Loyalty Program Scheme for Anonymous Payment Systems

Arrianto Mukti Wibowo[*] *and Kwok Yan Lam*[*]

[*] Computer Science Department,
School of Computing
National University of Singapore
{arrianto, lamky}@comp.nus.edu.sg

Abstract. Loyalty program is a marketing effort by the merchant to keep customers loyal to their stores. It tries to keep track of the purchasing-behavior of a customer by recording customer's purchase information, including his credit card number, as a key identifier to the customer. While it may benefit the customer, the drawback is that the privacy of the customer is intruded. If the customer is using an anonymous payment system such as electronic cash / digital coins, his privacy is protected, but he will not get any benefit from the loyalty program which tries to record his payment information. This paper suggests several solutions to this problem. Among the solutions, we present the idea of *blindly signed pseudo digital certificates*, which satisfies our requirement for a loyalty program scheme with an anonymous payment system. (20 February, 2000)

1 Introduction

Recent article by Barefoot [1], explicitly mentioned a real world problem, where banks and merchants are gathering information on customer's purchases. Although the reason for mining the sales data is to provide better customer service such like in loyalty programs, the drawback is that the privacy of the customer is intruded.

Of course, if the customer is using an anonymous payment system, which the identity of the customer is concealed, his privacy is guaranteed. But on the other hand, the customer will loose the benefit of the extra customer service offered by the merchant, since the merchant will not be able to track down the purchasing-behavior of each customer.

In this paper, we propose several methods to allow a merchant to keep track of its customer purchasing-behavior, even if the customer uses an anonymous payment system such as electronic cash. Thus, the seemingly two conflicting interests, which are customer's privacy and merchant's need to gather statistical data from customer's behavior, can be resolved.

We begin by describing loyalty program, or some called it customer retention program, in section 2, along with its importance. We also examine how merchant can gather the needed information for loyalty program. In section 3, we take a detour to illustrate various anonymous payment systems along with its motivations. At this point, we will see incompatibility to use anonymous payment system with a loyalty program. Section 4 digs deeper in our apparent problem and then formally defines the basic problem. Section 5 shares our preliminary thoughts and describes detailed requirements. In section 6, we discuss several plausible solutions to the requirement and therefore answer the basic problem. Finally, we end our discussion with the conclusion.

2 Loyalty Program

2.1 Definitions and importance

Sharp and Sharp define *loyalty programs* as structured marketing efforts that reward, and therefore encourage, loyal behavior (of the customer), for the benefit of the merchant [27]. Another term for loyalty program is *customer retention program*, which Harris defines as a continuous attempt to satisfy and keep current customers actively involved in conducting business [13].

The objective of a customer loyalty program is to keep existing customer and to increase their repeat-purchase loyalty, in contrast to other marketing activities on winning new customers. The loyalty program tries to minimize the chance the customers would switch to another competing products or services. Bolton, Kannan, and Bramlett study on credit card loyalty program [2], showed that the existing customer in a loyalty program are less sensitive to some issues which others might consider important, such as a low quality rating of customer's current credit card company, or if the billing scheme is not the best among the credit card companies. One possible reason, was probably they perceive that they are getting better quality and service for the price or, in other words, good value.

Intimate and interpersonal relationship between salesperson and the customer is a very important aspect in customer loyalty. The salesperson must have an understanding of each customer's needs. As shown by Macintosh and Lockshin in their study on retail relationship and store loyalty [18], customer's trust and commitment to the salesperson are directly linked with purchase intention. Without interpersonal salesperson relationship, store loyalty is influenced only by customer's trust in the store. Therefore, knowing exactly what *each* customer wants - as apparently done by a good salesperson - is an important factor in customer loyalty to the merchant. The argument complement Harris' argument that a well-developed loyalty program plan should create an environment which current customers' needs are met and new needs are explored [13].

The financial importance of loyalty program was underlined by Pearson in [23], since loyalty program gives something of guarantee of future earnings. Even if current earnings are high, a low level of customer loyalty means that future earnings may be at risk.

2.2 Mining data for loyalty program

Among several methods to obtain information of existing customers' needs, one of them is by 'mining' the historical point of sales data. It must be noted here that there are several ways to look at the data. The merchant may want to observe the buying pattern for a typical *single* purchase. For example, the merchant may want to know, when customers buy a box of cereal, what are other products bought along with it. It may found out that for nearly every cereal purchased, many customers also bought fresh milk.

