1)$ and $R_i^j(0) = 0$, where period 0 denotes the initial period of the protocol.

The reputation is not static. If there are no specific instructions, in the following sections, we denote by P_j the other parties except for P_i. Party P_i adjusts his reputation of the $(t+1)$th period according to P_j's action in the tth period (Definition 2). To prevent parties from maliciously finking, we set $|\alpha| < |\beta|$, where α is the positive evidence to reward the parties who cooperate and β is the negative evidence to punish the parties who fink. In other words, the reputation grows slowly when parties cooperate while it drops quickly once parties fink.

Definition 2. After the tth stage game, reputation $R_i^j(t+1)$ is updated according to the rules in Table 1.

Under incomplete information scenarios, each party has a private type. Here, we assume that parties have two types: rational parties maximizing their utilities and TFTer parties adopting the TFT strategy. It is obvious that the utility is higher when they both obtain the correct value than when they do not. Parties would be apt to cooperate with other parties with high reputation. The more frequently parties cooperate, the higher utilities they obtain. Thus parties have incentives to cooperate with others in order to maintain a higher reputation. Meanwhile, high reputation will in turn make it easier for the other party to cooperate. This forms a virtuous cycle. We simulate the reputation value of Definition 2 in Figure 1, where the horizontal axis denotes the total periods (50 times here) and T denotes the outset of the deviating period.

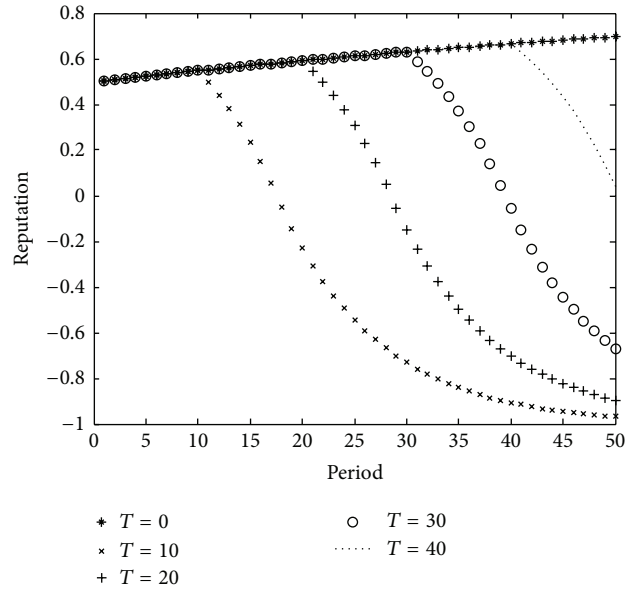

Figure 1: Reputation for each party when $\alpha = 0.01$ and $\beta = -0.1$.

We observe that the reputation will decrease once parties deviate, so parties have no incentives to deviate in each stage game if they want to preserve a higher reputation. Thus far, we give the third assumption if the protocol is considered to be a long-term process.

(c) Reputation. Each party has incentives to preserve a higher reputation for the sake of inducing reciprocally cooperation and the mutual cooperation consequently promotes parties' whole utilities in the long run.

In fact, the reputation assumption is a virtual part in the definition of utilities. Its main role is to warn other parties not to fink. Otherwise, the protocol will consequently enter into mutual fink. If so, all parties will not get the correct results and their utilities will decrease in the long run. Namely, although reputation does not intervene with the direct utilities in the current iteration, it actually affects the future utilities. In the future work, we will add reputation assumption as a real part into the definition of utilities.

3. Ideal-Real World Paradigm

3.1. Execution in the Ideal World. In the ideal world where a third trusted party (TTP) exists, it is trivial to achieve fairness. For completeness we represent the two-party (P_0, P_1) protocol in a natural way.

(1) Each party knows his private type and the other party only has a prior probability on the private type of his opponent.

