An Efficient Electronic Payment System Protecting Privacy

Jan L. Camenisch[1], Jean-Marc Piveteau[2], Markus A. Stadler[1]

[1] Institute for Theoretical Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland
Email: {camenisch, stadler}@inf.ethz.ch

[2] UBILAB
Union Bank of Switzerland
Bahnhofstrasse 45
CH-8021 Zurich, Switzerland
Email: piveteau@ubilab.ubs.ch

Abstract. Previously proposed anonymous electronic payment systems have the drawback that the bank has to maintain large databases, which is a handicap for the realization of such systems. In this paper, we present a practical anonymous payment system that significantly reduces the size of such databases. It uses the concept of anonymous accounts and offers anonymity as an add-on feature to existing EFTPOS systems.

Keywords: electronic payment systems, privacy, cryptography

1 Introduction

The number of private and corporate financial transactions that are done electronically is growing rapidly. From a user's point of view security, efficiency, and flexibility are the main advantages of existing or emerging electronic payment systems. However, most of the systems used commercially do not combine a high level of security with privacy protection, although several theoretical proposals for secure anonymous payment systems have been published [1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. While the market needs are not clearly established, governments and organizations like banks usually consider anonymity as an obstruction to the system security surveillance, and they prefer to protect users' privacy by legal and administrative steps. Furthermore, two technical characteristics shared by all of these theoretical proposals of secure payment systems protecting privacy compromise their realization:

- they present implementation difficulties, often related to the maintenance and the consultation of large databases necessary to prevent frauds;

[1] The first and the third author are jointly supported by the Swiss Federal Commission for the Advancement of Scientific Research (KWF), and the Union Bank of Switzerland.

- they are incompatible with existing electronic payment systems; this implies that their introduction would necessitate a complete redesign of currently used systems.

A secure electronic payment system protecting privacy can be seen as a protocol involving a customer, a shop and a bank. Both the customer and the shop have an account with the bank. One can distinguish between *on-line* payment systems, where all parties, the customer, the shop, and the bank, need to be connected on-line (at least once), and *off-line* payment systems, where each interaction during the protocol requires two communicating parties only. On-line systems have already been proposed for electronic coins [4, 6], and have been generalized to electronic cheques [7]. However, their applicability is significantly limited by the very large size of the database consulted on-line by the bank in order to prevent frauds (e.g. double-spending of an electronic coin). Off-line schemes have been proposed as an alternative. They do not present the drawback of the previous on-line schemes, since the bank consults its database after, and not during the payment. However, the published off-line systems do not prevent double-spending, but only allow to detect it and then to reveal the identity of the cheater.

In this paper, we propose a practical and efficient secure payment system protecting the customer's privacy. As for the majority of such systems, it is essentially based on the concept of blind signature [3]. Our protocol describes an on-line system which presents similar advantages as [4, 6, 7]. However, the database stored by the bank for preventing double-spending is significantly smaller, and its on-line consultation should not represent a handicap for concrete realization anymore[3]. Furthermore, our system is compatible with currently used electronic payment systems, i.e. it could be implemented as an added-value service offered by a bank to its customers.

2 Basic Concepts

The underlying model of an electronic payment system consists of three interacting entities: a bank B, a customer C, and a shop S. Both customer C and shop S have an account with the bank B. An electronic payment system consists of protocols that allow customer C to make a payment to the shop S. Although payment systems differ significantly from each other, it is often possible to identify three phases: a *withdrawal phase* involving the bank B and the customer C, a *payment phase* involving the customer C and the shop S, and a *deposit phase* involving the shop S and the bank B.

Customer, shop and bank have different security requirements. A shop, receiving a payment, wants to be sure that the bank will accept to credit its account with the paid amount. The bank wants to make sure that for each account credited, another account has been debited (i.e. the bank does not want anybody to

[3] In fact, the records consulted on-line are comparable to those used in existing on-line EFTPOS (=Electronic Funds Transfer at the Point Of Sale) systems.

to create money or to spend the same money more than once). Finally, a customer needs to be assured that money withdrawn from his or her account will be accepted for a payment; furthermore, he or she may desire privacy protection.

