A Privacy-Friendly Loyalty System for Electronic Marketplaces

Matthias Enzmann and Markus Schneider
Fraunhofer Gesellschaft (FhG), Institute for Secure Telecooperation (SIT)
Dolivostr. 15, D-64293 Darmstadt, Germany
firstname.lastname@sit.fraunhofer.de

Abstract

Loyalty systems provide an interesting possibility for vendors in customer relationship management. This holds for both real world and online vendors. Beside potential benefits of loyalty systems, customers may fear an invasion of privacy, and thus often refuse to participate in such programs. In this paper, we present two variants of a privacy-friendly loyalty system to be used by online vendors for issuing loyalty points. The systems prevent vendors from exploiting data for the creation of customer profiles by providing unconditional unlinkability of loyalty points with regard to purchases. We propose a simple token-based approach and a counter-based approach which is much more efficient while preserving the privacy and security properties. Furthermore, the counter-based loyalty system prevents pooling of loyalty points issued to distinct customers.

1. Introduction

In recent years, the World Wide Web has evolved to a business platform with worldwide reach and 24h/7 service for selling various kinds of goods. Presently, more than 600 million people have access to this business platform and thus, are potential customers for online vendors. Naturally, every online vendor’s interest lies in attracting new customers and creating a large base of loyal customers. Since loyal customers create regular revenues, the goal of online vendors, as well as real-world vendors, is to turn occasional customers into loyal ones. Thus, in the past, online and real-world vendors have introduced loyalty programs, e.g., frequent flyer programs, in order to retain customers.

Aside from customer retention, another incentive for vendors is to learn more about their customers to exploit this information for purposes like customer profiling, data mining, or direct marketing. Thus, from the customer’s perspective, loyalty programs have two sides. On the one hand, customers value the financial benefits, on the other hand, they may fear an infringement of their privacy. Hence, if privacy concerns outweigh the expected benefits from the loyalty program the vendor’s strategy for attracting and retaining customers will fail. Thus, if privacy is a barrier for customers to participate in the program, it may be worthwhile for vendors to reconsider their strategy of collecting personal data. Indeed, according to [9, 10], there are many customers that are concerned about their privacy in electronic commerce scenarios. Therefore, privacy non-invasive loyalty systems might be of particular interest to vendors.

In this work, we are dealing with loyalty systems in which customers receive points from vendors for their purchases. Points can be redeemed at the vendor’s in exchange for a reward, whereas the value of the reward depends on the number of points.

In order to enhance privacy for the customers, the vendor must not be able to generate consumer profiles by linking customers’ transactions through the loyalty program. Thus, it is our goal to prevent the vendor from using loyalty points to link any two customer transactions. Hence, when points are handed in by the customer, it is not possible for the vendor to determine the purchases in which the points were obtained. Of course this is only meaningful if there is no other linking information available to the vendor outside the loyalty system. In addition to unlinkability of points to transactions, there are security requirements with respect to unforgeability of points and preventing that the same points are redeemed more than once. Another aspect, which is potentially relevant for vendors, is to prevent distinct customers from pooling their loyalty points in order to add up their collected points for redemption. At first glance, one might think that the unlinkability of customer transactions through loyalty points and the prevention of pooling is contradictory. However, it is not. The proposed counter-based loyalty system fulfils both requirements. Both variants of the privacy-friendly loyalty system presented here are based on the usage of blind signatures as proposed by Chaum [5]. We propose a token-based and a counter-based solution in which blind signatures are iteratively applied. The proposed loyalty systems provide unconditional unlinkability of loyalty points with regard to purchases.

The paper is organised as follows. Section 2 gives some background on loyalty systems. In section 3 we define es-
sential privacy and security requirements for a point-based loyalty system. In Section 4, we sketch both variants for loyalty systems. In Sections 5 and 6, we present a simple token-based loyalty system and a refined counter-based variant, respectively, including their specific properties. Related work is discussed in section 7, before we draw some conclusions.

