International Journal of Engineering Research And Management (IJERM)
ISSN: 2349- 2058, Volume-04, Issue-09, September 2017

Improved Incentive-Based Electronic Payment Scheme for Digital Content

Baoyuan Kang, Dongyang Shao, Jiaqiang Wang

Abstract— **In recent years, more and more people have been purchasing digital contents through e-commerce. Under this circumstance, anonymous and fair electronic payment schemes are important issue. Recently, Lin et al. proposed an incentive-based electronic payment scheme for digital content transactions over the Internet. They claimed that their scheme can ensure the properties of fair exchange and customer anonymity and encourage authors to create digital contents by apportioning sales revenues immediately to payees when customers complete payments. But in this paper, we show that their scheme is not fair. In their scheme malicious customers may successfully get the digital contents, but merchants and the authors of digital content cannot timely get sale revenue. Furthermore, based on Lin et al.'s scheme, this paper proposes an improved scheme. In improved scheme neither the customer no the merchant has priority. So, the improved is a fair scheme for incentive-based electronic payment of digital content transactions over the Internet.**

Index Terms— **Electronic Payment; Fair Exchange; Anonymity; Digital Content; Cryptography**

I. INTRODUCTION

Digital contents are commercial products that are available in digital form. In recent years, more and more people have been purchasing digital content such as images, audio, and video through the Internet. Under this circumstance, better security and fair anonymous electronic payment schemes are important issue for digital content transactions over the Internet. In 1982, Chaum [1] proposed the concept of anonymous electronic payment. Since then, Fair and anonymous electronic payment schemes have been investigated by many researchers [2-9]. A fair payment protocol allows two parties to exchanging items so that either both parties obtain the exchange items or neither party does.

High-quality digital contents always need a lot of authors having motivation to create. Authors will obtain more incentive to improve their motivation on creating digital contents by means of shortening the time period of apportioning sales revenue. Based on above thinking, Lin et al. [6] proposed an incentive-based electronic payment scheme for digital content transactions over the Internet. Lin et al.'s scheme is a kind of multiple payees' electronic payment scheme [10]. Nevertheless, multiple payees' electronic payment scheme has seldom been proposed in the literature. There is much less the incentive-based electronic payment scheme for digital content transactions scheme. So, discussion of Lin et al.'s scheme is valuable.

There are five participants in Lin et al.'s scheme: a bank (P_B), a merchant (P_M), a customer (P_C), a trusted third party (P_{TTP}), and authors of digital contents. It is said that the scheme can ensure both important properties of fair exchange and customer anonymity and encourage motivation of authors to create digital contents by apportioning sales revenues immediately to payees when customers complete payments. And when a disputation occurs, participants can request the trusted third party to arbitrate unfair behaviors. Such as, if the merchant P_M sends the purchased digital content and the product certificate to the customer P_C, but P_C does not reply the unencrypted serial number of electronic cash, P_M can request the trusted third party P_{TTP} to arbitrate the P_C's misbehavior. In this case, P_{TTP} can decrypt the encrypted serial number and then replies the unencrypted serial number to P_M. However, this paper points out that in this case, due to P_C's intended misbehavior, the P_{TTP} cannot get the right serial number m of the electronic cash. So, Lin et al.'s scheme is not fair for incentive purpose.

To contribute a fair incentive-based electronic payment schemes for digital content transactions over the Internet, based on Lin et al.'s scheme, this paper propose an improved scheme. The improved scheme modifies some steps of initializing phase, purchasing phase and arbitrating phase in Lin et al.'s scheme, and add two steps in purchasing phase. In improved scheme neither the customer no the merchant has priority. So, the improved is fair and secure scheme for incentive-based electronic payment of digital content transactions over the Internet.

The remainder of this paper is organized as follows. Section 2 reviews Lin et al.'s scheme and points out its shortcoming. Section 3 proposes an improvement of Lin et al.'s scheme. Security analysis of the improved scheme is covered in Section 4. Finally conclusions are given in Section 5.

II. LIN ET AL.'S SCHEME AND ITS SHORTCOMING

2.1. Lin et al.'s scheme

There are five types of participants in Lin et al.'s scheme [6]: a bank (P_B), a merchant (P_M), a customer (P_C), a trusted third party (P_{TTP}). Lin et al.' scheme consists of four phases ：initializing, withdrawing, purchasing，and arbitrating phases.

