Transferability in Coin Systems with Observers

Christine Fremdt
Mathematical Institute
University of Giessen
Arndtstrasse 2
G-35392 Giessen
Christine.Fremdt@math.uni-giessen.de

Heike Neumann
Mathematical Institute
University of Giessen
Arndtstr. 2
G-35392 Giessen
Heike.B.Neumann@math.uni-giessen.de

Abstract

We examine the interference of transferability and observers in electronic cash systems. Since copying of coins cannot be prevented cryptographically in anonymous off-line coin systems, double-spending detection is one of the major tasks. An *observer* is a tamper resistant device that prevents double-spending physically, i.e., Alice has no access to her coins and therefore she cannot copy them.

Digital coin systems force the receiver of a coin to deposit it after the purchase. In a conventional cash system this is not necessary, the receiver can use the money to buy goods without contacting the bank between recieving of coins and spending them. This property is called *transferability.*

We present a coin system which features both observer and transferability. This shows that both concepts do not interfere and can be implemented simultanously without loss of security.

Keywords: Elektronic cash, digital coins, observer, transferability.

1 Introduction

Electronic commerce is one of the most important applications for the internet. The prerequisite for establishing an electronic marketplace is secure payment. Many protocols have been proposed to implement different kinds of payments: credit card payments, micropayments, and digital coins.

Cryptographically, the most challenging task is the design of digital coins. For every payment system mentioned above we have the requirement that the payment token has to be unforgeable. Usually, we reach this

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35413-2_36

R. Steinmetz et al. (eds.), *Communications and Multimedia Security Issues of the New Century*

goal by using digital signatures of the bank to validate a payment token. But in contrast to credit card payments and micropayments for digital coins we have an additional requirement: the anonymity of the currency, i.e., the bank is not able to link a purchase to a special user.

In 1982 D. Chaum presented the notion of *blind digital signatures* that offer the possibility to design electronic coins. The bank signs blindly a set of data chosen by Alice which guarantees both the unforgeability of the coins and their anonymity, since the bank does not get any information about the data it signed.

But blind signatures solve only half of the problem: since digital data can be copied, a user can spend a valid coin several times (*double-spending*) if the deposit of coins is not done on-line. To validate each coin on-line means that the vendor has to contact the bank in every purchase. From the efficiency's point of view this is undesirable. Therefore, we restrict our attention to off-line systems, i.e., the vendor has to check the validity of coins without contacting the bank.

But no vendor can distinguish an original coin from its copy, which implies that no cryptographic mechanism can prevent double-spending. In 1988 Chaum, Fiat, and Naor overcame the problem by presenting a double-spending detection mechanism. A coin is constructed in a way that allows its owner, Alice, to spend it anonymously once, but reveals her identity if she spent it twice.

From a theoretic point of view this solution is quite elegant. But in practice it is unsatisfactory. A way to prevent the user physically from copying her coins is to store essential parts of a coin in a tamper resistant device called *observer*.

Another drawback of the coin systems sketched so far is that the receiver of a coin cannot spend it himself but has to deposit it at the bank and get a new coin including his own identity. This means that the systems offers no *transferability* of coins.

Our concern is to modify a coin system with observers so that coins become transferable. Since crucial parts of the coins are stored by the observer and cannot be read by their owner, it is not obvious how to design a cash system which provides both properties: the physical line of defense against double-spending by an observer and the transferability of coins. We demonstrate how to combine the concept of [CP92a] with a coin system with observer in the system of Brands, but our construction works with every coin system with observer.

The paper is organized as follows: In section 2 we briefly sketch a coin system with observer, in section 3 we discuss the transferability of coins. In

section 4 we present a system that features both observers and transferability and we analyze its security in section 5.

2 Coins in Wallets with Observers

There are several proposals in literature to model the properties of conventional coins for digital purposes, e.g., [CFN88], [FY93] [Br93], [Fer93], [OO91], [ST99]. A digital coinsystem as a conventional one has to provide non-forgery, off-line verification, and untraceability.

