ITC 4/46
Journal of Information Technology and Control
Vol. 46 / No. 4 / 2017
pp. 470-483
DOI 10.5755/j01.itc.46.4.14163

An Electronic Public Engineering Project Bidding Protocol via a Subliminal Channel

Received 2017/03/15 | Accepted after revision 2017/10/23

http://dx.doi.org/10.5755/j01.itc.46.4.14163

An Electronic Public Engineering Project Bidding Protocol via a Subliminal Channel

Chin-Ling Chen
Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan, (R.O.C.), e-mail: clc@mail.cyut.edu.tw
School of Information Engineering, Changchun Sci-Tech University, 1699 Donghua Street, Shuangyang District, Changchun City, Jilin Province, 130600, China, e-mail: wkhyoyo@163.com

Kun-Hao Wang
School of Information Engineering, Changchun Sci-Tech University, 1699 Donghua Street, Shuangyang District, Changchun City, Jilin Province, 130600, China, e-mail: wkhyoyo@163.com

Woei-Jiunn Tsaur
Computer Center, National Taipei University, Taiwan, R.O.C., e-mail: wjtsaur@mail.ntpu.edu.tw

Jung-Hsuan Chen
Department of Industrial Education, National Taiwan Normal University, Taipei, 10610 Taiwan, R.O.C., e-mail: jhchen@ntnu.edu.tw

Chien-Hung Chen
Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan, (R.O.C.), e-mail: bitz823@hotmail.com

Corresponding author: clc@mail.cyut.edu.tw

Due to the rapid development of the Internet, many Internet applications have recently become very widely used. Internet security has therefore become an important issue. This paper proposes an electronic public engineering project bidding protocol via a subliminal channel. In the proposed scheme, the subliminal channel can protect a bidder's interests, while allowing an official agent to make a fair arbitration. The proposed scheme is non-repudiable, untraceable and offers fair arbitration of public engineering projects, but is also resistant to replay, forgery and insider attacks, thus enhancing both security and fairness.

KEYWORDS: Subliminal channel, Fair arbitration, Security, Non-repudiation, Digital signature.

1. Introduction

In recent years, the Internet has developed rapidly, and many Internet transaction applications have become popular. For example, many public construction engineering projects now conform to public, fair and efficient requirements via Internet technology. For example, in e-bidding cases, some important issues should be of concern. The bidding price should be protected to defend against insider attack, and there should be a fair arbitration mechanism to arbitrate accusations.

In 1983, Simmons [15-17] first proposed the subliminal channel mechanism. Subliminal channels are employed for secret communication; they can be used to deliver subliminal messages between sender and receiver. Subliminal messages cannot be accessed except through the specific receiver. In 1997, Harn and Gong [5] proposed a digital signature using a subliminal channel; they showed how to construct a digital signature scheme with a broadband subliminal channel that does not require a subliminal receiver to share the transmitter's secret signing key. In 2010, Lin et al. [9] proposed a digital signature with multiple subliminal channels, and its applications. The proposed scheme has the advantage that the subliminal receivers cannot forge a valid signature since they do not share the signer's secret key. It can also provide more than one independent subliminal message.

In 1998, Subramanian [18] presented the design and verification of a secure electronic auction protocol. This protocol ensured anonymity, security, privacy, atomicity and low overhead. Hwang et al. [6] proposed adding timestamps to the secure electronic auction protocol in 2002. They found the drawback of Subramanian's protocol and proposed an electronic auction protocol with improved robustness. In 2006, Liaw et al. [8] proposed an electronic online bidding auction protocol with both improved security and efficiency. This protocol not only satisfies the requirements for the electronic auction properties of anonymity, security, privacy, atomicity and low overhead cost, but also adds the properties of non-repudiation, untraceability, auditablity, one-time registration and unlinkability. In 2008, Chun et al. [3] proposed a bidder-anonymous English auction scheme with privacy and public verifiability. The proposed scheme provided the following security features: anonymity, traceability, no framing, unforgeability, non-repudiation, fairness, public verifiability, unlinkability among various auction rounds, linkability within a single auction round, bidding efficiency, one-time registration, and easy revocation. In 2012, Xiong et al. [19] proposed a bidder-anonymous English auction protocol based on revocable ring signature. The proposed protocol has three appealing characteristics: first, it offers conditional privacy-preservation: while the auctioneer can verify that a bidder is an authorized participant in the system, only the collaboration of auctioneer and registration manager can reveal the true identity of a malicious bidder. Second, it is a one-time registration: the bidder can take part in plural auctions with one time registration. Third, it is spontaneous: the bidder can bid without interaction with the auctioneer and other bidders. Fan et al. [4] proposed a multi-recastable e-bidding game with dual-blindness. The proposed protocol allows all participants to take part in a sequence of different auctions for various products unlimitedly after performing a one-time registration, where the winner does not need to re-register either. They formally proved the security of the proposed scheme and also provided comparisons to show that it was the most efficient one, compared with previous works. In order to defend against known attacks, some applications should embed authentication mechanisms [10-11] to ensure that security requirements can also be guaranteed.

This paper proposes a novel scheme for a fair bidding transaction for public construction engineering projects. The fair bidding transactions need to protect the bidder's privacy and uphold a fair transaction process. The proposed scheme is not only able to protect the bidder's privacy, but can also support fair arbitration via a subliminal channel.

The proposed scheme should have the following characteristics:

1. Non-repudiation [2]: Non-repudiation refers to the ability to ensure that parties cannot deny the authenticity of their signature on a message which they have sent.
2. Fair arbitration [1]: The fair arbitration mechanism can allow participating parties access to fair arbitration when they have doubts regarding aspects of the project.
3. Blind message [14]: The blind message mechanism can be provided to protect the bidder's privacy, and other persons cannot extract the message, aside from the owner of the blind factor.
4. Unlinkability [4]: No one can trace a specific bidder from the transaction message.
5. One-time registration [4]: The protocol only requires one-time registration for each bidder.
6. Auditability [4]: Auditability is a third-party application which can assist an auctioneer to find the real identity of a bidder in certain cases, or if disputes occur.
7. Defence against replay attack [1]: A replay attack occurs when an attacker copies the message between two parties and replays it to one or more parties in order to gain access to sensitive information.
8. Defence against forgery attack [14]: In a forgery attack, an attacker masquerading as a legal party transmits the message to obtain the other party's trust, and thereby gains access to sensitive information.
9. Defence against insider attack [14]: The attacker can access sensitive information using a legal identity to achieve an insider attack.

The remainder of this paper is arranged as follows. Section 2 introduces the framework of the proposed scheme. Section 3 offers a security analysis of the proposed scheme. Section 4 discusses the computation costs of the proposed scheme, and makes a security comparison with related works. Finally, conclusions regarding the proposed scheme are drawn in Section 5.

2. The Proposed Scheme

The overview of the proposed scheme is shown in Figure 1. There are five parties involved in the scheme:

1. Bidder (BI): A person or a company that wants to take part in a bidding case
2. Public Construction Commission (PCC): The organization which has a private enterprise or government entity hold a bidding operation
3. Bank (BK): The bank of the Bidder and Public Construction Commission
4. Proxy Server (PS): A trusted proxy server used to transfer and store important information
5. Official Agent (OA): A trusted and fair arbitrator

Step 1: BI → BK,PS & PCC→ BK, PS: BI and PCC register with the BK and PS, respectively.