Alternatively, the merchant can gather the shopping pattern of *each* particular customer from time to time, and can intelligently give specific suggestions to a particular customer, depending on his previous purchasing-behavior. For example, if a particular customer buys cereals regularly, the merchant may offer a discount prices for cereals, or suggest a brand new cereal for the customer to try. The merchant can also suggest which cereal is the best buy and suggest other microwave breakfast foods for complement. The merchant may choose not to offer these suggestions to a customer who rarely buys cereals or any breakfast foods, since the person may usually have a brunch at 10.30 AM.

Bolton, Kannan, and Bramlett research on loyalty programs by credit card companies [2], is another good example for us. They observe that the loyalty programs, allow the credit card companies to observe the purchasing pattern of each cardholder. In the loyalty program, members can accumulate points with each dollar transacted with their credit card. Those points are later redeemable for a wide variety of goods and services such as air certificates, car rental, vacation options, and retail gifts. It is worth to note, that even some of these credit card companies charge about US$40 to a customer who wants to join the loyalty program.

From the merchant's point of view, using credit card number as the key identification for each customer in a loyalty program seems natural. Firstly, the merchant does not need to ask every customer to participate in the loyalty program. It merely records every credit card transaction. It is a very convenient way to automatically enable loyalty program. As a manner of fact, many credit card companies have partnerships with merchants. Secondly, credit card is a very popular payment method, but every payment transaction is *traceable*. Which means, we can identify who made certain purchases. If the merchant have partnership with an issuing credit card company, it can even gather more valuable information about the customers. Debit cards, now gaining wide acceptance, also has the same properties as credit cards, in which every transaction is traceable.

In contras, *untraceable* payment like cash payments, would not allow the merchant to keep track which customer made certain purchases. We can also say that cash payments are one form of anonymous payment system.

3 Anonymous Payment System Revisited

3.1 Motivations for anonymity

In [5], Chaum argues that untraceable payment is very important, since it will protect the privacy of the payer (customer). Third parties, such as merchants or service companies, can keep track of the behavior of their customers, if the customers use some sort of a traceable payment system such as credit card, check, or debit card. Furthermore, all of these payment records can be linked so that they constitute in effect a single dossier on customer's life [6]. The customer may wish that his personal lifestyle, whereabouts and associations remain private.

Apparently, Chaum's advocacy in anonymous payment system was supported by a more recent survey by GVU WWW Surveying Team, Georgia Institute of Technology [12]. The survey revealed that just over half of respondents agree that they prefer anonymous payment systems (51%), a quarter are neutral (25%). In general, people prefer an anonymous payment system or they have no preference, few actually prefer a user-identified system. Either people who already know, or whose just been told, what an anonymous payment is, both have similar opinions, in that most prefer anonymous payment.

3.2 Two aspects of anonymity

In our paper, we are interested in two aspects of anonymity. The first aspect, as we mentioned before, is *untraceability*, in which the privacy of the user is protected, such that no one can trace the relation between a customer and his purchases. The identity of the payer (customer) in a particular payment can not even be traced although the merchant colludes with the issuing financial institution (such as bank).

We are also concerned about the aspect of *unlinkability* of an anonymous payment system. According to Tsiounis' definition in his paper about anonymous digital coins [28], unlinkability is the property in which given a set of coins (or in our case, a set of payments),

one can not identify whether those coins (payments) came from the same customer account or not. Tsiounis continued to argue that if several payments are linkable (although anonymous), identification can be performed by conventional means, such as correlating payment's locality, time, size, type, frequency, or by finding a single payment in which the user identified himself.

The first breed of proposed anonymous payment systems were electronic cash. Untraceability is a universal feature of electronic cash. Some called it digital coins, since in the real world, payment with coins are really untraceable.

However, when it comes to the unlinkability issue, several proposed digital coins are unlinkable [4, 3, 10, 17, 28], but others are actually linkable digital coins [9, 21, 22, 24, 30]. Some of the linkable digital coin authors proposed to 'rotate' several digital coin 'licenses' to obtain pseudo-unlinkability. Note that some unlinkable digital coins protocols can be modified to be spendable *n*-times, but it will make all the payments done using a single digital coin and its 'children' be linkable [3, 11].

The idea of anonymous electronic cash also lead to the development of other anonymous payment systems, such as anonymous check (which is actually an extension of e-cash protocols), anonymous credit card protocols [16] and anonymous bank account [8].

