International Journal of u- and e- Service, Science and Technology
Vol.8, No.5 (2015), pp.373-378
http://dx.doi.org/10.14257/ijunesst.2015.8.5.35

# The Motivation of Electronic Voting towards Game Theory

Lirong Qiu

*School of Information Engineering, Minzu University of China, China*
*qiu_lirong@126.com*

***Abstract***

*With rapid development of computer science and network technology, the technology of electronic voting is widely applied in various fields. There are lots of security requirements in electronic voting such as privacy, verifiability, fairness and robustness etc. Previous works mainly discuss how to guarantee these requirements by using cryptographic tools, such as encryption, commitment etc. There, most works assume that parties are honest who will follow the protocol or malicious who will arbitrarily break the security of the protocol. In fact parties in real life are neither honest nor malicious, but instead they may consider the benefits when they decide to participate in voting. This paper discusses the motivations of parties to participate into voting towards the view of game theory. More specifically, motivations are quantized as the notion of utilities just as those in game theory. Then we prove how to assign people to have motivations to vote by achieving Nash equilibrium.*

***Keywords:*** *Electronic voting; Game theory; Nash equilibrium; Motivation*

## 1. Introduction

Electronic voting means that a voting scheme utilizes electronic assistance devices when polling and tallying. There are two kinds of electronic voting schemes: off-line scheme and on-line scheme. The latter scheme is flexible such that voters who cannot arrive at polling station are able to vote. Normally, an electronic voting scheme consists of the following components: voters, registration authority, candidate, tally authority and scrutineer. The scheme should at least guarantee some security requirements except for basic polling and tallying requirements. (1)Eligibility: This requirement means that only parties who own the quality can vote. (2) Accuracy: This requirement means each voter can vote only once. (3) Privacy: This requirement means the contents of the votes are known only by the voters themselves. The voting scheme only publishes the result of the voting and no information about the votes will be revealed. (4) Verifiability: This requires that the results of tally can be verified such that no votes are missing or repeated counted. (5) Robust: This requirement means that electronic voting scheme may detect errors. For example one voter deliberately votes for an invalid vote. The scheme continues to work if the error level is tolerable. Otherwise stop to work. (6) Fairness: The statistical information about votes should not be revealed until the end of voting in case that the intermediate results of voting may effluent the inclination of other voters who do not vote yet. (7) Receipt-freeness or Uncoercibility: Voters cannot prove the contents of their votes to the third party and cannot generate a receipt to prove which candidate they support. This requirement prevents selling and buying votes.

The intuition to apply cryptography into electronic voting is to realize the above requirements. For example, encryption and zero knowledge [1] are two powerful tools to provide security. More specifically, encryption guarantees the requirement of privacy, where voters submit their ballot tickets in ciphertext form. Zero knowledge guarantees the requirement of verifiability, where tally agency can indicate that no corrupt transactions exist in counting process and no information about votes will be revealed by using no-

ISSN: 2005-4246 IJUNESST
Copyright ⓒ 2015 SERSC

interactive zero knowledge. The future works in electronic voting consist of the following fields: finding efficient encryption algorithms, zero knowledge proof method and simple schemes for voting.

So far, there are four kinds of voting scheme: (1) mix-net voting scheme [2–6] , (2) blind signature voting scheme [7–9], (3) voting scheme based on secret sharing [10–12] and (4) voting scheme based on homomorphic encryption [13–15]. In this paper, we stress on the voting scheme based on secret sharing, where voters split his vote into n shares. They then send the shares to n vote counter, who collect the shares of each voter and finally reconstruct the votes.

However, most electronic voting schemes assume that voters are either honest or malicious. They rarely consider the motivation why they vote, why the support one candidate rather than the other. Although some people may argue that the motivation for voting is not in the category of electronic voting schemes, we try to discuss it towards the view of game theory. We combine the motivation into the electronic voting schemes and try to design more efficient schemes to support voting.