- The non-forgery of digital coins is guaranteed by a digital signature of the bank. Hence, nobody except for the bank can generate coins, but everyone is able to verify the correctness of the signature. Forging a coin is as difficult as breaking the digital signature scheme, thus in general we have computational security.
- To achieve the untraceability of coins the banks computes a "blind" signature instead of a conventional one. This means that the customer and the bank generate a set of data and a corresponding signature so that the bank cannot reconstruct the coin after the withdrawal.

The central problem with off-line coins is the double-spending, i.e., the missing originality of the coins. Though a merchant can verify the validity of the bank's signature, he is not able to decide whether or not a coin has been double-spent. Since the coins provide the customer's unconditional anonymity, not even the bank knows who double-spent the coin.

The basic idea to solve this problem came from Chaum, Fiat, and Naor,[CFN88], and consists in including the customer's identity in the coin in a way that enables the bank to compute it after a double-spending (and only in that case!). This implies that a payment cannot be simply sending a coin to the vendor, but the customer has to reveal a part of his identity.

The coin systems proposed in [CFN88] and [OO91] cannot *prevent* double-spending, but detect it afterwards. This problem cannot be solved by cryptographic means. No one can prevent Alice from making copies of the information stored by her computer.

This means that coins should not be stored by Alice's computer, but tamper resistent hardware device which erases them after Alice spent them. To assure Alice's anonymity the tamper resistant device is controlled by Alice's computer. This concept is often called an "observer" and was presented by Chaum and Pedersen in [CP92b]. The observers are distributed by the bank.

To guarantee the prevention of double-spending the bank has to be sure that the observers cannot be tampered with by the users. This is twofold:

- It must not be possible for the user to construct valid coins from the information provided by the observer during the communication.
- It must be impossible to physically extract information from the observer which enables the user to construct valid coins.

On the other hand Alice's anonymity should not be compromised by the observer. Even if the observer gets back to the bank, the bank must not be able to link Alice to her payments. The main idea how to reach this goal is to let Alice control all communication between the observer and the world. This enables Alice to control the information given by the observer.

The use of an observer is a kind of first line of defense. If the user cannot manipulate the device the observer can prevent double-spending. If the user succeeds in tampering the observer, the double-spending detection identifies the user afterwards. The user has to break the observer physically and the electronic cash system mathematically to cheat the bank.

We demonstrate the double-spending detection and the use of an observer in the system of [Br93].

2.1 Preparations of the bank

The bank chooses a group G of prime order q of length k, three generators g, g_1, g_2 of G, a secret key $x \in Z_q$ and two one-way hash functions $\mathcal{H} : G^5 \rightarrow Z_q$ and $\mathcal{H}_0 : G^2 \times ID \times time \rightarrow Z_q$ where ID is the set of vendor identification numbers. The bank computes its public key $h := g^x$. All computations are done in G.

2.2 Opening an account

To open an account Alice authenticates towards the bank. She chooses secretly and randomly $u_1 \in Z_q^*$, sends $g_1^{u_1}$ to the bank. The bank chooses $o_1 \in Z_q^*$, stores it in the tamper resistant device, and hands the observer over to Alice. The observer computes $A_o := g_1^{o_1}$ and transmits A_o to Alice.

The bank stores $I := A_o \cdot g_1^{u_1}$ together with Alice's personal data.

Note that Alice does not know the representation of I.

2.3 Withdrawal

In principle, the withdrawal protocol is the generation of a Schnorr-signature by the bank on a set of data known only to Alice, [Sch89], as shown in figure 1.