2. Loyalty programs

A loyalty program is a structured marketing effort which rewards, and therefore encourages, loyal behaviour of customers, which is presumably beneficial to the vendor [16]. We say that a customer is loyal if she has a strong attitude to a certain vendor over its competitors. The motivation of vendors for adopting a loyalty program is, in general, twofold. First, vendors want to retain present customers and stimulate repeated purchase behaviour which would guarantee regular future earnings. And second, they want to learn more about their customers in order to refine their business strategy.

In general, the basic conditions for loyal customer behaviour in the real world are different from the electronic world [13]. Connecting to a vendor’s site is as easy as connecting to its competitor’s site. This is in contrast to the real world where barriers exist, such as geographical distance or an existing inter-personal relationship between customer and shop personnel, that may prevent customers from instantly switching vendors. Thus, online vendors must be even more interested in loyalty programs than their real-world counterparts.

There are different types of loyalty programs, e.g., rewarding systems and virtual communities. In general, rewarding systems give program members a financial incentive. They can be classified according to the point in time the reward is given with respect to a purchase. There are immediate and delayed rewarding systems. Examples for immediate rewarding systems are price promotions or rebates through membership credit cards; candidates for delayed rewarding systems are point collecting programs like frequent flyer miles or “buy 10 get one free”. Virtual communities focus on social and service aspects, e.g., online discussion panels on product related problems.

There are some variants for point-based loyalty programs. The number of points awarded to the customer may depend on the monetary value of a purchase, e.g., one point for each Euro spent, or it may depend on specific types of products, e.g., after having bought 10 mp3 files one can download one for free. Furthermore, we can categorize point programs according to the way points are collected. In a token-based approach, for each awarded point a token is issued, e.g., chips issued by a supermarket, while in a counter-based approach the number of points to be obtained is added to the current point balance, e.g., frequent flyer miles.

Members of loyalty programs have a greater propensity to be loyal to the vendor and also have an increased usage frequency compared to non-members [16]. Furthermore, it can be assumed that members are less willing to try offers of competing vendors, even when negative experiences with the vendor occur since these effects are moderated by the loyalty program membership [1]. According to [6], loyalty program members are also less price sensitive, spend more money and are more likely to pass on positive recommendations than non-members.

The customer information gathered in loyalty programs can be used by the vendor for direct marketing, data mining, and customer profiling in order to promote products, infer new customer data, and optimise their range of products, respectively. This means that vendors have a large consumer database where they record every single transaction of their customers. Thus, common loyalty programs do not look so bright anymore from the customer’s perspective since they may see this monitoring as an invasion to their privacy. In this context, customers may fear to lose control over their personal data, since vendors may disclose their data to other parties. Clearly, customer loyalty strongly depends on the customers’ trust in the vendor. Thus, if customers are convinced that they participate in a privacy-friendly loyalty program their loyalty may even increase.

In this paper, we propose point-based loyalty systems which may lead to increased customer loyalty due to enhanced privacy. At present, there are no other proposals for loyalty systems, the authors are aware of, which offer a comparable level of privacy.

3. Requirements

When designing an electronic loyalty system, both customers’ and vendors’ interests need to be taken into account. There are requirements such as customer privacy and security regarding the unforgeability of loyalty points that must be considered. In the following, we describe requirements that a loyalty system must fulfill.

Privacy. Customers have the fundamental requirement to protect their privacy. In our context, this means that it should not be possible for the vendor to create customer profiles from the awarding and redeeming processes of loyalty points. More precisely, it should not be possible for the vendor to link any two customer transactions by means of the loyalty system. This includes both awarding or redeeming transactions. Specifically, given a redeeming transaction, the vendor should be prevented from linking it to the corresponding awarding transactions and to other redeeming transactions of the same customer. And likewise, given an awarding transaction, the vendor cannot link it to awarding and redeeming transactions of the same customer. Note that we focus only on the loyalty systems’ properties that are necessary to achieve unlinkability. Clearly, linkability
may be possible outside the loyalty system. However, preventing this is out of scope of this work. In order to achieve unlikeliness for electronic purchases in general, additional technologies have to be used, e.g., unlikeliness of search and order phases proposed in [8], payment systems that allow the customer to remain anonymous with respect to the vendor [5, 2], anonymity networks as in [3, 14], or privacy-friendly delivery in case of hard goods similar to the approach proposed in [7].

