中正嶺學報 第四十六卷 第二期 民國 106.11
JOURNAL OF C.C.I.T., VOL.46, NO.2, NOV., 2017

An Offline Transferable and Divisible M-coupon Scheme

Jia-Ning Luo[1] and Ming-Hour Yang[2*]

[1]*Information and Telecommunications Engineering, Ming Chuan University*
[2]*Information and Computer Engineering, Chung Yuan Christian University*

ABSTRACT

In the emergence of mobile e-commerce, conventional printed coupons are gradually replaced by mobile coupons. Users may access various coupons by using mobile phones in exchange for discounts. Increasing numbers of mobile phones are currently equipped with near-field communication (NFC) functions. Therefore, researchers have proposed integrating M-coupons with NFC-equipped mobile phones so that users can access M-coupon transactions through NFC. The convenience of touch-interact data transfer in this technology increases the transfer efficiency of M-coupons. However, sensitive user information may be exposed during transaction processes when individuals access or analyze user transaction records without authorization. Without a secure and efficient scheme for transferring and dividing mobile coupons, users or adversaries can forge coupons or use voided coupons that have been transferred to other persons, consequently jeopardizing the financial conditions of issuers. This study proposes an NFC-based offline transferable and divisible mobile coupon scheme. This scheme comprised the following features: 1) unlinkability, 2) offline transferability, 3) divisibility, and 4) redeemability.

Keywords: near-field communication (NFC), mobile coupon, offline transfer, unlinkability

可轉移及分割之離線式行動折價卷機制

羅嘉寧[1]　楊明豪[2*]

[1]銘傳大學電腦與通訊工程學系
[2]中原大學資訊工程學系

摘　　要

在行動商務快速發展的時代，傳統紙本式折價卷已逐漸被電子式行動優惠卷取代。使用者可以使用行動裝置兌換優惠卷已獲得優惠。近年來行動裝置已大多配置有近場通訊(NFC)元件，也有許多學者提出整合近場通訊元件之行動商務交易機制，以便使用者可利用近場通訊之接觸式感應方式進行折價卷之交易，也增加了傳輸效率。然而，當使用者的交易紀錄在未經授權的形況下被惡意使用者或商家利用及分析時，則可能在交易過程期間暴露敏感的用戶信息。惡意使用者即可偽造優惠卷或使用已被轉移給其他人的無效優惠卷，從而對發行者造成財務威脅。本論文提出一個基於近場通訊之可離線轉移及可分割的行動優惠卷機制，本機制包含以下特性：不可鏈接性、可離線傳輸性、可分割性及可兌換性。

關鍵詞：近場通訊，行動優惠卷，離線轉移，不可鏈接性

文稿收件日期 106.2.22;文稿修正後接受日期 106.9.12; *通訊作者
Manuscript received February 22, 2017; revised September 12, 2017; * Corresponding author

Ⅰ. INTRODUCTION

Coupons and vouchers refer to the free tickets vendors distribute to users through the media to promote merchandise [1][2]. These include gift certificates from department stores and bookstores or toll tickets for public transportation.

In the emergence of mobile devices, numerous manufacturers have gradually converted conventional printed coupons onto mobile devices to increase convenience through digitization and portability. Numerous researchers have proposed mobile coupon technologies that enable coupon downloads on mobile devices [3]–[16]. Among these, some used near-field communication (NFC), which is a short-distance wireless communication technology. The secure elements (SEs) equipped on NFC cell phones can be used for encryption–decryption operations and information storage, thereby protecting confidential information on mobile devices. This technology can be widely applied for downloading and redeeming M-coupons [3][7][9][10].

An M-coupon system that protects user privacy must comprise the following features: 1) anonymity, 2) unlinkability, 3) offline transferability, 4) divisibility, 5) verifiability, and 6) double-spending prevention. These features provide the following functions: prevent anyone from accessing user identities from coupon contents, prevent adversaries from tracing user identity from coupon contents and other transaction records, enable the offline transfer or redemption of M-coupons to other users or vendors when the issuers cannot be timely connected to authenticate transactions, enable users of multiple coupons to selectively make partial coupon transfers to other users, enable anyone to authenticate coupon legitimacy, and prevent the double-spending of coupons.

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.

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 (OTCs) issued by trusted third parties (TTPs) and SEs in NFC cell phones were incorporated to support unlinkable, offline transferable, and divisible M-coupons.

The rest of the paper is organized as follows. Section 2 describes our transferable and divisible mobile coupon scheme. Section 3 analyses our scheme's security strength by using the common security attack models. Finally, section 4 presents our conclusions.

Ⅱ. NFC-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) offline transfer, and 4) offline redemption. First, all users must obtain OTCs 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 architecture is shown in Fig. 1.

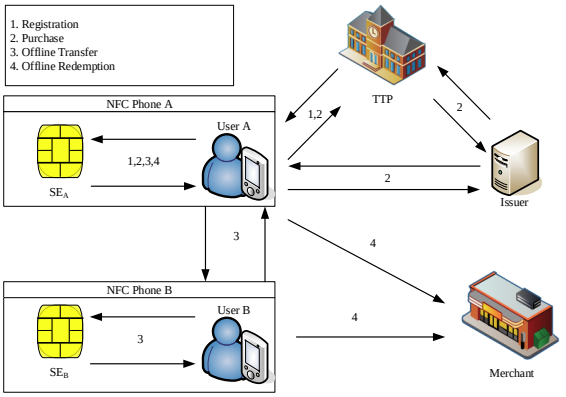

Fig. 1. Offline transfer system architecture.