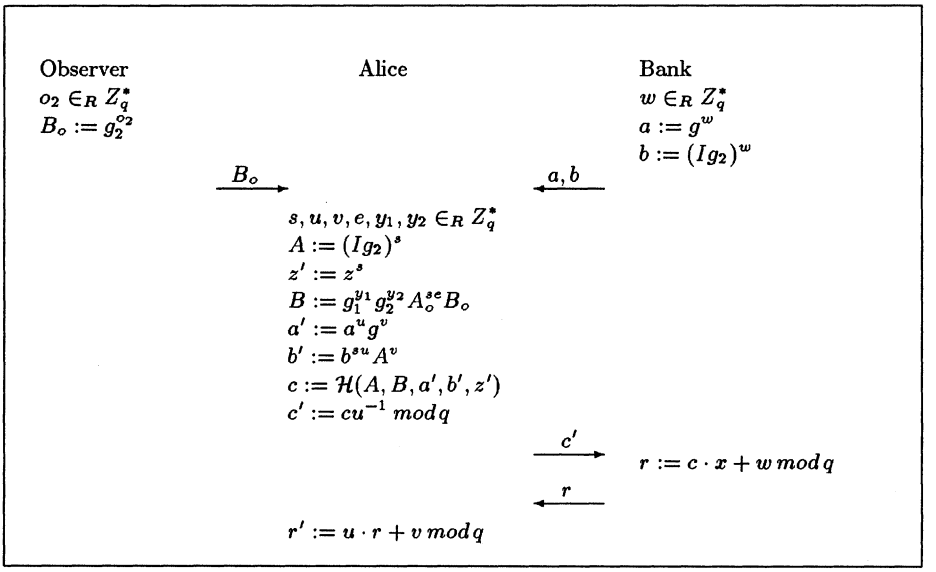

Figure 1: Withdrawal with observer

The validity of a coin can be checked as follows: One computes $c' := \mathcal{H}(A, B, z', a', b')$ and checks

$$\begin{aligned} A^{r'} &\stackrel{?}{=} z'^{c'} \cdot b' \\ g^{r'} &\stackrel{?}{=} h^{c'} \cdot a' \end{aligned}$$

2.4 Purchase

In a purchase, Alice sends the coin (A, B, a', b', z', r') to the merchant. Alice and the vendor perform a challenge-response-protocol: the vendor generates a challenge depending on the coin, the vendor's identification number and the time. Alice proves with the help of the observer that she knows a representation of A and B to the bases g_1 and g_2.

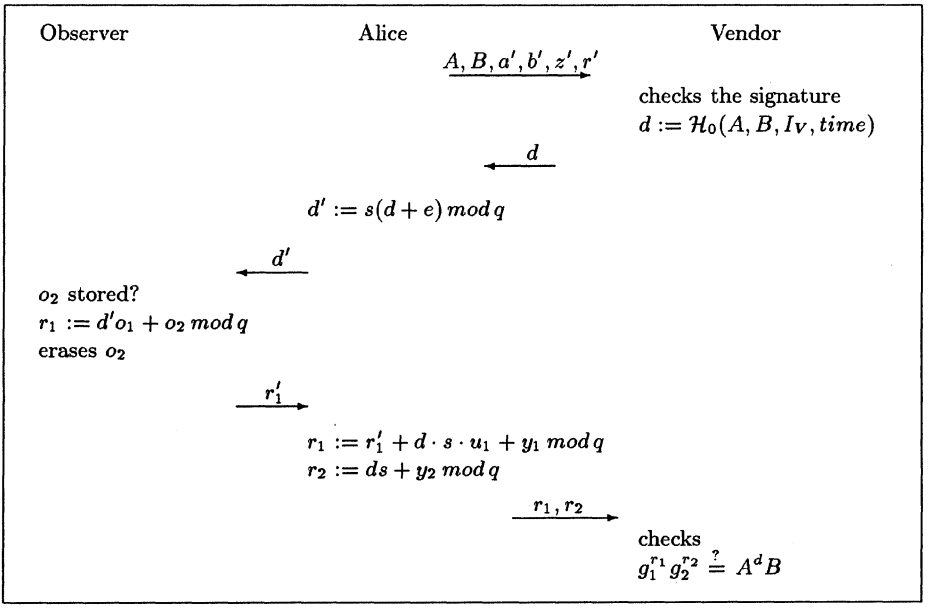

Figure 2: Purchase with observer

It is quite easy to see that Alice cannot compute o_1 and o_2 from the information provided by the observer under the assumption that she cannot compute discrete logarithm in G. This implies, that Alice is not able to perform the proof of knowledge without the interaction with the observer. And since the observer erases o_2 after the purchase, she cannot double-spend the coin.

