ISSN 1392 – 124X, ISSN 2335 – 884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2013, Vol.42, No.4

An Efficient Authenticated Encryption Scheme Based on ECC and its Application for Electronic Payment

Jen-Ho Yang[1], Ya-Fen Chang[2], Yi-Hui Chen[3]

[1] *Department of Multimedia and Mobile Commerce,*
Kainan University, Taoyuan County, 33857, Taiwan
e-mail: jenhoyang@mail.knu.edu.tw

[2] *Department of Computer Science and Information Engineering,*
National Taichung University of Science and Technology, Taichung, 404, Taiwan
e-mail: cyf @cs.ccu.edu.tw

[3] *Department of Applied Informatics and Multimedia,*
Asia University, Taichung 41354, Taiwan
e-mail: chenyh@asia.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.42.4.2150

Abstract. In this paper, we propose an efficient authenticated encryption scheme based on elliptic curve cryptography. The proposed scheme does not need to construct any digital signature, so the computation costs can be greatly reduced. In addition, we also use the proposed authenticated encryption scheme to design a secure electronic payment system. The proposed electronic payment system provides the security requirements of confidentiality, authenticity, integrity, privacy protection, and double-spending prevention. According to the results of this paper, the proposed authenticated encryption scheme can be easily implemented in mobile payment environments. Besides, it can be also applied to electronic auction, online meeting, and electronic voting.

Keywords: Authenticated encryption; elliptic curve; electronic payment; digital signature; electronic commerce.

1. Introduction

To authenticate and protect the secret information transmitted between a sender and a receiver on the Internet, the traditional approach is that the sender first uses a digital signature scheme [1] to sign the message. Then, the sender encrypts both the message and the signature using a symmetric encryption algorithm, such as AES [2] or DES [3]. Nevertheless, this kind of "signature-then-encryption" approach has high computation costs. Therefore, Zheng [4] firstly proposed an authenticated encryption scheme (it is also called the signcryption scheme), which combines the functions of the digital signature and encryption schemes in one logical step. Compared with the signature-then-encryption approach, the authenticated encryption scheme has lower computation costs. From then on, various authenticated encryption schemes were proposed [5-12].

However, we find that the previous authenticated encryption schemes have to generate and verify the digital signature to accomplish message authentication and confidentiality. For some applications, the receiver only wants to ensure that the message is really sent by the correct sender, but he/she does not want to obtain the sender's signature. In order to confirm the message is really sent by a valid sender, verifying the sender's signature is inefficient for the receiver. Up to now, no research discusses the above-mentioned circumstance. In addition, there is no practicable scheme which combines the functions of message authentication and encryption without constructing the digital signature.

Therefore, we propose an efficient authenticated encryption scheme based on elliptic curve cryptography (ECC). In the proposed scheme, the sender uses his/her private key and the receiver's public key to construct a symmetric key for encrypting the message as a cipher. After that, the receiver can utilize his private key to reconstruct the same symmetric key for decrypting the cipher to obtain the message. Since the symmetric key is constructed by the sender's private key, only the actual sender can encrypt the message. Thus, the receiver can ensure

that the message is really sent by an actual sender. Besides, only the designated receiver can decrypt the cipher to obtain the original message because the symmetric key can be also reconstructed by the receiver's private key. Without constructing any digital signature, the proposed authenticated encryption scheme can efficiently accomplish message confidentiality and user authentication at the same time. Compared with the previous authenticated encryption schemes, the proposed scheme does not need to verify the sender's signature so the computation costs can be greatly reduced.

Since the proposed authenticated encryption scheme can accomplish message confidentiality and user authentication efficient, it can be applied to many applications for electronic services, such as electronic payment (e-payment), electronic voting, and online auction. In this paper, we also utilize our authenticated encryption scheme to design an efficient e-payment system on ECC. Because the proposed e-payment system is based on our authenticated encryption scheme, it can efficiently protect the purchasing information and authenticate the message sender at the same time.

In addition, the proposed e-payment system has the advantages of message confidentiality, authenticity, integrity, privacy protection, and double-spending prevention. Therefore, the proposed e-payment system provides a secure and practical payment tool for the electronic services. Because the proposed scheme has very low computation costs, it can be also easily applied to mobile payment applications.

2. Related works

To show that the previous authenticated encryption schemes have to use digital signature for the authentication, we introduce Hwang and Sung's signcryption scheme [11] in this section. In their scheme, only the designated receiver can recover the encrypted message to verify the digital signature. The notations used in Hwang and Sung's scheme are shown in Table 1.

Table 1. The notations in Hwang and Sung's scheme

p, q	Two large public primes with $q \mid (p-1)$
l	A secure size of a symmetric key
g	A generator in Z_p^* with the order q
$E_k(\cdot)$ / $D_k(\cdot)$	A symmetric encryption/decryption with the key k
$H_1(\cdot)$	A public one-way hash function maps from $\{0, 1\}^*$ to Z_q^*
$H_2(\cdot)$	A public one-way hash function maps from $\{0, 1\}^*$ to $\{0, 1\}^l$
x_i / y_i	The private/public key of the user i satisfying $y_i = g^{x_i} \bmod p$

The signcryption phase:

In this phase, the sender Alice signs and encrypts a message m and sends the signcryption messages including the signature (V, S) to the receiver Bob. The steps are shown as follows.

Step 1. Alice randomly chooses two integers R and k in Z_q^*.

Step 2. Alice computes $V = H_1(g^k \bmod p \,\|\, m \,\|\, R \,\|\, y_B)$ and $s = k + V \cdot x_A \bmod q$ to generate $S = g^s \bmod p$ and $K = H_2(y_B{}^s \bmod p)$, where "||" is denoted as string concatenation.