## 2. Related Technology

*A, Secret Sharing*

Secret sharing is first proposed by Shamir [16] and Blakley [17] respectively in 1979. The most popular scheme is Shamir secret sharing, where one share is divided into *n* shares. Parties who get at least *t* shares can reconstruct the secret. Otherwise no one can get the secret. This is called (*t*,*n*) threshold secret share, where *t* is the threshold. More specifically, the dealer first chooses a polynomial *P(x)* with $t-1$ order such that *P* (0) =*s*. Then he randomly chooses *t* points $(x_i, y_i)$ such that $y_i$=*P* $(x_i)$ where $x_i \neq 0$ and $i$ =1, 2,…,n. $x_i$ is public value and $y_i$ is sent to each party as shares. When parties get enough shares, they can reconstruct the secret by Lagrange interpolation formula. Let $\{(x_i),(y_i)\}_{i\in[1,t]}$ denote the *t* nodes, $\lambda_i(x)$ denote the corresponding $i^{th}$ point in the interpolation formula $\lambda_i(x) = \Pi_{j=1,j\neq i}^{t} \frac{(x-x_j)}{x_i-x_j}$. We have P*(x)* =$\sum_{i=1}^{t} \lambda_i(x) y_i$ . Since *P (0)* = *s*, then we have

$$s = P(0) = \sum_{i=1}^{t} y_i \left( \prod_{j=1,j\neq i}^{t} \frac{(-x_j)}{x_i - x_j} \right)$$

.

*B. Homomorphic Encryption*

Homomorphic encryption is based on the mathematical problem of computational complexity theory of cryptography technology. For homomorphic encryption of data processing to obtain an output, the output decrypted the results with the same method of dealing with the unencrypted the output results of the original data is the same. More specifically, for a public key cryptography $PKCS = (g, E, D)$ and two computation $(\oplus,\otimes)$, we call $PKCS = (g, E, D)$ is homomorphic with respect to $(\oplus,\otimes)$, if the following conditions hold.

- Randomly choose $(pk, sk)$ using $g$, denoted as (*pk, sk*)$\leftarrow R\ g(1^k)$. Given plaintext space *P*, *(P,*$\oplus$*)* is a group.
- Randomly choose $(pk, sk)$ using$g$, denoted as (*pk, sk*)$\leftarrow R\ g(1^k)$. Given cypher text space *C*, *(C,*$\otimes$*)* is a group.

 Copyright ⓒ 2015 SERSC

- Given (*pk, sk*) $\leftarrow R\ g(1^k)$ , for any ( $c_1, c_2$ ) $\in$ *C*, we have $D(c_1 \otimes c_2) = D(c_1) \oplus c_2$.

*C. Rational Notions*

1) Rational parties: In reality people are regarded to participate in protocols with certain motivations. For example, someone promise to offer the adversary some favorable policies if he wins the vote. Thus adversary has incentives to make the one win the vote. In Byzantine protocols, the agreement of retreat minimizes the cost for the enemy, so the adversary tries to lead to the retreat agreement. These profits can be described by utility in game theory. The main task for adversaries is to maximize their utilities. To realize the task, the adversary may adopt some strategies. Meanwhile, parties who are not controlled by the adversary are no longer assumed to be honest parties. In fact, they also have certain incentives, which can be described as to prevent adversary from attacking the protocol. For example, in electronic voting, parties who are not corrupted hope all parties can correctly execute the protocol. They hope that the one who get most votes wins. Meanwhile they try to guarantee fairness for the voting by preventing some party win the vote by collusion with a subset of the whole parties. Therefore, these uncorrupted parties are also motivated by profits. In electronic voting, the profits are fairness such that the one who gets most votes wins. These profits can also be described by utility. Furthermore, they can also adopt some strategies to prevent adversaries. Thus, the protocol designers must consider such motivations when they construct a protocol. The previous notions of honest parties and adversaries are not fit for the scenarios where parties participate in the protocol with certain incentives. Therefore, new parties and models in the presence of these new parties should be proposed. Rational parties are new notions which fit for the requirement to describe the motivations. Secret sharing in the presence of rational parties are recently used to solve various problems in secret sharing [18-23].

New research directions combining rational parties with other fields are constantly proposed such as soci-rational secret sharing [24]. Figure 1 presents the relationships between rational secret sharing and social secrete sharing.