2.5 Deposit

To deposit the coin, the merchant sends the coin and the transcript of the challenge-response-protocol to the bank. The bank checks the correctness of the coin's signature, of the merchant's challenge d and of Alice's responses to the challenge. If everything is correct, the bank checks its database whether the coin has been already deposited. If it is not, the bank stores the coin, the merchant's challenge, and Alice's responses.

If it is, the bank compares the values of the challenge and the responses. If the challenge is the same, the merchant tries to cheat by depositing the same coin twice. Thus, the bank rejects the deposit. If the challenges

differ, so do Alice's responses, which enables the bank to compute Alice's identification number. Let d and $\tilde{d}$ be the merchants' challenges and r_1, r_2 and $\tilde{r_1}, \tilde{r_2}$ Alice's responses:

$$\begin{aligned} g_1^{(r_1-\tilde{r}_1)\cdot(r_2-\tilde{r}_2)^{-1}} &= g_1^{(r_1'+d\cdot s\cdot u_1+y_1-\tilde{r_1}'-\tilde{d}\cdot s\cdot u_1-y_1)\cdot(d\cdot s+y_2-\tilde{d}\cdot s-y_2)^{-1}} \\ &= g_1^{(s\cdot(d+e)\cdot o_1+d\cdot u_1\cdot s-s\cdot(\tilde{d}+e)\cdot o_1-\tilde{d}\cdot u_1\cdot s)\cdot(s\cdot d-s\cdot\tilde{d})^{-1}} \\ &= g_1^{o_1+u_1} = I \end{aligned}$$

Some remark on the user's anonymity: The tamper resistant device does not affect the user's anonymity. None of the values which the observer can store gets to the bank. It can be proven that the observer's view of the purchase and the banks view of the deposit are independent.

3 Transferability

In the presented coin system only the user who had withdrawn a coin is able to spend it, since spending the coin requires the knowledge of the user's secret key u_1. Therefore, the vendor cannot spent a received coin, but he has to deposit it and generate a new coin including his own secret key to be able to perform a purchase in the role of the user.

If we want to implement transferability, i.e. we want Alice to give the coin to Bob and Bob to perform a purchase (or Bob to give the coin to Carol), we have to require the following properties:

- Alice's (resp. Bob's) anonymity has to be guaranteed if Alice (resp. Bob) spent the coin only once and Bob (resp. Alice) double-spent it.
- The bank must be able to detect a double-spending and to identify the double-spender, even if both Alice and Bob double-spent a coin.
- Even if Alice and Bob cooperate, they must not be able to generate a coin which does not include one of their identification numbers.

By the second requirement we get immediately that Bob's identification number must be encoded in the transferred coin. It seems to be quite natural to construct this extension like a "normal" coin. This construction is applicable to every anonymous off-line coin system and was first proposed by Chaum and Pedersen, [CP92a].

To generate a coin extension Bob and the bank perform the same protocol as Alice and the bank in order to withdraw a coin, whereas the bank does not use its signing key x but x_t and does not debit Bob's account.

To transfer the coin from Alice to Bob they perform a purchase with Alice's coin and Bob in the role of a vendor. Bob includes his own coin extension to compute the challenge for Alice, which links the coin extension to Alice's coin. A vendor who gets a transferred coin can check its validity by checking the correctness of the coin and of the coin extension. The protocol differs only slightly from a purchase protocol in the basic system. Instead of taking his identification number Bob uses his coin extension to compute the challenge.