**Security.** The security requirements considered here can be summarised as system integrity. The property of system integrity in the context of a point-based loyalty system means that no other party beside the vendor should be able to increase the number of a customer’s loyalty points, i.e., the customer must not have more points than awarded to her by the vendor. We have three aspects of system integrity that need to be considered.

**Unforgeability.** Loyalty points may only be created by the vendor himself, i.e., customers should not be able to produce them. At the very least, the vendor should be able to tell false points from genuine ones.

**Double-spending detection.** In contrast to real-world loyalty points, their electronic counterparts can be easily copied and are indistinguishable. As a consequence, parties may try to hand in copies of loyalty points at the vendor’s. Thus, we require that it must be detectable whether loyalty points have been spent before.

**Pooling prevention.** Vendors expect customers to individually achieve some redeeming threshold. Thus, their interest lies in preventing customers from pooling loyalty points to reach the required threshold earlier or to reach a higher threshold in order to receive a more valuable reward. This means it should not be possible that, say, two customers, each having a counter of 5 loyalty points, can transform their individual counters into a joint one worth 10 points. Note that this is different from the problem of customers sharing a counter which, in general, cannot be prevented in systems with perfect privacy.

### 4. Electronic loyalty systems

In this section, we start by informally describing how the variants of the electronic loyalty systems work. In order to point out the advantages of the counter-based system over ad hoc solutions based on electronic coin systems, we will compare it to such systems. Henceforth, we will refer to coin systems as token-based systems, in contrast to the counter-based system proposed here. As an example for a token-based system we consider a scheme that is based on the idea proposed by Chaum [4], which uses blind signatures, and compare it to our scheme.

The main difference between a token-based system and our proposed counter-based system is that customers have to keep a token for every point issued to them, while in the counter-based system they have to keep only one token which represents a counter that is increased for every point issued to the customer. Figure 1 sketches the issue process for both types of loyalty systems, where the tickets represent the aforementioned tokens.

In the token-based scheme as well as in the counter-based scheme a random serial number $s_i$ and $s$, respectively, is chosen by the customer which identifies the ticket holding the customer’s point(s). This serial number is used by the vendor within the redeem phase in order to determine whether the ticket has been handed in before. In the counter-based scheme a single serial number $s$ is sufficient for collecting, e.g., $m$ loyalty points while in the token-based approach $m$ different serial numbers $s_1, \ldots, s_m$ are needed.

In both schemes, the ticket’s serial number must be hidden from the vendor to prevent him from linking the ticket to a particular issue step. This is necessary because a point, i.e., a ticket, is given to customers as a reward for their purchases and therefore the ticket’s serial number, if not hidden from the vendor, can be used to uniquely identify a certain purchase. Thus, in the token-based approach, the vendor would learn that $m$ certain purchases, identified by the tickets’ serial numbers, were made by the same person as soon as that person hands in her collected tickets, allowing the vendor to *a posteriori* create a profile for this customer. In the counter-based approach, protecting the customer’s privacy might be even more demanding, since the ticket’s serial number is always the same for all counter values. Thus, the vendor could easily build a purchase-by-purchase customer profile, based on the serial number, whenever another loyalty point is added to the customer’s ticket.

In order to prevent such building of customer profiles, the customer blinds her ticket before sending it to the vendor to hide her serial number from the vendor’s eyes — in the counter-based approach, this blinding also hides the current count of the ticket. In the next step, the vendor digitally signs the ticket given to him, without knowing its content — he will learn the ticket’s content only after it is handed in by the customer. In the counter-based scheme, the vendor increases the ticket’s counter by signing it (for the details see section 6). The signing itself is actually the ‘core’ issue step of a loyalty point and also serves to protect the ticket from unnoticeable tampering. The ticket is then returned to the customer who unblinds it and after that owns a ticket worth one (additional) loyalty point. The ticket is then returned to the customer who unblinds it and after that owns a ticket worth one (additional) loyalty point. Figure 1(a) shows that in the token-based approach $m$ different tokens, i.e., tickets, must be generated and stored by the customer in order to collect $m$ loyalty points. In Figure 1(b), it can be seen that in the counter-based approach only one ‘token’ needs to be generated and stored in order to hold $m$ loyalty points. If more than one point, e.g. $k$ points, is to be issued at once, the counter’s advantage becomes even more appar-
In this case, the vendor merely has to change the addend from 1 to \( k \) which means no additional effort for him. However in the token-based approach, the customer would practically have to go through \( k \) issuing processes, considerably reducing efficiency for both the customer and the vendor.

