Secure E-Auction for Mobile Users with Low-Capability Devices in Wireless Network

Kun Peng

Secure E-Auction For Mobile Users With Low-Capability Devices In Wireless Network

Kun Peng

Institute for Infocomm Research

Abstract. The existing secure e-auction schemes are shown to be too costly for users using mobile devices in wireless network as they heavily depend on costly asymmetric cipher. A new secure e-auction efficient enough for devices with low computation capability and limited communication bandwidth is designed in this paper. Most of its operations are symmetric cipher computations and the only asymmetric cipher operations it needs for a bidder are several multiplications. With so high efficiency, its still achieves the normal security properties of secure e-auction.

1 Introduction

E-auction is a popular e-commerce application to distribute resources. In e-auction applications, the bids are often sealed for fairness and security. More precisely, the bidders seal their bids and submit them to one or more auctioneer, who then open the bids and determine the winner. In sealed-bid e-auction applications, the following security properties are usually desired.

- Correctness: the auction result is determined strictly according to the auction rule, while no bid is ignored or tampered with.
- Fairness: all the bidders make their unique choice at the bidding phase and cannot change their bids afterwards such that no bidder can take advantage over other bidders.
- Robustness: in abnormal situations (e.g. at presence of invalid bid), the auction can still run properly.
- Privacy: no secret information (e.g. the losing bid) except for the auction-result is revealed. More precisely, the auction transcript including all the published information in the auction can be simulated by a party without any secret knowledge but the auction result such that the simulating transcript is indistinguishable from the real auction transcript.
- Verifiability: operations of the bidders and the auctioneer(s) can be verified to detect invalid operations.

Usually, multiple auctioneers are employed to share the bid-opening capability such that if the number of malicious auctioneers is not over a threshold, the auction is guaranteed to be correct and private. An obvious solution to protect privacy in e-auction is secure multiparty computation (called secure evaluation

in [11]) as e-auction can be regarded as computation (evaluation) of some secret inputs (the bids) to obtain an output (the auction result). Secure-multiparty-computation-based solution to e-auction includes a few schemes [9, 5, 4, 3, 2, 8]. As analysed in [11][1], these schemes are not efficient as they employ general multiparty computation techniques designed to evaluate any function. In comparison, special techniques designed to handle e-auction only are usually more efficient. A very popular such method is homomorphic bid opening [6, 7, 1, 10, 14, 12, 11, 15]. With this mechanism, each bidder employs a homomorphic encryption algorithm or a homomorphic secret sharing algorithm to seal their bids, while the auctioneers exploit homomorphism of the encryption algorithm or secret sharing algorithm to open the bids collectively instead of separately so that no losing bid is revealed. Homomorphic e-auction schemes usually employ binary search to determine the winning bid and are more efficient than the e-auction schemes employing the costly downward search [17, 19, 20, 16, 13].

To the best of our knowledge, the existing secure e-auction schemes heavily depend on asymmetric cipher in bid sealing, bid opening and verification of validity. So attempts to improve their efficiency are limited by an unchangeable fact: asymmetric cipher operations like bid encryption and decryption and zero knowledge proof usually cost some exponentiations whose bases, exponents and multiplicative moduli are hundreds of bits long. Such exponentiations and large integers involved in them lead to much higher cost than symmetric cipher operations in both computation and communication and they are inevitable in asymmetric-cipher-based e-auction. So, the existing secure e-auction schemes are not suitable for applications with critical requirements on efficiency.

With the development of wireless network and mobile computation-and-communication devices like mobile phone and smart cards, more and more users of e-auction hope to bid using wireless mobile devices in a wireless network. Such devices usually have much lower computation capability and communication bandwidth than the normal computers in high-speed networks. So the existing secure e-auction schemes cannot meet this new trend in e-auction application. Therefore, if security cannot be compromised in e-auction of mobile users, a more efficient secure e-auction scheme needs to be designed.

