Design and Implementation of a Secure Online Lottery System

Pramote Kuacharoen

Department of Computer Science, Graduate School of Applied Statistics
National Institute of Development Administration
118 Serithai Rd. Bangkapi, Bangkok 10240 Thailand
pramote@as.nida.ac.th

Abstract. Government has the authority to operate lottery schemes. Since the operation of the lottery system is controlled by the government, there are issues with public trust. The people may speculate that the lottery is rigged. This issue becomes critical with an online lottery system since the unprotected data can be easy manipulated. If all combinations which have been sold are known before the drawing, the government may draw winning numbers which pay the least. Moreover, winning tickets may be added after the drawing. As a result, corruption may be inevitable. The government should operate lottery schemes with integrity which include transparency and accountability.

This paper presents the design and the implementation of a secure online lottery system. The proposed system can provide accuracy, privacy, transparency, and verifiability. Using the proposed system, the government can operate lottery schemes with integrity.

Keywords: Online lottery system, secure online lottery system, information security

1 Introduction

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. The requirements of information security have undergone changes in the last several decades. When data was not accessible remotely, the security of information that was valuable was provided primarily by physical and administrative means. However, with the use of networks and communications facilities for carrying data between computers, different measures are needed to protect data. The importance of information security to the economic and national security interests has been recognized. The Federal Information Security Management Act (FISMA) defines three levels of potential impact; namely, low, moderate, and high, on organizations and individuals should there be a breach of security [2]. For a system that has a high level of the potential impact, a breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Therefore, such a system demands a high level of security requirements. Examples of

high level potential impact systems are electronic voting systems, classified document systems, and lottery systems. In this research, a system with a high level of the potential impact will be designed and implemented. The secure system will be applied to an online lottery system which has a significant implication in a high level of security requirements.

Government has the authority to operate lottery schemes. Since the government has total control of the operation of the lottery system, the integrity of such system becomes questionable. Public trust cannot be achieved. The people may speculate that the lottery is rigged. This issue becomes critical with an online lottery system since the unprotected data can be easy manipulated. If all of the sold combinations are known before the drawing, the government may rig the lottery so that the winning numbers are the least played combinations. Moreover, winning tickets may be added after the drawing. As a result, corruption may be inevitable.

According to the United Nations, good governance consists of eight major characteristics, namely, participatory, consensus oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive, and following the rule of law [3]. The government should practice good governance through the operation of the lottery system. The operation of the government should be transparent, open to scrutiny, and can be monitored by the people. This will reduce corruption in the government.

Furthermore, the operation of the lottery should adhere to the core values of the World Lottery Association which are responsibility, integrity, professionalism, and innovation [4]. The integrity value includes transparency and accountability. These are also important elements in good governance.

Besides promoting good governance, a secure online lottery system demonstrates the use of modern cryptography to provide security services which ensures adequate security of the systems. The security services can be divided into five categories, namely; authentication, access control, data confidentiality, data integrity, and non-repudiation. Various services will be used in designing and implementing the system.

When changing from a paper-based lottery system to an online lottery system, different types of threats emerge. Threats from cybercrime become prevalent. An assault on system security may be in the form of an active attack or a passive attack [5]. An active attack attempts to alter resources or affect the operation whereas a passive attack tries to obtain information. Without proper preventions, a reliable service cannot be offered.

2 Background and Related Work

This section provides background information related to this paper such as lottery, electronic lottery schemes, information security, and blind signature scheme.

2.1 Lottery

A lottery is a form of gambling in which many people purchase chances to win a prize [6]. Some governments regulate or organize lottery, while others outlaw it. The

first recorded signs of a lottery are dated back as early as between 205 and 187 B.C. during the Chinese Han Dynasty in what is now China. It is believed that the game called Keno, a lottery-like game, had helped finance major government projects like the Great Wall of China. References to lotteries have been found in many ancient texts from various civilizations such as Ancient China, Celtic, Ancient Greece, and the Roman Empire. The first European lotteries in the modern sense of the word appeared in 15th-century Burgundy and Flanders with towns attempting to raise money to fortify defenses or aid the poor.