Step3. Alice computes $C = E_K(m \,\|\, R)$ and sends the signcrypted text (C, V, S) to Bob, where (V, S) is the signature of the message m.

The unsigncryption phase:

In this phase, Bob decrypts the cipher C to obtain the message m and verifies the signature (V, S) to authenticate Alice.

Step 1. Bob computes the symmetric key $K = H_2(S^{x_B} \bmod p)$ to decrypt the message by $m \,\|\, R = D_K(C)$.

Step 2. Bob computes $V' = H_1(S \cdot (y_A)^{-V} \bmod p \,\|\, m \,\|\, R \,\|\, y_B)$ to verify if V' is equal to V or not. If $V' = V$, then Bob accepts that m is the correct message which is sent by Alice. Otherwise, Bob rejects it.

Hwang and Sung's scheme is shown in Figure 1. According to Hwang and Sung's scheme, we find that their scheme has two drawbacks. First, to ensure that the message m is really sent by Alice, Bob has to verify Alice's signature by computing $V' = H_1(S \cdot (y_A)^{-V} \bmod p \,\|\, m \,\|\, R \,\|\, y_B)$. This verification increases redundant computation costs if Bob does not want to obtain Alice's signature. Second, the signature (V, S) is directly sent to Bob via an open channel without performing any asymmetric or symmetric encryption algorithm. Thus, anyone can wiretap the communications between Alice and Bob to obtain (V, S). For some applications, this situation is very dangerous because the digital signature may be an important document. For example, a digital signature may be the electronic cash or electronic check on electronic payment systems so the signature cannot be revealed.

Similarly, the previous authenticated encryption schemes [5-12] have the above-mentioned drawbacks. That is, all these schemes have to construct and verify the digital signature for the authentication. To overcome the above drawbacks, we propose a new authenticated encryption scheme without constructing digital signature in the next section.

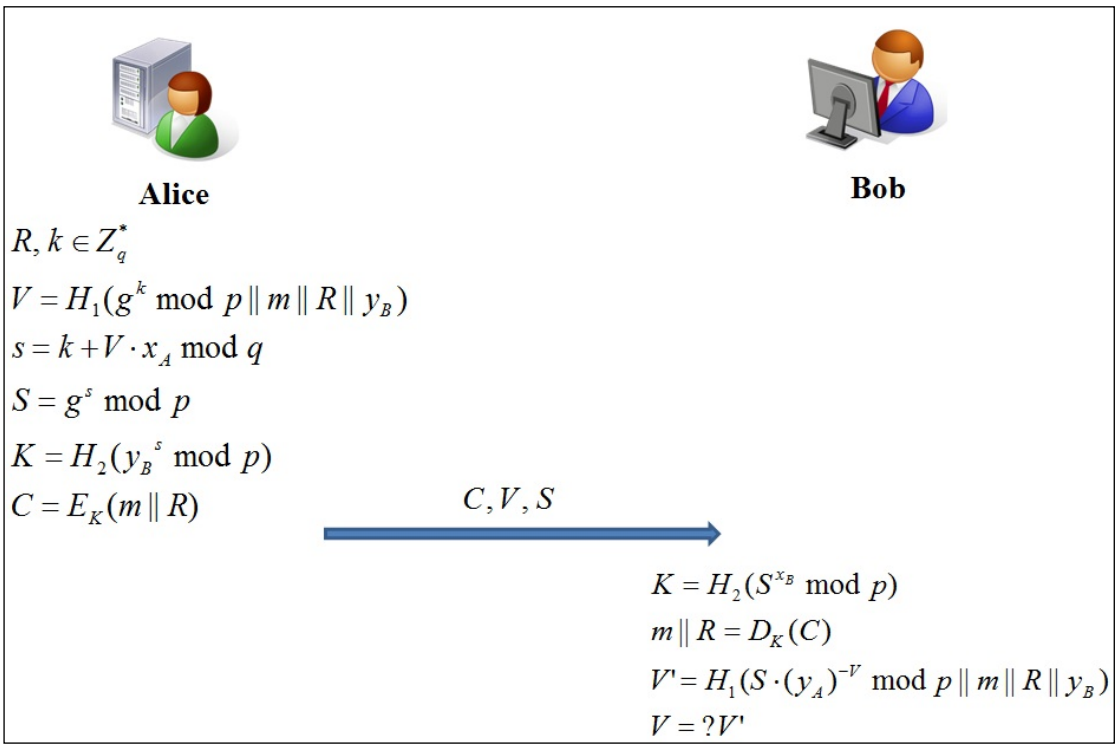

Figure 1. Hwang and Sung's authenticated encryption scheme

3. The proposed authenticated encryption scheme and its applications

In this section, we propose an efficient authenticated encryption scheme without involving the digital signature. In addition, we also use the authenticated encryption scheme to design an electronic payment system.

3.1. An efficient authenticated encryption scheme

To reduce the computation cost, we adopt elliptic curve cryptography [13-15] to design our authenticated encryption scheme. The proposed scheme is divided into three phases: the initialization phase, the authenticated encryption phase, and the verification phase.

The initialization phase:

In this phase, the system initializes and selects some parameters as follows.

Step 1. Choose a finite field F_q over a large odd prime $q > 2^{160}$.

Step 2. Choose an elliptic curve equation $E_q(a,b): y^2 = x^3 + ax + b \pmod q$ with the order n over F_q, where $a, b \in F_q$, $q > 3$, and $4a^3 + 27b^2 \neq 0 \pmod q$ [13, 14].