(2) P_0 (*resp.*, P_1) randomly chooses his input value x_0 (*resp.*, x_1) according to a joint probability distribution D over input pairs.

(3) Each party P_b sends its value x_b' to the TTP. In the fail-stop setting, x_b' is restricted to a special symbol $\perp$ and x_b.

(4) If $x_b' = \perp$ then the TTP sends $\perp$ to both parties and the protocol ends. Otherwise, the TTP sends $f(x_0, x_1)$ to both parties.

(5) Each party outputs some values and the protocol ends.

At the end of the protocol, both parties either get utility 1 (when both parties follow the protocol) or get utility 0 (when at least one party sends $\perp$ to the TTP). Since utility function is common knowledge, both parties will follow the protocol in the fail-stop setting. We assume that $f(x_0, x_1)$ has full support, if for every x_0 and x_1 the distribution $f(x_0, x_1)$ puts nonzero probability on one unique element in the range of f. In other words, there does not exist any element $x_0' \neq x_0$ (*resp.*, $x_1' \neq x_1$) such that $f(x_0, x_1) = f(x_0', x_1)$ (*resp.*, $f(x_0, x_1') = f(x_0, x_1)$). If one party sends a fictitious value to the TTP, both parties get utility zero, which is absolutely smaller than 1, so both parties have incentives to send their true values to the TTP.

3.2. Execution in the Real World. It is more complex to construct a protocol completing the computation without a TTP. A hybrid protocol including two stages is first proposed as a transition. The first stage is an ideal functionality *ShareGen* and the second stage consists of several rounds (Section 1.3). In each round, they communicate with each other and exchange some messages. Each rational party satisfies the utility assumptions (a) and (b) and reputation assumption (c). In the ideal world, the TTP is the arbitrator which restrains both parties from deviating. In the hybrid world, the TFT strategy, the reputation assumption, and the incomplete information stimulate both parties to comply with the protocol.

In the second stage, one party, say P_0, is not sure whether P_1 is a TFTer party. We assume that P_0 has a priori probability γ on the type of P_1. In other words, P_0 considers that P_1 is a rational party with probability $1 - \gamma$ and a TFTer party with a small probability γ. According to the TFT strategy, parties are required to begin with cooperation and keep it if the other party cooperated at the preceding stages. The fact that one party has a good/bad reputation means that the party has a reputation to cooperate/fink. From the utility definition, utility 1 when both cooperate is higher than utility 0 when both fink. So each party hopes to cooperate in each round. Mutual cooperation is easily realized when both parties are TFTers. However, parties will get into a dilemma when both parties are rational. Because the strategy profile, where both rational parties fink reach Nash equilibrium. Incomplete information can solve this dilemma to some extent. On the conditions that each party is not sure about his opponent true type, even rational parties have incentives to establish a good reputation hoping to obtain higher utilities in the future.

As the results of [21], the protocol is assumed to be in the hybrid world, where *ShareGen* is directed by a trusted dealer. We will remove this limitation here. Fortunately, Canetti [31] proves that a secure-with-abort protocol for *ShareGen* in the real world exists if there are enhanced trapdoor permutations. Therefore, a protocol in real world can be established using the composable theorem [32].

The protocols in this paper have finite rounds and parties know the last round when the protocols terminate. We will prove that mutual cooperation is a sequential equilibrium. To demonstrate a sequential equilibrium especially in the last round is cumbersome. Nevertheless, such a sequential equilibrium does exist [33]. We stress that the length of shares is the total iterations in the second stage, so the protocol will end in constant rounds. For clarity, we redescribe the lemma in [18].

