2015 10th Asia Joint Conference on Information Security

Secure Electronic Coupons

Chin-Chen Chang
Department of Information Engineering
and Computer Science
Feng Chia University
Taichung, Taiwan
Email: alan3c@gmail.com

Iuon-Chang Lin
Department of Management
Information Systems
National Chung Hsing University
Department of Photonics
and Communication Engineering
Asia University
Email: iclin@nchu.edu.tw

Yi-Lun Chi
Department of Computer Science
and Information Engineering
Asia University
Department of Marketing
and Supply Chain Management
Overseas Chinese University
Email:erin.chi@gmail.com

***Abstract*—Coupons are well-known and widely used in the market place to attract new customers looking for deals and to keep loyal customers. Generally speaking, coupons for loyal customers have more discount than coupons for new customers. In order to differentiate between new and loyal customers, we invented two schemes that allow firms to issue different types of e-coupons through a wireless network. The first scheme is used to generate e-coupons that are not assigned to specific customers. Thus, an unused e-coupon can be used by any customer. This scheme is more suitable for attracting new customers. The other scheme is used to generate e-coupons that are assigned to specific customers. Thus, unused e-coupons cannot be used by other customers. This second scheme is more suitable for keeping loyal customers. Both of the proposed schemes are designed for mobile electronic commerce and reduces the cost for processing coupons.**

I. Introduction

With the rapid growth of computer network technologies, many traditional transactions are conducted electronically. More and more applications such as electronic auction [11], electronic voting [3], electronic payments [10], [19], and others are developed to run over the Internet. In addition to the Internet, mobile communications revolutions are changing rapidly, and commercial interests abound. Mobile communications, such as *Personal Communication Services* (PCS) and *Universal Mobile Communication System* (UMCS), have been developed and have become very popular around the world. The technologies are designed for providing communications and computations with mobility. So far, there are many mobile networks that have been developed, such as GSM, USDC, PDC, and others [18]. The GSM system has now been implemented in more than 70 countries around the world. Furthermore, many applications and services are provided such as wireless application protocol (WAP) [7], secure teleconferencing [12], mobile payment system [9], location-awareness applications [14], and others. Mobile commerce is being used more widely in business and is becoming a very significant research topic.

In the traditional market place, issuing coupons is a useful and well-known strategy to increase sales. According to the profit line, firms can issue discount coupons to reach new customers. In addition, firms also can issue special coupons with heavy discounts to keep loyal customers. The results of issuing electronic coupons on the Internet are very obvious [2], [6]. Furthermore, if we can apply the concept of e-coupons to mobile environment, we can anticipate that this will attract more customers to purchase a product. Therefore, the idea of using e-coupons for mobile electronic commerce is raised. The main purpose of using electronic coupons is to make receiving and using coupons mobile for customers. The technology allows a customer to receive an e-coupon through his/her mobile phone. The customer can then forward the e-coupon to the merchant when he/she wants to buy the product.

However, in an electronic environment, information can be intercepted and tampered with easily. Hence, how to build a secure channel for transactions using e-coupons is a key issue in such technology. Therefore, some security requirements are essential to this technology. We summarize the security requirements for using e-coupons as follows:

1) *Authentication:* In order to prevent a customer from forging e-coupons, the origin of the e-coupons must be ascertained. Thus, a merchant must have the ability to authenticate the validity of all e-coupons received.
2) *Integrity:* In order to prevent a customer from modifying e-coupons, the integrity of e-coupons must be kept. Thus, a merchant has to ensure that a e-coupon that has been received has not been modified.
3) *Preventing repeated use:* In order to avoid unlimited use of e-coupons, the number of e-coupons issued should be limited. Therefore, the system must prevent a customer form using the same e-coupon twice.