From the discussion above, it is clear that any anonymous payment system must have untraceability as its properties, but not all anonymous payment systems have unlinkability as one of their properties.

4 Problem Statement

At this point, we can notice the apparent conflicting interest. Banks or merchants want to gather statistical data of customers' behavior from customer's payment information, but customers may want to use an anonymous payment system.

Before we formalize our problem, let us try to comprehend a closely related real world problem. Barefoot in [1] stated that the current issue is how the banks (or in our context, credit card companies) will be able to safeguard customer privacy completely, while undermining the most exciting innovations in banking. She argued that there are at least four focal points of privacy intrusion risk:

1. information transmitted over the Internet;
2. third-party relationships (such as partnership with merchants);
3. computerized credit scoring; and
4. data mining and customer relationship management (e.g. loyalty program).

She gave an example of Amazon.com, the largest Internet book store in the world:

> *"After months of glowing publicity regarding its trailblazing role and progress in bringing happy consumers into e-commerce, Amazon found itself attacked for compiling and disclosing data on customer reading habits. To the embarrassment of some parties, it publicly listed the books most frequently purchased by certain affinity groups, including the employees of specific companies. One well-known company's best seller was a book critical of its CEO, while another large firm's employees seemed quite interested in reading about sex. Amazon's assurance that the lists were disclosed in the spirit of "fun" did not dispel the unease of critics, some of whom had never realized that their own purchase information might be tracked and used."* [1]

While her example may not perfectly exemplify our discussion (we are interested in the behavior of a particular customer, not a group of customers), it may well illustrate what we should be aware of. Please be reminded that Amazon may actually try to give better customer service, but it does so by intruding the privacy of its customers.

To worsen things out, even some of the merchants know exactly how much amount of pre-approved credit the customers have [14], especially those who have partnership with credit card companies.

We also noticed that many e-commerce websites now require the customers to register their credit card information and their proper address, or else they won't deliver the goods. From a practical point of view, this security measure to prevent credit card fraud and misuse seems acceptable. But there is no guarantee that the merchant is not going to make use of customers' credit card information to track customers purchasing-behavior.

Barefoot's approach to solve the problem was apparently are more legalistic, rather than technical. She suggested the banks and the merchants should be ready to comply with the newly proposed act, which let the customers exclude their records from internal usage and external sharing arrangements, including third parties. She also suggested that voluntary privacy protection steps should be taken and privacy consciousness must become ingrained in the banking culture.

If the merchant used to gather credit card numbers (or any other traceable payment method) as the key identifier of each customer, then the merchant can use use this key to gather more statistical information on its customers. But because the inherent problem of traceability of those payment systems, eventually some of the customers may prefer to use anonymous payment system to protect their privacy. However, the merchant will loose valuable marketing information.

Now we formally define our problem.

Problem. *Given a set of customers who are using anonymous payment system, devise solution(s), to let the merchant still be able to keep track of the purchasing-behavior of each customer.*

5 Basic Idea & Detailed Requirements

Since we were doing research in anonymous digital coins, we originally thought of making the digital coins inherently support loyalty programs. Apparently, since typical payment consist of multiple coins, we thought that it would be a lot easier if we can mint another 'coin' with an encrypted identity on it. Then we shall proof that the coin with the encrypted identity is in the same group as the other coins.

It came out that the coin with an encrypted identity, is crucial in our study. The coin with the encrypted identity was minted nearly the same way as the other coins using a certain blind signature protocol, but without any nominal value. We reduce the digital coin with an encrypted identity 'problem', simply into a signed pseudo identity, which may be created using a blind signature protocol. *Signed* pseudo identity implies that the pseudo identity should be trusted. Therefore, our main solution relies on the use of *blindly signed pseudo digital certificates* or *digital unforgeable pseudonyms*, among other solutions to consider. Take note that three out of four suggested solutions actually rely on the use of another 'authenticated token', external to the payment itself.

We define pseudonym as:

"person's name that is not his real name, especially one used by an author, a pen-name" [15]

Of course in our context, the individual is not a book author or pen-pal, but a customer.

Now let us formally define the requirement of the proposed protocol to answer the stated problem above.