Lemma 3. *Given $m^* = 1 + (2a - 4c + 2\gamma)/\gamma$, where m^* denotes the remained rounds in the protocol, there exists a sequential equilibrium such that both parties cooperate before $n - m^*$ rounds in the protocol, where n denotes the total rounds of the protocol.*

4. Fairness with Constant Rounds

In complete information scenario, there is no two-party protocol to compute functionality f on account of backward induction [25]. When the last round n is reached, parties no longer fear the future punishment and prefer to fink. As we know that fink is dominating strategy with respect to cooperation, consequently, round $n - 1$ is now the last round, and players will take strategy fink as before. This process continues in this way backwards in times and shows that parties are better off finking in rounds $n-2, n-3, \ldots, 1$ as well. If we release this condition, the predicament will be broken. We assume that each party has a private type like rational party or TFTer party. According to Lemma 3, both parties cooperate before the last "few" rounds. Inspired by this result, we construct a protocol with fairness between two parties. The informal description is given in Section 1.3, and now we give particular representations of the protocol.

4.1. The Fail-Stop Setting. Just as Groce and Katz [21], our protocol $\Pi^{ShareGen}$ consists of two stages. In the fail-stop setting, the first stage is a functionality *ShareGen* (see Box 1). The second stage includes the protocol Π (see Box 2) where both parties exchange their shares under incomplete information.

Functionality *ShareGen*
(1) **Inputs**: *ShareGen* takes as input a value x_0 (*resp.* x_1) form P_0 (*resp.* P_1).
If either input is of no vail, then *ShareGen* returns $\perp$ to both parties.
(2) **Computation**: It includes the following steps:
(a) Choose a value n such that $n = t + m^*$ (t is a constant and is the threshold of Shamir's secret sharing scheme), so $t = n - m^*$ (see Lemma 3).
(b) Generate two shares $s_0 \neq 0$, $s_1 \neq 0$ of $f(x_0, x_1)$ such that $s_0 \oplus s_1 = f(x_0, x_1)$.
(c) Randomly select two $t-1$ degree polynomials g_0 and g_1, where $g_0(0) = s_0$ and $g_1(0) = s_1$.
(3) **Outputs**: *ShareGen* sends $g_0(i)$ to P_0 and $g_1(i)$ to P_1, where $i \in \{1, 2, \ldots, n\}$.

Box 1: The description of functionality *ShareGen* in the fail-stop setting.

Protocol II
(1) **Step one**: Both parties run functionality *ShareGen* to receive $g_0(i)$ and $g_1(i)$, where $i \in \{1, 2, \ldots, n\}$.
(2) **Step two**: For $i = 1$ to n, each party decides whether to exchange his shares with the other party using the TFT strategy. We highlight two premises.
(a) Each party satisfies assumptions (a)–(c).
(b) Meanwhile, parties do not know exactly whether his opponent is a TFTer party.
Note: The utility assumptions and the incomplete information compel cooperation before round m^*.
(3) **Outputs**: Parties decide the outputs according to messages they have received.

Box 2: The description of protocol II in the fail-stop setting.

4.2. Positive Results

Theorem 4 (main theorem). *Given the utility assumptions (a) and (b) and reputation assumption (c), there exists a completely fair protocol* Π *with* $n > 1 + (2a - 4c + 2\gamma)/\gamma$ *constant rounds to compute* f *under incomplete information in fail-stop setting, where a party is a TFTer party with probability* γ. *If enhanced trapdoor permutations exist, the completely fair protocol* Π *also is established in the real world.*

Proof. We will first analyze the protocol $\Pi^{ShareGen}$ in a hybrid world where there is a trusted dealer computing *ShareGen*. Then following [32], if the protocol $\Pi^{ShareGen}$ is computational in the hybrid world, it is also established in the real world when enhanced trapdoor permutations exist. The correctness and privacy of the protocol are guaranteed by the ideal functionality *ShareGen*. We omit the formal definitions and straightforward proofs here. We prove fairness in the fail-stop setting.

(i) When *step one* of Box 2 finishes, it is obvious that party P_b can obtain s_b using Lagrange's interpolation after he receives all $g_b(i)$. The rest to do is to exchange shares with his opponent and recover s_{-b} using Lagrange's interpolation. Then at last he gets $f(x_0, x_1)$.

