An Efficient Fair Payment System

Jan Camenisch*
Dept. of Computer Science
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich, Switzerland
Email: camenisch@inf.ethz.ch

Jean-Marc Piveteau
Union Bank of Switzerland
UBILAB
Bahnhofstrasse 45
CH-8021 Zürich, Switzerland
Email: piveteau@ubilab.ubs.ch

Markus Stadler*
Dept. of Computer Science
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich, Switzerland
Email: stadler@inf.ethz.ch

Abstract

Many proposed payment systems allow the payer to remain anonymous during a transaction. However, this unconditional privacy protection could be misused by criminals, e.g. for blackmailing or money laundering. With a fair payment system, anonymous payments are still possible, but the anonymity can be removed with the help of a trusted party which need not be involved in the transaction itself. In this paper, we present an efficient fair payment system and we discuss its security.

1 Introduction

Efficient electronic payment systems are an important prerequisite for electronic commerce. The design of such payment systems poses many security-related problems. Apart from the common security requirements such as the prevention of frauds, the protection of the participants' privacy is an important issue.

In many systems the protection of the user's privacy relies exclusively on administrative and legal measures. Using cryptographic tools such as blind signatures [7], it is possible to design electronic payment systems that allow participants to remain anonymous during a transaction, without affecting the security of the system (e.g. [2, 5, 8, 9]). Such systems offer an unconditional privacy protection, but they can be misused by criminals for perfect blackmailing [17] or for money laundering.

The concept of a *fair payment system*, independently proposed in [3] and [16], offers a compromise between the legitimate need of privacy protection and an effective prevention of misuse by criminals. On one hand, the customer's privacy cannot be compromised by the bank or by the payee. On the other hand, there is a trusted third party, called the judge, which can (in cooperation with the bank) remove the anonymity of a transaction if the system is being misused by criminals. Furthermore, the trusted third party is not involved in the transactions.

In this paper, we present an efficient fair payment system based on the anonymous payment system described in [5]. The system is currently realized as a prototype, with the customer functionality implemented on smart-cards.

The basic concepts of fair payment systems are discussed in Section 2. The new system is described in Section 3, followed by a discussion on its security. Some results on the prototype implementation are given in Section 4. Finally, in Section 5 we compare our proposal with other existing payment systems with similar properties.

2 Basic Concepts

An electronic payment system consists of a set of protocols between three interacting parties: a bank, a customer (the payer), and a shop (the payee). The customer and the shop have both an account with the bank. The goal of the system is to transfer money in a secure way from the customer's account to the shop's account. It is possible to identify three different phases: a *withdrawal phase* involving the bank and the customer, a *payment phase* involving the customer and the shop, and a *deposit phase* involving the shop and the bank. In an *off-line* system, each phase occurs in a separate transaction, whereas in an *on-line* system, such as ours, payment and deposit take place in a single transaction involving all three parties.

Bank, shop and customer have different security requirements. The bank wants to make sure that for each account credited, another account has been debited. The shop, receiving a payment, wants to be assured that the bank will accept to credit its account with the received amount. Finally, the customer wants to be sure that money he[1] has withdrawn will be accepted for a payment. Furthermore, the customer may require that his privacy be protected.

Anonymous electronic payment systems (e.g. [2, 5, 8, 9]) prevent anybody, including the bank, from violating the customer's privacy. Payments are anonymous and different payments of the same customer are unlinkable. This is achieved using cryptographic mechanisms such as blind signature schemes [4, 7].

* Supported by the Swiss Federal Commission for the Advancement of Scientific Research (KWF) and by the Union Bank of Switzerland.

[1] In this paper the customer is male whereas the judge is female.

CCS' 96, New Delhi, India
©1996 ACM 0-89791-892-0/96/03..$3.50

A problem with anonymous payment systems is that they could be misused by criminals, e.g. for perfect blackmailing [17] or for money laundering. This is possible because the anonymity of payments prevents the bank from tracing money.

Different measures have been proposed to offer a limited protection against this kind of threat. A restriction of the maximal possible amount transferred during a transaction should make the system unattractive for money laundering. However, this is effective only if the number of transactions that can be done during a short period of time is limited. In the case of blackmailing, a possible measure for systems such as [8] would be to stop the system when a withdrawal is done under threat, which is unrealistic.

