erschien in: Computers & Security 9/8 (1990) 715-721

Refereed Article

Value Exchange Systems Enabling Security and Unobservability

Holger Bürk *, Andreas Pfitzmann ‡

* Ascom Tech AG, Labor Solothurn,
Bielstr.122, P.O.Box 151, CH-4502 Solothurn, Switzerland

‡ Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe,
P.O.Box 6980, D-7500 Karlsruhe 1, West-Germany

Abstract

The main problem arising in value exchange over a network, e.g. in the exchange of digital money for other valuable information, is the lack of simultaneity of the exchange, yielding a temporary advantage for one party, who could then stop communication. The situation is even worse when this party is anonymous. This normally is the case when digital payment systems enabling unobservability are used. But third parties can be used to overcome this problem. We compare two rather different approaches using third parties. The first tries to provide security by third parties identifying perpetrators in case of detected fraud, whereas the second uses a third party as trustee who takes an active part in the value exchange and can be completely controlled by each absolutely anonymous party.

Keywords

Cashless payment, digital payment systems enabling unobservability of clients, digital pseudonyms, identification by third parties, trustee, unobservable value exchange

1. Introduction

The users of present-day cashless payment systems are observable since the banks and (by installing a Trojan Horse [4]) even the manufacturers of the computer equipment used can learn 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. Thereby, these payment systems become completely unacceptable, since compiling dossiers on the lifestyle and whereabouts of all clients will become easy. Therefore, in [2] we summarized the digital payment systems enabling unobservability of clients and explained the technical capabilities needed to support unobservability.

If these payment systems are used to anonymously buy *ware* (valuable information, e.g. the answer to a database query) for digital *money*, an additional security problem is posed: The lack of a simultaneous exchange between two remote and possibly anonymous parties causes a temporary advantage for one party, who could then stop communication. Thus, if this party stops communication prematurely, a claim against it will remain valid and should be called in if necessary. Therefore, a *value exchange* system is needed which enables unobservability and provides security against fraud.

Solutions for the simultaneity problem developed for signing contracts [1, 5] are not suitable for value exchange in general. For contracts it is possible to define that a contract is only binding if it is signed *n* times (with prefixes 1 to *n*) [1, 5], but for messages it makes no sense to define that a message only has meaning (i.e. is valuable information) if it is signed *n* times. Goldreich's solutions to the concurrent identification problem [6, 7] cannot be adapted either, because both solutions presuppose a fixed identity of persons which can be established and approved beforehand. This is in contrast to value exchange, where values not known beforehand (e.g. new information, a new cheque, etc.) are to be exchanged.

In Chapter 2 and 3, we describe two approaches to enable unobservable value exchange between two anonymous parties which is secure against fraud. Both approaches use third parties to bypass the simultaneity problem. Their advantages and disadvantages are summarized in Chapter 4.

Both approaches assume that anonymous parties choose keypairs of a *digital signature scheme*, where the public key to test signatures (*test key* for short) is used as *digital pseudonym*, cf. [3, 2 Chap. 2.2]. Thus, the identity of parties is given by their digital pseudonyms and the authenticity (and legal relevance) of their messages is conferred by signing them digitally with their corresponding private keys.

Please note that we use the term *value* to designate a category comprising both *ware* and *money*.

2. Security by Identification of Perpetrators in Case of Detected Fraud

This concept guarantees the identification of debtors who refuse to pay, thereby enabling satisfaction of their creditors as in the non-anonymous case.

2.1 How to Obtain Credentials for Digital Pseudonyms

To tackle this problem we first describe how to establish a digital signature scheme. Then we explain how to avoid linkability without degrading performance. Finally, we discuss who shall act as authenticating third party.

How to Bootstrap the "Digital World"

As stated in the introduction, we assume that in general each party chooses digital pseudonyms to authenticate its messages. To allow the identification of the originators of messages, for each digital pseudonym one party must have identified itself as its holder to a trusted and non-anonymous third party by signing and sending to it a corresponding document. The non-anonymous third party issues to the holder of the pseudonym a *credential* which proves that the holder of this particular digital pseudonym can be identified if necessary.
Irrespective of anonymity and the intended area of application, when for the first time someone wants to establish a digital signature scheme which is legally binding for him, it is necessary that he signs a contract in writing. This might require the presence of the signer and at least one human witness and in any case is clumsy and expensive. But thereafter, even the process of getting new digital pseudonyms can easily be automated: Computers are programmed to check the digital signature on the request to issue a credential. The computer simply has to check whether there is a manually or digitally signed document stating the holder of the test key and whether the request is correctly signed with respect to this test key. If both tests yield true, the computer signs the corresponding credential on behalf of the authenticating third party and sends it back to its originator, i.e. its submitter and prospective holder.