The systematic roles comprised the following: TTPs are responsible for managing user lists. Users and cell phone SEs are listed correspondingly, and OTCs 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.

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 1. Symbol Definitions

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 OTC (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 OTCs (the architecture is shown in Fig. 2). Users send request messages and personal identification codes to SEs in which sets of keys and user–SE binding signatures used for OTCs are generated. Through mutually certified secure channels, the public keys and signatures of OTCs are sent to TTPs for registration to confirm the current cell phone users. After registration, TTPs generate and return OTCs ($Cert_{T1}$) 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 seed (s_m) for the maximum permitted coupons that authenticated users may transfer.

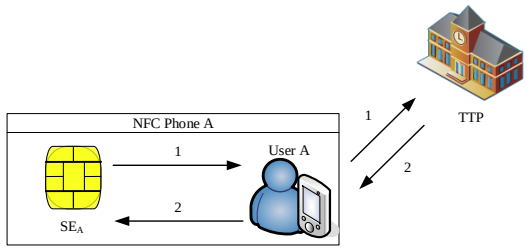

Fig. 2. Registration stage architecture.

The registration procedure is shown in Fig. 3. The detailed steps are described as follows:

1. The key pair PK_{T1} and SK_{T1} is generated from the SE for the OTC, communication key K_S (shared with TTPs), and random number Nonce1.
2. The key SK_A is used by the SE to encrypt user identification ID_A, 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.
3. After TTPs receive M_2, $Cert_{T1}$ is generated and comprises the identification code ID_{T1}, PK_{T1}, and time limit of the OTCs (TL_{T1}).
4. The TTPs then send $Cert_{T1}$ to the SE.

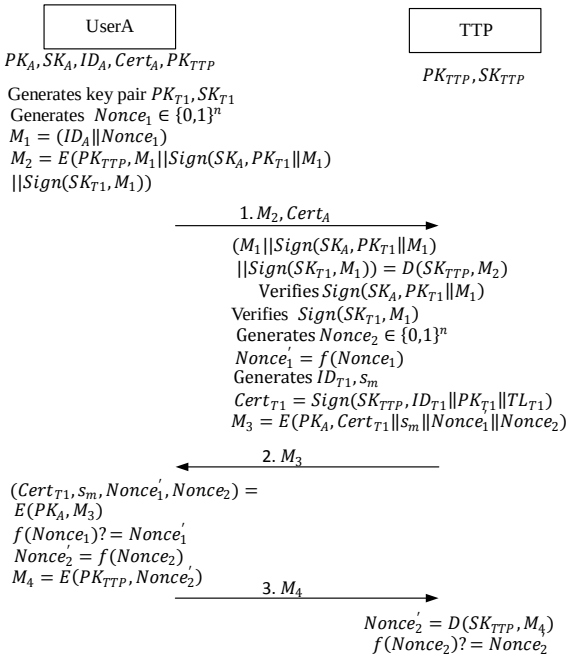

Fig. 3. Offline registration procedure.

B. Purchase Stage

At the purchase stage, users obtain M-coupons from issuers and store them in the SEs of their cell phones. This process is shown in Fig. 4. The detailed procedure is specified as follows:

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.

The issuer uses $K_{I,A}$ and the decryption message M_5 to generate Nonce4. $Nonce_3$ 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}, OTC 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.

User $_A$ uses the secret key of the user's 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 $Nonce_4$.

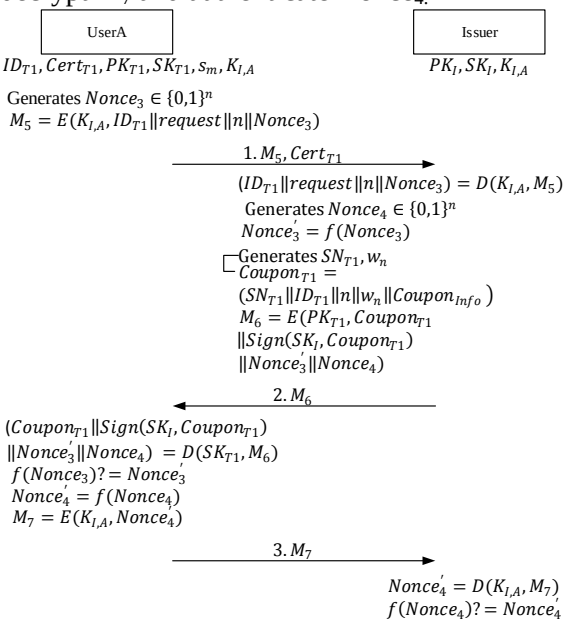

Fig. 4. Purchase stage procedure.

C. Offline Transfer Stage

In the offline transfer process, 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. The offline transfer architecture is shown in Fig. 5. 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.

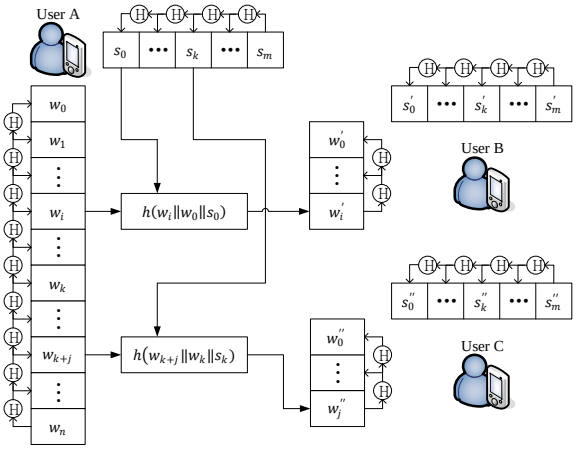

Fig. 5. Offline transfer architecture.

