An Offline Transferable and Divisible Mobile Coupon based on NFC

JiaNing Luo, and MingHour Yang

***Abstract*—**Researchers have proposed integrating vouchers with NFC-equipped cell phones. This study proposes an NFC-based offline transferable and divisible coupon scheme. Users can transfer the unused portions of M-coupons to other users. In this method, PayWord's dual hash chain was used for transferring and dividing M-vouchers and adding trusted third party-issued one-time passwords (One-time-certificate) and secure elements in the NFC cell phones to provide unlinkable, offline transferable, and divisible M-coupons functions. This scheme comprised the following features: 1) unlinkability, 2) offline transferability, 3) divisibility, and 4) redeemability. Using One-time-certificate, adversaries cannot trace user identity from the coupon contents. By using one-time-certificate obtained in advance through registration from trusted third parties, users can transfer or redeem the M-coupons without connecting to the issuers. When users have multiple vouchers, they may selectively make partial transfers to other users. In addition, users may redeem discounts using self-purchased or transferred coupons.

***Keywords*—**Divisible, mobile coupon (M-coupon), near-field communication (NFC), offline transfer, unlinkability.

I. Introduction

COUPONS [1] are vendors' crucial advertisement and sales instruments, which can be further divided into ordinary coupons and vouchers [2]. Numerous researchers have proposed mobile coupon (M-coupon) technologies that enable coupon downloads on mobile devices [3]–[18]. Among these, some used near-field communication (NFC), which is a short-distance wireless communication technology [3], [7], [9]–[10].

In 2006, Chang et al. [6] proposed an M-coupon system using the symmetric encryption technique. In Chang's system, users can transfer M-coupons to other users, but coupon transfers and redemptions must be processed through the issuers. However, Chang's protocol is a target of man-in-the-middle attack; moreover, existing owners may preferentially redeem their coupons during redemption processes. In 2007, Dominikus et al. [9] proposed an NFC-based M-coupon system. M-coupons can be obtained by accessing NFC tags on posters or advertisements by using NFC-equipped mobile devices. This protocol prevents forging, double-spending, and tempering but does not include the functions of user anonymity and coupon transferability and traceability.

JiaNing Luo is with the Information and Telecommunications Engineering department, Ming Chuan University, Taoyuan, Taiwan.

MingHour Yang was with the Information Computer Science department, Chung Yuan Christian University, Taoyuan, Taiwan.

In 2009, Hsiang et al. [10] proposed a secure M-coupon scheme that applies a quadratic residue theorem and hash function and NFC as a channel for transactions. In 2012, Sánchez-Silos et al. [14] proposed the WingBonus system, which uses NFC-equipped mobile devices for accessing, storing, managing, and redeeming mobile coupons. In 2010, Hsueh et al. [11] proposed an M-coupon sharing protocol that applies a word-of-mouth marketing strategy based on public key infrastructure and digital signature. Through this protocol, issuers generate original and recommended M-coupons to M-coupon owners. In addition to using existing M-coupons, owners can transfer the recommended M-coupons through word of mouth to other users, thereby increasing M-coupon usage.

Among various M-coupon solutions, several researchers have not provided user identity protections [6], [9], [11], [17]–[18] or coupon transfer functions [9]–[10].

To enhance coupon protection, an NFC-based M-coupon scheme, which enables offline transfer and division functions, was proposed. A PayWord-based dual hash chain was used for providing the transfer and division functions. One-time certificates issued by trusted third parties (TTPs) and SEs in NFC cell phones were incorporated to support unlinkable, offline transferable, and divisible M-coupons.

II. Near-field Communication-based Offline Transferable and Divisible mobilE-coupons

The offline-transfer M-coupon scheme proposed in this study was divided into four stages: 1) registration, 2) purchase, 3) transfer, and 4) authentication, as shown in Fig 1. First, all users must obtain One-time-certificate for their cell phones from TTPs and register. Next, users may purchase M-coupons from issuers and download them to their cell phones. Subsequently, users may make partial M-coupon transfers to other users or redeem their coupons from vendors under offline conditions. Finally, vendors authenticate the redeemed M-coupons with the issuers. The systematic roles comprised the following: TTPs are responsible for managing user lists. Users and cell phone SEs are listed correspondingly, and One-time-certificate are issued. Issuers are responsible for distributing M-coupons to users. Vendors are responsible for redeeming user's M-coupons. Users refer to the owners and users of NFC cell phones. SEs are secure storage spaces provided in the cell phones used for encryptions and key generations.