Step 2: BI → BK: When a bidder wants to take part in the bid, the bidder sends the bidding bond and related information to the bank.

Step 3: BK → BI: After receiving the message, BK stores the bidding bond, signs the response message and sends it to the BI.

Step 4: BI → PCC: The BI makes the bidding message and uses the blind factor to make a blind signature. It then sends the blind message to the PCC.

Step 5: PCC → BI: After receiving the blind message, the PCC will sign the message and send it back to the BI.

Step 6: BI → PS: The BI makes the bidding message, which includes the blind factor and the bidder's identity. After that, the BI sends the bidding message to the PS.

Step 7: PS → BI: The PS sends the response message to the BI.

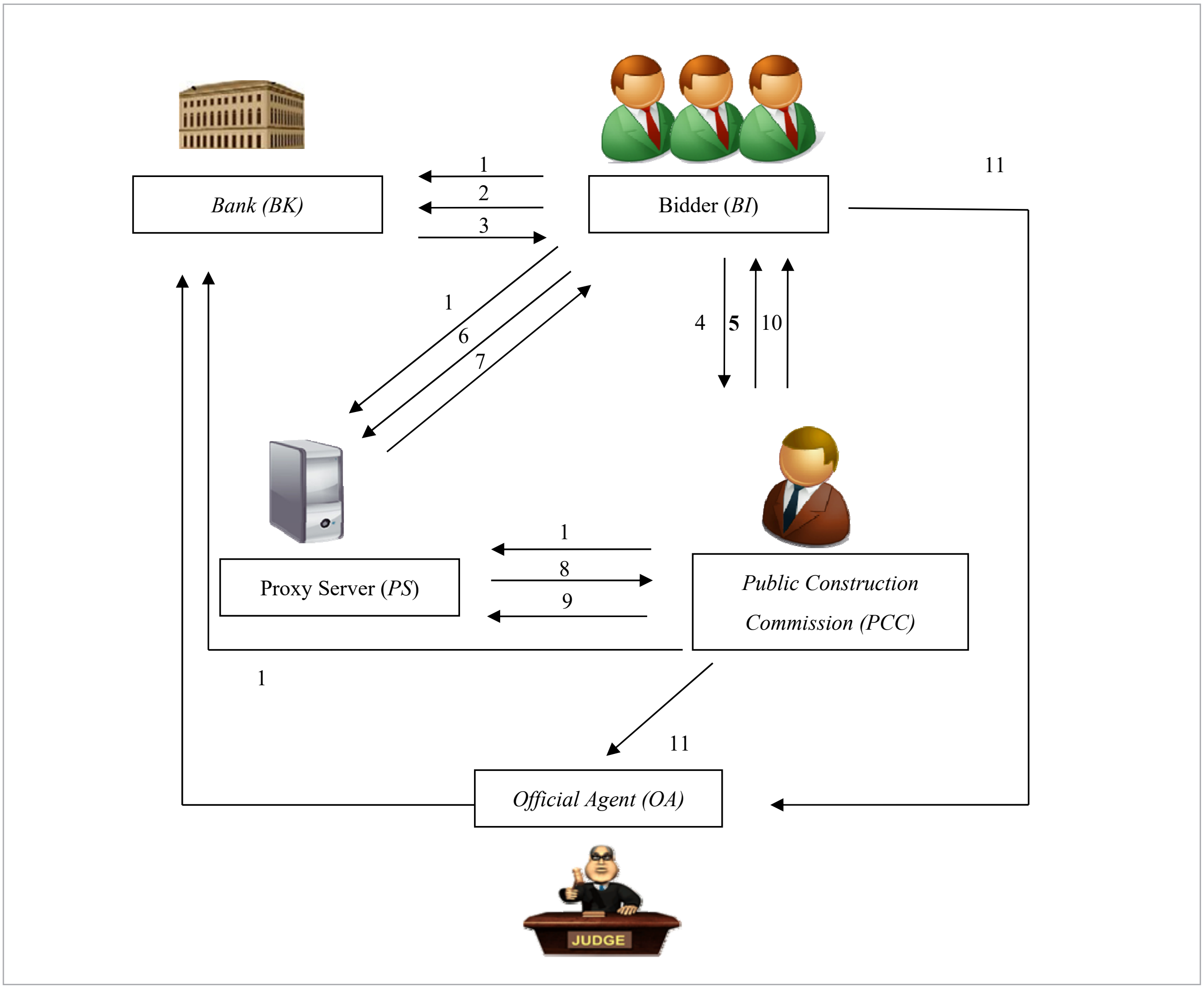
Step 8: PS → PCC: The PS sends the blind factor and bidding identity to the PCC.

Step 9: PCC → PS: the PCC sends the response message to the PS.

Step 10: PCC → BI: The PCC publishes the winner.

Step 11: BI → OA or PCC → OA: When the BI or PCC doubts this bidding case, they can send the blind message, blind factor and subliminal message to the OA to request arbitration.

Figure 1
The overview of our scheme



The following notations are used in the proposed protocol:

$x_{BI}, x_{BK}, x_{PCC}, x_{PS}, x_{OA}$: the BI, BK, PCC, PS and OA's private keys, respectively

$y_{BI}, y_{BK}, y_{PCC}, y_{PS}, y_{OA}$: the BI, BK, PCC, PS and OA's public keys, respectively, for example: $y_{BI} = g^{x_{BI}} \bmod p$, where g is a randomly chosen generator of the multiplicative group Zp

(d_i, s_i) : the ith signature pair

T_{X-Y} : the timestamp generated by X, and transferred to Y

M_s : the subliminal message

M_{X-Y} : the message is transferred from X to Y

C_i : the ith cipher message

$h()$: a one-way hash function

$A \overset{?}{=} B$: determine if A is equal to B.

2.1. The Registration Phase

In the proposed scheme, the encryption and decryption mechanism is used to protect messages, based on the ElGamal scheme. The BI and PCC need to register with the bank (*BK*) and proxy server (*PS*). Then, the bank and proxy server store the BI and PCC's identities: ID_{BI} and ID_{PCC}, respectively. After this, the participating parties receive their private and public keys.

Therefore, the participating parties can select their own private keys: x_{BI}, x_{BK}, x_{PCC}, x_{PS} and x_{OA}. It can then compute the responding public key.

Step 1: The BI, BK, PCC, PS and OA choose their private keys x_{BI}, x_{BK}, x_{PCC}, x_{PS} and x_{OA}, respectively. Then these parties compute public keys y_{BI}, y_{BK}, y_{PCC}, y_{PS} and y_{OA}, respectively, as follows:

$$y_{BI} = g^{x_{BI}} \bmod p \tag{1}$$

$$y_{BK} = g^{x_{BK}} \bmod p \tag{2}$$

$$y_{PCC} = g^{x_{PCC}} \bmod p \tag{3}$$

$$y_{PS} = g^{x_{PS}} \bmod p \tag{4}$$

$$y_{OA} = g^{x_{OA}} \bmod p. \tag{5}$$

2.2. The Bidding Phase

The BI sends the bidding bonds to the bank (BK), and then the BK returns the response message to the BI. After this, the BI sends the blind message to the PCC to sign it, and the PCC returns the blind message. The BI then sends the bidding message to the PS. The bidding phase is shown in Figure 2.