At the offline transfer stage, User A can divide and transfer parts of the M-coupons to User B or redeem them from vendors (Fig. 6). The detailed steps are specified as follows:

1. User A transfers the personal OTC identification code ID_{T1} and $Cert_{T1}$ to User B.
2. User B generates the personal OTC identification code ID_{T2}, number of M-coupon transfers *i*, $Nonce_5$, and $Cert_{T2}$ to User A.
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 seed 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 OTC identification code ID_{T2}, number of coupon transfers *i*, and new payword for the previous number of coupons w_i' to generate the new $Coupon_{T2}$.
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 *sk* to generate message Log_{M1} through one-way hash. User A then computes the request message Request through one-way hash to generate message Log_{M2}.
5. User A hashes (one-way) and signs Log_{M1} and Log_{M2} to generate the dual signature DS.
6. User A uses $K_{I,A}$ to encrypt ID_{T2}, w_{k+i}, w_k, *k*, *sk*, DS, and Log_{M2} and generate message Log_{M3}.
7. User A uses Log_{M1}, Log_{M3}, DS, and $Cert_{T1}$ to generate message Log_{M4} and then uses SN_{T1}, SN_{T2}, and the signature for the newly hashed $Coupon_{T1}$ to generate $TransferLog_{T2}$.
8. User A uses users' OTC 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.
9. After receiving M_8, User B uses SK_{T2} to decrypt M_8 and authenticate $Nonce_5'$. User B then obtains Log_{M1} from Log_{M4} and hashes (one-way) the hashed Log_{M1} and Request and authenticates whether the results match DS.

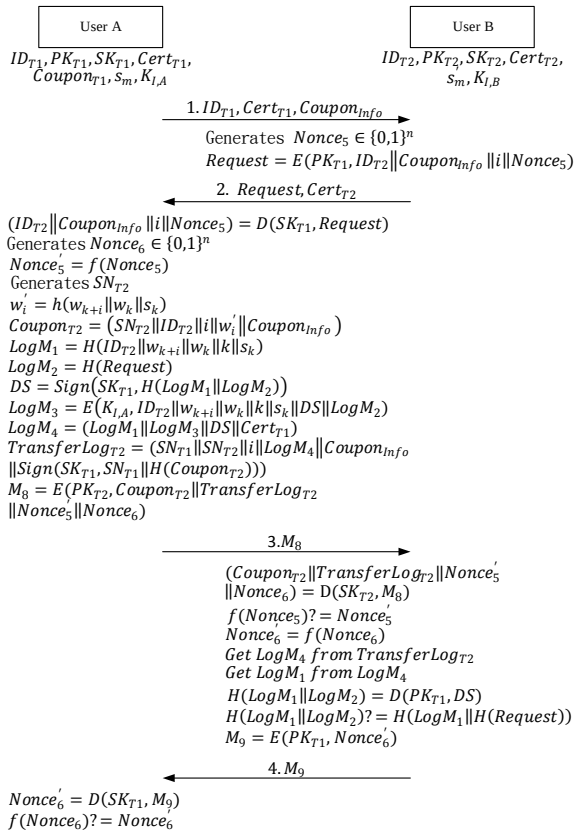

Fig. 6. Partial transfer procedure.

D. Offline Redemption Stage

At the offline redemption stage, vendors authenticate M-coupons with issuers. This procedure is shown in Fig. 7. The detailed steps are specified as follows:

1. The vendor sends $Coupon_M$ and $TransferLog_M$ to the issuer.
2. The issuer obtains Log_{M4}' from $TransferLog_M$, from which Log_{M3}' 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 Log_{M2}' to authenticate whether the results match the dual signature DS'.
3. The issuer obtains $TransferLog_{T2}$ and Log_{M4}' 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.
4. In this step, the number of coupon transfers (i and j) are verified to determine whether they exceed the number of redemptions.

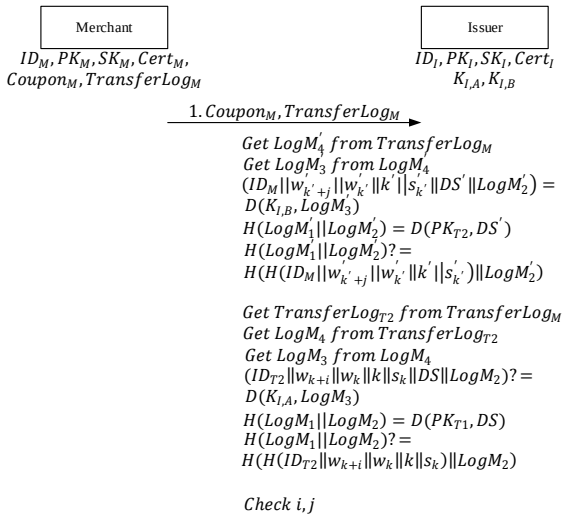

Fig. 7. Offline Redemption procedure.

