Provable Electronic Marketplace Bidding Auction Protocol with Bid Privacy

Wenbo SHI, Injoo JANG, Hyeong Seon YOO

Abstract—**In this paper, we proposed a provable electronic marketplace bidding auction protocol. The proposed protocol tries to reduce DOS attack and avoids replay data attack by providing ticket token and deal sequence number to the supplier. It utilizes efficient LPN-based authentication method to accomplish lightweight authentication. And it publishes an interpolating polynomial for sharing the data of determination process and avoids collusion between a customer and a certain supplier. Also it relaxes trust assumptions for three-party. According to comparison and analysis with other protocols, our proposed protocol shows good security and less computation cost.**

Keywords —**Anonymity, Electronic auction**

I. Introduction

IN 2002, Collins et al. presented a multi-agent marketplace, MAGNET (Multi-Agent Negotiation Test-bed) for electronic business-to-business market [1]. As business value and criticality of electronic transactions increase, it becomes ever more important to examine the security risks present and take steps to avoid them. So Jaiswal et al. proposed security protocol to improve MAGNET in 2004, which consider security problem into real-world networks [2]. But the improved protocol still has some weaknesses: vulnerable to the replay data attack, DOS (denial-of-service) attack, anonymity disclosure weakness, collusion between a customer and a certain supplier.

The proposed protocol adopts conference key concept [3] and ticket token in supplier group. Also market generates deal sequence number (*dsn*) and random number (*r*) for suppliers who have download requests for quotes (*RFQ*). It utilizes efficient LPN-based authentication method to accomplish lightweight authentication [4,5]. When auction is closed, market constructs a simple interpolating polynomial for sharing the data of determination process in supplier group who have taken part in this auction. Sharing the data of determination process can avoid collusion between a customer and a certain supplier. Furthermore, we relax the assumption about collusion between customer agent and supplier agents and trust assumptions for three-party in Jaiswal's scheme.

Sealed-bid security is inherent weakness, because it isn't easy to avoid auctioneer opening bids especially in two party's protocol. In Chang's protocol, there isn't a deliberate mechanism which can avoid opening bid before bidding phase is closed. It provides an auctioneer opportunity to collude with a certain bidder and leak updated information about bids to the bidder, so the anonymity of bidders depends on auctioneers [6]. In Liaw's protocol, the third party also can leak the information to a bidder whom he intends to collude with, so the anonymity of bidders depends on the third party [7]. In the proposed protocol, nobody else but the bidder himself can open bids before bidding phase is closed. It guarantees identity non-disclosure independently.

Wenbo Shi is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

Injoo Jang is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

Hyeong Seon Yoo is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

II. Proposed scheme

The proposed protocol has following phases: planning, bidding, auction close and winner determination (Fig. 1).

For convenience, we assume there are n_1 customers (C), n_2 suppliers (S) and one market (M) in our auction scheme. A certification authority (CA) is needed in key pre-distribution long-term key process. CA chooses and publishes large prime number p_1, p_2 such that p_1-1 and p_2-1 have large prime factors. Let q_1, q_2 are prime divisor of p_1-1 and p_2-1 separately, g_1 and g_2 are generator with order q_1, q_2 in GF(p_1) and GF(p_2) separately. Let S_i be the identity of a supplier, C_i be the identity of a customer.

CA assigns secret key $x_{i1} \in Z^* q_1$ and computes public key $y_{i1}=g_1^{x_{i1}} \bmod p_1$ for each C and M, where $1<i_1 \leqq n_1+1$ [3]. CA assigns secret key $x_{i2} \in Z^* q_2$ and computes public key $y_{i2}=g_2^{x_{i2}} \bmod p_2$ for each S and M, where $1<i_2 \leqq n_2+1$. CA assigns two symmetric key $x_{i3} \in_R \{0,1\}^k$, $y_{i3} \in_R \{0,1\}^k$, for each S and M, where $1<i_3 \leqq n_2+1$. Then, CA gives those secret keys to M,each C and S in a secure way.

