Research Article

Dynamic Symmetric Key Mobile Commerce Scheme Based on Self-Verified Mechanism

Jiachen Yang,^{1,2} Longsheng Xu,¹ Qinggang Meng,² and Shudong He¹

¹ School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China

² Department of Computer Science, Loughborough University, Loughborough LE11 3TU, UK

Correspondence should be addressed to Jiachen Yang; yangjiachen@tju.edu.cn

Received 6 June 2014; Accepted 13 August 2014; Published 18 December 2014

Academic Editor: He Huang

Copyright © 2014 Jiachen Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In terms of the security and efficiency of mobile e-commerce, the authors summarized the advantages and disadvantages of several related schemes, especially the self-verified mobile payment scheme based on the elliptic curve cryptosystem (ECC) and then proposed a new type of dynamic symmetric key mobile commerce scheme based on self-verified mechanism. The authors analyzed the basic algorithm based on self-verified mechanisms and detailed the complete transaction process of the proposed scheme. The authors analyzed the payment scheme based on the security and high efficiency index. The analysis shows that the proposed scheme not only meets the high efficiency of mobile electronic payment premise, but also takes the security into account. The user confirmation mechanism at the end of the proposed scheme further strengthens the security of the proposed scheme. In brief, the proposed scheme is more efficient and practical than most of the existing schemes.

1. Introduction

With the rapid development of mobile communication technology, more and more electronic trading has been introduced to the wireless network environment [1, 2]. The wireless mobile network in the electronic trading model not only provides numerous merchants with a new way of promoting the sale of products and increases the profit, but also greatly enriches the network shopping environment of the consumers [2]. Mobile electronic commerce has achieved rapid development, since the mobile users and merchants traded anywhere and anytime [3]. However, compared with fixed networks, there are some factors that have restricted the development of mobile commerce, such as lower bandwidth, longer delay time, unstable connection, limited storage space, and restricted computing power [2]. In order to reduce the risk of these problems, the priority of all kinds of mobile payment schemes is the security and efficiency of the solution.

Recently, with the development of mobile commerce based on the characteristics of the mobile network, some researchers have successively put forward certificate-based public key cryptosystem scheme (CBCS) [4, 5], ID-based

cryptography scheme (IDBCS) [2, 6, 7], and self-verified digital signature scheme (SVDSS) [3, 8, 9]. CBCS is similar to the scheme based on the Secure Electronic Transaction protocol, in which user's authentication requires the certificate preserved in the certificate authority (CA). When the node certificate is updated or canceled, each node directory needs to be updated synchronously. The requirements of this sort of certificate management for calculation, storage, and communication of the system are relatively high. In order to avoid the certificate management burden, IDBCS used key escrow (KE) features [10] and key distribution center (KDC) unified manage public/private key pair of all trading entity, which can generate a symmetric key, and then improve the efficiency of system. However, once the KDC public/private key leaks, the system will lose the security barrier. In addition, with the increase of the number of users, the KDC needs to maintain a set of large user authentication tables, resulting in increasing the burden of the system [2]. SVDSS is more efficient and secure than CBCS and IDBCS. On the one hand, its authentication mechanism does not need to rely on complex certificate management, which reduces the amount of calculation and traffic and improves the execution

TABLE 1: Comparison of performance of RSA and ECC.

Break time/MIPS	RSA key length/bit	ECC key length/bit	RSA/ECC key length ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{12}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

efficiency; on the other hand, it does not set public/private key to KDC. Thus SVDSS has extensive application prospect in the field of mobile e-commerce.

The core work of SVDSS is generating the authentication key and digital signature which verifies the identity of transaction entity. At present, the mainstream generative mechanism of SVDSS is based on ECC. Compared with the public key cryptosystem (PKC), ECC uses smaller key length to meet the same level of security and has very low computational burden [9, 11, 12]. The specific performance comparison can be seen in Table 1. Therefore, the electronic payment scheme based on ECC is more effective than that based on PKC.