Social rational secret sharing is similar to a repeated game such as sealed bid auction where each auctioneer should obtain the shares of a secure bid in independent auction. Assume that each party has a value of reputation and then they will be punished or rewarded when they spoil the reputation. Social rationality can boost cooperation among parties, so parties only need one interaction. Furthermore, social rational secret sharing does not rely on security assumptions and communication models

2) Utility and Nash equilibrium: The incentives of rational parties can be described by utility, which is important for them since the strategies they choose depend on utilities. The strategies help them to maximize their utilities. Here we inherit the notions in game theory to define actions and utilities for parties who participate in the protocol. Let $\Gamma(\{P_i\}_{i=1}^n, \{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$ denote a protocol with *n* parties, where $\{P_i\}_{i=1}^n$ denotes a set with n parities and $\mathrm{P}_i$ denotes one party. Let $\{\mathrm{A}_i\}_{i=1}^n$ denote an action set, where the possible actions for $\mathrm{P}_i$ is $\mathrm{A}_i$ .Let $\{\mathrm{u}_i\}_{i=1}^n$ denote utility function, which suffices $\mathrm{u}_i : A_1 \times \ldots \times A_n \rightarrow R$ .Let *A*= $A_1 \times \ldots \times A_n$ such that $a = (a_1, \ldots, a_n)$ is an outcome of a protocol. The utility function $\mathrm{u}_i$ denotes the preference of $P_i$ for a certain outcome. For example, if $P_i$ prefer $a$

Copyright ⓒ 2015 SERSC

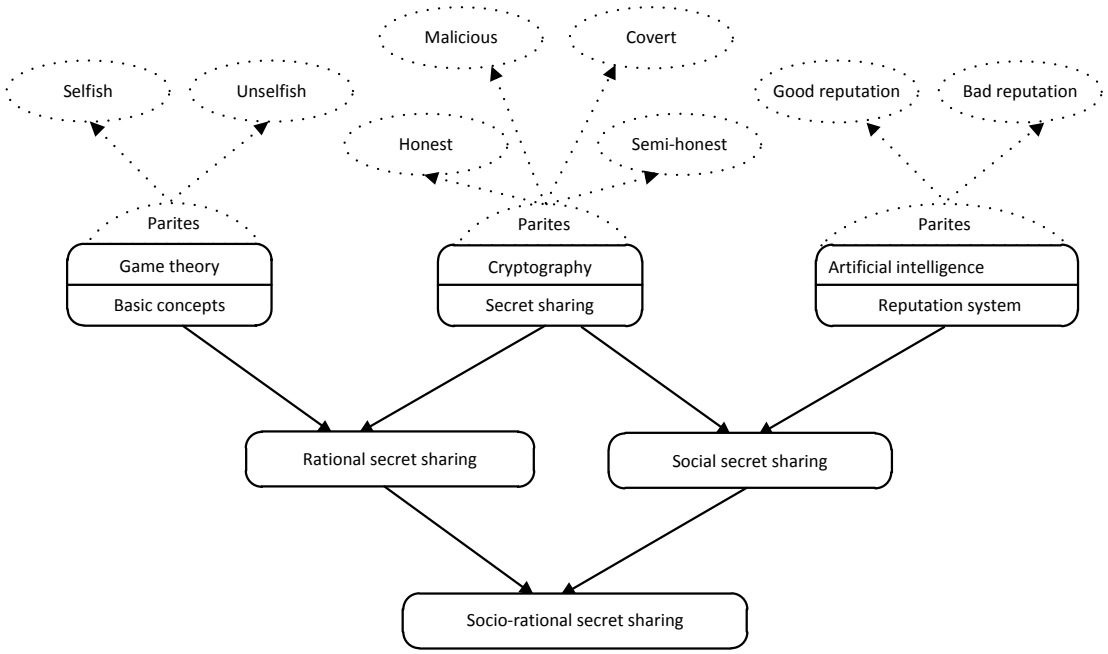


**Figure1. The Relationship between Rational Secret Sharing and Social Secrete Sharing**

With respect to $a'$ , then it can be denoted as $u_i(a) > u_i(a')$. If it suffices that $u_i(a) \geq u_i(a')$, we call $P_i$ weakly prefers $a$

Suppose utility function is common knowledge, if $P_1$ knows that other parties choose $a_1, \ldots, a_n$ then $P_1$ is sure to adopt $a_1 \in A_1$ to maximize his utility. $a_1$ is called best response of $P_1$ with respect to $a_2, \ldots, a_n$. Given $a_1$ , $P_2$ will choose $a' \in A_2$ and so on such that each party will choose his best response. The tuple $a$ is called self-enforcing if and only if $a_1$ is a best response with respect to $P_1$ .If one action tuple is a self-enforcing, it is called Nash equilibrium. Definition 1 gives the formal definition of Nash equilibrium.