The basic elements of modern lottery operations are recording the numbers and the amounts staked, drawing and determining the winning numbers, and collecting and pooling all the money placed as stakes. In a large-scale lottery, a computer system is used for recording purchases and printing tickets.

The types of lotteries which are popular in many countries are conventional lottery, lotto, instant lottery, the number game, and Toto. The following section is the summary of each type of lottery.

1. Conventional lottery or the classic lottery: A limited numbers of lottery tickets are preprinted. Bettors must choose from available tickets.
2. Lotto: Bettors can choose a set of numbers. For example, a 6/49 lotto allows the bettor any six numbers out of 49 numbers.
3. Instant lottery: Tickets are preprinted and the prizes are predetermined. After the bettor buys the ticket, the bettor can reveal whether or not it is a winning ticket. Scratch-off tickets are popular instant lottery tickets.
4. The number game: Bettors can choose a number. For example, in a four digit lottery, the bettor can pick a number from 0000 to 9999. Winning tickets can match all digits in order or a different order, match the front pair or the back pair, and the like.
5. Toto: It is the lottery which is used to bet on sports. The tickets contain several matches. The bettor can choose the outcome of each match.

The lotto is the leading form of lottery in the world, with an annual total turnover in excess of $150 billion.

In an online lottery system, tickets can be purchased using a lottery terminal. The tickets are recorded on the server and are printed out for the bettors. When the lottery is offered online, security is an important issue. The system must provide sufficient security services.

2.2 Electronic Lottery Schemes

Existing electronic lottery schemes proposed criteria that includes providing anonymity of bettors, randomized generation of the winning number, abilities to verify the winning number, and forge proof [7], [8]. In [7], the lottery number is revealed to the lottery authority.

Goldschlag and Stubblebine proposed a publicly verifiable lottery scheme based on a delaying function [9]. Each lottery ticket has an equal chance of being selected as a winning ticket. Since all information will be published, anyone can calculate the winning number based on the parameters of purchased tickets, and the winning num-

ber calculation is repeatable. Since the calculation uses a delaying function, nobody can get the result before the lottery closes. The winning ticket is selected among all purchased tickets. Therefore, each round must have a winner which is not suitable for a lottery scheme that allows rollover.

Sako presents an implementation of a digital lottery server as a Web application which offers an outcome that players can agree to be random [10]. The server allows users to define and start lottery sessions, participate in the session, and verify the outcome. The dealer initiates a lottery session on the lottery server. Each player chooses the session to participate in and submits a random string to the server. The server uses the submitted random strings among other parameters to calculate the result by using a cryptographic hash function. The outcome is published on the web, together with the players' random strings and other parameters. Each player can verify that the submitted random string was indeed included. However, this scheme places trust on the server. Should the server be compromised, the result could be altered.

2.3 Information Security

X.800 [11] defines security services to ensure adequate security of the systems or of data transfers. These services are categorized into authentication, access control, data confidentiality, data integrity, and non-repudiation. These services can be applied to the data in storage as well. A brief description of each category is described below.

1. Authentication: The authentication service is concerned with assuring that a communication is authentic. It is the process of reliably verifying the identity of someone.
2. Access control: This service has the ability to limit or control the access to systems and applications via communication links. Unauthorized access is denied.
3. Data confidentiality: The confidentiality service protects transmitted data from passive attacks. This service also provides protection of data saved in storage.
4. Data integrity: This service ensures that data received are the same as sent by an authorized entity.
5. Non-repudiation: The non-repudiation service prevents either sender or receiver from denying a transmitted or produce message.

Cryptography is one of the most important aspects of communications security. Two forms of cryptography are symmetric and asymmetric [12], [13], [14]. In symmetric cryptography, a single key is used in encryption and decryption. The most well-known symmetric cryptography algorithm is the Data Encryption Standard (DES) [15]. However, its strength is now questionable [16]. DES will be replaced by a more secure symmetric cryptography algorithm, the Advanced Encryption Standard (AES) [17]. On the other hand, in asymmetric cryptography, two keys, namely, public key and private key are used. These two keys are mathematically related. Data encrypted using one key can be decrypted using the other key.