One could think of improving the efficiency of the token-based scheme by issuing tickets of higher values, e.g., tickets worth \( k, 2k, \ldots \) points. From the privacy perspective, this approach discloses more information than the approach using uniformly valued tokens. This additional information can be exploited by the vendor to increase the probability for linking a redeem process to a particular purchase of some customer. For instance, if some customer is given a ticket worth \( k' \) points for some purchase and no one else is given a ticket of this value, the vendor will be able to link the corresponding purchase to the ticket, as soon as it is redeemed. This implies that counter-based schemes must follow our 'natural' understanding of counters, i.e., they have to represent the value of a sum. For instance, a counter-based scheme permitting recovery of the terms of its sum would just be as bad as token-based schemes with non-uniform values, since one of the terms might just be some re-identifiable \( k' \) as argued before. However, if a counter worth \( k' \) points is represented as a 'natural' sum, the vendor will never know if \( k' \) points have been issued at once or if they are the result of, e.g., \( k' \) issues worth 1 point each.
When the customer has collected a certain number of loyalty points, say \( m \), she may redeem them at the vendor’s for some reward. Figure 2 shows the redeem process for both schemes. The obvious disadvantages of the token-based scheme from Figure 2(a) are that \( m \) tokens must be transferred to the vendor and every single token must be verified by the vendor. In contrast, in the counter-based approach, depicted in Figure 2(b), the customer needs to send only a single token, which is worth \( m \) loyalty points, and consequently the vendor has to do only one verification.

In summary, the counter-based approach uses, for \( m > 1 \) loyalty points, less storage space\(^1\) on the customer side, less bandwidth in the redeem step, and less computation time in the vendor’s verification step than the token-based approach. This improvement in efficiency can be achieved without sacrificing privacy or security as we will show in the detailed protocol descriptions within the next sections. We start with the description of a token-based system and afterwards introduce our token-based scheme.

5. A token-based electronic loyalty system

In this section, we describe an electronic token-based loyalty system which uses blind signatures proposed by Chaum [5]. The following also provides an introduction to Chaum’s scheme for readers not familiar with it.

5.1. Protocols

The token-based loyalty scheme consists of two protocols, the issue and redeem protocol, which correspond to the withdrawal and deposit steps, respectively, of Chaum’s blind signature protocol [5]. Chaum’s blind signatures are in turn based on RSA [15]. In contrast to Chaum’s original proposal, which involves three parties, vendor, bank, and customer, we use it as a two-party protocol only involving vendor and customer. The vendor in our protocol also plays the role of the bank in Chaum’s protocol. The goal of Chaum’s protocol was to establish unlinkability of withdrawal and deposit transactions for the bank. Here, Chaum’s protocol can guarantee the unlinkability of issue and redeem. According to section 3, we also require the unlinkability of any two issue transactions and any two redeem transactions. This aspect is not considered in Chaum’s payment protocol, e.g., withdrawals are linkable. However, as we will point out, Chaum’s protocol can be used to achieve all unlinkability requirements of section 3.

Issue. First, the vendor chooses the system parameters for the underlying RSA cryptosystem. For this, let \( p, q \) be prime, and \( n := pq \). Unless otherwise noted, computations in the following are \( \mod n \). We denote the vendor’s public and private exponents by \( e \) and \( d \), respectively, where \( ed \equiv 1 \mod (p - 1)(q - 1) \). The values \( p, q, d \) are kept secret by the vendor and \((e, n)\) is published as his public key.