The only solution to break the efficiency limit of the existing secure e-auction schemes and design efficient e-auction for mobile users using wireless mobile devices is replacing asymmetric cipher with symmetric cipher. A symmetric-cipher-based e-auction scheme is proposed in this paper. Most operations in it are based on symmetric cipher and the only asymmetric cipher operations for a bidder are several multiplications. No costly exponentiations in asymmetric cipher is needed. With such a strict requirement on efficiency, it still achieves the security properties desired in secure e-auction. Our new e-auction scheme is proposed in two steps. An unverifiable prototype is proposed in Section 2 and it is optimised to be verifiable in Section 4. The new e-auction scheme can

[1] It is shown in [11] that the most recent and efficient secure-multiparty-computation-based e-auction scheme [8] is less efficient than some homomorphic e-auction schemes.

be applied to auction applications with critical requirements on efficiency and mobile users can use it to bid in a wireless network.

2 An Unverifiable Prototype

The parameters and symbols used in our e-auctions schemes are as follows.

- There are m auctioneers $A_1, A_2, \ldots, A_m$ and n bidders $B_1, B_2, \ldots, B_n$.
- Integer t smaller than m is the trust threshold such that cooperation of at least t auctioneers is necessary to open any bid.
- The biddable prices are denoted as $P_1, P_2, \ldots, P_L$ in descending order.
- $E_k()$ and $D_k()$ denote the encryption algorithm and decryption algorithm using key k of a symmetric cipher like AES, where the key space, message space and cipher space of them is Z_δ.
- ρ is the largest prime no larger than δ.
- $H()$ is a one-way and collision-resistent hash function to map a long message to Z_ρ.
- $H'()$ is a one-way and collision-resistent hash function to map a long message to Z_δ.
- p_j and q_j are secret large primes chosen by A_j, who publishes $N_j = p_j q_j$. As a asymmetric cipher parameter, each N_j should be larger than any key of the symmetric cipher, which is s useful property.

The unverifiable e-auction protocol is as follows.

1. Initial Phase
   (a) Each B_i chooses $k_{i,j}$ for every A_j, the session key to communicate with A_j. He sends it to A_j in the form $(a_{i,j}, b_{i,j}) = (r_{i,j}^2 \bmod N_j,\ k_{i,j} \oplus H'(r_{i,j} \bmod N_j)$ where $r_{i,j}$ is randomly chosen from Z_{N_j}.
   (b) Each A_j calculates his session keys $k_{i,j} = b_{i,j} \oplus H'(a_{i,j}^{1/2}) \bmod N_j$ for $i = 1, 2, \ldots, n$ using his knowledge of p_j and q_j.
2. Bidding and bid opening
   The auctioneers cooperate to run a binary search for the winning price among the biddable prices. The binary search starts at $P_{L/2}$ and the auctioneers test whether there is any bidder willing to pay that price. If there is, the search goes on to the higher prices; otherwise it goes on to the lower prices. Next search step is just like the previous one, starting in the middle and going on to one side. As the binary search goes on, the searched range of prices becomes smaller and smaller and finally the search ends at the highest price any bidder is willing to pay. The search at a price P_l on the binary searching route is as follows.
   (a) Each B_i chooses his bid at that price: $b_{i,l}$. If he is willing to pay P_l, $b_{i,l}$ is random positive integer in Z_ρ; otherwise it is zero.
   (b) Each B_i builds a polynomial $f_{i,l}(x) = \sum_{j=0}^{t-1} \alpha_{i,l,j} x^j \bmod \rho$ where $\alpha_{i,l,0} = b_{i,l}$ and $\alpha_{i,l,j}$ for $j = 1, 2, \ldots, t-1$ are random integers chosen from Z_ρ.

(c) Each B_i sends every A_j an encrypted bid share $c_{i,l,j} = E_{k_{i,j}}(f_{i,l}(j))$.
(d) Any t auctioneers can cooperate to calculate the sum of the all the bids at P_l as follows where the set of the indices of the participating auctioneers are denoted as S.
   i. Each A_j calculates $s_{j,l} = \sum_{i=1}^{n} D_{k_{i,j}}(c_{i,l,j}) \bmod \rho$.
   ii. The auctioneers cooperate to calculate $s_l = \sum_{j \in S} s_{j,l} u_j \bmod \rho$ where $u_j = \prod_{k \in S, k \neq j} k/(k-j) \bmod \rho$.
(e) If $s_l > 0$, the search goes to the higher prices; otherwise it goes to the lower prices. Finally, the binary search stops at a price P_L, which is the winning price.

