International Journal of Technology 13(6) 1222-1230 (2022)
Received April 2022 / Revised August 2022 / Accepted August 2022

International Journal of Technology

http://ijtech.eng.ui.ac.id

# Secure Cryptographic E-Auction System

Soo-Chin Tan[1], Swee-Huay Heng[1*]

[1]*Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450, Melaka, Malaysia*

**Abstract.** The evolution of the auction market has been on the upswing throughout the years as technology evolves at an accelerating rate. With the advanced technology nowadays, digital transformation has been applied to the auction markets as a means of transferring goods or services in an online form. Electronic auctions enable sellers to reach a broader range of prospective bidders and participate in the auctions anywhere-anytime. Nevertheless, the security aspects of the e-auction system have become the main concerns for the parties involved. Hence, a secure cryptographic electronic auction system is proposed by employing the underlying cryptographic schemes as the building blocks, namely, asymmetric encryption, digital signature scheme, and hash functions. The proposed e-auction system fulfills the security requirements, encompassing anonymity, correctness, confidentiality, privacy, integrity, and fairness. Performance analysis has also been performed on our proposed e-auction system.

*Keywords:* Asymmetric Encryption; Digital Signature; E-Auction; Security

## 1. Introduction

In recent years, the pace of information technology development and implementation has arrestingly accelerated. The rapid growth of technology influences people's lifestyles, especially in digital transformation (Tashenova et al., 2020). Several applications are transformed from physical to online systems, especially electronic auctions (e-auction). E-auction has become extremely popular and a trend in this modern era as it is convenient in allowing interested bidders to participate in an auction without physically attending it. Within a specified timeframe of the auctioned product, the bidders can place their bids effectively on an anywhere-anytime basis Lee et al. (2008). However, several privacy and security issues emerge, such as a prejudiced auctioneer, privacy issues of the participants, the integrity of the bid, and the correctness of the auction rule.

Therefore, various cryptographic primitives are used to mitigate the security concerns encountered in e-auction systems and achieve the security goals for an e-auction system, such as integrity, confidentiality, and fairness. In this work, a secure cryptographic e-auction system is developed with the implementation of both asymmetric encryption and digital signature using Java Cryptography Architecture (JCA) (Rabah, 2006). Then, the security properties evaluation of the proposed system and performance result have been determined in this paper.

*Corresponding author's email: shheng@mmu.edu.my, Tel.: +60-6-2523600; Fax: +60-6-2318840
doi: 10.14716/ijtech.v13i6.5827

### *1.1. First-Price Sealed-Bid Auction*

Generally, the sealed-bid auction is dubbed the blind auction, which allows the bidders to place their sealed bids concurrently to the auctioneer, and all the bids remain confidential (Guo et al., 2017). Unlike an open-outcry auction, where the bidders can make multiple bids and compete against each other actively, a bidder can only place one sealed bid on the auctioneer at one time without further modification. In this case, none of the bidders will be aware of the competing bids. After the auction closes, the highest bidder will be declared the winner. In FPSBA, the winner pays the amount of his bid for the winning auctioned product.

### *1.2. Security Properties*

Security has always been one of the primary concerns for any e-auction system, and it should be considerable attention during system development. An e-auction system should fulfill the following essential properties (Peng et al., 2002; Guo et al., 2017):

- **Anonymity.** During the bidding, bid information and participants' identities should be kept anonymous.
- **Correctness.** The auction result should be computed correctly based on the chosen auction rule.
- **Confidentiality.** During the bidding process, each bid will be kept confidential.
- **Privacy.** The public will know only the winning bid; other bids remain secret.
- **Integrity.** No one can modify bid prices after the bidder places the bid.
- **Fairness.** The bidder with the highest bids will be the winner of the auction and this ensures the honesty of the transaction between the winning bidder and auctioneer.

## 2. Related Works

### *2.1. Existing E-Auction Schemes*

The privacy of the sellers and buyers is very crucial in an e-auction. Hence, Gao et al. (2020) proposed an auction system called Enhanced Privacy-Preserving Auction Scheme (*EPPAS*) that uses homomorphic encryption to guarantee that all bids are encrypted during the auction. Paillier cryptosystem was used for the appliance of homomorphic encryption with a One-Time Pad (*OTP*).