In addition to the security requirements, the performance of e-coupons is also very important. Due to the small memory space and the low computational capability of mobile electronic equipments, the processing cost of e-coupons, including computational cost, memory space overhead, and communication cost, must be reduced to as low as possible. Therefore, a practical e-coupon system for mobile electronic commerce must be securely performed and efficiently managed with a low processing cost.

In order to satisfy these requirements, some efficient cryptographic techniques such as hash functions can help us to design such an e-coupon scheme. Furthermore, the strategies for issuing e-coupons for new customers or loyal customers may be different. For example, in order to increase sales and attract new customers, firms may wish that a customer can forward an unused e-coupon to another potential customer

978-1-4799-1989-5/15 $31.00 © 2015 IEEE
DOI 10.1109/AsiaJCIS.2015.10

if the customer does not want to use it. On the other hand, in order to keep loyal customers, firms may issue special e-coupons to loyal customers. The special e-coupons usually have mush more price discounts or offer a product for free. Thus, firms may not wish that the special e-coupons be used by another customer.

According to the two different strategies for issuing coupons, we invented two types of practical e-coupon schemes that satisfy all the requirements. In the first proposed scheme, e-coupons that are issued are not assigned to specific customers. Thus, it can be used by any customer. In the second proposed scheme, e-coupons that are issued are assigned to specific customers. Thus, it cannot be used by other customers. From our knowledge so far, we have not yet found any related schemes for discussing the distinction between e-coupons that are not associated with specific customers, and e-coupons that are associated with specific loyal customers.

The rest of this paper is organized as follows. In Section 2, the technology of message authentication code will be introduced. The technology will be used later in our proposed schemes. The system framework and the notations used throughout the rest of the paper are introduced in Section 3. In Section 4, we present the first proposed scheme for issuing e-coupons which are not assigned to specific customers. In Section 5, we present the second proposed scheme for issuing e-coupons which are assigned to specific customers. In Section 6, the properties and the performance of our schemes are examined. Section 7 concludes this paper.

II. Message Authentication Code

Message Authentication Code (MAC) is a useful cryptographic technology that will be helpful to our proposed schemes. Before introducing the MAC, we first introduce the technology of the one-way hash function. The one-way hash function is usually applied to authenticate the integrity of a message. For instance, MD5 is a well-known one-way hash function. Its input text is a 512-bit block. After processing with MD5, the output is a set of four 32-bit blocks. MD5 can take an input of an arbitrary-length and return an output of a fixed-length. In addition, it can create a one-way and collision-resistant result [4], [15], [16].

The features of the one-way hash function are summarized as follows [17]:

1) Given an input of an arbitrary-length, it always gives an output of a fixed-length.
2) Given an input, it is easy to derive the output through the function.
3) From an output, it is difficult to derive the input.
4) Given an input, it is difficult to find another input such that the two inputs have the same output.

The advantages of the one-way hash function are high speed and easy implementation using software or hardware.

The message authentication code is a special one-way hash function. MAC is a key-dependent one-way hash function [5]. The inputs of this function are a message M and a key K, and the output is a message digest. It has the same features as the one-way hash function, but it is augmented with a key to prevent someone from forging the hash value. A user who owns the key can easily verify the hash value, but others cannot do it. The MAC is an efficient cryptographic technology that achieves integrity and authentication with lower operation costs. The ISO standard of the MAC algorithm is described in [1]. It is the simplest way to perform the MAC function. The DES or FEAL encryption function is used in this algorithm. After processing with the one-way hash function, the hash value is encrypted using such an encryption algorithm. Hence the cost of MAC computation is hash computation and symmetric key encryption. The technology is suitable for use in electronic coupon systems.