Requirements. *The proposed solution, should have these following properties:*

1. *The protocol should allow merchant (payee) to link several payments made in different place and time to a particular customer (payer).*
2. *The protocol should conceal the true identity of the customer even if the merchant colludes with financial institution responsible for the payment system (i.e., the bank).*
3. *A pseudonym for a particular customer can not be used by another customer. A pseudonym is unique for each customer. In another word, the pseudonym is unforgeable.*
4. *A pseudonym is produced by the customer to the merchant, only under customer's will. It also means that the merchant would not be able to extract the pseudonym without user's consent.*
5. *The protocol should be able to be mounted on any anonymous payment system, including anonymous check, anonymous credit card and anonymous account.*
6. *A pseudonym may only be used after the customer's true identity has been verified/authenticated by the merchant. The customer then creates his own pseudonym, such that any other party can not link the pseudonym to the true identity. For example, a credit card company with its merchant partners may only let a customer be a member in their loyalty program, only if the customer show his credentials or has already been registered before.*
7. *To give some sort of flexibility, ideally, the protocol should be able to be implemented with several different kind of cryptographic primitives.*

Please note that in our discussion, we limit our focus and concern to the customer authentication protocol. Therefore, we leave other security issues such as transmission privacy as another problem.

6 Solutions

There are different solutions to the basic problem previously stated, but not all of these solutions address all of the formal requirements mentioned.

6.1 Cookies

Cookies are a standard mechanism that allows a website (or server) to deliver simple data to a client (end user); request that the client store the information; and, in certain circumstances, return the information to the website [20]. Cookies are a way of storing persistent client data so that a website can maintain information on a user across HTTP stateless connections.

Using cookies is a simple and practical way to resolve our problem. At the simplest model, the merchant web server merely checks whether the customer (client) already have a cookie or not. If not, then the merchant server creates a cookie for the customer in the client's computer hard disk. The merchant then stores the customer profile in the cookies, including his 'purchasing-behavior'. Whenever the merchant needs to get the customer profiles, it merely gets the information from the cookie.

For a certain degree, cookies are quite secure. Its specification defines that only the website that creates the cookie can retrieve it back again, so other websites can not peek at another cookie which was not theirs [29]. To enable server authentication and communication privacy, it may even optionally use SSL.

It has several drawbacks, though. If the client computer is shared for several users, and the operating system inherently has a low level security, such as Microsoft Windows 95/98, other users can see other user's cookies. In addition, cookies are not stored encrypted. They are just ordinary, editable, text files. If the customer authentication scheme is not well design, a customer can pretend to be another customer.

For some web applications, using cookies is probably sufficient. It definitely meets the first and fifth requirement. Its basic design does not rely on cryptographic protocols (other than SSL), so the seventh requirement is not applicable. Basically the client does not control the cookies (there exist applications to let users manually control cookies), so the fourth and the sixth requirement are generally not met. Depending on the application, the second requirement may or may not be met. Moreover, without proper security support from the operating system or the browser, the third requirement may not be achievable.

We must underline that cookie's basic security pretty much relies on a non-cryptographic HTTP specification. For some other applications, using cookies is not possible or just not sufficient, especially non-Web applications and those that demands much stronger cryptographic client authentication scheme.

6.2 Pseudo digital (public-key) certificates

Digital certificate, or to be more precise *public-key certificate*, is a vehicle by which public key may be stored, distributed or forwarded over unsecure media without the danger of manipulation [19]. Digital certificates are commonly used as a digital identification or authentication means over an unsecure public network such as the Internet. In general, it helps to tells us that the person named 'Alice' over the network is really Alice as we know her. As its name implies, public-key digital certificates employ a certain asymmetric cryptographic algorithm such as RSA, El-Gamal, DSA, etc.

To create a digital certificate, initially an entity generates his public-key pairs. He keeps his private key secret, then sends his public key along with his personal information to a *certificate authority* (CA). The CA then creates the digital certificate by signing the public key and necessary information with CA's private key. In its very basic form, a certificate is only a public key signed by a CA. However, usually it also contains other necessary information such as entity's personal information/address, expiry date, serial number, algorithm used, policies, etc. Any other entity who wants to verify the validity of the certificate needs to have CA's public key. A challenge-and-response protocol is usually employed to authenticate entities holding the digital certificates. Readers are encouraged to read more on public-key cryptography and digital certificates in [19, 26].