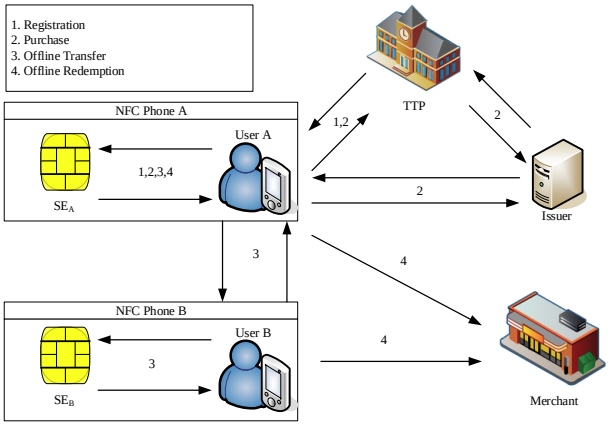

Fig.1 Offline Transfer System Architecture

During initialization, TTPs, issuers, vendors, users, and SEs each have a unique identification code (ID_{TTP}, ID_{Issuer}, ID_{User}, and ID_{SE}) and a set of asymmetric keys (PK_{ID} and SK_{ID}). In this study, the identities are assumed authenticated between each role during connection processes and all messages are transferred in secure channels. The symbols used in this study are defined in Table 1.

TABLE I
NOTATIONS

i	the systematic roles; comprising the TTP, issuer, vendor, user, and SE
ID_i	the identification code of role *i*
$Cert_i$	the certification of role *i*
$Cert_{Ti}$	the one-time-certificate (one-time certificate) of role *i*
PK_i, SK_i	the public and secret keys of role *i*
$PK_{i,j}$	the stage key between role *i* and system *j*
$Sign(SK_i, M)$	the function of using role *i*'s secret key for signing message *M*
$E(K_i, M)$	the function of using role *i*'s key K_i for encrypting message *M*
$D(K_i, M)$	the function of using role *i*'s key K_i for decrypting message *M*
$Nonce_a$	random number *a*
K_s	symmetric key shared by SE and TTP
$H()$	one-way hash function
DS	dual signature
$Coupon_i$	role *i*'s M-coupon
SN	the serial number of the M-coupon
$TransferLog$	the transfer log of M-coupons
$LogM$	partial message in the M-coupon transfer log

A. Registration Stage

During registration, users register to bind user identifications to cell phone SEs through TTPs and obtain a One-time certificate. Users send request messages and personal identification codes to SEs in which sets of keys and user–SE binding signatures used for the certificate are generated. Through mutually certified secure channels, the public keys and signatures of certificate are sent to TTPs for registration to confirm the current cell phone users. After registration, TTPs generate and return the certificate ($Cert_{T1}$) to the cell phones. This certificate comprises only one corresponding public key to each identification code and does not include the users' and SEs' identity information. Finally, TTPs generate the hash chain authentication values (s_m) for the maximum permitted coupons that authenticated users may transfer.

The detailed steps are described as follows:

Step 1: The key pair PK_{T1} and SK_{T1} is generated from the SE for the one-time-certificate, communication key K_S (shared with TTPs), and random number $Nonce_1$.

Step 2: The key SK_A is used by the SE to encrypt user identification ID_A, one-time-certificate public key PK_{T1}, symmetric key K_S, and random number $Nonce_1$. SK_{T1} is used to sign user identification ID_A, communication key K_S, and random number $Nonce_1$. The two messages are subsequently combined to generate M_2, which is sent to the TTPs.

Step 3: After TTPs receive M_2, $Cert_{T1}$ is generated and comprises the one-time-certificate identification code ID_{T1}, one-time-certificate public key (PK_{T1}), and time limit of the One-time-certificate (TL_{T1}).

Step 4: The TTPs then send $Cert_{T1}$ to the SE.

B. Purchase Stage

At the purchase stage, users obtain M-coupons from issuers and store them in the SEs of their cell phones. The detailed procedure is specified as follows:

Step 1: User A encrypts ID_{T1}, the number of M-coupons (n), and $Nonce_3$ using the key ($K_{I,A}$) shared with the issuer to generate message M_5, which is sent with $Cert_{T1}$ to the issuer.

Step 2: The issuer uses $K_{I,A}$ and the decryption message M_5 to generate $Nonce_4$. $Nonce_3$ is then used to generate the serial number SN_{T1} and payword w_n. In addition, $Coupon_{T1}$ is generated and comprises the M-coupon serial number SN_{T1}, one-time-certificate identification code ID_{T1}, number of M-coupons n, and payword w_n. Next, PK_{T1} is used to encrypt $Coupon_{T1}$, $Nonce_3$, and $Nonce_4$ to generate and send M_6 to User A.

