Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 3051 – 3057

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineeringand Information Science

An Electronic Auction Scheme Based on Group Signatures and Partially Blind Signatures

DING Yong[a], *Li Bin*[a], *Zheng Zhaoxia*[*b]

[a]*School of Mathematics and Computation Science,Guilin University of Electronic Technology, Guangxi, 541004, China*
[b]*Department of Electronic Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China*

Abstract

A new electronic auction scheme is proposed based on group signatures and partially blind signatures. At the same security strengthen, an optimization was done on the processes of electronic auction scheme and the dependence on trusted third party was reduced, moreover, multiple goods is auctioned at the same time, therefore, this scheme suited to large-scale electronic auction. Furthermore, due to application of vickrey auctions, the principle of optimal allocation of goods is easily satisfied.

Keywords: group signatures; partially blind signatures; electronic auction; trusted third party; vickrey auction

1. Introduction

Electronic auction which is one of the most important parts of electronic commerce is an electronic method of traditional auction. There are many types of auction categories [1], the sealed bid auction which is used as the electronic auction and the open bid auction according to whether the price is opened, the single-round and the multi-round auction according to the number of rounds at the auction, the first-price auction and the vickrey auction according to the price of winning.

Group signature [2] was firstly presented by Chaum and Heyst, which have anonymity, correctness, unforgeability, traceability, exculpability, unlinkability and other properties, so it constructed electronic auction scheme in [3-7]. Blind signature [8] which has been widely used on the confidentiality of message was firstly presented by Chaum in 1982 and partially blind signature [9] which can share parts of public

doi:10.1016/j.proeng.2011.08.572

information between users and signer compared with blind signature firstly presented by Abe and Fujsaki in 1982. After compared with other blind and partially blind signature protocols, Okamoto proposed his own protocol[10]. In the paper, we proposed based on group signature and partially blind signature, On the basis of safety and efficiency of the electronic auction scheme based on group signatures, an optimization was done on the new scheme. It didn't verify the identity of each bidder previous to the auction, however, in order to protect privacy of the successful bidder, we just verified the identity of successful bidder after the auction. Owing to reduce reliance on trusted third party, moreover, multiple goods are auctioned at the same time, therefore, this scheme suited to large-scale electronic auction. Furthermore, due to application of vickrey auctions on the two auction schemes in this thesis, the principle of optimal allocation of goods is easily satisfied, so it is more practical.

2. Background and Preview

2.1. Okamoto partially blind signature protocol

Let (G_1, G_2) be bilinear paring, we also assume that the message m, to be partially blindly signed is an element in Z_p^*, which is sharing message between user U and signer S, and m_1 is user message.

1. Key generation: Randomly select generators $g_2, u_2, v_2, h_2 \in G_2$ and set $g_1 = \psi(g_2)$, $u_1 = \psi(u_2)$, $v_1 = \psi(v_2)$ and $h_1 = \psi(h_2)$. Randomly select $x \in Z_p^*$ and compute $\omega_2 = g_2^x (g_2^x \in G_2)$. The public and secret keys are:

Public key: $g_1, g_2, u_2, v_2, h_2, \omega_2$

Secret key: x

2. Partially blind signature generation: Signer S and user U agree on common information m_0 in a predetermined way. user U randomly selects $s, t \in Z_p^*$, computes

$$X = h_1^{m_0 t} g_1^{m_1 t} u_1^t v_1^{st}$$

and sends X to S. Here, m_1 is the message to be blindly signed along with common information m_0. In addition, U proves to S that U knows $(t, m_1 t, t, st)$ for $X = h_1^{m_0 t} g_1^{m_1 t} u_1^t v_1^{st}$ using the witness indistinguishable proof as follows:

(1) U randomly selects a_1, a_2, a_3 from Z_p^*, computes

$$W = (h_1^{m_0})^{a_2} g_1^{a_1} u_1^{a_2} v_1^{a_3}$$

and sends W to S.

(2) S randomly selects $\eta \in Z_p^*$ and sends η to U.

(3) U computes

$$b_1 = a_1 + \eta m_1 t \bmod p, b_2 = a_2 + \eta t \bmod p, b_3 = a_3 + \eta st \bmod p$$

and sends (b_1, b_2, b_3) to S.

(4) S checks whether the following equation holds or not :

$$WX^{\eta} = (h_1^{m_0})^{b_2} g_1^{b_1} u_1^{b_2} v_1^{b_3}$$

If it holds, S accepts. Otherwise, S rejects and aborts.

If S accepts the above protocol, S randomly selects $r, l \in Z_p^*$ and computes

$$Y = \left(Xv_1^l\right)^{1/x+r}, R = g_2^r$$

and sends (Y, R, l) to U, here, $Y = \left(Xv_1^l\right)^{1/(x+r)} = \left(h_1^{m_0} g_1^{m_1} u_1 v_1^{s+l/t}\right)^{t/(x+r)}$. U randomly selects $f \in Z_p^*$, and computes

$$\tau = (ft)^{-1} \bmod p, \sigma = Y^{\tau}, \alpha = \omega_2^{f-1} R^f, \beta = s + l/t \bmod p$$

(σ, α, β) is the partially blind signature of (m_0, m_1), where m_0 is common information between S and U, and m_1 is blinded to S.

