Analysis and Comparison of Cryptographic Techniques in E-voting and E-auction

Her, Yong-Sork
Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyushu University : Graduate Student

Imamoto, Kenji
Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyushu University : Graduate Student

Sakurai, Kouichi
Department of Computer Science and Communication Engineering, Faculty of Information Science and Electrical Engineering, Kyushu University

https://doi.org/10.15017/1516212

九州大学大学院
システム情報科学紀要
第10巻 第2号 平成17年9月

Research Reports on Information Science and
Electrical Engineering of Kyushu University
Vol.10, No.2, September 2005

Analysis and Comparison of Cryptographic Techniques in E-voting and E-auction

Yong-Sork HER*, Kenji IMAMOTO* and Kouichi SAKURAI**

(Received June 10, 2005)

Abstract: Recently, many cryptographic techniques have been used for secure e-voting systems and e-auction systems. In this paper, we compare the used cryptographic techniques of e-voting systems with those of e-auction systems. We analyze advantages and disadvantages of various cryptographic techniques through e-voting systems and e-auction systems. Also, we discuss receipt-freeness which is one of the important requirements in e-voting systems and e-auction systems. Several receipt-free schemes have been proposed to prevent a vote-coercion (*e-voting*) or a bid-rigging (*e-auction*). In this paper, we analyze the existing receipt-free schemes and point out that the existing receipt-free schemes for the e-auction system do not prevent the bid-rigging. Moreover, we show the simulation results of computational costs in e-voting systems and e-auction systems which used the similar cryptographic techniques.

Keywords: E-voting, E-auction, Cryptography, Privacy, Receipt-freeness

1. Introduction

1.1 Background

According to development of the Internet and cryptography techniques, there has been a significant change in the quality and way of life. A diverse range of application programs such as an e-voting system and an e-auction have been researched on and developed, providing tangible benefits to our daily lives. In this paper, we focus on the e-voting system and the e-auction system. Two systems have most influence with our life.

E-voting system: There are a number of voting methods currently being employed by various countries. However, the losses related to manpower, time and money in carrying out voting are still far too great for most countries. Moreover, at the moment, the voters' political indifference poses a more significant threat. It translates directly to a decrease in voting ratio. Due to such reasons, the development of new voting method is said to be an important project of national significance. The fact that diverse forms of e-voting where convenience, efficiency and accuracy are punctuated via the advancement in electronic and information and telecommunications technologies are currently being developed is a testament to such claim.

E-auction system: An auction is a kind of trade for special goods which have not a fixed price. In real world, various type auctions have been enforced for decision of price. Recently, e-auctions using cryptography techniques have been proposed. Generally, e-auctions are classified into three types. One is an English auction scheme, another is a first-price sealed-bid auction scheme and the other is a second-price sealed-bid auction scheme. In the English auction scheme, seeing the bidding price, a bidder repeatedly makes a bid in real time. After the bidding time is over, the bidder who made a bid with the highest price becomes the winner. During bidding, all bidders can see the bidding price in the English auction. In case of the first-price sealed-bid auction, it is extracted only the highest price to decide the winner, and a bidder can not know bidding prices of other bidders. A decision method of a winner in the second-price sealed-bid auction is the same method with the first-price sealed-bid auction. However, the winner pays the second highest price to get the auction goods.

1.2 Related Works

The recent topic of e-voting systems and e-auction systems is receipt-freeness. Receipt-freeness of the e-voting system means that a voter can not construct a receipt to proving the content of his vote. That is, receipt-freeness prevents a vote-coercion. In case of the e-auction system, receipt-freeness means that a bidder can not prove how he bided to a coercer or a buyer. That is, receipt-freeness prevents a bid-rigging. Several receipt-free

* Department of Computer Science and Communication Engineering, Graduate Student

** Department of Computer Science and Communication Engineering

schemes[2,4,7,10,18,24] for the secure e-voting and e-auction have been developed.