Step 3: User A uses the secret key of the user's one-time-certificate SK_{T1}, decryption message M_6, and authenticates $Nonce_3$. After using $Nonce_4$ and encrypting $K_{I,A}$, User A generates message M_7, which is sent to the issuer. Subsequently, the issuer uses $K_{I,A}$ to decrypt M_7 and authenticate $Nonce_4$.

C. Offline Transfer Stage

In the offline transfer stage, the original owners of the M-coupons generate M-coupons for other users (or vendors) according to the paywords and quantity-based hash chain authentication values. These coupons can be passed on to subsequent users. Through the one-way hash function, User A generates new paywords for Users B and C by using unused paywords and the hash chain authentication values for the number of coupons currently transferred from authenticated users to other users. Furthermore, User B can use the identical method to generate new paywords to User D.

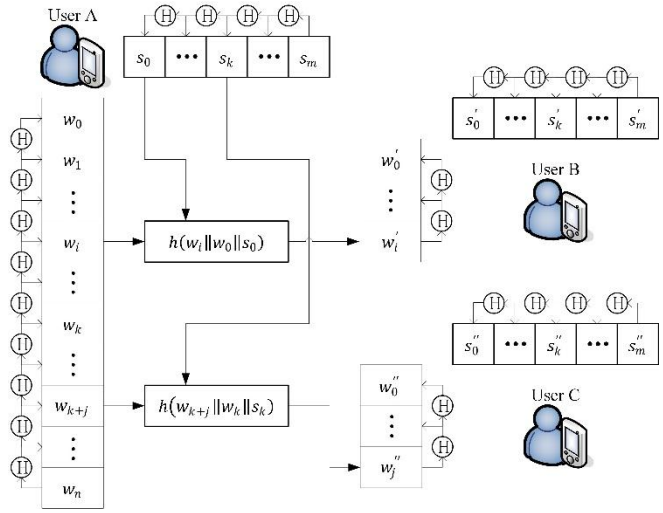

Fig. 2. Offline Redemption Architecture.

At the offline transfer stage, User A can divide and transfer parts of the M-coupons to User B or redeem them from vendors. The detailed steps are specified as follows:

Step 1: User A transfers the personal identification code ID_{T1} and $Cert_{T1}$ to User B.

Step 2: User B generates the personal one-time-certificate identification code ID_{T2}, number of M-coupon transfers i, $Nonce_5$, and $Cert_{T2}$ to User A.

Step 3: User A generates $Nonce_5$, $Nonce_6$, and a new serial number SN_{T2}. In addition, User A adds the paywords for the current number of coupons used and for the sum of the current number of coupons used and transferred (w_k and w_{k+i}) as well as the hash chain authentication value for the current number of coupons transferred to others (s_k) through one-way hash to generate a new payword for the previous number of coupons (w_i'). Subsequently, User A uses the new serial number SN_{T2}, User B's identification code ID_{T2}, number of coupon transfers i, and new payword for the previous number of coupons w_i' to generate the new $Coupon_{T2}$.

Step 4: User A uses ID_{T2}, w_{k+i}, w_k, and the current number of coupon transfers k and the hash chain authentication value thereof s_k to generate message $LogM_1$ through one-way hash. User A then computes the request message $Request$ through one-way hash to generate message $LogM_2$.

Step 5: User A hashes (one-way) and signs $LogM_1$ and $LogM_2$ to generate the dual signature DS.

Step 6: User A uses $K_{I,A}$ to encrypt ID_{T2}, w_{k+i}, w_k, k, s_k, DS, and $LogM_2$ and generate message $LogM_3$.

Step 7: User A uses $LogM_1$, $LogM_3$, DS, and $Cert_{T1}$ to generate message $LogM_4$ and then uses SN_{T1}, SN_{T2}, and the signature for the newly hashed $Coupon_{T1}$ to generate $TransferLog_{T2}$.

Step 8: User A uses users' public key PK_{T2} to encrypt $Coupon_{T2}$, $TransferLog_{T2}$, $Nonce_6$, and calculated $Nonce_5$ ($Nonce_5'$) to generate and send M_8 to User B.

Step 9: After receiving M_8, User B uses SK_{T2} to decrypt M_8 and authenticate $Nonce_5'$. User B then obtains $LogM_1$ from $LogM_4$ and hashes (one-way) the hashed $LogM_1$ and $Request$ and authenticates whether the results match DS.

D. Offline Redemption Stage

At the offline redemption stage, vendors authenticate M-coupons with issuers. The detailed steps are specified as follows:

Step 1: The vendor sends $Coupon_M$ and $TransferLog_M$ to the issuer.