A. Planning

C_i sends $M_1=S_{K_c}(RFQ)$ a RFQ message which is signed by C_i's secret key S_{K_c} to M for publishing. After receiving RFQ message, M verifies and publishes *RFQ*. M constructs ticket token polynomial by steps below:

1). Randomly chooses integer r and ticket token $T \in Z^* q_2$ and gets timestamp t from the system and computes $A=g^r \bmod p$, $B=r*T+H(t||A)* x_{m2} \bmod q_2$, where H() is a one-way hash function.

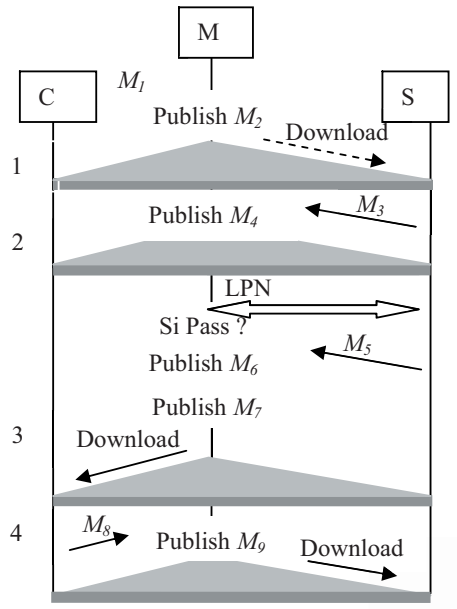

Fig. 1. The proposed protocol

2). Computes secret key shared with each S as: $k_{mi2}= y_{i2}{}^{r} \bmod p_2$, where $1 \leqq i_2 \leqq n_2$

3). Constructs ticket token polynomial $f(x)$ for publishing.

$$f(x)=\prod_{i_2=1}^{n_2}(x-k_{mi_2})+T \bmod p_2$$
$$=x^n+c_{n-1}x^{n-1}+.....+c_1x+c_0 \bmod p_2 \quad (1)$$

Where $c_{n-1},c_{n-2},\ldots\ldots c_1,c_0 \in Z^*q_2$

4). Publishes $M_2=A, B, t, c_{n-1}, c_{n-2},\ldots c_1, c_0$.

B. Bidding

If S_i is interested in this auction, S_i will do such steps:

1). Gets $A, B, t, c_{n-1}, c_{n-2},\ldots c_1, c_0$ from M's publish board.

2). Checks whether t is a valid data or not.

3). Computes the secret key shared with M as:

$$k_{i_2m}=A^{x_{i_2}} \bmod p_2 \quad (2)$$

4). Gets T by computing $f(k_{mi2})$

$$f(k_{i_2m})=(k_{i_2m})^n+c_{n-1}(k_{i_2m})^{n-1}+.....+c_1(k_{i_2m})+c_0 \bmod p_2$$
$$=T \bmod p_2 \quad (3)$$

5. Verify T by computing $H(t||A)$ and check the equation:

$$g^B \equiv A^T * y_{m_2}{}^{H(t||A)} \bmod p_2 \quad (4)$$

After getting T, S_i use T to download RFQ. When S_i downloads the RFQ, M generates dsn and r to S_i. After getting dsn and r from M, S_i generates a bid-message comprising of RFQ number ($RFQ\#$), dsn and r, symmetric auction-session key (k_a), bid data (bid), where k_a is generated by S_i himself. Then S_i signs, hashes and encrypts message and sends M_3 to market. Where $M_3=[RFQ\#,dsn,H(r,dsn),E_{k_a}(S_{S_{ks}}(bid)),H(r,E_{k_a}(S_{S_{ks}}(bid)))]$, $S_{S_{ks}}(bid)$ is a bid data block signed by S_i's secret key S_{k_s}, $E_{k_a}(S_{S_{ks}}(bid))$ is a data block encrypted by k_a. After receiving messages came from S, M publishes all $M_4=(RFQ\#, (dsn, M_3, H(M_3)))$ on publish board.