The customer randomly chooses a serial number \( s \in_R S_n \) from a special set \( S_n \subseteq \mathbb{Z}_n \setminus \{0\} \) which is predetermined by the vendor. Furthermore, she randomly chooses the blinding factor \( b \in_R \mathbb{Z}_n \setminus \{0\} \) for computing the blinded serial number \( t \). For instance, \( S_n \) can be a set of palindromes \( \mod n \), i.e., all numbers less than \( n \) whose binary representation is the same when read from left to right or from right to left. Other examples for \( S_n \) are considered in [5]. The reason for \( S_n \) to be some ‘special’ subset of \( \mathbb{Z}_n \) will be explained below. Figure 3 shows the protocol for issuing a loyalty point \((s, \sigma(s))\), where \( \sigma(s) := s^d \) denotes the signature on \( s \). If \( k > 1 \) loyalty points are awarded to the customer for some purchase, then the issue protocol is repeated \( k \) times and the customer receives \( k \) tokens \((s_1, \sigma(s_1)), \ldots, (s_k, \sigma(s_k))\).

Redeem. If the customer has reached some redeeming threshold \( m \), i.e., gathered enough points to hand them in for a reward, she may execute the redeem protocol shown in Figure 4. Afterwards, the vendor sends the reward to the customer. Finally, the vendor stores the serial numbers of all redeemed and valid loyalty points in a local database.

5.2. Properties

Privacy. The privacy requirement states that it should not be possible for the vendor to link any two customers’ transactions by means of the loyalty system. The unlinkability of issue and redeem transactions follows from the blind signature protocol. Blindness means that given the set of all issue protocol-runs in which the vendor obtains blinded serial numbers \( t \) and given the set of all redeem protocol-runs in which he gets points \((s, \sigma(s))\), the vendor cannot link blinded serial numbers \( t \) and points \((s, \sigma(s))\) with a probability better than pure guessing. This means that \( s \) is unconditionally hidden from the vendor in the issue protocol because \( t \) could have resulted from any product \( t = s'b^e \) with \( s' \in_R S_n, b' \in_R \mathbb{Z}_n \setminus \{0\} \). Using the same argument, \( t \) is unconditionally hidden from the vendor in the redeem protocol. Hence, the vendor cannot link \( t \) with \( s \) and thus, is unable to link issue and redeem transactions. Note that the values of \( s \) and \( b \) are truly chosen at random and anew for each issue protocol-run.

The unlinkability among the issue transactions follows from the statistical independence of the values \( t \) which is a consequence of the way that \( b \) and \( s \) are selected. This argument also gives the reason for the unlinkability among the redeem transactions.

Security. The goal of the security requirements given in section 3 is to prevent fraudsters from creating valid loyalty points \((s, \sigma(s))\). The fulfilment of these requirements follows from the security of both RSA and Chaum’s work.

\(^1\) This assumes, of course, that the space required to store counters only grows less than linear in the number of loyalty points. As we will see in section 6, this property holds for our counter-based loyalty system.
Unforgeability. We require that no one except for the vendor can create \((s, \sigma(s))\). This assumes that only the signer knows the signing key \(d\) and the signature scheme is secure. In the presented scheme, tokens are produced in the same way as electronic coins in Chaum’s payment system. The Chaum scheme is assumed to be secure against forging, i.e., a fraudster that makes the vendor produce \(k\) tokens at his discretion cannot produce a new \(k + 1\)-th token by himself.\(^2\) Hence, the security of the presented scheme, with regard to unforgeability, follows from Chaum’s scheme.

Double-spending detection. Since a customer can try to redeem copies of loyalty points, the vendor stores all serial numbers in a local database and compares each \(s\) from a newly submitted point to the database’s. If some \(s\) is already stored in the database then it has been double-spent and will not be accepted. The probability that two customers pick the same \(s\) as a serial number is \(1/|\mathbb{S}_n|\) which can be arbitrarily small.

Pooling prevention. Unfortunately, pooling of loyalty points cannot be prevented, since each point is represented by a serial number \(s_i\) which is uniformly chosen at random from the set \(\mathbb{S}_n\), and the vendor does not learn the number before redemption (assuming that the blind signature scheme is secure). Thus, loyalty points that were issued to distinct customers can be pooled and redeemed together.