Ⅲ. Security analysis

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

1. Unlinkability: At the purchase and transfer and redemption stages, users purchase M-coupons by using OTCs, which comprise only OTC identification codes and public keys and exclude user and SE identity information. Therefore, adversaries cannot trace user identities from coupon contents.
2. Offline transferability: Both transaction parties use the SEs in NFC through TTP-issued OTC secret keys to generate new M-coupons. Therefore, coupon owners can authenticate and transfer coupons through OTCs under offline conditions.
3. 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.
4. 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 OTC secret keys for signing and issuing M-coupons, which are legitimized through OTP authentication.
5. 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.
6. 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 OTCs. Double-spending can be identified when reconnected to issuers.
7. 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 OTCs; therefore, coupon tempering can be verified.

8. Nonrepudiation: Both parties during coupon transfers have records of OTC exchanges; therefore, they cannot deny actions performed in previous transactions.

Subsequently, the Gong–Needham–Yahalom logic was applied to test the security of this NFC-based M-coupon scheme.

Ⅳ. CONCLUSIONS

In this study, a PayWord-based dual hash chain payment protocol was proposed to provide a scheme capable of making offline transfers and dividing M-coupons. By using of NFC-integrated mobile devices, users may purchase the coupons from issuers and redeem the coupons from vendors. Moreover, the user can fully or partially transfer their coupons to other users.

In this method, users purchase, redeem, and transfer the coupons by using one-time-certificates obtained from the trust third parties, who have strict access to the user identities, thereby achieving unlinkability. In addition, the secure element of the mobile phone is added to provide the transferability and divisibility of the coupons. When disputes occur during transaction processes, exchange records can be traced through trust third parties, thereby reinforcing nonrepudiation.

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

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support from Ministry of Science and Technology under the grants MOST106-2221-E-130-001-, MOST 106-2221-E-033-002-, and MOST 106-3114-E-011-003-.

REFERENCES

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

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

[3] Aigner, M., Dominikus, S., Feldhofer, M., "A System of Secure Virtual Coupons Using NFC Technology," 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 362-366, 2007.

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

[5] Armknecht, F., Löhr, H., Manulis, M., Sadeghi, A. R., "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] Chang, C. C., Wu, C. C., Lin, I. C., "A Secure E-coupon System for Mobile Users," in International Journal of Computer Science and Network Security, 6(1), pp. 273-279, 2006.

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

[8] Damme, G. V., Wouters, K. M., Karahan,

H., Preneel, B., "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] Dominikus, S., Aigner, M., "mCoupons: An Application for Near Field Communication (NFC)," 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 421-428, 2007.
[10] Hsiang, H. C., Kuo, H. C., Shih, W. K., "A secure mCoupon scheme using near field communication," in International Journal of Innovative Computing, Information and Control, 5(11 (A)), pp. 3901-3909, 2009.
[11] Hsueh, S. C., Chen, J. M., "Sharing secure m-coupons for peer-generated targeting via eWOM communications," in Electronic Commerce Research and Applications, 9(4), pp. 283-293, 2010.
[12] Isern-Deya, A. P., Hinarejos, M. F., Ferrer-Gomila, J. L., Payeras-Capellà, M., "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] Meng, H., Zhang, D., "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] Sánchez-Silos, J. J., Velasco-Arjona, F. J., Ruiz, I. L., Gómez-Nieto, M. Á., "An NFC-Based Solution for Discount and Loyalty Mobile Coupons," 4th International Workshop on Near Field Communication (NFC), pp. 45-50, 2012.
[15] Xin, L., Qiu-liang, X., "Practical compact multi-coupon systems," IEEE International Conference on Intelligent Computing and Intelligent Systems, pp. 211-216, 2009.
[16] Zhang, B., Teng, J., Bai, X., Yang, Z., Xuan, D., "P3-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.
[17] Chang, C. K., "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] Lai, Y. J., "Transferable Valued Coupon for Mobile Applications," Master's Thesis, Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, 2012.
[19] Rivest, R., Shamir, A., "PayWord and MicroMint: Two simple micropayment schemes," in Security Protocols, M. Lomas, Editor, Springer Berlin Heidelberg, pp. 69-87, 1997.
[20] Sunhyoung, K., Wonjun, L., "A pay word-based micropayment protocol supporting multiple payments," The 12th International Conference on Computer Communications and Networks, pp. 609-612, 2003.

APPENDIX GNY PROOF

A. Notation:

TTP	Trust Third Party
I	Coupon Issuer
M	Merchant
U_A	User A
U_B	User B
$\{X\}_K, \{X\}_K^{-1}$	Uses a symmetric key K to encrypt/decrypt message X
$\{X\}_{+K}, \{X\}_{-K}$	Uses a public key (+K) or private key (-K) to encrypt/decrypt message X
$H(X)$	One-way hash function
$P \lhd X$	P received message X
$P \ni X$	P owns message X。
$^*X$	X is generated by others. For example, $P \lhd {}^*X$ means P received a message X from

	others.
$P\| \equiv \#(X)$	P believes message X is fresh.
$P\| \equiv \phi(X)$	P believes message X is recognizable.
$P\| \equiv P \xleftrightarrow{S} Q$	P believes secret S is shared by P and Q.
$P\| \equiv \xrightarrow{+K} Q$	P believes Q owns the private key (-K) correspondent to the public key (+K).
$P\| \equiv Q\|\sim X$	P believes Q sent X.