The concept of *fair payment systems*[2] was independently proposed in [3] and [16]. A fair payment system, like other anonymous payment systems, protects the privacy of the customer. But in contrast to payment systems that protect the privacy unconditionally, there is an additional, trusted party, called the *judge*. The judge has the following attributes:

- She can remove the anonymity of a transaction in cooperation with the bank. This can happen in two different ways: Either the bank provides the judge with the data of a (suspect) withdrawal and asks for information that allows to identify the corresponding deposit (or payment), or the bank provides her with data of a (suspect) deposit and asks for the corresponding withdrawal.

- She is only involved during the setup of the system, possibly in the opening of accounts, but not in the transactions.

- She is trusted only in privacy-related matters, e.g. the bank may not trust her about forging money.

Note that it is possible to share the functionality of the judge among several trusted parties (e.g. the trustees in [3]).

An adequate protection against money laundering is offered by fair payment systems because it is possible for the judge, in cooperation with the bank, to determine the origin or the destination of dubious money transfers.

Fair payment systems also prevent the "perfect crime" scenario described in [17], where a customer is blackmailed and forced to act as an intermediary between the blackmailer and the bank during the withdrawal of money. In a perfectly anonymous payment system, the ransom cannot be recognized later. However, in a fair payment system, the judge can trace the blackmailed money.

3 Description of the Payment System

The fair payment system presented in this section is based on the anonymous payment system of [5]. Let us briefly recall its principle. The bank manages two types of accounts: *personal accounts*, of which the owner is known to the bank, and *anonymous accounts*, of which only a pseudonym of the owner is known. An anonymous payment is simply a transfer from a customer's anonymous account to the shop's account. The main part of the system consists of an efficient method for transferring money from a personal account to an anonymous account without revealing the correspondence between them. This is realized using an electronic coin that can be paid only into a single anonymous account. Therefore double-spending of the coin can be prevented by a simple counter (instead of maintaining a large database containing all spent coins). Furthermore, the perfect unlinkability of personal and anonymous accounts is realized by using a blind signature scheme. In order to achieve *fairness*, this system is modified in the following way:

- The judge knows the correspondence between personal and anonymous accounts.

- A coin withdrawn from a personal account can only be deposited into a corresponding (i.e. registered) anonymous account.

The basic idea of the fair payment system presented in this paper can be informally described as follows. A public key is associated with each personal account. To open a new anonymous account, the customer has to provide a public key which is derived from the public key of his personal account. The correspondence between the two keys must be registered at the judge. When actually opening the anonymous account, the bank checks whether this registration has taken place and whether the public key of the anonymous account is correctly constructed.

Coins withdrawn from the personal account are signed by the bank with respect to the public key of the personal account. The customer can then derive a valid signature with respect to the public key of a corresponding anonymous account. Signatures valid for other anonymous accounts cannot be derived.

Because of the registration of corresponding public keys, it is possible to trace transactions in cases of money laundering. Furthermore, tracing is also possible if the customer is blackmailed: coins can be paid only into an anonymous account that corresponds to the customer's personal account (even if the blackmailer opens the anonymous account himself).

3.1 Protocols

We now give a detailed description of the system. The initialization of the system is divided into three different steps: the *Opening of a Personal Account* (Fig. 1), the *Registration at the Judge* (Fig. 2), and the *Opening of an Anonymous Account* (Fig. 3).

After the initialization has been completed, money can be transferred from a personal account to a corresponding anonymous account. This transfer is split into two steps. During the *Withdrawal from Personal Account* (Fig. 4), the customer debits his personal account. The withdrawn money is paid into the corresponding anonymous account using the protocol *Deposit into Anonymous Account* (Fig. 5). A payment to a shop is made as a simple transfer from the customer's anonymous account to the shop's account.

Most of the described protocols need a preceding mutual identification of the involved parties by some adequate protocol. However, in some of the protocols the customer must not

[2] The terminology *fair payment system* has been actually introduced in [6]. It corresponds to the concept of payment systems with *trustee-based tracing* introduced in [3].