To spend the transferred coin Bob sends the vendor the coin's "history", i.e., everything sent by Alice. To guarantee the double-spending detection Bob and the vendor have to perform a purchase protocol for Bob's extension where he proves the knowledge of his secret key.

To deposit the transferred coin the vendor sends all data to the bank, i.e., a transcript of the challenge-response-protocol performed by Alice and Bob and a transcript of the purchase protocol between Bob and himself.

Since both coin and extension are constructed to enable the bank to detect and identify a double-spender, neither Alice nor Bob can defraud the bank. On the other hand, Alice and Bob are anonymous as long as they do not double-spend. This can be seen easily since the transfer protocol corresponds to a purchase in the basic system. Since generating an extension is the same as generating a coin but with a different key, we certainly have that forging a coin extension is as hard as forging a coin.

4 Transferable Coins in Wallets with Observers

To combine both concepts we have the following initialisation chosen by the bank:

- a group G of prime order q of length k
- generators g, g_1, g_2 of G
- two secret keys $x, x_t \in Z_q$ and computes $h := g^x, h_t := g^{x_t}$
- three one-way hash functions $\mathcal{H} : G^5 \to Z_q$, $\mathcal{H}_0 : G^2 \times ID \times time \to Z_q$, $H_1 : G^4 \times time \longrightarrow Z_q$.

The second key pair (x_t, h_t) is not used to generate coins, but to generate coin extension for transferred coins.

4.1 Withdrawal

The withdrawal protocol performed by Alice and the bank is exactly the same as in section 2.3.

The generation of Bob's coin extension is the same as the withdrawal with one modification: replace the bank's secret key x by x_t.

4.2 Transfer

Alice has withdrawn the coin (A, B, a', b', z', r'). We assume that Bob has already generated a coin extension $(\tilde{A}, \tilde{B}, \tilde{a}, \tilde{b}, \tilde{z}, \tilde{r})$ with the bank.

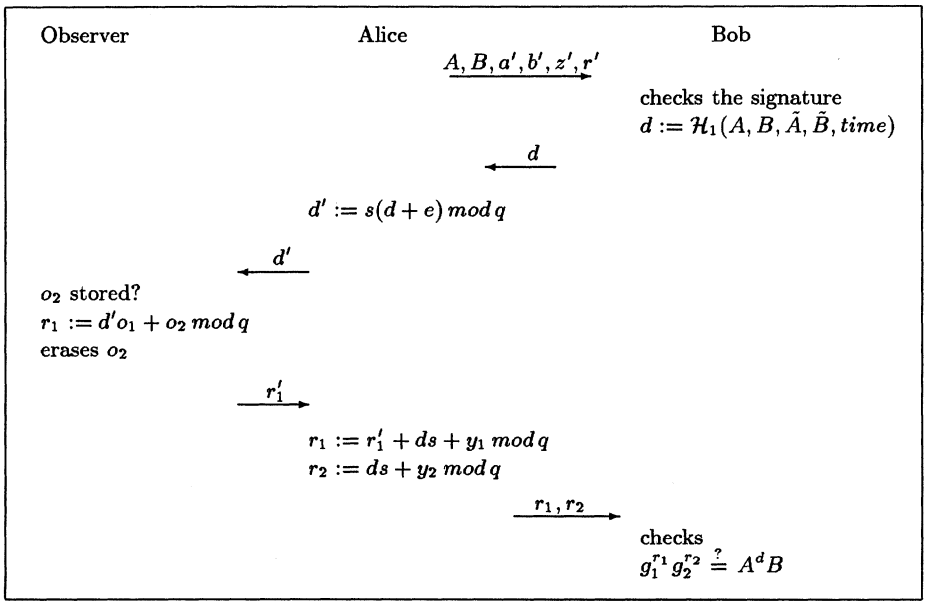

Figure 3: Transfer with observer

It is easy to see that this protocol is only a slight modification of the purchase with observer. The main difference is the generation of the challenge in which Bob includes essential parts of his coin extension to link Alice's to the extension. Note that Bob doesn't use his observer in this part of the coin system.