The symmetric key encryption system has a simple encryption processing, encryption speed, shorter key, and so forth [12]. The authors summarize the theory and experience of predecessors and propose a new type of dynamic symmetric key mobile commerce scheme based on self-verified mechanism in this paper. This proposed scheme meets the requirements of both security and high efficiency because of the application of ECC. Based on the self-verified signature concept, each transaction entity holds the verification key and the digital signature for a later user authentication [3, 13]. The symmetric keys held by two entities are generated dynamically by the verification key and the digital signature. This contributes to security and efficient information interaction. A special key management mechanism is not necessary to reduce the cost of key management. In this way, the network operator only needs to provide users with a secure network and does not need to maintain redundancy authentication table. Therefore, the electronic payment scheme can not only meet the requirements of the large-scale mobile users, but also execute secure and efficient information interaction with generated symmetric key between the two entities after successful authentication. The environment of the electronic payment scheme is very suitable for large-scale mobile user environments, because the network operator does not need to maintain redundancy authentication table. In addition, the proposed scheme supports user anonymity mechanism and confidentiality, and it can prevent impersonation attack effectively. With our efforts, the system safeguards the rights and interests of users and ensures security. This scheme adopts ECC. Compared with other mechanisms such as the PKC and pairing function encryption mechanism, ECC obviously improves the operating efficiency of the system [14–16]. To sum up, the proposed scheme is effective and practical in mobile commerce.

TABLE 2: The parameter self-authentication scheme.

Parameter	Explanation
F_q	Finite field F_q over a large odd prime q
$E_q(a, b)$	Elliptic curve equation with the order n over F_q
Q	Public point over $E_q(a, b)$
$H(\cdot)$	The one-way hash function
$*$	The point multiplication over $E_q(a, b)$
V_X	A verification key that is generated by O for the entity X
(E_X, S_X)	The self-verified signature that is generated by O for the entity X
ID_X	The unique identity of trading entity X

This paper is structured as follows. In Section 2, the authors summarize the main idea of the self-verified mechanism and basic steps. In Section 3, the paper presents detailed process of the proposed scheme. In Section 4, the authors analyze operational efficiency and security. Finally, conclusions are made in Section 5.

2. The Principle of Self-Verified Mechanism

Yang and Chang [3] proposed an authentication mechanism which is divided into three phases: the initialization phase, the registration phase, and the authentication phase.

2.1. The Initialization Phase. In this phase, the server S initializes the system parameters over an elliptic curve domain through the following steps. In order to facilitate subsequent statements, important parameters and explanations are listed in Table 2.

2.1.1. Elliptic Curve Equation. S chooses a finite field F_q over a large odd prime q and generates an elliptic curve equation $E_q(a, b)$:

$$y^2 = x^3 + ax + b \pmod{q}, \quad (1)$$

where parameters satisfy the following conditions:

$$\begin{aligned} a, b &\in F_q, \\ q &> 3, \end{aligned} \quad (2)$$

$$4a^3 + 27b^2 \not\equiv 0 \pmod{q}.$$

S selects a public point Q over $E_q(a, b)$ and a public one-way hash function $H(\cdot)$, where Q is the finite point over $E_q(a, b)$.

2.1.2. Generating Public Key. S chooses its private key $d_S \in Z_q$ to compute its public key by

$$U_S = d_S * Q. \quad (3)$$

2.2. The Registration Phase. Assume that user A wants to log in the server S . Prior to the logging, A must register to S .

2.2.1. Generating Verification Key and Self-Verified Signature. Firstly, A sends a registration request to S . S generates A 's verification key by

$$V_A = H(ID_A \| w_A), \quad (4)$$

where $w_A \in Z_q^*$ and ID_A is A 's identity. S computes W_A by

$$W_A = w_A * Q = (x, y), \quad (5)$$

where x and y denote the x -coordinate and y -coordinate of W_A , respectively. To generate the self-verified signature (E_A, S_A) , S computes

$$\begin{aligned} E_A &= H(x \| ID_A) \bmod n, \\ S_A &= (w_A - d \cdot E_A) \bmod n. \end{aligned} \quad (6)$$

2.2.2. Confirming the Legitimacy of Information. S sends $\{V_A, (E_A, S_A)\}$ to A via a secure channel. A verifies the legitimacy of the message by computing

$$\begin{aligned} W'_A &= S_A * Q + E_A * U_S = (x', y'), \\ E'_A &= H(x' \| ID_A). \end{aligned} \quad (7)$$

Then, A checks if E'_A is equal to E_A . If they are equal, then A confirms that $\{V_A, (E_A, S_A)\}$ is really generated by O .