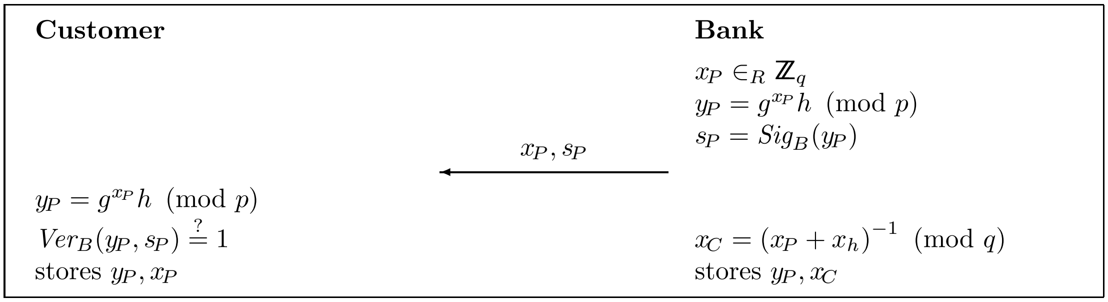
Customer
Bank
$x_P \in_R \mathbb{Z}_q$
$y_P = g^{x_P} h \pmod{p}$
$s_P = Sig_B(y_P)$
x_P, s_P
$y_P = g^{x_P} h \pmod{p}$
$Ver_B(y_P, s_P) \overset{?}{=} 1$
$x_C = (x_P + x_h)^{-1} \pmod{q}$
stores y_P, x_P
stores y_P, x_C

Figure 1: Opening of a Personal Account

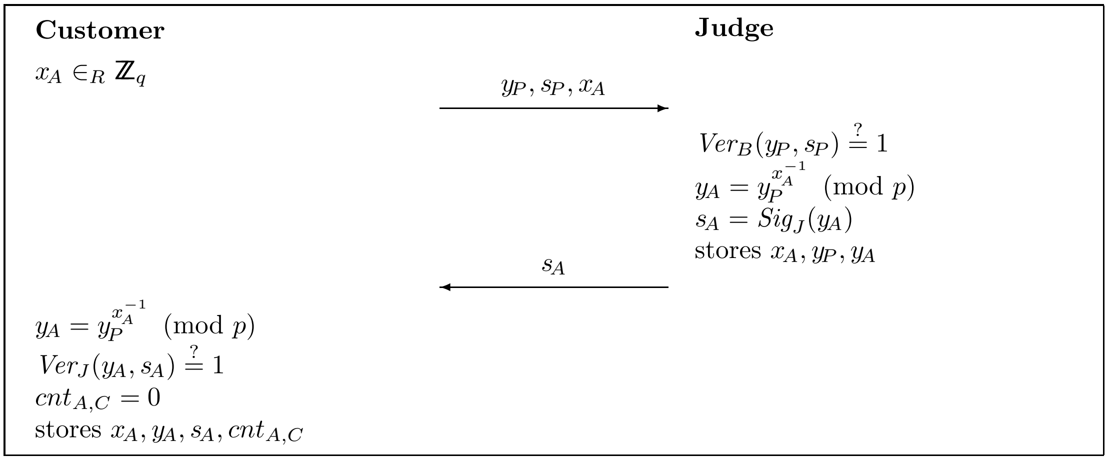
Customer
Judge
$x_A \in_R \mathbb{Z}_q$
y_P, s_P, x_A
$Ver_B(y_P, s_P) \overset{?}{=} 1$
$y_A = y_P^{x_A^{-1}} \pmod{p}$
$s_A = Sig_J(y_A)$
stores x_A, y_P, y_A
s_A
$y_A = y_P^{x_A^{-1}} \pmod{p}$
$Ver_J(y_A, s_A) \overset{?}{=} 1$
$cnt_{A,C} = 0$
stores $x_A, y_A, s_A, cnt_{A,C}$

Figure 2: Registration at the Judge

be identified, i.e. the *Registration at the Judge*, the *Opening of the Anonymous Account*, and the *Deposit into Anonymous Account*.

System parameters

Let p be a large prime, q a prime divisor of $p-1$, $g \in \mathbb{Z}_p^*$ of multiplicative order q, and $\mathcal{H}$ a one-way hash function. The computation of the discrete logarithm modulo p to the base g is assumed to be intractable. Let V be the set of possible transaction values.The bank selects $x_h \in \mathbb{Z}_q$, and $x_v \in \mathbb{Z}_q$ for each $v \in V$. The values $g, h = g^{x_h} \pmod{p}$ and $\{z_v\}_{v \in V}$ with $z_v = g^{x_v} \pmod{p}$ are public, while x_h and $\{x_v\}_{v \in V}$ are kept secret. Let (Sig_B, Ver_B) be a signature scheme of the bank. Sig_B is the bank's secret signature generation function and Ver_B is the public verification function. The following must hold: $\forall m, s : Ver_B(m, s) = 1 \iff s = Sig_B(m)$. Similarly, let (Sig_J, Ver_J) be a signature scheme of the judge.