Efficiency. Issuing \(m\) loyalty points always requires the creation of \(m\) tokens. Thus, costs in the issue protocol are linear in the number of issued loyalty points, even if some points are awarded in one purchase. This means that the size of data to be stored and transferred, and the amount of required serial numbers, and the customer’s effort for blind-signature verification, and the vendor’s effort for signature generation grow linearly in the number of loyalty points. The redeem protocol shows similar properties. Also here, the size of data to be transferred and stored (database for serial numbers), and the vendors’ signature verification costs grow linearly with the number of redeemed points.

### 6. A counter-based electronic loyalty system

In this section we introduce a counter-based optimisation of the scheme from the previous section. As in the token-based system, we have two protocols, add and redeem. Instead of issuing tokens, each of which represents a loyalty point as in the issue protocol of section 5, the vendor now adds the number of loyalty points to be issued to a counter.

The system setup for the counter-based system, i.e., vendor’s private and public key \(d\) and \((e, n)\), respectively, and the set \(\mathbb{S}_n\), is the same as in the token-based scheme. In the proposed system, a counter representing \(m\) loyalty points

---

\(^2\) For instance, fraudsters are prevented from using pairs \((x^e, x)\) for \(x \in \mathbb{Z}_n \setminus \{0\}\), with \(\sigma(x^e) = x\). Serial numbers have a special property that cannot be easily obtained by computing \(x^e\). The same trick prevents fraudsters from creating new loyalty points by using existing points \((s_1, \sigma(s_1)), (s_2, \sigma(s_2))\) and computing \(\sigma(s_1) \sigma(s_2) = s_1^e s_2^e = (s_1 s_2)^e = \sigma(s_1 s_2)\) which yields a new loyalty point \((s_1 s_2, \sigma(s_1 s_2))\). To thwart these attacks we require a special property for the serial numbers, e.g., palindromes as proposed in [5].
contains an $m$-times signature on a serial number $s$, i.e., $\sigma (\sigma (\ldots \sigma (\sigma (s)) \ldots )) := \sigma^m (s)$. Thus, each counter is associated with exactly one serial number $s$.

### 6.1. Protocols

**Add.** Before the customer starts the add protocol for the first time, she has to initialise the counter. This means that she randomly chooses a serial number $s \in \mathbb{Z}_n$ and the counter’s start value $m_0$; usually $m_0 = 0$. Assume that we have a counter with $m_{i-1} \geq 0$ points that the customer gathered in $i - 1$ purchases so far with $i \geq 1$. Further assume that she obtains $k_i > 0$ points in her $i$-th purchase, which yields $m_i := m_{i-1} + k_i$. In order to obtain $k_i$ points, she hands in a blinded counter value $t_i$ as shown in Figure 5. Then, the vendor blindly $k_i$-signs $t_i$ and returns the result to the customer. Here, $k_i$-signing means that the vendor raises $t_i$ to the $d^{k_i}$-th power, which can be done in one step. Upon receiving the $k_i$-signed $t_i$, the customer unblinds it and obtains an $m_i$-times signature of $s$. This scheme is then used for subsequent purchases in the same manner, i.e., the result of the add protocol in purchase $i - 1$ becomes an input for the add protocol in purchase $i$. After $i$ purchases with iterated $k_j$-signing for $j = 1, \ldots , i$, the customer has a serial number $s$ which is raised to the $d^{m_0 + \sum_{j=1}^i k_j}$-th power. Then, the actual counter value, which represents the number of loyalty points, is given by the number of signatures on $s$, i.e., $m_i = m_0 + \sum_{j=1}^i k_j$. The customer keeps the current balance of loyalty points by storing $(s, m_i, \sigma^{m_i}(s))$.

For carrying out exponentiations $b_i^{d^{k_i}}$, $(\sigma^{m_i}(s))^{e^{m_i}}$ on the customer side, and $t_i^{d^{k_i}}$ on the vendor side, efficient techniques can be applied, such as square-and-multiply algorithms or the Montgomery exponentiation algorithm. Furthermore, since the vendor knows the factorisation of $n$, he can also apply reductions $\mod \phi(n)$, where $\phi$ denotes Euler’s totient function.