Digital certificates may have different 'authenticity' levels. Class 1 certificates are the least authentic digital certificates. Higher class-number generally denotes higher certificate authenticity. Class 1 digital certificates, are created by the CA without verifying the identity of the entity that requested the certificate. The only security measure is forcing the entity to enter his e-mail address at registration, since usually the client will receive his requested certificate from an e-mail from the CA. However, with this type of digital certificates, Alice can pretend to be Bob, by submitting Bob's name, his personal information and *her* (newly created) e-mail address *honestlyiambob@e-mail.com* to the CA at registration.

The process of obtaining higher authenticity digital certificates, such ones that are used for commercial web servers, is a lot more complicated. Obtaining the highest quality certificates, requires the entity to register at the CA office *in person* to produce their original documents to support their authenticity. With this kind of digital certificates, the CA guarantees that a certificate with the name XYZ Co. Ltd., New York, USA, is really the XYZ Co. Ltd. which operated in New York, in the United States. The CA usually offers some insurance just in case the high authenticity digital certificate is misused.

In our discussion, we are particularly interested with the least authentic kind of digital certificates, such as (but not necessarily) class 1 digital certificates. It actually let someone (e.g., a customer) to declare his own pseudonym by letting him decide by what name shall he be known, which is fortunately unforgeable (by the definition of a digital certificate).

Our point is, therefore, if the CA does not examine the validity of the entity's (customer's) personal identity, the issued digital certificate is actually an unforgeable pseudo digital identity. This pseudo digital certificates actually complies to all of our requirements, except the sixth requirement, since the merchant never had a chance to verify the true identity of the customer. Nevertheless, for most applications that do not require the true identity of the customer to be known prior gathering data, definitely this scheme solves our problem.

6.3 Linkable anonymous payment system

As we have previously mentioned, there are several anonymous but linkable payment systems. In general, these linkable digital coin protocols try to speed up the minting process and minimize storage requirements. Many of them do so by letting the user (customer) to have an electronic anonymous 'license' of to mint a series of coins. The license acts like a 'head' or 'root' of a graph of coins, extendible 'on the fly' to the children.

If we were to use linkable anonymous payment system for sake of the loyalty program, ideally the customer should use one license for all payments in each particular merchant. Therefore, the merchant can still keep track of purchasing-behavior of each particular customer, although each of them is only known by its anonymous license.

Since in several payment protocols the license is limited to a certain amount of money, each license automatically expires when it has used all of its license to use that certain amount of money. In this case, the relation between an anonymous customer with his identity may not be persistent. In another words, the first requirement can not be achieved permanently. However, there is a way to tackle this difficulty. If the customer is using his subsequent license (as the old license expires), customer merely proofs in front of the merchant, that he can 'open' digital coins derived from both licenses. Of course if the old license has expired, the merchant should not accept the coins derived from the old license. The merchant will be required to keep track of the licenses that each customer used.

The second requirement is met, because basically the license is a blinded identification signed by the issuer (bank). The third requirement is also achieved. The forth requirement is not met, because customer implicitly shows his pseudo identity (the license) to the merchant at payment phase. In addition, since this method uses the inherent properties in the payment system, it can not be used in another payment method (fifth requirement). The sixth requirement can not be achieved because the merchant may not be able to authenticate the true identity of the customer using the linkable digital coins. Finally, it generally can not use other cryptographic algorithm other than the one used in the payment protocol (seventh requirement).

6.4 Blindly signed pseudo digital certificates

The basic idea of this solution is to use a blindly signed pseudo digital certificate as the pseudonym for each customer. Note that this solution is very much the same as our previously described (least authentic) pseudo digital certificate. Except now, the merchant (or any other trusted party, such as the bank or the credit card company) can verify the true identity of the customer, before the customer request a certificate to the trusted party. By signing blindly, implies that the signer (trusted party) do not have any knowledge whatsoever of the signed message, at anytime (prior, after or at the moment of signing).

Here we sketch how it works:

Setup phase:

1. A trusted party *T* (it can be the bank or the merchant itself) authenticates the customer in some certain way, such as using digital certificates, or other physical proof. This step is very important to correctly identify the customer, since not everyone is allowed to the loyalty program. Please be reminded, if the protocol is conducted over unsecure public network, then the exchanged messages in following steps must be signed to protect integrity and authenticity.
2. The customer generates a pair of public and private keys. The customer keeps the private key secret.
3. The customer blinds his public key and executes a blind signature protocol to let *T* blindly signs his public key. Both customer and *T* perform necessary steps in the agreed blind signature protocol.
4. At the end of the protocol, the customer will obtain a signature of *T* on his public key key (i.e., the blindly signed pseudo digital certificate), without *T* ever knowing his public.