The concatenation of the strings α and β is denoted by $\alpha \| \beta$. The expression $\xi \in_R X$ means that ξ is randomly chosen from the (finite) set X according to the uniform distribution.

Opening of a Personal Account

First, the customer identifies himself to the bank. Then the protocol in Figure 1 is carried out. The bank chooses x_P at random, calculates y_P and sends x_P and a signature of y_P to the customer. The public key y_P can be considered as the account number of the personal account. The integer x_P can be seen as the customer's part of the secret key of y_P while x_C is the bank's part of this secret key.

Registration at the Judge

In order to open a new anonymous account, the customer must first generate a new anonymous account number y_A and register the correspondence between y_A and his personal account number y_P at the judge. This is accomplished by the protocol given in Figure 2. The customer chooses x_A at random and sends it together with y_P and s_P to the judge. By checking the bank's signature s_P the judge verifies that y_P is a valid account number. After having calculated y_A the judge sends the customer her signature of it. This signature now enables the customer to open the anonymous account. The variable $cnt_{A,C}$ is the customer's counter for the number of transfers between the accounts y_P and y_A.

Opening of the Anonymous Account

To open the anonymous account corresponding to y_A the customer contacts the bank anonymously. Then the protocol in Figure 3 is carried out. This protocol is essentially a

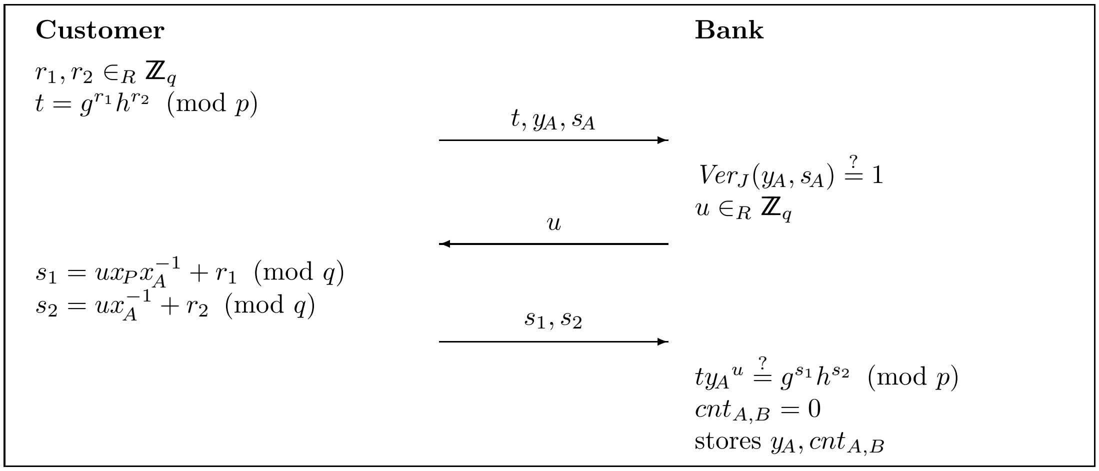
Customer
Bank
$r_1, r_2 \in_R \mathbb{Z}_q$
$t = g^{r_1} h^{r_2} \pmod p$
t, y_A, s_A
$Ver_J(y_A, s_A) \overset{?}{=} 1$
$u \in_R \mathbb{Z}_q$
u
$s_1 = u x_P x_A^{-1} + r_1 \pmod q$
$s_2 = u x_A^{-1} + r_2 \pmod q$
s_1, s_2
$t {y_A}^u \overset{?}{=} g^{s_1} h^{s_2} \pmod p$
$cnt_{A,B} = 0$
stores $y_A, cnt_{A,B}$

Figure 3: Opening of the Anonymous Account

proof by the customer to the bank that he knows the representation of y_A with respect to g and h, i.e. that he knows $\xi_1, \xi_2 \in \mathbb{Z}_q$ with $y_A = g^{\xi_1} h^{\xi_2}$ (see [1], section 8). By checking the validity of s_A, the bank verifies indirectly that the judge knows the personal account number corresponding to y_A and vice versa. The variable $cnt_{A,B}$ is the bank's counter for the number of deposits into the anonymous account y_A. The customer does no longer need to store s_A at the end of this step.