Manuscript received Sep 12, 2017

Baoyuan Kang, School of Computer science and software, Tianjin polytechnic university, Tianjin, 300387, China
Dongyang Shao, School of Computer science and software Tianjin polytechnic university, Tianjin, 300387, China
Jiaqiang Wang, School of Computer science and software Tianjin polytechnic university, Tianjin, 300387, China

- Initializing phase：

  I1. P_M、P_B、P_{TTP} and all authors $(P_{A1}, P_{A2}, \cdots, P_{Ap})$ generate their own public key pk_i and private key sk_i sk$_i$ by the RSA cryptosystem, and then register their public key to the certificate authority(CA).

  I2. P_B publishes a one-way hash function $H()$

  I3. When p authors create a digital content together, they acquire the product number pid from P_M. There are $p+1$ payees, p authors，and a merchant，for this digital content DC_{pid}

  I4. Payees negotiate AC_{pid} for DC_{pid} with each other. The AC_{pid} will be signed by $p+1$ payees to form the multisignature MS_{pid} . Subsequently, the representative of payees submits pid，AC_{pid} and MS_{pid} to P_B . After verifying the validity of MS_{pid}，P_B keeps these information

  I5. P_M registers the digital content DC_{pid} to P_{TTP} for selling purpose by sending pid，$desc_{pid}$，AC_{pid}，MS_{pid} and DC_{pid} to P_{TTP} . P_{TTP} checks the correctness of MS_{pid} based on payees' public keys and checks DC_{pid} based on pid and $desc_{pid}$, and then computes and keeps the certificate $Cert_{pid}$ in its database and issues $Cert_{pid}$ to P_M . P_{TTP} only needs to certify DC_{pid} to P_M once, then P_M can sell DC_{pid} for as many times as P_M can without any involvement of P_{TTP}

- .Withdrawing phase：P_C browses P_M 's webpage and obtains pid and *price* of a digital content that she/he would like to purchase.

  W1. P_C and P_B establish a secure channel and obtain a session key sek_{CB} . And then，P_C logins P_B 's banking service

  W2. P_C prepares v and submits $E_{sek_{CB}}(v)$ to P_B

  W3. P_B checks v . If P_C 's account has enough amount of money, P_B randomly chooses its randonmizing factor $x \in Z^*_{n_B}$ and replies $E_{sek_{CB}}(y)$ to P_C where $y = x^{e_B} \bmod n_B$. The integer y is the commitment of P_B 's randomizing factor

  W4. After receiving $E_{sek_{CB}}(y)$, P_C randomly chooses a random message m , which represents the serial number of electronic cash, a randomizing factor $u \in Z^*_{n_B}$ and a blinding factor $r \in Z^*_{n_B}$. P_C computes the blinded message $\alpha = r^{e_B} \times u \times H(m', (u^{e_B} y) \bmod n_B) \bmod n_B$ where $m' = E_{pk_{TTP}}(m)$,and then sends $E_{sek_{CB}}(\alpha)$ to P_B.

  W5. After receiving $E_{sek_{CB}}(\alpha)$, P_B debits the denomination of electronic cash in v from P_C 's account. P_B injects its x into α and computes the blinded signature $t = ((\alpha \times x)^{d_B \tau(v)})^{-1} \bmod n_B$ using its private key sk_B , where the message $(\alpha \times x)$ is determined by both P_C and P_B . P_B then replies $E_{sek_{CB}}(t, x)$ to P_C

  W6. P_C computes $c = u \times x \bmod n_B$ and computes $s = r^{\tau(v)} \times t \bmod n_B$ to remove r from t . The message (s, m', v, c) denotes the electronic cash

- Purchasing phase: Customers are anonymous in this phase.

  P1. P_C and P_M establish a secure channel and obtain a session key sek_{CM} . P_C also gets a system-wide transaction number tn from P_M

  P2. P_C sends $E_{SEK_{CM}}(tn, pid, (s, m', v, c))$ to P_M . In this step, P_C starts her/his timer of the purchasing phase

  P3. P_M verifies (s, m', v, c) through $s^{e_B}(H(m', (c^{e_B} \bmod \mathrm{n}_B))c)^{\tau(v)} \equiv 1 \bmod n_B$ and checks whether pid received from step P2 is the same as pid in v and the denomination in v is equal to the price of the purchased digital content DC_{pid} or not. If P_M 's verification and check are all passed, P_M forwards $E_{pk_B}(tn, P_M, Veri, (s, m', v, c), Sign_{M1})$ to P_B . Where $Veri$ means that P_B requests P_B to verify *(s, m', v, c)* and $Sign_{M1} = E_{pk_B}(H(tn, P_M, Veri, (s, m', v, c)))$ is P_M ' signature. In this step, P_M starts her/his timer of the purchasing phase.