Step 1: The BI computes the bidding bonds message $M_{BI\text{-}BK}$:

$$M_{BI-BK} = (ACC_{BI}, ACC_{PCC}, ID_{pro}, AMOUNT, ID_{BI}, T_{BI-BK}). \tag{6}$$

The BI then chooses a random number r_1 and computes the ciphertexts C_1 and C_2 as follows:

$$C_1 = g^{r_1} \bmod p \tag{7}$$

$$C_2 = M_{BI-BK} \times y_{BK}{}^{r_1} \bmod p. \tag{8}$$

The BI then sends the ciphertexts (C_1, C_2) to the BK.

Step 2: Upon receiving the ciphertexts (C_1, C_2), the BK uses the private key x_{BK} to decrypt the message:

$$w = (C_1{}^{x_{BK}})^{-1} \bmod p \tag{9}$$

$$M_{BI-BK} = C_2 \times w \bmod p \tag{10}$$

$$M_{BK-BI} = (ACC_{BI}, ACC_{PCC}, M_{tra}, ID_{pro}, T_{BK-BI}). \tag{11}$$

The BK then chooses a random number r_2, makes a response message $M_{BK\text{-}BI}$ and computes a signature (d_1, s_1):

$$d_1 = g^{r_2} \bmod p \tag{12}$$

$$s_1 = r_2^{-1}(M_{BK-BI} - x_{BK} d_1) \bmod p-1. \tag{13}$$

After this, the BK sends the signature (d_1, s_1) and message $M_{BK\text{-}BI}$ to the BI.

Step 3: After receiving the signature (d_1, s_1) and message $M_{BK\text{-}BI}$, the BI uses the public key y_{BK} to verify the signature:

$$y_{BK}{}^{d_1} \times d_1{}^{s_1} \overset{?}{=} g^{M_{BK-BI}} \bmod p. \tag{14}$$

Then, the BI creates a subliminal message M_s and message $M_{BI\text{-}PCC}$ as follows:

$$M_s = ((d_1, s_1), x_{BI}, ID_{BI}, ID_{PCC}, M_{\inf}, ID_{pro}) \tag{15}$$

$$M_{BI-PCC} = ID_{pro}{}^{Ms} \bmod p-1. \tag{16}$$

It sends a blind signature request message M_{req} to the PCC.

Step 4: The PCC chooses a random number k and computes parameter $\tilde{d}_2$:

$$\tilde{d}_2 = g^k \bmod p. \tag{17}$$

The PCC sends the parameter $\tilde{d}_2$ to the BI.

Step 5: The BI chooses random numbers (a, b, c) and computes:

$$d_2 = \tilde{d}_2{}^a y^b g^c \bmod p \tag{18}$$

$$\tilde{M}_{BI-PCC} = a^{-1}(d_2 + h(M_{BI-PCC}) - b) - \tilde{d}_2 \bmod p\text{-}1. \tag{19}$$

$\tilde{M}_{BI-PCC}$ is then sent to the PCC to sign the message.

Step 6: The PCC computes:

$$\tilde{s}_2 = (\tilde{d}_2 + \tilde{M}_{BI-PCC})x_{PCC} - k \bmod p-1 \tag{20}$$

and then sends $\tilde{s}_2$ to the BI.

Step 7: After receiving the blind signature $\tilde{s}_2$, the BI decrypts the blind message and obtains the signature:

$$s_2 = a\tilde{s}_2 - c \bmod p\text{-}1 \tag{21}$$

Figure 2
The scenario of the bidding phase

BI

private key x_{BI}

$y_{BI} = g^{x_{BI}} \bmod p$

BK

private key x_{BK}

$y_{BK} = g^{x_{BK}} \bmod p$

PCC

private key x_{PCC}

$y_{PCC} = g^{x_{PCC}} \bmod p$

PS

private key x_{PS}

$y_{PS} = g^{x_{PS}} \bmod p$

BI:

$M_{BI-BK} = (ACC_{BI}, ACC_{PCC}, ID_{pro}, AMOUNT, ID_{BI}, T_{BI-BK})$

choose a random number r_1

$C_1 = g^{r_1} \bmod p$

$C_2 = M_{BI-BK} \times y_2^{r_1} \bmod p$

BI $\xrightarrow{(C_1, C_2)}$ BK

BK:

$w = (C_1^{x_{BK}})^{-1} \bmod p$

$M_{BI-BK} = C_2 \times w \bmod p$

$M_{BK-BI} = (ACC_{BI}, ACC_{PCC}, M_{tra}, ID_{pro}, T_{BK-BI})$

choose a random number r_2

$d_1 = g^{r_2} \bmod p$

$s_1 = r_2^{-1}(M_{BK-BI} - x_{BK} d_1) \bmod p-1$

BI $\xleftarrow{M_{BK-BI}, (d_1, s_1)}$ BK

BI:

$y_{BK}^{d_1} \times d_1^{s_1} \stackrel{?}{=} g^{M_{BK-BI}} \bmod p$

$M_s = ((d_1, s_1), x_{BI}, ID_{BI}, ID_{PCC}, M_{\inf}, ID_{pro})$

$M_{BI-PCC} = ID_{pro}^{M_s} \bmod p-1$

BI $\xrightarrow{M_{req}}$ PCC

PCC:

choose a random number k

$\tilde{d}_2 = g^k \bmod p$

BI $\xleftarrow{\tilde{d}_2}$ PCC

BI:

choose random numbers (a, b, c)

$d_2 = \tilde{d}_2^{a} y^b g^c \bmod p$

$\tilde{M}_{BI-PCC} = a^{-1}(d_2 + h(M_{BI-PCC}) - b) - \tilde{d}_2 \bmod p\text{-}1$

BI $\xrightarrow{\tilde{M}_{BI-PCC}}$ PCC

PCC:

$\tilde{s}_2 = (\tilde{d}_2 + \tilde{M}_{BI-PCC})x_{PCC} - k \bmod p\text{-}1$

BI $\xleftarrow{\tilde{s}_2}$ PCC

BI:

$s_2 = a\tilde{s}_2 - c \bmod p-1$

(M_{BI-PCC}, d_2, s_2)

$M_{BI-PS} = (a, c, Amount, ID_{BI}, ID_{PCC}, T_{tra}, ID_{pro}, T_{BI-PS})$

choose a random number r_3

$C_3 = g^{r_3} \bmod p$

$C_4 = M_{BI-PS} \times y_{PS}^{r_3} \bmod p$

BI $\xrightarrow{(C_3, C_4)}$ PS

PS:

$w_1 = (C_3^{x_{PS}})^{-1} \bmod p$

$M_{BI-PS} = C_4 \times w_1 \bmod p$

$M_{PS-BI} = (M_{BI-PS}, T_{BI-PS})$

choose a random number k_1

$d_3 = g^{k_1} \bmod p$

$s_3 = k_1^{-1}(M_{PS-BI} - x_{PS} d_3) \bmod p-1$

(d_3, s_3)

BI $\xleftarrow{(M_{PS-BI}, d_3, s_3)}$ PS

BI:

$y_{PS}^{d_3} \times d_3^{s_3} \stackrel{?}{=} g^{M_{PS-BI}} \bmod p$

so that the BI can obtain the signature $(M_{BI\text{-}PCC}, d_2, s_2)$. The BI makes a bidding message for the PS:

$$M_{BI-PS}=(a,c,AMOUNT,ID_{BI},ID_{PCC},T_{tra},ID_{pro},T_{BI-PS}). \quad (22)$$

It chooses a random number r_3 and computes ciphertexts (C_3, C_4):

$$C_3 = g^{r_3} \bmod p \quad (23)$$

$$C_4 = M_{BI-PS} \times y_{PS}{}^{r_3} \bmod p \quad (24)$$

It sends the ciphertexts (C_3, C_4) to the PS.