Step 2: The issuer obtains $LogM_4'$ from $TransferLog_M$, from which $LogM_3'$ can be derived. Subsequently, after decryption using the key shared with User B ($K_{I,B}$), the vendor's authenticated identification code (ID_M), payword for the currently used numbers of coupons and coupon transfers ($w_{k'+j}'$), payword for the currently used numbers of coupons ($w_{k'}'$), number of coupons currently transferred to others (k'), and hash chain authentication value for the number of coupons currently transferred to others ($s_{k'}'$) are hashed. Next, one-way hash is performed with $LogM_2'$ to authenticate whether the results match the dual signature DS'.

Step 3: The issuer obtains $TransferLog_{T2}$ and $LogM_4'$ from $TransferLog_M$ and $TransferLog_{T2}$, respectively, and decrypts $LogM_3$ by using $K_{I,A}$. Next, ID_{T2}, w_{k+i}, w_k, k, and s_k are hashed. One-way hash is then performed with $LogM_2$ to authenticate whether the results match DS.

Step 4: In this step, the number of coupon transfers (i and j) are verified to determine whether they exceed the number of redemptions.

III. Security Analysis

This section presents an analysis of the security of the proposed method.

Unlinkability: At the purchase and transfer and redemption stages, users purchase M-coupons by using One-time-certificate, which comprise only one-time-certificate identification codes and public keys and exclude user and SE identity information. Therefore, adversaries cannot trace user identities from coupon contents.

Offline transferability: Both transaction parties use the SEs in NFC through TTP-issued one-time-certificate secret keys to generate new M-coupons. Therefore, coupon owners can authenticate and transfer coupons through One-time-certificate under offline conditions.

Divisibility: During the offline transfer stage, users use paywords and s_k to generate new paywords and use dual signatures to enable issuers to trace the sources of coupon transfers.

Verifiability: At the purchase stage and online transfer and redemption stage, coupon issuance requires the signing of issuers. Therefore, anyone can authenticate the legitimacy of M-coupons. During offline transfer and redemption, the original coupon owners use secret keys for signing and issuing M-coupons, which are legitimized through one-time-certificate authentication.

Forgery prevention: During the purchase stage and online coupon transfer and redemption stages, issuers have the only secret keys to sign and issue M-coupons. Therefore, M-coupons cannot be forged. In offline transfer and redemption, M-coupons are issued by the original coupon owners, who own the only secret keys to one-time signatures and coupon issuance. Therefore, M-coupons cannot be forged under offline conditions either.

Double-spending prevention: During the online transfer and redemption stages, the processes must be completed through the issuers; therefore, issuers may prevent transferrers and redeemers from double-spending. Under offline conditions, coupon transfers and redemption bypass the issuers, but new M-coupons must be signed through One-time-certificate. Double-spending can be identified when reconnected to issuers.

Tempering: During the purchase stage, issuers determine whether the purchase-related information message digests and order-related information hash values agree with the dual signatures, and TTPs determines whether the purchase-related information hash values and order-related information message digests agree with the dual signatures. Tempered information is deemed to fail in this verification process. In coupon transfer and redemption, M-coupons are signed through the issuers or user One-time-certificate; therefore, coupon tempering can be verified.

Nonrepudiation: Both parties during coupon transfers have records of one-time-certificate exchanges; therefore, they cannot deny actions performed in previous transactions.

III. Conclusion

In this study, a PayWord-based dual hash chain was integrated with NFC-equipped mobile devices to provide a scheme capable of making offline transfers and dividing M-coupons. NFC exhibits the convenience of data transfer through touch-interaction of NFC-equipped devices. By using these devices, users may purchase M-coupons from issuers and redeem coupons from vendors. Moreover, they may fully or partially transfer their M-coupons to other users.

In this method, users purchase, redeem, and transfer M-coupons by using OTPs obtained from TTPs, who have strict access to the user identities, thereby achieving unlinkability. The application of this method was based on PayWord's dual hash chain. In addition, SEs from NFC cell phones were added to provide the transferability and divisibility of M-coupons. When disputes occur during transaction processes, exchange records can be traced through TTPs, thereby reinforcing nonrepudiation.

This method stimulates the willingness of consumers to consume by using M-coupons and promotes issuers' and vendors' increased revenues, thereby providing mutually beneficial effects.

References

[1] M. Kumar, A. Rangachari, A. Jhingran, and R. Mohan, "Sales promotions on the internet," *3rd USENIX workshop on Electronic Commerce*, Boston, pp. 167-176, 1998.