4.3 Purchase

To spend the transferred coin, Bob sends Alice's coin, the transcript of the challenge-response-protocol and his coin to the vendor. The merchant checks Alice's coin, the challenge-response-protocol and Bob's coin extension, then he and Bob perform another challenge-response-protocol with respect to Bob's secret key. At this point Bob has to use his observer. To verify the correctness of Bob's responses the merchant takes the bank public key for transfers h_t and does the same computation as in a usual purchase.

5 Discussion

Though there is no proof that forging a coin is as hard as forging a Schnorr-signature, we can show that forging a coin or a coin extension in our system with observer and transferability is as hard as forging a coin in the basic system. Therefore, we do not lose any security by implementing observers and transferability. On the other hand, transferable coins have an important influence on the user's anonymity: Bob is not anonymous towards a coalition of Alice and the bank, since Alice can always recognize her own coins. This seems to be a quite fundamental disadvantage of this construction of transferability which was first observed by Chaum and Pedersen, [CP92a].

Also in [CP92a] Chaum and Pedersen proved that this construction of transferability, although it is extremly inefficient, is close to optimal with respect to efficiency. Their proof applies to our construction in systems with observers, too, since the view of the merchant in an system with observer is the same as in one without this device.

Especially, the missing anonymity and the loss of efficiency show that the observer does not solve the fundamental problems with transferability. On the other hand, we have seen that the concepts do not interfere and can be implemented simultanously.

6 Conclusion

We presented a digital coin system which provides a physical defense against double-spending additionally to a double-spending detection in case the observer is tampered by its owner and the transferability of coins. We have seen that our systems inherits the fundamental problems of transferability which limits the practical use of transferable coins in coin systems with observers.

References

[Br93] S. Brands, "Untraceable off-line cash in wallets with observers," *Proc. of Crypto '93*, Lecture Notes in Computer Science 773, Springer-Verlag, 302-318

[CFN88] D. Chaum, A. Fiat, M. Naor, "Untraceable Electronic Cash," *Proc. of Crypto '88,* Lecture Notes in Computer Science 403, Springer-Verlag, 319-327

[Ch82] D. Chaum, "Blind signatures for untraceable payments," *Proc. of Crypto '82*, Plenum Publishing, New York 1982

[CP92a] D. Chaum, T. P. Pedersen, "Transferred cash grows in size," *Proc. of Eurocrypt '92,* Lecture Notes in Computer Science 658, Springer-Verlag

[CP92b] D. Chaum, T.P. Pedersen, "Wallet Databases with Obsersers," *Proc. of Crypto '92,* Lecture Notes in Computer Science 740, Springer-Verlag

[CP93] R. Cramer, T.P. Pedersen, "Improved Privacy in Wallets with Observers," *Proc. of Eurocrypt '93,* Lecture Notes in Computer Science 765, Springer-Verlag

[Fer93] N. Ferguson, "Extensions of Single-term Coins," *Proc. of Crypto '93*, Lecture Notes in Computer Science 773, Springer-Verlag

[FY93] M. Franklin, M. Yung, "Secure and efficient off-line digital money," *Proc. of Automata, Languages and Programming, ICAPL '93,* Lecture Notes in Computer Science 700, Springer-Verlag

[OO91] T. Okamoto, K. Ohta, "Universal Electronic Cash," *Proc. of Crypto '91,* Lecture Notes in Computer Science 576, Springer-Verlag

[ST99] T. Sander, A. Ta-Shma, "Auditable, Anonymous Electronic Cash,", *Proc. of Crypto '99,* Lecture Notes in Computer Science 1666, Springer-Verlag

[Sch89] C. Schnorr, "Efficient signature generation by smart cards," *Proc. of Crypto '89, Lecture Notes in Computer Science,* Springer-Verlag