(ii) When *step two* of Box 2 finishes, we know that even if the parties know the value m^*, they still cooperate at the first t rounds (Lemma 3). Therefore both parties have no incentives to deviate before the previous t rounds, where $t = n - 1 - (2a - 4c + 2\gamma)/\gamma$ is the threshold of Shamir's secret sharing scheme. Under this circumstance, both parties will receive at least t shares from their opponents. In other words, party P_b may retrieve s_{-b} using Lagrange's interpolation and finally learn $f(x_0, x_1)$.

To sum up, fairness is achieved in both settings. The round complexity is $O(1)$ which is more efficient than $O(1/p)$ in [21]. We stress that our conclusion of Nash equilibrium is stronger than that of [21], where only computational Nash equilibrium is established. Here, a sequential equilibrium in the fail-stop setting is met according to Lemma 3. □

4.3. The Applications of Our Protocol. The most important property of our protocol is the achievement of fairness in rational secure two-party computations. Although fairness is achieved in previous works, this is the first time that it is achieved through reputation assumptions, where parties in the protocol adopt TFT strategy. The property of fairness is essential in most secure multiparty computations, such as electronic voting and electronic auction. Take electronic voting; for instance, voters vote for candidates and wish to receive a fair and correct result. That is, the result cannot be biased by adversaries and should truly reflect their opinions. Traditional secure multiparty computations cannot achieve the property of fairness. Therefore, they cannot prevent adversaries from biasing the result. Fortunately, rational secure multiparty computations can realize fairness. On one hand, our rational protocols guarantee that each party may receive the same voting result. On the other hand, the adversary cannot bias the result.

The application of protocol $\Pi^{ShareGen}$ in electronic voting is present as follows. We describe the electronic voting

protocol in the fail-stop setting using the protocol $\Pi^{ShareGen}$. Suppose that voters who participate in the voting may meet in the future to participate in other voting. When they meet again, they will evaluate each other through previous interactions. After several meetings, each voter win a reputation about his type. The type indicates that voters are rational or that they may adopt TFT strategy. As mentioned above, there is a probability γ to describe the prior probability about the type. So far, voters in electronic voting have the same features as those in $\Pi^{ShareGen}$. Next we will describe the process of electronic voting in which the voters mentioned above have participated.

(i) Voters run *ShareGen* using their specific inputs and receive their outputs, respectively (Box 1).

(ii) Voters run protocol Π according to their types and update reputation after each step (Box 2).

(iii) Voters output what they received in the protocol.

We prove that, given proper parameters, fairness can be achieved in protocol $\Pi^{ShareGen}$. Since voters have the same features as parties in $\Pi^{ShareGen}$, Theorem 4 can be applied rightly into electronic voting, where fairness is also achieved.

5. Conclusions

The importance of security guarantee in mobile social networks and telecommunication services is rapidly increasing since the applications in mobile social networks are more and more popular. The property of fairness is becoming an eye-catching aspect in secure computation especially between two rational parties. Game theory opens up another avenue to intensively study fairness of secure multiparty computation. Asharov et al. [34] give negative results based on improper utility assumptions. They conclude that no parties have incentives to cooperate with others. Groce and Katz [21] amend the deficiencies with new utility assumptions and two modifications which bring some new troubles. Consequently, the protocol in [21] has large round complexity and the trust dealer is required to participate in the protocol Π even in the real world.

Inspired by the fact that parties in mobile social networks value their reputation, which can boost cooperation between two rational parties, we modify the utility definition and allow parties to consider the effect of reputation derived from mobile social networks when they interact in the protocol. The results show that cooperation appears before the last "few" rounds even when they know the terminal round in finitely repeated games under incomplete information. Then we construct a protocol just like Groce and Katz [21]. Finally, with the help of the TFT strategy and the reputation from mobile social networks, the protocol Π in this paper can achieve fairness and sequential equilibrium.