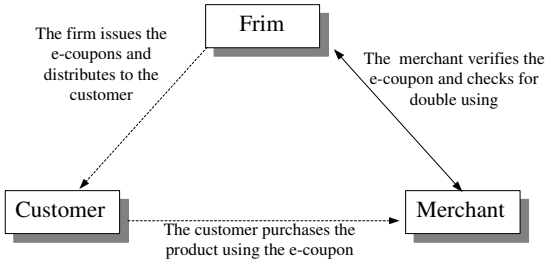

Fig. 1. The framework of e-coupons

III. System Framework and Notations

The proposed electronic coupon schemes consist of three entities: a firm, customers, and merchants. The firm is the entity that issues e-coupons and distributes the e-coupons to potential customers through a wireless network. Upon receiving an e-coupon, a customer can forward the e-coupon to a merchant through his/her mobile phone and purchase the product. A firm may have none, one, or many merchants. A merchant is an agency of the firm that sells the products. The merchant holds an electronic point-of-sale device which is issued by the firm. A tamper-resistant chip, such as a smart card or a SIM card, is embedded into the device and contains the firm's secret key and the verification function. The integrated circuit chip in the device protects the information stored in a secret area from duplication or leaking out [8], [13]. During the verification process, the device does not reveal any secret information. Furthermore, the firm establishes a database system which stores each e-coupon issued and checks whether the coupon has been used before. This mechanism can prevent unlimited use of the same e-coupons.. Upon receiving an e-coupon, the merchant first verifies the validity of the e-coupon using the point-of-sale device and then connects to the firm's database system to check whether the e-coupon has been used twice. The connection between the firm and the merchants could be a financial network. The framework of the proposed e-coupon systems is illustrated in Figure 1. The dotted lines represent the wireless network. The solid line represents the financial network.

Before proceeding to our schemes, we first introduce the following notations:

- *MAC(K,M):* The function for message authentication code. The inputs of this function are a message M and a key K. The output of this function is a fixed-length message digest.

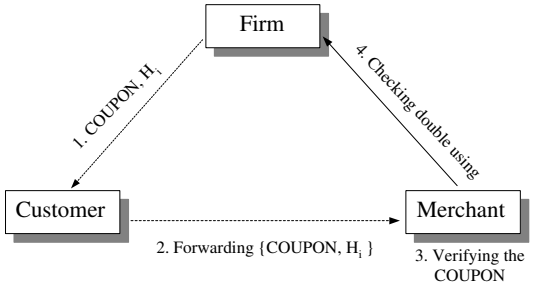

Fig. 2. The processes of scheme 1

- ID_C: Each customer's unique identity such as mobile phone number.
- K_F/K_C: The firm/customer's secret key, where $K_C = MAC(K_F, ID_C)$.
- *PRODUCT:* The information on discounted products, such as products' ID numbers.
- *SER:* An unique serial number for each e-coupon.
- *VDATE:* A valid date for an e-coupon.
- *COUPON:* The issued e-coupon which includes the messages $PRODUCT$, SER, and $VDATE$.

IV. Scheme 1: Electronic Coupons not Assigned to Specific Customers

In this section, we shall describe the first scheme that issues electronic coupons that are not assigned to specific customers such that the e-coupon can be used by other potential customers if the customer receiving the e-coupon does not use it. Our scheme makes use of the MAC as the basic operation. The process in our scheme consists of three phases: the e-coupon issuing and distributing phase, the purchase phase, and the verification phase. These phases are described as follows.

1) *The e-coupon issuing and distributing phase:* The firm first makes the decision on how many e-coupons will be issued for a product. Suppose that the number of e-coupons to be issued is n. Then the e-coupons can be generated by the firm using the following formula

$$H_i = MAC(K_F, PRODUCT \| SER_i \| VDATE), \quad (1)$$

where i is from 1 to n and the symbol $\|$ denotes the concatenation. After that, the firm distributes the e-coupons $\{PRODUCT, SER_i, VDATE\}$ with H_i to potential customer C_i through a wireless network.

2) *The purchase phase:* After receiving the e-coupon, the customer can forward the e-coupon $\{PRODUCT, SER_i, VDATE\}$ and H_i to the merchant if the customer wants to buy the product with the discounted price.