Step 8: After receiving the ciphertext (C_3, C_4), the PS uses the private key x_{PS} to decrypt the messages C_3 and C_4:

$$w_1 = (C_3{}^{x_{PS}})^{-1} \bmod p \quad (25)$$

$$M_{BI-PS} = C_4 \times w_1 \bmod p. \quad (26)$$

Then, the BK chooses a random number k_1 and sends a response message $M_{PS\text{-}BI}$ (where $M_{PS\text{-}BI} = (M_{BI\text{-}PS}, T_{BI\text{-}PS})$), chooses a random number k_1 and computes a signature (d_3, s_3):

$$d_3 = g^{k_1} \bmod p \quad (27)$$

$$s_3 = k_1^{-1}(M_{PS-BI} - x_{PS} d_3) \bmod p-1. \quad (28)$$

After this, the PS sends the signature (d_3, s_3) and message $M_{PS\text{-}BI}$ to the BI.

Step 9: Upon receiving the signature (d_3, s_3) and message $M_{PS\text{-}BI}$, the BI verifies the signature as follows:

$$y_{PS}{}^{d_3} \times d_3{}^{s_3} \overset{?}{=} g^{M_{PS-BI}} \bmod p. \quad (29)$$

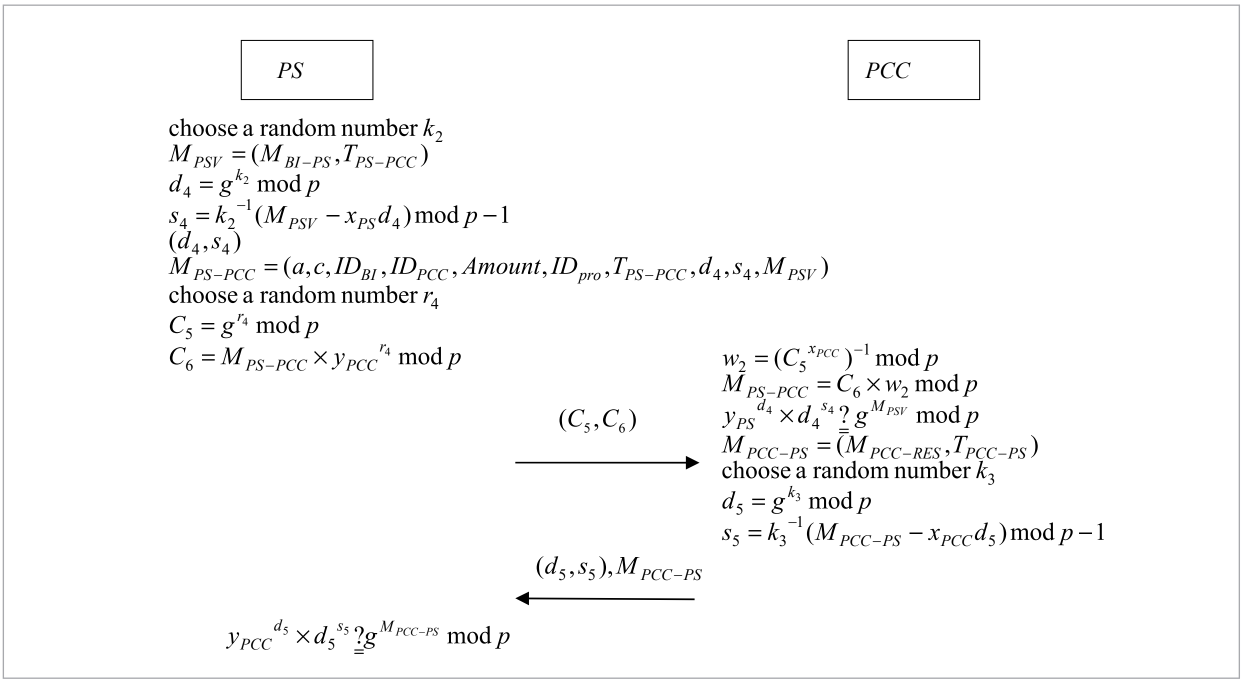
2.3. The Bidding Phase

After the deadline of the casting bid, PS sends the blind factor to the PCC. The PCC then uses the blind factor to obtain the bidding price. After this, the PCC publishes the winner. The scenario of the opening bid phase is shown in Figure 3.

Step 1: The PS chooses a random number k_2, and creates a message M_{PSV} (where $M_{PSV} = (M_{BI-PS}, T_{PS-PCC})$) and a signature (d_4, s_4):

$$d_4 = g^{k_2} \bmod p \quad (30)$$

Figure 3
The scenario of the opening bid phase



$$s_4 = k_2^{-1}(M_{PSV} - x_{PC}d_4) \bmod p-1. \quad (31)$$

The PS then creates a bidding message:

$$M_{PS-PCC} = (a, c, ID_{BI}, ID_{PCC}, Amount, ID_{pro}, T_{PS-PCC}, d_4, s_4, M_{PSV}). \quad (32)$$

Next it chooses a random number r_4 and computes ciphertexts (C_5, C_6):

$$C_5 = g^{r_4} \bmod p \quad (33)$$

$$C_6 = M_{PS-PCC} \times y_{PCC}^{r_4} \bmod p. \quad (34)$$

It then sends the ciphertexts (C_5, C_6) to *the* PCC.

Step 2: After receiving the ciphertexts (C_5, C_6), the PCC uses the private key x_{PCC} to decrypt the message:

$$w_2 = (C_5^{x_{PCC}})^{-1} \bmod p \quad (35)$$

$$M_{PS-PCC} = C_6 \times w_2 \bmod p. \quad (36)$$

The PCC verifies if the bidding message is valid or not:

$$y_{PS}^{d_4} \times d_4^{s_4} \overset{?}{=} g^{M_{PSV}} \bmod p. \quad (37)$$

Then, the PCC generates a response message M_{PCC-PS} (where $M_{PCC-PS} = (M_{PCC-RES}, T_{PCC-PS})$).

The PCC chooses a random number k_3 and computes the signature (d_5, s_5) as follows:

$$d_5 = g^{k_3} \bmod p \quad (38)$$

$$s_5 = k_3^{-1}(M_{PCC-PS} - x_{PCC}d_5) \bmod p-1. \quad (39)$$

Afterwards, the PCC sends the signature (d_5, s_5) and M_{PCC-PS} to the PS.

Step 3: Upon receiving the signature (d_5, s_5), the PS verifies the signature:

$$y_{PCC}^{d_5} \times d_5^{s_5} \overset{?}{=} g^{M_{PCC-PS}} \bmod p. \quad (40)$$

2.4. The Official Agent Arbitration Phase

In this phase, if there are concerns regarding the BI or PCC, the OA can offer fair arbitration by blind message and subliminal message. Once the accusation holds, the winner can request the bank to reveal the information of the accused party.