2.3. The Authentication Phase. In this phase, A wants to log in S ; S can verify the user's legality [12].

2.3.1. Obtaining Data Set. A uses $H(\cdot)$ to compute

$$C = H(ID_A \| V_A \| TS), \quad (8)$$

where TS is the timestamp; A sends data set (ID_A, C, E_A, S_A) to S .

2.3.2. Identity Authentication. After receiving (ID_A, C, E_A, S_A) , S computes

$$\begin{aligned} w'_A &= (S_A - d_S * E_A) \bmod n, \\ V'_A &= H(ID_A \| w'_A), \\ C' &= H(ID_A \| V'_A \| TS). \end{aligned} \quad (9)$$

S checks if C' is equal to C that is sent from A . If they are equal, then S can authenticate that A is a legal user.

3. Proposed Scheme

There are three transaction entities in the proposed e-payment scheme: the provider of electronic goods P , the mobile user U , and the network operator O that is a collection of financial institutions. O provides the wireless network bearer services to P and U , such as 3G services. Before being involved in trading officially, P and U must register to O

FIGURE 1: Trading model.

and obtain the exclusive account. Only in this way can O provide service for user's transaction. The trading model of the proposed scheme is shown in Figure 1.

The proposed electronic trading scheme is divided into four phases: the registration phase, the withdrawing phase, the paying phase, and the depositing phase. During the registration phase, P and U need to register to O for obtaining their verification keys and self-verified signatures. The function of withdrawing phase is that U not only obtains an electronic identification of account balance but also completes the identity authentication with P . In the paying phase, U and P perform authentication with each other; then U will obtain the electronic goods from P . During the depositing phase, U agrees on this transaction and then P redeems the price from the account of U .

3.1. The Registration Phase. Before the depositing phase, P and U need to register to O for obtaining their verification keys and self-verified signatures. The steps of this phase are demonstrated as follows.

3.1.1. Generating $\{V_U, (E_U, S_U)\}$. U sends a registration request to O , and O generates the verification key V_U and the self-verified signature (E_U, S_U) . Through the secure way, O sends authentication information $\{V_U, (E_U, S_U)\}$ to U . Then U stores $\{V_U, (E_U, S_U)\}$ into its mobile device for subsequent authentications.

3.1.2. Generating $\{V_P, (E_P, S_P)\}$. In a similar way, P gets the authentication information $\{V_P, (E_P, S_P)\}$ from O and stores it into its mobile device.

3.1.3. Storing Authentication Information. O stores the registration information of U and P to its database. The information provides the foundation of authentication, generating keys, information transfer, and payment in later transaction.

3.2. The Withdrawing Phase. According to the registration information in the registration phase, U obtains an electronic identification of account balance that the maximum value is

V_N . In the subsequent transactions, the value of electronic goods bought by U from P will not exceed V_N . In this phase, U and P not only complete the identity authentication but also generate a pair of symmetric key between themselves, and the symmetric key will be applied during user confirmation mechanism in the depositing phase. The steps of this phase are shown as follows and the specific flow chart is shown in Figure 2.

Step 1. U makes use of $\{V_U, (E_U, S_U)\}$ to compute

$$C_{UO} = h(ID_U \| ID_P \| V_U \| TS), \quad (10)$$

where TS is the timestamp and U sends $ID_U, ID_P, (E_U, S_U), TS$, and C_{AO} to O .