The security uses of symmetric cryptography are transmitting data over an insecure channel, secure storage on insecure media, authentication, and integrity check. The

security uses of asymmetric cryptography include the aforementioned operations and digital signatures. Most widely used asymmetric algorithm is RSA [18].

2.4 Blind Signature Scheme

Blind signature [19] schemes can be used in applications where author privacy is important. The signing authority can certify certain information without revealing the information being signed.

A RSA signature is computed by raising the message *m* to the secret exponent *d* modulo the public modulus *n*. However, the blind version uses a random number *k*, such that *k* is relatively prime to *n*. *k* is raised to the public exponent *e* modulo *n*. The resulting value $k^e \ (mod\ n)$ is used as a blinding factor. The product of the message *m* and the blinding factor, $m' \equiv mk^e \ (mod\ n)$, can be sent to the signing authority. The blinded message m' does not leak any information about *m*. The signing authority computes the blinded signature as $s' \equiv (m')^d \ (mod\ n)$ and sends it back to the author of the message. The author of the message can remove the blinding factor to reveal the valid RSA signature of m as $s \equiv s' \cdot k^{-1} (mod\ n)$. The following equation proves that valid RSA signature of *m* can be obtained.

$$s \equiv s' \cdot k^{-1} (mod\ n) \equiv (m')^d k^{-1} \equiv m^d k^{ed} k^{-1} \equiv m^d k k^{-1} \equiv m^d (mod\ n)$$

This scheme can be used in the online lottery since the lottery information is needed to be certified and cannot be known to the signing authority.

3 System Design

This section presents the design of a secure online lottery system. First, the design objectives are defined. Then, the system design is presented. The system design consists of three parts, specifically, the design of lottery purchase process, the closing time process, and the verifying winning number process. Finally, the evaluation of the system is discussed.

3.1 Design Objectives

The following properties are the design goals of a secure online lottery system.

1. Accuracy: A system is accurate if it is not possible for the sold lottery numbers to be modified.
2. Privacy: A system is private if neither authorities nor anyone else can reveal the identity of the buyer without the buyer's consent.
3. Transparency: A system is transparent if it does not permit the authorities or anyone to obtain information from the system on the lottery numbers sold before the drawing and to add new numbers after the drawing.
4. Verifiability: A system is verifiable if the buyer can claim the winning number even the data in the system is completely destroyed.

3.2 Lottery Purchase Process

The secure online lottery system consists of three modules, namely; auditor, lottery terminal, and lottery authority. The auditor is the signing authority who ensures that the lottery system is conducted according to the policy. The responsibility of the auditor is to sign the purchased lottery information without having the knowledge of the information, to decrypt the session keys, and to release the session keys to the lottery authority when the lottery drawing has ended. The lottery terminal allows the player to buy a lottery ticket. The responsibility of the lottery terminal is to have the purchased lottery certified by the auditor and to submit the certified lottery to the lottery authority. Finally, the lottery authority is responsible for verifying the winning ticket.

Fig. 1 shows the overview of the secure online lottery purchase protocol. The process is initiated when the buyer purchases a lottery. The lottery terminal acts as the buyer agent. The lottery information is hashed to obtain the message digest *m*. The obtained message digest is multiplied by the blinding factor as k^{ae} *(mod an)*. The blinded message digest and the signature are encrypted using the auditor's public key and sent to the auditor to be certified. The auditor cannot learn the lottery number being purchased. When the auditor receives the message from the lottery terminal, the auditor decrypts the message using the auditor's public key and verifies the signature of the lottery terminal. Upon successful verification, the auditor signs the blinded message digest. The signed blinded message digest is encrypted using the lottery terminal's public key and then is sent to the lottery terminal.

When the lottery terminal receives the message from the auditor, the lottery terminal decrypts the message using the lottery terminal's public key. The real signature of the auditor can be computed from the blinded signature. The lottery terminal also verifies that the signature is valid. After verifying the signature, the lottery terminal randomly selects a session key *ks* for the current lottery ticket. The lottery terminal encrypts the lottery information and the certified signature of the auditor using the session key. The session key is then encrypted using the lottery authority's public key. The encrypted certified lottery information, the encrypted session key and the transaction signature are encrypted using the lottery authority's public key and are sent to the lottery authority.

