A Secure E-coupon System for Mobile Users

Chin-Chen Chang††, Chia-Chi Wu††, Iuon-Chang Lin†††

†Department of Information Engineering and Computer Science Feng Chia University, Taichung, Taiwan
††Department of Computer Science and Information Engineering National Chung Cheng University, Chiayi, Taiwan
†††Department of Management Information Systems National Chung Hsing University, Taichung, Taiwan

Summary
Since nowadays mobile phone messages are flourishing, the application of electronic coupon (e-coupon) will become a trend for mobile users. E-coupon for mobile commerce can provide mobility for users and distribution flexibility for issuers. However, most of the existed e-coupon schemes usually apply public-key cryptosystem to achieve the security, which will not be implemented in mobile devices due to the complex computations. In this paper, we propose a novel mobile e-coupon system that just applies some simple cryptographic techniques, such as one-way hash function and message authentication code. In our system, the issuer can control the number of issued e-coupons and prevent them from double-redeeming. The merchant can verify the validity of the e-coupon and the customers can securely transfer the e-coupon to others. The customer does not need to perform any exponential computation in redeeming and transferring the coupons.

Key words:
e-commerce, e-coupon, mobile commerce

1. Introduction
Issuing coupons is a useful and effective strategy to prompt the customer’s purchase desires to increase sales volume. For example, the on-line store can issue the e-coupon to customers when they browse the web sites, or when they complete their purchases. Conventionally, customers can obtain coupons from Internet and print out such a coupon with printer and redeem them like any other coupon. Differently, the electronic coupon (e-coupon) earlier was defined as [10]: “a customer needs not print e-coupons as they can be captured electronically in an electronic coupon-caddy, and later redeemed electronically.” The idea of e-coupons is raised and we can anticipate that the results of using e-coupons are very obvious.

With the development of SMS (Short Message Service), WAP (Wireless Application Protocol) and MMS (Multimedia Message Services), mobile communications have become very popular around the world, and many applications and services are provided in mobile environment. Thus, if an e-coupon system can allow a customer to receive an e-coupon through his/her mobile device, the customer can not only redeem the coupon over Internet but also can forward this e-coupon to others or merchant through SMS (Short Message Service) or Bluetooth. Thus, the coupon issuer can cooperate with telecommunications industry to carry out marketing activities. Due to this kind of e-coupon is convenient and mobile, hence, that can be applied to E-commerce widely, such as gift certificates, new products promotion, advertisement, and so on. We believe that the e-coupon will soon become a life style for mobile users. A practical e-coupon system must be designed concerning security, efficiency and manageability [11], however, relative researches are few.

Anand et al. [1] designed a distributing e-coupon method in the Internet, they focus on discussing e-coupon content, life cycle and the way distributing the e-coupon to the customer for stimulating her/his purchase desire. Chang et al. [4,5] designed about digital gift certificates and mobile payment mechanisms. Bao designed a kind of digital ticket [3]. He focused on the format of the digital ticket and application cases. Shojima et al. [16] proposed a peer to peer (P2P) e-coupon system. In that system, a service provider provides incentives to mediators who forward e-coupons to potential users. Thus, it is required that the service provider must get the distribution history; nevertheless, the history may be altered in P2P system. They apply the queue structure and some cryptographic techniques to maintain distribution history and prevent altering attack. They use public key cryptosystem that must perform complex exponential computations, it is more suitable to implement in the personal computers and Internet.

However, the conventional e-coupon schemes
may be not suitable for mobile environment. If the e-coupon system can be used in mobile devices, we have to consider the processing cost. According to Rivest and Shamir’s evaluation [15] that hash functions are about 100 times faster than RSA signature verification, and about 10,000 times faster than RSA signature generation. In general, the mobile equipments have small memory space and low computational capability. Thus, a practical e-coupon system for mobile users must be efficiently performed with low computational cost, low communication cost, and small memory space overhead.

In this paper, we proposed a novel complete e-coupon transaction system, which uses the smart card and the hash computations to solve the e-coupon transaction problems with security and processing efficiency, and the whole process can be performed mobility. The rest of this paper is organized as follows. In Section 2, we shall propose the requirements of e-coupon system. Then, in Section 3, we present our proposed system, followed by some discussions as to how the new system performs in terms of security and efficiency in Section 4. Finally, a concluding remark will be given in Section 5.