C. Auction close

When the auction is closed, M authenticates each S's agent by steps below:

1. S_i chooses a blinding vector a_1 randomly $a_1 \in_R \{0,1\}^k$, and sends $\{dsn, S_i, a_1, T_1\}$ to M, where T_1 denotes a valid timestamp.
2. After receiving $\{dsn, S_i, a_1, b_1\}$, M checks T_1 and chooses challenge b_1 randomly $b_1 \in_R \{0,1\}^k$, publishes $(dsn, S_i, a_1, b_1, T_2)$, where T_2 denotes a valid timestamp.
3. S_i gets b_1 from publish board, then computes response $z_1= a_1 \cdot x \oplus b_1 \cdot y \oplus v$, and sends $\{dsn, S_i, z_1, T_3\}$, where v denotes a noise bit, T_3 denotes a valid timestamp.
4. After receiving $\{dsn, S_i, z_1, T_3\}$, M checks T_3 and publishes (dsn, S_i, z_1) and accepts the round if $a_1 \cdot x \oplus b_1 \cdot y = z_1$.

After that, M announces whether S_i's agent passes the authentication or not. If passed, S_i's agent send $M_5= S_{S_{ks}}(dsn, r, x_{i3} \oplus y_{i3} \oplus k_a)$. After receiving it, M publishes $M_6 =dsn, r, x_{i3} \oplus y_{i3} \oplus k_a$. S can check and verify whether their messages were actually received and displayed by M. M publish $M_7 =RFQ\#, E_{Pk_c}((dsn_1,r_1,k_{a1}),\ldots(dsn_i, r_i, k_{ai}),\ldots(dsn_n,r_n,k_{an}))$, where $E_{Pk_c}()$ is encrypted by C_i's public key y_{i1}. According to the message published by M, C_i will download corresponding M_3 from the publish/subscribe system, and decrypt the data block and get all valid bid information. Having authenticated S group twice, M can make sure that each participant is legitimate S.

D. Winner determination

C_i sends message about winner information $M_8=S_{Sk_c}(RFQ\#, r_{winder})$ to M. After M receiving C_i's message, M checks whether the winner contained in legitimate S list $(dsn_1,r_1,k_{a1}),\ldots(dsn_i, r_i, k_{ai}),\ldots(dsn_n,r_n,k_{an})$. If the winner is contained, M publishes the winner information on board for notifying S. If there is a controversy about winner, M will choose a large prime number p and a primitive element g for GF(p), where GF(p) is the set of integers $\{0,1, \ldots, p-1\}$ with arithmetic operations defined modulo p. And M generates a symmetric session key K, $K \in Z^*q$. Then M uses the signature datum of S who have taken part in current auction to construct a derivation function $F(x)$ and conceals K in it. After that, M publish the coefficient $c'_{n-1}, c'_{n-2},\ldots c'_1, c'_0$ of the $F(x)$, where $S_{Sksi}(k_{ai}, r_i)$ are S's signature data (i=1,2,…,n). M encrypts bid data of determination process and publish $M_9=RFQ\#, E_k$(bid determination process).

$$F(x)=\prod_{i=1}^{n}(x-h_i)+K \bmod p$$
$$=x^n+c_{n-1}x^{n-1}+.....+c_1x+c_0 \bmod p \quad (5)$$

Where $h_i = g^{S_{Sksi}(k_{ai},r_i) \bmod p-1}$ (6)

$c'_{n-1}, c'_{n-2},\ldots\ldots c'_1, c'_0 \in Z^*q$

III. Security Analysis

Theorem 1. Assume no man can modify publish message except M. After M publish $A=g^r \bmod p$, $B=r*T+H(t||A)* x_{m2} \bmod q_2$, t, coefficients $c_{n-1}, c_{n-2},\ldots c_1, c_0 \in Z^*q_2$ of ticket token function (1), no man can get ticket token T besides S group.

Proof. Because M has computed each S's secret key k_{mi2} as the solution of the ticket token polynomial function $f(x)$, where $k_{mi2} = y_{i2}^{r} \bmod p_2$, $1 \leqq i_2 \leqq n_2$. Furthermore, only legal S can compute $k_{mi2} = y_{i2}^{r} \bmod p_2$, where $k_{mi2} = k_{i2m}$. So legal S can have the valid k_{mi2} that satisfies $f(k_{mi2}) = T \bmod p_2$ for getting T.