The lottery authority decrypts the received information using the private key and verifies the signature. Subsequently, the lottery authority issues a sequence number of the lottery ticket. A receipt for the lottery ticket is generated by signing the sequence number and the encrypted lottery information. The sequence number and receipt are then sent to the lottery terminal. The lottery authority does not know the lottery number since the session key is not available. It is encrypted using the auditor's public key.

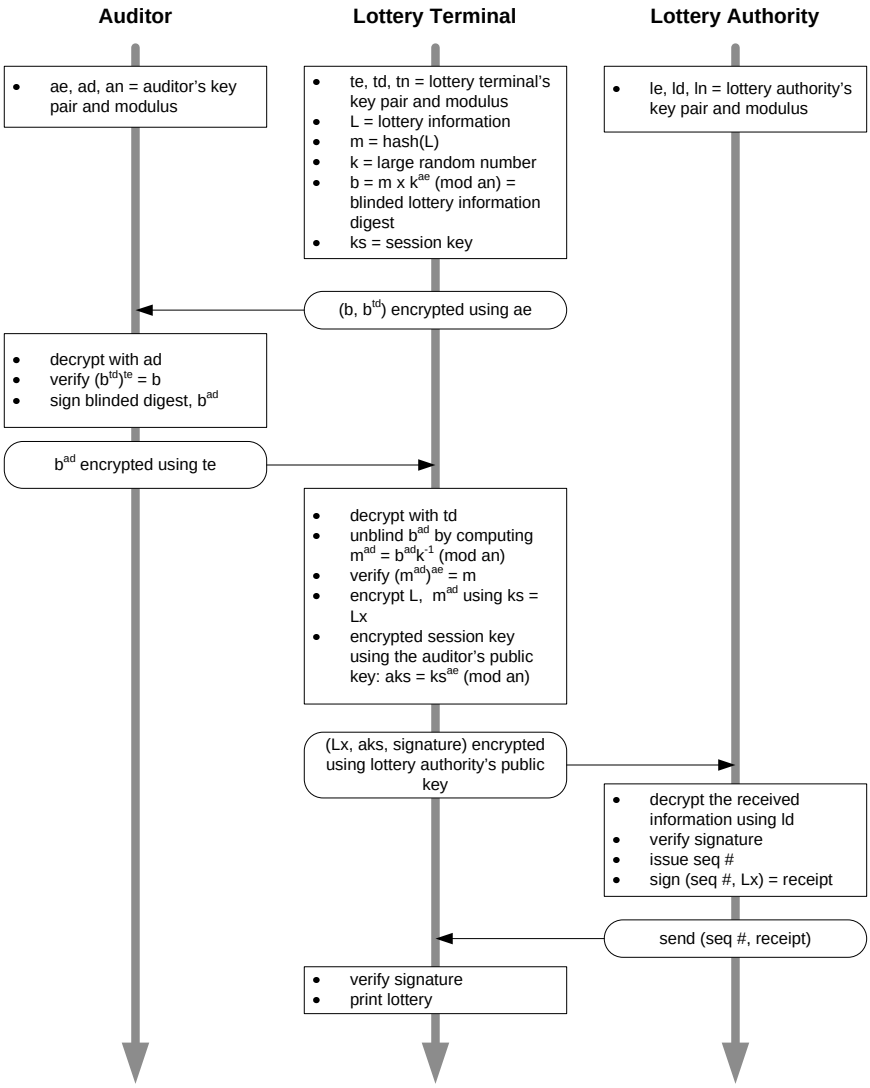

Fig. 1. Secure online lottery purchase protocol overview

When the lottery terminal receives the receipt from the lottery authority, the lottery terminal verifies the signature. After verifying the signature, the lottery terminal prints the lottery ticket. The bettor successfully purchases the lottery ticket. Note that the payment transaction description is omitted.