Step 3. Choose the symmetric encryption/decryption system $E_k(\cdot)/D_k(\cdot)$ such as AES [2], where k is the symmetric key.

Step 4. Choose a public point Q over $E_q(a,b)$ with the order n.

Step 5. Publish $E_q(a,b)$, $E_k(\cdot)$, $D_k(\cdot)$, and Q to all users.

The authenticated encryption phase:

In this phase, the sender Alice wants to send a message M to the receiver Bob. Then, Alice computes a common symmetric key to encrypt M such that only Bob can decrypt the cipher to obtain M. Assume that Alice has the private key $d_A \in Z_q$ and the public key U_A, where $U_A = d_A * Q$. Here, "*" denotes the point multiplication over $E_q(a,b)$. In addition, Bob has his private key $d_B \in Z_q$ and the public key U_B, where $U_B = d_B * Q$. Note that both Alice and Bob have to get the certificates for their public keys U_A and U_B from the certificate authority. Now, we describe this phase as follows.

Step 1. Alice verifies Bob's public key U_B by using the corresponding certificate.

Step 2. Alice randomly chooses an integer $r \in Z_q$ to compute $R = r * U_A$.

Step 3. Alice computes $\overline{R} = r * U_B$ and $K = d_A * \overline{R} = (k_1, k_2)$, where k_1 and k_2 are *x* and *y* coordinates of *K*, respectively.

Step 4. Alice uses k_1 as the common symmetric key to compute $C = E_{k_1}(ID_A \| M \| k_1 \| T)$ and sends (*C*, *R*, *T*) to Bob, where ID_A is the identity of Alice and *T* is a timestamp.

The verification phase:

In this phase, Bob decrypts the cipher *C* to obtain the message *M*, and he verifies that if *M* is really sent by Alice.

Step 1. After receiving (*C*, *R*, *T*), Bob computes $K = d_B * R = (k_1, k_2)$ to obtain the common symmetric key k_1.

Step 2. Bob uses k_1 to decrypt the cipher by $ID_A \| M \| k_1 \| T = D_{k_1}(C)$, and he checks if *T* is valid or not. If *T* is valid, then Bob checks if k_1 is the same as that he computes in Step 1. If T and k_1 are both correct, then Bob makes sure that *M* is actually sent by Alice. Otherwise, Bob rejects it.

The steps of the proposed scheme are illustrated in Figure 2. In the proposed scheme, Bob can make sure that the message *M* is really sent by Alice because only Alice can generate the symmetric key k_1 by d_A to encrypt *M*. On the other hand, only Bob can decrypt the cipher *C* to get *M* because the symmetric key k_1 can be also computed by Bob's private key d_B. Thus, the proposed scheme can accomplish the requirements of authentication and confidentiality at the same time, which satisfies the property of authenticated encryption scheme.

According to the proposed scheme, it has the following advantages. First, no digital signature is involved in the proposed scheme so it is more efficient than the related works. Second, the proposed scheme provides the anonymity because only the intended receiver can decrypt the cipher to get the sender's identity. This property is very useful for some applications such as electronic payment (e-payment), electronic voting (e-voting), and online auction, which can be implemented by the authenticated encryption scheme.

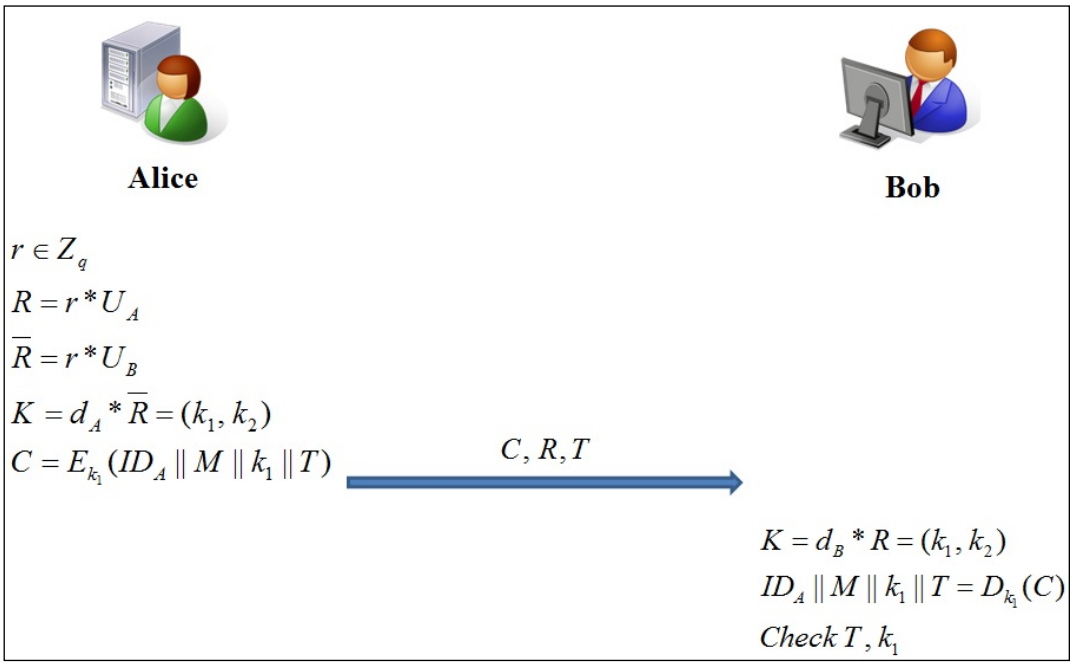

Figure 2. The proposed scheme

3.2. An e-payment system using the proposed authenticated encryption scheme

The proposed authenticated encryption scheme provides the user authentication and the message encryption at the same time. Thus, it can be applied to various applications on the Internet, such as e-payment, online meeting, and e-voting. In these applications, the e-payment is the most popular research topic so many e-payment systems [16-20] have been proposed in recent years. In this subsection, we show how to use the proposed scheme to implement an e-payment system as follows. The proposed e-payment system is divided into five phases: the initializing phase, the buying phase, the paying phase, the exchanging phase, and the transferring phase. In addition, the participants of the proposed system are the payer, the merchant, and the bank. Both the payer and the merchant already have

their own accounts in the bank. The buying, paying, and exchanging phases are illustrated in Figures 3 to 5, respectively. The details of the proposed e-payment system are as follows.

