Securing Electronic Bidding System with Self-healing Broadcast Encryption Scheme

Fengjun Kang, Mingming Chen, Bo Chen

College of Computer Science, Zhejiang University of Technology, Hangzhou, China

lingguang502a@126.com, naivechen@foxmail.com, cb@zjut.edu.cn

Keywords: Electronic bidding, bilinear pairing, self-healing, group key distribution

Abstract. Electronic bidding system has become an increasingly popular method for transacting business, especially over the Internet. A self-healing key distribution scheme enables a group of users to establish a group key over an unreliable channel. We propose a group key distribution scheme with self-healing feature to suitable internet context. With this scheme, a group of colluding bidders cannot control the contract price arbitrarily and all bidders are never revealed to anyone, while the other losers can verify the fact that the winner belongs to their group. The bidder can recover the result message which has been lost.

Introduction

Electronic bidding system has become an increasingly popular method for transacting business, especially over the Internet. Communication between bidders usually is forbidden to prevent collusions (i.e., through separate compartments and supervision). We investigate these auctions from the cryptographic point of view and identify that the usual implementation by a succession of (traditional) sealed-bid auctions. The auctioneer announces at least the winner and winning bid of each round offers a covert channel to the bidders. The announcement should be limited to the minimum a bidder needs to know for taking part in the next round. We suggest that the bids made are kept private and he only gets to know which items he currently wins. Only at the end, overall winners and winning bids are revealed[1].

Our scheme uses self-healing group key distribution to construct a relatively efficient secure multicast model,which is revoverability of lost message and using the broadcast to update the keys when the members change dynamically.

The property of an ideal electronic auction. As is known, with public-key cryptographic techniques, auction scheme should satisfy the following requirements.

(i)Secrecy of bidding price: All bidding prices except the contract price are never revealed to anybody. the service center can't figure out the price before receives all legal standard price. The ideal condition is only the winner's price can be disclosed when the auction finishes.

(ii)Validity of the successful bid: The bidders submit their bid price after the auction announced the start of an auction. The price of the successful bid is the highest one among all bidding prices.

(iii)Fairness: Nobody can get any advantage than the other bidders.

(iv)Keep bidders' identity secret: The identities of the bidders in the auction can't be leaked. Only the winner's identity can be published, while the others can verify if the winner belongs to their registered group.

Overview of Our Approach.

Bidder: The user who is interested in the items on sale and take part in auction.

Auction house: It plays the role of a KGC and in charge of the whole process of each auction, including distribution system parameters, accept the bidder's registration, verify winner's identity after the auction.

Auctioneer: It computes who is the winner after receives the bid messages of the bidders, then broadcast the winning message.

The process of our auction scheme is that each bidder u$_i$ gets bidder's personal key after getting registration from the auction house, when the auction start, each bidder uses personal key to encrypt his own bidding message and send it to auctioneers. The auctioneer start to compute the highest price, at the end of auction, it broadcast the highest price and winner's serial-number. The losers can recognize the winner belongs to the advanced registered group. If a bidder lost the broadcast, it can recover the message which he need by using another broadcast without requesting to the auctioneer for once more broadcast.

Preliminaries

Bilinear Pairings. Let G_1 and G_2 be two cyclic groups of prime order p . G_1 is a cycle additive group and G_2 is a cycle multiplicative group. We assume that is a generator of G_1 .Let g is a generator of G_1 .Let $e: G_1 \times G_1 \rightarrow G_2$ be a function that has the following properties:

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

②Non-degenerate: $e(g,g) \neq 1$.

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

Definiton: Let $U = \{u_1,...,u_n\}$ and $j \in \{1,...,m\}$.

. **Session key distribution:** The scheme is a session key distribution with privacy if, for any member u_i , the session key K_j is determined by broadcast B_j and the private key d_i .what member u_i learn from B_j cannot be determined from broadcasts or personal key alone.

Revocation capability: For each session j and $R_j \subseteq \{u_1,...,u_n\}$ GM can generate a broadcast message B_j such that for all $u_i \notin R_j$ can efficiently recover the session key K_j , but the revoked members in R_j cannot recover any of the keys in sessions $1,...,j$.