[2] F. Borrego-Jaraba, P. C. Garrido, G. C. García, I. L. Ruiz, and M. Á. Gómez-Nieto, "A Ubiquitous NFC Solution for the Development of Tailored Marketing Strategies Based on Discount Vouchers and Loyalty Cards," in *Sensors,* Vol. 13(5), pp. 6334-6354, 2013.

[3] M. Aigner, S. Dominikus, and M. Feldhofer, "A System of Secure Virtual Coupons Using NFC Technology," *5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 362-366, 2007. http://dx.doi.org/10.1109/percomw.2007.15

[4] A. Alshehri, J. A. Briffa, S. Schneider, and S. Wesemeyer, "Formal security analysis of NFC M-coupon protocols using Casper/FDR," *5th International Workshop on Near Field Communication (NFC)*, pp. 1-6, 2013. http://dx.doi.org/10.1109/nfc.2013.6482439

[5] F. Armknecht, A. N. E. B., H. Löhr, M. Manulis, and A.-R. Sadeghi, "Secure Multi-Coupons for Federated Environments: Privacy-Preserving and Customer-Friendly," in *Information Security Practice and Experience*, L. Chen, Y. Mu, and W. Susilo, Editors, Springer Berlin Heidelberg, pp. 29-44, 2008.

[6] C. C. Chang, C. C. Wu, and I. C. Lin, "A Secure E-coupon System for Mobile Users," in *International Journal of Computer Science and Network Security,* Vol. 6(1), pp. 273-279, 2006.

[7] [7] H.-C. Cheng, J.-W. Chen, T.-Y. Chi, and P.-H. Chen, "A generic model for NFC-based mobile commerce," *11th International Conference on Advanced Communication Technology*, pp. 2009-2014, 2009.

[8] [8] G. V. Damme, K. M. Wouters, H. Karahan, and B. Preneel, "Offline NFC payments with electronic vouchers," in *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds* pp. 25-30, 2009.

[9] [9] S. Dominikus and M. Aigner, "mCoupons: An Application for Near Field Communication (NFC)," *21st International Conference on Advanced Information Networking and Applications Workshops*, pp. 421-428, 2007.

[10] [10] H.-C. Hsiang, H.-C. Kuo, and W.-K. Shih, "A secure mCoupon scheme using near field communication," in *International Journal of Innovative Computing, Information and Control,* Vol. 5(11 (A)), pp. 3901-3909, 2009.

[11] S.-C. Hsueh and J.-M. Chen, "Sharing secure m-coupons for peer-generated targeting via eWOM communications," in *Electronic Commerce Research and Applications,* Vol. 9(4), pp. 283-293, 2010. http://dx.doi.org/10.1016/j.elerap.2010.01.002

[12] A. P. Isern-Deya, M. F. Hinarejos, J.-L. Ferrer-Gomila, and M. Payeras-Capellà, "A Secure Multicoupon Solution for Multi-vendor Scenarios," *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 655-663, 2011.

[13] H. Meng and D. Zhang, "Research on the digital coupon of mobile two-dimensional code based on RSA digital signature," *Second International Conference on Computational Intelligence and Natural Computing Proceedings (CINC)*, pp. 368-371, 2010.

[14] J. J. Sánchez-Silos, F. J. Velasco-Arjona, I. L. Ruiz, and M. Á. Gómez-Nieto, "An NFC-Based Solution for Discount and Loyalty Mobile Coupons," *4th International Workshop on Near Field Communication (NFC)*, pp. 45-50, 2012.

[15] L. Xin and X. Qiu-liang, "Practical compact multi-coupon systems," *IEEE International Conference on Intelligent Computing and Intelligent Systems*, pp. 211-216, 2009.

[16] B. Zhang, J. Teng, X. Bai, Z. Yang, and D. Xuan, "P^3-coupon: A probabilistic system for Prompt and Privacy-preserving electronic coupon distribution," *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 93-101, 2011. http://dx.doi.org/10.1109/PERCOM.2011.5767599

[17] C. -K. Chang, "An Improved E-Coupon Scheme and Its Extension to E-Gift Certificate," Master's Thesis, Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, 2007.

[18] Y. -J. Lai, "Transferable Valued Coupon for Mobile Applications," Master's Thesis, Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, 2012.

[19] R. Rivest and A. Shamir, "PayWord and MicroMint: Two simple micropayment schemes," in *Security Protocols*, M. Lomas, Editor, Springer Berlin Heidelberg, pp. 69-87, 1997.

[20] K. Sunhyoung and L. Wonjun, "A pay word-based micropayment protocol supporting multiple payments," *The 12th International Conference on Computer Communications and Networks*, pp. 609-612, 2003. http://dx.doi.org/10.1109/icccn.2003.1284234