In case of the e-voting system, Benaloh and Tuinstra[4] proposed the first receipt-free scheme in the e-voting system, and Abe and Suzuki[2] proposed the first receipt-free scheme for the e-auction system. The common point in the first receipt-free schemes of e-voting and e-auction is the physical assumptions, which are called voting booth and bidding booth. Sako and Kilian[24] proposed the receipt-free scheme using untappable channel. Okamoto[18] proposed the receipt-free scheme based on trap-door bit-commitment using untappable channel such as physical assumption. Chen, Lee and Kim[7] proposed a new receipt-free sealed bid auction scheme using the homomorphic encryption.

On the other hand, Kikuchi, Harkavy and Tygar[14] proposed the method that deals with tie-breaking in sealed-bid auctions. Omote and Miyaji [19,20] proposed the sealed-bid action with binary trees which is emphasized efficiency and entertainment. Naor, Pinkas and Sumner[17]introduced the sealed-bid auction that uses two-server auction system in order to ensure privacy and correctness. Juels and Szydlo[13] improved the scheme of Naor *et al.*[17] in aspect of the amount of computation and communication. Baudron and Stern[3] proposed the sealed-bid auction based on circuit evaluation using homomorphic encryption. Abe and Suzuki [1]proposed M+1-st price auction using homomorphic encryption.

2. Requirements for Secure E-voting and E-auction

In this section, we introduce the requirements for a secure e-voting system and e-auction system, and compare those in **Table 1**. **Table 2** shows the used cryptographic techniques to satisfy the requirements.

2.1 Requirements for Secure E-voting System

- *Privacy*: All votes must be secret.
- *Receipt-freeness*: A voter should not prove other parties or people how he voted.
- *Individual verifiability*: A sender can check whether or not his message has reached its destination.
- *Universal verifiability*: Everyone can check whether or not the other messages have reached its destination. Some researchers call this verifiability public verifiability.
- *Robustness*: The voting system should be successful regardless of partial failure of the system.
- *Fairness*: Nothing can affect the voting.
- *Completeness*: All valid votes should be counted exactly.
- *Unreusability*: All legal voters can vote only one-time.
- *Eligibility*: No one who is not allowed to vote can vote.
- *Soundness*: Anyone cannot disturb the voting.

Table 1 Requirements of e-voting and e-auction.

E-voting	E-auction
Privacy	Privacy
Receipt-freeness	Receipt-freeness
Universal verifiability (Public verifiability)	Public verifiability
Robustness	Robustness
Completeness	Non-repudiation
Eligibility	Bid security
Unreusability	Proof of winner

2.2 Requirements for Secure E-auction System

- *Privacy*: No auction bid is revealed except for the winning bid.
- *Receipt-freeness*: Anyone including bidders should not prove any bidding information to any party.
- *Public verifiability*: Anybody can publicly verify that a winning bid is the highest value of all bids.
- *Proof of winner*: The special auctioneer can verify the relation between the winner and the winning price.
- *Non-repudiation*: The winner cannot repudiate his/her bidding at the winning price.
- *Bid Security*: Nobody can forge and tap a bid.
- *Robustness*: Even if a bidder sends an invalid bid, the auction process is unaffected.

3. Analysis of Receipt-free Schemes and Its Problems

In this section, we analyze the existing receipt-free schemes. Especially, we point out that the receipt-free schemes for the e-auction system do not prevent a bid-rigging perfectly.

3.1 Receipt-free Scheme in E-voting

Table 2 Relation between cryptographic techniques and requirements.

Requirements	Cryptographic techniques
Privacy	Public-key cryptosystem, Secret Sharing scheme, Mix-net scheme, $(t+1, N)$ threshold encryption
Receipt-freeness	Secret channel (including untappable channel), Voting booth(or bidding booth) Mix-net scheme, Homomorphic encryption, Bit-commitment scheme
Universal verifiability (Public verifiability)	Bulletin board, Zero-knowledge proof, Interactive proofs/ Non-interactive proofs
Robustness	Secret Sharing scheme, $(t+1, N)$ threshold encryption
Completeness	Homomorphic encryption
Non-repudiation	Blind signature, Digital signature, Bit-commitment scheme
Eligibility	Secret channel (including untappable channel)
Unreusability	Bulletin board, Blind signature, Hash funciton

System

As mentioned in section 1.2, Benaloh and Tuinstra[4] proposed the first receipt-free scheme for the e-voting system. They used physically guarantees secret communication, as a voting booth, between the authorities and each voter. Also, they proposed two voting protocols using homomorphic encryption: one is used a single authority and the other is used a multi-authority. However, the e-voting protocol based on the single authority is shown the weakness of maintain vote secrete during the single authority enforcing receipt-freeness. Also, the single authority knows how each vote was cast. The other e-voting protocol which uses the multi-authority was shown as not receipt-freeness, too[10].