3. Winner identification
The auctioneers opens all the bids at P_L

$$b_i = \sum_{j \in S} s_{i,L,j} u_j \bmod \rho \text{ for } i = 1, 2, \ldots, n.$$

A bidder B_i is a winner if $b_i > 0$. If there is only one winner, he wins the auction. If there are multiple winners, the final winner is determined according to a tie-breaking algorithm. Depending on the concrete auction application, the tie-breaking algorithm may differ. For example, it may employ the first-come-first-win strategy or ask the winners to bid again in a new round of auction.

This prototype is called Protocol 1. It actually employs Shamir's threshold secret sharing based on a polynomial [18] to share the bids among the auctioneers. When the auctioneers and the bidders are honest, Protocol 1 can work and the correct winning price and winner can be found as illustrated in Theorem 1, which is based on homomorphism of polynomial-based threshold secret sharing defined in Definition 1.

Definition 1 *In Shamir's threshold secret sharing, suppose* $\beta_{1,1}, \beta_{1,2}, \ldots, \beta_{1,m}$ *are shares of* β_1 *and* $\beta_{2,1}, \beta_{2,2}, \ldots, \beta_{2,m}$ *are shares of* β_2. *Then* $\beta_{1,1} + \beta_{2,1}, \beta_{1,2} + \beta_{2,2}, \ldots, \beta_{1,m} + \beta_{2,m}$ *are shares of* $\beta_1 + \beta_2$. *More generally, if* $\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,m}$ *are shares of* β_i *for* $i = 1, 2, \ldots, n$, *then* $\sum_{i=1}^{n} R_i\beta_{i,1}, \sum_{i=1}^{n} R_i\beta_{i,2}, \ldots, \sum_{i=1}^{n} R_i\beta_{i,m}$ *are shares of* $\sum_{i=1}^{n} R_i\beta_i$ *where* R_i *is any integer.*

Theorem 1. *In Protocol 1, if the bidders and auctioneers are honest, with an overwhelmingly large probability* s_l *is non-zero if and only if there is at least one bidder willing to pay* P_l.

In Protocol 1, all the bids are shared among the auctioneers and every share is encrypted. So no losing bid is revealed if the employed encryption algorithm is secure and the number of malicious auctioneers is smaller than t. So correctness of auction is achieved in Protocol 1 when the auctioneers and bidders are honest and its privacy is achieved under a threshold thrust assumption. For each bidder, the only operations in asymmetric cipher are m instances of session key

distribution, each costing a square. For each auctioneer, the only operations in asymmetric cipher are n instances of session key extraction, each calculating a square root. All the other operations are efficient symmetric cipher operations. Moreover, most of the integers transfered in the communication of Protocol 1 are ρ-bit integers used in symmetric cipher, which are much shorter and cost much less communication than the integers used in the asymmetric-cipher-based e-auction schemes. So high efficiency is achieved in Protocol 1 and it can be applied to mobile bidders with limited computation capability and communication bandwidth. However, when there are dishonest auctioneers and bidders, they can break robustness of Protocol 1 using the attacks described in Section 3.

3 Attacks by Dishonest Auctioneers and Bidders

As the operations of neither the auctioneers nor the bidders are verified in Protocol 1, they may deviate from Protocol 1 and launch some attacks. An obvious attack is for a malicious auctioneer to tamper with the bid shares to lead the auction to an incorrect result. For example, at a price P_l which no bidder is willing to pay, a malicious auctioneer A_j can publish a random $s_{j,l}$ in Z_ρ. As $s_{j,l}$ is randomly distributed in Z_ρ, the secret reconstructed from t shares including it, namely the opened sum of bids at P_l, is non-zero with a probability $1 - 1/\rho$, while the sum of the bids at P_l should be zero as every bidder submits zero at that price to indicate their unwillingness to pay. Under this attack, the auctioneer will declare a winning price higher than the highest bid and cannot find any winner at the that price, and so the auction fails. In this attack, the malicious auctioneer have some other options. For example, he can tamper with the bid share of a bidder at P_l as well to help the bidder to change his bid and win the auction. Moreover, the malicious auctioneer can use a changed bid share to make s_l discovered as zero in secret reconstruction while there is some positive bid at P_l.

