Research Article

Journal of Algorithms & Computational Technology

Journal of Algorithms & Computational Technology
0(0) 1–7

DOI: 10.1177/1748301817727123
journals.sagepub.com/home/act

SAGE

A fair electronic payment system for digital content using elliptic curve cryptography

Baoyuan Kang, Dongyang Shao and Jiaqiang Wang

Abstract

With rapid development of information and communication technologies purchasing digital content through the Internet has been greatly increased. Therefore, secure and fair electronic payment systems are important issue. To reduce system computational, communication and storage costs in many existing electronic schemes, Yang et al. recently proposed a novel electronic payment system based on authenticated encryption technology. But, Chaudhry et al. showed that Yang et al.'s electronic payment system is vulnerable to impersonation attack. Furthermore, Chaudhry et al. proposed improved electronic payment system. But, in this paper we point that Chaudhry et al.'s improved electronic payment system does not satisfy anonymity and fairness properties and the dispute resolution means in Chaudhry et al.'s electronic payment system are not effective. Furthermore, combining authenticated encryption and verifiably encrypted signatures technologies, we propose an improvement on Chaudhry et al.'s electronic payment system. Compared with Chaudhry et al.'s electronic payment system, the major changes of the proposed electronic payment system are in exchange phase. In this phase the private key and public key of the user are not needed, and the user generates verifiably encrypted signatures on his payment voucher. These changes guarantee the user anonymity, eliminate the advantages of the merchant, ensure the fairness of the payment system and the effectiveness of the dispute resolution phase. We also give the comparisons of proposed electronic payment system with some existing electronic payment systems.

Keywords

Electronic payment, fair exchange, anonymity, digital content, cryptography

Date received: 6 April 2017; revised: 28 June 2017; accepted: 29 July 2017

Introduction

In recent years, with rapid development of information and communication technologies purchasing digital content such as images, audio, and video through the Internet has been greatly increased. Therefore, secure electronic payment schemes as an integral part of any electronic commerce system are important for digital content transactions over the internet. After the first anonymous electronic payment scheme proposed by Chaum[1] many payment schemes were proposed.[2–16]

In a typical electronic payment scheme there are three participants: a user, a merchant, and a bank. Before one transaction, the user and the merchant must register with the bank, and open their account to benefit electronic payment. When the user wants to buy digital goods from the merchant, the user first gets a payment voucher (e-cash) from the bank. Then, he pays the payment voucher to the merchant. After verifying the validity of the payment voucher, the merchant sends the goods to the user, and sends the payment voucher to the bank, and the bank transfers money to the merchant's account. A secure well-designed electronic payment system should ensure the user's anonymity, fair exchange, and dispute resolution. The anonymity ensures the user's identity and purchasing information are confidential to the merchant and the bank, respectively. Fair exchange provides the guarantee that none of the participant has unfair advantage. To resolve the dispute caused by some participant who

School of Computer Science and Software, Tianjin Polytechnic University, Tianjin, China

Corresponding author:
Baoyuan Kang, School of Computer Science and Software, Tianjin Polytechnic University, Tianjin 300387, China.
Email: baoyuankang@aliyun.com

does not execute some terms of the protocol, a trusted third party (TTP) is needed in the payment system.

Recently, to reduce system computational, communication and storage costs in many existing electronic payment schemes, for resource constrained environments Yang et al.[17] proposed a novel authenticated encryption scheme and an electronic payment system based on their authenticated encryption scheme. But, Chaudhry et al.[18] and Heydari et al.[19] cryptanalyzed Yang et al.'s authenticated encryption scheme and electronic payment system and showed both to be vulnerable to impersonation attack. An adversary just having the knowledge of public parameters can impersonate as a legitimate user. The attacker can easily exploit the weakness of Yang et al.'s electronic payment scheme and can fraudulently purchase digital contents by deceiving the bank and merchant. Furthermore, Chaudhry et al.[18] improved both Yang et al.'s authenticated encryption scheme and electronic payment system. Chaudhry et al. claimed that the improved electronic payment system ensures robustness against all known attacks, while reducing about 66% computation cost on user side as compared to Yang et al.'s electronic payment scheme, and the improved electronic payment system is more suitable for resource constrained environments. But, in this paper we point that Chaudhry et al.'s electronic payment system does not satisfy the basic anonymity and fairness properties, and the dispute resolution means in Chaudhry et al.'s electronic payment system are not effective.