The initializing phase:

In this phase, the system initializes the public parameters $E_q(a,b)$, $E_k(\cdot)$, $D_k(\cdot)$, and Q defined in Section 3. In addition, the system publishes $E_q(a,b)$, $E_k(\cdot)$, $D_k(\cdot)$, and Q.

The buying phase:

In this phase, the payer (Alice) downloads good information (*GI*) that he/she wants to buy from the merchant's website. Here, the goods may be the electronic goods such as software, music, or movie. Then, Alice uses *GI* to generate the payment information and utilizes the proposed authenticated encryption scheme to encrypt the payment information. In addition, she sends the encrypted information to the bank for paying the money. In this e-payment scheme, Alice, the bank, and the merchant have their private/public key pairs d_A/U_A, d_B/U_B, and d_M/U_M, where $U_A = d_A * Q$, $U_B = d_B * Q$, and $U_M = d_M * Q$, respectively.

Step 1. Alice chooses the goods and downloads *GI* = {(*goods*_1, *price*_1), (*goods*_2, *price*_2), …, (*goods_l*, *price_l*)} from the merchant's website, where *goods_i* and *price_i* ($i = 1, 2, ..., l$) are denoted as the information and the price of the electronic goods *i*, respectively.

Step 2. Alice randomly selects an integer $r \in Z_q$ to compute $R = r * U_A$.

Step 3. Alice computes $\overline{R} = r * U_B$ and $K = d_A * \overline{R} = (k_1, k_2)$, where k_1 and k_2 are *x* and *y* coordinates of *K*, respectively.

Step 4. Alice generates the payment information $m = H(AD \| P \| ID_B)$, where $P = \sum_{i=1}^{l} price\_i$ and $H(\cdot)$ is a public one-way hash function.

Step 5. Alice uses k_1 as a symmetric key to compute $C_1 = E_{k_1}(ID_A \| m \| P \| k_1 \| T_1)$, where ID_A is the identity of Alice and T_1 is a timestamp. Then, Alice sends (C_1, R, T_1) to the bank.

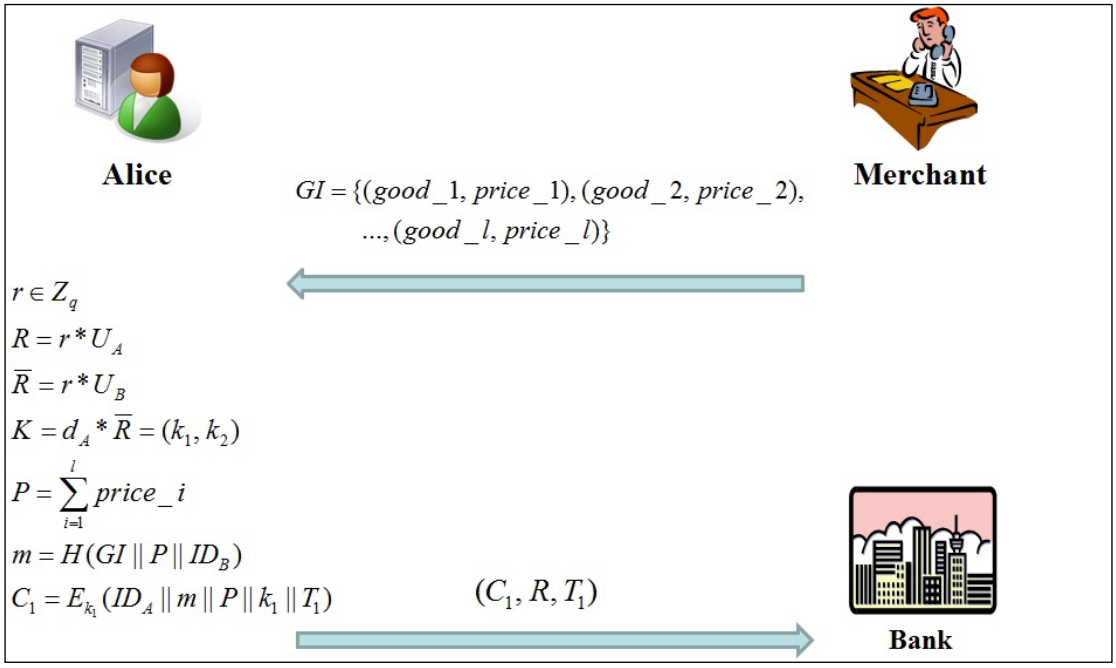

Figure 3. The buying phase

The paying phase:

In this phase, the bank withdraws the money from Alice's account and deposits it to a temporary account. Then, the bank generates a digital signature (*DS*) to be Alice's payment information. Note that *DS* is also the payment proof which implies Alice has already paid the money.

Step 1. The bank computes $K = d_B * R = (k_1, k_2)$ to obtain the common symmetric key k_1. Then, the bank computes $ID_A \| m \| P \| k_1 \| T_1 = D_{k_1}(C_1)$ and checks if T_1 is valid or not.