One or more dishonest bidder can attack Protocol 1 as well. For example, a malicious bidder may submit a set of inconsistent shares to the auctioneers such that some subsets containing t of them hold shares of zero and some subsets containing t of them hold shares of an positive integer. Usually this attack happens at a high price and a malicious bidder can carry it out as follows to break fairness of the auction.

1. The malicious bidder expects that he can win an auction by bidding P_μ, while the highest price he is willing to pay is a higher price P_ν.
2. He submits his bids at all the prices normally except at P_ν. More precisely, he submits and shares a positive integer at the prices no higher than P_μ and zero at the prices higher than P_μ except for P_ν, while at P_ν, he shares zero among some auctioneers and positive integers among other auctioneers.
3. If the malicious bidder wins the auction at P_μ (e.g. P_ν is not on the binary search route or the auctioneers carrying out bid opening at P_ν get shares of zero from the malicious bidder), the malicious bidder does nothing. If P_μ is not high enough and another bidder submits a positive bid at a price higher

than P_μ, the malicious bidder can dispute the auction result and claim his winning at P_ν. More precisely, if P_ν is higher than the other bidders' positive bids, the malicious bidder claims winning at P_ν and ask the auctioneers sharing zero from him to carry out bid opening at P_ν to recover the malicious bidder's positive bid.

Even if this attack can be detected afterwards and the malicious bidder may be punished, this attack is still harmful as it makes the auction liable to two possible auction results depending on which t auctioneers participate bid opening. Actually, malicious bidders have more options in their attacks, some of which are even simpler and more effective. For example, two malicious bidders can even attack Protocol 1 without collusion of any auctioneer to break its fairness as follows.

1. Two colluding bidders B_μ and B_ν submit and share among the auctioneers d and $\rho - d$ respectively at the highest price they are willing two pay. At other biddable prices, they bid normally (e.g. only submitting non-zero bids at the prices no higher than their expectation of winning bid).
2. After bid opening, if either B_μ or B_ν wins, they accept the auction result and do nothing. If another bidder wins at a price lower than the highest price they are willing two pay, they claim winning and publish their bids at the highest price they are willing two pay to prove their claim.

The two attacks by malicious bidders allow them to win the auction at a price as low as possible while keeping their right to win at a higher price when being challenged by other bidders. This obviously violate fairness of sealed-bid auction, which does not allow any bidder change or choose his bid after bid submission. The attacks in this section shows that robustness of protocol is weak.

4 Verifiable E-Auction for Capability-Limited Mobile Bidders

If the operations of the auctioneers and bidders are verified, the attacks in Section 3 can be prevented. So Protocol 1 can be optimised into a verifiable e-auction protocol to achieve stronger robustness. Of course, high efficiency and suitability for mobile bidders with limited computation capability and communication bandwidth cannot be compromised. More precisely, costly asymmetric cipher operations like zero knowledge proof cannot be adopted in the optimisation. Our optimisation employs several efficient verification mechanisms to detect dishonest behaviours of the bidders or auctioneers. Firstly, the shares of the bids are verified by the auctioneers to guarantee their validity and consistency. More precisely, besides the bid another random integer is shared at every biddable price by each bidder among the auctioneers and the two sets of shares are randomly combined such that validity of the combined shares can guarantee validity of the bid shares with an overwhelmingly large probability. Secondly, the bids from all the bidders are randomized before they are summed up such that no matter

how the bidders choose the integers in their bids, the sum of the randomized bids at any price is zero if and only if all the bids at that price are zeros with an overwhelmingly large probability. Thirdly, bid opening is verified against the public commitments of the bidders about their bids such that cheating auctioneers carrying out invalid bid opening can be detected with an overwhelmingly large probability except that all the auctioneers participating in bid opening are dishonest. The optimised e-auction protocol is described in details in the following.