Self-healing: for any r , $1 \leq r < j \leq m$: For any member $u_i \in G_r$ who is also a member in session j, the session key K_j is determined by broadcast B_j and the private key d_i .

An Electronic Bidding Scheme

We propose a new auction protocol such that only the auction house can recognize the winner's identity, whereas the other losers can verify the fact that the winner exists in the advanced registered group.

Registration. Auction house firstly checks in the merchandise and list their serial number in order, let m be the total number and the subset of the merchandises denoted by $P = \{p_1,..., p_m\}$,for the merchandise $p_j (1 < j < m)$ has its corresponding public-key $K_j = e(w, g_j)^s \in G_1$,the bidders must send their ID to auction house for registration and the registry marked the bidders' serial number ,let n be the total number of the bidders and the subset of the bidders denoted by $S = \{u_1,...,u_n\}$ .The bidders submit their own identify ID_i to registration authority. Registration authority computes $Q_\mathrm{i} = H_1(ID_i)$,let G_1 be a bilinear group of prime order p ,it picks $h, w \in G_1$,next it picks a random $s, x \in \mathbb{Z}_p$,it issues the $d_i = w \bullet h^{\frac{1}{(x+i)}} \in G_1$ as the bidder u_i 's individual private key, and $D_i = e(d_i, Q_i)$ be its corresponding u_i 's individual public-key to corresponding ciphertext with auctioneer, The registration authority send (d_i, Q_i) to u_i and $(K_j(1 < j < m), D_i(1 \leq i \leq n))$ to the auctioneer use a secret channel.

Bidding process. This process can divided into four procedures: broadcast, decryption, self-healing,adding and revoking node.

. **Broadcast.** The bidder firstly confirms his own message of $m_i = \{product_j, time, price(p_j) \| ...\}$,and encrypts this message $C_{m_i} = m_i \oplus H_2(e(d_i, Q_i))$,then send this encrypted message C_{m_i} to the auctioneer. The auctioneer extracts information through using individual public-key $D_i (1 \le i \le n)$,statistics the message from each bidder, and classifies them by the item's id. The auctioneer computes the winner of item $\mathrm{p}_j (1 < j < m)$, generates the message $M_j = \{product_j, winner\_price, winner\_number\}$ and picks j-th session key K_j as broadcast key to broadcast from auctioneer to the bidder group in which all bidders are bidding for the same j-th item. Suppose the $|S_j|$ denotes the number of the bidders who has bided for the j-th item. For each session $1 \le j \le m$, according to the session group G_j,for a random $g_j \in G_1$,set $C_{M_j} = H(K_j) \oplus M_j$,$U_i = g_j^{\frac{1}{(x+i)}} (1 \le i \le |S_j|)$, $HA_j = (\mathrm{h} \prod_{j \in S_j} U_j)^s$, $HB_j = (g_j)^s$.Let $z_j = (x, S_j, U_i (1 \le i \le |S_j|), HA_j, HB_j, C_{M_j})$.The ciphertext for the j-th broadcast is in the following form: $B_j = \{z_1, ..., z_j\}$.

Decryption. Suppose bidder u_i belongs to S_j,and he receives the broadcast message B_j,it can decrypt the M_j as long as he has bid to the j-th item by using his private key d_i as follows:

$$
\begin{aligned}
& C_{M_j} \oplus H_2\Big(\frac{e(d_i \bullet (\prod_{k \in S_j} U_k)^{\frac{1}{(x+i)}}, HB_j)}{e(HA_j, U_i)}\Big) \\
&= C_{M_j} \oplus H_2\Big(\frac{e(w \bullet h^{\frac{1}{(x+i)}} \bullet \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)(x+i)}}, (g_j)^s)}{e((\mathrm{h} \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^s, (g_j)^{\frac{1}{(x+i)}})}\Big) \\
&= C_{M_j} \oplus H_2\Big(\frac{e(w, g_j)^s \bullet e(h^{\frac{1}{(x+i)}} \bullet \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)(x+i)}}, (g_j)^s)}{e((\mathrm{h} \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^s, (g_j)^{\frac{1}{(x+i)}})}\Big) \\
&= C_{M_j} \oplus H_2\Big(\frac{e(w, g_j)^s \bullet e((h \bullet \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^{\frac{1}{(x+i)}}, (g_j)^s)}{e((\mathrm{h} \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^s, (g_j)^{\frac{1}{(x+i)}})}\Big) \\
&= C_{M_j} \oplus H_2\Big(\frac{e(w, g_j)^s \bullet e((h \bullet \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^s, (g_j)^{\frac{1}{(x+i)}})}{e((\mathrm{h} \prod_{k \in S_j} (g_j)^{\frac{1}{(x+k)}})^s, (g_j)^{\frac{1}{(x+i)}})}\Big) \\
&= C_{M_j} \oplus H_2(e(w, g_j)^s) \\
&= C_{M_j} \oplus H_2(K_j) \\
&= M_j
\end{aligned}
$$