Case 1: The BI takes the subliminal message, blind message and blind factor to the OA. The OA then uses the related information to make a fair arbitration. The overview of the arbitration phase (PCC is accused) is shown in Figure 4:

Step 1: The BI generates an accusation message M_{BI-OA}:

$$M_{BI-OA} = (M_S, ID_{BI}, ID_{PCC}, ID_{pro}, M_{BI-PCC}, M_{PSV}, d_2, s_2). \quad (41)$$

It then chooses a random number r_5 and computes the ciphertexts (C_7, C_8):

$$C_7 = g^{r_5} \bmod p \quad (42)$$

$$C_8 = M_{BI-OA} \times y_{OA}^{r_5} \bmod p. \quad (43)$$

It then sends the ciphertexts (C_7, C_8) to the OA.

Step 2: Upon receiving the ciphertexts (C_7, C_8), the OA uses the private key x_{OA} to decrypt the message:

$$w_3 = (C_7^{x_{OA}})^{-1} \bmod p \quad (44)$$

$$M_{BI-OA} = C_8 \times w_3 \bmod p. \quad (45)$$

The OA then verifies the signature (d_2, s_2):

$$y_{PCC}^{d_2 + h(M_{BI-PCC})} \overset{?}{=} d_2 g^{s_2} \bmod p. \quad (46)$$

If Equation (47) holds, it then verifies the message M_{BI-PCC}:

$$M_{BI-PCC} \overset{?}{=} ID_{pro}^{M_S} \bmod p-1. \quad (47)$$

Using subliminal message M_S and accusation message M_{BI-OA}, the OA is able to make a fair arbitration.

Case 2: The PCC takes the blind message and blind factor to the OA. Then, the OA uses the related information to make a fair arbitration. The overview of the arbitration phase (BI is accused) is shown in Figure 5:

Step 1: The PCC generates an accusation message M_{PCC-OA} (where $M_{PCC-OA} = (ID_{BI}, ID_{PCC}, ID_{pro}, M_{PS-PCC}, D_{PS}, d_4, s_4)$).

The PCC then chooses a random number r_6 and computes ciphertexts (C_9, C_{10}):

Figure 4

The overview of the arbitration phase (PCC is accused)

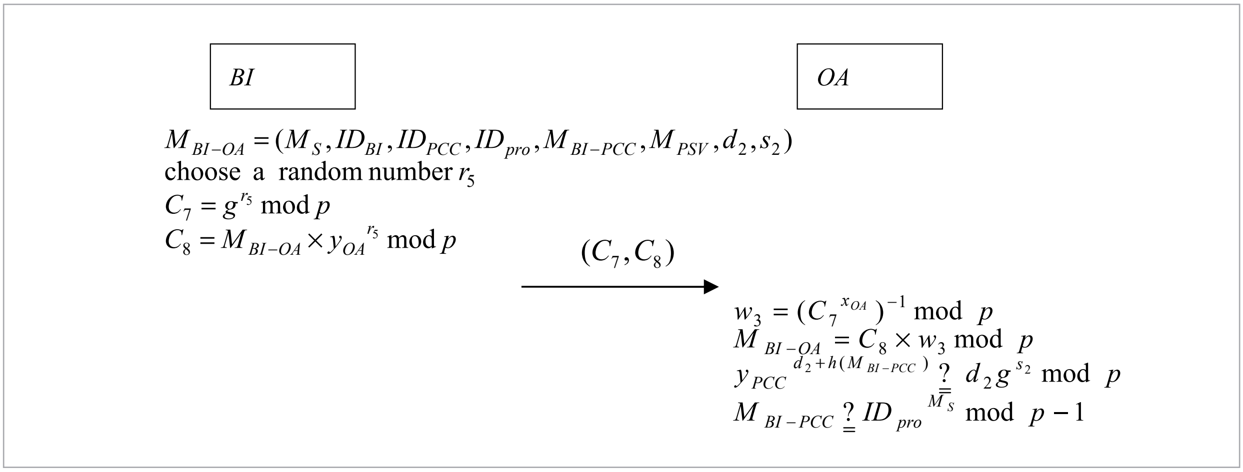
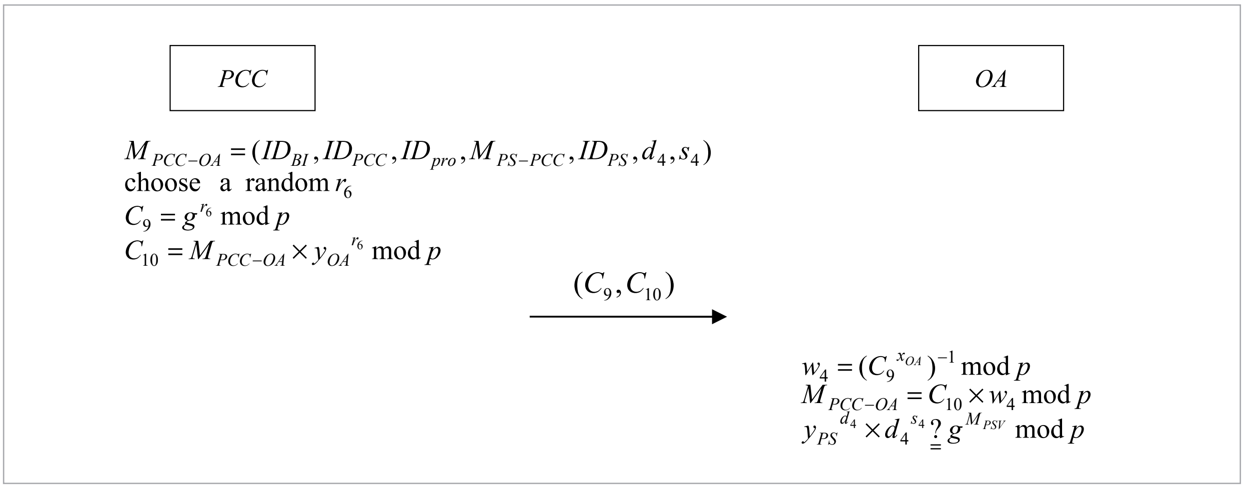


Figure 5

The overview of the arbitration phase (BI is accused)



$$C_9 = g^{r_6} \bmod p \tag{48}$$

$$C_{10} = M_{PCC-OA} \times y_{OA}^{r_6} \bmod p. \tag{49}$$

It then sends the ciphertexts (C_9, C_{10}) to the OA.