2. The Requirements of the e-coupon system

The e-coupon system must satisfy the following requirements to achieve security and manageability.
1. Identification: Each e-coupon must be identified its ownership so as to prevent the attacker masquerading as eligible owner to consume it.
2. Transferability: Each e-coupon can be transferred among customers, but the original owner must authorize it.
3. Unforgeability: Only issuer can offer valid e-coupons, any other entities cannot forge them.
4. Non-repudiation: Each entity cannot deny the transactions in which she/he has participated.
5. Expired: E-coupon can set expired date [6,7].
6. States manageability [8,9]: Whether the e-coupon is consumed or not must be considered in the system.
7. Independence: E-coupon system can be implemented in heterogeneous platforms.

Fig. 1 The e-coupon system mode

3. The Proposed Scheme

In this section, we will propose a secure e-coupon system for mobile users. Generally, if the enterprises want to increase sales, they might make effort in sales promotion: for example, give some coupons when the customer buys a considerable amount of merchandises or services. However, they must issue coupons in a limited number, or sales revenue will be reduced. Therefore, we simply construct the e-coupon model as Fig. 1.

In this model, the issuer, such as enterprise headquarter or manufacture, issues and controls the number of coupons; the branch stores (the service providers) provide the merchandises or services for customers when they redeem the coupons. Besides, the customer may redeem the coupon using the mobile device, so low computation power and communication capabilities must be considered in the customer end. On the other hand, the issuers do not want the coupons to be suffered from forging, which will result in great damage. The e-coupon system can be divided into four phases: registration phase, issuing phase, redemption phase and transferring phase. We first explain the notations in Section 3.1, and then, describe the proposed system in Section 3.2.

3.1 The notations

We divide notations into four parts such that we can observe clearly that each entity must maintain parameters and store information. The public parameters and computation functions are listed as follows.

CertA: Certification for entity A.
b: The identification number for service provider Sb.
W: The upper bound of the service provider’s identification number.
When ISU determines to issue an e-coupon to the customer, he must notify and deliver related messages to ISU for verifying. In this phase, all messages can be transferred in a public channel. This phase performs communications as in Fig. 2.

1. First, ISU sends \((W, \text{EXD})\) to \(C_i\) and notifies her/him to get the coupon. \(C_i\) generates four random numbers \(\alpha_1, \alpha_2, \alpha_3, \alpha_4\) and sets \(D=|H^{\alpha_1}(\alpha)|H^{\alpha_2}(\alpha)|H^{\text{EXD}}(\alpha_1)|H^{\text{EXD}}(\alpha_3)|\). Then, \(ISU\) computes \(E_k[\alpha_1, \alpha_2, \alpha_3, \alpha_4, D]\) and sends the outcome to \(ISU\).

2. Once receiving the above message, \(ISU\) decrypts it using the key \(k_i\) to get \(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, D\}\). Then, \(ISU\) computes \(H^\alpha(\alpha_1), H^\alpha(\alpha_2), H^{\text{EXD}}(\alpha_1), H^{\text{EXD}}(\alpha_3)\) and compares the result with the received \(D\). If they are equal, \(ISU\) generates the \(\text{SN}\) to set \(m = |\text{SN}|D\) and computes \(s'=\text{Sign}_{\text{ISU}}(|H(m)|)\) and delivers \(|\text{SN}, s\rangle\) to \(C_i\).

3. \(C_i\) computes \(H(|\text{SN}|D)\) and uses \(ISU\)'s public key to get \(H(m)\) from \(s\). If they are equal, \(C_i\) can make sure that she/he has gotten the coupon \(|\{m, s\}\rangle\).

**Redemption phase**

In this phase, \(C_i\) can redeem the coupon to exchange proper services to the service provider. \(S_b\). \(S_b\) can verify the coupon, and prevent double spending through checking redeemed e-coupons by \(ISU\). All the communications can be performed via a public channel as in Fig. 3, since the messages are protected and verified.

