

# On the anonymity of electronic cash

*Bart De Win*

*Report CW316, June 2001*



Katholieke Universiteit Leuven  
Department of Computer Science

Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

# On the anonymity of electronic cash

*Bart De Win*

*Report CW 316, June 2001*

Department of Computer Science, K.U.Leuven

## **Abstract**

This paper gives an short overview of anonymity enabling techniques used in existing electronic cash payment systems.

**Keywords :** electronic cash, anonymity control

# ON THE ANONYMITY OF ELECTRONIC CASH

*Bart De Win*

Department of Computer Science, K.U.Leuven  
bart.dewin@cs.kuleuven.ac.be

**Keywords:** electronic cash, anonymity control

The paper in its current form is meant to be an essay, written as part of the evaluation of the students that participated in the IPICS2000 summer school. Later it will probably be reused to write a more detailed technical report about this matter. Therefore, please take into account that it sometimes resembles more like the latter.

## 1. Introduction

Nowadays electronic commerce on the Internet is more than just a buzzword. The number of commerce transactions performed electronically actually grows every day. While it all started with very simple web shops that could merely display a product catalogue, modern electronic commerce applications are quite powerful and different application types are being used (think for example of an electronic auction). If we can trust statistics, there seems to be a slow, but certain shift from regular stores towards their electronic counterpart. Of course the applicability of such applications remains limited if customers cannot pay for the requested services or products with electronic payment systems. Therefore electronic payment systems are a very important research topic since several years.

In real life several types of payment systems are used frequently. Cash payment is probably the most frequently used money transfer system in the world. Coins and notes can be exchanged easily between customers and it requires no intervention from a financial institution. Because it is quite awkward to use cash when amounts get larger, banks have created checks that represent money. From a customer point of view checks are easier to carry, but cashing a check requires intervention from a financial institution. Since the 1950's payment cards were introduced to tackle the considerable risk of using checks. For a further overview of the properties of these different payment systems and for a good comparison, we invite you to read [9].

This document will focus on one of the properties of electronic cash systems: its anonymity. Some cash systems provide perfect anonymity for the customer and respect as such his privacy. Other systems reveal the identity only when the system is misused (e.g. in the case of double spending). And yet other systems always reveal the identity of their users. This paper will try to present an overview of the different techniques used to provide this anonymity from a technical point of view. It is not our intention to discuss the ethics of this matter.

The structure of this document is as follows. The first section provides some clear definitions on what we want to discuss in this paper. It will discuss the anonymity property in more detail and as such form a basis for the rest of the paper. After that we present an overview of the different techniques used to obtain such anonymity. This overview is then followed by a discussion. Finally we end this paper with a conclusion.

## 2. Definitions

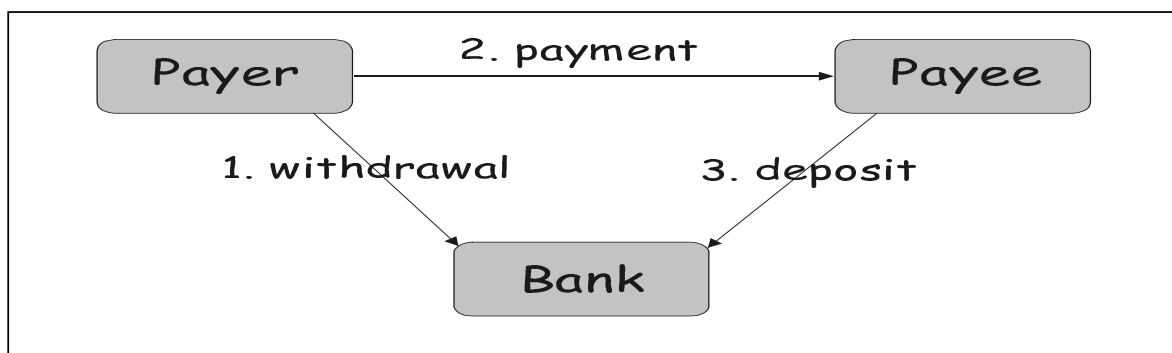
First it is important to identify the different parties that are involved in a typical electronic cash payment scenario. We can distinguish three players here:

- the **payer** or customer, which wants to buy certain products or use particular services
- the **payee** or merchant, which delivers the products/services
- a **bank** that plays the role of a financial institution

Now, what do we mean exactly when we talk about the anonymity of a payment system? Based on the literature ([8]) we define payment system anonymity to consist of the following properties:

- **payer anonymity**: guarantees that by using that particular payment system, the identity of the payer cannot be revealed to any other party.
- **payee anonymity**: this property is the same as the previous property, except for the party that is involved in it. In this case it is the identity of the payee that should not be revealed.
- **payment untraceability**: this property ensures that nor the bank nor any other party can find out whose money is spent in a particular payment. Moreover, one cannot determine whether any two payment transactions originate from the same user or not. The latter makes it impossible to keep track of the buying habits of the payer.