Step 2. In order to verify the legitimacy of U , O uses its private key d_O to compute

$$\begin{aligned} w'_U &= (S_U - d_O * E_U) \bmod n, \\ V'_U &= H(ID_U \| w'_U). \end{aligned} \quad (11)$$

Then, O checks validity of TS . If TS is valid, O computes

$$C'_{UO} = h(ID_U \| ID_P \| V'_U \| TS). \quad (12)$$

O confirms that U is legal and above withdrawing information is really sent from U when C'_{UO} equals C_{UO} . Otherwise, O rejects the transaction.

Step 3. O generates an electronic identification of account balance that the maximum value is V_N . In the subsequent transactions, the value of electronic goods bought by U from P will not exceed V_N . Meanwhile, O generates a serial number SN of V_N .

Step 4. O makes use of w'_U, ID_O, ID_U to generate the symmetric key

$$K_{sO,U} = H(w'_U \| ID_O \| ID_U). \quad (13)$$

Based on ECC, O generates the digital signature $\text{Sig}(V_N \| SN \| ID_P)$ and computes

$$C_{OU} = E_{V'_U}(K_{sO,U}, V_N, SN, V'_U, \text{Sig}(V_N \| SN \| ID_P)), \quad (14)$$

and then it sends C_{OU} to U and stores (V_N, SN) in the local database and deducts the cost of V_N from mobile user's account.

Step 5. U uses symmetric key to decrypt C_{OU} for $K_{sO,U}, V_N, SN, V'_U, \text{Sig}(V_N \| SN \| ID_P)$.

Then whether the equation $V'_U = V_U$ is established is checked. If it is established, U confirms that C_{OU} is really sent by O , stores (V_N, SN) into the users' database, and obtains symmetric key $K_{sO,U}$.

3.3. The Paying Phase. In this phase, U sends good information GI to P ; then U and P perform authentication with

FIGURE 2: Flow chat of withdrawing phase.

each other. After the authentication is legalized, U will obtain the electronic goods encrypted by the symmetric key $K_{sP,U}$ generated between the two entities. The steps of this phase are shown as follows and the specific flow chart is shown in Figure 3.

Step 1.1. U browses P 's online shop and generates the good information GI_1 that contains the descriptions and the prices defined by P_1 of the electronic goods. Meanwhile, U arbitrarily selects an integer $r_U \in Z_q$ and obtains the value k_x by

$$\begin{aligned} R_U &= r_U * Q, \\ K_U &= r_U * U_P = (k_x, k_y). \end{aligned} \quad (15)$$

U generates the dynamic symmetric key $K_{sP,U}$ between P and U by

$$K_{sP,U} = H(r_U \| ID_P \| ID_U), \quad (16)$$

where ID_P and ID_U is the unique identification of P and U . U encrypts the payment message with the key k_x

$$PI = E_{k_x}\{GI_1, K_{sP,U}, V_N, SN, \text{Sig}(V_N \| SN \| ID_P)\}. \quad (17)$$

Step 1.2. After receiving the encrypted payment message PI , P obtains k'_x by

$$K'_U = d_P * R_U = (k'_x, k'_y). \quad (18)$$

P decrypts PI and obtains payment message DI by

$$DI = D_{k'_x}\{PI\} = \{GI_1, K_{sP,U}, V_N, SN, \text{Sig}(V_N \| SN \| ID_P)\}. \quad (19)$$

FIGURE 3: Flow chart of paying phase.

P verifies the legitimacy of digital signature with computing $\text{Ver}(\text{Sig}(V_N || SN || ID_P))$. If the signature is legal, P can confirm PI is really sent by U. Therefore, P confirms that $(K_{sP,U}, V_N, SN)$ is legal and obtains the dynamic symmetric key $K_{sP,U}$.

Step 1.3. P obtains the good information GI and then determines whether inequality $P_1 \leq V_N$ was established. If V_N is greater than or equal to P_1 , P stores (GI_1, ID_U, V_N, SN) in the database and sends $E_{K_{sP,U}}(EG_1)$ to U, where EG_1 is the electronic goods. Then U obtains the EG_1 encrypted by $K_{sP,U}$. Otherwise, U rejects the transaction.

