erschien in: Computers & Security 8/5 (1989) 399-416

Refereed Article

Digital Payment Systems Enabling Security and Unobservability

Holger Bürk *, Andreas Pfitzmann ‡

* Ascom Tech AG, Labor Solothurn
Ziegelmattstr.1-15, CH-4503 Solothurn, Switzerland

‡ Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe,
Postfach 6980, D-7500 Karlsruhe 1, F.R.G.

Abstract

In present-day cashless payment systems, the banks and (by installing a Trojan Horse) even the manufacturers of the computer equipment used could easily observe who pays what amount to whom and when. With the increasing digitization of these systems, e.g. point-of-sale terminals and home banking, the amount of transaction data and their computerization drastically increases. Therefore these payment systems become completely unacceptable, since compiling dossiers on the lifestyle and whereabouts of all clients will become easy.

We describe the *digital payment systems enabling unobservability* of clients and arrange them in a general model to compare their different degrees of unobservability and their different levels of security. Since no single system has all desired features, we propose a suitable synthesis.

Keywords

Cashless payment, digital payment systems enabling unobservability of clients, linkability of actions, anonymous numbered accounts, tamper-resistant devices, blindly signed digital banknotes

Table of Contents

1 Introduction 1

2 Necessary Technical Capabilities 2
2.1 Networks Without User Observability 2
2.2 Authentication 2

3 A General Model for Unobservable Payment Systems 4
3.1 Towards a General Model 4
3.2 Clearing Anonymity – Who Should Realize It? 6
3.3 Security Problems posed by "Unlinkability of each Currency with Itself" and How They Can Be Solved 8

4 Arranging the Payment Systems in the General Model 10
4.1 Anonymous Numbered Accounts 10
4.2 Mutually Trusted Tamper-Resistant Devices 11
4.3 Blindly Signed Digital Banknotes 12
4.4 Anonymously Transferable Standard Values 18

5 Combinations and Interest 21
5.1 Combinations To Get Maximal Anonymity 21
5.2 Combinations Enabling Off-line Payments Even Without Absolutely Tamper-Resistant Devices 22
5.3 Interest 22

6 What Needs To Be Shortly Mentioned and Persistently Done 23

Acknowledgements 24
References 24

Table of Figures

Figure 1: Relations between banks and their clients 4
Figure 2: Anonymity cuts within payment circulation graph 5
Figure 3: Unlinkability of different currencies 7
Figure 4: Unlinkability of each currency with itself 8
Figure 5: Payment circulation for blindly signed digital banknotes 13
Figure 6: Payment circulation for anonymously transferable standard values 20
Figure 7: Combination to get maximal anonymity 21

1 Introduction

In present-day cashless payment systems, the banks and (by installing a Trojan Horse [13]) even the manufacturers of the computer equipment used could easily observe who pays what amount to whom and when. With the increasing digitization of these systems, e.g. point-of-sale terminals and home banking, the amount of transaction data and their computerization drastically increases.
Therefore these payment systems become completely unacceptable, since compiling dossiers on the lifestyle and whereabouts of all clients will become easy. Measures of law and jurisdiction alone are insufficient to prevent collection and use of these data, since infringements can hardly be discovered and restoration of privacy is impossible in most cases. Hence, *payment systems*, not only guaranteeing *security against fraud* but also enabling *unobservability of clients*, are necessary. Unobservability of clients means:

1. Each client may do his business *anonymously*, i.e. the banks and the client's business partners (e.g. international providers of information services) together are not able to find out his identity without his cooperation.
2. Each payment is *unobservable* for inquisitive unconcerned third parties.
3. Each action of a client is *unlinkable* to actions which have taken place earlier, unless such a concatenation of actions is intentionally enabled by the client.

In view of these harder requirements, it should be noted that most cashless payment systems used today, e.g. home banking via BTX (interactive videotex in Germany) or all automatic teller machines using passive (for example magnetic stripe) cards, do not even provide sufficient, i.e. both-sided, security. Clients are forced to trust banks completely, since the handwritten signature (which until now gave at least a minimum level of protection to the clients) is replaced by "proofs" the bank could imitate very easily and perfectly. To give an example, appending a TAN (Transaction Number) or a PIN (Personal Identification Number) to messages, both generated by the bank, nowadays is supposed to create legally binding declarations.

This paper is organized in six chapters. Chapter 2 presents a brief overview of necessary and feasible technical capabilities to solve the security and unobservability problems. In chapter 3 we develop a general model for payment systems satisfying the above listed requirements. In chapter 4 we arrange all published payment systems of this kind in our model. Since no single system has all desired features, we propose a suitiable synthesis in chapter 5. Finally, we discuss some socio-political impacts when these digital payment systems will work in practice.

The use of payment systems enabling security and unobservability for *unobservable value exchange* over a network (e.g. money against information) between two remote parties poses an additional security problem: the lack of a simultaneous exchange causes a temporary advantage for one party, who could then stop communication. How this problem can be overcome will be described in a companion paper appearing in a later issue.

2 Necessary Technical Capabilities

2.1 Networks Without User Observability

To enable unobservable (i.e. anonymous, unobservable by unconcerned third parties, and unlinkable) digital payments, networks without user observability are necessary. Such networks guarantee that nobody, not even the network manager, is able to figure out sender and recipient of transmitted messages, unless the sender and receiver of the respective message are cooperating. For this, it is not sufficient to hide only the content of a message, which can be done by *end-to-end-encryption* [24], since an attacker could still see who sends how many messages to whom and at what time (*traffic analysis*). To hide these traffic data too, the relation between sender and recipient must be kept secret (*unlinkability*), or more secure, both sender and recipient of a message are kept secret. A survey on measures to hide traffic data in a network is given in ref. [20].

2.2 Authentication

New applications of networks like digital payment systems require elaborate measures for authentication, e.g. transmitted messages may be legally binding declarations which are effective only if a proof of authorization is shown.
For authentication, digital signatures [13] are used, ensuring that a declaration of an individual can only be signed by that individual and that everybody can verify if a declaration is actually signed with the signature belonging to that individual. Digital signatures can be formed, e.g. by encryption of the declaration with the best known but old-fashioned public key cryptosystem (PKCS) RSA [13] or by using any efficient digital signature system which is provably as secure as factoring is difficult [15, 16]. The latter alternative is more secure, since RSA is not provably as secure as factoring is difficult, but is clearly broken if factoring the modulus is feasible.

In the following, we use

sign$_X$(*m*) to describe the result of a message *m* signed by *X*, and
auth$_X$(*m'*) to describe the check of authentication, whether a message *m'* is signed by *X*, i.e. whether *m'*=sign$_X$(*m*) for some *m*.

In order to guarantee anonymity of individuals, a digital signature must not be associated with an individual directly but with a *digital pseudonym* [4, 6] which is used by that individual. Digital pseudonyms are just (almost unique) numbers (or pairs thereof) which are created by individuals through a special random process. It is assumed that every individual uses different digital pseudonyms wherever possible to restrict linkability to a minimum.

There are two forms of authentication which should be distinguished: *self-authentication* and *granted authentication* [21].
The form of authentication when someone refers to previous declarations of his own is called *self-authentication.* This form corresponds to one's hand-written signature. With self-authentication linkability of different declarations of the same client is intentionally enabled by the client: he uses the same digital pseudonym and digital signature for the corresponding declarations.

The form of authentication corresponding to showing one's identity card, driver's license, etc., is *granted authentication*. Granted authentication is applied in those cases when a declaration can be made only when an authorization from another (e.g. superior) instance can be shown. These authorizations or *credentials* should be issued to digital pseudonyms, not directly to the individuals. Special measures [6] can prevent the third parties (e.g. banks) which grant authentication from deriving undesired concatenations, even in cooperation with those to whom the credentials are shown.

3 A General Model for Unobservable Payment Systems

In the following we assume that networks without user observability are used. Then the degree of anonymity only depends on the form of authentication used (cf. section 2.2), which is discussed in detail for each payment system.
To understand thoroughly how to design payment systems which meet all three requirements stated in chapter 1, a general model is developed first.

3.1 Towards a General Model

The starting point of our analysis is the relation between banks and their clients from today's point of view. This leads us to a general model for any cashless payment system. Since clients and banks are different acting entities, we arrange them on two different levels, namely a level of banks and a level of clients. Some of the clients will have business relations with each other. These relations are called *dynamic*, since they often change. Each client has a relation to a bank, that is, he has established at least one account at this bank, and of course for clearing, the banks must have relations with each other, but we are not concerned whether this happens via a central bank CB or directly. All these relations are called *static*, since they are relatively enduring. Moreover, unlike the dynamic relations where only a very small fraction of all possible pairs of clients have relations with each other, the static relations are always present to a much larger extent.
Figure 1 shows the relation graph for an example with three clients X, Y, and Z, who presently have business relations with each other. Their banks are B_X, B_Y, and B_Z, respectively.

