Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5537965, 3 pages
https://doi.org/10.1155/2021/5537965

Research Article

Mobile, Divisible, and Safe E-Cash System

Ting Huang

College of Computer and Information Technology, China Three Gorges University, Yichang, Hubei 443002, China

Correspondence should be addressed to Ting Huang; 3451292652@qq.com

Received 6 January 2021; Revised 26 February 2021; Accepted 11 March 2021; Published 19 April 2021

Academic Editor: Mohammed Fattah

Mobile, divisible, and safe e-cash system adapts on mobile terminals for e-payment which can circulate in multiple banks. The usage of the divisible e-cash does not need pass bank, which the bank has not the bottleneck of e-business. The author's thesis discusses on the withdrawal protocol, payment protocol, transferable protocol, deposit protocol, and update of e-cash, based on elliptic curve cryptography (ECC).The system is simple, efficient, secure, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted. The system can protect from double spending, non-frameability, eavesdropping, tampering, and "perfect crime" effectively too. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks.

1. Introduction

With the development of science and technology and the progress of society, e-cash began to enter people's lives and gradually changed people's consumption concept and mode. Compared with the traditional paper money, e-cash has the advantages of fast transmission, wide coverage, and convenient use, which has replaced the paper money with an irreversible trend. But the e-cash systems use online payment nowadays. The usage of every e-cash system must pass the bank [1]; thus, the bank has turned into the bottleneck of the payment. The e-cash [2] only circulates in a single bank, which cannot meet the needs of reality. The e-cash system [3] based on RSA encryption algorithm problem which needs exponentiation compute. The e-cash [4] cannot be circulated in user's e-business. This paper researches on mobile, divisible, and safe e-cash system. The e-cash in this study is divisible, and the usage of the divisible e-cash system need not pass bank, which the bank has not the bottleneck of e-business. Meanwhile, the system can protect from double spending. ECC in this paper needs no exponentiation operation compared to RSA. The research effectively improves the efficiency and security of mobile e-cash system, which provides the theoretical basis and technical support for an electronic transaction system nowadays. In the system, the consumer can recover the lost money even if the phone has crashed and all the files are removed accidentally or the e-cash wallet has been lost. The e-cash in this study can circulate in all the banks, which can meet the needs of reality. The e-cash in this study can circulate in user's e-business, which circulates any time offline between the users before getting saved in the bank. In comparison with the protocol in [5], the proposed protocol can protect from eavesdropping, tampering, and "perfect crime" effectively too. The e-cash in this study and its signatures cannot be forgery. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks. The system is simple, efficient, secure, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted. The e-cash in the system has a usage period. When the usage period ends, the bank will delete the e-cash. Thus, the storage space of the bank is saved.

2. Design of Protocol

2.1. Withdrawal Protocol

(1) The user withdraws I yuan from the bank_m. He takes $a \in_R Z_n$ and then computes $\delta = H(a + SK_U)$. Next, he enters δ in the database, encrypts IDnU, δ, and ,I by the symmetric key, and sends them to the bank_m.

(2) The bank_m produces the e-cash: $\alpha_\text{I} = H[(ISK_{Bm1} + \delta SK_{Bm2})\|SK_{Bm}\|t_1\|b]$ and computes $\beta_I = H\ [(cG_x)\|\alpha_I\|t_1\|I]$, $\gamma_I = c + \beta_I \text{SK}_\text{Bm}$, and $b, c \in_R Z_n$. The bank_m enters $\alpha_\text{I}, b, \delta, t_1$, in the database, encrypts IDnU, I, α_I, β_I, γ_I, and t_1 and sends to the user.

(3) The user decrypts IDnU, I, α_I, β_I, γ_I, andt_1 and saves them to the database.

2.2. Payment Protocol. The user pays the e-cash to the merchant_0 by the credit center. First $\alpha_\text{i} = H(b_1\|t_2\|SK_U\|\alpha_I\|j\|i)$, $\beta_\text{i} = H[(c_1G)_x\|\alpha_i\|t_2\|j\|i]$, $\gamma_i = c_1 + \beta_i SK_U$, $b_1, c_1 \in Z_n$, $d, e_1, e_2 \in Z_n$, $d \neq 0$, $\varepsilon = H(\alpha_i)$, $\varepsilon_1 = dI\,D_{nU} - \varepsilon e_1$, $\varepsilon_2 = d - \varepsilon e_2$, α_i, β_i, γ_i, i, j, t_2, ε, ε_1,ε_2 are sent to the credit center. The e-cash cannot be used the next time. Then the credit center checks $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_U)\|\alpha_i\|t_2\|j\|i]$ and saves i, α_i, β_i, γ_i, ε, ε_1,ε_2. It gets $\varphi = H[i\|(SK_C PK_M)_x]$ and sends φ, NAU, and Timestamp to the merchant_0. The merchant_0 checks $\varphi \stackrel{?}{=} H[i\|(PK_C SK_M)_x]$ and then sends the goods to the user. The user receives the goods, gets $f = H[(SK_U PK_C)_x]$, deletesα_i, β_i, γ_i, i, and sends f, merchant's address, NAU, and timestamp to the credit center. The credit center checks $f \stackrel{?}{=} H[(SK_C PK_M)_x]$, comupters $\varphi\prime = H[i\|(SK_C PK_M)_x\|\alpha_i]$, and sends i, α_i, NAU, f, ε, ε_1, ε_2, and timestamp to the merchant_0. The merchant_0 tests $\varphi\prime \stackrel{?}{=} H[i\|(SK_M PK_C)_x\|\alpha_i]$ and saves α_i, i, ε, ε_1, ε_2.