Self-healing. Suppose u_i lost the broadcast message for a session $t < j$.As far as it belongs to the session group G_t,it picks up the polynomial z_t from the broadcast B_j and it can get the message M_t as follows:

$$
\begin{aligned}
&C_{M_t} \oplus H_2\left(\frac{e(d_i \bullet (\prod_{k\in S_t} U_k)^{\frac{1}{(x+i)}}, HB_t)}{e(HA_t, U_i)}\right) \\
&= C_{M_t} \oplus H_2\left(\frac{e(w \bullet h^{\frac{1}{(x+i)}} \bullet \prod_{k\in S_t} (g_t)^{\frac{1}{(x+k)(x+i)}}, (g_t)^s)}{e((\mathrm{h} \prod_{k\in S_t} (g_t)^{\frac{1}{(x+k)}})^s, (g_t)^{\frac{1}{(x+i)}})}\right) \\
&= C_{M_t} \oplus H_2(K_t) \\
&= M_t
\end{aligned}
$$

Adding and revoking node. If a new user u_{new} applies for joining the session j ,GM checks the validity of its identity firstly, then give an private key d_{new} to this group member via a secure communication channel between them. If a user u_{rov} is revoked from the session j ,the GM delete the number which u_{rov} belongs to and delete U_{rov} in session j .

The bidder can verifty if he is win after encrypting the message, the winner should use what he got from the auction house to prove his identity to the auction house ,the registration authority check it, the winner should pay for the item by that price he has bidden after get passed.

Security analysis

Forward and backward secrecy: It used to prevent a revoked user from continued accessing the session key even if it keeps receiving the broadcast messages or a new user from decoding messages broadcasted before it joins the group. Whether member u_i joins after the session or revoked before the session j , GM can't generate a U_i ,so the member can't decrypt the session key K_j .

Collusion resistance: The collaboration of the newly joined users and revoked users are not be able to recover the session keys which they are not entitled to. This is a strong and practical security requirement.

Conclusions

We have developed a new electronic bidding system using self-healing group key distribution in broadcast mode, which allows bid over the Internet through an Android Smartphone. Our protocol based on bilinear pairings for achieving lower overhead, lower overhead to communication by self-healing than other electronic bidding protocols. The scheme with strong anonymity and bidding privacy, it's very difficult for adversary to steal any secret values from network.

References

[1] Sakurai K, Miyazaki S. An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme[J]. Lecture Notes in Computer Science, 2000:385-399.

[2] D. Boneh,C.Gentry. Collusion resistant broadcast encryption with short ciphertexts and private keys.Advances in Cryptology-CRYPTO 2005,LNCS,vol. 3621, Springer-Verlag (2005), pp.258-275.

[3] Tian B, Han S, Hu J, et al. A mutual-healing key distribution scheme in wireless sensor networks[J]. Journal of Network and Computer Applications, 2011, 34(1): 80-88..

[4] Y. Dodis, N. Fazio. Public key broadcast encryption for stateless receiver. DRM Workshop 2002, LNCS, vol. 2696, Springer-Verlag (2002), pp. 61 – 80.

[5] MJ Li, JST Juan, JHC Tsai. Practical electronic auction scheme with strong anonymity and bidding privacy.[J]. Information Sciences, 2011, 181(12):2576-2586.

[6] Staddon J, Miner S, Franklin M, et al. Self-healing key distribution with revocation. Proceedings of IEEE Symposium on Research in Security and Privacy. pp. 241 - 257. May 2002.