1. Initial phase is not changed and the session keys $k_{i,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ are exchanged between the bidders and auctioneers.
2. Bidding and bid opening
   The auctioneers cooperate to run a binary search for the winning price among the biddable prices like in Protocol 1. The search at a price P_l on the binary searching route is as follows.
   (a) Each B_i chooses his bid at that price: $b_{i,l}$. If he is willing to pay P_l, $b_{i,l}$ is random positive integer in Z_ρ; otherwise it is zero.
   (b) Each B_i builds a polynomial $f_{i,l}(x) = \sum_{\kappa=0}^{t-1} \alpha_{i,l,\kappa} x^\kappa \bmod \rho$ where $\alpha_{i,l,0} = b_{i,l}$ and $\alpha_{i,l,\kappa}$ for $\kappa = 1, 2, \ldots, t-1$ are random integers chosen from Z_ρ.
   (c) Each B_i builds a polynomial $g_{i,l}(x) = \sum_{\kappa=0}^{t-1} \gamma_{i,l,\kappa} x^\kappa \bmod \rho$ where $\gamma_{i,l,\kappa}$ for $\kappa = 0, 1, \ldots, t-1$ are random integers chosen from Z_ρ.
   (d) Each B_i publishes encrypted bid shares $c_{i,l,j} = E_{k_{i,j}}(f_{i,l}(j))$ for $j = 1, 2, \ldots, m$.
   (e) Each B_i publishes another set of encrypted shares $c'_{i,l,j} = E_{k_{i,j}}(g_{i,l}(j))$ for $j = 1, 2, \ldots, m$.
   (f) $w_{i,l} = H(c_{i,l,1}, c_{i,l,2}, \ldots, c_{i,l,m}, c'_{i,l,1}, c'_{i,l,2}, \ldots, c'_{i,l,m})$ for $i = 1, 2, \ldots, n$ are challenges to validity of bidding and bid opening.
   (g) Each B_i publishes $\phi_{i,l,j} = w_{i,l}\alpha_{i,l,j} + \gamma_{i,l,j} \bmod \rho$ for $j = 0, 1, \ldots, t-1$.
   (h) Each A_j verifies that his share from B_i is valid as follows.
      i. He calculates $s_{i,l,j} = D_{k_{i,j}}(c_{i,l,j})$.
      ii. He calculates $s'_{i,l,j} = D_{k_{i,j}}(c'_{i,l,j})$.
      iii. He verifies

$$w_{i,l} s_{j,l,j} + s'_{j,l,j} = \sum_{\kappa=0}^{t-1} \phi_{i,l,\kappa} j^\kappa \bmod \rho. \tag{1}$$

      If the verification fails, A_j claims that B_i has sent him an invalid bid share. He publishes $k_{i,j}$, $s_{i,l,j}$ and $s'_{i,l,j}$ such that any one can verify failure of (1) and that $s_{i,l,j}$ and $s'_{i,l,j}$ are shares sent to A_j by B_i. This public verification can detect dishonest bidders, who are kicked out and their bids are deleted.
   (i) After the shares are verified and only valid shares are kept, any t auctioneers can cooperate to calculate the sum of the all the bids at P_l as follows where the set of the indices of the participating auctioneers are denoted as S.
      i. Each auctioneer A_j in S calculates $s_{j,l} = \sum_{i=1}^{n} w_{i,l} s_{i,l,j} \bmod \rho$.

ii. Each auctioneer A_j in S calculates $s'_{j,l} = \sum_{i=1}^{n} s'_{i,l,j} \bmod \rho$.
iii. Each auctioneer A_j in S publishes $S_{j,l} = H(s_{j,l}, s'_{j,l})$.
iv. After $S_{j,l}$ for $j = 1, 2, \ldots, m$ are published, each auctioneer A_j in S publishes $s_{j,l}$ and $s'_{j,l}$.
v. It is publicly verified $S_{j,l} = H(s_{j,l}, s'_{j,l})$ for $j = 1, 2, \ldots, m$. Any auctioneer failing to pass the verification is required to publish $s_{j,l}$ and $s'_{j,l}$ again. Any auctioneer cannot provide correct $s_{j,l}$ and $s'_{j,l}$ is replaced by one of the $n - t$ stand-by auctioneers.
vi. $s_l = \sum_{j \in S} s_{j,l} u_j \bmod \rho$ and $s'_l = \sum_{j \in S} s'_{j,l} u_j \bmod \rho$ are calculated where $u_j = \prod_{k \in S, k \neq j} k/(k - j) \bmod \rho$.
vii. I can be publicly verified

$$s_l + s'_l = \sum_{\kappa=0}^{t-1} (\sum_{i=1}^{n} \phi_{i,l,\kappa}) j^{\kappa} \bmod \rho. \quad (2)$$