The protocol that the merchant_0 pays the e-cash to the merchant_i (i =1, 2, ..., n) or factory is the same as the payments that the user pays to merchant.

2.3. Transferable Protocol. The e-cash can circulate in the user's e-business. First, the user_1 computes $\varepsilon = H(\alpha_i)$, $\varepsilon_1 = \text{d}ID_{nU1} - \varepsilon e_1$, $\varepsilon_2 = d - \varepsilon e_2$, d, $e_1, e_2 \in Z_n$, $d \neq 0$, $b_1, c_1 \in Z_n$, $\alpha_i = H(b_1\|t_3\|SK_{U1}\|\alpha_I\|j\|i)$, $\beta_\text{i} = H[(c_1G)_x\|\alpha_i\|t_3\|j\|i]$,$\gamma_i = c_1 + \beta_i SK_{U1}$, and sends α_i, β_i, γ_i, i, j, t_3, ε, ε_1, and timestamp the e-cash cannot use again. Then the user 2 tests $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_{U1})\|\alpha_i\|t_3\|j\|i]$ and saves α_i, β_i, γ_i, i, j, t_3, ε, ε_1, ε_2.

2.4. Deposit Protocol. When the person saves the e-cash to the bank, the bank must verify the correctness of the e-cash. The distributed bank must check whether the used e-cash is less than or equal to the distributed e-cash. If the used e-cash is more than the distributed e-cash, the bank can trace the person's identification. When the person saves the e-cash to the bank_n, the e-cash will save in the bank_n; when the person saves the e-cash to the bank_m (not the distributed bank_n), the bank_m will send the e-cash to the bank_n. After the e-cash in the bank_n is dealt well, the person finishes the deposit. The central bank that has the highest grade among banks can test the trading process of the bank to check the business errors and punishment them. Thus, the e-cash can circulate in all the banks, which can meet the needs of reality.

2.5. Update of the E-Cash. When the usage period of the e-cash is over, the person tells the bank and fetches the new e-cash.

3. Discussion of Safety and Efficiency

α_i, β_i, and γ_i are the right signatures of the e-cash i. Because $\gamma_i G - \beta_i PK_U = (c + \beta_i SK_U)G - \beta_i PK_U = cG$, $\beta_i \stackrel{?}{=} H[(\gamma_i G - \beta_i PK_U)\|\alpha_i\|t_2\|j\|i]$ is verified. The e-cash and its signatures cannot be forged.

The e-cash and its signatures contain SK. Any attacker must gain SK so as to forge the e-cash and its signatures, which must solve ECDLP. ECDLP cannot be solved, so that the e-cash and its signatures cannot be forged. It can save from mis-identity attacks, two-layer anonymity attacks, and linking attacks. Therefore, the e-cash is safe and divisible.

When the user pays the e-cash with value i for the first time, the user sends $\alpha_i = H(b_1\|t_2\|SK_U\|\alpha_I\|i\|i)$ ($i < I$). The e-cash with value I-i can use next. When he pays the e-cash with value k for the second time, the user sends $\alpha_i = H(b_1\|t_2\|SK_U\|\alpha_I\|j\|k)$ ($j = i + k$). Similarly, the e-cash can be used repeatedly until ($j = I$). Thus, the usage of the divisible e-cash need not pass bank, which the bank has not the bottleneck of e-business.

3.1. Non-Frameability. $\varepsilon_1 = dI\,D_{nU} - \varepsilon e_1$, so the user's identification is sent with the e-cash. Thus, illegal users cannot frame other users, due to the security against mis-identity attacks, two-layer anonymity attacks, and linking attacks.

When a person uses the e-cash normally, his identity cannot be gained. However, the bank will trace the identity of the user when his e-cash is used repeatedly.

If the person spends the e-cash repeatedly, the bank will find when his e-cash was deposited. Because b is not the same as different e-cash, $\varepsilon = H(\alpha_i)$ and $\alpha_I = H[(ISK_{Bm1} + \delta SK_{Bm2})\|SK_{Bm}\|t_1\|b]$ are different when the user's demand is the same. When the person uses the same e-cash repeatedly, the bank will fetch the other $(\varepsilon\prime,\ \varepsilon_1'\ ,\ \varepsilon_2').d \neq 0$, $\varepsilon_1' = dI\,D_{nU} - \varepsilon\prime e_1$, and $\varepsilon_2' = d - \varepsilon\prime e_2$ .Thus, $\text{ID}_\text{nU} = ((\varepsilon\prime\varepsilon_1 - \varepsilon\varepsilon_1')/(\varepsilon\prime\varepsilon_2 - \varepsilon\varepsilon_2'))\ (\text{mod n}) = ((\varepsilon\prime dI\,D_{nU} - \varepsilon\,dI\,D_{nU})/(\varepsilon\prime d - \varepsilon\,d))$. The bank will check the user's identity ID_nU. Thus, the system can prevent from double spending. So the system is safe, and the bank must be reliable and safe.