Bank and customer also agree on some form of future authentication for the customer as the owner of this anonymous account.

Withdrawal from Personal Account

After having opened the anonymous account y_A the customer can transfer money to it. To do so he first withdraws money from his personal account y_P. After he is identified by the bank as the owner of the account, bank and customer execute the protocol as indicated in Figure 4. It is a protocol to blindly obtain a Schnorr-signature [15] (s', c) of the message $y_A \| cnt_{A,C}$ for the public key z_v with respect to the base y_P. Before the customer can pay the withdrawn money into his anonymous account, he must transform the obtained signature into one with respect to the base y_A. This can be done by simply multiplying s' by x_A. Thus the pair (s, c) is the signature of the message $y_A \| cnt_{A,C}$ for the public key z_v with respect to the base y_A. The corresponding verification equation is:

$$c = \mathcal{H}(t \| y_A \| cnt_{A,C})$$

where $t = y_A^s z_v^c \pmod p$.

Deposit into Anonymous Account

The protocol given in Figure 5 allows the customer to deposit the withdrawn money into the appropriate anonymous account. For this protocol there is no need for the bank to identify the customer.

Payment

When the money has been paid into the anonymous account, the customer can use it for a payment. For such a payment, the shop, the customer and the bank have to be on-line. The customer is identified by the bank as the owner of the anonymous account y_A. The payment itself is then a on-line transaction from account y_A to the shop's account. The bank only has to prevent overdraft, i.e. to check on-line the balance of the account used for the payment.

Although the customer's identity is not revealed, the bank can still link different transactions when the same anonymous account is used for different payments. However, for transactions that should not be linked by the bank, the customer can use different anonymous accounts corresponding to the same personal account.

Removal of the Anonymity

Since the judge knows the correspondence between personal and anonymous accounts, she can at any time find the origin or the destination of a transfer, when provided with anonymous or personal account numbers.

3.2 Security Analysis

Signature generated during the withdrawal protocol

The bank wants to be sure that the customer, even with the help of the judge, is not able to compute a valid coin without carrying out the withdrawal protocol. It appears to be practically impossible for the customer to generate a valid signature without knowing the discrete logarithm of z_v to the base y_A. In particular, it is easy to see that breaking the withdrawal protocol would imply that Okamoto's blind version [13] of Schnorr's scheme is insecure.

Furthermore, it is easy to see that the customer cannot compute the discrete logarithm of z_v to the base y_A, even in collaboration with the judge. The customer has indeed proved during the opening of the anonymous account that he knows ξ_1 and ξ_2 with $y_A = g^{\xi_1} h^{\xi_2} \pmod p$. Assume