To contribute an anonymous and fair electronic payment system for digital contents, this paper, combining authenticated encryption and verifiably encrypted signatures technologies,[20] proposes an improved electronic payment system. Furthermore, the comparisons of security and computation cost of proposed electronic payment system with some existing electronic payment systems are given.

The remainder of this paper is organized as follows. Next section reviews Chaudhry et al.'s electronic payment system. Shortcomings of Chaudhry et al.'s electronic payment system are shown in ''Shortcomings of Chaudhry et al.'s electronic payment system'' section. ''The proposed scheme'' section proposes an improved fair electronic payment system. Security analysis is covered in ''Security analysis of the proposed electronic payment system'' section. The comparisons of security and computation cost are shown in ''Comparisons'' section. Finally conclusions are given in ''Conclusion'' section.

Brief review of Chaudhry et al.'s electronic payment system

Chaudhry et al.'s electronic payment system consists of six phases: initialization phase, buying phase, paying phase, exchange phase, transferring phase, and dispute resolution phase.

Initialization phase

During this phase, system selects finite field F_P over a large prime $p \geq 2^{160}$ and an elliptic curve $E_P(a, b)$. Further it selects a base point P in $E_P(a, b)$ and symmetric key algorithm $E_k(\cdot)/D_k(\cdot)$. Each legal participant with identity ID_i chooses his private key d_i and computes his public key $Y_i = d_iP$. Finally system parameters and each participant's public key are published, while each participant keeps his private key secret.

Buying phase

This phase starts when a legal user U wants to purchase some electronic goods. Initially U downloads the goods information (GI) from the merchant M's website. Then U selects a random number $r \in Z_p$, and computes

$$R = r(d_U + T_1)^{-1} \quad \text{and} \quad K = rY_b = (k_x, k_y)$$

Here T_1 is time stamp. Further U accumulates the goods price $p = \sum_{i=1}^{n} price_i$ and generates payment text $m = H(GI||p||ID_b)$. Finally U generates

$$C_1 = E_{k_x}(ID_u||m||p||k_x||T_1)$$

and sends the tuple (C_1, R, T_1) to the bank B.

Paying phase

Upon receiving the authenticated encrypted message tuple (C_1, R, T_1), the bank B, first computes $K = R(Y_u + T_1P)d_b = (k_x, k_y)$ then use k_x to compute $(ID_u||m||p||k_x||T_1) = D_{k_x}(C_1)$. Further B checks the validity of time stamp T_1 and verifies whether k_x is same as found after decryption of C_1. B accepts the message if both T_1 and k_x are valid. Otherwise rejects the message. Further B deducts the money amounting p from U's account and transfers p into a temporary account. B selects an expiry date E and computes $M = m||E$. Further B creates M's digital signature DS based on elliptic curve cryptography. Finally, B computes and sends $C_2 = E_{k_x}(DS||E||k_x|T_2)$ to U and stores (DS, M) in his database.

Exchange phase

The exchange phase consists of following three steps:

Step 1: After receiving encrypted message, U first decrypts C_2 to obtain DS and expiry date E. Then U selects $r' \in Z_p$, and computes

$$R' = r'(d_u + T_3)^{-1}, K = r' Y_m = (k'_x, k'_y),$$
$$C_3 = E_{k_x}(ID_b||DS||E||GI||k'_x||T_3)$$

Finally U sends (C_3, R', T_3) to M.

Step 2: Upon receiving (C_3, R', T_3), M computes

$$K = R'(Y_u + T_3 P)d_m = (k'_x, k'_y)$$

then decrypts C_3 using k'_x decryption key. Then M verifies validity of T_3 and k'_x if both are valid, M computes p and $m = H(GI||p||ID_b)$. Further M calculates $M = m||E$ and verifies the signature DS by using B's public key. If DS is not valid M aborts the session. Otherwise, M computes and sends $C_4 = E_{k'_x}(\textit{Electronic goods})$ to U.

Step 3: U decrypts C_4 to acquire electronic goods.