According to Wu et al. (2008), the processing speed for symmetric encryption is more expeditious than asymmetric encryption. Thus, they proposed a sealed-bid e-auction using symmetric encryption. To ensure secure communication, the web exists in the third party's internal network and is protected by the third party. Accordingly, only a third party can broadcast the information, while other participants are only permitted to download it. Wu et al. (2008) claimed that the proposed system is secure enough as it provides both functionality and efficiency.

Lee et al. (2008) have proposed a reliable sealed-bid e-auction system based on a group signature scheme with the authenticated encryption function. Public cryptosystems are used to secure communication through a public channel, while the group signature approach is implemented to safeguard confidential information. The proposed group signature-based e-auction scheme involves four parties: bidders, a registration manager (*RM*), an auction manager (*AM*), and an identity manager (*IM*) (Lee et al., 2008).

Meanwhile, a blockchain is used to access, verify, and transmit information through distributed nodes. It offers identity authentication to prevent counterfeiting attacks through public key cryptosystems. Blockchain uses a peer-to-peer technique to perform communication between each node and broadcasting. The transactions stored in a block are verifiable and recorded in the same ledger (Berawi et al., 2021).

Several e-auction systems based on blockchain have been proposed and developed. For instance, Chen et al. (2018) introduced an e-auction system based on blockchain with the implementation of smart contracts. The smart contract, which is comprised of the auctioneer's data, the starting and ending time of the auction, the ongoing winner's address, and the ongoing highest bid, is implemented through the Ethereum platform and will be triggered when certain events occur. However, the proposed system by Chen et al. (2018) might have an issue with the contract function calls due to the intricacy of the smart contract. The authors also provided a solution for the issue: to adjust the authority level for different functions.

Furthermore, Khan et al. (2019) proposed a blockchain-based e-auction system that aims to diminish the security weakness of e-auction systems through a decentralized, trustless, and autonomous auction system, where the role of a middle trading agent is allocated among all the parties of the auction.

In addition, Blass and Kerschbaum (2020) proposed a sealed-bid auction system based on blockchain and named BOREALIS. A multi-party computation of pairwise comparisons has been performed in the proposed BOREALIS without revealing bids. The authors chose additively homomorphic ElGamal encryption to ensure that the integer values are not visible among the parties when performing core comparisons. Furthermore, BOREALIS completes in three rounds only.

### *2.2. Comparative Analysis among E-Auction Schemes*

In general, the primary goals of employing the respective cryptographic schemes (Lee et al., 2008; Wu et al., 2008; Chen et al., 2018; Khan et al., 2019; Blass and Kerschbaum, 2020; Gao et al., 2020) in constructing e-auction systems are to fulfill the security requirements such as confidentiality, anonymity, privacy, and integrity. Table 1 presents a comparison of the secure e-auction schemes.

## 3. Proposed Secure E-Auction System

According to Wu et al. (2008), the proposed e-auction system with a symmetric encryption scheme is vulnerable to the point of failure since it relies on the existence of a third party. Hence, the authors were motivated to create a secure e-auction system with both asymmetric encryption and digital signature implementation in this research. It is developed using Java programming language and an H2 database for storing data. The proposed system utilized the Java Cryptography packages, such as *java.security* and *javax.crypto*. Our proposed e-auction system only involves two entities, which are Auctioneer and Bidder. It utilizes an RSA key pair consisting of a public key (*pk*) and private key (*sk*) to perform encryption, decryption, signature creation, and signature verification. More specifically, the following cryptographic schemes will be deployed, namely, hash functions, asymmetric encryption scheme, and digital signature scheme.

### *3.1. Hash Function*

The integrity and security of the participant information is the main priority in developing a secure e-auction system. Hence, the hash function is useful as it can be used to perform verification of the integrity of data against the stored hash. A hash function performs data mapping from arbitrary size to fixed-size values. Table 2 demonstrates the security properties of a secure hash function. The proposed scheme utilized jBCrypt and SHA-256 hash functions to hash the credential information.