1. If \(C_i\) wants to redeem the coupon, she/he computes \(\beta_1=H^\alpha(\alpha_1), \beta_2=H^\alpha(\alpha_2), \beta_3=H^{\text{EXD}-\text{NOF}}(\alpha_1), \beta_4=H^{\text{EXD}-\text{NOF}}(\alpha_3)\) and then sends \(|\text{EXD}, \beta_1, \beta_2, \beta_3, \beta_4, \text{coupon}\rangle\) to \(S_b\). \(S_b\) can verify the signature \(s\) using \(ISU\)'s public key. If it holds, then the coupon is valid. \(S_b\) must forward \(|\text{EXD}, \beta_1, \beta_2, \beta_3, \beta_4, \text{coupon}\rangle\) to \(ISU\).

3. \(ISU\) uses the received information to compute \(y_1=H^{\beta_1}(\beta_1), y_2=H^{\beta_2}(\beta_2), y_3=H^{\text{EXD}-\text{NOF}}(\beta_3), \) and \(y_4=H^{\text{EXD}-\text{NOF}}(\beta_4)\). After completion, \(ISU\) then executes the following two checking:

   1. She/he computes \(H(|\text{SN}|y_1|y_2|y_3|y_4|y)|\) which can be verified by the signature \(s\) using \(ISU\)'s public key. If
it holds, then ISU checks whether this SN exists in Redeemed table, else notifies Sb that the transaction does not pass the validation checking.

(2) If SN does not appear in Redeemed table, ISU must record it into Redeemed table and deliver the valid information to Sb, or else ISU notifies Sb that this coupon is redeemed.

4. After Sb receives the valid response from ISU, Sb must provide the merchandises or services to Ci according to the coupon declared.

5. If the coupon passes the ISU validation, Sb must keep the coupon for settling the account with ISU to obtain subvention.
that Ci and Cj are registered already, this phase changing the signature of the coupon. Assuming since Cj cannot know the transferred coupon’s status (unredeemed/redeemed), this coupon must be transferred to ISU for checking its status and changing the signature of the coupon. Assuming that Ci and Cj are registered already, this phase performs communications as Fig. 4, we describe the procedures as follows.

1. Ci delivers a transfer request to Cj. Once receiving the request, Cj immediately transmits Eki(coupon||CIDj) to ISU.

2. When ISU receives the message, she/he can decrypt it using kj and verify validation of the coupon via signature s. If they are valid, then ISU checks Redeemed table to confirm this coupon has not been redeemed.

3. ISU generates four random numbers (γ1, γ2, γ3, γ4) to compute Hb(γ1), Hb(γ2), HExD-NOW(γ3), and HExD-NOW(γ4), and s'=SignSN[Hb(SN)||Hb(γ1)||Hb(γ2)||HExD-NOW(γ3)||HExD-NOW(γ4)]. Then, ISU transfers {Ekj(γ1, γ2, γ3, γ4)||SN||s'||Hb||HExD-NOW} to Cj.

4. Upon receiving the above message, Cj decrypts the (γ1, γ2, γ3, γ4) using the key kj. At last, Cj computes H(m')=H(SN)||Hb(γ1)||Hb(γ2)||HExD-NOW(γ3)||HExD-NOW(γ4) to verify the signature s’ using ISU’s public key. If it holds, the coupon (m’, s’) is confirmed to be transferred.

4. Security and Practicability

Discussion

In this section, we analyze the security and efficiency of our e-coupon system. The security requirements are explained in Section 4.1. The performance is discussed in Section 4.2.

4.1 Security Discussions

This system can satisfy the security characteristics as follows.

1. Confidentiality: The system protects the secure parameters (ISU, α1, α2, α3, α4) using symmetric encryption scheme from eavesdropping.

2. Verifiability:

   (1) The coupon can be verified by any entity, since s was signed by ISU.

   (2) ISU can easily validate the Redemption date and Sb’s identification number, because (α1, α2, α3, α4) are secret and the hash values are unique and not reversible. If Sb tampers b, she/he will lose the subvention from ISU. Without knowing (α1, α2, α3, α4), the attacker cannot tamper Hb(α1), Hb(α2), Hb(α3), or HExD-NOW(α4).

3. Preventing forgery: The coupon is not forged, because it must be signed by ISU. Anyone else is unable to get the ISU’s private key.