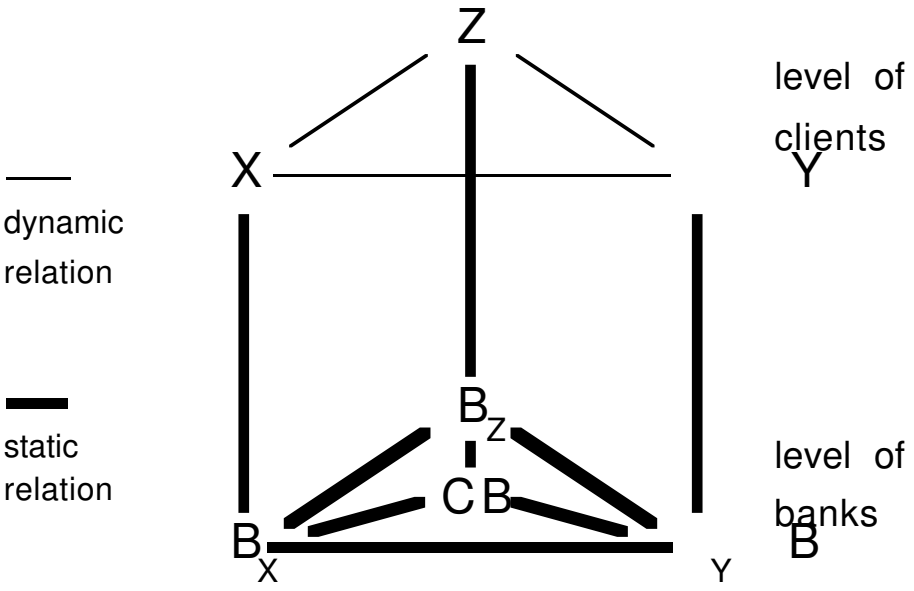

Figure 1: Relations between banks and their clients

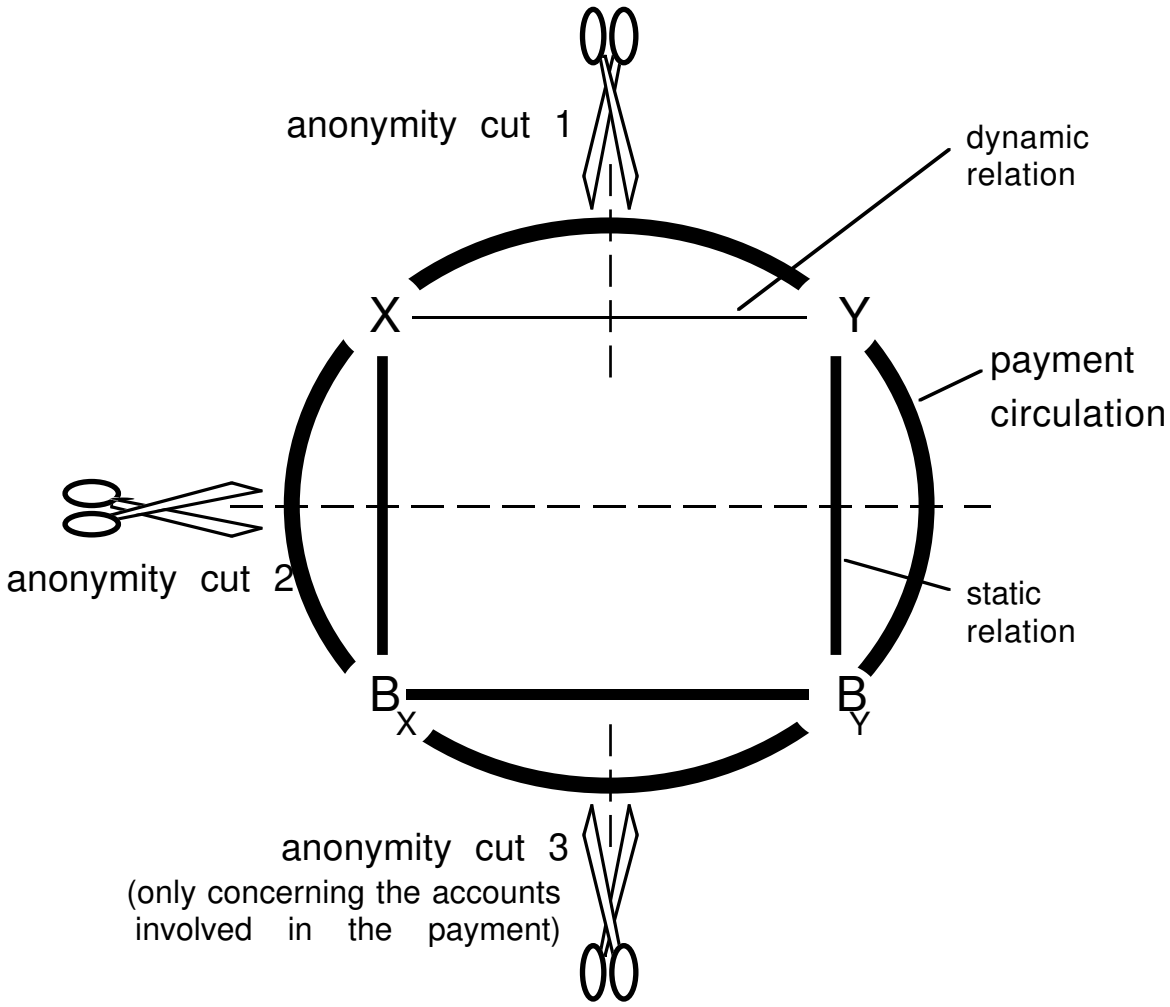

Figure 2: Anonymity cuts within payment circulation graph

The dynamic relations are those which must be particularly protected with respect to the payment system, since only they can give substantial information about the lifestyle and whereabouts of the clients. If a payment between two clients, say X and Y, is made, in general at least four entities X, Y, B_X, and B_Y, and possibly CB are involved. We obtain a payment circulation graph as shown in figure 2, which is specified in detail by the payment system used. To guarantee unobservability of clients X and Y, we will show that the payment circulation graph has to be entirely partitioned by the three *anonymity cuts* 1, 2, and 3, as shown in figure 2.

Anonymity cut 1 stands for mutual anonymity of clients and unobservability of their payments for inquisitive third parties. Anonymity cut 2 stands for anonymity of clients towards their banks. Both anonymity cuts affect mainly the relations of the clients to the other parties involved in the payment. Therefore we call this form of anonymity *relation anonymity*.

Networks without user observability (cf. section 2.1), enabling anonymous communication, are necessary to realize anonymity cut 1. Since authentication is necessary in most applications, digital pseudonyms and credentials (cf. section 2.2) are used as well. With the usual authentication techniques, mutual anonymity may be reduced to one-sided anonymity or no anonymity at all whenever desired. Special forms of anonymous accounts (see subsections 4.1, 4.2 and 4.4) are introduced to realize anonymity cut 2. But even if relation anonymity is given, this by itself does neither prevent a one-to-one correspondence client $\leftrightarrow$ account nor observability of the money transfer between banks. Therefore, in the long run, the clients can become completely identifiable and observable. Anonymity cut 3 is needed to overcome this problem.

Anonymity cut 3 signifies that payments are unlinkable to other payments (or any other actions) for the banks, though the banks are actually involved in the payment process. (Please note, as shown in figure 2, that anonymity cut 3 does not cut the static relations between the banks.) Payments are unlinkable if all banks together have no better chance to find out from where money comes and to where it goes than observing when and how balances change (provided that there are any, see subsections 4.2 and 4.3). We call this form of anonymity *clearing anonymity*. It is important to have clearing anonymity because otherwise any established relation anonymity of the clients would gradually be forfeited.Since the quantity of information about the anonymous holders of the accounts increases with each payment, at some point it becomes feasible to break anonymity.

3.2 Clearing Anonymity – Who Should Realize It?

Clearing anonymity is necessary mainly because banks cannot be trustworthy with regard to the privacy of the payments made by their clients because of technical reasons:
More and more complex computer systems are being designed, produced and maintained with more and more complex tools and (international) teamwork. This prevents adequate validation, not to speak about rigorous verification, that their functionality is restricted to what they should do, e.g. that they contain no *Trojan Horses*.
These Trojan Horses cannot only be generated by members of the team, but also by the complex tools used. Moreover, the Trojan Horse in the first tool may be implanted by another tool used to generate the first one and so on. An example for this technically unavoidable possibility is given by Thompson [23]. The more general attack by a *virus* as described by Cohen [10] can be restricted to the one just described by signing programs digitally, as proposed – for slightly other reasons – in p.317 of ref. [13], and checking the signature before execution. For all these technical reasons, the complex computer equipment used for digital payments cannot be trustworthy, and thus, neither can the banks using such equipment.

The best way to solve the trustworthyness problem described above is to let the clients realize anonymity cut 3. Only then, can they be convinced completely that their privacy is maintained.
Since with accounts all payments involving an account are naturally linkable, the first step to realize anonymity cut 3 is to substitute the payment systems with accounts by payment systems which are based upon more appropriate representations of money. In the following we denote these representations simply as *digitally transferable currencies*, as long as they are not defined in detail. Obviously, digitally transferable currencies must be transferable between any two clients and must in some way be unlinkable for the banks. It is the latter quality which provides clearing anonymity.