The auction continues only if the verification is passed. If the verification fails, another set of t auctioneers is selected to carry out bid opening. If at least t auctioneers are honest, correct bid opening is obtained.

(j) If $s_l > 0$, the search goes to the higher prices; otherwise it goes to the lower prices. Finally, the binary search stops at a price P_L, which is the winning price.

3. Winner identification is not changed and all the bids at the winning price are opened to identify the winner(s).

This optimised e-auction protocol is called Protocol 2. It can detects dishonest behaviours of bidders and auctioneers and achieve robustness. Theorem 2, Theorem 3 and Theorem 4 illustrate that invalid operations in bidding and bid opening in Protocol 2 can be detected by the receiving auctioneer. More precisely, Theorem 2 shows that invalid bid sharing by any malicious bidder can be detected by the auctioneers with an overwhelmingly large probability; Theorem 3 shows that no matter how the bidders choose the integers in their bids the auction result is correct with an overwhelmingly large probability if the auctioneers carries out bid opening honestly; Theorem 4 shows that invalid bid opening operation can be detected with an overwhelmingly large probability.

Theorem 2. *If (1) is satisfied for a bidder B_i with a probability larger than $1/\rho$ at a price P_l, any share $s_{i,j,l}$ from that B_i at the price P_l is guaranteed to be the j^{th} share generated by a unique polynomial.*

Theorem 3. *If the auctioneers follow Protocol 2 to recover s_l, $s_l = 0$ iff $b_{1,l}, b_{2,l}, \ldots, b_{n,l}$ are all zeros with an overwhelmingly large probability.*

Theorem 4. *Unless all the t auctioneers in S are dishonest, satisfaction of (2) with a non-negligible probability guarantees that the auctioneers strictly follow Protocol 2 to recover s_l.*

All the additional verification operations in Protocol 2 are symmetric cipher operations, which are efficient in both computation (using simple calculation)

and communication (transferring short integers). So they do not increase cost of the e-auction scheme significantly. Therefore, like Protocol 1, Protocol 2 is an efficient e-auction protocol suitable for mobile users with limited computation capability and communication bandwidth.

5 Conclusion

The secure e-auction scheme proposed in this paper satisfies the desired security properties in e-auction and is very efficient. Most of its operations only involve symmetric cipher so are efficient in both computation and communication. The only asymmetric cipher operations needed in the new e-auction scheme are several squares for a bidder and some calculation of square root using knowledge of factorization of multiplicative modulus for an auctioneer. In comparison, the existing secure e-auction schemes [9, 5, 4, 3, 2, 8, 17, 19, 20, 16, 13, 6, 7, 1, 10, 14, 12, 11, 15] cost a lot of modulo exponentiations in asymmetric cipher operations for both the bidders and auctioneers and transfer large integers used in asymmetric cipher. So our e-auction scheme is especially suitable for e-auction schemes requiring both strong security and high efficiency like e-auction in wireless network with mobile users who use mobile wireless devices with limited computation capability and communication bandwidth.