Sako and Kilian[24] proposed the receipt-free voting protocol based on a mix-net channel. They assumed the existence of one-way secret communication, as an untappable private channel, between each authority and each voter. The important disadvantage of this scheme is that much load can be happened in tallying because of mix-net scheme[10]. Hirt and Sako[10] introduced the efficient receipt-free voting based on homomorphic encryption. They used Sako *et al.*'s scheme[24] and Cramer *et al.*'s scheme[5]. For the practical receipt-free voting scheme, they introduced one-way communication channels from the authorities to the voters, as Sako *et al.*'s scheme[24] and receipt-free 1-out-of-2 voting based on 1-out-of L re-encryption proof of Cramer *et al.*'s scheme[5].

Juels and Jakobsson[11]introduced the concept of coercion-resistant, not receipt-freeness. They say that a coercion-resistant scheme provides not only receipt-freeness, but also defense against randomization, forced-abstention and simulation attacks [11]. The concept of coercion implies to the broad receipt-freeness. For the coercion-resistant, they used multi-authority, multi-registers and anonymous credential. Lee and Kim[16] extended Lee *et al.*'s scheme[15] and Hirt's scheme[9]. Hirt[9] introduced a tamper-resistant randomizer (TRR). The TRR is the same role with *Honest Verifier* of Lee *et al.*'s scheme[15]. They presented the reason using TRR that tamper-resistant hardware device seems to be more practical assumption than untappable channel and trusted third party.

3.2 Receipt-free Scheme in E-auction System

As mentioned in section 1.2, Abe and Suzuki [2] proposed the first receipt-free scheme for an e-auction. The reason which is required receipt-freeness in the e-auction introduced as follows.

A coercer orders other bidders to bid very low price, he then can win the auction at an unreasonably low price. To make other bidders obey his order, the coercer punishes bidders who do not cast the ordered bidding price, and rewards for bidders who cast the ordered bidding price.

The goals of the coercer are that he becomes the winner and wants to buy the auction item with an unreasonable low price. For the receipt-free scheme, Abe and Suzuki[2] used the physical assumptions such as a bidding booth and a one-way untappable channel. Chen, Lee and Kim[7] pointed out that the receipt-free scheme of Abe and Suzuki does not provide receipt-freeness for a winner. Also, they proposed a new receipt-free scheme. In Chen *et al.*'s scheme[7], the auctioneer computes the winning price. The winner should prove securely that the winning price is his bidding price. The winner is not

Table 3 E-voting vs. E-auction.

	E-voting	E-auction
Results	Summation of all ballots	Abstraction of only the highest price (or the lowest price)
Relation between a voter and a ballot (or a bidder and a bidding price)	Keep anonymity	Do not keep anonymity of the winner
An aim of the receipt-free scheme	To prevent the ballot-selling	To prevent the bid-rigging

published for receipt-freeness. That is, for receipt-freeness, it is required that all bidders do not know who the winner is.

Winner = Coercer

Suppose that other bidders cast the ordered bidding price and the coercer becomes the winner, then the coercer rewards for other bidders. Although some bidders did not obey the order of the coercer, they can require a reward to the coercer, because the coercer becomes the winner with an unreasonably low price. Then, other bidders do not need to prove his bidding price. That is, it does not need the receipt-free scheme.