Step 2. The bank also checks if k_1 is equal to the key computed in Step 1. If T_1 and k_1 are both correct, then the bank accepts this transaction. Otherwise, the bank rejects it.

Step 3. According to ID_A and P, the bank withdraws the money from Alice's account and deposits the money to a temporary account. Next, the bank computes $= m \| E$, where E is the expiration date. The bank also uses d_B to generate a digital signature DS of M by using any ECC-based signature scheme such as [21, 22]. Then, the bank records $\{DS, M\}$ in its database.

Step 5. The bank uses k_1 to compute $C_2 = E_{k_1}(DS \| E \| k_1 \| T_2)$ and sends (C_2, T_2) to Alice, where T_2 is the timestamp.

Step 6. After receiving (C_2, T_2), Alice computes $DS \| E \| k_1 \| T_2 = D_{k_1}(C_2)$. Then, she checks if k_1 and T_2 are correct or not. If k_1 and T_2 are both correct, then she accepts the signature DS as a paying proof. Otherwise, she rejects it.

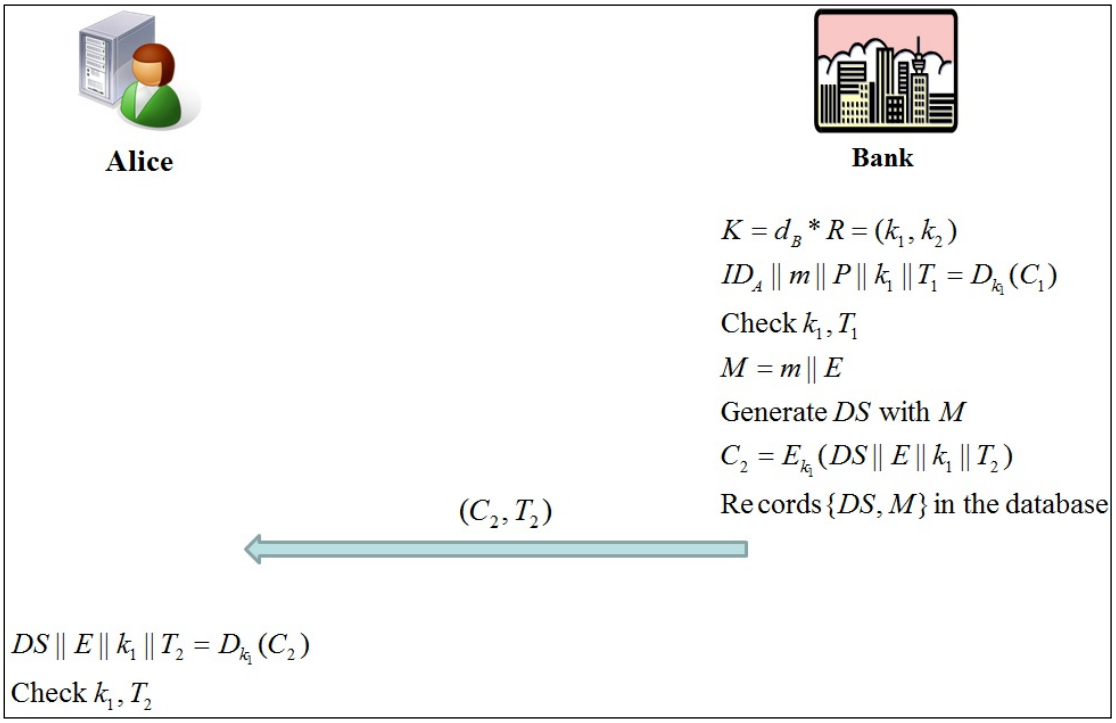

Figure 4. The paying phase

The exchanging phase:

In this phase, Alice utilizes the signature DS as the paying proof, and she sends the encrypted paying proof to the merchant for exchanging the goods.

Step 1. Alice randomly selects an integer $r' \in Z_q$ to compute $R' = r' * U_A$, $\overline{R}' = r' * U_M$ and $K' = d_A * \overline{R}' = (k_1', k_2')$.

Step 2. Alice uses k_1 to compute $C_3 = E_{k_1'}(ID_B \| DS \| E \| GI \| k_1' \| T_3)$ and sends (C_3, R_3, T_3) to the merchant, where T_3 denotes the current time.

Step 3. The merchant computes $K' = d_M * R' = (k_1', k_2')$ and uses k_1 to decrypt C_3 by $ID_B \| DS \| E \| GI \| k_1' \| T_3 = D_{k_1'}(C_3)$. Then, the merchant checks if k_1' and T_3 are correct or not. If they are both correct, then the merchant accepts this transaction. Otherwise, the merchant rejects it.

Step 4. According to GI, the merchant computes $P = \sum_{i=1}^{l} price\_i$ and $m = H(GI \| P \| ID_B)$. Then, the merchant computes $M = m \| E$ and uses the bank's public key U_B to verify DS with M [21, 22]. If DS is valid, then the merchant computes $C_4 = E_{k_1'}(Electronic\ goods)$ to encrypt the electronic goods. Next, the merchant sends C_4 to Alice and keeps the record of $\{DS, M\}$ in its database for double-spending checks.

Step 5. After Alice receives $C_4 = E_{k_1'}(Electronic\ goods)$, she uses k_1' to compute $Electronic\ goods = D_{k_1'}(C_4)$. Finally, Alice can obtain the electronic goods that she wants to buy.