Time of Transactions

This model leads to a classification of payment systems according to the sequential ordering of the three phases. Let t_w (t_p, t_d) denote the time of the withdrawal (payment, deposit). Since the bank will not allow to deposit money which has not been withdrawn previously (assuming that the bank gives no credit), we have $t_w \leq t_d$, and a deposit will only be possible after a payment: $t_p \leq t_d$. With these conditions the three phases can take place in six orders. For most of these there are existing or proposed payment systems:

$t_p = t_w = t_d$ EFTPOS
$t_p < t_w = t_d$ cheque
$t_w < t_p = t_d$ on-line digital cash protecting privacy[4]
$t_p = t_w < t_d$
$t_w < t_p < t_d$ off-line digital cash protecting privacy[5]
$t_p < t_w < t_d$

Some of the security requirements mentioned above strongly depend on the order of these phases. For instance, the prevention of multiple spending of money is not a problem if the withdrawal takes place during the payment, i.e. $t_w = t_p$, because the shop can be sure that the customer's account has been debited for the payment. However this condition seems to be incompatible with any form of privacy protection if the bank knows the identifier of the customer during withdrawal (which seems necessary because the customer's account is debited): the shop could always tell the bank the exact time t_p which allows the bank to recover the customer's identity assuming that all withdrawals have been stored.

For this reason, all published payment systems protecting privacy have introduced a delay between withdrawal and payment. But such a delay could facilitate multiple spending of money. One way to solve this problem is that the bank stores all previously spent coins. However this implies the maintenance of large databases.

Anonymity, Untraceability and Privacy

Anonymity and untraceability are often used as synonyms. We prefer to make a difference between these terms, grasping in this way different levels of protection. Each customer is characterized by an identifier (e.g. name, account number, social security number). A customer is said to be *anonymous* if his or her identifier cannot be linked to the sent messages. However, it may be feasible to link the

[4] See [2, 4, 6, 7].
[5] See [1, 5, 8, 10, 11, 12, 13, 14].

different messages transmitted by the same customer. An anonymous customer is said to be *untraceable* if no message can be linked not only to the customer's identifier, but also to any previously sent messages; so *untraceability* is stronger than *anonymity*. A system providing either anonymity or untraceability is said to *protect privacy*.

Blind Signature Scheme

A blind signature scheme is a tuple $(Bl(\cdot,\cdot), Sig(\cdot), Ex(\cdot,\cdot), Ver(\cdot,\cdot))$. For a message m and a random value ρ, $Bl(\rho, m)$ is the blinded message, $\sigma' = Sig(Bl(\rho, m))$ is the blind signature and $\sigma = Ex(\rho, Sig(Bl(\rho, m)))$ is the 'real' signature extracted from σ' using ρ. The variable ρ, called *blinding factor*, is chosen at random to prevent the signer from learning m and to guarantee that $Bl(\rho, m)$ and σ' are not linkable to m and σ. The predicate $Ver(\cdot,\cdot)$ is used to check the validity of the signature:

$$\forall \rho, \forall m: \qquad Ver(m, Ex(\rho, (Sig(Bl(\rho, m))))) = 1$$

3 Secure Payment System with Anonymous Accounts

The basic idea of our proposal is to conceal the customer's identity during the withdrawal phase. This is achieved by introducing anonymous accounts[6]. The bank B is responsible for the maintenance of two types of accounts: personal accounts and anonymous accounts. Personal accounts are normal bank accounts associated with a customer's identifier, whereas the identity of the owner of an anonymous account is unknown. The main part of our new system is a set of protocols which allows a customer to anonymously transfer money between accounts. Payments are done on-line by debiting the payer's account and simultaneously paying the same amount into the payee's account. If the payer uses an anonymous account, his or her identity cannot be linked to the payment.

Let us now describe our payment system in detail. The system parameters are a one-way hash function $\mathcal{H}$ and a set of blind signature schemes $\{(Bl_v, Sig_v, Ex_v, Ver_v)\}$. Each signature scheme is used to associate a transaction with a certain value v, e.g. the use of Sig_{100} would indicate a transaction worth hundred dollars.

For the opening of anonymous accounts and for the anonymous transfer of money, two new phases are required: the *anonymous account opening phase* and the *anonymous deposit phase*[7]. The payment and deposit phases merge into the *transaction phase*.

[6] Anonymous accounts have also been introduced in [1] and [2], but they do not share the same characteristics as in our protocol.

[7] Here deposit means a deposit to the customers anonymous account and not to the shop's account.

Anonymous Account Opening Phase

To open an anonymous account, the customer C proceeds as follows:

1. C contacts the bank B without showing his or her actual identifier (therefore B does not know anything about the true identity of C during this phase). B opens a new anonymous account A with account number acc_A, secret parameter k_A, and a counter cnt_{AB}. B sets $cnt_{AB} = 0$.
2. B sends acc_A and k_A to C.
3. C stores acc_A, k_A and initializes a counter $cnt_{AC} = 0$.