3) *The verification phase:* Upon successfully receiving the e-coupon, the merchant first checks the date of the e-coupon to see if it is valid. If the e-coupon is still valid, the merchant uses the point-of-sale device to verify whether the relation $H_i = MAC(K_F, PRODUCT \| SER_i \| VDATE)$ holds or not, where the firm's secret key K_F was stored in the device and obtains the information $PRODUCT$, SER_i, and $VDATE$ from the received message. If the relation holds, the $\{PRODUCT \| SER_i \| VDATE\}$ is accepted as a valid coupon. Then the merchant transfers the e-coupon to the firm to check to see if it has been used before. The firm finds the record of the e-coupon according to SER_i and checks the coupon to see if it has be used or not. If the check indicates the e-coupon is valid, the firm sends an acceptance message to the merchant and records the e-coupon as used. If the check indicates the e-coupon is invalid, it means the e-coupon has been used more than once. The merchant ignores this transaction and sends a rejection message to the customer.

In this scheme, the issued e-coupons are not assigned to specific customers for their individual use. Thus, if a customer does not use the e-coupon, the e-coupon can be forwarded to another potential customer. The firm only prevents the e-coupon from being used twice. If the firm does not care that the e-coupons are used without limit, the process for checking whether the e-coupon has been used can be ignored. Figure 2 shows the process of the proposed first scheme. The dotted lines represent the wireless network. The solid line represents the financial network.

V. Scheme 2: Electronic Coupons Assigned to Specific Customers

Different from scheme 1, the e-coupons issued using this scheme are assigned to specific customers. Thus, the e-coupons can not be haphazardly used by other potential customers if the customer receiving the e-coupon does not use it. Scheme 2 is described as follows.

1) *The registration phase:* Loyal customers are usually invited to become members of the firm. First, the customer sends his/her identity information ID_C, such as mobile phone number or something else, to the firm. Then the firm generates a secret key K_C for the authorized customer using the following formula

$$K_C = MAC(K'_F, ID_C), \quad (2)$$

where K'_F is the firm's other secret key that generates the customer's secret key. Finally, the firm returns the secret key K_C to the customer in a highly secure manner. This phase is performed only once.

2) *The e-coupon issuing and distributing phase:* The firm makes the decision of who will receive the e-coupon and how many e-coupons will be issued for a product. Suppose that the number of e-coupons to be issued is n and the receivers' identities are $ID_{C_1}, ID_{C_2}, \cdots, ID_{C_n}$. Then the e-coupons can be generated by the firm using the following formula

$$H_i = MAC(K_F, PRODUCT \| SER_i \| VDATE \| ID_{C_i} \| S_i), \quad (3)$$

where S_i equals

$$S_i = MAC(MAC(K'_F, ID_{C_i}), SER_i) = MAC(K_{C_i}, SER_i), \quad (4)$$

and i is from 1 to n. After that, the firm distributes the e-coupons $\{PRODUCT, SER_i, VDATE\}$ with H_i to the assigned customers through a wireless network.

3) *The purchase phase:* After receiving the e-coupon $\{PRODUCT, SER_i, VDATE\}$ and H_i, the customer first uses his/her secret key K_{C_i} to compute S_i such that $S_i = MAC(K_{C_i}, SER_i)$. Then, the customer forwards the e-coupon $\{PRODUCT, SER_i, VDATE\}$ with S_i, ID_{C_i}, and H_i to the merchant.

4) *The verification phase:* Upon receiving the e-coupon, the merchant first checks whether the date of the e-coupon is valid and then verifies whether the relation

$$H_i = MAC(K_F, PRODUCT \| SER_i \| VDATE \| ID_{C_i} \| S_i) \quad (5)$$

holds or not, where ID_{C_i} can be obtained from the mobile phone number that appears on the received message. If the verification shows the relation holds, the $\{PRODUCT, SER_i, VDATE\}$ is accepted as a valid coupon. Then the merchant transfers the e-coupon $\{PRODUCT, SER_i, VDATE\}$, ID_{C_i} and S_i to the firm to check if it has been used before. The step is similar to scheme 1. If the e-coupon is valid, the firm sends an acceptance message to the merchant and the merchant accepts the purchase by the customer using the e-coupon.