There are two possibilities by which the clients can establish clearing anonymity:

1. *Unlinkability of different currencies:*
   This possibility proceeds from the fact that each digitally transferable currency can be properly identified and thereby traced. To disable the banks nevertheless from deriving undesired concatenations when these currencies are used for payments, the currencies should be unlinkable. In particular, special care has to be taken that they are not linkable to the person who owns them or to other currencies. Unfortunately, the latter cannot be realized completely, even if the payment system itself does so, since currencies which are transferred simultaneously are thereby linkable.
2. *Unlinkability of each currency with itself:*

To obtain a second possibility, measures have to be taken to overcome the fact that each digitally transferable currency can be properly identified and thereby traced. Therefore, their identity must be changed, so that they are not linkable for anybody, except the one who made the changes. To prevent the banks from tracing, the clients must change the identity of the currencies while they are withdrawn from the banks and before or after they are spent.

If clearing anonymity is to be established by unlinkability of different currencies, the digitally transferable currencies must be unlinkable with exception of linkability by simultaneous transfer. Obviously, this is the case when the pseudonym of the owner of each currency is unlinkable to any other pseudonym (known to the banks). Hence, whenever a payment is made, i.e. the ownership of the currencies used for payments is transferred, the corresponding pseudonyms have to be changed and must not have been used for anything else before. If they are used only once, i.e. for exactly one payment and then never again, the currencies are indeed unlinkable. The situation is shown in figure 3.

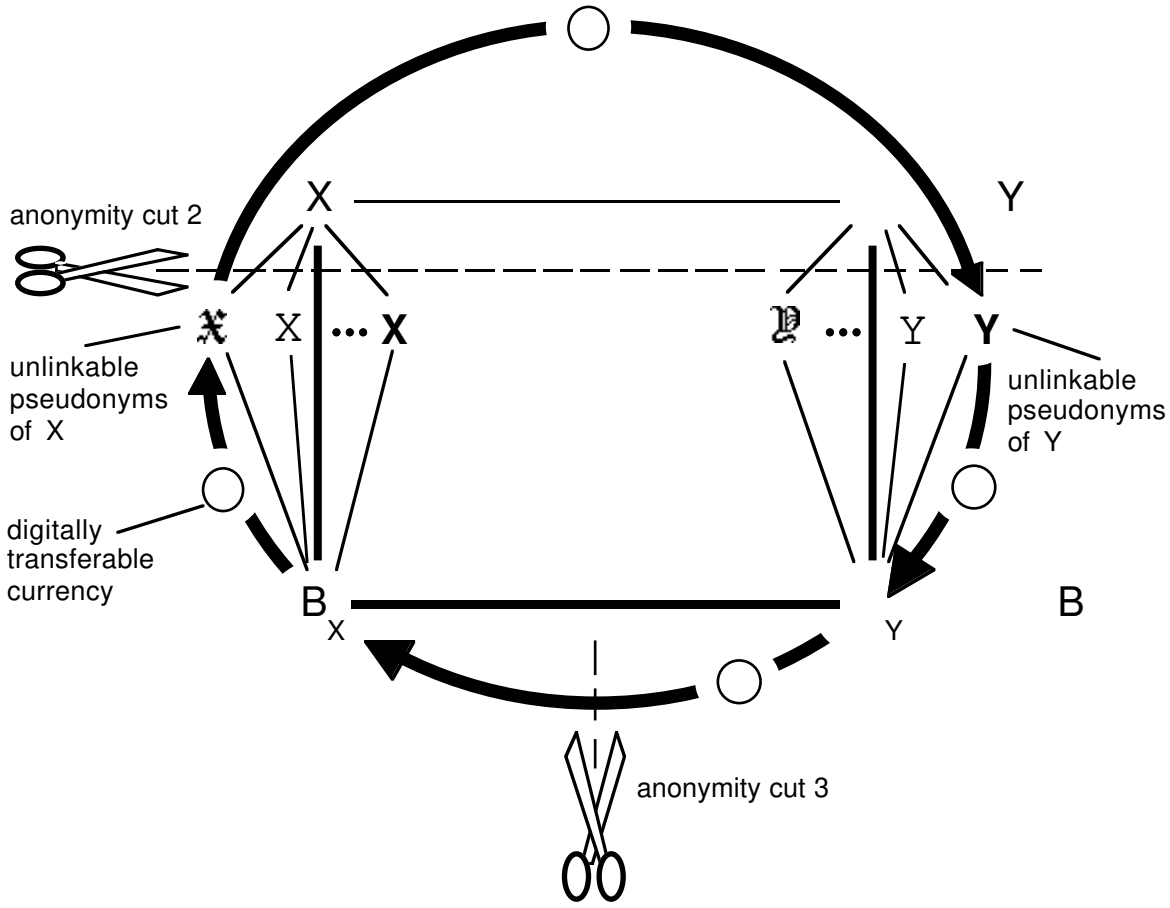

Figure 3: Unlinkability of different currencies

If the second possibility, i.e. unlinkability of each currency with itself, is used to establish clearing anonymity, the identity of the digitally transferable currencies has to be changed. This is possible in case the currencies are represented by specially encoded messages so that their identity can be changed by changing their encodings, but without invalidating them. Therefore special methods (see subsection 4.3) are necessary. The situation is shown in figure 4. Since the bank should not, by observation of the withdrawn and deposited currencies, be able to find out which parties are actually involved in a particular payment, a varying amount of time should pass between withdrawal and

deposit and the values of the currencies should not be arbitrary. Instead, a few standardized ones should be used as today.

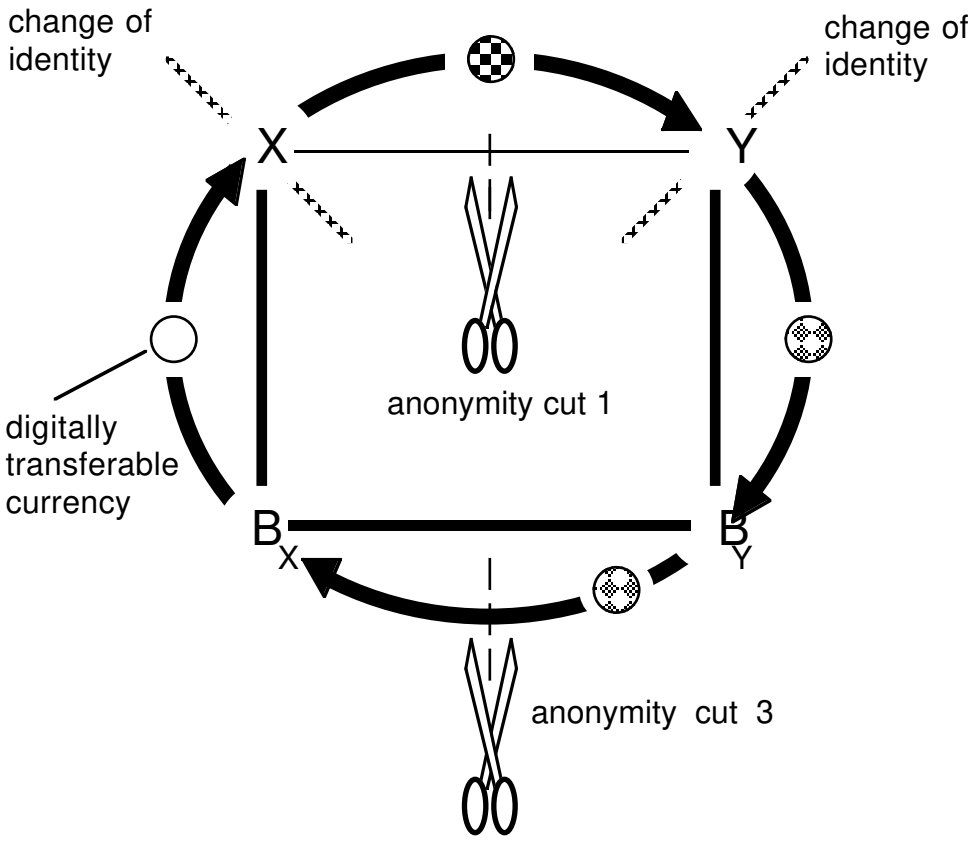

Figure 4: Unlinkability of each currency with itself

3.3 Security Problems posed by "Unlinkability of each Currency with Itself" and How They Can Be Solved

In this section, we discuss the security problem arising when the digitally transferable currencies are temporarily not under control of the bank as in the case just considered in figure 4. Of course, unauthorized persons must not have the possibility to increase the number or value of the digitally transferable currencies. This can be accomplished by using the following two methods:

1. Use of *tamper-resistant devices* trusted by mutually suspicious groups.
2. *Coding* only.

The security of both methods (as of seemingly all other digital payment systems, also those not enabling unobservability) depends on cryptography, though unfortunately as yet the security of cryptosystems cannot be proved from scratch.
The first method additionally uses tamper-resistant devices [12] (e.g. chipcards) where the digitally transferable currencies are stored. However, the existence of appropriate devices is admittedly questionable, since they must be trusted by mutually suspicious groups, so that the same, but to some

extent reverse problematic arising when banks realize anonymity cut 3, is present. On the one hand their function has to be checkable by their users, especially they must not contain Trojan Horses which reveal information about the payments. On the other hand they must be tamper-resistant against their users, who must not be able to increase the money in the devices nor, even by destroying the device, to extract secret information, e.g. keys of a cryptosystem, in order to build imitations.
The second method merely uses cryptography. In this case the digitally transferable currencies are encoded messages. Since encoded messages can be copied, but must represent money only once, in each payment a bank must guarantee the payee that the information still represents money. So usually the payments have to take place on-line; only if the payee is known in advance and specified as sole recipient in the digitally transferable currencies can he verify locally whether they had not been received by him some time ago. Thus he can be sure that they still represent money.