Withdrawal Phase

In order to transfer v dollars from his or her personal account to the anonymous account acc_A, C first withdraws v dollars as follows:

1. C proves his or her identity to B, randomly selects r and ρ, computes the message $m = \mathcal{H}(acc_A, cnt_{AC}, r)$, and sends the blinded message $m' = Bl_v(\rho, m)$ together with v to B.
2. B debits C's personal account with v dollars, and returns the blinded signature $\sigma' = Sig_v(m')$.
3. C extracts the valid signature $\sigma_v = Ex_v(\rho, \sigma')$ of m.
4. C increments cnt_{AC} by one.

The signed message $m = \mathcal{H}(acc_A, cnt_{AC}, r)$ may be seen as an anonymous coin (like a metal coin). The fact that the message contains acc_A prevents anybody from paying the same anonymous coin into different anonymous accounts. This offers simultaneously a protection against loss or theft of anonymous coins. The counters cnt_{AC} and cnt_{AB} guarantee that the customer cannot deposit the same coin more than once in the same account.

Anonymous Deposit Phase

1. C sends acc_A, r, v and σ_v to B.
2. B computes $m = \mathcal{H}(acc_A, cnt_{AB}, r)$, using cnt_{AB} stored in the account data of account A, and checks the validity of the signature σ_v.
3. B pays v dollars into acc_A.
4. B increments cnt_{AB} by one.

To guarantee the acceptance of all deposits it is necessary that the anonymous electronic coins are deposited in the same order as they have been withdrawn, i.e. the customer has to deposit the coin containing the current value of cnt_{AB}.

Transaction Phase

We assume that the three parties communicate on-line, i.e. every communication between any two of them is heard by the third, and that C has to pay p dollars to the shop S.

1. C is identified by B through the knowledge of k_A as the owner of the anonymous account acc_A.
2. B debits acc_A with p dollars.
3. B pays p dollars into S's account.

The shop S who hears on-line the conversation between B and C knows that the requested payment has taken place, and the transaction between C and S can be completed.

Note that the protocol of the withdrawal phase can easily be modified to transfer money from an anonymous account to another.

It has often been argued that on-line systems are unpractical for technical reasons. This is true if searching in a large database has to be realized on-line. However, using current telecommunication technology, the connection itself between three entities, even if one of them (the bank B) is involved in each transaction, does not present an unsolvable problem. In fact, many existing EFTPOS systems use an on-line link between a bank (or a clearing center), a shop and a customer[8].

Our payment system assures the customer's anonymity, but not untraceability if the same anonymous account is used for several transactions. Complete untraceability is provided if every anonymous account is used only once.

4 Related Work

Let us compare our proposal with some previously proposed on-line payment systems.

The first secure anonymous payment system was described by Chaum in [4]. Let us recall the essential idea of this scheme:

1. **Withdrawal:** B provides C with a signature of a blinded coin. C extracts a valid signature of the coin.
2. **Payment and Deposit:** C presents the signed coin to S, which sends it directly to B, and B consults on-line a database to check whether the coin has not been spent up to now.

A blinded coin in [4] is comparable to a anonymous account used only once (to provide perfect untraceability) in our scheme. Both are indeed anonymous pieces of information used to credit the shop's account. However, there is an

[8] Note that in EFTPOS systems the connection is established between the bank and the shop, so the connection itself does not give information about the customer.

essential difference: in our proposal, the account number is chosen by the bank B during the anonymous account opening phase, while in [4] the generation of a blinded coin preceding the withdrawal does not necessitate the intervention of the bank.

This apparently subtle difference has an important practical consequence: our scheme requires the bank B to maintain only a list of open anonymous accounts, which can be interpreted (if the accounts are used only once) as a record of coins which have already been debited from some (personal) account, but have not been spent yet. Such a database can be expected to have a reasonable size.

Several variations on this first scheme have been presented in [6]. One of them, providing untraceability for a payer with a designated payee, presents similarities with the part of our proposal where the customer transfers money from his or her personal account to an anonymous account. However, the fact that in this part of our scheme the payer and the payee, corresponding to the same person, trust each other (what could not be assumed in [6]) allows to prevent a double deposit by introducing a sequence number. This considerably reduces the amount of data to be stored. Such a simple method would not be adequate in the general case [6].