If user wants to execute subsequent transactions, the proposed scheme can make full use of symmetric key $K_{sP,U}$, which is generated in the previous process. In the J th transaction, both entities apply hash function $H_K(\cdot)$, symmetric key $K_{sP,U}$, and good information GI_J to complete the transaction. The steps of this phase are shown as follows.

Step J.1. U browses P's online shop and generates the J th good information GI_J . In the meantime U updates symmetric key $K_{sP,U}^J = H_K^J(K_{sP,U})$, where $H_K^J(\cdot)$ represents performing the hash operation J times.

Step J.2. U uses $K_{sP,U}^J$ to compute the payment message by

$$PI_J = E_{K_{sP,U}^J} \{GI_J, ID_U, V_N, SN\}, \quad (20)$$

where GI_J contains the price information P_J and sends PI_J to P. P updates the symmetric key $K_{sP,U}^J$ and obtains the payment message by

$$DI = D_{K_{sP,U}^J} \{PI_J\} = (GI_J, ID_U, V_N, SN). \quad (21)$$

Step J.3. After receiving DI, P judges the condition

$$I = P_1 + P_2 + \dots + P_J \leq V_N. \quad (22)$$

If the inequality is not established, P rejects the transaction. If the inequality is established, P stores $(G_1 + G_2 + \dots + G_J, ID_U, V_N, SN)$ into the database and sends $E_{K_{sP,U}^J}(EG_J)$ to U. Finally, U obtains electronic goods EG_J encrypted by $K_{sP,U}^J$.

3.4. The Depositing Phase. After the paying phase, P obtains $I = P_1 + P_2 + \dots + P_J$ from U and wants to redeem them from O in this phase. The steps of this phase are shown as follows and the specific flow chart is shown in Figure 4.

Step 1. P makes use of V_P to generate

$$EP_{P,O} = E_{V_P} (ID_P, ID_U, SN, V_P, GI). \quad (23)$$

Then it sends $EP_{P,O}, ID_P, (E_P, S_P)$ to O, where is the collection of $GI_1, GI_2, \dots, GI_J$.

Step 2. In order to verify P, O uses private key d_O to generate V'_P and compute $EP'_{P,O}$ by

$$w'_p = (S_p - d_O \cdot E_p) \bmod n, \quad (24)$$

$$V'_p = H(ID_P || w'_p),$$

$$EP'_{P,O} = E_{V'_P} (ID_P, ID_U, SN, V'_P, GI).$$

O checks if the equation $EP'_{P,O} = EP_{P,O}$ holds. If the equation holds, then O confirms that P is legal.

Step 3. O uses $K_{sO,U}$ to compute

$$EP_{O,U} = E_{K_{sO,U}} (ID_P, ID_U, GI, SN) \quad (25)$$

and sends $EP_{O,U}$ to U. U makes use of $K_{sO,U}$ and obtains ID_P, ID_U, GI, SN . If U agrees on this transaction and replies confirmation information to O, then O completes the deposit. Otherwise, O rejects this transaction.

4. The Performance and the Security Analyses

This scheme will be compared to the related schemes in terms of performance and security analysis in order to identify the characteristics and advantages of proposed scheme. Compared with previous trading models [2, 3], the proposed scheme further compresses the computation costs, and the dynamic symmetric key introduced improves the dynamic efficiency of the system. Considering the complexity and integration of current system, the proposed scheme adds the user confirmation mechanism which can maximize the protection of the rights of the user.

FIGURE 4: Flow chart of depositing phase.

4.1. The Performance Analysis. Compared with authentication mechanism of CBCS and IDBCS, the efficiency SVDSS authentication is higher. The reason is that this scheme adopts the self-verified signature mechanism to implement authentication between transactions entities, eliminate the need for frequent transfer certificate and verification, and save communication cost. In the specific verification process, the proposed scheme adopts the mechanism based on ECC. Compared with the public key cryptosystem (PKC) [8], ECC uses smaller key length to meet the same level of security and bear very low computational burden [9, 10]. After trading entity verifies that each side is legal object, it achieves symmetric encryption/decryption using the symmetric key. In the concrete scheme, it further improves the system efficiency from the following two aspects.