B. Initial Assumption:

TTP:

$TTP \ni ID_{TTP}, PK_{TTP}, SK_{TTP}, Nonce_2, Cert_A$

$TTP\| \equiv TTP \xleftrightarrow{PK_{TTP}} I$

$TTP\| \equiv TTP \xleftrightarrow{PK_{TTP}} M$

$TTP\| \equiv TTP \xleftrightarrow{PK_{TTP}} U_A$

Issuer:

$I \ni ID_I, PK_I, SK_I$

$I\| \equiv I \xleftrightarrow{PK_I} TTP$

$I\| \equiv I \xleftrightarrow{PK_I} M$

$I\| \equiv I \xleftrightarrow{PK_I} U_A$

Merchant:

$M \ni ID_M, PK_M, SK_M$

$M\| \equiv M \xleftrightarrow{PK_M} TTP$

$M\| \equiv M \xleftrightarrow{PK_M} I$

$M\| \equiv M \xleftrightarrow{PK_M} U_A$

User A:

$U_A \ni ID_A, PK_A SK_A,$

$U_A\| \equiv U_A \xleftrightarrow{PK_A} TTP$

$U_A\| \equiv U_A \xleftrightarrow{PK_{TTP}} TTP$

C. Goal:

Goal 1.1 $TTP\| \equiv \xrightarrow{+PK_{T1}} U_A$

Goal 1.2 $TTP\| \equiv U_A\|\sim\#(Nonce_1)$

Goal 1.3 $U_A\| \equiv TTP\|\sim\#\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}$

Goal 1.4 $U_A\| \equiv TTP\|\sim\#(ID_{T1}, PK_{T1}, TL_{T1})$

Goal 1.5 $U_A\| \equiv TTP\|\sim\#(Nonce_2)$

Goal 1.6 $U_A\| \equiv TTP\|\sim\#(f(Nonce_1))$

Goal 1.7 $TTP\| \equiv U_A\|\sim\#(f(Nonce_2))$

Goal 2.1 $I\| \equiv \xrightarrow{+PK_{T1}} U_A$

Goal 2.2 $I\| \equiv U_A\|\sim\#(Nonce_3)$

Goal 2.3 $U_A\| \equiv I\|\sim\#\{SN_{T1}, ID_{T1}, n, w_n, Coupon_{Info}\}_{-SK_I}$

Goal 2.4 $U_A\| \equiv I\|\sim\#(SN_{T1}, ID_{T1}, n, w_n, Coupon_{Info})$

Goal 2.5 $U_A\| \equiv I\|\sim\#(Nonce_4)$

Goal 2.6 $U_A\| \equiv I\|\sim\#(f(Nonce_3))$

Goal 2.7 $I\| \equiv U_A\|\sim\#(f(Nonce_4))$

Goal 3.1 $U_A\|\equiv U_B\|\sim\#(ID_{T2}, Coupon_{Info}, i, Nonce_5)$

Goal 3.2 $U_A\| \equiv \xrightarrow{+PK_{T2}} U_B$

Goal 3.3 $U_A\| \equiv U_B\|\sim\#(Nonce_5)$

Goal 3.4 $U_B\| \equiv U_A\|\sim\#(Coupon_{T2})$

Goal 3.5 $U_B\| \equiv U_A\|\sim\#(TransferLog_{T2})$

Goal 3.6 $U_B\| \equiv U_A\|\sim\#(Nonce_6)$

Goal 3.7 $U_B\| \equiv U_A\|\sim\#(f(Nonce_5))$

Goal 3.8 $U_A\| \equiv U_B\|\sim\#(f(Nonce_6))$

Goal 4.1 $I\| \equiv U_B\|\sim\#(TransferLog_M)$

Goal 4.2 $I\| \equiv U_A\|\sim\#(TransferLog_{T2})$

D. Proof:

(1) Registration Stage

Message1.1

$U_A \ni PK_{TTP}, PK_A, SK_A, ID_A, PK_{T1}, SK_{T1}, Nonce_1$

$U_A\| \equiv \#(M_1)$

$U_A\| \equiv \#\left(\{PK_{T1}, M_1\}_{-SK_A}\right)$ /*F1*/

$U_A\| \equiv \#\left(\{M_1\}_{-SK_{T1}}\right)$ /*F1*/

$U_A\| \equiv \#\left(M_1, \{PK_{T1}, M_1\}_{-SK_A}, \{M_1\}_{-SK_{T1}}\right)$

$U_A\| \equiv \#\left(\{M_1, \{PK_{T1}, M_1\}_{-SK_A}, \{M_1\}_{-SK_{T1}}\}_{+PK_{TTP}}\right)$