In a practical system however it is often not advisable to have payee anonymity. Customers don't want to spend their money to an anonymous identity, since the risk of being deceived is too high. Therefore from now on, when we talk about anonymity we only have in mind payer anonymity and payment untraceability.



A last important issue is the different sub steps of an electronic cash payment scenario (see figure). We can distinguish three different sub steps. First during the **withdrawal** phase, the payer will contact the bank in order to receive a certain amount of electronic coins. After that the payer will transfer some of these coins to the payee in the **payment** phase. Finally, during the **deposit** phase, the payee will ask the bank to cash the coins and transfer the value of them onto his account.

### 3. Overview

This section discusses several techniques to introduce anonymity into a cash payment system. Note that this is not an exhaustive list. We discuss the most important techniques, but others might be available.

Before presenting the overview, we will first briefly discuss the anonymity properties of regular cash payment systems. During the withdrawal phase the payer contacts a bank for new coins. These coins are generated by the bank and consist of a random number and possibly some extra information. The bank actually mints a coin by signing this information,

normally with his secret key. The random information of the coin is either introduced by the customer (by sending the bank random numbers) or by the bank. If we analyze this scenario, we can easily see that in either case the bank knows the contents of the coins it is signing. Therefore it always knows which coins are given to which payer. By maintaining good logs, the bank can link every incoming coin to a payer. This means that normal electronic cash schemes don't provide anonymity of the payer towards the bank. Whether they provide anonymity of the payer towards other parties (e.g. the payee) actually depends on the extra information that is part of the coin. If this information includes the identity of the payer, then of course it does not provide payer anonymity. Otherwise, a payee cannot extract that information from a coin. And what about the untraceability of the purchases? In the supposition that coins are not exchanged between payers without contacting the bank<sup>1</sup>, the bank can track the payer's buying habits, since it knows where the coins came from and to whom the coins were given. So untraceability is also not provided. The following paragraphs discuss several techniques to add this anonymity property to electronic cash systems.

### 3.1. Blind Signatures

The concept of blind signature schemes was introduced by Chaum. It is a protocol for obtaining a signature on a message such that no information about the message or its signature is revealed to the signer. This technique is being used by anonymous electronic cash payment systems in the following manner. During the withdrawal phase the payer sends blinded random numbers to the bank after which the bank signs them and sends them back. After reception of these blinded coins, the payer unblinds the signed messages and can now use them as regular coins. This procedure ensures that the bank is no longer able to link the coins to the customer. It knows that a particular payer requested some coins, but the exact content of the coins is not revealed. It is therefore not difficult to see that this scheme provides payer anonymity towards all party's and purchase untraceability.

I will not go into detail about the mathematics of these blind signing techniques. I will only discuss some of them very briefly. The first and probably the most famous blind signing technique is the one proposed by Chaum and now used in the DigiCash payment system ([4]). It is based on the principals of RSA and on the fact that in a finite field exponentiation is associative towards multiplication. More details about this technique can be found in [11] and [9]. Another system, introduced by David Wagner, provides a more lightweight solution. [5] gives an explanation of his system based on elliptic curve cryptography, but it should also be applicable to systems using exponentiation in a finite field<sup>2</sup>. For the generation of a blinded coin, this system only requires a multiplication (instead of a exponentiation for Chaum's system). Some other blind signature schemes can be found in [3].

The blind signature schemes described above provide perfect anonymity. Since criminals could misuse this, fair blind signatures were proposed as a weaker form of blind signature schemes. These schemes have the additional property that a trusted entity can provide extra information allowing the signer to link his blinded signed coins to the actual used ones. [12] proposes three such systems, including one system where a combination of pseudonyms is used to protect the identity and only one trusted party (e.g. a judge) knows the link between these pseudonyms. The other systems described in this paper are more mathematical systems, based on techniques such as cut-and-choose or oblivious transfer. Several other blind signature schemes with special properties have been proposed (like for example [7]). A thorough explanation

---

<sup>1</sup> This is a perfectly reasonable assumption, because otherwise both payers should trust each other blindly, since they might not be able to establish certainty about the value of the coins. Moreover, they cannot know whether the coin was already used or not.