4 Arranging the Payment Systems in the General Model

The anonymity cut model developed in the preceeding chapter allows us to arrange all known digital payment systems enabling unobservability to a certain degree according to which anonymity cuts they realize. All these payment systems have the basic ability to enable payments between mutually anonymous individuals according to anonymity cut 1. It is important that in spite of anonymity the payer is sure to get a receipt for payment. Therefore we propose an arbitration court which writes receipts of payments by way of substitution after the payer has proved that he has really made a payment. Thus, the payment system should enable payers to collect evidence for the payments made. This problem is addressed below.

Three further criteria have to be considered:

1. Is it possible for payees to verify[1] if they really received money without using the network?
   We will see that this can be arranged using any of the known digital payment systems enabling unobservability if the payee is known to the payer in advance and the payer makes special pre-arrangements using the network. Therefore the more interesting criterion is:
2. Is it possible for the payer to make off-line payments to arbitrary payees in a way that the payees can verify without using the network that they really received money?
3. What is the security and anonymity of the payment system based on:
   Tamper-resistance of devices against their owners, strength of cryptosystems used (and, if a special cryptosystem is needed, how secure is this believed or proven to be?) or, best of all, information theoretic proofs?

First, we mention a simple payment system realizing anonymity cut 2 only. After some remarks on mutually trusted tamper-resistant devices which can realize all three anonymity cuts depending on implementation we stress payment systems realizing anonymity cut 3 using coding only (cf. section 3.3). These systems are arranged in increasing order according to how much checkable unobservability they provide for the clients.

4.1 Anonymous Numbered Accounts

This proposal [19] is a "digital version" of the very popular anonymous numbered accounts already existing in Austria and in a not really anonymous form in Switzerland. A client establishes an account anonymously, e.g. by means of a network. He never has to identify himself since he randomly chooses a digital pseudonym (cf. section 2.2) which is made known to the bank in order that the bank can subsequently use it to authenticate his messages. Money is transferred between banks in the usual way [12]. However, in lieu of special banking forms and handwritten signatures, digitally signed messages (in standard formats) are used. The bank signs messages digitally as well, which can be verified by every party in the system. A complete description is given in ref. [3].

---

[1] We don't recommend to base "verification" on the identifiability of cheaters, as is done in ref. [9]. Since it is only later that it is (really) verified that the payer is able to pay, uncovered claims may arise.

Since this payment system realizes only anonymity cuts 1 and 2, no clearing anonymity has been established. Thus, the use of this system is recommended only in combination with the following proposals realizing anonymity cut 3. Further characteristics of this system are as follows:

* Payers can always prove that a payment was made, since the bank is obliged to store and confirm the money transfer orders. (If the bank refuses to confirm the money transfer order, it is sent again via a judge as witness.)
* The off-line verification of prearranged off-line payments is possible: the payer reserves a certain amount of money in his anonymous numbered account exclusively for payments to a specified other anonymous numbered account until an expiry date. The payer gets a corresponding confirmation signed by his bank which he can give to the payee, who checks whether he is the owner of the specified account and whether the expiry date is not too early. If both conditions are satisfied, he can be sure that every money transfer order signed by the payer and drawn to the account of the payee is covered, as long as their overall amount does not exceed the amount specified in the confirmation of the reservation.
* Off-line payments to arbitrary payees cannot be verified by the payee without using the network.
* A payment is linkable to all other actions which have earlier affected an account.

4.2 Mutually Trusted Tamper-Resistant Devices

Chipcards (smart cards) are the prototypes of mass-produced tamper-resistant devices, which may be used especially for off-line money transfer between anonymous clients. Chipcards used in this way serve as "electronic wallets" [14, 17] or minibanks with one account [19], since the tasks of a bank are substituted for and manipulation is (or should be) impossible. Thus a chipcard is a substitute for a trusted third party by whom the payments are conducted. The trustworthiness of these devices has been discussed earlier (cf. section 3.3).

In principle, chipcards can realize all anonymity cuts, depending on implementation. If we assume that the banks issue the chipcards to their clients, anonymity cut 2 is realized if neither the identity of the holder of a chipcard (which is not needed to conduct transactions) is noted nor any of his physiological characteristics are registered. A chipcard with identity issued in this way is a kind of substitute for a digital pseudonym of its holder. Obviously, in this case and in case the chipcard has no identity at all, anonymity cut 1 is realized.
If the identity of a chipcard is made known to the transaction partner, e.g. exchanging a serial number within each transaction, the chipcard's actions are linkable in principle. Therefore, the identity of a chipcard (if there is one at all) has to be concealed from its transaction partners, implying that all authentic chipcards should have a key in common to allow secure authentication. Sharing one key with all chipcards is admittedly problematical if any unauthorized party should be able to learn that key, but otherwise means no loss of security during authentication or money transfer, since secure authentication schemes for chipcards without identity exist (p. 351 of ref. [18]) and for money transfer only the transaction number, not the identity of chipcards is needed.
If all actions made by a single chipcard are unlinkable for banks without the cooperation of other parties, i.e. clearing anonymity is established in a weak form, it suffices to avoid generating an audit trail within the chipcard, or if an audit trail has to be maintained for security reasons, to make it unintelligible for banks without the cooperation of the chipcard's holder.

A complete description is given in ref. [3]. Measures to tolerate even complete failures or losses of chipcards taking into account not only security but also unobservability are described in refs. [25] and [26].

4.3 Blindly Signed Digital Banknotes

Next, we describe a payment system invented by Chaum [5, 6] realizing anonymity cut 3 only, i.e. independently whether anonymity cuts 1 and 2 are realized or not. This payment system establishes clearing anonymity by unobservability of each currency with itself, cf. section 3.2. Consequently, the digitally transferable currencies in this payment system are encoded messages which are transferred between clients. We refer to them as *digital banknotes* in analogy to banknotes in payment systems using cash, though this denotation is slightly inaccurate because these digital "banknotes" are rather digital bank cheques in standard values issued by the banks. Their full denotation *blindly signed digital banknotes* results from the fact that the bank signs the banknotes *blindly*, i.e. without actually seeing them, which is a precondition that their identity can be changed by the respective owner, cf. section 3.2.

A blindly signed digital banknote consists of a randomly chosen number n providing uniqueness and a redundant part enabling distinction of banknotes from other information. A banknote becomes valid when the bank signs it. Its nominal value is determined by the key used for the signature, i.e. different keys are attached to different nominal values.

To get a digital banknote, a client has to form a note number as described above and to submit it to the bank for signing. The note number, however, is encrypted in a special way. This disables the bank from recognizing the note number whilst signing it, but enables the client to decrypt it after signing without invalidating the signature of the bank, i.e. he changes the identity of the note known (only in encrypted form) to the bank. (This procedure is given formally at the end of this subsection.) After the bank has signed the digital banknote, its nominal value is withdrawn from the client's bank account.

If the banknote will sometime be deposited, the bank is not able to find out to whom of its clients the banknote was originally issued, so that anonymity cut 3 is realized, as shown in figure 5. As mentioned in section 3.2, it is necessary to have some supply of unspent notes to avoid linkability of withdrawal and deposit by unusual amounts or time. Clearly, all withdrawals and deposits on the same account are linkable.