Winner $\neq$ Coercer

If the coercer is not the winner, he will look for the winner. Then, it needs the receipt-free scheme. And, it can happen the dispute that the bidders who cast the ordered bidding prices require a reward to the coercer. After all, although the e-auction gives the perfect receipt-free scheme, if the coercer becomes the winner, the receipt-free scheme is meaningless. Moreover, to success the bid-rigging, it is required two conditions as follows:

- The coercer should control all the bidders in the e-auction.
- The coercer should not perform non-reputation.

3.3 Analysis of Receipt-free Schemes

The important difference between the receipt-free schemes of e-voting and e-auction is the last computation method. In case of the e-voting, it is published the summation of all ballots. Also, the aim of the receipt-free scheme is to guarantee privacy. That is, everyone should not know the relation between a voter and a ballot. However, in case of the e-auction, it needs only the highest price (or the lowest price), and is published the winner with the highest price. Therefore, anyone should know the relation between a bidder and a bidding price because of the last publishing. The aim of the receipt-free scheme is to prevent the bid-rigging. If it is not guaranteed the receipt-free scheme, a coercer will win in all auctions with an unreasonably low price. It is a very important problem in the e-auction system, not exist a paper-based sealed-bid auction. **Table 3** shows the differences between the e-voting system and the e-auction system.

4. Security Analysis of E-voting System and E-auction System

4.1 Comparison of Mix-net Model

4.1.1 Overview of Mix-net Model

David Chaum[6] introduced the first mix-net scheme as anonymous channel. A mix-net takes a list of ciphertexts of users and outputs a permuted list of the plaintexts without revealing the relationship between plaintexts and ciphertexts. The important point in the mix-net is that if at least one mix-server is trust, it can guarantee privacy between a sender and a sender's message. There are n mix-servers $M_1, ..., M_n$; each mix-server has a public key E_j and a private key D_j, where $1 \leq j \leq n$. When someone wants to send a message m through anonymous channel, he encrypts it

$$E_1(E_2(...E_n(m))...)$$

and sends to M_1.

M_1 waits until more encrypted message arrive. Then it takes the received messages, removes one level of encryption, permutes them in random order, and sends them to M_2. Mix-server M_j receives the encrypted messages. It removes one layer of encryption, shuffles them and sends $E_{j+1}(E_{j+2}(...E_n(m)...)$ to M_{j+1}. The last mix-server M_n decrypts the message and sends them to their recipients.

4.1.2 Mix-net Model in E-voting System

Several e-voting systems based on the mix-net scheme have been proposed. Generally, there are two methods which is used the mix-net scheme in e-voting system. One is that the mix-net is used to mix the voting list[10]. For example, a mix-center mixes the voting list and the mixing result is sent to the voter securely. The voter receives the last voting list from the last mix-center, and chooses the vote from the last voting list.

The other is that the mix-center mixes the encrypted votes of voters[21,24]. The last mix-center or a third trust party decrypts the mixed and encrypted votes, and computes the final tally. Then, if the last mix-center or the third trust party who computes the final tally is malicious, the e-voting system is failed. So, a secret sharing scheme was developed for the tally computation by multi-party. Recently, the mix-net scheme has been used with secret sharing scheme or publicly verifiable secret sharing since Shamir[23] proposed $(t+1, N)$ secret sharing scheme. $(t+1, N)$ secret sharing scheme allows any coalition of $t+1$ from N mix-centers to get the secret. Any set of at most t mix-centers knows nothing about the secret.

4.1.3 Mix-net Model in E-auction System

Usually, the e-auction system did not use the mix-net scheme. The mix-net scheme achieves anonymity between a sender and his message. When the mix-net scheme is applied to e-auction system, the winner can not prove that the winning price is his bidding price.

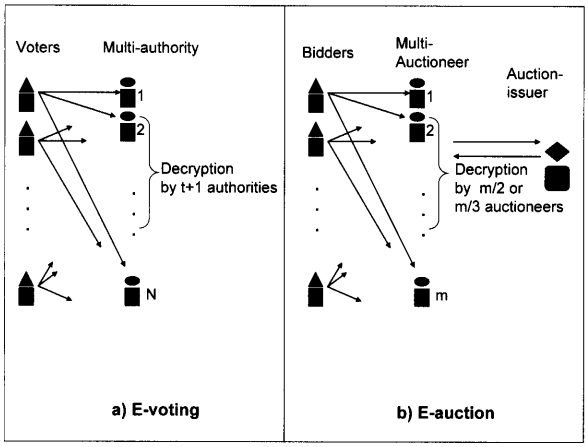

Fig. 1 Comparison of a threshold party model.