Situation 1. If one attacker wants to obtain r from $A = g^{r} \bmod p$, he will face the difficulty of solving the intractable discrete logarithm problem.

Situation 2. If one attacker wants to obtain T from $B = r*T + H(t||A)* x_{m2} \bmod q_2$, because there are two unknown parameters r and x_{m2}, still he must solve the intractable discrete logarithm problem.

Situation 3. If one attacker wants to compute T from the function $f(x)$, he should know the valid k_{mi2} that satisfies $f(k_{mi2}) = T \bmod p_2$. It means that the attacker must solve the intractable discrete logarithm problem.

Theorem 2. Assume M received S's message M_3 safely. M can make sure that M_3 comes from legal S group. After M publish M_4 on board, S can make sure that M receive RFQ very well.

Proof. S open RFQ# and *dsn* information for temporary identity in M_3. We make sure that the key k_a larger than 160 bits and therefore is able to withstand the exhaustive key search attack on data block $E_{ka}(S_{Sks}(bid))$ [8]. Because M cannot decrypt the data block $E_{ka}(S_{Sks}(bid))$, and M has recorded r as r' in planning phase, market can just verify whether information *dsn* and data block $E_{ka}(S_{Sks}(bid))$ are valid by computing $hash(r,dsn) \stackrel{?}{=} hash(r',dsn)$ and $hash(r,E_{ka}(S_{Sks}(bid))) \stackrel{?}{=} hash(r',E_{ka}(S_{Sks}(bid)))$. Because an attack cannot get valid r to forge $hash(r,dsn)$ and $hash(r,E_{ka}(S_{Sks}(bid)))$. After verifying the data block, M can make sure whether M_3 come from legal S or not. After M published $M_4 = (RFQ\#, (dsn, M_3, hash(M_3)))$ on board, S can verify whether M receive their message M_3 correctly by computing $hash(M_3) \stackrel{?}{=} hash(M_3')$.

Theorem 3. Assume M finished the communication with S by LPN authentication method. Mutual authentication has achieved between M and each S.

Proof. The hardness of the computational LPN problem has been shown to be NP-complete [4]. Our LPN-based authentication method adopted HB^{+} computing prototype. Even though Gilbert proposed that HB^{+} is not secure against a man-in-the-middle attack [5], because our auction scheme inherits the idea of publish system, we can make sure that the process of authentication is secure and sets up mutual authentication.

The condition when HB^{+} protocol attack happen is that the attacker can manipulate challenges sent by M to a S during the authentication message exchanges. In our LPN-based authentication process, M utilizes publish system to show messages which S have sent. So S can check and verify whether their messages were actually received and displayed by market. We assume that there is an attacker in the middle, and he can manipulate message sent by S to M. But the attacker cannot modify any information, because S can check the message on board each round. Due to the publish system, the attacker cannot manipulate the challenges published by M. According to what is mentioned above, the attacker doesn't have any opportunity to disturb the authentication process.

Theorem 4. Assume M publish message correctly, where message are coefficients $c'_{n-1}, c'_{n-2}, \ldots c'_1, c'_0 \in Z^*q$ of function $F(x)$ and E_k(bid determination process), then M can make sure that S who have taken part in this auction can check fair deal.

Proof. Because M computes each S's signature data $S_{Sksi}(k_{ai}, r_i)$ as the solution h_i (see equation (6)) of the polynomial function $F(x)$, where $S_{Sksi}(k_{ai}, r_i)$ is S's signature data (i=1,2,….n). So only legal S who have taken part in this auction session have the valid h_i that satisfies $f(h_i) = K \bmod p$ for computing K from the function. After getting K, each legal S can decrypt data block E_k(bid determination process) and check the fair deal.

Situation 1. If an attacker want to compute K from the coefficients of function(5), he should know the valid h_i that satisfies $f(h_i) = K \bmod p$. It means that the attacker must solve the intractable discrete logarithm problem. Therefore, the attacker certainly cannot reconstruct the $F(x)$ to get the session key K from there n points $(1, F_i(1))$, $(2, F_i(2))$,……,and $(n, F_i(n))$ only.