  P4. P_B verifies *(s, m', v, c)* through $s^{e_B}(H(m', (c^{e_B} \bmod \mathrm{n}_B))c)^{\tau(v)} \equiv 1 \bmod n_B$ and makes double-spending check. If above verification are all passed, P_B keeps (tn , P_M , (s, m', v, c)) in its database with a certain period of Time T. And then P_B acknowledges P_M the message $E_{pk_M}(tn, Vok, Sign_{B1})$ in which Vok means the verification of *(s, m', v, c)* is passed. $Sign_{B1} = E_{sk_B}(H(tn, Vok))$ is P_B 's signature.

P5. If the verification of (*s, m', v, c*) in step P4 is passed, P_M sends $E_{sek_{CM}}(tn, Cert_{pid}, DC_{pid})$ to P_C within the reasonable time period T. Otherwise, P_C can inquire P_{TTP} about the transaction tn through the serial number of electronic cash m.

P6. P_C verifies the validity of $Cert_{pid}$ using P_{TTP}'s public key . If $Cert_{pid}$ is valid, P_C computes $H(DC_{pid})$ and checks whether it is equal to the $H(DC_{pid})$ in $Cert_{pid}$. If the check is passed, P_C sends $E_{sek_{CM}}(tn, m)$ to P_M

P7 P_M sends $E_{pk_B}(tn, P_M, Depo, (s, m, v, c), Sign_{M2})$ to P_B where Depo means that P_M request P_B to redeem (s, m', v, c) kept by P_B in step P4 and $Sign_{M2} = E_{sk_M}(H(tn, P_M, Depo, (s, m, v, c)))$ is P_M's signature. P_B checks (*s, m', v ,c*) through $s^{e_B}(H(E_{pk_{TTP}}(m), (c^{e_B} \bmod n_B))c)^{\tau(v)} \equiv 1 \bmod n_B$. If the equation is hold, P_B apportions the denomination of (s, m', v, c) to payees' account according to AC_{pid} , and then P_B appends m to the record (*tn*, P_M ,(*s, m', v, c*)) in its database.

P8. After P_B apportions the denomination of (s, m', v, c) to payees' accounts, P_B replies $E_{pk_M}(tn, Dok, Sign_{B2})$ to P_M , where Dok indicates the denomination of P_C's electronic cash had been apportioned, and $Sign_{B2} = E_{sk_B}(H(tn, Dok))$ is P_B's signature.

- Arbitrating phase: After P_M sends $(tn, Cert_{pid}, DC_{pid})$ to P_C in step P5, if P_C does not sends (tn, m) to P_M in step 6 within the reasonable time period T or P_C sends $m''(\neq m)$ to P_M and then P_B detects an error in step P7 and replies an error message in step P8, P_M can request P_{TTP} to recover the plaintext of m'.

  A1. P_M sends $E_{pk_{TTP}}(tn, P_M, (s, m', v, c), DC_{pid}, Sign_{M3})$ to P_{TTP} where $Sign_{M3} = E_{sk_M}(H(tn, P_M, (s, m', v, c), DC_{pid}))$ is P_M 's signature.

  A2. P_{TTP} verifies (s, m', v ,c) through $s^{e_B}(H(m', (c^{e_B} \bmod n_B))c)^{\tau(v)} \equiv 1 \bmod n_B$ .If the validity of (*s, m', v ,c*) is positive, P_{TTP} retrieves $Cert_{pid}$ from its database according to pid in *v*, and then computes $H(DC_{pid})$ and computes whether $H(DC_{pid})$ is equal to the $H(DC_{pid})$ in $Cert_{pid}$ or not . If above comparison is equal, P_{TTP} computes $E_{sk_{TTP}}(m')$ to get m and replies $E_{pk_M}(tn, m, Sign_{TTP})$ to P_M where $Sign_{TTP} = E_{sk_{TTP}}(H(tn, m))$ is P_{TTP}'s signature. P_{TTP} also keeps (m, DC_{pid}) for a certain period of time $2T$, and P_C can get DC_{pid} from P_{TTP} using m within the time period $2T$

.