Transferring phase

M sends the payment proof to B before expiry date. U is having the facility to ask B to terminate the transaction if he did not receive the goods, in that case B transfers back the money from temporary account to U's account. After expiry date B transfers the money to M's account and removes $\{DS, M\}$ from his database.

Dispute resolution phase

If user does not get the desired product or merchant do not get the correct payment voucher then they can initiate dispute resolution phase. A TTP is responsible for resolving the dispute, in either cases TTP will be given the merchant's private key to verify the correctness of key k'_x. TTP after getting message (C_3, R', T_3) can verify legality of customer by computing following

$$K' = R'(Y_u + T_3 P)d_m$$
$$= (k'_x, k'_y), (ID_b||DS||E||GI||k'_x||T_3) = D_{k'_x}(C_3)$$

TTP compares T_3 received in plain text and got after decryption. Similarly TTP compares k'_x computed in first equation given above and decrypted in second equation given above, if both are equal the customer and merchant both are legal. TTP can further verify the encrypted digital signature DS and product's information. Hence TTP can resolve the dispute among both customer and merchant.

Shortcomings of Chaudhry et al.'s electronic payment system

In this section, we discuss how Chaudhry et al.'s electronic payment system is subjected to the following three attacks.

The system cannot ensure user anonymity

In the exchange phase of Chaudhry et al.'s electronic payment system, in step 2 when the merchant M computes $K = R'(Y_u + T_3 P)d_m = (k'_x, k'_y)$, the user U's public key Y_u is needed. So, in step 1 the message (C_3, R', T_3) should be rewritten into (ID_u, C_3, R', T_3). Then the identity of the user must be exposed to the merchant. Chaudhry et al.'s electronic payment system does not satisfy the important anonymity property for electronic payment system.

The system does not satisfy the fairness property

The fairness property is an important property for digital content electronic payment system. In exchange phase of Chaudhry et al.'s electronic payment system, once the user sends (C_3, R', T_3) to the merchant, the merchant can get the payment voucher from decrypting C_3 without sending electronic goods to the user. So, Chaudhry et al.'s electronic payment system is advantageous to the merchant, the user faces the risk of paying payment voucher to the merchant, but not getting the goods.

In the dispute resolution phase, TTP cannot effectively resolve the dispute among both customer and merchant

In the dispute resolution phase of Chaudhry et al.'s electronic payment system, the authors claimed that if the user does not get the desired product or the merchant does not get the correct payment voucher then they can beg TTP to resolve the dispute. Firstly, to resolve the dispute, TTP must get the merchant's private key. It is an obvious regrettable thing to expose private key for the merchant. Secondly, after obtaining the merchant's private key TTP must do lots of computation to verify if the customer and merchant are legal. Then TTP verifies the validity of the payment poof generated by the bank. This is clearly not an ideal dispute resolution means.

The proposed scheme

In this section, combining authenticated encryption and verifiably encrypted signatures technologies, we will improve Chaudhry et al.'s electronic payment system and propose a fair electronic payment system for digital content. In the proposed system, there are four participants: a user, a merchant, a bank, and a TTP. The proposed scheme consists of six phases: initialization phase, buying phase, paying phase, exchange phase, transferring phases, and dispute resolution phase. When the user wants to buy digital content from the merchant, he first asks a payment voucher

from the bank. Then, the user generates a verifiably encrypted signature of the payment voucher and sends the verifiably encrypted signature to the merchant. After verifying the validity of the verifiably encrypted signature, the merchant sends the digital content to the user. After receiving the digital content, the user sends the payment voucher to the merchant. Before expiry date the merchant sends the payment voucher to the bank, and the bank transfers the money to the merchant's account. If there is a dispute between the user and the merchant in one transaction, they can initiate dispute resolution phase to ask TTP to resolve the dispute.

Compared with Chaudhry et al.'s electronic payment system, the major changes of the proposed electronic payment system are in exchange phase. In step 1 the private key of the user is not needed. So, in step 2 the public key of the user is not needed for the merchant's computation. Also in step 1 the user generates the verifiably encrypted signature on the payment voucher, and sends the verifiably encrypted signature instead of payment voucher itself to the merchant. These changes guarantee the user anonymity, eliminate the advantages of the merchant, ensure the effectiveness of the dispute resolution phase, and the fairness of the payment system.