4.1.1. Payment Efficiency. In the previous mobile commerce, hash function was used to generate electronic money instead of cash. T_H denotes the execution time for executing the hash function for token generation and verification. As for T_H denotes 0.006 ms on 15 a Pentium IV 3.0 GHz with 2 GB [17]. In the literature [2], in order to generate and verify N tokens, the total number of hash operation performed is $3N$ in the entire transaction process (including the generating, using, and redeeming of electronic token). In the literature [3], when U obtains the tokens from O , U did not use hash function but did get the tokens directly. So the total number of hash operation performed is $2N$. According to literature [2, 3], the total execution time for token generation and verification is $3NT_H$ and $2NT_H$. Usually, the number N is from 50 to 50,000. The total execution time of token generation and verification is illustrated in Figure 5, where the literature [2, 3] introduces the Lin et al.'s scheme and Yang and chang's scheme, respectively. In the proposed scheme, U does not use hash function to generate the electronic tokens;

FIGURE 5: The analysis of payment efficiency.

the user directly obtains V_N from O . The total price of the goods purchased keeps accumulating in P , as long as the price does not exceed V_N . Therefore, compared with literature [2, 3], payment efficiency of proposed scheme has been greatly improved.

4.1.2. Message Encryption and Decryption. Recently, in order to improve the efficiency of mobile commerce, symmetric key mechanisms have been applied actively. However, due to the difficulties of key management of symmetric key, the concrete scheme of mobile commerce is based on asymmetric keys, to generate a symmetric key between trading entity. According to literature [2], the system generates symmetric key between entities, but the public/private key that can generate symmetric key exists in the KDC. Once the KDC information leakage occurs, the security of the whole system will be under threat. And the generated symmetric keys in subsequent transactions are not continuously updated, which will result in the insecurity of the system. In the literature [3], both the symmetric keys are generated by executing three times point multiplication over $E_q(a, b)$ during each paying phase. In the paying phase, assume U and P execute J times payment, the total execution time for generating the symmetric keys is $3JT_{ECC}$.

T_{ECC} denotes the time of the multiplication on an elliptic curve $E_q(a, b)$. In this paper, the scheme generates the first pair symmetric key in the first process during the paying phase. In the subsequent transaction, only the hash function is used to update the symmetric key $K_{SP,U}^j = H_K(K_{SP,U})$. The total execution time for generating the symmetric keys is $3T_{ECC} + (J - 1) * 2 * T_H$. In fact, T_{ECC} is much larger than T_H . This will further reduce the computing cost of the system and improve the execution efficiency. As is shown in Figure 6, the computational cost of generating symmetric key in the proposed scheme is higher than that in the literature [3].

FIGURE 6: The analysis of generating symmetric key.

4.2. The Security Analysis. The authors analyze the security of proposed scheme as follows.

4.2.1. Prevent Impersonation Attack. Assume that an attacker makes an attempt to modify the response information returned to O [18–21]. Obviously, the attacker needs to forge a set of data, including V_U , (E_u, S_u) . After receiving the forged information, O will naturally enter into the verification mode by computing (11) and (12).

If $C_{U,O}$ is not equal to $C'_{U,O}$, O discovers the user is illegal and then rejects the transaction. The same authentication mechanism also occurs between O user and P . The proposed scheme makes full use of this authentication mechanism to prevent impersonation attack.

4.2.2. User Anonymity. In electronic payment schemes, the vender (service provider) does not need to know the user's real identity to protect the user's privacy [22–24]. Provider obtains the payment information (17).

It does not contain identity information about user; service providers' judgment of the source information is based on the validity of $\text{Sig}(V_N \| \text{SN} \| \text{ID}_P)$. Subsequent transactions are based on $(K_{sP,U}, V_N, \text{SN})$; as long as the total price of the purchased goods does not exceed V_N , the entire transaction can continue proceeding. P redeems the $I = P_1 + P_2 + \dots + P_J$ from O based on SN in the depositing phase. In the process of the whole system, vender has no access to the user's identity information.