How to Avoid Linkability and Maximize Performance

A digital pseudonym need not be created and the corresponding credential need not be issued for a particular value exchange, but could in principle be used for many purposes. Since multiple use of one digital pseudonym enables linkability, it is recommended to use each digital pseudonym and the corresponding credential for only one purpose, e.g. in one value exchange. This causes no special performance problems since many credentials for different digital pseudonyms of the same holder can be obtained in one transaction with the authenticating third party.

Who Shall Act as Authenticating Third Party and Why?

Owing to the generic nature of such credentials, it is conceivable that the government, certain organizations (banks, value-added network providers, postal and telecommunications services) and even individuals (lawyers, public notaries) will act as authenticating third parties. Since only the initialization of the digital signature scheme is expensive, acting as an authenticating third party may be well honored by small fees.

2.2 Main Protocol Idea

Before each value exchange, the parties have to authenticate themselves mutually by means of the credentials described in Section 2.1 and agree upon what they wish to exchange. Subsequently business proceeds as usual. Messages sent are authenticated and made legally binding by digital signatures linked to digital pseudonyms.
For the authentication of the pseudonyms, a single trusted third party [8] or a chain of trusted third parties [3] may be used. The second method has the property that a party exchanging values can be identified only if all authenticating third parties of the chain are cooperating. It can be extended to tolerate faults or sabotage from a few third parties with the techniques described in [9]. For brevity, we only describe the first method. Of course the third party (as well as the chain of third parties) may be different for each party exchanging values, as shown in Figure 1.