<sup>2</sup> Unfortunately, I haven't found any further literature on this.

of these techniques would be out of the scope of this paper.

### **3.2. Misuse Control**

A different anonymity control system is used in CAFE. It is an off-line payment system, which means that the bank must not be contacted during the payment phase. It uses tramper-resistant hardware to protect the security and the correctness of the system. In CAFE, the identity of the payer is encoded into the coin number, which is constructed of two parts. When the coin is used in a payment, the payer must reveal only one part of the coin. If the same coin is used again, the user will have to reveal the second part of the coin. The coin is constructed especially such that revealing a single part of the coin will not identify the payer, but revealing both parts will. The details of this technique can be found in [9].

Under normal circumstances this system is fully anonymous and purchase untraceable, since the coin does not reveal the identity of the payer. The strength of this system lies in the payer's responsibility for its own anonymity. His identity will be revealed when he double spends his coins. By doing so, CAFE combines the anonymity properties and the double spending prevention in a powerful combination. However, CAFE does not guarantee the correctness of the system when the hardware has been tampered with. By doing so a payer might use the same part of the coin twice, such that his identity cannot be revealed. In our opinion this is the weakest part of the system. Using a software only solution in which a challenge-response method is used during the payment phase could solve this weakness. When the coin is used in more than one transaction, the randomness of the challenge-response protocol ensures that the identity of the payer will be revealed.

This system resembles very much the system proposed by Stefan Brands, which has more or less the same properties as CAFE. It uses the notion of restrictive blind signatures, a blind signature scheme with special properties. More information on this system can be found in [6].

### **3.3. Exchange**

NetCash [9] normally does not provide anonymity. The coins consist of a serial number and some additional information, signed by the bank. Since the identity of the payer is known to the bank during the withdrawal phase and since the contents of each coin are known to the bank, NetCash does not provide payer anonymity towards the bank, nor does it provide untraceability. It does however provide payer anonymity towards the payee, unless the bank and the payee cooperate with each other.

The level of anonymity in the NetCash system can be augmented using the following technique<sup>3</sup>. Normal coins consist of a serial number that is known to the bank. If the payer takes these coins to another bank and exchanges them for new coins, then the second bank doesn't know the identity of the payer and the first bank doesn't know the serial number of the new coins. Therefore, the payer can safely spend these new coins without revealing his identity. There are two remarks to this technique. First, the second bank knows the network address, which might reveal his identity. Using a secure proxy in between the payer and the bank easily solves this problem. Second, this technique only provides a limited kind of anonymity, since the involved banks can cooperate and as such trace the purchases. This is easy to understand as follows. The first bank is able to link the identity of the payer with the first serial number. The other banks know the relationship between two consecutive serial numbers. Thus, by working together they can trace back the history serial numbers of the coin and find out the identity of the payer. Note that in practice this situation is very unlikely to happen, but it is not impossible.

---

<sup>3</sup> Note that this technique is applicable to all systems where coins can be exchanged.

### **3.4. Anonymous Accounts**

Another anonymous electronic payment system is based on the use of anonymous accounts. It was introduced in [1] by Camenisch and works as follows. The bank has two types of accounts: personal and anonymous. The former are just regular accounts while the latter are special accounts created to transfer money anonymously. The system consists of four phases. First the customer opens an anonymous account without revealing his identity. Then, the customer identifies himself to the bank and withdraws money from his personal account. In this phase it is important that blind signature techniques are applied in such manner that the withdrawn money cannot be linked to the identity of the payer. In a third phase the money is deposited onto the anonymous account. Finally, this anonymous account is used to actually transfer the money from the payer to the account (personal or anonymous) of the payee.

As a first remark, we should note that it is not really a cash system, since the payer does not directly hand over coins to the payee. Instead it works with accounts and money is transferred from one account to another. However, the transfer of money from the payer's personal account to his anonymous account resembles a cash payment. Therefore, the system is comparable to an electronic cash payment system. Moreover, the anonymity properties of this system are good. First the system is fully payer anonymous, since the bank cannot reveal the identity of the payer. Second, when a new anonymous account is used for every transaction, the system provides perfect untraceability.

To cope with the perfect anonymity problems as mentioned earlier, fair extensions of this system have also been proposed in [3].

### **3.5. Pseudonyms**

A last technique we will be discussing is the use of secure pseudonyms. In this system, payers do not use their real identity to perform transactions, but a pseudonym. Some third party first creates a pseudonym and after that it can be used in an electronic cash payment scheme. This method provides payer's anonymity towards the payee and the bank, but not to the third party. His purchases can be traced if the different parties cooperate.