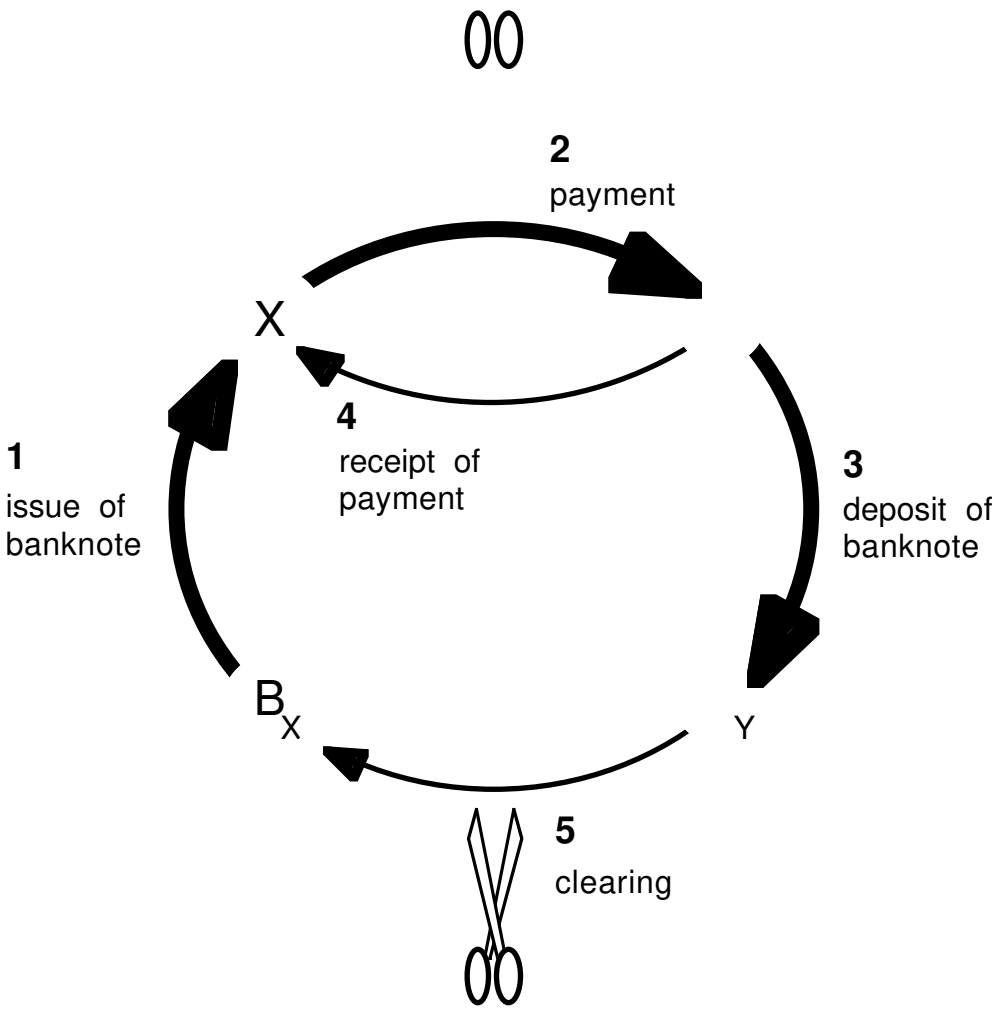

Figure 5: Payment circulation for blindly signed digital banknotes

Only the client who formed the note number is able to decrypt it after the bank signed it. By decrypting it, he can establish clearing anonymity (independently whether he is payer or payee), even against a coalition of the other and the bank. Clearly, the protocols for a payment vary slightly depending on who encrypts and later decrypts the banknote [7]. To allow payer and payee to verify clearing anonymity, both parties have to encrypt and later decrypt the banknote.[2] In the following, we will only consider in detail the variation, where the payer encrypts the note number. Therefore, it seems appropriate to outline the other variations.

If the payee forms the note number, it has to be sent to the payer first, who submits it to the bank for signing. The payer may submit the note number unchanged or encrypted by him a second time implying that he has to decrypt it before passing the signed note back to the payee. Since in any case only the payee has the information to decrypt the digital banknote yielding a valid banknote, the bank (even with the cooperation of the payer) cannot recognize the note number when it is submitted for deposit. For the same reason, the payee can be sure, that the digital banknote received from the payer has not already been deposited. If the payer would form the banknote (as described in full detail in the following), he and the bank together could of course link withdrawal and deposit, so that the payee cannot verify that clearing anonymity exists.

---

[2] The duality is, that the bank and either payer or payee may cancel clearing anonymity because of certain circumstances. This can be achieved if the party who encrypts the note number gives the information necessary to decrypt it to the other.

With this payment system usually only on-line payments are possible (cf. section 3.3), independently of who formed the note number. In case the payee forms the note number, the payer has to submit the note number to the bank when the payment takes place. In the other case where the payer forms the note number, the payee has to ask the bank first if a received digital banknote has not already been deposited.
Only in case the payee is known to the payer in advance, the account number of the payee together with an expiry date of the reservation may be encoded into the note number, allowing the digital banknotes to be deposited only to the specified account during reservation. Before the expiry date the payee can verify that the banknote is covered locally. Afterwards the banknote may be deposited to arbitrary accounts, so that it may be used for other payments than the originally intended one, in case the payer changed his mind or the intended business comes to nothing.

Care has to be taken to prevent the banks from falsely claiming that a particular banknote has already been deposited. Therefore the note numbers contain some secret information known only to the payer who forms the note number. This information has to be revealed to the payee who discloses it to the bank only after he has received a confirmation that the banknote was not yet deposited. In order to prove that a banknote had already been deposited, the bank has to show this secret information.
The problem to form messages which contain secret information is one of the basic problems of cryptography and can be solved in various ways. The method applied in this case uses a public one-way-function f [12]. The note numbers are of the form $f(x)$ completed by redundancy. The argument x is known to the payer only and is called *precursor* to $f(x)$ and to the resulting note number. By definition of a one-way-function, it is impossible to compute the precursor out of the note number efficiently. Another method offering more flexibility applies digital signatures linked to digital pseudonyms [3].

The following protocol shows withdrawal, payment and deposit of a digital banknote. This is an extended version of Chaum's original and still unpublished *bank-proof payer anonymity protocol* [7]. The extension is necessary to use this payment system for payments between two remote and anonymous parties. The substantial improvements are the introduction of an expiry date for each reservation and receipts of payments. It should be noted that the secrecy and authentication mechanisms for the messages are not shown. Besides the notation introduced in section 2.2, the following notation is used to formalize the protocols throughout this and the next section:

X* --- *m* ---> *B means *X* sends message *m* to *B*. *m* may contain text to clarify its meaning. To distinguish explanatory text from parameters, it is written in capital letters whereas parameters are written in small letters, e.g. *m* = ("MY NAME IS *x*").
If the message is signed to enable the receiver to check the authentication (which is done by applying the corresponding operator auth_x), its origin is recorded in the message by specifying that operator (which is not shown in the protocols).

***X* : operation** means *X* performs an operation described by "operation" locally. Some of these operations may not be formalized. In these cases the operation is explained by text enclosed in quotation-marks.

=?= denotes a boolean condition that is true only if the expressions on both sides have the same value. If a boolean condition yields "false", the protocol is aborted and, if necessary, appropriate recovery measures are taken.

Signing *blindly* exploits a special property of the public key cryptosystem RSA[3] and is explained in the following:

A keypair of RSA is denoted as (e_x, d_x) where e_x is the key for encryption and d_x the key for decryption. Encryption and decryption of a message m is denoted as $e_x(m)$ and $d_x(m)$, respectively. Encryption and decryption are inverse operations. The cryptosystem RSA has the additional property that both operations are commutative. Thus we have the following identities which hold for all keypairs and all messages m from the allowed message space:

$$d_x(e_x(m)) = e_x(d_x(m)) = m$$

The above-mentioned special property of RSA is denoted as multiplicative homomorphism, i.e. for all keypairs (e_x, d_x) and all messages m_1, m_2 we have:

$$e_x(m_1 \bullet m_2) = e_x(m_1) \bullet e_x(m_2)$$
$$d_x(m_1 \bullet m_2) = d_x(m_1) \bullet d_x(m_2)$$

(It should be noted that the messages are represented in binary digits and are interpreted as binary numbers in the above operations.) The property that RSA is a multiplicative homomorphism is used to get *blind signatures* by multiplying the message m to be signed by a random "blinding factor" r encrypted with the encryption key e_x. The resulting product will be signed by applying the decryption key d_x. Thus the signing party sees only $m \bullet e_x(r)$ which gives no clue about the message m. By applying d_x on the product, we have:

$$d_x(m \bullet e_x(r)) = d_x(m) \bullet d_x(e_x(r)) = d_x(m) \bullet r$$

The blinding factor r can be removed from the resulting product by multiplication with its multiplicative inverse r^{-1} which yields the signed message $d_x(m)$.

A few special primitive operators are used:

x := random	denotes the operation of choosing an argument x at random from the allowed message space.
x^* := special (x)	denotes the operation to form x^* out of x by addition of redundancy, such that check (x^*) becomes true.
check (x)	denotes a predicate that is true only if x is the result of a preceeding operation special (x).
***f*(x)**	denotes the image of an argument x under f, a public one-way-function.

Prerequisite:
We assume that bank B uses the operator sign_B for signing its messages. The operator auth_B to check whether a message has been signed by B is publicly known. The bank uses a keypair (e_B, d_B) of the RSA public key cryptosystem exclusively to sign banknotes; d_B is kept secret, e_B is publicly known and determines the nominal value of a banknote signed with d_B.

[1] X forms a blinded note number and submits it to the bank for signing in step [1.5]:
  [1.1] $X : n'$:= random
  [1.2] $X : n := f(n')$

---

[3] This was true at the time we wrote this paper (spring 1987). In the meantime, universal translation techniques have been invented [1, 8] which can be used to implement blind signatures using an arbitrary signature system [27, 11]. But the expense of this universal translation techniques seems to be extraordinarily high.

[1.3] X : n^* := special (n)
[1.4] X : r := random
[1.5] X --- $n^* \bullet e_B(r)$ ---> B

Note:
n' is the secret information which prevents the bank from falsely claiming a particular note had already been deposited, since n' cannot be obtained from n.
n is the actual note number. Since n is formed under a one-way-function, attacks to obtain the banks signature on $n = f(n')$ when n' is given or vice versa are ineffective.
$\boldsymbol{n^*}$ is the note number extended by redundancy, e.g. $n^* = n,f(n)$. This will be used to prevent reservation of fake notes for deposit (cf. step [6] of the protocol).
r is a random "blinding factor" which disables the bank to recognize the note number n^* whilst signing it.

[2] The bank checks the authentication of the message received in step [1.5] and signs the submitted blinded note number. At the same time, the nominal value of the note is withdrawn from the account of X:
[2.1] B : "account of X covered?"
[2.2] B : "withdraw from account of X"
[2.3] B : "form $d_B(n^*) \bullet r = d_B$ ([1.5])"
[2.4] B --- $d_B(n^*) \bullet r$ ---> X
[2.5] B --- "STATEMENT OF ACCOUNT" ---> X

Note: The procedure in step [2.3] describes the bank's "blind signature" as explained in the preliminary remark at the begin of the protocol.