2.2. The shortcoming of Lin et al.'s schem

The main shortcoming of Lin et al.'s scheme is it is unfair. In the fair exchange analyses of Lin et al.'s scheme, it is said that if P_C does not sends the serial number of electronic cash m , in step P6, P_M can request P_{TTP} to arbitrate P_C 's misbehavior through P_{TTP} decrypt m' using its private key to get m and reply m to P_M in Arbitrating phase. But, we find that the malicious P_C may use a m' being not equal to $E_{pk_{TTP}}(m)$ compute α in step w4. It is to say that m' may not be resulted from the encryption of m . Also, In the next steps of Lin et al.'s scheme, there is not the verification of $m' = E_{pk_{TTP}}(m)$. So, the malicious P_C 's misbehavior cannot be found until in step P7 P_B find it by verifying the equation $s^{e_B}(H(E_{pk_{TTP}}(m), (c^{e_B} \bmod n_B))c)^{\tau(v)} \equiv 1 \bmod n_B$. And when P_M send m' to P_{TTP} for arbitration, P_{TTP} cannot get the right m , because $m' \neq E_{pk_{TTP}}(m)$. So, the malicious P_C successfully get the digital content DC_{pid} and its certificate $Cert_{pid}$ in step p5, but P_M and the authors of digital content cannot timely get sale revenue. Thus, Lin et al.'s scheme is unfair. .

III. AN IMPROVED SCHEME

The improved scheme is modifying some steps of Lin et al.'s scheme. The rest is identical to Lin et al.'s scheme. The modification includes:

- In Initializing phase, modify I5 in Lin et al.'s scheme into steps I5'
- In Purchasing phase, modify step P5, P6 in Lin et al.'s scheme into steps P5', P6', respectively.
- In Purchasing phase, add P9, P10 steps.
- In Arbitrating phase, modify step A1, A2 in Lin et al.'s scheme into steps A1', A2', respectively

Following is the detailed description of steps I5', P5', P6', P9, P10, A1', A2'.

I5'. P_M registers the digital content DC_{pid} to P_{TTP} for selling purpose by sending pid , $desc_{pid}$, AC_{pid} , MS_{pid} and DC_{pid} to P_{TTP} . P_{TTP} checks the correctness of MS_{pid} based on payees' public keys and checks DC_{pid} based on pid and $desc_{pid}$, and then use pid , P_{TTP} 's private key, $H(DC_{pid})$ and $E_{pk_{TTP}}(DC_{pid})$ computes the certificate $Cert_{pid}$ and keeps DC_{pid} and $Cert_{pid}$ in its database and issues $Cert_{pid}$ to P_M . P_{TTP} only needs to certify DC_{pid} to P_M once, then P_M can sell DC_{pid} for as many times as P_M can without any involvement of P_{TTP}

P5'. If the verification of (s, m', v, c) in step P4 is passed, P_M sends $E_{sek_{CM}}(tn, Cert_{pid}, E_{pk_{TTP}}(DC_{pid}), H(DC_{pid}), Sign_M)$ to P_C within the reasonable time period T. Where $Sign_M = E_{sk_M}(H(tn, Cert_{pid}, E_{pk_{TTP}}(DC_{pid}), H(DC_{pid}))$. Otherwise, P_C can inquire P_{TTP} about the transaction tn through the serial number of electronic cash m .

P6'. P_C verifies the validity of $Sign_M$ and $Cert_{pid}$ using P_M 's public key. If $Cert_{pid}$ is valid, P_C sends $E_{sek_{CM}}(tn, m)$ to P_M .

P9. When P_M get $E_{pk_M}(tn, Dok, Sign_{B2})$ in step P8, P_M sends $E_{sek_{CM}}(tn, DC_{pid})$ to P_C .

P10. P_C computes $H(DC_{pid})$ and checks whether it is equal to the $H(DC_{pid})$ in $Cert_{pid}$. If the check is passed, P_C believes he gets right content from P_M . Otherwise, P_C can show $(tn, Cer_{pid}, E_{pk_{TTP}}(DC_{pid}), Sign_M)$ to P_{TTP} in arbitrating phase to request DC_{pid}

If after P_C sends $E_{sek_{CM}}(tn, m)$ to P_M in step p6', P_M does not send $E_{sek_{CM}}(tn, DC_{pid})$ to P_C in step P9 within the reasonable time period T, in arbitrating phase, P_C can request P_{TTP} to get digital content DC_{pid} .