4. Preventing alternation:

   This system can prevent two kinds of alternation attack:

   -- No one can change the content of the coupon, since it is signed by ISU.

   -- The service provider Sb cannot change Hb(α1), Hb(α2), Hb(α3), or HExD-NOW(α4), because she/he can not get (α1, α2, α3, α4).

5. Preventing duplicate-redemption: ISU can collect each SN of the redeemed coupon. If a customer repeatedly redeems it, ISU will find out immediately.

6. Preventing reproduction: If the malicious customer reproduces the coupon that will not be feasible, since both the coupon and owner have been signed by ISU.

7. Non-repudiation:

   (1) In issuing phase, the customer generates [α1, α2, α3, D] and ISU signs the coupon, so that they can not deny them.

   (2) In redemption phase, Sb gets the (EXD, β1, β2, β3, β4, coupon) from Cj and ISU stores

Fig. 3 The protocol of redemption phase

Fig. 4 The protocol of transferring phase
the redeemed $SN$ of the coupon. The customer thus cannot to deny this redemption, since the customer knows $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. ISU will not generate a fake coupon, though he/she got $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Because ISU is a payer in this scenario, the fake coupon will damage ISU's profit.

3. In the coupon transferring, ISU can manage the transferring process to achieve non-repudiation between $Ci$ and $Cj$.

8. Expired: E-coupon uses $H^{EXD}(\alpha_4)$ and $H^{EXD}(\alpha_4)$ to set expired date. When the customer uses the coupon out of the expired date, he/she will not to redeem it, because he/she can not generate $\beta_i=H^{EXD-NOW}(\alpha_4)$. If he/she changes $EXD$ to generate $\beta_i'=H^{EXD-NOW}(\alpha_4)$, then $Sb$ computes $x'=H^{NOW}(\beta'_i)$ will not be equal to $H^{EXD}(\alpha_i)$ of the $D$.

9. States manageability: ISU can easily manage the status of the coupon, because he/she has redeemed table to collect $SN$ of the redeemed coupon.

4.2 Efficiency analyses

1. Computation efficiency: In redemption phase, the customer only computes hash values. In coupon transferring, the original customer performs symmetric encryption, unlike a public key system that needs a great deal of computation resources. According to Xiao et al.'s measurement [17], DES [12] computation is about 1000 times faster than RSA [13] computation. This system can be implemented in mobile phone or PDA, since customers do not perform any exponential computations in the redemption phase.

2. Controllability: The ISU can control the number of $SN$s that issued, which can avoid damaging estimated profits.

3. Trust manageability: In the coupon transferring, ISU can manage the transaction and check coupon content to achieve reliability for customers.

5. Conclusions

In this paper, we have proposed the first secure electronic coupon system for mobile users. In our system, the e-coupon can be applied to e-commerce flexibly and securely. The issuer can control the number of issued coupons and prevent double spending. Furthermore, the coupon can be verified by anyone to prevent forging attack. According to the analyses above, our system's computation cost is less than that of public key system, which is more practical and convenient for applications using mobile devices or smart cards.

References


Chin-Chen Chang received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, a Fellow of IEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Chia-Chi Wu was born on December 9, 1967 in Taoyuan, Taiwan, Republic of China (ROC.). He received the B.S. in Information Management from National Defense Management College, Taipei, Taiwan, Republic of China, in 1991; the M.S. in Information Management from National Defense Management College, Taiwan, in 1999. He is currently pursuing his Ph.D. degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Iuon-Chang Lin was born on December 21, 1974 in Taipei, Taiwan, Republic of China (ROC.). He received the B.S. in Computer and Information Sciences from Tung Hai University, Taichung, Taiwan, Republic of China, in 1998; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 2000. He received his Ph.D. in Computer Science and Information Engineering in March 2004 from National Chung Cheng University, Chiayi, Taiwan. From 2004 to 2005, he was an assistant professor of the Department of Information Management, National Kaohsiung University of Applied Sciences, Taiwan, ROC. He is currently an assistant professor of the Department of Management Information Systems, National Chung Hsing University, Taichung, Taiwan, ROC. His current research interests include, but not limited to, electronic commerce, information security, cryptography, neural networks, and electronic image processing.