3.3 Closing Time Process

The auditor has certified all purchased lottery tickets and maintains a list of the corresponding sequence numbers and the encrypted session keys. However, the auditor does not have any knowledge of the purchased lottery numbers. On the other hand, the lottery authority has encrypted purchased lottery numbers and encrypted session keys, but the lottery authority cannot obtain any information on the purchased lottery numbers. This provides a balance of power between two authorities.

When the closing time has passed, the lottery authority publishes all sequence numbers along with the corresponding receipts and signs the published information. The lottery authority also sends the list of sequence numbers, encrypted session keys, and the receipts to the auditor. The auditor stops blind signing. The signature is verified.

After the all winning numbers have been drawn, the auditor sends a list of the sequence numbers and the session keys to the lottery authority. The lottery authority verifies the signature. For each lottery ticket, the lottery information together with the certified signature can be obtained using the corresponding session key. Then, the lottery authority verifies the signature. The closing time process is depicted in Fig. 2.

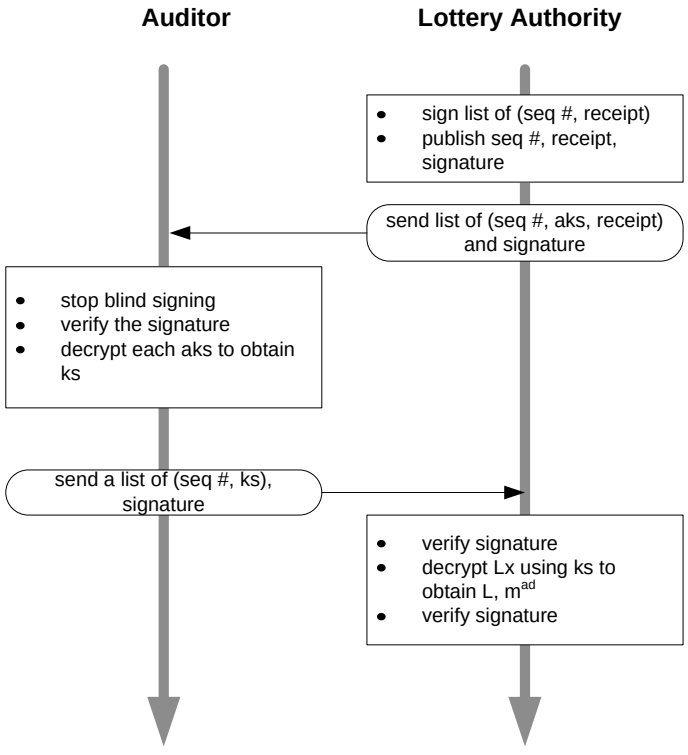

Fig. 2. Closing time process

3.4 Verifying Winning Number Process

The bettor can check if the purchased lottery ticket is the winner by presenting the lottery ticket to the lottery terminal or the lottery authority. The lottery ticket is scanned to obtain information such as the sequence number, the lottery information, the certified signature, the receipt information, and the session key. The certified signature is verified by comparing the hash value of the lottery information with the value obtained from decrypting the signature using the auditor's public key. This ensures that the lottery ticket was certified properly. To verify the receipt information, the lottery information is encrypted using the session key *ks*. The hash of the sequence number and the encrypted lottery information is compared with the one obtained from decrypting the receipt using the lottery authority's public key. The last step is to compare the purchased lottery number against the winning numbers and display the result to the player. The process for verifying the winning number is illustrated in Fig. 3.