3. Signature verification: Given a public-key $(g_1, g_2, w_2, u_2, v_2, h_2)$, common information m_0, message m_1, and a signature (σ, α, β), check

$$m_0, m_1 \in Z_p^*, \beta \in Z_p^*$$
$$\sigma, U \in G_1, \sigma \neq 1$$
$$\alpha, V \in G_2, \alpha \neq 1$$
$$e(\sigma, \alpha) = e\left(g_1, h_2^{m_0} g_2^{m_1} u_2 v_2^{\beta}\right), e(U, \alpha) = e(w_1, w_2) \cdot e(g_1, V)$$

If they hold, the verification result is valid; otherwise the result is invalid.

3. The electronic auction scheme

3.1. System initialization

Let H_1 is a GDH group. We assume that the order is t which is a large prime number, and the generator is Q. Set bilinear mapping f is $f : H_1 \times H_1 \to H_2$.

The auctioneer must published all of auction symmetric keys. We assume that there are n auction, and their keys are $k_1, k_2, \cdots, k_n \in Z_p^*$. Set r bidders in the auction, and their public key are $P_1, P_2, \cdots, P_r$.

Firstly, randomly generate $g_{i2}, u_{i2}, v_{i2}, h_{i2} \in G_2$ for i auction goods, set $g_{i1} = \psi(g_{i2}), u_{i1} = \psi(u_{i2}), v_{i1} = \psi(v_{i2}), h_{i1} = \psi(h_{i2})$. Secondly, randomly select $x_i \in Z_p^*$, compute $\omega_{i2} = g_{i2}^x \in G_2$ and set tender value is $m_i \in Z_p^*$ for i auction goods. The auctioneer compute public and secret keys are:

Public key: $g_{i1}, g_{i2}, u_{i2}, v_{i2}, h_{i2}, \omega_{i2}$

Secret key: x_i

3.2. Tender information generation

In order to confirm i auction goods, auctioneer S and bidders U agree on common information k_i in a predetermined way.

U randomly select $s_i, t_i \in Z_p^*$ and compute $X = h_{i1}^{k_i t_i} g_{i1}^{m_i t_i} u_{i1}^{t_i} v_{i1}^{s_i t_i}$ which is shared on between S and U in a predetermined way. In order to gain the trust of S, U prove that they have $(t_i, m_i t_i, t_i, s_i t_i)$ as follows:

1. U randomly select a_1, a_2, a_3 from Z_p and computes $W = (h_{i1}^{k_i})^{a_2} g_{i1}^{a_1} u_{i1}^{a_2} v_{i1}^{a_3}$ which is shared with S in a predetermined way.

2. S randomly select $\eta \in Z_p^*$ which is shared with U in a predetermined way.

3. U computes $b_1 = a_1 + \eta m_i t_i \bmod p, b_2 = a_2 + \eta t_i \bmod p, b_3 = a_3 + \eta s_i t_i \bmod p$ and share (b_1, b_2, b_3) with S in a predetermined way.

4. S checks whether the following equation holds or not :

$$(h_{i1}^{k_i})^{b_2} g_{i1}^{b_1} u_{i1}^{b_2} v_{i1}^{b_3} = WX^{\eta}$$

If it holds, S accepts. Otherwise, S rejects and aborts.

If S accepts U, S randomly selects $r, l \in Z_p^*$ and computes

$$Y = \left(Xv_1^l\right)^{1/x+r}, R = g_2^r$$

and sends (Y, R, l) to U. U randomly selects $f \in Z_p^*$, and computes

$$\tau = (ft)^{-1} \bmod p, \sigma = Y^{\tau}, \alpha = \omega_2^{f-1} R^f, \beta = s + l/t \bmod p$$

(σ, α, β) is the partially blind signature of (k_i, m_i). U sends $(k_i, \sigma, \alpha, \beta)$ to S at last.

3.3. Tender information submission

The stage of tender information generation is over when the fixed time. S stops all the tender information exchange. U need to send his tender value (k_i, m_i) to S at the same time.

Because auction is the large-scale network events, U can send much tender information of different goods in the stage of tender information generation without additional burden and share tender value which can distinguish different goods through the secret key k_i with S.

3.4. Winning bid information published

S don't accept any tender information of U after the stage of tender information submission and compute the highest value and the second high value through compare every tender value of goods. So the second high value $M_1, M_2, \cdots, M_n$ is the bid value of goods.

3.5. Identity verification

U send his partially blind signature and identity to S when tender value higher than the winning bid.

U prove to S that his identity is legitimate as follows:

1. P_j randomly select $v_j \in Z_p^*$.
2. P_j randomly select $x_i \in Z_p^*$ for other bidders $P_i\left(1 \le i \le r, i \ne j\right)$ and compute $y_i = x_i P_i (1 \le i \le r, i \ne j)$
3. P_j compute $f_{kj,vj}(y_1, y_2, \cdots, y_r) = v_j$ which is only solution y_j and can solve the equation easily.
4. Because P_j is legitimate bidder, he can compute x_j through bilinear mapping.