After executing the setup phase protocol, the customer receives a signed public key (a digital certificate). But since the key was blinded when the trusted party *T* signed it, *T* can not correctly correlate the signed public key to a particular setup phase transcript. Because no one is able to link a particular setup phase transcript to a particular blindly signed digital certificate, it also mean that no one can link a blindly signed digital certificate to a true identity. It is actually this property which satisfies the sixth requirement.

The authentication process is just a digital certificate verification and authentication.

Authentication on payment phase:

1. Before customer pays, the merchant asks the customer to present his blindly signed pseudo digital certificate.
2. The customer complies by sending the blindly signed pseudo digital certificate to the merchant.
3. The merchant verifies the validity of public key in the certificate by using the appropriate verification process, depending on the algorithm used. The merchant will accept if the signature in the certificate is valid. The merchant sends back a challenge to the customer to prove his pseudo authenticity.
4. The customer complies by sending an appropriate response to the merchant. Refer to [19, 26] for more information on authentication process using digital certificates.
5. After verifying the response, the merchant tells the customer that the merchant is ready to accept the payment.
6. The customer pays.

7. Merchant records the blindly signed pseudo digital certificate (or just the public key) along with the purchase information, as data source for the loyalty program.

Optionally, the authentication process can be done before the customer browses the shop, so the merchant can offer suggestions while the customer shops.

The solution satisfies all of our seven requirements. If the customer keeps using just one blindly signed pseudo digital certificate, the merchant can link his payments to his 'blinded identity', so the first requirement is met. The 'blinded identity' implies that the true identity of the customer is shrouded, so the second requirement is met. Since only the rightful holder of the corresponding private key can comply to a challenge-and-response authentication process, the third requirement is met. The solution also met the forth requirement, since the customer may not choose to use his blindly signed digital certificate if he do not want his behavior be tracked. Fifth requirement is also addressed, because it is basically an authentication token outside the payment protocol. The sixth requirement is met by the blind signature process in the setup phase. And since the signing process can use several kind of blind signature protocols, it may be implemented with different primitive cryptographic algorithms.

To prevent several merchants cooperate together monitoring the behavior of a customer, the customer should create multiple blindly signed pseudo digital certificate, one for each merchant, by executing the setup phase several times. Alternatively, the customer may also use the same blindly signed digital certificate for several merchants, which have integrated loyalty program for added benefit.

At the appendix, we present several examples of blind signature protocols based on RSA and discrete log, along with their signature verification process. Note that the customer, may also include a pseudonym of his own choice along with the public key, before those information is blinded at setup phase.

7 Conclusions

We have shown in this paper that it is possible for the merchant to conduct a customer loyalty program although the customers are using an anonymous payment system. Several solutions exist, such as using cookies, least authentic type of digital certificates (pseudo digital certificates), linkable anonymous payment system, and blindly signed pseudo digital certificates. Amongst those solutions, the blindly signed pseudo digital certificates satisfies all of our requirements and the most versatile.

Three of the solutions basically relies on an additional 'authentication token', which might be considered 'external' or not inherent in the payment protocol. Despite several requirements which are not addressed, the solution to use linkable anonymous payments still make use the inherent design of the payment protocol itself.

We also acknowledge several limitations. One of the most obvious limitation is that the merchants still do not have the ability to gather maximum information it can get, such as customer's mailing address. Of course, the customers can fill those information, only if they are willing to do so and know the consequences. The second limitation is, especially with the blindly signed pseudo digital certificate, that these solution may require the customer to willingly join the loyalty program. From a practical point of view, probably the setup can be awkward for the customers, if not well designed. On the other hand, this limitation may also be an advantage, since law in several states may prohibit merchants to observe the behavior of the customers without their consent.

It should also be noted, that mining historical point of sale data is not the only way to gather information for loyalty program. Other possibilities exist as well, such by conducting survey, or asking the customers to fill in complain forms or registration forms.

8 Acknowledgments

Special thanks to … for preliminary discussions and sharing some thoughts.