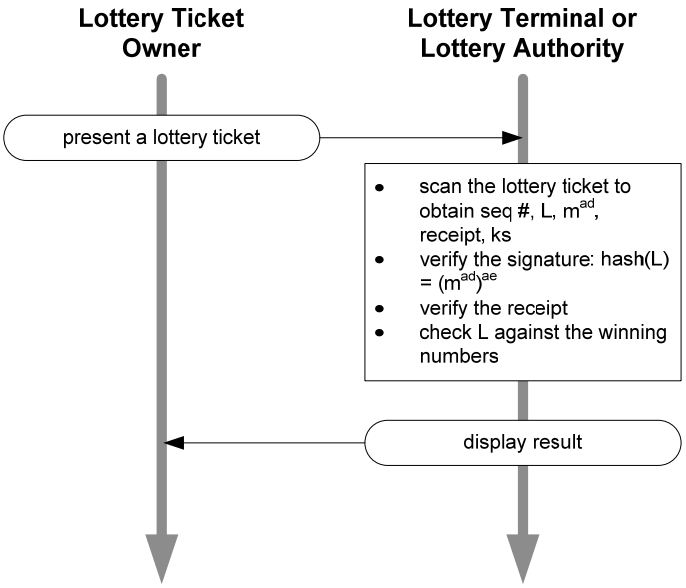

Fig. 3. Verifying the winning number process

3.5 Evaluation

Four properties of the secure online lottery were given earlier. In this section, the secure online lottery system is evaluated accordingly. While evaluating the secure online lottery system, there are assumptions about other aspects of security that have been put into place. For example, the application security has been audited and the lottery terminal does not keep records on the sold lottery tickets.

Accuracy: The secure online lottery system satisfies the accuracy property. The sold lottery numbers cannot be modified. If they are modified, the signature verification will fail. If the auditor modifies the numbers and regenerates the signature, the receipt (the signature of the lottery authority) verification will not pass. Similarly, if the lottery authority modifies the lottery numbers and regenerates the receipt, the auditor's signature verification will fail. If both auditor and lottery authority collude, the modified receipt would not match any of the receipts published before the drawing.

Privacy: The secure online lottery system satisfies the privacy property well. There is no personally identifiable information collected. The owner of the ticket must possess the physical ticket to claim the winnings. At that time, the identity of the bettor is revealed.

Transparency: The secure online lottery system satisfies the transparency property to a certain extent. The auditor does not have knowledge about the sold lottery information. The lottery authority only has the encrypted lottery information. Therefore, neither authority can obtain information from the system on the lottery sold before the drawing. However, if both the auditor and the lottery authority collude, all lottery information can be revealed. The system can be designed to prevent this event by only storing the session key on the lottery ticket. However, it would be inconvenient to the lottery authority since the lottery authority will not have any information until the ticket owner comes forward to present the ticket. Even with collusion, no new numbers can be added after the drawing without being detected since the lottery authority must publish all sequence numbers and receipts before the drawing.

Verifiability: The secure online lottery system satisfies the verifiability property. The purpose of this property is to protect the player from being denied from claiming the winning ticket. The lottery ticket contains both the auditor's and lottery authority's signatures. This provides non-repudiation from both authorities. However, if the data in the system is completely destroyed, there must be an investigation into the incident to ensure that no collusion occurred.

4 Prototype of the System

A prototype of the secure online lottery system is implemented using Java programming language.

4.1 Architecture of the System

The system consists of three modules, namely; the auditor module, the lottery terminal module, and the lottery authority module as illustrated in Fig. 4. The auditor module and the lottery authority module are web services while the lottery terminal module is an application. The interactions between modules and web services are done using SOAP messages.

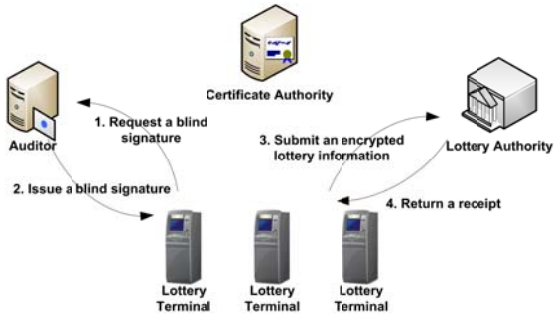

Fig. 4. The architecture of the secure online lottery system

4.2 Cryptographic Library

Java Cryptography Architecture (JCA) for Java Platform Standard Edition 6 is used to implement the secure online lottery system. For symmetric cryptographic operations such as encryption and decryption, AES is used. The key length is 256 bits. However, RSA is used for asymmetric cryptographic operations that enable the encryption and decryption of data, and signing and verifying signatures. The key length is 2048 bits.