4.2.3. Confidentiality. Through the analysis of the concrete transaction process, information of the transaction between entities is held by pairwise symmetric key to encrypt/decrypt. Concrete example is as follows.

Equations (17) and (19) achieve the secure transfer of information between U and P .

Equations (20) and (21) achieve the secure transfer of information between U and O . However, compared to

the asymmetric keys, symmetric keys are easy to crack [25, 26]. Thus during the transaction phase, the symmetric key between the user and the service provider is continuously updated, which can also prevent the Man-in-the-Middle attack.

4.2.4. User Confirmation Mechanism. In fact, the operation of a whole system is not isolated, and the attack also exists. In order to improve the system security and protect the lawful rights and interests of customers, the proposed scheme particularly introduces this mechanism. First of all, symmetric key is generated between U and O in the withdrawing phase. In the depositing phase, O obtains ID_P , ID_U , SN , and GI and computes (25).

After receiving $\text{EP}_{O,U}$ from O , U can decrypt it and generate a feedback (agree on or reject the transaction). Finally, according to the user's feedback information, O completes/terminates the depositing process.

5. Conclusions

This scheme is based on the self-verified mechanism, the application of ECC, key agreement mechanism, prepayment mechanism, and other technologies to guarantee security and high efficiency of this proposed scheme. The proposed scheme does not need certificate management, which avoids the burden of network node storage certificate in CBCS and the communication overhead due to transferring certificate at the same time. The use of the self-verified mechanism avoids the defects of key escrow of IDBCS and no longer requires KDC to maintain a set of large user authentication tables, which can greatly reduce the system burden. The proposed scheme also takes advantage of updated symmetric key and user confirmation mechanism to guarantee the security. In a word, this scheme possesses the advantages of the current trading system which ensures the real time and user anonymity and further improves efficiency and security of system.

Conflict of Interests

The authors declare that they have no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is partially supported by the National Natural Science Foundation of China (no. 61101224) and Natural Science Foundation of Tianjin (no. 12jcqnjc00500) and supported by Program for New Century Excellent Talents in University (NCET-12-0400) and Postdoctoral Fund in China (2012M520574).

References

- [1] L. Chang, Y. Ouzrout, A. Nongailard, A. Bouras, and Z. Jiliu, "The reputation evaluation based on optimized Hidden Markov Model in E-commerce," *Mathematical Problems in Engineering*, vol. 2013, Article ID 391720, 11 pages, 2013.