References

1. Jo Ann S. Barefoot. Privacy under scrutiny. In *Banking Strategies*, Nov/Dec 1999.
2. Ruth N. Bolton, P. K. Kannan and Matthew D. Bramlett. Implications of loyalty program membership and service experiences for customer retention and value. In *Journal of Academy of Marketing Science*. Greenvale, Winter 2000.
3. Stefan Brands. An efficient off-line electronic cash system based on the representation problem. Report CS-R9323, Centrum voor Wiskunde en Informatica, March 1993.
4. David Chaum, Amos Fiat and Moni Naor. Untraceable electronic cash. In *Advances in Cryptology – proceedings of CRYPTO 88,* Lecture Notes in Computer Science 403, Springer-Verlag, 1990.
5. David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology – proceedings of CRYPTO 82,* Plenum Press, New York, 1983.
6. David Chaum. Achieving Electronic Privacy. In *Scientific American*, August 1992.
7. David Chaum and Torben Pryds Pedersen. Wallet databases with observers. In *Advances in Cryptology – CRYPTO 92.* Lecture Notes in Computer Science 740, Springer-Verlag, 1993.
8. Jan L. Camenish, Jean-Marc Piveteau and Markus A. Stadler. An Efficient Electronic Payment System Protecting Privacy. In *Proceedings of ESORICS '94.* Lecture Notes in Computer Science 875, Springer-Verlag, 1995.
9. Tony Eng and Tatsuaki Okamoto. Single term divisible electronic coins. In *Advances in Cryptology – EUROCRYPT 94.* Lecture Notes in Computer Science 960, Springer-Verlag, 1995.
10. Niels Ferguson. Single term off-line coins. In *Advances in Cryptology – EUROCRYPT 93,* Lecture Notes in Computer Science 765, Springer-Verlag, 1994.
11. Niels Ferguson. Extensions of single term coins. In *Advances in Cryptology – CRYPTO 93,* Lecture Notes in Computer Science 773, Springer-Verlag, 1994.
12. GVU WWW Surveying Team, Georgia Institute of Technology, *GVU's 8th WWW User Survey.* Available at *http://www.gvu.gatech.edu/user_surveys/,* 1997.
13. Elaine K. Harris. *Customer Service: A Practical Approach,* Prentice Hall, Upper Saddle River, 1996.
14. Denison Hatch. Privacy: how much data do direct marketers really need?. In Rob Kling (ed.), *Computerization and Controversy: Value Conflicts and Social Choices, 2nd edition.* Academic Press, San Diego, 1996.
15. A.S. Hornby and A.P. Cowie (editor), *Oxford Advanced Learner's Dictionary of Current English*, Oxford University Press, Oxford, 1992

16. Stephen H. Low, Nicholas F. Maxemchuk and Sanjoy Paul. Anonymous Credit Cards. In *Proceedings of the 2nd ACM Conference on Computer and Communication Security.* 1994.
17. Anna Lysyanskaya and Zulfikar Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In *Financial Cryptography, 2nd International Conference, FC 98,* Lecture Notes in Computer Science 1465, Springer, 1998.
18. Gerrard Macintosh and Lawrence S. Lockshin. Retail relationship and store loyalty: A multi-level perspective. In *International Journal of Research in Marketing*, vol. 14, 1997.
19. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.
20. Netscape Communications Security, Cookies and Privacy FAQ, available at *http://www.cookiecentral.com/n_cookie_faq.htm*, 1997
21. Tatsuaki Okamoto. An efficient divisible electronic cash scheme. In *Advances in Cryptology – CRYPTO 95.* Lecture Notes in Computer Science 963, Springer-Verlag, 1995.
22. Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In *Advances in Cryptology – CRYPTO 91*. Lecture Notes in Computer Science 576, Springer-Verlag, 1992.
23. S. Pearson. How to achieve return on investment from customer loyalty – part 1. In *Journal of Targeting, Measurement and Analysis for Marketing,* vol. 3 no.1, 1994.
24. Cristian Radu, René Govaerts and Joss Vandewalle. Efficient electronic cash with restricted privacy. In *Financial Cryptography, 1st International Conference, FC 97,* Lecture Notes in Computer Science 1318, Springer, 1997.
25. Ronald. L. Rivest, Adi Shamir and Leonard Adlemann. A method for obtaining digital signatures and public-key cryptosystem. *Communications of the ACM,* vol. 21 no.2, 1978.
26. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition,* John Wiley & Sons. Inc., New York, 1996.
27. Byron Sharp and Anne Sharp. Loyalty programs and their impact on repeat-purchase loyalty patterns. In *International Journal of Research in Marketing*, vol. 14, 1997.
28. Yiannis S. Tsiounis. Efficient electronic cash: new notions and techniques. Ph.D. thesis. Department of Computer Science, Northeastern University, 1997.
29. David Whaler, The Unofficial Cookie FAQ, available at *http//www.cookiecentral.com/faq/*, 1999.
30. Yacov Yacobi. Efficient electronic money. In *Advances in Cryptology – ASIACRYPT 94.* Lecture Notes in Computer Science 917, Springer-Verlag, 1995.