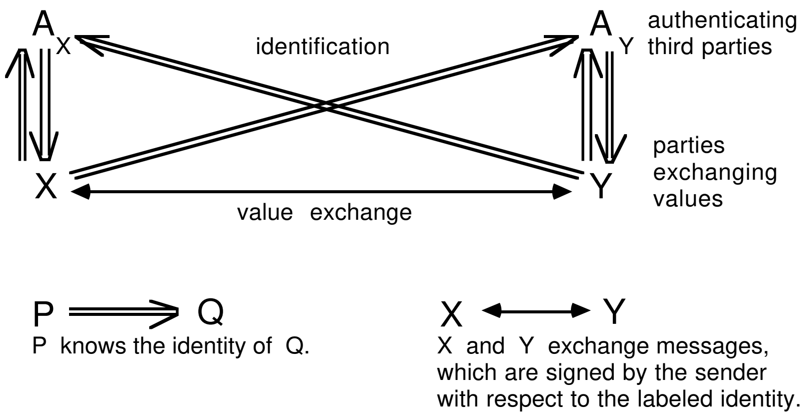

Figure 1: Security by authenticating third parties

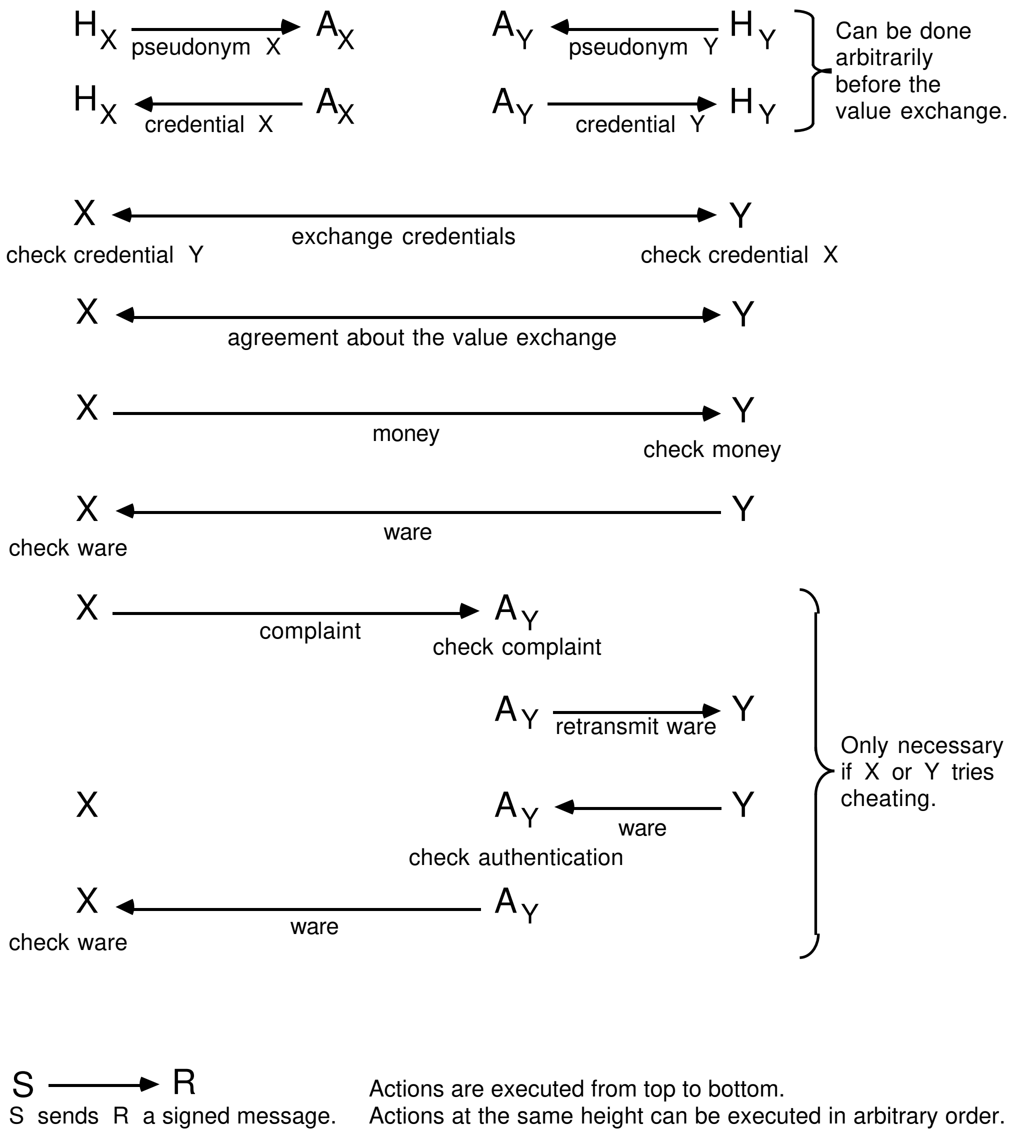

Figure 2: The three phases of value exchange using authenticating third parties

Knowing the identity of an authenticating third party is trivial since this party is not anonymous. If P knows the identity H_Q of the holder of a digital pseudonym Q, this means that P has a document signed by H_Q stating that Q is one of his digital pseudonyms.

In a case in which one party, e.g. the one denoted by the pseudonym *X*, complains (falsely or correctly) to the authenticating third party A_Y of its business partner denoted by the pseudonym *Y* that this "bad guy" has broken off the communication prematurely, *X* first has to submit signed messages from *Y*, e.g. the agreement about the value exchange, to show that a communication between *X* and *Y* existed. When A_Y has verified this, it requests the accused *Y* to continue the communication, cf. Figure 2. If *Y* refuses, it will be identified by A_Y and examination proceeds as in the non-anonymous case.
The only inconvenience that is incurred if *Y* is falsely accused of having broken off communication prematurely is that *Y* is obliged to send the rest of the messages again. Given the capacity of todays mass storage devices, this presents no problem for *Y*. On the other hand, by receiving the messages twice, *X* gains nothing, since *X* could copy these messages alone as well. In case of a complaint the messages are sent via the authenticating third party of the accused party to the complainant. Thus, the complainant cannot falsely claim again that he has not received the messages. By charging a small fee for each complaint to the authenticating third party, abuse can be reduced to a tolerable level.