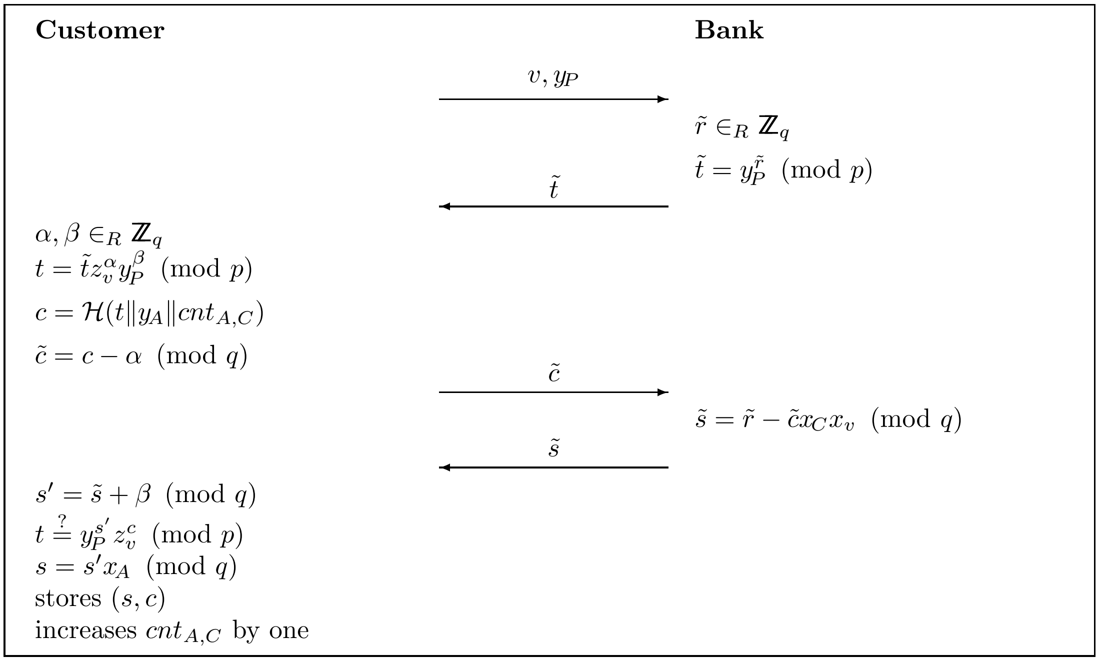
Customer
Bank
v, y_P
$\tilde{r} \in_R \mathbb{Z}_q$
$\tilde{t} = y_P^{\tilde{r}} \pmod{p}$
$\tilde{t}$
$\alpha, \beta \in_R \mathbb{Z}_q$
$t = \tilde{t} z_v^{\alpha} y_P^{\beta} \pmod{p}$
$c = \mathcal{H}(t \| y_A \| cnt_{A,C})$
$\tilde{c} = c - \alpha \pmod{q}$
$\tilde{c}$
$\tilde{s} = \tilde{r} - \tilde{c} x_C x_v \pmod{q}$
$\tilde{s}$
$s' = \tilde{s} + \beta \pmod{q}$
$t \overset{?}{=} y_P^{s'} z_v^{c} \pmod{p}$
$s = s' x_A \pmod{q}$
stores (s, c)
increases $cnt_{A,C}$ by one

Figure 4: Withdrawal from Personal Account

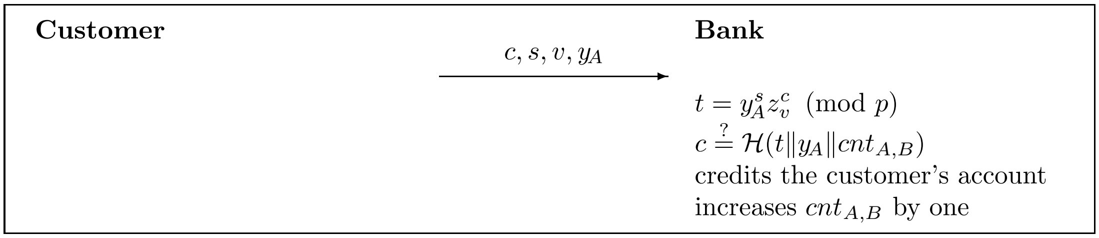
Customer
Bank
c, s, v, y_A
$t = y_A^{s} z_v^{c} \pmod{p}$
$c \overset{?}{=} \mathcal{H}(t \| y_A \| cnt_{A,B})$
credits the customer's account
increases $cnt_{A,B}$ by one

Figure 5: Deposit into Anonymous Account

furthermore that he can determine the discrete logarithm of z_v to the base y_A. This means that he has an algorithm allowing, on input g, h, z_v, to compute ξ_1, ξ_2, ξ_A, y_A with $y_A = g^{\xi_1} h^{\xi_2} \pmod{p}$ and $z_v = y_A^{\xi_A} \pmod{p}$. This implies that, for given g, h, z_v, he has a procedure to find $\xi_1, \xi_2, \xi_3 \in \mathbb{Z}_q^*$ with $1 = g^{\xi_1} h^{\xi_2} z_v^{\xi_3} \pmod{p}$. However, the existence of such a procedure is known to be equivalent to the existence of an algorithm solving the discrete logarithm problem [1].

Multiple payments

Because the electronic coin contains the anonymous account number, the customer cannot pay the same coin into different anonymous accounts. The counters cnt_{AC} and cnt_{AB} guarantee that the customer cannot deposit the same coin more than once into the same account.