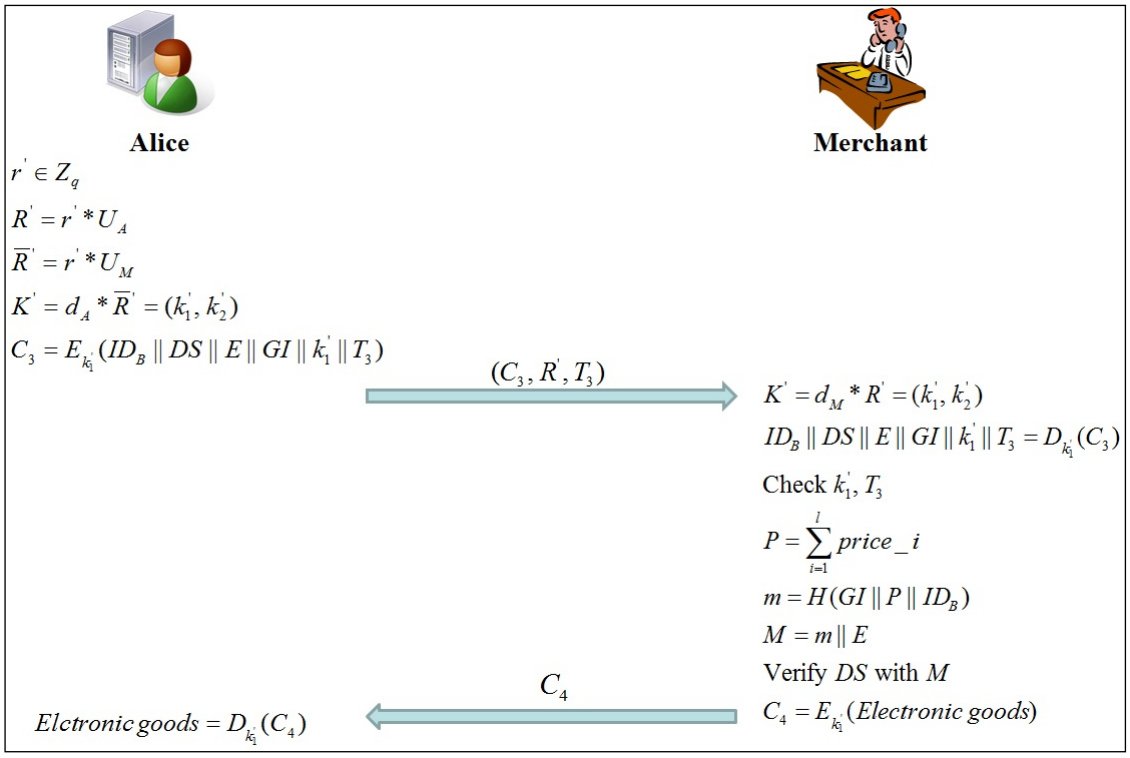

Figure 5. The exchanging phase

The transferring phase:

If Alice does not receive the goods, she will ask the bank to stop the transaction in this phase. Besides, the merchant can send the payment proof to the bank, and then the bank deposits the money to the merchant's account.

Step 1. Until the expiration date exceeds, the merchant can use *DS* to ask the bank to transfer the corresponding payment to its account.

Step 2. If Alice does not receive the goods before the expiration date, Alice can ask the bank to terminate this transaction. Then, the bank transfers the payment from the temporary account back to Alice's account.

Step 3. After transferring the payment from the temporary account to the merchant's account (or Alice's account), the bank removes the record {*DS*, *M*} from its database.

The e-payment system can provide secure transactions because the proposed authenticated encryption scheme is used. In addition, the proposed e-payment system is an efficient e-payment tool, which provides message confidentiality, authenticity, integrity, privacy protection, and double-spending prevention for the electronic transactions on Internet. The above-mentioned advantages of the e-payment system are discussed in the next section.

4. Discussions

In this section, we discuss the security of the proposed authenticated encryption scheme by performing some possible attacks on it. In addition, we also show how the proposed e-payment system can accomplish the properties of confidentiality, authenticity, integrity, privacy protection, and double-spending prevention.

4.1. Security analysis

In this subsection, we perform some possible attacks on the proposed authenticated scheme to analyze its security as follows.

Replay attack:

Assume that an attacker wiretaps the communication between the sender (Alice) and the receiver (Bob), and the attacker can obtain the message (*C*, *R*, *T*), where $C = E_{k_1}(ID_A \| M \| k_1 \| T)$. Then, the attacker may re-send (*C*, *R*, *T*) to Bob to pretend that he/she is Alice. However, this attack is infeasible because *C* contains the timestamp *T*, which denotes the real sending time. That is, Bob can

discover the message (*C*, *R*, *T*) is sent from an attacker by checking *T*. Therefore, the proposed scheme can prevent the replay attack.

Outsider attack:

Assume that an attacker collects the information (*C*, *R*, *T*) from the communication between Alice and Bob. Then, the attacker tries to get the message *M* form *C*. To decrypt *C*, the attacker has to know the symmetric key k_1. However, the attacker cannot obtain k_1 which is computed by $K = d_A * \overline{R} = (k_1, k_2)$ or $K = d_B * R = (k_1, k_2)$. This attack is impossible because the attacker needs to face the difficulty of elliptic curve discrete logarithm (ECDLP) [13, 14]. Therefore, the outsider attack does not work for the proposed scheme.