Step 2: After receiving the ciphertexts (C_9, C_{10}), the OA uses the private key x_{OA} to decrypt the message $M_{PCC\text{-}OA}$:

$$w_4 = (C_9^{x_{OA}})^{-1} \bmod p \tag{50}$$

$$M_{PCC-OA} = C_{10} \times w_4 \bmod p. \tag{51}$$

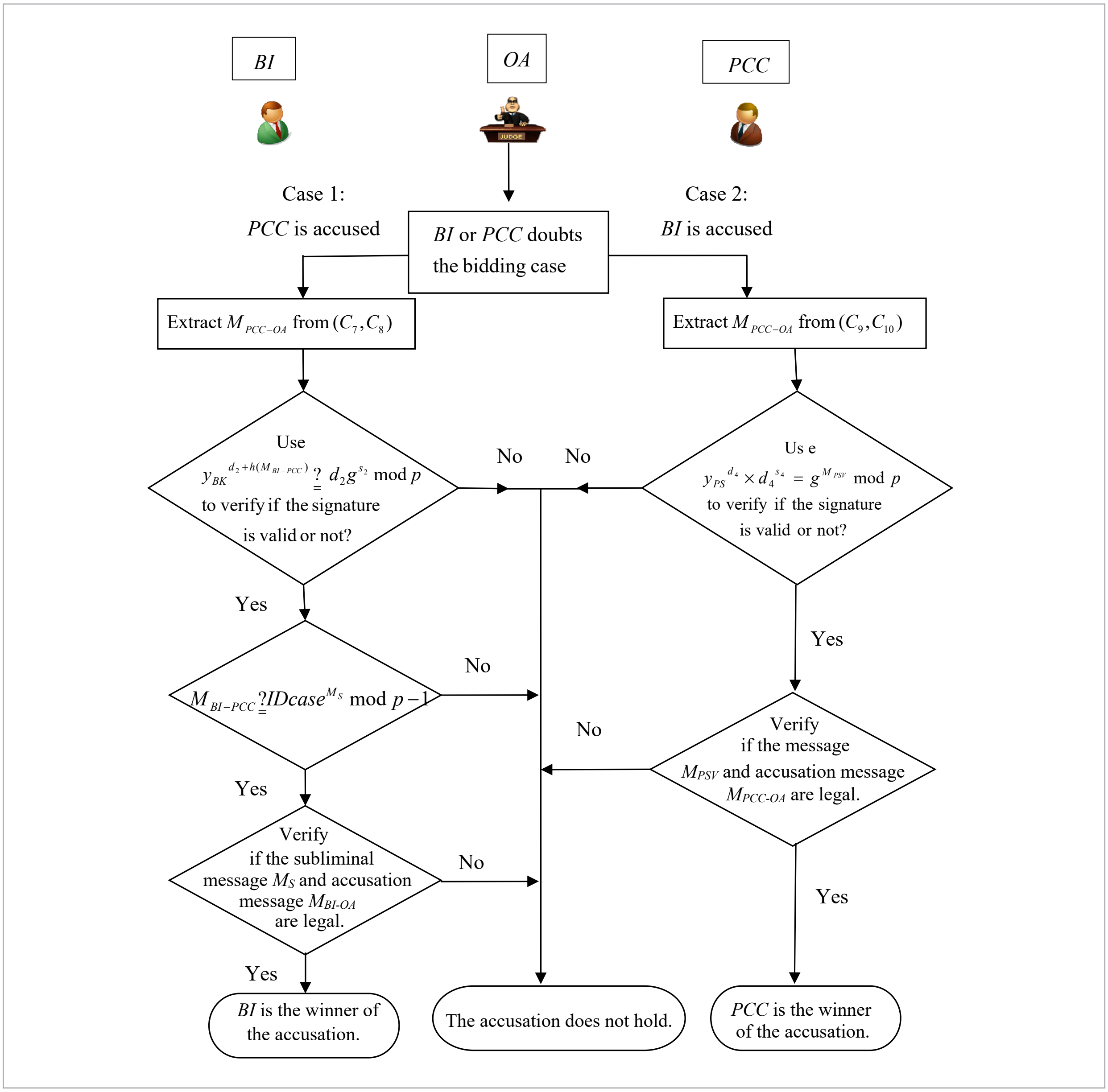
The OA then verifies the signature (d_4, s_4):

$$y_{PS}^{d_4} \times d_4^{s_4} \stackrel{?}{=} g^{M_{PSV}} \bmod p. \tag{52}$$

Using verified message M_{PSV} and accusation message $M_{PCC\text{-}OA}$, the OA can make a fair arbitration. The summary flowchart of the arbitration phase is shown in Figure 6.

Figure 6

The flowchart of the arbitration phase



3. Security Analysis

3.1. The Official Agent Arbitration Phase

The proposed protocol employs a digital signature mechanism to solve the non-repudiation problem with ElGamal signature and blind signature. The verifications are shown in Table 1.

3.2. Fair Arbitration

This section will illustrate how the proposed scheme provides fair arbitration.

Case 1: The BI doubts the PCC

In the arbitration phase, after receiving the message (C_7, C_8) from the BI, the OA will decrypt the ci-

Table 1
The non-repudiation issues

Non-repudiation proof	Proof issuer	Proof holder	Verification
(M_{BK-BI}, d_1, s_1)	BK	BI	$y_{BK}{}^{d_1} \times d_1{}^{s_1} \overset{?}{=} g^{M_{BK-BI}} \bmod p$
(M_{BI-PCC}, d_2, s_2)	BK	BI	$y_{BK}{}^{d_2+h(M_{BI-PCC})} \bmod p \overset{?}{=} d_2 g^{s_2} \bmod p$
(M_{PS-BI}, d_3, s_3)	PS	BI	$y_{PS}{}^{d_3} \times d_3{}^{s_3} \overset{?}{=} g^{M_{PS-BI}} \bmod p$
(M_{PSV}, d_4, s_4)	PS	PCC	$y_{PS}{}^{d_4} \times d_4{}^{s_4} \overset{?}{=} g^{M_{PSV}} \bmod p$
(M_{PCC-PS}, d_5, s_5)	PCC	PS	$y_{PCC}{}^{d_5} \times d_5{}^{s_5} \overset{?}{=} g^{M_{PCC-PS}} \bmod p$

phertexts and verify the BI's blind message $M_{BI\text{-}PCC}$: $y_{BK}{}^{d_2+h(M_{BI-PCC})} \bmod p \overset{?}{=} d_2 g^{s_2} \bmod p$. If the equation holds, the OA will verify the reality of message $M_{BI\text{-}PCC}$: $M_{BI-PCC} \overset{?}{=} ID_{case}{}^{M_S} \bmod p-1$. Then, the OA uses $M_{BI\text{-}PCC}$ and M_S to arbitrate the accusation.

The derivation of the blind signature verification is shown as follows:

$$
\begin{aligned}
& y_{PCC}{}^{d_2+h(M_{BI-PCC})} \bmod p \\
& = d_2 g^{s_2} \bmod p \\
& = (g^{ka} g^{x_{PCC} b} g^{c}) g^{a \tilde{s}_2 - c} \\
& = g^{ka} g^{x_{PCC} b} g^{a \tilde{s}_2} \\
& = g^{ka} g^{x_{PCC} b} g^{a[(\tilde{d}_2 + \tilde{M}_{BI-PCC}) x_{PCC} - k]} \\
& = g^{ka} g^{x_{PCC} b} g^{a x_{PCC} \tilde{d}_2} g^{a x_2 \tilde{M}_{BI-PCC}} / g^{ka} \\
& = g^{x_{PCC} b} g^{a x_{PCC} \tilde{d}_2} g^{a x_{PCC} \tilde{M}_{BI-PCC}} \\
& = g^{x_2 b} g^{a x_2 \tilde{d}_2} g^{a x_2 (a^{-1}(d_2 + h(\tilde{M}_{BI-PCC}) - b) - \tilde{d}_2)} \\
& = g^{x_{PCC} b} g^{a x_{PCC} \tilde{d}_2} g^{x_{PCC}(d_2 + h(\tilde{M}_{BI-PCC}))} / g^{b x_{PCC}} g^{a x_{PCC} \tilde{d}_2} \\
& = g^{x_{PCC}(d_2 + h(\tilde{M}_{BI-PCC}))} \\
& = y_{PCC}{}^{d_2+h(M_{BI-PCC})}
\end{aligned}
$$

Case 2: The BI doubts the PCC

In the arbitration phase, after receiving the message (C_9, C_{10}) from the PCC, the OA will decrypt the ciphertexts and send the message $M_{PCC\text{-}OA}$. It then verifies the PS's signature (M_{PSV}, d_4, s_4): $y_{PS}{}^{d_4} \times d_4{}^{s_4} \overset{?}{=} g^{M_{PSV}} \bmod p$. If the equation holds, then the OA uses M_{PSV} to arbitrate the accusation. This design can ensure fair arbitration.