If one of the parties exchanging values complains that what it has received from the other party does not meet its expectations (or, more exactly, the agreement between them specifying the value exchange), it has to go to court and submit its evidence. Then the court has to decide whether the identity of the accused party has to be revealed by the authenticating third party to enable appropriate criminal proceedings to be undertaken.

The advantages and disadvantages of this concept are summarized in Chapter 4.

3. Security Between Absolutely Anonymous Parties by Active Participation of a Trustee

The second approach to security and anonymity for value exchange uses active participation of a non-anonymous trustee who executes the value exchange between the absolutely anonymous parties.

3.1 Main Protocol Idea

We first consider the usual case in which some ware, e.g. useful information, is exchanged for money between two absolutely anonymous parties denoted by the digital pseudonyms *X* and *Y* respectively. The value exchange uses the active participation of a non-anonymous trustee *T*. The situation is shown in Figure 3.

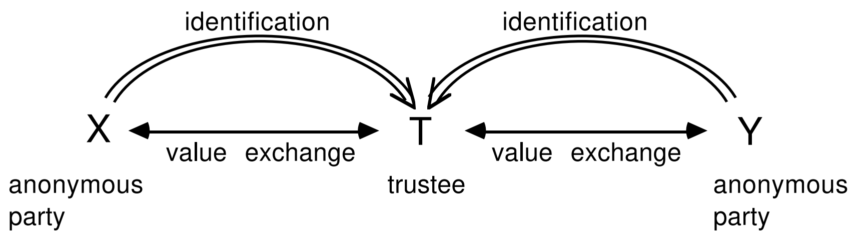

Figure 3: Security by an active trustee

Before the value exchange takes place, *X* and *Y* inform the trustee what they wish to exchange and agree upon the form and extent of the trustee's service concerning the value exchange. In this way *X* and *Y* are able to control the actions of the trustee and bring him to court if he does not adhere to the agreement.
Then *X* sends the money and subsequently *Y* the ware to *T*, who checks whether what he receives is what has been agreed upon. According to the result of this check, money and ware are passed on to the intended recipients, or the exchange is broken off and money and ware are returned to their respective senders together with a justification for the breaking off. In order to make collusion between the trustee and *X* against *Y* ineffective, the ware should not be sent until the trustee has confirmed to *Y* that he has received the money from *X*. Otherwise the trustee could return the ware to *Y* with the justification that *X* has not sent the money while actually sending a copy of the ware to *X* in secret. The protocol is sketched in Figure 4.
Another possibility is to pass ware and money to the trustee concurrently, but let *Y* choose the trustee, so that collusions of *X* and the trustee are unlikely.