In this scheme, the e-coupons issued are assigned to specific customers for use. Thus, only when the specified customer uses his/her secret key to compute a valid S_i and sends the e-coupon using his/her mobile phone can the e-coupon be used.

VI. Discussions

Traditional coupons need to meet security requirements: (1) authentication, (2) integrity, and (3) single use. However, the design of electronic coupons are more complicated in that. In addition to the three basic functions of traditional coupons, they also need to satisfy requirements specific to the applications of electronic coupons. In this section, we analyze the functions and performance strength of the proposed scheme.

A. Analysis of Security Functions

1) Authentication: In the electronic environment, a customer is able to forge a e-coupon and sends the e-coupon to a merchant. This is dangerous and therefore we have to authenticate the validity of all coupons received. This requirement is called authentication. Our proposed scheme meets this requirement by allowing a merchant to ascertain the origin of the e-coupons. In the e-coupon issuing and distributing phase of our schemes, an e-coupon is generated according to Equations 1 and 3. A valid e-coupon can only be generated by the genuine firm with the secret key. Any other user in the system has no means of generating a valid e-coupon without the knowledge of the secret key of the genuine firm. It is impossible for a customer attempting to forge a e-coupon on behalf of a firm because the forger will find it hard to get a valid H_i. Thus, a merchant can verify an e-coupon's validity in this system.

Furthermore, in scheme 2, a merchant also has to verify whether the e-coupon received is from an assigned customer. In the verification phase of scheme 2, the S_i is generated from Equation 4 using the customer's secret key K_{C_i}. The secret key is stored in the SIM card which is embedded in the customer's mobile phone. The SIM card is tamper resistant and protects data which cannot be read. In addition, we can assume the firm issuing the customer's secret key is a trusted party. Since the secret key $K_{C_i} = MAC(K'_F, ID_{C_i})$ is generated with the firm's secret key K'_F, nobody can derive the valid secret key of the customer without the firm's secret key. Thus, the merchant can be certain that the e-coupon is sent by the assigned customer if the verification is correct in Equation 5.

Therefore, the proposed schemes protect against forgery. Any forged or false e-coupon can be successfully detected in our proposed schemes.

2) Integrity: Electronic document can be modified easily especially when it is on transit. Therefore, when a merchant receives an e-coupon and its associated H_i, we have to ensure that the received e-coupon has not been modified. This requirement is called integrity. For example, someone may replace a coupon's $PRODUCT$ information with another. Our proposed schemes also verify the integrity of the received e-coupons.

Suppose that a customer attempts to alter $PRODUCT$ to change the product information or alter $VDATE$ to extend the period of validity. The modification will not succeed because the customer cannot generate the valid H_i for the modified e-coupon. The modification cannot pass the verification phase of our proposed schemes.

In the scheme 2, the integrity also can be kept. If a customer attempts to alter SER to use an e-coupon more than once, the modification also cannot succeed. Although the customer can derive the S_i for the modified SER, he/her cannot also derive the valid H_i for the modified information. Thus, integrity is ensured in our schemes.

3) Single Use: In order to prevent the e-coupons from unlimited use, the single use requirement must be satisfied. In our schemes, a merchant can make sure that a received e-coupon is used only once by checking the firm's database. If a customer duplicates an e-coupon in order to use it twice, the firm can easily detect the problem by using its database system. Thus, anyone attempting to repeat the use of an e-coupon will be thwarted.

B. Performance Analysis

In this subsection, we discuss the performance of our schemes.