$TTP \lhd *\{M_1, \{PK_{T1}, M_1\}_{-SK_A}, \{M_1\}_{-SK_{T1}}\}_{+PK_{TTP}}$

$TTP \lhd *Cert_A$

Message1.2

$TTP \ni \{M_1, \{PK_{T1}, M_1\}_{-SK_A}, \{M_1\}_{-SK_{T1}}\}_{+PK_{TTP}}$ /*T1,P1*/

$TTP \ni (M_1, \{PK_{T1}, M_1\}_{-SK_A}, \{M_1\}_{-SK_{T1}})$ /*T4*/

$TTP \ni (ID_A, Nonce_1)$

$TTP| \equiv \phi(ID_A)$

$TTP| \equiv \phi(ID_A, Nonce_1)$ /*R1*/

$TTP| \equiv \phi(M_1)$

$TTP \ni \{PK_{T1}, M_1\}_{-SK_A}$

$TTP| \equiv \xrightarrow{+PK_A} U_A$

$TTP| \equiv \#(Nonce_1)$

$TTP| \equiv \#(PK_{T1}, ID_A, Nonce_1)$ /*F1*/

$TTP| \equiv U_A| \sim \#(PK_{T1}, M_1)$ /*I4*/

$TTP| \equiv U_A| \sim \#\{PK_{T1}, M_1\}_{-SK_A}$ /*I4*/

$TTP| \equiv U_A| \sim \#(ID_A, Nonce_1)$

$TTP| \equiv U_A| \sim \#(Nonce_1)$ /*Goal 1.2*/

$TTP \ni \{M_1\}_{-SK_{T1}}$

$TTP| \equiv \xrightarrow{+PK_{T1}} U_A$ /*Goal 1.1*/

$TTP \ni Nonce_2, ID_{T1}, s_m, TL_{T1}$

$TTP| \equiv \#(Nonce_2)$

$TTP| \equiv \#(ID_{T1})$

$TTP| \equiv \#(s_m)$

$TTP| \equiv \#(TL_{T1})$

$TTP \ni f(Nonce_1)$

$TTP| \equiv \#(f(Nonce_1))$

$TTP| \equiv \#(\{\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2\}_{+PK_A}$

$U_A \lhd *\{\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2\}_{+PK_A}$

Message1.3

$U_A \ni$

$\{\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2\}_{+PK_A}$

/*T1,P1*/

$U_A \ni$

$\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2$ /*T4*/

$U_A \ni f(Nonce_1)$

$U_A| \equiv \#(Nonce_2)$

$U_A| \equiv \#(\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2)$

$U_A| \equiv \phi(\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}})$ /*R1*/

$U_A| \equiv \phi(s_m)$ /*R1*/

$U_A| \equiv TTP| \sim \#(f(Nonce_1))$ /*Goal 1.6*/

$U_A| \equiv TTP| \sim \#(\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}, s_m, f(Nonce_1), Nonce_2)$

$U_A| \equiv TTP| \sim \#(\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}})$ /*Goal 1.3*/