U send identity and partially blind signature to S as follows:

$$(k_j, v_j, x_1, x_2, \cdots, x_r), (g_1, g_2, u_{i2}, v_{i2}, h_2, \omega_2, \sigma, \alpha, \beta)$$

S need to verify identity and partially blind signature as follows:

(1) S compute x_i and y_i through $y_i = g_i(x_i)(i = 1, 2, \cdots, r)$.

(2) S get $y_i (i = 1, 2, \cdots, r)$ and checks whether the following equation holds or not :

$$f_{kj,vj}(y_1, y_2, \cdots, y_r) = v_j$$

If it holds, S accepts and continue. Otherwise, S rejects and restart until the new bidder identity is legitimate.

(3) When U is a legitimate bidder, S checks whether the following equations holds or not:

$$m_0 \in Z_p^*, m_1 \in Z_p^*, \beta \in Z_p, \sigma \neq 1, \alpha \in G_2$$

$$e(\sigma, \omega_2 \alpha) = e\left(g_1, h_2^{k_i} g_2^{m_i} u_{i2} v_{i2}^{\beta}\right)$$

If they hold, U is the successful bidder. Otherwise, S rejects and restart until define the successful bidder.

4. Security analysis

1. The security of tender information. If dishonest auctioneer S' generate other public-key $(g_2, \omega_2, u_2, v_2) \in g_2^4$ and $g_1 = \psi(g_2)$. Because $(X, W, \eta, b_1, b_2, b_3)$ and $(m_i, \sigma, \alpha, \beta)$ which is partially blind signature completely independent, tender value is perfectly blind and is safe.

2. The security of successful bidder price. If dishonest bidder P' get other bidder tender value through illegal methods, he also can't generate a new tender value which is higher than the old one. Because the security message in the tender information isn't fake and bidder P' can't compute another tender information.

3. The security of successful bidder identity. Because every k and v have $\left(2^b\right)^{r-1}$ solutions in bilinear mapping, which is same probability in stage of tender information generation and is nothing with successful tenderer. The unsuccessful tenderer identity is secret, so bidders identity are safe.

4. The fairness of the auction. After the close of auction, the successful tenderer can't deny, because he can be determined by auctioneer. The auctioneer can't deny too, because the successful tenderer can complaint to management center.

5. Conclusion

In this paper, a new electronic auction scheme is proposed based on group signatures and partially blind signatures. At the same security strengthen, an optimization was done on the processes of electronic auction scheme and all dependence on trusted third party was reduced, moreover, multiple goods is auctioned at the same time, therefore, this scheme suited to large-scale electronic auction. Furthermore, due to application of vickrey auctions on the auction scheme, the principle of optimal allocation of goods is easily satisfied, so it is more practical.

Acknowledgements

The work discribed in this paper was supported by National Natural Science Foundation(60963024, 61006020) and Guangxi Natural Science Foundation(0991079).

References

[1]Chen Xiaofeng, Wang yumin. A Survey of Research on Electronic Auction. Journal on Communication, 2002, 23(12):73-81.

[2]CHAUM D,VAN HEYST E. Group Signatures. EUROCRYPT 1991, Lecture Notes in Computer Science. Berlin: Springer-Verlag,1991:257-265.

[3]LIU X,XU Q L,SHANG J Q.A Public Auction Scheme Based on Group Signature. Proceedings of the 3rd International Conference on Information Security.New York:ACM,2004:136-142.

[4]NGUYEN K Q,TRAORE J.An Online Public Auction Protocol Protecting Bidder Privacy. ACISP 2000,Lecture Notes in Computer Science 1841.Berlin:Springer-Verlag,2000:427-442.

[5]Ji Dongyao, Wang Yumin. A Secure Electronic Auction Based on Group Signature, ACTA ELECTRONICA SINICA,2002,30(1):18-21.

[6]OMOTE K,MIYAJI A.A Practical English Auction with One-Time Registration. ACISP 2001,Lecture Notes in Computer Science 2119.Berlin:Springer-Verlag,2001:221-234.

[7]SAKURAI K,MIYAZAKI S.An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme[C].ACISP 2000,Lecture Notes in Computer Science1841.Berlin:Springer-Verlag,2000:385-399.

[8]CHAUM D.Blind Signatures for Untraceable Payments[C].Proceedings of CRYPTO 1982.In Advances in Cryptology.Plenum Press,1983:199-203.

[9]ABE M,FUJISAKI E.How to Date Blind Signatures[C].ASIACRYPTO 1996.Lecture Notes in Computer Science 1163.Berlin: Springer-Verlag,1996:244-251.

[10]OKAMOTO T.Efficient Blind and Partially Blind Signatures Without Random Oracles[C].TCC 2006.Lecture Notes in Computer Science 3876.Berlin: Springer-Verlag,2006:80-90.