Following is the detailed description of the proposed system.

Initialization phase

During this phase, system selects finite field F_P over a large prime $p \geq 2^{160}$ and an elliptic curve $E_P(a, b)$. Further it selects a base point P in $E_P(a, b)$ and symmetric key algorithm $E_k(\cdot)/D_k(\cdot)$, each participant with identity ID_i chooses his private key d_i, and computes his public key $Y_i = d_i P$. Finally system parameters and each participant's public key are published, while each participant keeps his private key secret. The user and the merchant must register with the bank, and open their account to benefit electronic payment.

Buying phase

This phase starts when a legal user U wants to purchase some electronic goods. Initially U downloads GI from merchant M's website. Then U selects a random number $r \in Z_q$, and computes $R = r(d_U + T_1)^{-1}$ and $K = rY_b = (k_x, k_y)$. Here T_1 is time stamp. Further U accumulates the goods price $p = \sum_{i=1}^{n} price_i$ and generates payment text $m = H(GI||p||ID_b)$. Finally U generates

$$C_1 = E_{k_x}(ID_u||m||p||k_x||T_1)$$

and sends the tuple (ID_u, C_1, R, T_1) to the bank B.

Paying phase

Upon receiving the authenticated encrypted message tuple (ID_u, C_1, R, T_1), the bank B, first computes $K = R(Y_u + T_1 P)d_b = (k_x, k_y)$ then uses k_x to compute $(ID_u||m||p||k_x||T_1) = D_{k_x}(C_1)$. Further B checks the validity of time stamp T_1 and verifies whether k_x is same as found after decryption of C_1. B accepts the message if both T_1 and k_x are valid. Otherwise rejects the message. Further B deducts the money amounting p from U's account and transfers p into a temporary account. B selects an expiry date E and computes $M = m||E$. Further B creates M's digital signature DS based on elliptic curve cryptography. Finally, B computes and sends $C_2 = E_{k_x}(DS||E||k_x|T_2)$ to U and stores (DS, M) in his database. Here T_2 is time stamp.

Exchange phase

The exchange phase consists of following four steps:

Step 1: U after receiving encrypted message, first decrypts C_2 to obtain DS and expiry date E. Then U selects $r', z \in Z_q$, and computes $R' = r'P$, $Z = zP$ $K' = r'Y_m = (k'_x, k'_y)$, $C_3 = E_{k'_x}(ID_b||DS'||E||GI||k'_x||T_3)$. Here DS' is a verifiably encrypted signature generated by using random number z, TTP's public key and the payment voucher DS, T_3 is time stamp. Finally U sends (C_3, Z, R', T_3) to M.

Step 2: Upon receiving (C_3, Z, R', T_3), M computes $K' = d_m R' = (k'_x, k'_y)$, then decrypts C_3 using k'_x decryption key. Then M verifies validity of T_3 and k'_x if both are valid, M computes p and $m = H(GI||p||ID_b)$. Further M calculates $M = m||E$ and verifies the verifiably encrypted signature DS' by using B's public key, TTP's public key, M and Z. If DS' is not valid M aborts the session. Otherwise, M computes and sends $C_4 = E_{k'_x}(Electronic\ goods)$ to U.

Step 3: U decrypts C_4 to acquire electronic goods, and sends $C_5 = E_{k'_x}(DS)$ to M.

Step 4: M decrypts C_5 to acquire the payment voucher DS and verify it.

Transferring phase

M sends the payment voucher DS to B before expiry date. If B can find $\{DS, M\}$ in his database B transfers the money in the temporary account to M's account and removes $\{DS, M\}$ from his database.

Dispute resolution phase

If the merchant does not get the correct payment voucher DS after he sends the electronic goods to the user, the merchant can initiate dispute resolution phase. He can show $(DS', \textit{Electronic goods}, GI, T_3, Z, E)$ to TTP. TTP computes $p = \sum_{i=1}^{n} price_i$, $m = H(GI||p||ID_b)$, $M = m||E$, and verifies DS'. If DS' is valid, TTP will compute DS from DS' using his private key, then give DS to the merchant and keeps (DS, *Electronic goods*) in his database.