Modification of the transfer value

The system should prevent a dishonest customer from withdrawing an electronic coin of value v and transforming it into a coin of value $v' > v$. This would be possible if the customer was able to compute the discrete logarithm of $z_{v'}$ to the base z_v; however, this is assumed to be an intractable problem. There seems to be no other way to modify the value of a given electronic coin.

Unlinkability of withdrawal and deposit

Obviously, unlinkability between the withdrawal from the personal account and the deposit into the anonymous account can be achieved only if many transactions (of each transaction value) take place. Additionally, the following has to be satisfied: First, it must not be possible for the bank to link transactions by analyzing the time they have taken place. Therefore, the customer should choose the period of time between withdrawal and deposit appropriately. Second, the bank's view of two corresponding transactions must be unlinkable. This is fulfilled because for each $v \in V$, the random variables $View_1^v = (x_C, y_P, \tilde{r}, \tilde{t}, \tilde{c}, \tilde{s})$ and $View_2^v = (y_A, s, c, cnt_{A,B})$ are statistically independent: For a given pair $(View_1^v, View_2^v)$, let x_A be the discrete logarithm of y_A to the base y_P, $\alpha = c - \tilde{c} \pmod{q}$ and

$\beta = sx_A^{-1} - \tilde{s} \pmod q$. It is easy to see that this is the only possible choice for α and β if $View_1^v$ has to be the bank's view during the withdrawal phase corresponding to the deposit with bank's view given by $View_2^v$. It remains to show that this choice is always valid, i.e. that we have $c = \mathcal{H}(t \| y_A \| cnt_{A,B})$ where $t = \tilde{t} z_v^{\alpha} y_P^{\beta} \pmod p$. The following equalities are easy to check:

$$\begin{aligned}
\tilde{t}\, z_v^{\alpha} y_P^{\beta} &= y_P^{\tilde{r}}\, z_v^{c-\tilde{c}} y_P^{sx_A^{-1}-\tilde{s}} && \pmod p \\
&= y_P^{\tilde{r}-(\tilde{r}-\tilde{c}x_C x_v)} z_v^{c-\tilde{c}} y_P^{sx_A^{-1}} && \pmod p \\
&= y_P^{\tilde{c}x_C x_v}\, z_v^{c-\tilde{c}} y_A^{s} && \pmod p \\
&= z_v^{\tilde{c}} z_v^{c-\tilde{c}} y_A^{s} && \pmod p \\
&= y_A^{s} z_v^{c} && \pmod p
\end{aligned}$$

and therefore:

$$\mathcal{H}(t \| y_A \| cnt_{A,B}) = \mathcal{H}(y_A^s z_v^c \pmod p) \| y_A \| cnt_{A,B}) = c.$$

The last equality follows from the fact that (c, s) is a valid signature.

Cross-payments

A cross-payment is a transfer from a personal account y_P to an anonymous account $\tilde{y}_A$ which is registered at the judge to belong to another personal account $\tilde{y}_P$. To do such a cross-payment, it seems necessary that an attacker knows the discrete logarithm of $\tilde{y}_P$ to the base y_P, which would imply that he knows the secret value $x_h = \log_g h$. But this is assumed to be intractable and so cross-payments are not possible.

4 Implementation

It is essential for the customer that his private data (e.g. identification information, or secrete encryption key) are securely stored and not endangered when carrying out a protocol. This becomes even more important if the customer wants to be mobile and have access to the network at any point, even through untrusted terminals (e.g. shop's terminal). To fulfill these requirements, the customer needs a portable secure computing device such as a smart-card. This device is limited in size, thus its computation power and storage capacity are restricted.

To demonstrate the practicability and efficiency of the fair payment system described in this article, we decided to implement the customer's functionality on a smart-card (the Philips Cryptocard [14] with the 83C852-chip[3]). To simulate a real payment system environment, the implementation includes a key management, a mutual authentication procedure, and an encryption mechanism (based on the cipher IDEA [11]). The implementation allows the customer to manage one personal and two anonymous accounts on the card.

5 Related Work

There exist several other proposals for payment systems offering a conditional privacy protection [6, 3, 12] with a trusted third party.

In the anonymous credit card system [12] each customer is provided with a personal account and an anonymous account on another (Swiss) bank. Anonymous transfers between these two accounts are realized using an intermediary, called communication exchange. The information needed to link personal and anonymous accounts is shared among the customer's banks and the communication exchange, i.e. the banks have to cooperate with the communication exchange to recover this correspondence.