In [2] Bürk and Pfitzmann proposed a payment system using so called standard values. A standard value may be seen as an anonymous account upon which a predefined value has been deposited. The owner of a standard value is known to the bank by a pseudonym. Payments are done by transferring the ownership of a standard value: the bank replaces the pseudonym of the payer (who was registered as the owner of the standard value) by the pseudonym of the payee (who is the new owner of the standard value). Such a payment is anonymous, but it is possible for the bank to link two transactions where the payee of the first transaction is the payer of the second. As suggested in [2], this problem could be solved using techniques described in [4] to change a pseudonym, but further modifications seem to be necessary in order to prevent double-spending. In our proposal, this problem is solved by the way money is transferred anonymously from one account to another.

5 Conclusions

The version of our system providing perfect untraceability, even if it appears to be more practical than previous proposals with similar characteristics, is not completely satisfactory since each transaction requires the opening of a new anonymous account. We believe that our scheme is particularly suited for a customer requiring anonymity (and not untraceability), because of its relative simplicity and its high flexibility. From a practical point of view, it is interesting to observe that the use of anonymous accounts allows intermediary levels of privacy protection, between the simple anonymity and the complete untraceability. It suffices indeed for the customer to have different anonymous accounts with the bank. Whenever he or she desires that two transactions remain unlinkable, two different anonymous accounts must be used.

Furthermore, the following facts might support the acceptance of this anonymous payment system:

- It is compatible with existing EFTPOS systems, since for the majority of them, a link to the bank (or a clearing center) is created when the customer is visiting the shop. This means that the three parties actually communicate on-line during the transaction. Furthermore, from the shop's viewpoint, it does not matter whether the customer is using a personal account or an anonymous account. A realization of this scheme would therefore neither require a modification of the communication system itself, nor the replacement of the shop's installation.
- It considers anonymity as an added-value service which may be requested by the customer. Its management (e.g. charging) is simplified by the fact that the payee does not have to modify its behaviour for an anonymous transaction.

Acknowledgment

The authors would like to thank U. Maurer and H.P. Frei for their support and the anonymous referee for valuable remarks.

References

1. S. Brands: Untraceable Off-line Cash in Wallets with Observers, *Advances in Cryptology, Crypto '93*, LNCS 773, Springer-Verlag, pp.302-318.
2. H. Bürk, A. Pfitzmann: Digital Payment Systems Enabling Security and Unobservability, *Computer & Security, 8 (1989)*, pp. 399-416
3. D. Chaum: Blind Signature Systems, *Advances in Cryptology, Crypto '83*, Plenum, p. 153.
4. D. Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, 28 (1985), pp. 1030-1044.
5. D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, *Advances in Cryptology, Crypto '88*, LNCS 403, Springer-Verlag, pp. 319-327.
6. D. Chaum: Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V. (North-Holland), 1989, pp. 69-93.
7. D. Chaum: Online Cash Checks, *Advances in Cryptology, Eurocrypt '89*, LNCS 434, Springer-Verlag, pp. 289-293.
8. D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, A. Steenbeek: Efficient Offline Electronic Checks, *Advances in Cryptology, Eurocrypt '89*, LNCS 434, Springer-Verlag, 294-301.
9. D. Chaum, T. Pedersen: Wallet databases with observers, *Advances in Cryptology, Crypto '92*, LNCS 740, Springer-Verlag, pp. 89-105.
10. A. De Santis, G. Persiano: Communication Efficient Zero-Knowledge Proofs of Knowledge (with Applications to Electronic Cash), *Proceedings of STACS '92*, LNCS 577, Springer-Verlag, pp. 449-460.
11. N. Ferguson: Single Term Off-line Coins, *Advances in Cryptology, Eurocrypt '93*, LNCS 765, Springer-Verlag, pp. 318-328.

12. M. Franklin, M. Yung: Towards Provably Secure Efficient Electronic Cash, Columbia University, Dept. of Computer Science, TR CUSC-018-92, April 24, 1992.
13. T. Okamoto, K. Ohta: Disposable Zero-Knowledge Authentication and Their Application to Untraceable Electronic Cash, *Advances in Cryptology, Crypto '89*, LNCS 435, Springer-Verlag, pp. 134-149.
14. T. Okamoto, K. Ohta: Universal Electronic Cash, *Advances in Cryptology, Crypto '91*, LNCS 576, Springer-Verlag, pp. 324-337.