4.3 Printing Lottery Ticket

Human readable information such as the lottery numbers, the date, and the lottery period are printed on the lottery ticket. This is for the player to read only. The lottery ticket information which include the lottery number, data, lottery period, sequence number, certified signature, receipt, and the session key are stored in a two-dimensional barcode [20], specifically the QR Code [21]. This provides a convenient way to transfer data from the lottery ticket to the lottery verification program by scanning the QR Code. Since the QR Code includes error correction, correct reading can be achieved even though a portion of the barcode is damaged.

5 Conclusion

The online lottery system can be implemented in a secure manner through four desirable properties which include accuracy, privacy, transparency, and verifiability. The system is accurate since it is not possible for the sold lottery numbers to be modified. The privacy of the player is protected since no personally identifiable information is included in the lottery information. The system is transparent since it does not allow anyone to obtain the information of sold lottery numbers or to add new lottery tickets after the drawing. Finally, the system is verifiable since the buyer can claim the winning number even the data in the system is completely destroyed. Therefore, through this system, the lottery operation of the government can be transparent.

References

1. Title 44 of the United States Code § 3542 (b) (1), United States Government Printing Office (2008)
2. U.S. Department of Commerce/National Institute of Standards and Technology (NIST), Standards for Security Categorization of Federal Information and Information Systems (FIPS PUB 199) (2004)
3. "What is good governance?" UNESCAP, 2009. http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp (2009)
4. World Lottery Association, "The World Lottery Association Values", http://www.world-lotteries.org/
5. The Internet Engineering Task Force (IETF), Internet Security Glossary (RFC 2828) (2000)
6. "lottery," in Encyclopædia Britannica 2009, Encyclopædia Britannica Online, http://www.britannica.com/EBchecked/topic/348555/lottery
7. Zhou, J. and Tan, C.: Playing Lottery on the Internet. In: Information and Communications Security, LNCS, vol. 2229, pp. 189-201. Springer, Heidelberg (2001).
8. Liu, Y. et al.: A New Efficient E-Lottery Scheme Using Multi-Level Hash Chain. In: International Conference on Communication Technology, pp. 1-4. (2006)
9. Goldschlag, D. M. and Stubblebine, S. G.: Publicly verifiable lotteries: Applications of delaying functions. In: Proceedings of 1998 Financial Cryptography. LNCS, vol. 1465, pp. 214-226. Springer, Heidelberg (1998)
10. Sako, L.: Implementation of a digital lottery server on WWW. In: Proceedings of CQRE'99, LNCS, vol. 1740, pp. 101-108. Springer, Heidelberg (1999)
11. The International Telecommunication Union (ITU), Data Communication Network: Open Systems Interconnection (OSI); Security, Structure and Applications (1991)
12. Kaufman C., Perlman R., and Speciner M.: Network Security: Private Communication in a Public World, 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR (2002)
13. Stallings, W.: Cryptography and Network Security, 4th ed. Upper Saddle River, NJ: Prentice Hall (2006)
14. Katz, J. and Lindell, Y.: Introduction to Modern Cryptography: Principles and Protocols, New York: Chapman & Hall/CRC (2007)
15. U.S. Department of Commerce/National Institute of Standards and Technology (NIST), Data Encryption Standard (DES) (FIPS PUB 46-3) (1999)
16. Hevia, A. and Kiwi, M.: Strength of Two Data Encryption Standard Implementations under Timing Attacks. In: ACM Transactions on Information and System Security, vol. 2, no. 4, pp. 416–437. (1999)
17. U.S. Department of Commerce/ National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES) (FIPS PUB 197) (2001)
18. RSA Cryptography Standard, PKCS #1 v2.1. (2002)
19. Chaum, D.: Blind Signatures for Untraceable Payments. In: Advances in Cryptology: Proceedings of Crypto, pp. 199-203. (1982)
20. Gao, J.Z., Prakash, L., Jagatesan, R.: Understanding 2D-Barcode Technology and Applications in M Commerce–Design and Implementation of a 2D Barcode Processing Solution. In: 31st Annual International Conference on Computer Software and Applications, vol. 2pp.49-56. (2007)
21. QR Code, http://www.denso-wave.com/qrcode/