If the user does not get the *Electronic goods* after he sends DS' to the merchant, the user can initiate dispute resolution phase. The user can show DS to TTP. If TTP can find $(DS, \textit{Electronic goods})$ in his database, TTP give *Electronic goods* to the user. Otherwise, TTP rejects the user's appeal.

Security analysis of the proposed electronic payment system

As Chaudhry et al.'s electronic payment system, the proposed electronic payment system ensures mutual authentication, confidentiality, integrity, resists replay attack, and double spending attack.

In the proposed electronic payment system all important messages transmitted include time stamps which in encrypted part cannot be altered by any adversary. So, the proposed electronic payment system can resist replay attack. In the proposed electronic payment system the user U sends GI protected by one hash function to the bank, and the digital signature DS does not reveal the user's information. Therefore, the proposed system protects the user's buying privacy. Once the payment is transferred to merchant's account, the bank deletes the signature DS. So, DS can be used only once, the proposed electronic payment system prevents double spending of same payment voucher.

In this section, to aim at the shortcomings of Chaudhry et al.'s electronic payment system, we deal mainly with the anonymity and fairness of the proposed electronic payment system.

Anonymity

In the exchange phase, the user can securely communicate with the merchant by selecting a random number r' and generating share key $r'Y_m$ without using his private key and no user's identity and public key be known by the merchant. So, the user's identity is anonymous to the merchant. Since the bank only keeps (DS, M) in his database, DS and M are irrelevant to the user's identity. So, in transferring phase, the bank cannot trace the user who drew DS from the bank. Therefore, the user's identity is also anonymous to the bank in transferring phase.

Table 1. Comparison of security features of our scheme with other schemes.[17–19]

	F1	F2	F3	F4	F5
Yang et al.[17]	Yes	Yes-	No	Yes	No
Chaudhry et al.[18]	No-	Yes-	Yes	Yes	No
Heydari et al.[19]	No	Yes	Yes	Yes	No
Ours	Yes	Yes	Yes	Yes	Yes

F1: anonymity; F2: replay attack; F3: impersonation attack; F4: double spending detection; F5: fairness.

Fairness issue

In the step 1 of the exchange phase, the user does not send the payment voucher DS to the merchant, the merchant only get the verifiably encrypted signature DS' on DS. In the step 2, when the merchant verifies that DS' is valid, the merchant sends *Electronic goods* to the user. If the user does not execute the step 3, the merchant can get the payment voucher DS in dispute resolution phase. If in step 1 after getting DS' the merchant does not executes the step 2, the user also can ask TTP to check whether there is a record (DS, *Electronic goods*) in TTP's database. If there is no record (DS, *Electronic goods*), it indicates that the merchant does not get DS. The user also cannot get *Electronic goods*. If there is the record (DS, *Electronic goods*), it indicates that the merchant gets DS by TTP. So, TTP can give *Electronic goods* to the user. Therefore, the electronic payment system is fair to both the user and the merchant.

Comparisons

In this section the comparisons of the proposed electronic payment system with some existing electronic payment systems[17–19] are given. The security comparison is shown in Table 1, and the comparison of computation cost in major three phases of each electronic payment system is shown in Table 2.

Table 2. Comparison of computation cost.

	P1	P2	P3
Yang et al.[17]	3L + H + E	L + E + D + S	4L + H + 2E + 3D + V
Chaudhry et al.[18]	M + I + L + H + E	L + E + D + S	2M + I + 2L + H + 2E + 3D + V
Heydari et al.[19]	M + I + L + H + E	L + E + D + S	2M + I + 2L + H + 2E + 3D + V
Ours	M + I + L + H + E	L + E + D + S	4L + H + 3E + 4D + S + V

P1: buying phase; P2: paying phase; P3: exchanging phase, M: multiplication operation; I: inverse operation; L: scalar multiplication; H: hash computation; E: encryption operation; D: decryption operation; S: signature operation; V: signature verification operation.