Disclosure

An abstract of this paper has been presented in the INCOS2013 conference, pages 309–314, 2013 [35].

Conflict of Interests

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

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant nos. 61173139 and 61202475, Natural Science Foundation of Shandong Province under Grant no. BS2014DX016, Ph.D. Programs Foundation of Ludong University under Grant no. LY2015033.

References

[1] M. Kimura and K. Saito, "Tractable models for information diffusion in social networks," in *Knowledge Discovery in Databases: PKDD 2006*, vol. 4213, pp. 259–271, Springer, Berlin, Germany, 2006.

[2] H. Ma, H. Yang, M. R. Lyu, and I. King, "Mining social networks using heat diffusion processes for marketing candidates selection," in *Proceedings of the 17th ACM Conference on Information and Knowledge Management (CIKM '08)*, pp. 233–242, ACM, October 2008.

[3] A. B. Waluyo, W. Rahayu, D. Taniar, and B. Scrinivasan, "A novel structure and access mechanism for mobile data broadcast in digital ecosystems," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 6, pp. 2173–2182, 2011.

[4] J. Goh and D. Taniar, "Mining frequency pattern from mobile users," in *Knowledge-Based Intelligent Information and Engineering Systems*, pp. 795–801, Springer, 2004.

[5] D. Taniar and J. Goh, "On mining movement pattern from mobile users," *International Journal of Distributed Sensor Networks*, vol. 3, no. 1, pp. 69–86, 2007.

[6] J. Y. Goh and D. Taniar, "Mobile data mining by location dependencies," in *Intelligent Data Engineering and Automated Learning—IDEAL 2004*, vol. 3177 of *Lecture Notes in Computer Science*, pp. 225–231, Springer, Berlin, Germany, 2004.

[7] A. Yao, "Protocols for secure computation," in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (FOCS '82)*, pp. 160–164, IEEE Computer Society, Chicago, Ill, USA, November 1982.

[8] R. Cleve, "Limits on the security of coin flips when half the processors are faulty," in *STOC 1986*, J. Hartmanis, Ed., pp. 364–369, ACM, Berkeley, Calif, USA, 1986.

[9] O. Goldreich, *Foundations of Cryptography*, vol. 2, Cambridge University Press, 2004.

[10] J. Urry, "Social networks, travel and talk," *British Journal of Sociology*, vol. 54, no. 2, pp. 155–175, 2003.

[11] K. W. Axhausen, "Social networks and travel: some hypotheses," in *Social Dimensions of Sustainable Transport: Transatlantic Perspectives*, pp. 90–108, 2005.

[12] B. Wellman, B. Hogan, K. Berg et al., "Connected lives: the project1," in *Networked Neighbourhoods*, pp. 161–216, Springer, 2006.

[13] J. Larsen, J. Urry, and K. Axhausen, "Coordinating face-to-face meetings in mobile network societies," *Information Communication & Society*, vol. 11, no. 5, pp. 640–658, 2008.

[14] Y. Wang, G. Cong, G. Song, and K. Xie, "Community-based greedy algorithm for mining top-k influential nodes in mobile

social networks," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1039–1048, ACM, 2010.

[15] E. Miluzzo, N. D. Lane, K. Fodor et al., "Sensing meets mobile social networks: the design, implementation and evaluation of the CenceMe application," in *Proceedings of the 6th ACM Conference on Embedded Networked Sensor Systems (SenSys '08)*, pp. 337–350, ACM, New York, NY, USA, November 2008.

[16] M. C. González, P. G. Lind, and H. J. Herrmann, "System of mobile agents to model social networks," *Physical Review Letters*, vol. 96, no. 8, Article ID 088702, 2006.

[17] A. Beach, M. Gartrell, S. Akkala et al., "WhozThat? Evolving an ecosystem for context-aware mobile social networks," *IEEE Network*, vol. 22, no. 4, pp. 50–55, 2008.

