A Non-Sequential Unsplittable Privacy-Protecting Multi-Coupon Scheme

Alberto N. Escalante B. Hans Löhr Ahmad-Reza Sadeghi

Horst Görtz Institute for IT Security, Ruhr-University of Bochum, Germany
{eban|loehr|sadeghi}@crypto.rub.de

Abstract: A multi-coupon (MC) represents a collection of k coupons that a user can redeem to a vendor in exchange for a *benefit* (some good or service). Recently, Chen et al. [CEL+07] proposed an unforgeable privacy-protecting multi-coupon scheme (MCS), which discourages sharing of coupons through a property called *unsplittability*, where the coupons of a single MC cannot be separately used by two users. Previous MCSs relied on the *all-or-nothing principle*, a weaker form of unsplittability, where sharing a single coupon implies sharing the whole multi-coupon. The construction proposed in [CEL+07] supports coupons with practical attributes: independent benefits, and validity periods (e.g., expiration dates). However, it has the disadvantage that the coupons contained in an MC must be redeemed in *sequential order*. Hence, it is suitable for fewer applications. In this paper, we address this problem and propose a scheme that satisfies the same set of security requirements, supports the same practical attributes, and offers similar efficiency, but in which users are able to choose which coupon they redeem.

Keywords: Coupon, privacy, unsplittability, unlinkability, non-sequential.

1 Introduction

Coupons are a powerful and versatile marketing tool widely used by manufacturers, retailers, and advertisers to manipulate the buying behaviour of their current and potential customers. Coupons are fundamental in marketing strategies because they can be employed [KRJM98] to make potential customers aware of the existence of a product, to attract customers to the shop (to increase overall sales), to increase sales in specific seasons, and to bind different products in a package. A coupon is a document (in printed or electronic form) that gives a *customer* the right to claim a good or service (e.g., a gift or a reduction) from the issuer, called *vendor*.

A *multi-coupon* (MC) [CES+05, Ngu06, CEL+07] denotes a collection of e-coupons that is handled as a single unit. In general, the procedure in which the vendor provides (e.g., sells) a coupon to a customer is called *issue*. In the *redeem* procedure, a customer holding a coupon interacts with the vendor to claim the benefit (a.k.a. coupon's object [CEL+07]) implied by the coupon. Here, the vendor verifies that the coupon is valid (i.e., that the

preconditions to use the coupon are fulfilled) and authentic (i.e., that the coupon was not tampered with). A typical application of MCs are electronic discount booklets.

In this paper we consider a *multi-coupon scheme* (MCS) that protects the privacy of the customers, and encourages their loyalty by providing *unsplittability* [CES+05], i.e., two users cannot redeem coupons from the same MC separately and independently. Kumar et al. [KRJM98] distinguish two central properties that should be considered when developing a coupon-based system: *targeting* and *distribution*. *Targeting* is the capability of the coupon system to select which customer should receive a coupon. For instance, a vendor might only be interested in giving discount coupons precisely to those users who would not buy a product without it. *Distribution* measures how much restrictions are imposed on the number of coupons distributed. Each application requires a particular level of targeting and distribution. In this paper we focus on *targeted* coupons with *limited distribution*. When dealing with an MCS we must consider attacks in which different users collude and attempt to "split multi-coupons" (decreasing the targeting level), or to forge coupons (which violates the limited distribution goal). This justifies the need for unsplittable and unforgeable MCSs. Moreover, in the digital world anonymity of customers becomes more important since the vendor may try to infer and store additional information about them. This might harm privacy and allow client profiling and price discrimination [Odl03], e.g., different customers are offered the same goods by the same vendor, but at different prices.

Contribution and Organization. We start in Section 2 with the description of previous work on multi-coupon schemes. In Section 3, we recall the syntax and security properties required from an MCS. Thereafter, we propose in Section 4 the first construction of a non-sequential unforgeable and unsplittable privacy-protecting MCS, which is more useful to the customers because they can redeem their coupons in whatever order they prefer. Our construction satisfies the requirements established in [CEL+07], provides the same features for practical applications, and has a similar efficiency. Finally, we conclude in Section 5.

2 Previous Work on Multi-Coupon Systems

Syverson et al. [SSG97] introduced the concept of "unsplittability" in the context of unlinkable serial transactions to discourage sharing, and suggested an (abstract) extension of their scheme to implement coupon books (i.e., multi-coupons).

Later, Chen et al. [CES+05] described the properties that a privacy-protecting multi-coupon system should provide, justified the use of unsplittability over other means to discourage sharing (e.g., hiding credit card numbers in the multi-coupons), and proposed the first concrete construction of an MCS.