Definition 1: (Nash equilibrium of pure strategy) Let $\Gamma(\{P_i\}_{i=1}^n, \{A_i\}_{i=1}^n, \{u_i\}_{i=1}^n)$ denote a normal game with *n* parties. An action tuple $a$ is Nash equilibrium of pure strategy, if for every $i$ and $' \in A_i$ , we have

$$u_i(a'_i, a_{-i}) \leq u_i(a).$$

## 3. Construction of Electronic Voting Towards Game Theory

Intuitively, voting seems to be a personal issue to sup-port a certain candidate. However, most time voters have to consider other factors just like a social choice when they decide to vote. However, voters may consider both individual and social preferences in large elections. That is, sometimes voters have to vote according to the social welfare instead of his own welfare. It's well known that voting in large elections is not able to be considered as individual preference. Previous works do not consider the effect of preference to the voting, they are inclined to design voting protocols toward the view of cryptographic. Therefore, voters in these protocols are assumed to be honest or malicious. Consequently, the protocol should only consider how to guarantee security requirements under such assumption. However, previous protocol neglects a basic premise, which is the motivation for voters to vote. Suppose that no voters have incentives to vote, it's meaningless to design a perfect secure voting protocol since no one will participate in the protocol. So, the most important issue before we discuss the construction of the voting

 Copyright ⓒ 2015 SERSC

protocol is to describe the motivations for voters to vote and present it in proper form. Fortunately, game theory can solve this problem. The basic idea is to regard the voters as rational parties who wish to maximize their utilities. Here utility is the preference of voters.

As mentioned above, utility here include two parts: individual part and social part. The individual part denotes voter's own preference and the social part denotes the social preference. Note that sometimes, social preference is bigger than individual part. The elements in electronic voting protocol consist of the following components: rational voters, registration authority, candidate, tally authority and scrutineer. Note that there are action and utility sets for rational voters. Voters have two choices in the action set: to vote or not to vote. Their utility consists of two parts, which are formally defined as follows.

$$U = \alpha U_{individual} + \beta U_{social}$$

Here $\alpha$ and $\beta$ denote the ratio of individual and social part respectively, which suffice that $\alpha, \beta \in [0,1]$ and $\alpha + \beta = 1$. Note that we call the voter a social voter if $\alpha = 0$ and a selfish voter if $\beta = 0$

In previous electronic voting protocols, the cost of voters is not considered when designing the protocol. In fact, there does exist some cost when voters vote for a certain candidate. Therefore, we consider the cost for voting in this paper. Thus finally the total utility is the utility equation (1) minus the cost.

$$U_{total} = U - cost$$

As for the action set, voters have two choices: to vote or not. If they vote they will get utility $U_{total}$ , otherwise he will not get any utility. For simplicity, we assume that if voters do not participate in the voting protocol he will get nothing. That is, they will not get *U* meanwhile they will not pay the cost. Therefore, the total utility is zero. According to the definition of Nash equilibrium, we conclude that some parameters must satisfy certain conditions in order to assign enough motivations for voters to vote.

Theorem 1: Given *U* > *cost*, voters have motivations to vote. Not voting.

Assigning motivations to voters, they all have motivations to participate in the voting protocols. Then voters can participate in the electronic voting systems on the basis of secret sharing [12]. It can prove that we achieve the same result as [12].

## 4. Conclusion

Most works of electronic voting consider the problem of how to guarantee the security of the voting systems such as eligibility, privacy and fairness etc. In this paper, we study the motivations of voters towards the view of game theory. That is, why voters have to participate in the protocol and how to guarantee voters to vote. Suppose that voters have motivations to vote, and then each of them will follow the protocol to vote. So no one will deviate from the protocol, voters in this situation can be considered The basic idea is to let utility when voting is bigger than that when as rational parties. However, many other problems should consider in the presence of rational voters. For example, the may consider how to define the utility, how to reach Nash equilibrium and how to resist the collusion. These problems will be discussed in the future works.