1) Computational Costs: MAC is the main operation for generating and verifying e-coupons in our proposed schemes. Hence the number of MAC operations can be used to determine the computational cost. According to the ISO standard of a MAC algorithm [1], the MAC algorithm uses DES

TABLE I. THE COMPARISONS OF THE COMPUTATIONAL SPEED

Operation	Number per second
Public key signature (1024 bits RSA)	2
Symmetric key encryption (DES)	2,000
One-way hash function (MD5/SHA)	20,000

TABLE II. THE SUMMARY OF THE COMPUTATIONAL COST FOR THE ENTITIES IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
Symmetric key encryption		
F	1	2
C	0	1
M	1	1
One-way hash function		
F	1	2
C	0	1
M	1	1

encryption function to encrypt the hash value that is computed using the MD5 hash function. Thus, the computational cost of MAC is one hash function computation and one DES encryption function computation. Table 1 shows the numbers of public key signature, symmetric key encryption, and one-way hash function that can be performed per second on a typical workstation [17]. According to the simulation results, we discover that the one-way hash function and the symmetric key encryption are much cheaper than the public key signature.

Table 2 shows the computational cost for each entity in our proposed schemes. In this table, F represents the firm, C represents the customer, and M represents the merchant. We can see that the proposed schemes indeed require very low computational cost. Furthermore, the computational capability of the customer's mobile phone is usually smaller than the computational capability of the merchant's device. Thus, a practical scheme has to reduce the load of the customer's mobile phone. Our proposed schemes satisfy this realistic situation.

2) Memory Space Overhead: The memory space overhead depends on the size of an e-coupon and its associated hash value. Since the MD5 is considered a hash function in the ISO standard of MAC algorithm and is also used in our proposed schemes, the input size for MD5 can be used for determining the length of each variable in an e-coupon. According to the standard for MD5, the input text is a 512-bit block and the output is a set of four 32-bit blocks. We can concatenate the results to form a single 128-bit hash value.

Therefore, we can determine that the length of the message $\{PRODUCT \| SER \| VDATE\}$ is 256 bits, the length of S is 128 bits, and length of ID_{C_i} is 128 bits. Of course, we can flexibly determine the length of these messages. In scheme 1, since the size of the variables in the input text of MAC totals less than 512 bits, we can pad them with a few zeros to fix the input size. After the processing of MD5, the associated hash value H is 128 bits. Table 3 shows the required memory space in the terminals of the customer, merchant, and firm, respectively. In this table, n represents the number of issued e-coupons, m represents the number of e-coupons received by a customer, and r represents the number of e-coupons that be used in a merchant. Since the firm has to check whether the same e-coupon has been used before, a database for all issued e-coupons has to be maintained by the firm. Thus, the required memory space of the database depends on the number of issued e-coupons.

TABLE III. THE SUMMARY OF THE MEMORY SPACE OVERHEAD FOR THE ENTITIES IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
F	256 bits $\times n$	256 bits $\times n$
C	384 bits $\times m$	384 bits $\times m$
M	384 bits $\times r$	640 bits $\times r$

TABLE IV. THE SUMMARY OF THE COMMUNICATION COST FOR THE CONNECTIONS IN THE PROPOSED SCHEMES

Schemes	Scheme 1	Scheme 2
F-C	384 bits	384 bits
C-M	384 bits	640 bits
M-F	256 bits	256 bits

3) Communication Cost: The size of transmitted messages is regarded as the communication cost. Similar to the memory space overhead, we can regard the total size of the variables in an e-coupon to be 256 bits and the associated hash value to be 128 bits. Table 4 shows the communication cost for each connection in our schemes. In this table, $F - C$ means that the firm sends a message to the customer, $C - M$ means that the customer sends a message to the merchant, and $M - F$ means that the merchant sends a message to the firm.

VII. CONCLUSIONS

In this paper, we presented two novel schemes for issuing electronic coupons: one scheme issues electronic coupons which are not assigned to specific customers; the other issues electronic coupons which are assigned to specific customers. In addition to meeting the three security requirements-(1) authentication, (2) integrity, and (3) single use, the proposed schemes also have the following desirable features.