Recently, Nguyen [Ngu06] addressed some disadvantages of [CES+05], and defined a security model for MCSs, followed by an efficient construction. Its issue and redeem complexity is constant w.r.t. the number of coupons, it offers the same security properties as in [CES+05], and adds a new feature to *revoke* multi-coupons.

More recently, Chen et al. [CEL+07] defined a more precise security model for MCSs than the one in [Ngu06] requiring unsplittability instead of the all-or-nothing principle.

Accordingly, they propose a construction that satisfies the new requirements, and that provides additional features for practical applications: independent benefits and validity periods (e.g., expiration dates) for each coupon within an MC. This construction has the peculiar property that the coupons contained in a multi-coupon must be redeemed sequentially.

As previously explained in [CES+05, Ngu06], most related schemes (e.g., e-cash, digital credentials) cannot be employed as privacy-protecting unsplittable MCSs because they have different usage patterns, are inefficient in this setup, or lack at least one of the required properties, in particular unsplittability. Some e-cash systems can be used as unlinkable or at least anonymous MCSs (e.g., [CGH06]). However, they achieve at most all-or-nothing sharing, not unsplittability.

3 A Security Model for Multi-Coupon Schemes

In this section we briefly present the security framework for unsplittable multi-coupon schemes. For a more detailed treatment, we refer the reader to [CEL+07]. A *multi-coupon scheme* (MCS) is defined by an initialization algorithm `Setup`, which is executed by the vendor only once, and by a pair of interactive protocols: `Issue`, and `Redeem`. As a result of a successful execution of the `Issue` protocol, the customer obtains an MC with k coupons. In the `Redeem` protocol, a customer uses her MC to redeem a coupon, and to obtain an updated MC. An MCS is *correct* if any honest customer who obtains an MC from a fresh honest vendor succeeds at redeeming every coupon contained in the MC.

We focus on *unforgeability*, *unlinkability*, and *unsplittability* because, as pointed out in [CGH06, CES+05, Ngu06], these are the essential properties of an MCS.

Unforgeability. There is an intrinsic monetary value associated to any coupon, either explicitly or implicitly. Moreover, coupon cloning might spoil the vendor's distribution strategy (as any customer might illegally obtain coupons). Therefore, vendors want their multi-coupons to be *unforgeable*, in the sense that no coalition of customers with χ_C coupons in total (comprised in, say, m multi-coupons), should be able to redeem χ_R coupons, with $\chi_R > \chi_C$.

Unlinkability. This property ensures anonymity of customers. It requires that it is infeasible for a vendor to link a redeem procedure made by a customer to the corresponding issue procedure, or to link two different redeem procedures executed by the same customer (significantly better than by a random guess).

Unsplittability. *All-or-nothing sharing*, also known as *weak unsplittability* (WU) [CES+05], intuitively, requires that whenever a user intends to share a single coupon with a second user, she has to provide her with *all* the secret information related to the MC. Thus, in case that both users do not trust each other, WU discourages sharing.

A stronger version, called *(ordinary) unsplittability*, requires that it is infeasible for a coalition of customers to produce more *autonomous* redemption algorithms than the number of MCs it has rightfully obtained, where by autonomous we mean that such algorithms do not share any information gained during the redemption. This implies that if a customer

gives a single coupon to a second customer, then that second customer has to send back some information to the first one after redeeming; otherwise the first customer cannot spend further coupons from such an MC. Hence, sharing is more cumbersome with this stronger version of unsplittability than with weak unsplittability because it requires a trust relationship and additional interaction between the customers.

4 Description of our Multi-Coupon Scheme

We propose an unsplittable privacy-protecting MCS where coupons can be redeemed by a customer in any order. The scheme can be easily extended with arbitrary attributes for each coupon, which might be used to implement purchase restrictions, additional rewards, and expiration dates. This construction is useful, e.g., to implement a personalized electronic discount booklet, where a vendor can offer variable discounts for different products.

Our scheme utilizes a digital signature scheme with efficient protocols that allows to obtain a signature on a (partially) blinded tuple (i.e., some elements of the tuple are disclosed, while others are only committed to), and to prove the knowledge of a signature on a (partially) blinded tuple without disclosing any useful information, other than the fact that the signature is valid. An example of such a signature is [CL02].