References

1. Masayuki Abe and Koutarou Suzuki. M+1-st price auction using homomorphic encryption. In *Public Key Cryptology 2002*, volume 2288 of *Lecture Notes in Computer Science*, pages 115–124, Berlin, 2002. Springer-Verlag.
2. Christian Cachin. Efficient private bidding and auctions with an oblivious third party. In *the 6th ACM Conference on Computer and Communications Security*, 1999. Also available as `http://www.tml.hut.fi/~helger/crypto/link/protocols/auctions.html`.
3. Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. Multiparty computation from threshold homomorphic encryption. In *EUROCRYPT '01*, volume 2045 of *Lecture Notes in Computer Science*, pages 280–299, Berlin, 2001. Springer.
4. M Jakobsson and A Juels. Mix and match: Secure function evaluation via ciphertexts. In *ASIACRYPT '00*, volume 1976 of *Lecture Notes in Computer Science*, pages 143–161, Berlin, 2000. Springer-Verlag.
5. A. Juels and M. Szydlo. A two-server, sealed-bid auction protocol. In *The Sixth International Conference on Financial Cryptography 2002*, volume 2357 of *Lecture Notes in Computer Science*, pages 72–86, Berlin, 2002. Springer-Verlag.
6. H Kikuchi, Michael Harkavy, and J D Tygar. Multi-round anonymous auction. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, June 1998.
7. Hiroaki Kikuchi, Shinji Hotta, Kensuke Abe, and Shohachiro Nakanishi. Distributed auction servers resolving winner and winning bid without revealing privacy of bids. In *proc. of International Workshop on Next Generation Internet (NGITA2000), IEEE*, pages 307–312, July 2000.

8. Kaoru Kurosawa and Wakaha Ogata. Bit-slice auction circuit. In *7th European Symposium on Research in Computer Security, ESORICS2002*, volume 2502 of *Lecture Notes in Computer Science*, pages 24–38, Berlin, 2002. Springer-Verlag.
9. Moni Naor, Benny Pinkas, and Reuben Sumner. Privacy perserving auctions and mechanism design. In *ACM Conference on Electronic Commerce 1999*, pages 129–139, 1999.
10. Kazumasa Omote and Atsuko Miyaji. A second-price sealed-bid auction with the discriminant of the p-th root. In *Financial Cryptography 2002*, volume 2357 of *Lecture Notes in Computer Science*, pages 57–71, Berlin, 2002. Springer.
11. Kun Peng, Colin Boyd, and Ed Dawson. A multiplicative homomorphic sealed-bid auction based on Goldwasser-Micali encryption. In *ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 374–388, Berlin, 2005. Springer-Verlag.
12. Kun Peng, Colin Boyd, and Ed Dawson. Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing. In *Mycrypt 2005*, volume 3715 of *Lecture Notes in Computer Science*, pages 84–98, Berlin, 2005. Springer-Verlag.
13. Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Non-interactive auction scheme with strong privacy. In *5th International Conference of Information Security and Cryptology - ICISC 2002*, volume 2587 of *Lecture Notes in Computer Science*, pages 407 – 420, Berlin, 2002. Springer.
14. Kun Peng, Colin Boyd, Ed Dawson, and Kapali Viswanathan. Robust, privacy protecting and publicly verifiable sealed-bid auction. In *4th International Conference of Information and Communications Security, ICICS 2002*, volume 2513 of *Lecture Notes in Computer Science*, pages 147 – 159, Berlin, 2002. Springer.
15. K Peng and F Bao. Efficiency improvement of homomorphic e-auction. In *TRUSTBUS '10*, *LNCS6264*, pages 238–249.
16. K Sako. An auction scheme which hides the bids of losers. In *Public Key Cryptology 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 422–432, Berlin, 2000. Springer-Verlag.
17. Kouichi Sakurai and S Miyazaki. A bulletin-board based digital auction scheme with bidding down strategy -towards anonymous electronic bidding without anonymous channels nor trusted centers. In *Proc. International Workshop on Cryptographic Techniques and E-Commerce*, pages 180–187, Hong Kong, 1999. City University of Hong Kong Press.
18. A Shamir. How to share a secret. *Communication of the ACM*, 22(11):612–613, Nov 1979.
19. Koutarou Suzuki, Kunio Kobayashi, and Hikaru Morita. Efficient sealed-bid auction using hash chain. In *International Conference on Information Security and Cryptology 2000*, volume 2015 of *Lecture Notes in Computer Science*, pages 183–191, Berlin, 2000. Springer-Verlag.
20. Yuji Watanabe and Hideki Imai. Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp. In *STOC 2000*, pages 80–86. ACM, 2000.