The level of anonymity in such schemes can be augmented by a technique in which pseudonyms can be exchanged in a secure way, such that no one knows the link between the different pseudonyms. Unfortunately I haven't found any literature that provides more details about this technique. Therefore, I cannot discuss the anonymity properties of this system in more detail.

## **4. Discussion**

When comparing these different techniques, we can distinguish very different anonymity properties. First, it is important to realize that many electronic cash systems provide neither payer anonymity nor untraceability. Systems like NetCash include the payer's identity into the coin such that both the payee and the bank can reveal it. Moreover, the bank or any other party can log the buying habits of the payer. At the other end of the balance, systems using blind signatures (DigiCash or the anonymous accounts) provide perfect anonymity and untraceability. This often calls forth the remark that it offers the possibility to commit a perfect crime [13]. Clearly, this poses a serious problem, but it is out of the scope of this paper to discuss this here. Moreover, good technical solutions have been provided to cope with this problem. In between these two extremes, we find systems with moderate anonymity properties. Here, the identity of the payer might be revealed, but in practice it is very hard to perform. An example of such a system is the exchange system. A particular interesting technique is the misuse control system proposed in CAFE. Here the system has different levels of anonymity and the payer is responsible for it.

Besides the anonymity properties of the systems, it is useful to look at the practical applicability of these systems. Here, the rule clearly applies that the safer the system is constructed, the harder it will be to use. This is especially true for systems like DigiCash that require an unmanageable double spending list. The anonymous accounts system leverages the problem considerable, but it still should be taken into account. Some systems also require special hardware, which is in our opinion a disadvantage, because customers don't like to get forced to buy such devices and they often don't trust them.

A last important issue concerns several patents that limit the applicability of such systems. The very powerful blind signature scheme proposed by Chaum was patented. DigiCash, which was invented by Chaum, is able to use them without a problem, but any other electronic cash system must pay for them. Unfortunately this system is the only one that really provides true anonymity. Of course other perfect blind signature schemes were proposed, but they often risk to be covered by this patent. Another patent is the one that Microsoft received concerning anonymous electronic cash [10]. I haven't seen the contents of it yet, but I certainly hope that its coverage is not very wide.

## 5. Conclusion

This paper presented different anonymity control techniques used in electronic cash system. Each system was discussed briefly and we compared them based on several issues, among which the anonymity properties, the practical applicability and others.

## References

1. Jan L. Camenisch, Jean-Marc Piveteau and Markus A. Stadler, *An Efficient Electronic Payment System Protecting Privacy*, <http://www.brics.dk/~camenisch/publications.html>
2. Jan L. Camenisch, Jean-Marc Piveteau and Markus A. Stadler, *An Efficient Fair Payment System*, <http://www.brics.dk/~camenisch/publications.html>
3. Jan L. Camenisch, Jean-Marc Piveteau and Markus A. Stadler, *Blind Signatures Based on the Discrete Logarithm Problem*, <http://www.brics.dk/~camenisch/publications.html>
4. *Digicash Webserver*, <http://www.digicash.com>
5. James D., *Anonymous Electronic Cash*, [http://catalog.com/jamesd/kong/anon\\_transfer.htm](http://catalog.com/jamesd/kong/anon_transfer.htm)
6. J. Orlin Grabbe, *Strefan Brands' System of Digital Cash*, <http://www.aci.net/kalliste/stefbrdc.htm>
7. Ildar M. Khamitov, Andrey G. Moshonkin and Alexander L. Smirnov, *Blind unanticipated RSA-signature schemes*, <ftp://demo.paycash.ru/blind.zip>
8. Larie Law, Susan Sabett and Jerry Solinas, *How to make a mint: the cryptography of anonymous electronic cash*, National Security Agency Office, 18 June 1996
9. Donal O'Mahony, Michael Peirce and Hitesh Tewari, *Electronic Payment Systems*, published by Artech House Inc., 1997, ISBN 0-89006-925-5
10. Chris Oakes, *MS Patents Anonymous Ecash*, <http://www.wired.com/news/news/story/13277.html>
11. Berry Schoenmakers, *Basic Security of the ecash Payment System*, State of the Art in Applied Cryptography, June 3-6 1997, Vol. 1528 of Lecture Notes in Computer Science, pp.338-352. Springer-Verlag.
12. Markus Stadler, Jean-Marc Piveteau and Jan Camenisch, *Fair Blind Signatures*, <http://www.brics.dk/~camenisch/publications.html>
13. S. Von Solms and D. Naccache, *On blind signatures and perfect crimes*, Computer & Security, 1992