Multiple-Denomination E-Cash

Jia-Ning Luo[1] and Ming-Hour Yang[2]
[1]Department of Information and Telecommunication Engineering, Ming Chuan University, Taoyuan 33348, Taiwan
[2]Department of Information and Computer Engineering, Chung Yuan Christian University, Taoyuan 32023, Taiwan

***Abstract*—E-commerce has developed rapidly in recent years and online transactions and digital services have become popular. However, existing trading systems such as ATMs, credit cards, Paypal, and prepaid systems are potentially unsecure and users' privacy is not sufficiently protected. This study proposed an e-cash system with multiple denominations that enables e-merchants to give customers change when in an offline environment. The proposed system results in convenient transactions regardless of transaction amount and reduces the amount of e-cash users need to deposit in advance.**

I. Introduction

Electronic cash (e-cash) protects the privacy of online transactions through anonymity. Consequently, neither banks nor merchants can analyze consumer behaviors through their e-cash transactions. Such transactions provide security and anonymity guarantees to all parties involved in a transaction [1], [2].

In reality, it is difficult for users to predict the amount of currency required for future transactions and buy the corresponding amount of e-cash in advance. Additionally, a user's real-time balance cannot be identified in an offline environment. Therefore, Sarkar proposed a transferable e-cash scheme [3] that extends online transferable e-cash [1], [2] into offline environments. [4] recorded the e-cash transfer process using a group signature to solve merchants' verification problems. [5] used bounded accumulators to increase the binary-tree computation representing various e-cash combinations during e-cash withdrawal.

This study proposed an e-cash scheme with multiple denominations and applicable to both online and offline transactions. Compared with existing offline divisible e-cash schemes, the proposed scheme requires less data storage and has lower computation complexity during transactions. Banks generate balance of online transactions to reduce the data stored on users' e-cash devices, whereas merchants are responsible for the change given to consumers (i.e., e-cash balance) during offline transactions, which is provided through offline transfer. The e-cash transaction protocol proposed in this study satisfies the following offline e-cash transaction security requirements:

- Anonymity: The user's spending records are protected by the untraceability of e-cash usage even in the occurrence of collusion between the bank and merchant.
- Unlinkability: The proposed e-cash scheme ensures users' anonymity and transaction unlinkability by disallowing the identification of any similarity between e-cash users.
- Unforgeability: Valid e-cash cannot be created from known e-cash or from anywhere other than the bank itself.
- Double spending detection: The bank can detect double spending regardless of whether transactions occur online or offline.
- Anonymity revocability: When double spending occurs, the bank can revoke user anonymity using the double-spending detector provided by the TTP.
- Traceability: When double spending occurs, user anonymity revocation reveals the user's spending history through the device provided by the TTP.

II. System Architecture

In this section, an e-cash scheme is proposed. The parties involved in the proposed scheme comprise the e-cash-issuing bank, the merchant (who is not anonymous), and e-cash users.

There are four steps of the proposed e-cash scheme from issuance to write-off: registration, withdrawal, online or offline transaction, and redemption. When a consumer wishes to use the e-cash scheme, they must register with the bank and complete a user ID application using their mobile device. The user can withdraw e-cash multiples upon the completion of registration, and the bank issues e-cash through TTP verification, storing the user's balance on their mobile device. The online transaction protocol is implemented when users make a purchase at merchants with Internet access, wherein the purchase amount is immediately converted from e-cash to cash and transferred to the merchant's account. In the offline transaction protocol, the merchant redeems the purchase amount via the Internet at a later point in time.

A. Registration

When a consumer wishes to use the e-cash scheme, they must register with the bank and complete a user ID application using their mobile device.

B. E-cash withdrawal

The user's credit, approved by the bank, is used to generate e-cash of corresponding value through the validator which is owned by a TTP and is stored on the user's mobile device.

C. E-cash transaction

The user places an order with the merchant. After receiving the order, the merchant sends the user an invoice. The user confirms the invoice and selects an amount of e-cash. The merchant sends the message received from the user and the

OI to the bank. The bank compares the OI from both the user and merchant and authenticates the user's e-cash status. The bank then generates new e-cash for customer change and sends it with a blind signature and message of successful transaction back to the merchant before adding the transaction amount to the merchant's account. Upon receiving the change from the bank, the merchant transfers the e-cash change to the user.

D. E-cash Redemption

The merchant sends the e-cash and all attached parameters to the bank for redemption. Upon receiving the e-cash from the merchant, the bank verifies the legitimacy of the e-cash and whether double spending has occurred using its database before signing and verifying the zero-knowledge proof. If all verifications pass, the bank deposits the corresponding e-cash value in the merchant's account and archives it in the database.

III. Conclusion

This study proposed an e-cash scheme suitable for both online and offline transactions. The proposed scheme has various security measures: unlinkability, verifiability, unforgeability, double spending detection, tamper resistance, and nonrepudiation. When double spending occurs, the bank is entitled to trace fraudulent users and revoke their anonymity using an validator device without compromising the anonymity of nonfraudulent users.

Acknowledgements

The authors gratefully acknowledge the support from Ministry of Science and Technology under the grants MOST 106-2221-E-130-001, and MOST 106-3114-E-011-00, and MOST 106-3114-E-011-003.

References

[1] R. S. Anand and C. V. Madhavan, "An online, transferable e-cash payment system," in *International Conference on Cryptology in India*. Springer, 2000, pp. 93–103.

[2] B. Carbunar, W. L. Shi, and R. Sion, "Conditional e-payments with transferability," *Journal of Parallel and Distributed Computing*, vol. 71, no. 1, pp. 16–26, 2011.

[3] P. Sarkar, "Multiple-use transferable e-cash," *International journal of computer applications*, vol. 77, no. 6, 2013.

[4] G. Fuchsbauer, D. Pointcheval, and D. Vergnaud, "Transferable constant-size fair e-cash," in *International Conference on Cryptology and Network Security*. Springer, 2009, pp. 226–247.

[5] M. H. Au, W. Susilo, and Y. Mu, "Practical anonymous divisible e-cash from bounded accumulators," in *International Conference on Financial Cryptography and Data Security*. Springer, 2008, pp. 287–301.