**Table 1** Comparative Analysis of E-Auction Schemes

| Underlying Cryptographic Scheme | Strengths | Weaknesses |
|---|---|---|
| Homomorphic Encryption | • Achieve auction privacy, correctness, public verifiability, and receipt-freeness<br>• Prevent bid-rigging attacks, tampered data, and harmful entities | • Not suitable for large-scale auction<br>• Slow processing due to heavy computation in the signature verification mechanism |
| Symmetric Encryption | • Fast processing speed<br>• Can mitigate eavesdropping, replay, and impersonation attacks<br>• Prevent conspiracy attacks between third parties and malicious bidders | • Point of failure as it relies on the third party<br>• No formal proof available to achieve desirable security |
| Group Signatures | • Achieve privacy, anonymity, verifiability, non-repudiation, and performance in terms of efficiency and time complexity | • Can lead to forgeability issues due to the potential conspiration between the registration manager and auction manager<br>• Modification attack |
| Blockchain | • Communicate, verify, and transmit information through distributed nodes<br>• Eliminate the cost of the intermediary or mediator<br>• Address concerns related to distrust or lack of trading party information<br>• Prevent the bid price from leaked by the lead bidder | Could be vulnerable to the following security attacks:<br>• Replay<br>• Manipulation<br>• Repudiation |

**Table 2** Security Properties for a Secure Hash Function (Thiyagarajan & Ganesan, 2015)

| Requirement | Description |
|---|---|
| Efficiency | Given $x$, $h(x)$ is easy to be computed. |
| Pre-image resistant | Given $y$, it is computationally infeasible to find another input $x$. |
| Second | It is weak collision resistance. |
| pre-image resistant | Given $x_1$, it is computationally infeasible to find $x_2$ which satisfies the equation $h(x_1) = h(x_2)$. |
| Collision resistant | It is strong collision resistance.<br>It is computationally infeasible to find any pair,<br>e.g., $x_1$ and $x_2$, which satisfies the equation $h(x_1) = h(x_2)$. |

### *3.2. RSA Asymmetric Encryption and Digital Signature Scheme*

The proposed scheme utilized RSA asymmetric encryption and digital signature with the support of Java Cryptography Architecture (JCA) (Rabah, 2006). Table 3 lists the five RSA algorithms used in the proposed scheme.

**Table 3** Algorithm of RSA Asymmetric Encryption and Digital Signature Scheme

| Algorithm | Input | Output | Description |
|---|---|---|---|
| Key Generation | Asymmetric algorithm (RSA) and key size | The public key and private key | RSA key pair generation is done with the Java Security package, *java.security.KeyFactory* |
| Encryption | Original bid price and auctioneer's public key | Token (encrypted bid) | Token generation is done with the Java Crypto package, *javax.crypto.Cipher* |
| Signature Generation | Signing algorithm (RSA), token, and bidder's private key | Signature of bid | Signature generation is done with the Java Security package, *java.security.Signature* |
| Signature Verification | Signing algorithm (RSA), token, the signature of the bid, and the bidder's public key | Result verification | Signature verification is done with the Java Security package, *java.security.Signature* |
| Decryption | Encrypted bid and auctioneer's private key | Decrypted bid | Bid decryption is done with the Java Crypto package, *javax.crypto.Cipher* |

### *3.3. Algorithms of the Proposed System*

The proposed e-auction scheme consists of three phases: *Setup*, *Bid*, and *Open*.

- **Setup**. Once the user registers for an account, either an auctioneer account or a bidder account, the system generates an RSA key pair, which are the public key (*pk*) and private key (*sk*). Please refer to Table 4.

**Table 4** Algorithm for *Setup* phase

**Algorithm:** *Setup*

1. *n*: secure random number
2. User registers a new account
3. Generate key pair with a key size of 2048:
4. *keypair* ← (2048, *n*)
5. Get *pk*, *sk* from *keypair*
6. Update *pk*, *sk* on database

- **Bid**. Bidder performs bid creation that conceals his entered bidding price using auctioneer's *pk*. Then, the digital signature of the sealed bid is created using the bidder's *sk* to ensure the integrity of the bid. The sealed bid and its signature are transmitted and updated on the database. Please refer to Table 5.

**Table 5** Algorithm for *Bid* phase

Algorithm**:** *Bid*

1. *t*: token
2. *s*: signature of the token
3. Bidder submits *bid* to join the auction
4. Retrieve auctioneer's *pk*, bidder's *sk*
5. Generates sealed-bid:
6. *t* ← *Enc*(*bid*, auctioneer's *pk*)
7. Generates signature:
8. *s* ← (bidder's *sk*, *t*)
9. Update *t*, *s* on the database

- **Open**. Upon the auction deadline, all the sealed bids will be decrypted and compared to determine the winning bidder once the verification of the signature is passed. Then, the system updates the winning bid on the participant's panel, and only the winner can see his winning product in his panel, as depicted in Table 6.