$U_A| \equiv TTP| \sim \#(ID_{T1}, PK_{T1}, TL_{T1})$ /*Goal 1.4*/

$U_A| \equiv TTP| \sim \#(Nonce_2)$ /*Goal 1.5*/

$U_A| \equiv \#(f(Nonce_2))$

$U_A| \equiv \#(\{f(Nonce_2)\}_{+PK_{TTP}})$

$\mathrm{TTP} \lhd * \{f(Nonce_2)\}_{+PK_{TTP}}$

$\mathrm{TTP} \ni \{f(Nonce_2)\}_{+PK_{TTP}}$ /*T1,P1*/

$\mathrm{TTP} \ni f(Nonce_2)$ /*IA,T4*/

$TTP| \equiv TTP \xleftrightarrow{Nonce_2} U_A$

$TTP| \equiv U_A| \sim \#(f(Nonce_2))$ /*Goal 1.7*/

(2) Purchase Stage

Message2.1

$U_A \ni ID_{T1}. PK_{T1}, SK_{T1}, K_{I,A}, Nonce_3, request, n$

$U_A| \equiv \#(\{ID_{T1}, request, n, Nonce_3\}_{K_{I,A}})$ /*F1*/

$I \lhd *\{ID_{T1}, request, n, Nonce_3\}_{K_{I,A}}$

$I \lhd *\{ID_{T1}, PK_{T1}, TL_{T1}\}_{-SK_{TTP}}$

Message2.2

$I \lhd \{ID_{T1}, request, n, Nonce_3\}_{K_{I,A}}$ /*T1*/

$I \lhd Cert_{T1}$

$I \lhd PK_{T1}$

$I \ni K_{I,A}$

$I \ni (ID_{T1}, request, n, Nonce_3)$ /*T3,P1*/

$I| \equiv \#(Nonce_3)$

$I| \equiv \#(ID_{T1}, request, n, Nonce_3)$ /*F1*/

$I| \equiv \phi(ID_{T1})$

$I| \equiv \phi(ID_{T1}, request, n, Nonce_3)$ /*R1*/

$I| \equiv \phi(Cert_{T1})$

$I| \equiv I \xleftrightarrow{K_{I,A}} U_A$

$I| \equiv U_A| \sim \#\{ID_{T1}, request, n, Nonce_3\}_{K_{I,A}}$

$I| \equiv U_A| \sim \#(ID_{T1}, request, n, Nonce_3)$

$I| \equiv U_A| \sim \#(Nonce_3)$ /*Goal 2.2*/

$I|\equiv U_A|\sim\#(ID_{T1})$

$I|\equiv \xrightarrow{+PK_{T1}} U_A$ /*Goal 2.1*/

$I \ni Nonce_4, f(Nonce_3), SN_{T1}, w_n, Coupon_{info}$

$I \ni (SN_{T1}, ID_{T1}, n, w_n, Coupon_{info})$

$I \ni Coupon_{T1}$

$I \ni \{Coupon_{T1}\}_{-SK_I}$

$I \ni$

$\{Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4\}_{K_{I,A}}$

$I|\equiv \#(Nonce_4)$

$I|\equiv \#(f(Nonce_3))$

$I|\equiv \#(SN_{T1})$

$I|\equiv \#(w_n)$

$I|\equiv \#(Coupon_{info})$

$I|\equiv \#(SN_{T1}, ID_{T1}, n, w_n, Coupon_{info})$

$I|\equiv \#(Coupon_{T1})$

$I|\equiv \#(\{Coupon_{T1}\}_{-SK_I})$

$I|\equiv$

$\#(\{Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4\}_{K_{I,A}})$

$U_A \lhd *$

$\{Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4\}_{K_{I,A}}$

Message2.3

$U_A \lhd$

$\{Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4\}_{K_{I,A}}$

$U_A \ni (Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4)$

$U_A \ni f(Nonce_3)$

$U_A|\equiv \#(f(Nonce_3))$

$U_A|\equiv \#(Nonce_4)$

$U_A|\equiv$

$\#((Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4))$

$U_A|\equiv$

$\#((Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4))$

$U_A|\equiv \#(SN_{T1}, ID_{T1}, n, w_n, Coupon_{info})$

$U_A|\equiv \#\{SN_{T1}, ID_{T1}, n, w_n, Coupon_{info}\}_{-SK_I}$

$U_A|\equiv \phi(f(Nonce_3))$

$U_A|\equiv I|\sim\#(f(Nonce_3))$ /*Goal 2.6*/

$U_A|\equiv$

$\phi((Coupon_{T1}, \{Coupon_{T1}\}_{-SK_I}, f(Nonce_3), Nonce_4))$

$U_A|\equiv \phi(SN_{T1}, ID_{T1}, n, w_n, Coupon_{info})$

$U_A|\equiv \phi\{SN_{T1}, ID_{T1}, n, w_n, Coupon_{info}\}_{-SK_I}$

$U_A|\equiv I|\sim\#\{SN_{T1}, ID_{T1}, n, w_n, Coupon_{Info}\}_{-SK_I}$ /*Goal 2.3*/

$U_A|\equiv I|\sim\#(SN_{T1}, ID_{T1}, n, w_n, Coupon_{Info})$ /*Goal 2.4*/

$U_A|\equiv I|\sim\#(Nonce_4)$ /*Goal 2.5*/

$U_A \ni f(Nonce_4)$

$U_A|\equiv \#(f(Nonce_4))$

$U_A|\equiv \#(\{f(Nonce_4)\}_{K_{I,A}})$

$I \lhd * \{f(Nonce_4)\}_{K_{I,A}}$

$I \lhd \{f(Nonce_4)\}_{K_{I,A}}$

$I \ni f(Nonce_4)$

$I|\equiv I \xleftarrow{Nonce_4} U_A$

$I|\equiv U_A|\sim\#(f(Nonce_4))$ /*Goal 2.7*/

(3) Offline Transfer

Message3.1

$U_B \lhd *(ID_{T1}, Cert_{T1}, Coupon_{Info})$

Message3.2

$U_B \ni ID_{T2}, PK_{T2}, SK_{T2}$

$U_B \ni (ID_{T1}, Cert_{T1}, Coupon_{Info})$ /*T1,P1*/

$U_B|\equiv \phi(Cert_{T1})$

$U_B|\equiv \phi(ID_{T1}, Cert_{T1}, Coupon_{Info})$ /*R1 */

$U_B \ni Nonce_5$

$U_B \ni ID_{T2}$

$U_B \ni i$

$U_B|\equiv \#(Nonce_5)$

$U_B|\equiv \#(i)$

$U_B|\equiv \phi(ID_{T2})$

$U_B|\equiv \#\{ID_{T2}, Coupon_{Info}, i, Nonce_5\}_{+PK_{T1}}$

$U_B|\equiv \#(Request)$

$U_A \lhd *Request$

$U_A \lhd *\{ID_{T2}, Coupon_{Info}, i, Nonce_5\}_{+PK_{T1}}$

$U_A \lhd *Cert_{T2}$

Message3.3

$U_A \ni \{ID_{T2}, Coupon_{Info}, i, Nonce_5\}_{+PK_{T1}}$ /*T1,P1*/

$U_A \ni (ID_{T2}, Coupon_{Info}, i, Nonce_5)$ /*T4*/

$U_A \ni Cert_{T2}$ /*T1,P1*/

$U_A \ni PK_{T2}$

$U_A| \equiv \xrightarrow{+PK_{T2}} U_B$ /*Goal 3.2*/

$U_A| \equiv \#(Nonce_5)$

$U_A| \equiv \#(ID_{T2}, Coupon_{Info}, i, Nonce_5)$ /F1/

$U_A| \equiv \phi(ID_{T2})$

$U_A| \equiv \phi(ID_{T2}, Coupon_{Info}, i, Nonce_5)$ /*R1*/

$U_A| \equiv U_B|\sim\#(ID_{T2}, Coupon_{Info}, i, Nonce_5)$ /*Goal 3.1*/

$U_A| \equiv U_B|\sim\#(Nonce_5)$ /*Goal 3.3*/

$U_A \ni f(Nonce_5), SN_{T2}, i$

$U_A \ni H(w_{k+i}, w_k, s_k)$

$U_A \ni w_i^{'}$

$U_A \ni (SN_{T2}, ID_{T2}, i, w_i^{'}, Coupon_{Info})$

$U_A \ni Coupon_{T2}$

$U_A \ni H(ID_{T2}, w_{k+i}, w_k, k, s_k)$

$U_A \ni H(Request)$

$U_A \ni \{H(LogM_1, LogM_2)\}_{-SK_{T1}}$

$U_A \ni DS$

$U_A \ni \{ID_{T2}, w_{k+i}, w_k, k, s_k, DS, LogM_2\}_{K_{I,A}}$

$U_A \ni (LogM_1, LogM_3, DS, Cert_{T1})$

$U_A \ni LogM_4$

$U_A \ni$

$(SN_{T1}, SN_{T2}, i, LogM_4, Coupon_{Info}, \{SN_{T1}, H(Coupon_{T2})\}_{-SK_{T1}})$(4) Offline Redemption Stage