IV. Security analysis

In this section, we discuss Chang's protocol (a), Liaw's protocol (b) and proposed protocol (c) [6, 7]. The comparisons of computation operations of the initial phase and bidding phase among those protocols are shown in TABLE I. Assume length of the prime number p is 1024 bits in Diffie-Hellman and public key encryption, symmetric key length is 128 bits (for AES), hash function digest is 160 bits (for SHA-1), public key certification is 1024 bits, signature length is 320 bits (for DSA).Because operation of RSA's computation can be summarized as a modular exponentiation operation, and the computation cost of a modular exponentiation computation is about O(|n|) times that of a modular multiplication computation where |n| denotes bit length of n. So compared with a modular multiplication computation in Zn*, the computation time consumed by hashing operations, symmetric encryptions or decryptions can be neglected. And symmetric cryptosystem is 1000 times faster than asymmetric cryptosystem and hash function is 10 times faster than symmetric cryptosystem [9].

V. Conclusions

As mentioned above, the current paper proposed an electronic marketplace bidding auction protocol whose security is based on the well-known Discrete Logarithm assumption. It satisfies security requirements of an electronic auction, such as anonymity, non-repudiation, verifiability etc. And the proposed scheme relaxes trust assumptions for three-party in Jaiswal's scheme. According to discussion and analysis with Chang et

al.'s protocol and Liaw et al.'s protocol, our proposed protocol shows better security in anonymity, fairness and reliance on the third party. Therefore, the advantages of our proposed bidding auction protocol are difficulty collusion.

TABLE I.
NUMBER OF OPERATIONS FOR PHASES

Phase	a	b	c
Initiation phase	4 HF	5 HF	2HF
	2 SKE	0	0
	2 SKD	0	0
	2 PKE	3 PKE	1 PKE
	2 PKD	3 PKD	1 PKD
	4 ME	0	6ME
	2 R	5 R	3 R
Bidding phase	0	0	4 HF
	2 SKE	0	1 SKE
	2 SKD	0	0
	1 PKE	5 PKE	1 PKE
	1 PKD	5 PKD	0
	0	0	1MM

PKE: Public Key Encryption; PKD: Public Key Decryption;
SKE: Symmetric Key Encryption; SKD: Symmetric key decryption;
HF: Hash Function; ME: Modular Exponentiation;
R: generate a random number; MM: Modular multiplication

REFERENCES

[1] J. Collins, W. Ketter and M. Gini, "A multi-agent negotiation testbed for contracting tasks with temporal and precedence constraints," International Journal of Electronic Commerce, vol.7, no.1, pp.35–57, 2002

[2] A.Jaiswal, Y. kim and M. Gini, "design and implementation of a secure multi-agent marketplace," Electronic Commerce Research and Applications, vol.3, no.4, pp.355-368,2004

[3] E.K. Ryu, J.-Y. Im and K.Y. Yoo, "Security of Tseng – Jan's conference key distribution system," Applied Mathematics and Computation, 167(2), 833-839,2005

[4] O.Regev, "On Lattices, Learning with errors, Random Linear Codes. and Cryptography," 37th ACM symposium on theory of computing, 84-93,2005

[5] H. Gilbert, M. Robshaw, H. Silbert, "An active attack against HB+ – a provable secure lightweight authentication protocol,"Cryptology ePrint Archive, Report 2005/237, 2005

[6] Chang, Y.F. and Chang ,C.C, "Enhanced anonymous auction protocols with freewheeling bids", 20th International Conference on Advanced Information Networking and Applications, AINA (1), 353-358 ,2006

[7] Horng-Twu Liaw, Wen-Shenq Juang and Chi-Kai Lin, "An electronic online bidding auction protocol with both security and efficiency," Applied Mathematics and Computation, 174(2), 1487-1497, 2006

[8] National Institute of Standards and Technology (NIST), Digital signature standard. Federal Information Processing Standards Publication, FIPS PUB 186, p. 20, 1994

[9] Chun-I Fan, Yung-Cheng Chan and Zhi-Kai Zhang, "Robust remote authentication scheme with smart cards," Computers & Security , 24(8) , 619-628, 2005