**Table 6** Algorithm for *Open* phase

**Algorithm:** *Open*

1. $T = \{t_1, t_2, \ldots\ldots t_n\}$
2. $S = \{s_{t1}, s_{t2}, \ldots\ldots s_{tn}\}$
3. *B*: list of original *bids*
4. Retrieve auctioneer's *sk*, bidder's *pk*, *T*, *S*
5. **for** each item *i* **in** *T* **do**
6. | **for** each item *i* **in** *S* **do**
7. | | *signature verification* ← ($t_i$, $s_i$, bidder's $pk_i$)
8. | | **if** *signature verification* fails **then**
9. | | | $bid_i$ ← 0
10. | | **else**
11. | | | $bid_i$ ← *Dec*($t_i$, auctioneer' $sk_i$)
12. | | **end if**
13. | | add $bid_i$ → *B*
14. | **end for**
15. **end for**
16. Initialise *max* = 0
17. **for** each item *bid* **in** *B* **do**
18. | **if** *bid* > *max* **and** *bid* ∈ *B* **then**
19. | | *max* ← *bid*
20. | **else**
21. | | *max* ← *max*
22. | **end if**
23. **end for**
24. Determine the winner which placed *max*
25. Update winning result

### *3.4. Implementation of the Proposed System*

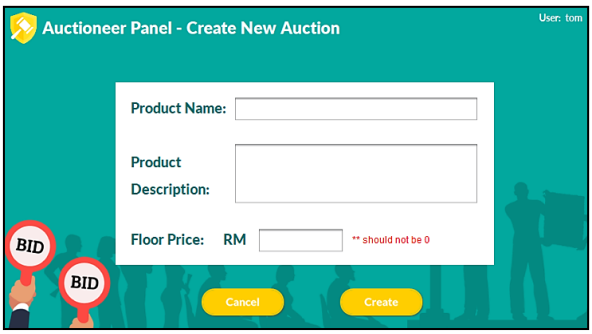
The proposed system utilizes jBCrypt to hash the user password using a computationally intensive algorithm based on Bruce Schneier's Blowfish cipher. The system also utilizes the SHA-256 hash function to hash the user information, such as username. Furthermore, the proposed system uses RSA encryption to perform encryption and decryption of the bid. First, the proposed system generates an RSA key pair for each registered auctioneer and bidder. The key pair is developed with a default modulus key size of 2048-bit and a cryptographically strong random number. The RSA function is implemented using *java.security* package and the latest version of RSA used is 2.2 which follows the PKCS #1 standard (Wikipedia, 2021).

In the proposed system, the bidder's plain bid is encrypted first using the auctioneer's *pk* of the selected auction by the bidder during the transmission of a bid to the system. Next, the encrypted bid ($s_t$) signature is created and stored in the database to ensure the integrity of the bid. The proposed system follows the auction rule of FPSBA, as all the bidders can only place one bid for the same auction. Following the auction deadline, the proposed system moves on to bid opening. It retrieves the lists of sealed-bid ($T$) and signature of sealed-bid ($S_T$), then decrypts the sealed-bid using the auctioneer's *sk* once it passes the signature verification. All the opening bids are then compared to determine the winner. Once the highest bid (*max*) is determined, the system publishes and updates the winning price. All the auction participants can view the winning price only, and only the winner can view his winning product in his bidder panel.

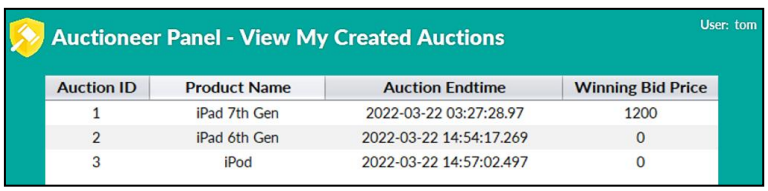
### *3.5. Proposed System User Interface*

#### 3.5.1. Auctioneer Panel

Once the auctioneer is successfully logged in, the system displays the Auctioneer Panel. There are two main features offered to the auctioneer: *Create New Auction* and *View My Created Auctions*. Figure 1(a) portrays the *Create New Auction* menu, where the auctioneer can create a new auction by entering the product details and setting the floor price. Then, the auctioneer can view his created auction records in *View My Created Auctions* menu, as depicted in Figure 1(b). The winning bid price is displayed after the winner's determination. If the winning bid price is 0, it means that the auction is not closed yet or there is no bidder participation.