[3] X removes the blinding factor and checks whether he has received a valid banknote or not:
[3.1] X : $d_B(n^*)$:= [2.4] $\bullet\ r^{-1}$
[3.2] X : e_B ([3.1]) =?= n^*

[4] X transfers the note to Y:
[4.1] X --- $d_B(n^*)$ ---> Y

[5] Y checks the signature on the note and submits it to the bank for deposit to one of his accounts:
[5.1] Y : n^* := e_B ([4.1])
[5.2] Y : check (n^*)
[5.3] Y --- $d_B(n^*)$ ---> B

[6] The bank verifies the validity of the submitted note:
[6.1] B : n^* := e_B ([5.3])
[6.2] B : check (n^*)
[6.3] B : "n^* already cashed or reserved?"
[6.4] B : "register n^* as reserved for Y until t"
[6.5] B --- sign_B ("n^* RESERVED FOR Y UNTIL t") ---> Y

Note: Notes which are submitted for deposit but whose precursor to the note number has not been shown yet, will be registered as reserved for deposit. Therefore it is important that notes cannot be reserved without having the bank's signature which is checked in step [6.1] and

[6.2]. If the note numbers n^* submitted for reservation are just random numbers not having any redundancy, it will be easy to reserve a multitude of notes by submitting randomly chosen numbers m. Each result $e_B(m)$ of encryption by e_B could be reserved. This would cause the banks a lot of unnecessary work and storage overhead, since the precursor to $e_B(m)$ cannot be shown (otherwise f would be no one-way-function).
In order to limit the time span of the above-mentioned storage overhead and in order to prevent the bank from refusing forever to accept a submitted note argueing the note has already been reserved for someone else, an expiry date t is used. If the precursor to the note number is not shown until this expiry date, the reservation will be cancelled.
The specification of Y in step [6.5] may be any digital pseudonym of Y, e.g. the digital pseudonym under which Y is known to the bank as holder of an anonymous numbered account.

[7] Y checks the confirmation of reservation received in step [6.5] and forwards it to X:
[7.1] Y : auth_B ([6.5])
[7.2] Y --- [6.5] ---> X

[8] X checks the confirmation of reservation received from Y in step [7.2] and sends Y the precursor to the note number:
[8.1] X : auth_B ([7.2])
[8.2] X --- n' ---> Y

[9] Y verifies the precursor received from X in step [8.2] and sends a receipt of payment to X and the precursor to the bank:
[9.1] Y : special (f([8.2])) =?= n^*
[9.2] Y --- "RECEIPT OF PAYMENT" ---> X
[9.3] Y --- [8.2] ---> B

[10] The bank verifies the supplied precursor and deposits the note to the account of Y:
[10.1] B : special (f([8.2])) =?= n^*
[10.2] B : "n^* marked for Y?"
[10.3] B : "mark n^* as cashed"
[10.4] B : "deposit to account of Y"
[10.5] B --- "NOTE NUMBER n^* CASHED, STATEMENT OF ACCOUNT" ---> Y

If an anonymous payee refuses to give a receipt of payment to the payer (cf. step [9.2]), though the precursor has already been sent, then the payer can prove that he has made a payment since he can show the confirmation of the bank saying that the note has been reserved for the payee. Of course this serves as proof only before the expiration of the reservation has elapsed. However, it does not prove whether the payer has sent the precursor to the note number to the payee or not. Therefore the precursor to the note number has to be made known to the payee by publishing it (encrypted and therefore only readable for the intended payee) on an electronic blackboard. Thus, the payer is sure to get at least a substitutional receipt of payment issued by a court.

4.4 Anonymously Transferable Standard Values

This payment system establishes clearing anonymity by unlinkability of different currencies, cf. section 3.2. It uses digitally transferable currencies called *anonymously transferable standard values* which can be thought of as accounts upon which standard values are deposited [2]. The value in standard denominations is encoded in the *value number*. The anonymously transferable standard values are administered by the bank similar to anonymous numbered accounts, cf. subsection 4.1. The owners of these anonymously transferable standard values are known to the bank only by their digital pseudonyms which are unlinkable to anything else which is known to the banks. Payments are made by transferring the ownership of these values.
If a payment is made, the payee has to choose a new digital pseudonym and to sign a declaration proving that he wants to become (under this newly generated identity) the owner of an anonymously transferable standard value currently held by the payer. The signed declaration can be checked by applying the corresponding auth-operator which is an older digital pseudonym under which the payee is known to the payer. Obviously, this newly generated digital pseudonym should differ from the older digital pseudonym to prevent the bank from deriving undesired concatenations without the cooperation of the payer. To disable the payer, too, from linking pseudonyms without the cooperation of the bank, the newly generated pseudonym can be shown to him encrypted only with a public key of the bank. After the payer has received this declaration, he orders the bank to register the digital pseudonym of the payee, as specified in the declaration, as new owner of the anonymously transferable standard value held by him. The bank confirms execution of the order either to the payer who then forwards this confirmation to the payee, or to payer and payee. In any case the payer should receive a receipt of payment from the payee as soon as the payee has received the confirmation of execution. If the payee refuses to give a receipt of payment, the payer has sufficient evidence proving that a payment was made: the declaration of the payee and the confirmation of the bank.

The protocol for the transfer of ownership of an anonymously transferable standard value from payer *X* to payee *Y* is as follows:

Prerequisite:
We assume that *X*, the current owner of an anonymously transferable standard value v_n, has chosen the operator $sign_x$ to sign the transfer order when this value is to be transferred. Therefore $auth_x$, the corresponding operator to verify the authentication of the transfer order, is registered at the bank *B* administering this value as the digital pseudonym of the current holder.
The bank uses the operator $sign_B$ for signing its messages. The operator $auth_B$, to check whether a message has been signed by *B*, is publicly known.
Messages from *Y* to *X* are signed by $sign_{yx}$ and checked by $auth_{yx}$,, which is a digital pseudonym of *Y* known to *X*.

[1] *Y* gives his consent to *X* to become the new owner of the anonymously transferable standard value v_n currently held by *X*. *Y* has to choose the operators $sign_y$ and $auth_y$ at random, which will be used for signing and verifying authentication of messages respectively. The auth-operator is communicated to *X*:
[1.1] *Y* --- $sign_{yx}$ ("AGREEMENT TO REGISTER $auth_y$ AS NEW OWNER OF v_n") ---> *X*

[2] *X* checks the authentication of the message received in step [1.1] and gives order to the bank to register $auth_y$, the randomly chosen digital pseudonym of *Y*, as new owner:
[2.1] *X* : $auth_{yx}$ ([1.1])
[2.2] *X* --- $sign_x$ ("REGISTER $auth_y$ AS CURRENT OWNER OF v_n") ---> *B*

[3] The bank checks the authentication of the transfer order received in step [2.2] and executes it:
[3.1] B : auth_x ([2.2])
[3.2] B : "insert auth_x and [2.2] in the list of former owners of v_n"
[3.3] B : "register auth_y as current owner of v_n"
[3.4] B --- sign_B ("auth_y REGISTERED AS CURRENT OWNER OF v_n") ---> X
[3.5] B --- sign_B ("auth_y REGISTERED AS CURRENT OWNER OF v_n") ---> Y

[4] X checks the confirmation of transference from B received in step [3.4]:
[4.1] X : auth_B ([3.4])

[5] Y checks the confirmation of transference from B received step [3.5] and sends a receipt of payment:
[5.1] Y : auth_B([3.5])
[5.2] Y --- sign_{yx} ("RECEIPT OF PAYMENT") ---> X

Two modifications of this protocol should be mentioned:
Of course, it is also possible that the bank sends the confirmation of transference to X only who then has to forward it to Y. This possibility has the advantage that in case the payer has not obtained a receipt of payment and has to prove that a payment was made, it is not necessary to ask the bank whether it has sent the confirmation of execution to the payee, since the payer is responsible for sending the confirmation of execution to the payee.
The expense of generating a new pair of operators for each transfer of an anonymously transferable standard value can be saved by using arguments under a public one-way-function which are taken as the digital pseudonyms of the owners. The resulting impacts are described in ref. [3].

Obviously, this payment system provides both, relation anonymity and clearing anonymity, cf. figure 6. However, it should be mentioned that whenever the ownership of such a value is transferred, the digital pseudonyms of the current owner X and the intended next owner Y of the anonymously transferable value become linkable to the digital pseudonyms under which they are known to each other if one of them has the cooperation of the bank. This linkability can be avoided if special measures (cf. section 5.1) are taken.