In our scheme, each single coupon $C \stackrel{\text{def}}{=} (id, be, \sigma)$ is specified by a coupon's identifier id, a coupon's benefit be, and a signature σ on the triple (id, be, mc), where mc is the multi-coupon's identifier. A multi-coupon of size k with multi-coupon identifier mc is a list of k single coupons $\{(id_1, be_1, \sigma_1), \ldots, (id_k, be_k, \sigma_k)\}$ sharing the same value mc, and a signature σ' on the pair (fr, mc), where fr is the multi-coupon's freshness identifier. A valid coupon can only be used in conjunction with an unused multi-coupon's freshness fr and a valid signature σ'. In the *issue* protocol, the customer obtains a multi-coupon, where the multi-coupon's freshness identifier fr and each coupon identifier $id_1, \ldots, id_k$ are chosen and kept private by the customer. The other fields: σ', $be_1, \ldots, be_k, \sigma_1, \ldots, \sigma_k$ are known by the vendor. During the *redemption*, the customer chooses an unused coupon, say the j-th single coupon $C_j \stackrel{\text{def}}{=} (id_j, be_j, \sigma_j)$. She proves that the coupon has never been used before (by disclosing id_j), that it is indeed redeemable (by proving knowledge of a signature σ_j on (id_j, be_j, mc)), that the multi-coupon is fresh (by disclosing fr and proving knowledge of a signature σ' on (fr, mc')), and that the coupon belongs to the multi-coupon (by proving that mc equals mc'), where the value mc is never disclosed to the vendor. Finally, the customer interacts with the vendor to generate a new freshness identifier $fr^\star$, and to obtain a signature $\sigma'^\star$ on the pair $(fr^\star, mc)$.

It can be shown that our construction is unforgeable and unsplittable. If the coupon benefits be are constant, then the construction is also unlinkable. Otherwise, in an extreme scenario, the vendor can track his customers by assigning unique benefits to each of them. In practice, the customer's privacy is protected if there is only a small set of benefits, which are employed by several customers. Intuitively, *unforgeability* relies on the security of the underlying signature scheme (CL signatures). *Unlinkability* is ensured by the zero-knowledge property of the proofs of knowledge we use. *Unsplittability* is achieved by including a multi-coupon identifier mc in the signed messages – of course, here we also

rely on the security of the underlying signature scheme.

The redeem complexity (both computation and communication) is constant w.r.t. the size k of the multi-coupon (i.e., the number of coupons it contains), and the complexity of the protocol for issuing multi-coupons is linear in k, which is the best we can aim to when each coupon has individual attributes.

5 Conclusion and Future Work

In this paper, we introduced a simple construction of a privacy-protecting multi-coupon system, which is unsplittable, but at the same time allows non-sequential redemption of coupons, and thus, proves that the unsplittability property does not imply sequentiality. Unlike alternative approaches, unsplittable multi-coupons do not require the encoding of any valuable information into the coupons to discourage the customers from sharing them. Therefore, it can be considered more privacy-friendly. Moreover, the coupon's structure can be extended with additional fields, which can indicate additional conditions to use the coupons (e.g., a minimum purchase requirement), an expiration date, or an additional reward (e.g., bonus points).

An open problem is to design an MCS with the properties above, but suitable for more general scenarios, such as for a federation of (collaborative) vendors.

References

[CEL+07] Liqun Chen, Alberto N. Escalante B., Hans Löhr, Mark Manulis, and Ahmad-Reza Sadeghi. A Privacy-Protecting Multi-Coupon Scheme with Stronger Protection against Splitting. In *Financial Cryptography*, LNCS. Springer Verlag, 2007. (To appear).

[CES+05] Liqun Chen, Matthias Enzmann, Ahmad-Reza Sadeghi, Markus Schneider, and Michael Steiner. A Privacy-Protecting Coupon System. In *Financial Cryptography*, volume 3570 of *LNCS*, pages 93–108, Berlin, 2005. Springer-Verlag.

[CGH06] Sébastien Canard, Aline Gouget, and Emeline Hufschmitt. A Handy Multi-coupon System. In *Applied Cryptography and Network Security, ACNS*, pages 66–81, 2006.

[CL02] Jan Camenisch and Anna Lysyanskaya. A Signature Scheme with Efficient Protocols. In *Third Conference on Security in Communication Networks – SCN'02*, number 2576 in LNCS, pages 268–289. Springer Verlag, 2002.

[KRJM98] M. Kumar, A. Rangachari, A. Jhingran, and R. Mohan. Sales Promotions on the Internet. In *Third Usenix Workshop on Electronic Commerce*, pages 167–176, 1998.

[Ngu06] Lan Nguyen. Privacy-Protecting Coupon System Revisited. In *Financial Cryptography*, number 4107 in LNCS, pages 266–280. Springer Verlag, 2006.

[Odl03] Andrew Odlyzko. Privacy, economics, and price discrimination on the Internet. In *ICEC '03: Proceedings of the 5th international conference on Electronic commerce*, pages 355–366, New York, NY, USA, 2003. ACM Press.

[SSG97] Paul F. Syverson, Stuart G. Stubblebine, and David M. Goldschlag. Unlinkable Serial Transactions. In *Financial Cryptography*, number 1318 in LNCS, pages 39–56. Springer Verlag, 1997.