4.2 Comparison of a Threshold Party Model

In this section, we compare a threshold party model of e-voting system with that of e-auction (see **Fig. 1**). In case of the e-voting system, the threshold party model is used ElGamal encryption and $(t+1, N)$ secret sharing scheme. At most t authorities' secret value can be disclosed, as from the $t+1$ known values a secret key can be computed using Lagrange interpolation, and the vote can be directly recovered as in ElGamal decryption. The proposed 1-out-of-L voting systems require much computing resources. In case of the e-auction system, Naor *et al.*[17] proposed a threshold trust model. There are m auctioneers in the threshold trust model, out of which a fraction (e.g. more than $m/3$ or $m/2$) are assumed to be trusted. The auctioneers jointly compute the winning price by using inefficient techniques of secure multi-party function evaluation.

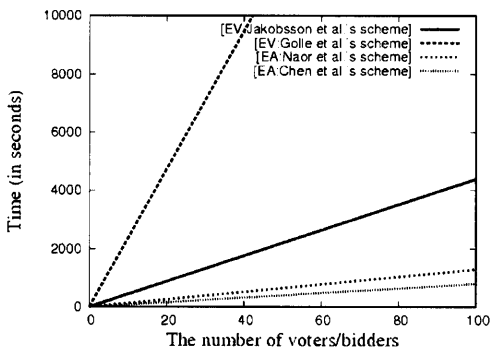

Fig. 2 Simulation results of computational costs.

5. Simulation

In **Fig. 2**, we show the simulation results of computational costs of e-voting system and e-auction system. We compare computational costs of Jakobsson *et al.*'s scheme[12] and Golle *et al.*'s scheme[8] of e-voting system with those of Naor *et al.*'s scheme[17] and Chen *et al.*'s scheme[7] of e-auction system in **Table 4**. In **Table 4**, n means the number of voters or bidders, a is the number of auctioneer, and k is the number of mix-center. In order to compare the computational cost of e-voting system with that of e-auction system, we assume that the number of mix-center is same with the number of auctioneer. The other conditions are as follows.

- The number of mix-center / auctioneer : 10
- The number of voters / bidders : from 0 to 100
- Range of time (seconds) : from 0 to 10000

In **Fig. 2**, we can know that computational costs of e-voting system are higher than those of e-auction system. The e-voting system should compute all voters to get the final tally. However, the e-auction system extracts the highest price (or lowest price). If the highest price (or lowest price) is found, the computation is stopped.

6. Conclusion

An e-voting and an e-auction are very useful systems in the information-oriented society. Both systems have points of common and difference in re-

Table 4 Computational costs.

Cryptographic techniques	Voting/Bidding	Proof	Counting/Opening	Trading
Randomized Partial Checking[12]	$2n$	$n/2(2k-1)$	$(2+4k)n$	
Optimistic Mixing[8]	$6n$	$6+12k$	$(5+10k)n$	
1-out-of-2-Proxy-oblivious transfer[17]	$a \times n$	$2n$	n	
Homomorphic encryption[7]	$3n$	$4n$	n	1

quirements. In this paper, we compared both e-voting system and e-auction system from a cryptography point of view. A few receipt-free schemes have been proposed to prevent the vote-coercion or the bid-rigging in both e-voting system and e-auction system. We concentrate on the receipt-free scheme of e-auction. We showed that the existed receipt-free schemes of e-auction do not guarantee the bid-rigging. Also, we showed the simulation results of computational costs in both e-voting system and e-auction system which used the similar cryptographic techniques.

Acknowledgement

The first author supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Research on System LSI Design Methodology for Social Infrastructure) of the Ministry of Education,Science, Sports and Culture(MEXT).