$U_A \ni TransferLog_{T2}$

$U_A \ni Nonce_6$

Message 4.1

$U_A \ni \{Coupon_{T2}, TransferLog_{T2}, f(Nonce_5), Nonce_6\}_{+PK_{T2}}$

$M \ni TransferLog_M$

$U_A| \equiv \#(f(Nonce_5))$

$I \lhd *TransferLog_M$ Message 4.2

$U_A| \equiv \#(SN_{T2})$

$I \ni K_{I,B}, TransferLog_M$

$U_A| \equiv \#(H(w_{k+i}, w_k, s_k))$

$I \ni$

$U_A| \equiv \#(w_i^{'})$

$(SN_{T2}, SN_M, j, LogM_4^{'}, Coupon_{Info}, \{SN_{T2}, H(Coupon_M)\}_{-SK_{T2}},$

$U_A| \equiv \#(SN_{T2}, ID_{T2}, i, w_i^{'}, Coupon_{Info})$

$TransferLog_{T2})$

$U_A| \equiv \#(Coupon_{T2})$

$I \ni LogM_4^{'}, Cert_{T2}, PK_{T2}, LogM_3^{'}$

$U_A| \equiv \#(H(ID_{T2}, w_{k+i}, w_k, k, s_k))$

$I \ni \{ID_M, w_{k^{'}+i}^{'}, w_{k^{'}}^{'}, k, s_{k^{'}}^{'}, DS^{'}, LogM_2^{'}\}_{K_{I,B}}$

$U_A| \equiv \#(H(Request))$

$U_A| \equiv \#(\{H(LogM_1, LogM_2)\}_{-SK_{T1}})$

$U_A| \equiv \#(DS)$

$U_A| \equiv \#(\{ID_{T2}, w_{k+i}, w_k, k, s_k, DS, LogM_2\}_{K_{I,A}})$

$U_A| \equiv \#(LogM_1, LogM_3, DS, Cert_{T1})$

$U_A| \equiv \#(LogM_4)$

$U_A| \equiv$

$\#(SN_{T1}, SN_{T2}, i, LogM_4, Coupon_{Info}, \{SN_{T1}, H(Coupon_{T2})\}_{-SK_{T1}})$

$U_A| \equiv \#(TransferLog_{T2})$

$U_A| \equiv \#(Nonce_6)$

$U_A| \equiv$

$\#(\{Coupon_{T2}, TransferLog_{T2}, f(Nonce_5), Nonce_6\}_{+PK_{T2}})$

$U_B \lhd *$

$\{Coupon_{T2}, TransferLog_{T2}, f(Nonce_5), Nonce_6\}_{+PK_{T2}}$

$U_B| \equiv U_A|\sim\#(Coupon_{T2})$ /*Goal 3.4*/

$U_B| \equiv U_A|\sim\#(TransferLog_{T2})$ /*Goal 3.5*/

$U_B| \equiv U_A|\sim\#(Nonce_6)$ /*Goal 3.6*/

$U_B| \equiv \#(\{f(Nonce_6)\}_{+PK_{T1}})$

$U_A \lhd *\{f(Nonce_6)\}_{+PK_{T1}}$

$U_A \ni \{f(Nonce_6)\}_{+PK_{T1}}$ /*T1,P1*/

$U_A \ni f(Nonce_6)$ /*IA,T4*/

$U_A| \equiv U_A \xleftrightarrow{Nonce_6} U_B$

$U_A| \equiv U_B|\sim\#(f(Nonce_6))$ /*Goal 3.8*/

$I \ni (ID_M, w'_{k'+i}, w'_{k'}, k, s'_{k'}, DS', LogM'_2)$

$I \ni DS' \; I \ni \{H(LogM'_1, LogM'_2)\}_{-SK_{T2}}$

$I \ni H(LogM'_1, LogM'_2)$

$I \ni H(H(ID_M, w'_{k'+i}, w'_{k'}, s'_{k'}), LogM'_2)$

$I| \equiv \xrightarrow{+PK_{T3}} U_B$

$I| \equiv U_B| \sim \#(DS')$

$I| \equiv U_B| \sim \#(TransferLog_M)$ /* Goal 4.1*/

$\ni K_{I,B}, TransferLog_M, TransferLog_{T2}$

$I \ni (SN_{T1}, SN_{T2}, i, LogM_4, Coupon_{Info}, \{SN_{T1}, H(Coupon_{T2})\}_{-SK_{T1}})$

$I \ni LogM_4, Cert_{T1}, PK_{T1}, LogM_3$

$I \ni \{ID_{T2}, w_{k+i}, w_k, k, s_k, DS, LogM_2\}_{K_{I,A}}$

$I \ni (ID_{T2}, w_{k+i}, w_k, k, s_k, DS, LogM_2)$

$I \ni DS$

$I \ni \{H(LogM_1, LogM_2)\}_{-SK_{T1}}$

$I \ni H(LogM_1, LogM_2)$

$I \ni H(H(ID_{T2}, w_{k+i}, w_k, s_k), LogM'_2)$

$I| \equiv \xrightarrow{+PK_{T1}} U_A$

$I| \equiv U_A| \sim \#(DS)$

$I| \equiv U_A| \sim \#(TransferLog_{T2})$ /* Goal 4.2*/