Impersonating attack:

Assume that an attacker impersonates Alice to send a forged message to Bob, and then he/she randomly chooses an integer $r' \in Z_q$ to compute $R' = r' * U_A$. Thus, the attacker chooses a forged private key $d_A^{'}$ to compute $\overline{R}' = r' * U_B$, $K' = d_A^{'} * \overline{R}' = (k_1^{'}, k_2^{'})$, and $C' = E_{k_1^{'}}(ID_A \| M' \| k_1^{'} \| T')$. Then, the attacker sends (C', R', T') to Bob and pretends he/she is Alice. However, the impersonating attack is impossible because Bob computes the symmetric key $K = d_B * R' = d_B * r' * U_A$ which is not equal to $K' = d_A^{'} * \overline{R}' = d_A^{'} * r' * U_B$. Thus, Bob cannot compute the correct key to decrypt the cipher C'. That is, Bob will find that the attacker is not Alice. According to the above reason, the proposed scheme can prevent the impersonating attack.

Server spoofing attack:

Assume that an attacker wants to pretend that he is a bank server. Then, the attacker uses a forged k_1' to compute $C_2' = E_{k_1}(DS' \| E' \| k_1' \| T_2)$ and sends (C_2', T_2) to Alice. However, this attack is impossible because the attacker does not know d_B to compute $K = d_B * R = (k_1, k_2)$. That is, Alice cannot use the correct k_1 to decrypt C_2', and Alice will detect that (C_2', T_2) is sent by an attacker.

Man-in-the-middle attack:

Assume that an attacker wiretaps the communication to get the payment information $(C_3, R^{'}, T_3)$, and he wants to use the payment information to obtain the goods. Therefore, the attacker may change the timestamp T_3 by T_3' and send $(C_3, R^{'}, T_3')$ to the merchant. Then, the merchant computes $ID_B \| DS \| E \| GI \| k_1^{'} \| T_3 = D_{k_1^{'}}(C_3)$ and checks if $k_1^{'}$ and T_3 are correct or not. Finally, the merchant can discover that $(C_3, R^{'}, T_3')$ is invalid because $T_3 \neq T_3'$. Thus, the man-in-the-middle attack is infeasible for the proposed scheme.

Identity theft attack:

The identity theft attack means that an attacker has already obtained the user's identity and some other information kept in user's device. Then, the attacker can use the information to impersonate a legal user. However, the user does not need to keep any information in user's side. In addition, the proposed scheme does not require the user's identity for authentication and verification. According to the above analysis, the identity theft attack is impossible for the proposed scheme.

4.2. The advantages of the proposed e-payment system

The proposed e-payment system has the following advantages: confidentiality, authenticity, integrity, privacy protection, and double-spending prevention. These advantages are discussed as follows.

Confidentiality:

The proposed e-payment system provides message confidentiality because it is designed by the authenticated encryption scheme of Subsection 3.1. In the proposed e-payment system, the secret messages are encrypted by a symmetric encryption algorithm. An attacker has to know the symmetric keys k_1 and $k_1^{'}$ to decrypt the cipher. However, it is infeasible because k_1 and $k_1^{'}$ can be only computed by the private keys (d_A, d_B) and (d_A, d_M), respectively. The attacker does not know these private keys. That is, only the designated receiver, who has the correct private key, has the ability to decrypt the cipher.

Authenticity:

The proposed payment system provides authenticity because it is designed by the authenticated encryption scheme of Subsection 3.1. That is, only Alice can compute k_1 by $K = d_A * \overline{R} = (k_1, k_2)$ and encrypt *m* by $C_1 = E_{k_1}(ID_A \| m \| P \| k_1 \| T_1)$. When the bank computes the same k_1 to decrypt C_1, it can check the correctness of k_1 to make sure that *m* is really sent by Alice. Similarly, only the bank can compute k_1 to encrypt $C_2 = E_{k_1}(DS \| E \| k_1 \| T_2)$. Thus, Alice can ensure that the message $(DS \| E \| k_1 \| T_2)$ is really sent from the bank without verifying *DS*.

Integrity:

The proposed e-payment system provides the message integrity because the payment information is sent by the ciphertext form, such as C_1, C_2, and C_3. No one can alter the payment information without knowing the symmetric keys k_1 and $k_1^{'}$. If R, $R^{'}$, T_1,

T_2 , or T_{31} is changed by an attacker, the valid receivers can discover the change by decrypting the cipher to check them. According to the above reasons, the proposed e-payment system provides the message integrity.

Privacy protection:

The proposed e-payment system protects the buying privacy because the goods information *GI* is protected by the one-way hash function $H(\cdot)$. The bank cannot obtain *GI* from $m = H(GI \| P \| ID_B)$, and thus the buying privacy can be protected from the bank. Besides, the payer's identification is not sent to the merchant in the exchanging phase. Moreover, the digital signature *DS* does not contain any payer's information. Therefore, the merchant does not know who the payer is. According to the above reasons, the buying privacy can be protected in the proposed e-payment system.

Double-Spending prevention:

Assume that Alice re-sends a used payment proof *DS* to the merchant for paying again. In this case, the merchant will discover the double-spending behavior because {*DS*, *M*} is still stored in the merchant's database. Similarly, the merchant cannot use *DS* for asking the bank to transfer the money again. This is because that the bank also keeps the record {*DS*, *M*} in its database. According to the above discussions, the double spending does not occur in the proposed e-payment system.

4.3. The performance analysis

In the subsection, we analyze the computation costs of the related e-payment schemes. Table 2 shows the computation costs of Wang et al.'s scheme [23], Oros and Popescu's scheme [24], and the proposed scheme.

Table 2. The computation costs of the related works

Schem / Cost	Wang et al.'s	Oros and Popescu's	Ours
Buying phase	9ME	8PM	3PM+1SY
Paying phase	11ME	2PM+3PA	1PM+2SY
Exchanging phase	5ME	3PA	4PM+2SY
Total costs	25ME	10PM+6PA	8PM+5SY

In Table 2, ME, PM, PA, and SY are modular exponentiation, point multiplication on ECC, pairing computation on ECC, and symmetric cryptosystem computations, respectively. In fact, the magnitude of these computation costs can be denoted as ME>PA>PM>SY. According to Table 2, the computation cost of the proposed scheme is much less than those of the related approaches.