- [2] P. Lin, H.-Y. Chen, Y. Fang, J.-Y. Jeng, and F.-S. Lu, "A secure mobile electronic payment architecture platform for wireless mobile networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2705–2713, 2008.
- [3] J.-H. Yang and C.-C. Chang, "A low computational-cost electronic payment scheme for mobile commerce with large-scale mobile users," *Wireless Personal Communications*, vol. 63, no. 1, pp. 83–99, 2012.
- [4] M. Damrudi and N. Ithnin, "An optimization of tree topology based parallel cryptography," *Mathematical Problems in Engineering*, vol. 2012, Article ID 871091, 10 pages, 2012.
- [5] Y.-J. Chen, W.-C. Hsieh, W. Chen, and Z.-Y. Meng, "An efficient and secure micro-payment protocol for mobile commerce," in *Proceedings of the 9th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI '05)*, pp. 7–12, Orlando, Fla, USA, July 2005.
- [6] D. He, Y. Chen, and J. Chen, "An id-based three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments," *Arabian Journal for Science and Engineering*, vol. 38, no. 8, pp. 2055–2061, 2013.
- [7] X. Zhu, X. Shang, C. Wang, and R. Zhang, "MOTP: an identity authentication scheme for M-commerce," *Chinese Journal of Electronics*, vol. 22, no. 1, pp. 146–150, 2013.
- [8] W.-J. Tsaur, "Several security schemes constructed using ECC-based self-certified public key cryptosystems," *Applied Mathematics and Computation*, vol. 168, no. 1, pp. 447–464, 2005.
- [9] Y.-P. Liao and C.-M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886–900, 2013.
- [10] R. Guo, Q. Wen, H. Shi, Z. Jin, and H. Zhang, "Certificateless public key encryption scheme with hybrid problems and its application to internet of things," *Mathematical Problems in Engineering*, vol. 2014, Article ID 980274, 9 pages, 2014.
- [11] J.-H. Yang, Y.-F. Chang, and Y.-H. Chen, "An efficient authenticated encryption scheme based on ECC and its application for electronic payment," *Information Technology and Control*, vol. 42, no. 4, pp. 315–324, 2013.
- [12] A. Zakerolhosseini and M. Nikooghadam, "Secure transmission of mobile agent in dynamic distributed environments," *Wireless Personal Communications*, vol. 70, no. 2, pp. 641–656, 2013.
- [13] Z. Li, Y. Zhuang, B. Zhang, and C. Zhang, "Novel frequency hopping sequences generator based on AES algorithm," *Transactions of Tianjin University*, vol. 16, no. 1, pp. 22–27, 2010.
- [14] C.-H. Chou, K.-Y. Tsai, T.-C. Wu, and K.-H. Yeh, "Efficient and secure three-party authenticated key exchange protocol for mobile environments," *Journal of Zhejiang University: Science C*, vol. 14, no. 5, pp. 347–355, 2013.
- [15] A. K. Rahuman and G. Athisha, "Reconfigurable architecture for elliptic curve cryptography using FPGA," *Mathematical Problems in Engineering*, vol. 2013, Article ID 675161, 8 pages, 2013.
- [16] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Ad-Hoc and Sensor Wireless Networks*, vol. 21, no. 1-2, pp. 121–149, 2014.
- [17] J.-Y. Kim and H.-K. Choi, "An enhanced security protocol for VANET-based entertainment services," *IEICE Transactions on Communications*, vol. E95-B, no. 7, pp. 2245–2256, 2012.
- [18] J. Wei, W. Liu, and X. Hu, "Cryptanalysis and improvement of a robust smart card authentication scheme for multi-server architecture," *Wireless Personal Communications*, vol. 77, no. 3, pp. 2255–2269, 2014.
- [19] F. Wen, D. Guo, and X. Li, "Cryptanalysis of a new dynamic ID-based user authentication scheme to resist smart-card-theft attack," *Applied Mathematics and Information Sciences*, vol. 8, no. 4, pp. 1855–1858, 2014.
- [20] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 591–601, 2014.
- [21] X. Li, J. Niu, M. K. Khan, and Z. Wang, "Applying LU decomposition of matrices to design anonymity bilateral remote user authentication scheme," *Mathematical Problems in Engineering*, vol. 2013, Article ID 910409, 10 pages, 2013.
- [22] Y. Choi, D. Lee, J. Kim et al., "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.
- [23] H. Lai, J. Xiao, L. Li, and Y. Yang, "Applying semigroup property of enhanced chebyshev polynomials to anonymous authentication protocol," *Mathematical Problems in Engineering*, vol. 2012, Article ID 454823, 17 pages, 2012.
- [24] W.-B. Hsieh and J.-S. Leu, "Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks," *Wireless Communications and Mobile Computing*, vol. 14, no. 10, pp. 995–1006, 2014.
- [25] W.-J. Liu, C. Liu, H.-B. Wang, J.-F. Liu, F. Wang, and X.-M. Yuan, "Secure quantum private comparison of equality based on asymmetric W state," *International Journal of Theoretical Physics*, vol. 53, no. 6, pp. 1804–1813, 2014.
- [26] C.-Y. Lin and T. Hwang, "CNOT extraction attack on 'quantum asymmetric cryptography with symmetric keys'," *Science China: Physics, Mechanics and Astronomy*, vol. 57, no. 5, pp. 1001–1003, 2014.