References

1) Abe,M., and Suzuki,K., "M+1-st Price Auction using Homomorphic Encryption," Proc. of PKC 2002, LNCS 2274, pp.115-124, 2002.
2) Abe,M., and Suzuki,K., "Receipt-Free Sealed-Bid Auction," ISC2002, LNCS2433, pp191-199, 2002.
3) Baudron,O., and Stern,J., "Non-interactive Private Auctions." Proc. of Financial Cryptography2001, 2001.
4) Benaloh,C.J., and Tuinstra,D., "Receipt-Free Secret-Ballot Elections." In STOC 94, pp544-553, 1994.
5) Cramer,R., Gennaro,R., and Schoenmakers,B., "A secure and optimally efficient multi-authority election scheme." European Transactions on Telecommunication, 8:481-489, Eurocrypt 1997.
6) Chaum,D., "Untraceable electronic mail, return addresses, and digital pseudonyms." In Communications of the ACM, pp84-88, 1981.
7) Chen,A.,Lee,B.C., and Kim,K.J., "Receipt-Free Electronic Auction Scheme Using Homomorphic Encryption." Proc. of ICISC2003, pp275-290, 2003.
8) Golle,P., Zhong,S., Boneh,D., Jakobsson,M., and Juels,A., "Optimistic Mixing for Exit-Polls." Asiacrypt2002, 2002.
9) Hirt,M., "Multi-Party computation: Efficient Protocols, General Adversaries, and Voting.", Ph.D. Thesis, ETH Zurich, Reprint as vol. 3 of ETH Series in Information Security and Cryptology, Hartung-Gorre Verlag, Konstanz, 2001.
10) Hirt,M and Sako,K., "Efficient receipt-free voting based on homomorphic encryption." Eurocrypt 2000, LNCS1807, pp539-556, 2000.
11) Juels,A., and Jakobsson,M., "Coercion-resistant Electronic Elections." *http://eprint.iacr.org/2002/165/* Nov, 2002.
12) Jakobsson,M., Juels,A., and Rivest,R., "Making mixnets robust for electronic voting by randomized partial checking." USENIX ' 02, 2002.
13) Juels,A., and Szydlo,M., "A Two-Server, Sealed-Bid Aucion Protocol." Proc. of Financial Cryptography2002, 2002.
14) Kikuchi,H., Harkavy,M., and Tygar,J.D., "Multi-round Anonymous Auction Protocols." Proc. of Third USENIX Workshop on Electronic Commerce, pp61-74, 1998.
15) Lee,B.C., and Kim,K.J., "Receipt-free electronic voting through collabo-ration of voter and honest verifier." Proc. of JW-ISC2000, pages 101 • 08, Jan. 25-26, 2000.
16) Lee,B.C., and Kim,K.J., "Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer." ICISC2002, vol.5, No.1 pp405-422, 2002.
17) Naor,M., Pinkas,B., and Summer,R., "Privacy Preserving Auctions and Mechanism Design." Proc. of ACM conference of E-commerce, pp129-139, 1999.
18) Okamoto,T., "Receipt-Free Electronic Voting Schemes for Large Scale Elections." Security Protocols Workshop, 1997.
19) Omote,K., and Miyaji,A., "An anonymous auction protocol with a single non-trusted center binary trees." Information security workshop-Proc. of ISW2000, LNCS 1975, Springer-Verlag, pp108-120, 2000.
20) Omote,K., and Miyaji,A., "An Anonymous Sealed-bid Auction with a Feature of Entertainment." Transactions of Information Processing Society of Japan, Vol.42, No.8, Aug. 2001.
21) Park,C., Itoh,K., and Kurosawa,K., "Efficient Anonymous Channel and All / Nothing Election Scheme." EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.
22) Peng,K., Boyd,D., Dawson,E., and Viswanathan,K., "Efficient Implementation of Relative Bid Privacy in Sealed-Bid Auction." WISA'03, LNCS2908, 2004.
23) Shamir,A., "How to share a secret." Communications of the ACM,22: pp612-613, 1979.
24) Sako,K., and Kilian,J., "Receipt -Free Mix-Type Voting Scheme." EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.