## Acknowledgements

Our work is supported by the National nature science foundation of China (No. 61103161), the 985 special funds in School of information engineering, Minzu university of China and the Program for New Century Excellent Talents in University (NCET-12-0579)

Copyright ⓒ 2015 SERSC

## References

[1] D. Beaver, "Secure multi-party protocols and zero-knowledge proof systems tolerating a faulty minority", Journal of Cryptology, vol. 4, no. 2, **(1991)**, pp. 75–122.
[2] C. D, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, vol. 24, no. 2, **(1981)**, pp. 84-88.
[3] P. C., I. K. and K. K., "Efficient anonymous channel and all / nothing election scheme", EUROCRYPT, Springer, **(1994)**, pp. 248–259.
[4] F. J and S. K, "An efficient scheme for proving a shuffle", CRYPTO, Springer, **(2001)**, pp. 368–387.
[5] N. A. C., "A verifiable secret shuffle and its application to e-voting", ACM Conference on Computer and Communications Security (CCS), ACM Press, **(2001)**.
[6] G. J., "A verifiable secret shuffle of homomorphic encryption-s", CRYPTO, Springer, **(2003)**, pp. 145–160.
[7] C. D., "Blind signatures for untraceable payments", CRYP-TO, Springer, **(2003)**, pp. 199–203.
[8] F. A., O. T. and O. K., "A practical secret voting scheme for large scale elections", AUSACRYPT, Springer, **(1993)**, pp. 244–251.
[9] O. M., M. F. and A. M., "An improvement on a practical secret voting scheme", ISW, Springer, **(1999)**, pp. 225– 234.
[10] C. B. J. D and F. M. J., "A robust and verifiable crypto-graphically secure election scheme", Proceedings of the 26th IEEE Symposium on Foundations of Computer Science (FOCS), Springer, **(1985)**.
[11] C. B. J. D. and Y. M., "Distributing the power of a government to enhance the privacy of voters", Proceedings of the 5th annual ACM symposium on Principles of distributed computing (PODC), ACM, **(1986)**.
[12] S. B., "A simple publicly verifiable secret sharing scheme and its application to electronic voting", CRYPTO, Springer, **(1999)**, pp. 148–164.
[13] D. I. and J. M., "A generation, a simplification and some applications of paillers probabilistic public-key system", PKC, Springer, **(2001)**, pp. 119–136.
[14] G. J., "Non-interactive zero-knowledge arguments for voting", ACNS, Springer, **(2005)**, pp. 467–482.
[15] D. I., G. J. and S. G., "The theory and implementation of an electronic voting system", Secure Electronic Voting, Springer, **(2003)**, pp. 77–100.
[16] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612–613.
[17] G. Blakley, "Safeguarding cryptographic keys", Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings, **(1979)**.
[18] I. Abraham, D. Dolev, R. Gonen and J. Halpern, "Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty com- putation", 25th ACM Symposium Annual on Principles of Distributed Com-puting, **(2006)**; New York, NY, USA.
[19] G. Asharov and Y. Lindell, "Utility dependence in correct and fair rational secret sharing", Dwork, C. (ed.) CRYPTO, Heidelberg, **(2009)**, pp. 559–576.
[20] G. Fuchsbauer, J. Katz and D. Naccache, "Efficient rational secret sharing in standard communication networks", TCC, LNCS 5978, **(2010)**, pp. 419–436.
[21] S. Gordon and J. Katz, "Rational secret sharing, revisited", De Prisco, R., Yung, M. (eds.) SCN, Heidelberg, **(2006)**, pp. 229–241.
[22] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation: extended abstract", STOC: Proceedings of the thirty-sixth annual ACM symposium on Theory of computing, **(2004)**; New York, NY, USA.
[23] J. Andreoni and J. H. Miller, "Rational cooperation in the finitely repeated prisoner's dilemma: Experimental evidence", The Economic Journal, vol. 103, no. 418, **(1993)**, pp. 570–585.
[24] M. Nojoumian and T. Lethbridge, "A new approach for the trust caculation in social network", 3rd International Coference on E-business, Springer, **(2008)**.

## Authors

**Lirong Qiu**, she received her Ph.D. in Computer Sciences (2007) from Chinese Academy of Science. Now she is an associate professor of computer sciences at Information Engineering Department, Minzu University of China. Her current research interests include different aspects of natural language processing, artificial intelligence and distributed systems.

 Copyright ⓒ 2015 SERSC