**Redeem.** Assuming that $m$ loyalty points are needed to gain a reward, the customer may execute the redeem protocol as shown in Figure 6. The vendor grants the reward if $(s, m, \sigma^m(s))$ is a valid triple and then stores the serial number of the triple in a local database. In order to reduce the computation costs for exponentiations $(\sigma^m(s))^{e^m}$ in the verification, the vendor may precompute repeatedly used values, such as $e^{m} \mod \phi(n)$, and also apply the same methods as proposed in the add protocol.

Note that the customer always has to hand in the triple with the most current counter value in the redeem protocol. Handing in triples with an intermediate counter value is to the customer’s disadvantage since each serial number is only accepted once by the vendor. In case a customer hands in a counter representing $m$ loyalty points but chooses a reward for $u < m$ points, the redeem protocol is carried out in combination with the add protocol initialised with a new serial number $s'$, $m_0 = 0$, and $k_1 = m - u$. This is similar to change given in payments. Regarding this aspect, the
token-based approach has a certain advantage since there is no necessity for change to be given.

6.2. Properties

Privacy. The unlinkability among add transactions follows from the same argument as the unlinkability of issue transactions in the token-based scheme. This holds even if the same serial number is used in subsequent runs of the add protocol. The unlinkability among redeem transactions follows from the statistical independence of the serial numbers used in counter initialisations. In general, redeem and add transactions are not linkable as well since the vendor obtains no information about the serial number in the add protocol. The only exception occurs if unused points are given back to the customer, i.e., add and redeem protocol are carried out in combination. However, the vendor gains no advantage from this since the redeem and add protocol use different serial numbers s and s', respectively, and the add protocol is not related to a purchase, i.e., there is no data available for the creation of profiles.

Security. The arguments given in the security part of section 5.2 also apply for the security of the counter-based scheme. However, there are some additional aspects regarding unforgeability that need to be considered here.

Unforgeability. The unforgeability of the counter mainly depends on the security property of the Chaum system. If there exists a forger for the counter-based loyalty system, then one could immediately apply this forger to forge signatures in the Chaum system quite easily. However, forging signatures in the Chaum system is assumed to be hard. There are some further aspects to be considered. A fraudster may repeatedly apply the public exponent e to some \( x \in \mathbb{Z}_n \) until he obtains \( s = x^e \in \mathbb{Z}_n \) for some \( v \), in order to forge \( \langle s, v, \sigma^v(s) \rangle \). However, since \( x^{e+1} = \sigma(s) \) this would provide a method for generating a valid pair \( \langle s, \sigma(s) \rangle \) without knowing \( d \), and thus, a method to break the security of Chaum’s system. But this attack is assumed to be infeasible, and hence, it is infeasible to generate valid triples in this way.

Another aspect to be considered is related to the fact that exponents can be reduced \( \mod \lambda(n) \), where \( \lambda \) is the Carmichael function which gives the smallest number \( r > 0 \) such that \( a^r = 1 \mod n \) for all \( a \in \mathbb{Z}_n^* \). [19]. This means that for \( s \in R \mathbb{Z}_n \), there exists a number \( w > 0 \) with \( e^w = 1 \mod \lambda(n) \) such that \( s^w = s \mod \lambda(n) \). In words, applying \( e \) iteratively \( z \) times to \( s \) yields the same result as applying \( d \) iteratedly \( w - z \) times to \( s \). One can argue that such an iterated application of \( e \) might be exploited by fraudsters.

But for a successful attack, a fraudster has to find an appropriate \( w \). If a fraudster would know an efficient algorithm to find \( w \), then he would be able to carry out the iterated-encryption attack on the RSA cryptosystem which would eventually reveal \( d \). In [12], it is shown how system parameters \( p, q \) have to be chosen to satisfy the security constraints of the iterated encryption attack. If we choose the parameters according to [12], then forging counters by repeatedly applying \( e \) to \( s \) is infeasible.

Double-spending detection. In order to cope with the double-spending problem, the vendor maintains a database where he stores serial numbers of redeemed loyalty points as in the token-based approach.