In the security comparison, the proposed system is more secure than the three electronic payment systems.[17–19] In comparison of computation cost with Yang et al.[17] in exchanging phase, there are more one signature operation, one encryption operation, and one decryption operation in the proposed electronic payment system. Compared with Chaudhry et al.[18] and Heydari et al.,[19] in exchanging phase there are more two scalar multiplication operation, one signature operation, one encryption operation, one decryption operation and few two multiplication operation and one inverse operation in the proposed electronic payment system. The computation cost of the proposed electronic payment system is slightly higher. But, the proposed electronic payment system is more secure.

Conclusion

In this paper we point that Chaudhry et al.'s electronic payment system does not satisfy the anonymity and fairness properties and the dispute resolution means in Chaudhry et al.'s electronic payment system are not effective. Furthermore, based on verifiably encrypted signatures technique, this paper proposes an improved electronic payment system and compares the security and computation cost of the proposed electronic payment system with some existing electronic payment systems. The proposed system is more secure and suitable for resource constrained environments.

Acknowledgement

We would like to thank the reviewers for their helpful comments.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: the Applied Basic and Advanced Technology Research Programs of Tianjin (No. 15JCYBJC15900).

References

1. Chaum D. Blind signatures for untraceable payments. In: *Crypto 82*. New York, NY: Plenum Press, 1983, pp.199–203.
2. Luo J, Yang M and Huang S. An unlinkable anonymous payment scheme based on near field communication. *Comput Electr Eng* 2016; 49: 198–206.
3. Yang J and Lin P. A mobile payment mechanism with anonymity for cloud computing. *J Syst Software* 2016; 116: 69–74.
4. Li W, Wen Q, Su Q, et al. An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Comput Commun* 2012; 35: 188–195.
5. Chen C and Liao J. A fair online payment system for digital content via subliminal channel. *Electron Commerce Res Appl* 2011; 10: 279–287.
6. Lin S and Liu D. An incentive-based electronic payment scheme for digital content transactions over the internet. *J Network Comput Appl* 2009; 32: 589–598.
7. Isaac J and Zeadally S. An anonymous secure payment protocol in a payment gateway centric model. *Program Comput Sci* 2012; 10: 758–765.
8. Pourghomi P, Saeed M and Ghinea G. A secure cloud-based NFC mobile payment protocol. *Int J Adv Comput Sci Appl* 2014; 5: 24–31.
9. Wang J, Liu J, Li X, et al. Fair e-payment protocol based on blind signature. *J China Univ Posts Telecommun* 2009; 16: 114–118.
10. Fan C, Huang V and Yu Y. User efficient recoverable off-line e-cash with fast anonymity revoking. *Math Comput Modell* 2013; 58: 227–237.
11. Juang W. Ro-cash: an efficient and practical recoverable pre-paid off-line e-cash scheme using bilinear pairings. *J Syst Software* 2010; 83: 638–645.
12. Zhang L. Provably-secure electronic cash based on certificateless partially-blind signatures. *Electron Commerce Res Appl* 2011; 10: 545–552.
13. Chen YL, Chou JS, Sun HM, et al. A novel electronic cash system with trustee-based anonymity revocation from pairing. *Electron Commerce Res Appl* 2011; 10: 673–682.

14. Kang B and Xu D. Secure electronic cash scheme with anonymity revocation. *Mobile Inf Syst* 2016; 2016: Article ID 2620141, 10 p..
15. Kang B and Xu D. An untraceable off-line electronic cash scheme without merchant frauds. *Int J Hybrid Inf Technol* 2016; 9: 431–442.
16. Kang B, Wang M and Jing D. An off-line payment scheme for digital content via subliminal channel. *J Inf Sci Eng*,http://journal.iis.sinica.edu.tw/paper/1/160155-2.pdf?cd = C1EF7D1B861006BEC.
17. Yang J-H, Chang Y-F and Chen Y-H. An efficient authenticated encryption scheme based on ECC and its application for electronic payment. *Inf Technol Control* 2013; 42: 315–324.
18. Chaudhry S-A, Farash M-S, Naqvi H, et al. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. *Electron Commerce Res* 2016; 16: 113–139.
19. Heydari M, Sadough S, Chaudhry S-A, et al. An improved authenticated scheme for electronic payment systems in global mobility networks. *Inf Technol Control* 2015; 44: 387–403.
20. Kang B. New types of verifiably encrypted signature schemes. *Adv Mater Res* 2012; 490–495: 914–918.