[18] Y. Wang, Z. Liu, H. Wang, and Q. Xu, "Social rational secure multi-party computation," *Concurrency Computation Practice and Experience*, vol. 26, no. 5, pp. 1067–1083, 2014.

[19] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation: extended abstract," in *Proceedings of the Symposium of Theory of Computing (STOC '04)*, pp. 623–632, ACM, Chicago, Ill, USA.

[20] S. Maleka, A. Shareef, and C. P. Rangan, "Rational secret sharing with repeated games," in *Information Security Practice and Experience: Proceedings of the 4th International Conference, ISPEC 2008 Sydney, Australia, April 21–23, 2008*, L. Chen, Y. Mu, and W. Susilo, Eds., vol. 4991 of *Lecture Notes in Computer Science*, pp. 334–346, Springer, Berlin, Germany, 2008.

[21] A. Groce and J. Katz, "Fair computation with rational players," in *Advances in Cryptology—EUROCRYPT 2012*, D. Pointcheval and T. Johansson, Eds., vol. 7237, pp. 81–98, Springer, Cambridge, UK, 2012.

[22] Y. Wang, Q. Xu, and Z. Liu, "Fair computation with tit-for-tat strategy," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, pp. 309–314, Xi'an, China, September 2013.

[23] R. Axelrod, *The Evolution of Cooperation*, Penguin Press, London, UK, 1990.

[24] M. A. Nowak and K. Sigmund, "Tit for tat in heterogeneous populations," *Nature*, vol. 355, no. 6357, pp. 250–253, 1992.

[25] D. Fudenberg and J. Tirole, *Game Theory, 1991*, MIT Press, Cambridge, Mass, USA, 1991.

[26] S. Gordon, C. Hazay, J. Katz, and Y. Lindell, "Complete fairness in secure two-party computation," in *Proceedings of the Symposium on Theory of Computing Conference (STOC '08)*, C. Dwork, Ed., pp. 413–422, ACM, Victoria, Canada, May 2008.

[27] J. Katz, "On achieving the best of both worlds in secure multiparty computation," in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing (STOC '07)*, pp. 11–20, ACM, San Diego, Calif, USA, 2007.

[28] T. Moran, M. Naor, and G. Segev, "An optimally fair coin toss," in *Theory of Cryptography*, O. Reingold, Ed., vol. 5444 of *Lecture Notes in Computer Science*, pp. 1–18, San Francisco, Calif, USA, 2009.

[29] B. Yu and M. P. Singh, "A social mechanism of reputation management in electronic communities," in *Cooperative Information Agents IV—The Future of Information Agents in Cyberspace*, pp. 154–165, Springer, Boston, MA, USA, 2000.

[30] M. Nojoumian and T. C. Lethbridge, "A new approach for the trust calculation in social networks," in *E-Business and Telecommunication Networks*, pp. 64–77, Springer, Berlin, Germany, 2008.

[31] R. Canetti, "Security and composition of multiparty cryptographic protocols," *Journal of Cryptology*, vol. 13, no. 1, pp. 143–202, 2000.

[32] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS '01)*, pp. 136–145, IEEE Computer Society, Las Vegas, Nev, USA, October 2001.

[33] D. M. Kreps and R. Wilson, "Reputation and imperfect information," *Journal of Economic Theory*, vol. 27, no. 2, pp. 253–279, 1982.

[34] G. Asharov, R. Canetti, and C. Hazay, "Towards a game theoretic view of secure computation," in *Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '11)*, K. G. Paterson, Ed., pp. 426–445, Springer, Tallinn, Estonia, 2011.

[35] Y. Wang, Q. Xu, and Z. Liu, "Fair computation with tit-for-tat strategy," in *Proceedings of the 5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, pp. 309–314, IEEE, Los Alamitos, Calif, USA, September 2013.