5. Conclusions

To eliminate the computation costs of the digital signature, we propose an efficient authenticated encryption scheme based on elliptic curve cryptography in this paper. The proposed scheme can efficiently accomplish the message encryption and authentication at the same time. Compared with the related works, the proposed scheme is more efficient because it does not need to compute any digital signature. Besides, we also use the proposed authenticated encryption scheme to implement an e-payment system in this paper. Since the authenticated encryption scheme is used, the proposed e-payment system provides confidentiality, authenticity, integrity, privacy protection, and double-spending prevention. According to the results of this paper, the proposed authenticated encryption scheme can be easily applied to mobile payment applications in the future.

Acknowledgement

This work was supported in part by National Science Council under the grant NSC 100-2221-E-424-006.

References

[1] **R. L. Rivest, A. Shamir, L. Adleman.** A method for obtaining digital signatures and public key cryptosystems". *Communications of the ACM*, 1978, Vol. 21, No. 2, 120–126.

[2] Advanced Encryption Standard, http://csrc.nist.gov/archieve/aes.

[3] **B. Schneier.** Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. *John Wiley & Sons, Inc., New York, USA*, 1996.

[4] **Y. Zhang.** Digital signcryption or how to achieve cost (signature & encryption) <<cost(signature)+cost(encryption)". In: *Advances in Cryptology-CRYPTO'97*, 1997, LNCS, Springer-Verlag, pp. 165–179.

[5] **Y. Zheng, H. Imai.** How to construct efficient signcryption schemes on elliptic curves. *Information Processing Letters*, 1998, Vol. 68, 227–233.

[6] **Y. M. Tseng, J. K. Jan**. An efficient authenticated encryption scheme with message linkages and low communication costs. *Journal of Information Science and Engineering*, 2002, Vol. 18, 41–56.

[7] **K. F. Hwang, C. C. Chang**. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Transactions on Wireless Communications*, 2003, Vol. 2, No. 2, 400–407.

[8] **R. J. Hwang, C. H. Lai, F. F. Su.** An efficient signcryption scheme with forward secrecy based on elliptic curve. *Applied Mathematics and Computation*, 2005, Vol. 167, 870–881.

[9] **S. Y. Xie, B. Xu.** A publicly verifiable authenticated encryption scheme without using one-way function. In: *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics*, 2007, pp. 2511–2514.

[10] **F. Li, X. Xin, Y. Hu**. Identity-based broadcast signcryption. *Computer Standards & Interfaces*, 2008, Vol. 30, 89–94.

[11] **S. J. Hwang, Y. H. Sung.** Confidential deniable authentication using promised signcryption. *The Journal of Systems and Software*, 2011, Vol. 84, 1652–1659.

[12] **F. Li, M. K. Khan, K. Alghathbar, T. Takagi.** Identity-based online/offline signcryption for low power devices. *Journal of Network and Computer Applications*, 2012, Vol. 35, No. 1, 340–347.

[13] **N. Koblitz.** Elliptic curve cryptosystem. *Mathematics of Computation*, 1987, Vol. 48, 203–209.

[14] **D. Hankerson, A. Menezes, S. Vanstone.** Guide to Elliptic Curve Cryptography, *Springer-Verlag. New York, USA*, 2004.

[15] **J. W. Hong, S. Y. Yoon, D. I. Park, M. J. Choi, E. J. Yoon, K. Y. Yoo.** A new efficient key agreement scheme for VSAT satellite communications based on elliptic curve cryptosystem. *Information Technology and Control*, 2011, Vol. 40, No. 3, 252–259.

[16] **C. C. Chang, Y. F. Chang, J. S. Lee.** Mobile payment for off-line vender machines. *International Journal of Computer Science and Network Security*, 2005, Vol. 5, No. 9, 119–126.

[17] **W. K. Chen.** Efficient on-line electronic checks. *Applied Mathematics and Computation*, 2005, Vol. 162, 1259–1263.

[18] **V. Pasupathinathan, J. Pieprzyk, H. Wang.** Privacy enhanced electronic cheque system. In: *Proceedings of Seventh IEEE International Conference on E-Commerce Technology*, 2005, pp. 431–434.

[19] **R. J. Hwang, S. H. Shiau, D. F. Jan**. A new mobile payment scheme for roaming services. *Electronic Commerce Research and Applications*, 2007, Vol. 6, 184–191.

[20] **J. H. Yang, C. C. Chang.** An efficient payment scheme by using electronic bill of lading. *International Journal of Innovative Computing, Information and Control*, 2010, Vol. 6, No. 4, 1773–1779.

[21] **D. Johnson, A. Menezes, S. Vanstone.** The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, 2001, Vol. 1, No. 1, 36–63.

[22] **A. Khalique, K. Singh, S. Sood.** Implementation of elliptic curve digital signature algorithm. *International Journal of Computer Applications*, 2010, Vol. 2, No. 2, 21–27.

[23] **H. Wang, J. Cao, Y. Zhang.** A flexible payment scheme and its role-based access control. *IEEE Transactions on Knowledge and Data Engineering*, 2005, Vol. 17, No. 3, 425–436.

[24] **H. Oros, C. Popescu.** A Secure and Efficient Off-line Electronic Payment System for Wireless Networks. *International Journal of Computers, Communications & Control*, 2010, Vol. 5, No. 4, 551–557.

Received August 2012.