The derivation of signature verification is shown as follows:

$$
\begin{aligned}
& g^{M_{PSV}} \bmod p \\
& = y_{PS}{}^{d_4} \times d_4{}^{s_4} \bmod p \\
& = g^{x_{PS} d_4} \times g^{k_2 k_2^{-1}(M_{PSV} - x_{PS} d_4)} \\
& = g^{x_{PS} d_4} \times g^{(M_{PSV} - x_{PS} d_4)} \\
& = g^{M_{PSV}}.
\end{aligned}
$$

3.3. The Blind and Unlinkable Issue

In the bidding phase, the BI sends the blind message to the PCC to sign the message. The blind signature scheme is secure against malicious attackers who work in the PCC. Even if the PCC receives the bidding message from the BI, the PCC does not know the message in the bidding phase. In the opening bid phase, the PCC retrieves the blind message in order to use the blind factor and other information from the PS. Therefore, the malicious attacker cannot obtain the BI's bidding message and identity in the bidding phase.

3.4. Auditability

In the official agent arbitration phase, the OA can ask the bank for the information of the BI and PCC when it receives an accusation message. Therefore, the proposed protocol provides auditability to help the OA offer fair arbitration.

3.5. One-Time Registration

The BI and PCC only need to register once with the BK and PS. This reduces computation cost and creates greater convenience for the bidder.

3.6. Defense Against Known Attacks

3.6.1. Replay Attack

The proposed scheme includes a timestamp mechanism, which varies for each transaction. If a malicious attacker attempts to replay a message, it will fail, making replay attacks impossible.

3.6.2. Forgery Attack

In the bidding phase, when the BI sends the bidding message to the PCC, it only sends the blind message; it is very difficult for an attacker to forge the message to pretend to be the bidder or other parties. The proposed scheme uses ElGamal encryption and decryption mechanism in each transaction. For example: the encryptions in the bidding phase are:

$C_1 = g^{r_1} \bmod p,\ C_2 = M_{BI-BK} \times {y_2}^{r_1} \bmod p$,

$C_3 = g^{r_3} \bmod p,\ C_4 = M_{BI-PS} \times {y_{PS}}^{r_3} \bmod p$

And the decryptions are:

$w = ({C_1}^{x_{BK}})^{-1} \bmod p$,

$M_{BI-BK} = C_2 \times w \bmod p$,

$w_1 = ({C_3}^{x_{PS}})^{-1} \bmod p$ and

$M_{BI-PS} = C_4 \times w_1 \bmod p$.

Thus, only the real receiver has his/her own private key, and can decrypt the message. Thus attackers cannot achieve forgery attacks.

3.6.3. Insider Attack

If an attacker works in the PCC or has a relationship with PCC staff, he/she will only be able to obtain the deadline of the bid in the bidding phase from these sources, not the bidding price; the proxy server transfers the bidding message to the PCC and uses the blind signature (d_2, s_2) to protect the bidding price $M_{\inf}$ in the bidding phase.

4. Discussion

This paper compares the computation cost in Table 2, and makes a security comparison in Table 3. In the

Table 2

The computation cost of our scheme

Phase	Hwang et al.'s scheme [6]	Liaw et al.'s scheme [8]	Chung et al.'s scheme [3]	Xiong et al.'s scheme [19]	Our scheme
The registration phase	$5T_{Exp}$	$6T_{Exp}$	$5T_{Exp}$+$2T_{Mut}$+ $2T_H$	$4T_{Exp}$+$1T_{Mut}$+ $2T_H$	NA
The bidding phase	$12T_{Exp}$	$10T_{Exp}$	$8T_{Exp}$+$7T_{Mut}$+$6T_H$	$2T_{pair}$+$2T_{Exp}$+ $2nT_{sca}$	$2T_H$+$18T_{Exp}$+ $20T_{XOR}$+$20T_{Mut}$
The opening bid phase	NA	NA	$3T_{Exp}$+$1T_{Mut}$+ $1T_H$	$1T_{pair}$+$2T_{Exp}$+ $2nT_{sca}$	$13T_{Exp}$+$11T_{XOR}$+$9T_{Mut}$
The product exchange and the payment phase	$10T_{Exp}$	$8T_{Exp}$	NA	NA	NA
The official agent arbitration phase	NA	NA	NA	NA	$13T_{Exp}$+$13T_{XOR}$+ $10T_{Mut}$
Total	27nT_{Exp}	24nT_{Exp}	($11T_{Exp}$+$8T_{Mut}$+ $7T_H$)n+$6T_{Exp}$+ $2T_{Mut}$+ $2T_H$	($3T_{pair}$+$4T_{Exp}$+ $4nT_{sca}$)n+$4T_{sca}$+ $1T_{Mut}$+ $2T_H$	$44T_{Exp}$+$39T_{Mut}$+ $44T_{XOR}$ +$2T_H$
Execution time	≈16.2n ms	≈14.88n ms	≈(6.84n+3.73)ms	≈(11.78+0.3n)n ms	≈27.38n ms

Note: n is the number of bidders; T_H is the time complexity of one-way hash function; T_{Exp} is the time for executing the modular exponential operation; T_{Mut} *is the* time complexity for executing the modular multiplication; T_{XOR} is the time for exclusion or operation; T_{sca}: the time cost of a scalar multiplication; and T_{pair}: the time cost of a pairing operation.

T_{pair}= 3.10 ms, T_{Exp}= 0.62 ms (on 3 GHz Pentium IV [13]). $T_{pair} \approx 5T_{Exp}$, $T_{sca} \approx 29T_{Mut}$, $T_{Exp} \approx 240T_{Mut}$ [7,12,20].

Table 3
The security comparison of the related works and our scheme

Security Issues	Hwang et al.'s scheme [6]	Liaw et al.'s scheme [8]	Chung et al.'s scheme [3]	Xiong et al.'s scheme [19]	Our scheme
Privacy	No	No	Yes	Yes	Yes
Atomicity	Yes	Yes	Yes	Yes	Yes
Non-repudiation	Yes	Yes	Yes	Yes	Yes
Unforgeability	Yes	Yes	Yes	Yes	Yes
Unlinkability	No	No	Yes	Yes	Yes
One-time registration	No	No	No	No	Yes
Auditability	No	Yes	Yes	Yes	Yes
Off-line TTP	No	No	Yes	Yes	Yes
Fair arbitration protocol	No	No	No	No	Yes

proposed scheme, an exponential operation is used to achieve a secure protocol. Although the proposed scheme requires greater computation cost, it is more secure than related works.