A1'. P_C sends $E_{TTP}((tn, Cer_{pid}, E_{pk_{TTP}}(DC_{pid}), Sign_M))$ to P_{TTP}

A2'. P_{TTP} verifies the signature $Sign_M$. If the validity of $Sign_M$ is positive, P_{TTP} P_{TTP} computes $E_{sk_{TTP}}(E_{pk_{TTP}}(DC_{pid}))$ to get DC_{pid} and computes $H(DC_{pid})$ and checks whether it is equal to the $H(DC_{pid})$ in $Cert_{pid}$. If the check is passed, P_{TTP} replies DC_{pid} to P_C . If the check is not passed, P_{TTP} can check its database and get right DC_{pid} and send it to P_C .

IV. SECURITY ANALYSIS OF THE IMPROVED SCHEME

In this section, we analyse the security of the improved scheme on the following aspects.

Claim 1. P_C has no priority in getting DC_{pid} in the improved scheme

In step P5' P_C can only verify the validity of digital content DC_{pid} , P_C cannot get DC_{pid} from step P5'. In step P6' P_C sends m to P_M , but only when in step p8 P_M receives the information Dok indicating the denomination of P_C 's e-cash had been apportioned, P_M send DC_{pid} to P_C in step P9. So, in improved scheme the customer P_C has no priority in getting DC_{pid} .

Claim 2. P_M cannot cheat P_C in the improved scheme

In improved scheme, only when in step P5' P_C receive valid certificate $Cert_{pid}$ of DC_{pid} from P_M , P_C send m to P_M in step P6'. If in step P9 P_M does not send DC_{pid} to P_C , in arbitrating phase P_C can sends $E_{TTP}((tn, Cer_{pid}, E_{pk_{TTP}}(DC_{pid}), Sign_M))$ received in step P5' to P_{TTP} . After verification of the validity of the signature $Sign_M$, P_{TTP} computes $E_{sk_{TTP}}(E_{pk_{TTP}}(DC_{pid}))$ to get DC_{pid} and computes $H(DC_{pid})$ and checks whether it is equal to the $H(DC_{pid})$ in $Cert_{pid}$. If the check is passed, P_{TTP} replies DC_{pid} to P_C . If the check is not passed, P_{TTP} can check its database and get right DC_{pid} obtained in initializing phase I5'and send it to P_C .

Based on the above two claims, the improved scheme is fair incentive-based electronic payment scheme for digital content transactions over Internet.

CONCLUSION

In this paper, we show that Lin et al.'s incentive-based electronic payment scheme of digital content is not fair. In their scheme malicious customers may successfully get the digital contents, but merchants and the authors of digital content cannot timely get sale revenue. Furthermore, based on Lin et al.'s scheme, this paper proposes an improved scheme. In improved scheme neither the customer no the merchant has priority. So, the improved is a fair scheme for incentive-based electronic payment of digital content transactions over the Internet.

ACKNOWLEDGEMENTS

This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (No. 15JCYBJC15900).

REFERENCES

[1] Chaum, D. "Blind signatures for untraceable payments", In Crypto 82, Plenum Press, New York, 1983, 199-203.
[2] Luo, J., Yang, M. and Huang, S. "An unlinkable anonymous payment scheme based on near field communication", Computers and Electrical Engineering (2015) (in press)
[3] Yang, J., Lin, P., "A mobile payment mechanism with anonymity for cloud computing", The Journal of Systems and Software (2015) (in press)
[4] Li, W., Wen, Q., Su, Q. and Jin Z. "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network", Computer Communications 35 (2012) 188-195.
[5] Chen, C., Liao, J. "A fair online payment system for digital content via subliminal channel" Electronic Commerce Research and Applications 10 (2011) 279-287.
[6] Lin, S., Liu, D. "An incentive-based electronic payment scheme for digital content transactions over the internet" Journal of Network and Computer Applications 32 (2009) 589-598.
[7] Isaac, J., Zeadally, S. "An anonymous secure payment protocol in a payment gateway centric model", Pro. Comput. Sci. 10 (2), 2012, 758-765.
[8] Pourghomi, P., Saeed, M. and Ghinea, G. "A secure cloud-based NFC mobile payment protocol. Int. J. Adv. Comput. Sci. Appl. 5 (10) 2014, 24-31.
[9] Wang, J., Liu, J., Li, X. and Kou, W. "Fair e-payment protocol based on blind signature", The Journal of China Universities of Posts and Telecommunications 16(5) 2009, 114-118.
[10] Weyland, A., Staub, T. and Braun, T. "Comparison of motivation-based cooperation mechanisms for hybrid wireless networks, Comput. Commun., 2006,29(13-14): 2661-70.