(a)

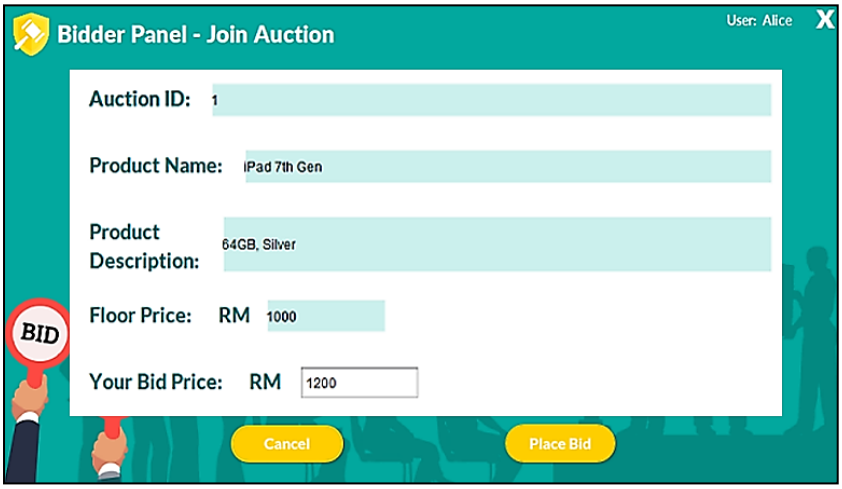



(b)

**Figure 1** Auctioneer Panel: (a) *Create New Auction* Menu; (b) *View My Created Auctions* Menu

3.5.2. Bidder Panel

The system displays the Bidder once a bidder has successfully logged in. The Bidder has four main features: *View Ongoing Auctions*, *Join Auction*, *View My Participated Auctions*, and *View My Winning Products*. To join an auction, the bidder can place a bid higher than the floor price set by the auctioneer, as illustrated in Figure 2(a). When a bidder attempts to resubmit a bid for a previously joined auction, the system will display an error message. The auction records are displayed in the *View My Participated Auctions* menu, a similar interface to Auctioneer Panel – *View My Created Auctions* menu. If the bidder has been awarded as the winner of the auction, the auction details will be shown in the winner's *View My Winning Products* menu, as shown in Figure 2(b). The winner information is not published.




(a)


(b)

**Figure 2** Bidder Panel: (a) *Join Auction* Menu; (b) *View My Winning Products* Menu

## 4. Testing and Evaluation

### *4.1. Security Requirements Evaluation*

The proposed system is a secure e-auction system as it had fulfilled the following security properties:

- **Anonymity**. The participants' identity remains anonymous during the bidding as all the bidders only know the auction ID. Only the winning price is published, and the identity of the winner remains anonymous.
- **Correctness**. Based on the FPSBA auction rule, the auction result is computed correctly. If multiple bidders place bids at the same bid price, the system will select the winning bidder as the first bidder.
- **Confidentiality**. Each bid is encrypted and remains confidential during the bidding phase.

- **Privacy**. Only the winning bid will be publicly released and known by the participants; other bids remain secret.
- **Integrity**. Each bidder is only allowed to submit one bid, and they cannot submit a second bid that replaces the previous bid. To ensure the integrity of the bid, a signature is created based on the encrypted bid. If the signature does not match, then the bid price is set to 0 to avoid it becoming the winning price.
- **Fairness**. The bidder with the highest bids will be the winner of the auction, and the winner can view his products on his bidder panel.

Table 7 illustrates a comparative analysis of existing schemes and the proposed system. Compared to other existing systems, the proposed system is considered to be more secure. It is also a better choice than the symmetric encryption scheme proposed by Wu et al. (2008) as it does not rely on a third party and thus eliminates the single point of failure. Furthermore, the proposed system could reduce impersonate attacks as during the bidding phase, only the bidder owner can sign the sealed bid.

**Table 7** Comparative Analysis between Existing Schemes and Proposed System

| Security Property | Homomorphic Encryption | Symmetric Encryption | Group Signature | Blockchain | Proposed System |
|---|---|---|---|---|---|
| Anonymity | | ✓ | ✓ | | ✓ |
| Correctness | ✓ | ✓ | ✓ | ✓ | ✓ |
| Confidentiality | ✓ | ✓ | ✓ | ✓ | ✓ |
| Privacy | ✓ | ✓ | ✓ | ✓ | ✓ |
| Integrity | ✓ | ✓ | ✓ | ✓ | ✓ |
| Fairness | | ✓ | | ✓ | ✓ |