1) Low computational cost.
2) Low memory space overhead.
3) Low communication cost.

Therefore, the proposed schemes are very efficient and practical. They can not only be used on the Internet, but they are also especially suitable for use on wireless networks. We hope the proposed schemes can speed up the development of mobile commerce.

REFERENCES

[1] ISO/IEC 9797, "Data cryptographic techniques-data integrity mechanism using a cryptographic check functionemploying a block cipher algorithm," Internal Organization for Standardization.

[2] R. Anand, M. Kumar, and A. Jhingran, "Distributing e-coupons on the Internet," *Proceedings of the 9th Conference on Internet Society (INET'99)*, San Jose, 1999.

[3] R. Cramer, R. Gennaro, and J. Borrell, "A secure and optimally efficient multi-authority election scheme," *Advances in Cryptology-EUROCRYPT'97*, Lecture Notes in Computer Science, vol. 1233, pp. 103–117, 1997.

[4] I. B. Damgard, "A design principle for hash functions," *Advances in Cryptology-CRYPTO'89*, Lecture Notes in Computer Science, vol. 0435, pp. 416–427, 1989.

[5] D. W. Davies, “A message authentication algorithm suitable for a mainframe computer,” *Advances in Cryptology-CRYPTO’84*, Lecture Notes in Computer Science, vol. 0196, pp. 393–400, 1984.

[6] R. Garg, P. Mittal, V. Agarwal, and N. Modani, “An architecture for secure generation and verification of electronic coupons,” *Proceedings of 2001 USENIX Annual Technical Conference*, pp. 51–63, Boston, USA, 2001.

[7] WAP forum, “Wireless applicaion protocol,” see *http://www.wapforum.org*.

[8] M. Hendry, *Smart card security and applications*, Artech House, 1997.

[9] K. F. Hwang, I. C. Lin, and C. C. Chang, “A credit card-based mobile payment system,” *Proceedings of 2002 International Conference on Information Security (InfoSecu02)*, pp. 82–88, Shanghai, China, July 2002.

[10] M. S. Hwang, I.C. Lin, and L. H. Li, “A simple micro-payment scheme,” *The Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, 2001.

[11] M. S. Hwang, E. J. L. Lu, and I. C. Lin, “Adding timestamps to the secure electronic auction protocol,” *Data and Knowledge Engineering*, vol. 40, no. 2, pp. 155–162, 2002.

[12] M. S. Hwang and W. P. Yang, “Conference key distribution schemes for secure digital mobile communications,” *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 2, pp. 416–420, Feb. 1995.

[13] H. W. E. Jones, A. C. Watson, and T. J. O’Neill, “Vehicle security using smartcards,” *Security Journal*, vol. 10, no. 2, pp. 79–87, 1998.

[14] H. Maass, “Location-aware mobile applications based on directory services,” *Mobile Networks and Applications*, vol. 3, no. 2, pp. 157–173, Aug. 1998.

[15] R. C. Merkle, “One way hash function and DES,” *Advances in Cryptology-CRYPTO’89*, Lecture Notes in Computer Science, vol. 0435, pp. 428–446, 1989.

[16] R. C. Merkle, “A fast software one-way hash function,” *Journal of Cryptology*, vol. 3, no. 1, pp. 43–58, 1990.

[17] B. Schneier, *Applied cryptography*, John Wiley and Sons, second edition edition, 1996.

[18] S. Suzuki and K. Nakada, “An authentication technique based on distributed security management for the global mobility network,” *IEEE Journal on Selected Areas in Communications*, vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[19] C. T. Wang, C. C. Chang, and C. H. Lin, “A new micro-payment system using general payword chain,” *Electronic Commerce Research*, vol. 2, no. 2, pp. 159–168, 2002.