Pooling prevention. In contrast to the token-based scheme pooling of loyalty points can be prevented within our counter-based scheme. Since the points collected by means of our counter are associated to one specific serial number. If vendors do not accept more than one counter within one redeem transaction, then there is no known possibility for the pooling of counters in this way. Without such a restrictive policy by vendors, \( m > 1 \) customers could collude, and one of them would just have to send their \( m \) counters \( \{s_1, k_1, \sigma^{k_1}(s_1)\} \) worth \( \sum_{i=1}^{m} k_i \) points. Customers may still try to add up their valid counters \( \{s_1, k_1, \sigma^{k_1}(s_1)\} \) and \( \{s_2, k_2, \sigma^{k_2}(s_2)\} \) to create a valid counter \( \{s, k = k_1 + k_2, \sigma^k(s)\} \) for \( s_1, s_2, s \in \mathbb{Z}_n \). However, this attack is assumed to be infeasible because of the security of the signature scheme and the application of the redundancy scheme, i.e., \( s \in \mathbb{Z}_n \).

Efficiency. Loyalty points awarded to one customer are represented by the counter. In contrast to the token-based approach, the costs in the add protocol are no longer linearly related to the number of loyalty points. Instead, the size of data that has to be transferred and stored is constant for each purchase regardless of the number of points awarded in this purchase. This means, that the costs regarding this data size only grow linearly with the number of purchases. The same holds for the customer’s effort regarding the number of blinding and verifying actions, and for the vendor’s effort regarding the number of signatures that have to be generated. While in the token-based approach each token required its own serial number, the counter-based approach requires only one serial number for a counter, regardless of the counter value. The redeem protocol of the counter-based approach is also more efficient than the redeem protocol of the token-based variant. The size of transferred data is constant in the number of redeemed points and so is the vendor’s cost regarding the number of signature verifications. Storage costs for serial numbers are only linear in the number of redeem protocol runs in contrast to linear costs in loyalty points within the token-based approach.
On the other hand, in the counter-based approach elementary operations such as blinding, blindly signing, and verifying signatures are not less expensive than the in the token-based approach. However, when dealing with more than one loyalty point less operations are needed in total in the counter-based variant. Furthermore, efficient computation methods make the counter-based approach more attractive.

7. Related Work

Much work has been done by economic and marketing experts in the field of loyalty systems, e.g., see [1, 16, 6]. Furthermore, there has been lots of work stressing the importance of privacy for electronic commerce, e.g., see [9]. A common goal of proposals for privacy enhancing systems in the area of electronic commerce is to prevent certain parties from linking activities of the same customer. In typical commercial relationships, there are many possibilities to link customer transactions. For instance, in the area of payment systems, the unlinkability of withdrawal and deposit has been considered [5, 2]. In [8], a solution to establish the unlinkability of the customer’s search and order phases has been proposed. In this context, we provide a solution to guarantee that unlinkability achieved by other techniques still holds when using a loyalty system. Other work regarding technical proposals for loyalty systems can be found in [11]. In this work, an infrastructure based on smart cards is proposed which allows individuals to introduce their on currencies or loyalty systems. However, they do not consider the problem of achieving privacy in loyalty systems. Another proposal for a loyalty system was presented in [17]. In this work, the authors respect the privacy aspect. However, the goal of the system was not to provide unlinkability of transactions. The solution is based on pseudonymity, and thus provides a weaker form of privacy protection.

8. Conclusion

We have presented two variants of privacy-friendly loyalty systems that do not allow vendors to link customers’ transactions. Both presented approaches use Chaum’s blind signature protocol, but they differ in efficiency. The proposed counter-based approach is more efficient than the token-based approach in terms of processing time, used bandwidth, and storage space if more than one loyalty point is to be issued and redeemed. Furthermore, the counter-based system prevents customers from pooling their collected loyalty points. Loyalty systems can provide an important strategy for vendors’ customer relationship management to retain customers and to increase the incentive for repeated buying. The privacy property of our proposal may attract customers that usually refuse to become members of a loyalty program since they fear infringements of their privacy.

References