### *4.2. Performance Analysis*

The proposed system is developed using Java language with the utilization of Java Security and Cryptography packages. The testing activity was performed on a Window machine with an Intel® Core™ i5-8250U processor running at 1.60GHz and 8GB of RAM. Table 8 depicts the performance result of the proposed system from the aspect of RSA key pair generation, encryption, and decryption which are employed in the algorithms, *Setup*, *Bid*, and, *Open*. The proposed system is fast since the signature verification, and decryption for an encrypted bid included in the *Open* phase only takes up an average of 2580.89 milliseconds. For the *Setup* phase, it takes up an average of 208.27 milliseconds, while it takes up an average of 1148.30 milliseconds for the *Bid* phase, where the bid encryption and signature creation are being carried out.

**Table 8** Performance Result

| Algorithm | Average Build Time (*ms*) |
|---|---|
| Setup | 208.27 |
| Bid | 1148.30 |
| Open | 2580.89 |

## 5. Conclusions

In conclusion, the proposed e-auction system based on asymmetric encryption and the digital signature scheme satisfies the necessary security properties for an auction.

Anonymity, confidentiality, privacy, correctness, integrity, and fairness are all fulfilled, and it is simple to implement. However, the proposed system still needs some improvement in the future, especially regarding system features, security, performance, and scalability. Other suitable cryptographic building blocks can be used together to produce a more secure and efficient cryptographic scheme to withstand the potential vulnerabilities and the advanced development of technology and techniques. Future work is needed to ensure the stability and durability of the proposed system in real-time environments.

**Acknowledgements**

This work was supported by the Telekom Malaysia Research & Development Grant (RDTC/221045) and the Ministry of Higher Education of Malaysia's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01).

**References**

Berawi, M.A., Sari, M., Addiani, F.A.F., Madyaningrum, N., 2021. Developing a Blockchain-Based Data Storage System Model to Improve Government Agencies' Organizational Performance. *International Journal of Technology,* Volume 12(5), pp. 1038

Blass, E.O., Kerschbaum, F., 2020. BOREALIS: Building Block for Sealed Bid Auctions on Blockchains. *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, pp. 558–571

Chen, Y.H., Chen, S.H., Lin, I.C., 2018. Blockchain Based Smart Contract for Bidding System. *2018 IEEE International Conference on Applied System Invention (ICASI)*, pp. 208–211

Gao, W., Yu, W., Liang, F., Hatcher, W. G., Lu, C., 2020. Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption. *IEEE Transactions on Network Science and Engineering*, Volume 7(2), pp. 776–791

Guo, Z., Fu, Y., Cao, C., 2017. Secure First-Price Sealed-Bid Auction Scheme. *EURASIP Journal on Information Security*, Volume 2017(1), pp. 1–6

Khan, A.S., Rahulamathavan, Y., Basutli, B., Zheng, G., Assadhan, B., Lambotharan, S., 2019. Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications. *IEEE Access,* Volume 7, pp. 95555–95568

Lee, C.C., Ho, P.F., Hwang, M.S., 2009. A Secure E-Auction Scheme based on Group Signatures. *Information Systems Frontiers*, Volume 11(3), pp. 335–343

Peng, K., Boyd, C., Dawson, E., Viswanathan, K., 2002. Robust, Privacy Protecting and Publicly Verifiable Sealed-Bid Auction. In *International Conference on Information and Communications Security,* Volume 2531, pp. 147–159

Rabah, K., 2006. Implementing Secure RSA Cryptosystems using Your Own Cryptographic JCE Provider. *Journal of Applied Sciences*, Volume 6(3), pp. 482–510

Tashenova, L., Babkin, A., Mamrayeva, D., Babkin, I., 2020. Method for Evaluating the Digital Potential of a Backbone Innovative Active Industrial Cluster. *International Journal of Technology,* Volume 11(8), p. 1499

Thiyagarajan, D., Ganesan, R., 2015. Data Security Model Employing Hyperelliptic Curve Cryptography (HECC) and Secure Hash Algorithm-3 (Sha-3) in Cloud Computing. *International Journal of Technology,* Volume 3, pp. 327–335

Wikipedia, 2021. PKCS 1. Available online at https://en.wikipedia.org/wiki/PKCS1#Version_history, Accessed on November 20, 2021

Wu, C.C., Chang, C.C., Lin, I.C., 2008. New Sealed-Bid Electronic Auction with Fairness, Security, and Efficiency. *Journal of Computer Science and Technology*, Volume 23(2), pp. 253–264