The first fair payment systems with an "off-line" trusted party have been proposed in [3], where unconditionally anonymous payment systems [2, 10] are extended by the concept of trustee-based tracing.

Independently, [16] described the concept of fair blind signature schemes, which allows a trusted third party to link a signed message to the corresponding signature generation and vice versa. By replacing the signature scheme it is possible transform unconditionally anonymous payment systems into fair payment systems. In [6] two variations of this method are described.

6 Conclusion

We have presented a new fair payment system. It allows customers to perform anonymous payments. However the anonymity can be removed on request by a trusted party. We believe that this approach offers a acceptable compromise between the legitimate right for privacy protection and the need for effective methods to prevent criminal misuses of this privacy. Furthermore, the efficiency of our proposal makes is well suited as a payment system over networks such as Internet and for implementations on smart cards.

Acknowledgments

The authors thank Ueli Maurer and H.-P. Frei for their support. Roberto Citrini, Markus Isler, Arthur Marxer and Martin Perewusnyk implemented the prototype. We are grateful for the help of Moti Yung in preparing this paper. Also the comments of the anonymous referees were much appreciated.

References

[1] S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, CWI, Apr. 1993.

[2] S. Brands. Electronic cash systems based on the representation problem in groups of prime order. In *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 302–318. Springer Verlag, 1994.

[3] E. Brickell, P. Gemmel, and D. Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *Proceedings of the 6th Annual*

[3] 8-bit CPU (Intel 8051 family), 6 kByte ROM, 256 Byte RAM, 2 kByte EEPROM, 1-6 MHz clock frequency.

Symposium on Discrete Algorithms, pages pp 457– 466, Jan. 1995.

[4] J. Camenisch, J.-M. Piveteau, and M. Stadler. Blind signatures based on the discrete logaritm problem. In A. D. Santis, editor, *Advances in Cryptology- EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432. Springer Verlag Berlin, 1994.

[5] J. Camenisch, J.-M. Piveteau, and M. Stadler. An efficient payment system protecting privacy. In *Computer Security - ESORICS 94*, volume 875 of *Lecture Notes in Computer Science*, pages 207–215. Springer Verlag, 1994.

[6] J. Camenisch, J.-M. Piveteau, and M. Stadler. Faire Anonyme Zahlungssysteme. In F. Huber-Wäschle, H. Schauer, and P. Widmayer, editors, *GISI 95*, Informatik aktuell, pages 254–265. Springer Verlag Berlin, Sept. 1995.

[7] D. Chaum. Blind signature systems. In D. Chaum, editor, *Advances in Cryptology - CRYPTO '83*, page 153. Plenum, 1983.

[8] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030– 1044, Oct. 1985.

[9] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 319–327. Springer Verlag, 1990.

[10] M. Franklin and M. Yung. Towards provably secure efficient electronic cash. Technical Report TR CUSC-018-92, Columbia University, Dept. of Computer Science, Apr. 1992. Also in: Proceedings of ICALP 93, Lund, Sweden, July 1993, volume 700 of LNCS, Springer Verlag.

[11] X. Lai. *On the Design and Security of Block Ciphers*, volume 1 of *ETH Series in Information Processing*. Hartung-Gorre Verlag Konstanz, 1992.

[12] S. H. Low, N. F. Maxemchuk, and S. Paul. Anonymous credit cards. In *2nd ACM Conference on Computer and Communication Security*, pages 108–117. acm press, Nov. 1994.

[13] T. Okamoto. Provable secure and practical identification schemes and corresponding signature schemes. In E. F. Brickell, editor, *Advances in Cryptology — CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer-Verlag, 1993.

[14] Philips Semiconductor Hamburg- SCM. *83C852, Secured 8-bit microcontroller*, Sept. 1991. Data-Sheet.

[15] C. P. Schnorr. Efficient signature generation for smart cards. *Journal of Cryptology*, 4(3):239–252, 1991.

[16] M. Stadler, J.-M. Piveteau, and J. Camenisch. Fair blind signatures. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology - EUROCRYPT '95*, volume 921 of *Lecture Notes in Computer Science*, pages 209–219. Springer Verlag, 1995.

[17] S. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computer & Security*, 11(6):581–583, 1992.