5. Conclusions

This paper proposes an electronic public engineering project bidding protocol via a subliminal channel which is suitable for the bidding protocol for public construction projects. The proposed scheme satisfies the following properties: non-repudiation, fair arbitration, blind message, unlinkable, one-time registration and auditability. An exponential operation and ElGamal encryption are used to ensure transaction processing safety, and subliminal messages and blind signatures are used to ensure bidders' privacy and security. Moreover, a fair arbitration protocol was designed to ensure fair transactions.

Although the computation cost of the proposed scheme is higher than related works, the scheme is more secure and suitable for public engineering projects.

Acknowledgements

This research was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract number MOST 106-2622-E-305-001-CC2, MOST 106-2221-E-324 -013 and MOST103-2632-E-324-001-MY3.

References

1. Chen, C. L., Liao, J. J. A Fair Online Payment System for Digital Content via Subliminal Channel. Electronic Commerce Research and Applications, 2011, 10(3), 279-287. https://doi.org/10.1016/j.elerap.2010.09.001
2. Chen, C. L., Liu, M. H. A Traceable E-Cash Transfer System Against Blackmail via Subliminal Channel. Electronic Commerce Research and Applications, 2009, 8(6), 327-333. https://doi.org/10.1016/j.elerap.2009.04.012
3. Chung, Y. F., Huang, K. H., Lee, H. H., Lai, F., Chen, T. S. Bidder-Anonymous English Auction Scheme with Privacy and Public Verifiability. Journal of Systems and Software, 2008, 81(1), 113-119. https://doi.org/10.1016/j.jss.2007.03.029
4. Fan, C. I., Wu, C. N., Sun, W. Z., Chen, W. K. Multi-Recastable E-Bidding Game with Dual-Blindness. Mathematical and Computer Modelling, 2013, 58(1-2), 68-78. https://doi.org/10.1016/j.mcm.2012.06.003
5. Harn, L., Gong, G. A Digital Signature with a Subliminal Channel. IEE Proceedings, Computers and Digital Techniques, 1997, 144(6), 387-389. https://doi.org/10.1049/ip-cdt:19971511
6. Hwang, M. S., Lu, E. J. L., Lin, I. C. Adding Timestamps to the Secure Electronic Auction Protocol. Data & Knowledge Engineering, 2002, 40(2), 155-162. https://doi.org/10.1016/S0169-023X(01)00048-9
7. Koblitz, N., Menezes, A. J., Vanstone, S. A. The State of Elliptic Curve Cryptography. Design, Codes and Cryptography, 2000, 19(2-3), 173-193. https://doi.org/10.1023/A:1008354106356

8. Liaw, H. T., Juang, W. S., Lin, C. K. An Electronic Online Bidding Auction Protocol with Both Security and Efficiency. Applied Mathematics and Computation, 2006, 174(2), 1487-1497. https://doi.org/10.1016/j.amc.2005.06.016
9. Lin, D. R., Wang, C. I., Zhang, Z. K., Guan, D. J. A Digital Signature with Multiple Subliminal Channels and Its Applications. Computers & Mathematics with Applications, 2010, 60(2), 276-284. https://doi.org/10.1016/j.camwa.2010.01.001
10. Lu, Y., Li, L., Peng, H., Yang, Y. A Biometrics and Smart Cards Based Authentication Scheme for Multi-Server Environments. Security and Communication Networks, 2015, 8(17), 3219-3228. https://doi.org/10.1002/sec.1246
11. Lu, Y., Li, L., Yang, X., Yang, Y. Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards. PLoS ONE, 2015, 10(5), e0126323.doi:10.1371/journal.pone.0126323. https://doi.org/10.1371/journal.pone.0126323
12. Menezes, A. J., Oorschot, P. C. V., Vanstone, S. A. Handbook of Applied Cryptography. CRC Press LLC, Boca Raton, 1996. https://doi.org/10.1201/9781439821916
13. Scott, M. Implementing Cryptographic Pairings. Proceedings of the 1st International Conference on Pairing-Based Cryptography, 2007, 177-196.
14. Seo, S. H., Choi, K. Y., Hwang, J. Y., Kim, S. Efficient Certificateless Proxy Signature Scheme with Provable Security. Information Sciences, 2012, 188(1), 322-337. https://doi.org/10.1016/j.ins.2011.11.005
15. Simmons, G. J. The Prisoner's Problem and the Subliminal Channel. Proceedings of Crypto '83, New York, 1983, 51-67.
16. Simmons, G. J. The Subliminal Channel and Digital Signatures. Lecture Notes in Computer Science (LNCS), 1985, 209, 364-378. https://doi.org/10.1007/3-540-39757-4_25
17. Simmons, G. J. Subliminal Communication Is Easy Using the DSA. Lecture Notes in Computer Science (LNCS), 1994, 765, 218-232. https://doi.org/10.1007/3-540-48285-7_18
18. Subramanian, S. Design and Verification of a Secure Electronic Auction Protocol. Proceedings of 17th IEEE Symposium on Reliable Distributed Systems, 1998, 204-210. https://doi.org/10.1109/RELDIS.1998.740497
19. Xiong, H., Chen, Z., Li, F. Bidder-Anonymous English Auction Protocol Based on Revocable Ring Signature. Expert Systems with Applications, 2012, 39(8), 7062-7066. https://doi.org/10.1016/j.eswa.2012.01.040
20. Zhang, Y., Liu, W., Lou, W., Fang, Y. Securing Mobile Ad Hoc Networks with Certificateless Public Keys. IEEE Transactions on Dependable and Secure Computing, 2006, 3(4), 386-399. https://doi.org/10.1109/TDSC.2006.58

Summary / Santrauka

Due to the rapid development of the Internet, many Internet applications have recently become very widely used. Internet security has therefore become an important issue. This paper proposes an electronic public engineering project bidding protocol via a subliminal channel. In the proposed scheme, the subliminal channel can protect a bidder's interests, while allowing an official agent to make a fair arbitration. The proposed scheme is non-repudiable, untraceable and offers fair arbitration of public engineering projects, but is also resistant to replay, forgery and insider attacks, thus enhancing both security and fairness.

Dėl sparčios interneto plėtros daugelis interneto programų tapo labai plačiai naudojamos. Tai lėmė, kad interneto saugumas tapo svarbiu klausimu. Straipsnyje pateikiamas elektroninių viešųjų inžinerinių projektų siūlymo per užslaptintą kanalą protokolas. Siūlomoje schemoje užslaptintas kanalas gali apsaugoti konkurso dalyvio interesus, tuo tarpu leidžiant oficialiam agentui atlikti sąžiningą arbitražą. Siūloma schema yra ne tik neatmetama, nesusekama ir siūlanti sąžiningą viešųjų inžinerinių projektų arbitražą, bet taip pat ir atspari pakartojimo atakoms, klastojimui ir atakuotojams tinklo viduje. Straipsnio autorių siūloma schema taip pat padidina tiek saugumą, tiek sąžiningumą.