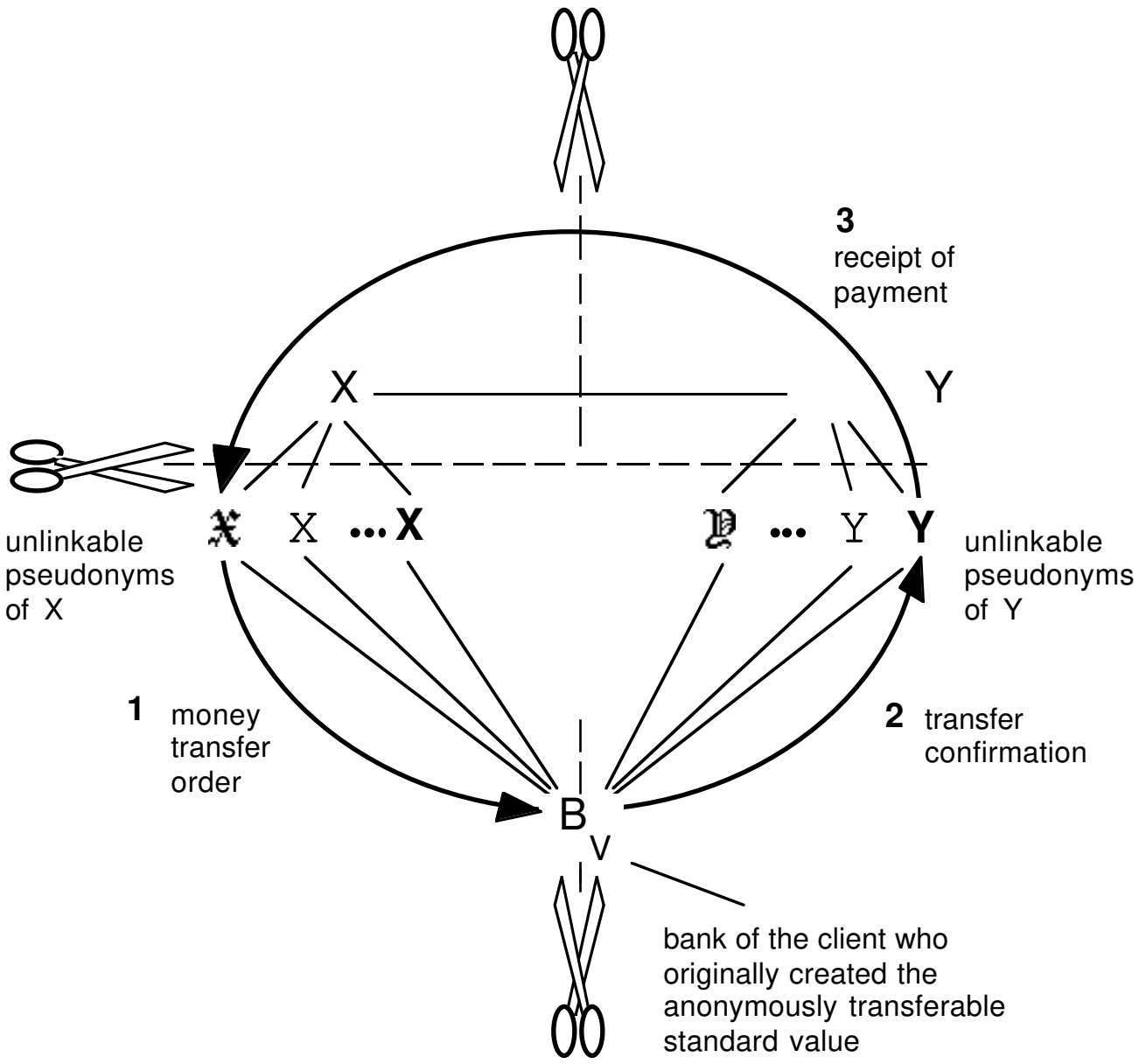

Figure 6: Payment circulation for anonymously transferable standard values

The further characteristics with respect to the possibility for off-line payments of this system are:

* Off-line verification of prearranged off-line payments is possible: the payer reserves some anonymously transferable standard values exclusively for payments to specified digital pseudonyms of the payee until an expiry date. The payer gets a corresponding confirmation signed by his bank which he can give the payee, who checks whether he is the owner of the specified pseudonyms and whether the expiry date does not occur too early. If both conditions are satisfied, he can be sure that every transfer of ownership signed by the payer is covered.
* Off-line payments to arbitrary payees cannot be verified by the payee without using the network.

A comparison of *anonymously transferable standard values* and *blindly signed digital banknotes* with respect to unobservability, security, and expense is given in ref. [3].

5 Combinations and Interest

It is clear from section 3.1 that it is appropriate to unite the system realizing anonymity cut 2 only (anonymous numbered accounts) with the one realizing anonymity cut 3 only (blindly signed digital banknotes) to get both relation and clearing anonymity. Further and more elaborate combinations are described in the following two subsections.

5.1 Combinations To Get Maximal Anonymity

In section 3.1, we started the discussion about digital payment systems enabling unobservability of clients in view of the fact that the bank can clearly link all actions involving an account. Then we showed two dual possibilities by which the clients can establish the desired clearing anonymity. These dual possibilities are unlinkability of different currencies and unlinkability of each currency with itself. Obviously, a payment system which combines both possibilities will provide a maximum of clearing anonymity, as shown in figure 7.

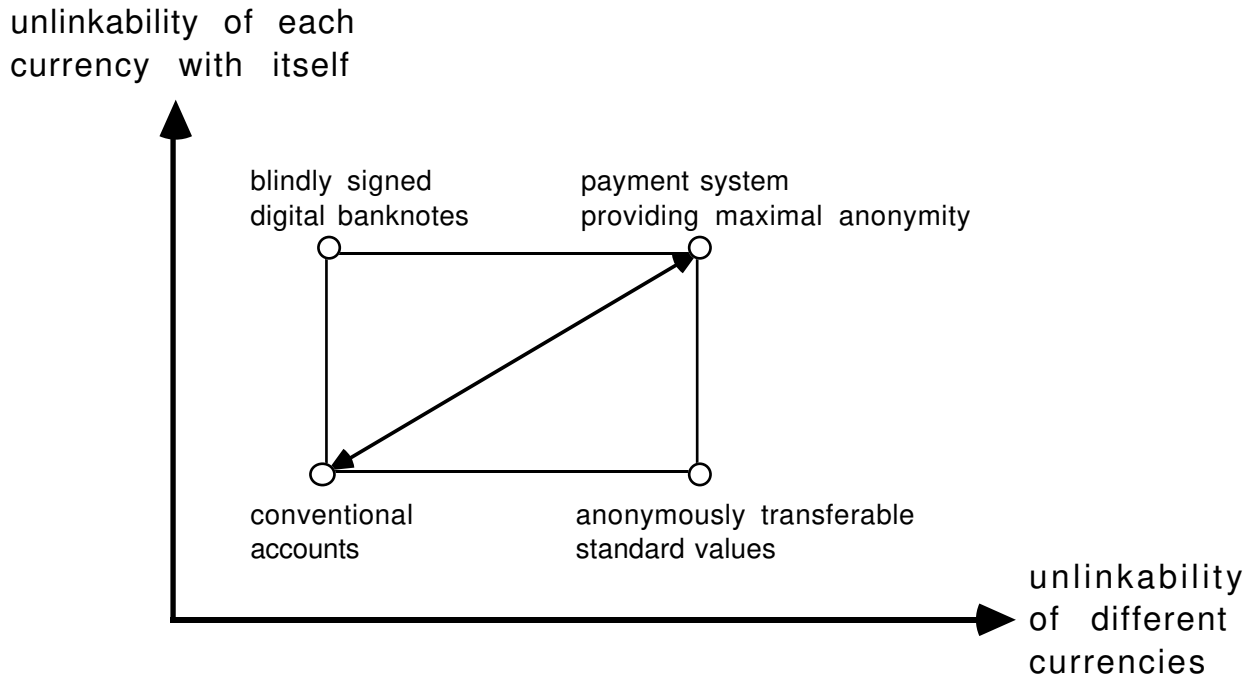

Figure 7: Combination to get maximal anonymity

In order to obtain a payment system which provides maximal anonymity, the measures by which the payment systems with blindly signed digital banknotes and anonymously transferable standard values, respectively, establish clearing anonymity have to be combined suitably. But what should such a combination look like?

Consider the case that anonymously transferable standard values are used for a payment. It is quite obvious, that the digital pseudonym under which a client is known to the bank as the holder of an anonymously transferable standard value is linkable to the digital pseudonym under which he is known to his transaction partner if bank and transaction partner collude. This would cause no harm as long as the digital pseudonym under which a client is known to the bank as the holder of an anony-

mously transferable standard value is used for one transaction only. Then it cannot be linked to anything else and each holder of an anonymously transferable standard value must clearly be known to the bank by a digital pseudonym anyway. As a matter of fact, however, this digital pseudonym is used for a second transaction, that is, when the payee wants to use the received anonymously transferable standard value for another payment. To unlink the two transactions described above, clients should be able to change the identity of their digital pseudonyms known to the bank the same way as they can with blindly signed digital banknotes. This can be done by using the same special measure [6] which is applied to hinder the credentials-issuing organizations from deriving undesired concatenations (cf. section 2.2) and which is based on blind signatures as well.

5.2 Combinations Enabling Off-line Payments Even Without Absolutely Tamper-Resistant Devices

Obviously, the usability of digital payment systems increases when they can be used not only for secure on-line but also for secure off-line payments. Therefore, it is appropriate to use two systems side by side, namely

- the only one enabling off-line payments in general (tamper-resistant devices) but in a modified form to confine damage in case the devices are not as tamper-resistant as supposed, and
- one not depending on tamper-resistant devices for more secure on-line payments.