The anonymity and untraceability of signatures facilitate criminals to kidnap, launder, and extort money. So it is necessary to design a fair and controllable e-cash system. If he extorts money from the victim, the criminal can only ask the victim to transfer the money. After the victim transfers the e-cash, the criminal obtains the e-cash (I, α_I, ε, ε_1,ε_2) and releases the victim. Then the victim can report to the bank that the e-cash (I, α_I , ε , ε_1 , ε_2) is obtained by extorting means. When the criminal is spending the e-cash, the merchant can call the police and arrest the criminal. After the case is solved, the bank will return the recovered e-cash to the victim. The system can protect from non-frameability, eavesdropping, tampering, and "perfect crime" effectively. So the system is secure.

The time of protocol realization and storage capacity in mobile, divisible, and safe e-cash systems are key to efficiency. 160b of ECC of the paper has the same function with 1024b of RSA [6]. The e-cash system [3] is based on RSA. ECC in the paper needs no exponentiation operation

compared to RSA. The calculation of ECC is very little compared to RSA. Therefore the efficiency of the system runs faster. The e-cash of spending process [3] is $\overline{S}\prime, \overline{T}\prime, \overline{R}\prime, \widehat{K}, \widehat{S}, \widehat{S}_0, \widehat{S}_1, \widehat{S}_2, \widetilde{C}, \widetilde{T}$,b,t,$B_1$,$D_1$,$D_2$, π_2 , the storage space of the e-cash is $1024 * 10 + 128 + 1024 * 5 = 15488$ bit. While the e-cash of spending process in the paper is i, α_i, β_i, and γ_i, the storage space of the e-cash is $32 + 128 + 128 + 192 = 480$ bit(The actual cost in the experimental system), which decreases 96.9% of the storage space and the network bandwidth. Therefore, the system is simple, efficient, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted.

The e-cash in the system has a usage period. When the usage period ends, the bank will delete the e-cash. Thus, the storage space is saved.

The e-cash in the system can circulate in multiple banks, which does not confine to the bank that distributes the e-cash.

The e-cash [1] is inseparable. When the user withdraws the money from the bank, he can only use the money at one time. The merchant has to deposit it in the bank to verify the authenticity. Therefore, the bank has become a bottleneck. The e-cash can be divided. After the user withdraws the money from the bank, he can spend several times without frequently looking for the bank to withdraw money. The merchant does not have to deposit every money that they receive into the bank for verification. When the merchant needs to deposit money, the bank will verify the authenticity of the cash and find out the illegal e-cash.

The e-cash [4] cannot work between the users. However, the e-cash in the system can circulate any time offline between the users before getting saved in the bank.

4. Conclusions

The mobile, divisible, and safe e-cash system adapts on mobile terminals for e-payment which can circulate in multiple banks. The usage of the divisible e-cash needs not pass bank, which the bank has not the bottleneck of e-business. Experimental tests have been made, which prove that the system is simple, efficient, security, and fit for the mobile e-payment terminals in which storage, power, operand capacity, and network bandwidth supply are extraordinarily restricted.

Data Availability

The data used in the study are available at https://www.hindawi.com/publish-research/authors/research-data/#composing-a-data-availability-satement.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The author thanks 2020 International Conference on Artificial Intelligence and Advanced Manufacture for publishing the article “Electronic Cash System based on Multi-Bank Mobile Divisible, Recoverable and Transferable”.

References

[1] X. Liu and Q. Xu, “Improved e-cash system with anonymous user suspension”” *Application Research of Computers*, vol. 33, no. 10, pp. 3099–3104, Oct.2016.

[2] D. Shao, B. Kang, and J. Wang, “Analysis and improvement of two electronic cash schemes,” *Journal of Computer Applications*, vol. 37, pp. 1–6, 2017.

[3] X. Liu and Bo Zhang, “improved endorsed E-cash system with DAA-A,” *Journal of Computer Research and Development*, vol. 53, no. 10, pp. 2412–2429, 2016.

[4] Y. Liang, X. Zhang, and Z. Zheng, “Electronic cash system based on certificateless group signature,” *Journal on Communications*, vol. 37, no. 5, pp. 184–190, 2016.

[5] Z. Jiang-xiao, F. Chun-hui, Ma Jin-xin et al., “Transferable e-cash system with arbitrarily spending order,” *Transactions of Beijing Institute of Technology*, vol. 39, no. 3, pp. 283–289, 2019.

[6] A. J. Menezes, T. Okamoto, and S. A. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.