Appendix: Blind Signature Protocols

For the following protocol descriptions, we will use the notation *C* for the customer and *T* as the trusted party (bank or merchant). Note that the message *m*, in our context, is the customer's public key, plus an optional pseudonym and relevant information.

Chaum Blind Signature

The Chaum blind signature protocol [5] is based on RSA. Let $n = pq$ be product of two large random primes. *T*'s RSA public keys are (n, e) and its private key is d. C wants *T* to sign *m* blindly, where $0 \le m \le n - 1$. Note that *T* has no knowledge of *m* whatsoever.

Signing protocol:

1. C chooses a random number k, where $1 \le k \le n - 1$. Frequently k is referred as the blinding factor. C blinds the message *m* by computing $m_0 = mk^e \bmod n$. C sends m_0 to *T*.
2. *T* signs the blinded message by computing $s_0 = (m_0)^d \bmod n$. *T* sends s_0 back to C.
3. C unblinds the signed blinded message s_0 by computing $s = k^{-1}s_0 \bmod n$. The result is a valid RSA signature *s* of *T* on *m*.

Verification process:

The verification process is the same like ordinary RSA signature verification. Refer to [25].

Chaum-Pedersen Blind Signature

Chaum and Pedersen presented a discrete log based blind signature in [7]. The protocol operates for any group G_q of order prime q. Let $q \mid (p - 1)$, where p is a prime. We define G_q as the unique subgroup of $\boldsymbol{Z}_p^*$ of order q. We also consider $g \in G_q$ as a generator of G_q. The discrete logarithm of $h \in G_q$ with respect to g is denoted by $\log_g h$.

We assume that p, q, and g are publicly known to all parties. *T*'s public key is the tuple (p, q, g, h), and the corresponding private key is x, where x satisfies $x = \log_g h$ or $g^x = h \bmod p$. *C* wants to obtain a signature of *T* on some message *m*, such that *T* never have any knowledge of *m*. Basically *T* should prove to *C* that $\log_g h = \log_{m_0} z_0$, where m_0 is the blinded message and z_0 is the 'signed' blinded message.

Signing protocol:

1. *C* chooses some random number $t \in \boldsymbol{Z}_q^*$ and then blinds the message *m* into $m_0 = m^t$, and sends m_0 to *T*.
2. *T* uses his private key x to calculate $z_0 = m_0^x$. *T* selects a random number $s \in \boldsymbol{Z}_q^*$. Then *T* sends z_0, $a_0 = g^s$, $b_0 = m_0^s$ back to C.
3. *C* chooses some random number $u \in \boldsymbol{Z}_q^*$ and $v \in \boldsymbol{Z}_q$. *C* calculates $a = (a_0 g^v)^u$ and $b = (b_0^{1/t} m^v)^u$. Then *C* computes $z = z_0^{1/t}$. Note that z is actually *T*'s 'signature', if *C* sent an unblinded message *m* at step 1. Also observe that if the protocol is done correctly, $a = (g^{s+v})^u$ and $b = (m^{s+v})^u$.

   C also creates a challenge $c = H(m, z, a, b)$. Since one of the objective of the blind signature is prevent *T* to link any blind signature request transcript to a resulting signature $\sigma = (z, a, b, r)$, we must also blind the challenge c into $c_0 = c/u \bmod q$. *C* then sends c_0 to T.
4. *T* responses back to *C* by sending $r_0 = s + c_0 x$.
5. *C* accepts if $g^{r_0} = a_0 h^{c_0}$ and $m_0^{r_0} = b_0 z_0^{c_0}$. Finally *C* computes $r = (r_0 + v)u \bmod q$. We now have $\sigma = (z, a, b, r)$, which is a valid signature of *T* on message *m*.

Verification process:

Provided that $\sigma = (z, a, b, r)$ is a signature of T on message m, let $c = H(m, z, a, b)$. Anyone can verify off-line that $g^r = ah^c$ and $m^r = bz^c$.