A modification of tamper-resistant devices cannot consist only in restricting the maximum value of off-line payments since in case the tamper-resistance is severely injured, e.g. if the secret parameters could be derived by recording and decoding the electromagnetic radiation, no restricting measure can limit the damage. It is essential that any damage arising when someone has broken the mechanism of the tamper-resistant device can be ascertained quickly and that the knowledge of the secret parameters stored within the device is not sufficient to produce an unlimited amount of money. Both can be achieved if the devices contain, e.g. blindly signed digital banknotes. Then their function is restricted to the storage and transfer of digital money, which will be erased from the storage of the device as soon as it is spent. Yet their main purpose is to guarantee that each banknote is spent only once. Then in case someone breaks the mechanism of the tamper-resistant devices, he can only cheat by spending banknotes several times. This fraud is discovered when somebody tries in vain to deposit a banknote which has been deposited before. As in off-line payments anonymity cut 1 is not completely realized anyway (because the clients see each other), one can try to trace the origin of the duplicated banknote. To increase the chance of discovery, the number of off-line transactions with each banknote should be restricted to one.

5.3 Interest

Obviously, in any digital payment system where banks or tamper-resistant devices administer the money, interest can be paid without any technical problems. Special methods even allow accrual of interest for digital banknotes [7].

6 Required Future Action

Of course the existence of a payment system enabling unobservability does not necessarily mean that it must be used for all kinds of payments. Each client can determine for himself how much unobservability of his payments he wishes, unless there are restrictions by law. For instance, such restrictions could be decreed because collecting progressive taxes will become even more problematical than today when people receive several incomes under different pseudonyms. But also for this problem solutions enabling unobservability using the credential mechanism are conceivable. An advantage of an anonymous payment system can be that it may be more generally accepted as substitute for cash, so that cash could even be abolished. This would make theft more difficult, since active cooperation of the victim is required. Black markets and illicit work would possibly thin out, since sales and income tax could be collected automatically whenever the payment system is used and/or possession of money could be taxed.

So far, our arguments mainly used the interests of individuals. But the state should have an interest in payment systems enabling unobservability as well, since enforcing its own policy concerning security and privacy is possible only then. Without the use of such payment systems, national sovereignty (at least concerning privacy) would be heavily endangered whenever computer equipment containing secret "know how" is used, especially when bought from abroad.

Before these payment systems and other appropriate anonymous transaction protocols can be used in practice, the legal framework has to be adapted appropriately [21]. But this would be necessary for any digital payment and transaction system anyway.

Today the state bears the full risk of the cash system without installing a nearly perfect supervision and control system encircling everyone everywhere. If banks de facto replace cash, they have to take over this risk from the state without installing payment systems with nearly perfect supervision and control to locate the weak spot quickly if the system should be misused or broken. As a matter of fact, most digital payment systems used today, e.g home banking via BTX (interactive videotex in Germany) are immature and insecure from a technical point of view. The circumstance that great frauds were rare (or at least not reported) up to now and could have been covered by insurance [22], together with the missing awareness of the clients that their privacy is extremely endangered by these systems (and cannot be covered by any insurance) should not induce anybody to hold on to inadequate payment systems.

Acknowledgements

We are indebted to Dr. Klaus Dittrich, Dr. Klaus Echtle, Prof. Winfried Görke, Birgit Pfitzmann, and Michael Waidner for their valuable suggestions and to the German Science Foundation (DFG) for financial support.

References

[1] G. Brassard, D. Chaum, C. Crépeau: Minimum Disclosure Proofs of Knowledge; Draft July 1987

[2] H. Bürk: Digitale Zahlungssysteme und betrugssicherer, anonymer Wertetransfer; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, April 1986
[3] H. Bürk, A. Pfitzmann: Value Transfer Systems Enabling Security and Unobservability; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 2/87
[4] D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM Vol. 24, No. 2, February 1981, pp. 84-88
[5] D. Chaum: Blind Signatures for untraceable payments; Advances in Cryptology, Proc. of Crypto 82, D.Chaum, R.L.Rivest, A.T.Sherman (eds.), Plenum Press, New York, 1983, pp. 199-203
[6] D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM Vol. 28, No. 10, October 1985, pp. 1030-1044
[7] D. Chaum: Privacy Protected Payments. Unconditional Payer and/or Payee Untraceability; received October 31, 1986
[8] D. Chaum, I. B. Damgård, J. van de Graaf: Multiparty Computations ensuring privacy of each party´s input and correctness of the result; Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, pp. 87-119
[9] D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash; Crypto '88, August 21-25, 1988, Abstracts.
[10] F. Cohen: Computer Viruses – Theory and Experiments; Proc. of the 7th National Computer Security Conference, 1984, National Bureau of Standards, Gaithersburg, MD; USA, pp. 240-263; Computers & Security, North-Holland, Vol. 6, No. 1, February 1987, pp. 22-35
[11] I. B. Damgård: Payment systems and credential mechanisms with provable security against abuse by individuals; Crypto '88, August 21-25, 1988, Abstracts.
[12] D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, Chichester, New York, 1984
[13] D. Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading, Mass.; 1982
[14] S. Even, O. Goldreich, Y. Yacobi: Electronic Wallet; 1984 International Zurich Seminar on Digital Communications, March 6-8, Zurich, Switzerland, IEEE, pp. 199-201
[15] O. Goldreich: Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme; Advances in Cryptology – CRYPTO '86, August 1986, A. M. Odlyzko (ed.), Lecture Notes in Computer Science LNCS 263, Springer-Verlag, Heidelberg, 1987, pp. 104-110
[16] S. Goldwasser, S. Micali, R. L. Rivest: A "Paradoxical" Solution to the Signature Problem; 25th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, October 24-26, 1984, pp. 441-448; revised and extended version entitled "A digital signature scheme secure against adaptive chosen-message attacks" appeared in SIAM J. Comput. Vol. 17, No. 2, 1988, pp. 281-308
[17] H. Maurer, N. Rozsenich, I. Sebestyen: Videotex without "Big Brother"; IIG, Universität Graz, Bericht F128, January 1984
[18] C. H. Meyer, S. M. Matyas: Cryptography - A New Dimension in Computer Data Security; John Wiley & Sons, 1982
[19] A. Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 International Zurich Seminar on Digital Communications, March 6-8, Zurich, Switzerland, IEEE, pp. 183-190
[20] A. Pfitzmann, M. Waidner: Networks without user observability; Computers & Security, North-Holland, Vol. 6, No. 2, April 1987, pp. 158-166
[21] B. Pfitzmann, M. Waidner, A. Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht (CR), Verlag Dr. Otto Schmidt KG, Köln, Vol. 3, Oct., Nov., Dec. 1987, No. 10, 11, 12, pp. 712-717, 796-803, 898-904
[22] R. M. Richards, J. L. Guynes: A Strategic Plan for Reducing Consumer Anxiety About EFTS Security; acm SIGSAC Security, Audit&Control Review Vol. 4, No. 2, Spring 1986, pp. 4-8
[23] K. Thompson: Reflections on Trusting Trust; Communications of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763
[24] V. L. Voydock, S. T. Kent: Security Mechanisms in High-Level Network Protocols; acm computing surveys Vol. 15, No. 2, June 1983, pp. 135-171
[25] M. Waidner, B. Pfitzmann: Verlusttolerante anonyme elektronische Brieftaschen; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 1/87
[26] M. Waidner, B. Pfitzmann: Verlusttolerante elektronische Brieftaschen; Fault-Tolerant Computing-Systems, Sept. 9-11, 1987, Bremerhaven, Informatik-Fachberichte 147, Springer-Verlag, Heidelberg, pp. 36-50, revised version appeared in DuD, Datenschutz und Datensicherung, Vieweg Verlag, Braunschweig, No. 10, October 1987, pp. 487-497

[27] M. Waidner: Betrugssicherheit durch kryptographische Protokolle beim Wertetransfer über Kommunikationsnetze; Arbeitsbericht über das DFG-Projekt "Betrugssicherheit" September 1986 bis April 1988; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 7/88

Note added in proof:
In the meantime, some additional bibliographical data and newer versions of papers are available.
[1] appeared in: Journal of Computer and System Sciences 37 (1988) 156-189.
[7] revised and extended in: Smart Card 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conf.; Laxenburg (Austria), Oct. 1987; North-Holland, 1989, pp. 69-93.
[9] efficiency improvement presented at: EUROCRYPT'89.
[14] revised and extended in: S. Even, Secure Off-Line Electronic Fund Transfer Between Nontrusting Parties, Smart Card 2000: The Future of IC Cards, Proc. of the IFIP WG 11.6 Intern. Conf.; Laxenburg (Austria), Oct. 1987; North-Holland, 1989, pp. 57-66.

Holger Bürk studied computer science at the University of Karlsruhe from 1982 to 1988. He is now with Ascom Tech AG, Switzerland, where he does applied research in the area of secure communication.
His research interests include security and privacy aspects in digital commmunication networks and cryptographic protocols. He is a member of IACR and GI.

Andreas Pfitzmann studied computer science at the University of Karlsruhe from 1977 to 1982 and graduated with first-class honors.
Since then he has done research and has taught as assistant in the department of computer science of the same university. He is author or coauthor of about two dozen papers for national and international conferences and journals on reliability and fault tolerance of computer systems and on privacy and security against fraud in digital communication and payment systems.
Mr. Pfitzmann's current research interests include technical means to protect the privacy and security of data in networks, fault tolerance in these networks, and higher transaction protocols to prevent fraud in spite of anonymity of the transaction partners.
He is a member of ACM, IACR, IEEE, DVD, and GI.