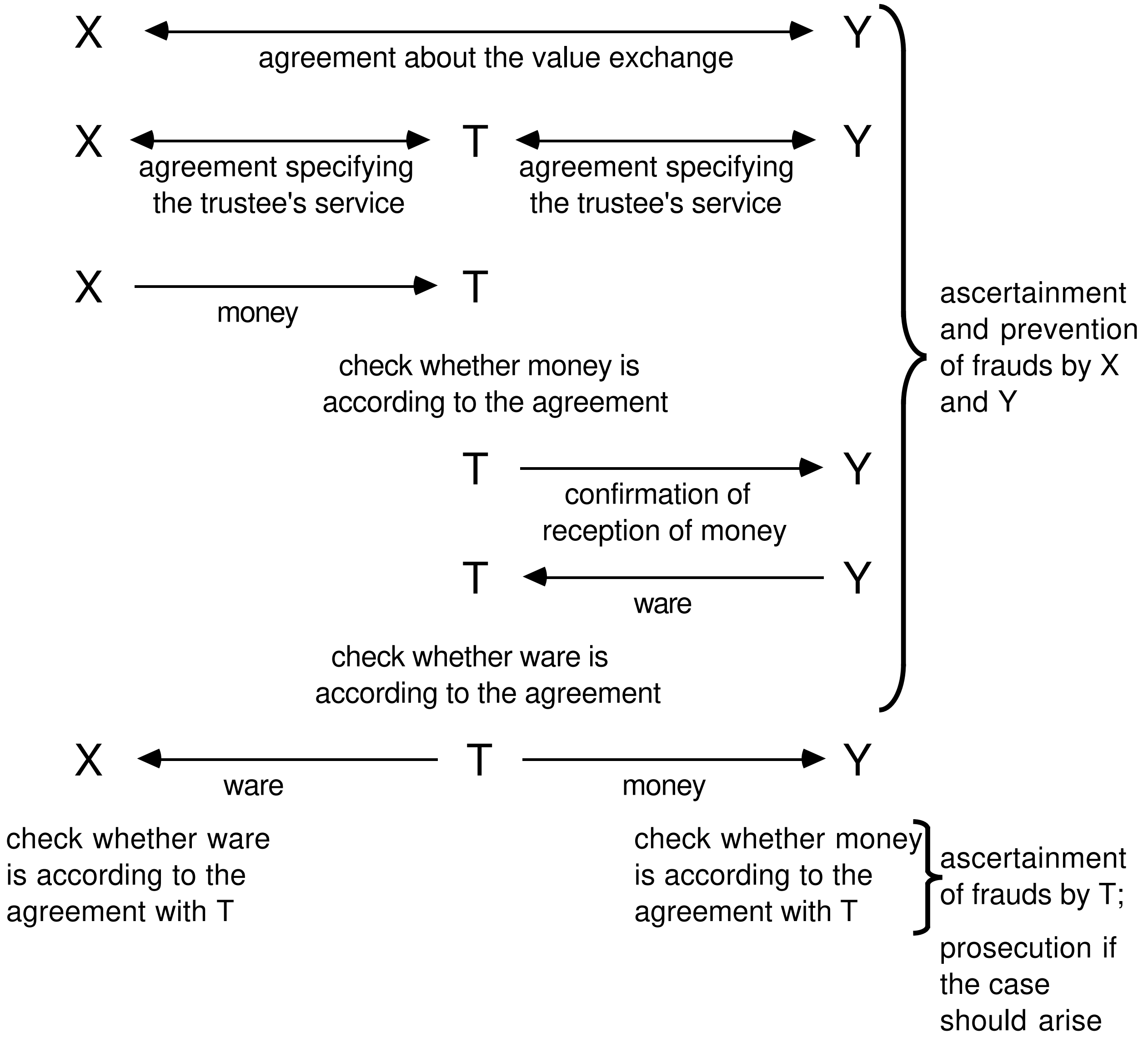

Figure 4: Procedure of value exchange by an active trustee

If X claims that it has not received the ware, it can be sent again with negligible costs for T, because information can be copied virtually for free. Because the payment is made in two parts, i.e. X pays T first and T pays Y afterwards, it is also impossible to cheat by falsely claiming not to have received the money, since with all payment systems allowing unobservable payments presented in [2], the payer can prove that he has made a payment.

3.2 Protocol Variations

We describe two further protocol variations: The first handles the case in which the trustee is unable to check the ware. The second sketches a scheme for exchanging two wares.

How to Cope if the Trustee is Unable to Check the Ware

If the trustee is not or should not be able to check the transmitted ware (e.g. for reasons of informal properties of the ware or for reasons of privacy), X and Y may agree upon a complaint time during which the trustee retains X's money but passes the ware from Y to X without checking it. If X complains that the ware does not meet its expectations (or, more exactly, the agreement between X and Y specifying ware and price), it may forbid T to pass the money to Y and has to prove that the ware is indeed faulty. If an eventually called court works fast enough no appreciable damages, i.e. loss of interest, will arise.

Even if it is not possible to provide rapid decision, loss of interest can be limited if T is obliged to deposit the money in a bank to gain interest. For that period the money is available neither to X nor Y. The case may arise that X or Y is forced to borrow money in the meantime implying that a usually much higher interest must be payed than that earned by the deposited money. To compensate for this loss, X and Y may have agreed with T before starting the value exchange that both have to pay regularly the difference in interest to T, who deposits this money with the bank as well. Of course, since X and Y are absolutely anonymous, it is not possible to force X or Y to pay the difference to T. But this can be compensated for by establishing the rule that if X or Y does not pay the difference to T, the other party receives the whole sum immediately. If both pay regularly, the court has to decide and T has to give the money to X and Y as decided.

How to Exchange Wares

The case in which the values to be exchanged are both wares which T cannot or should not inspect can be solved by splitting the exchange into two coordinated parts "ware against money" and "money against ware" and setting up the additional rule that T does not give money to X or Y until both are satisfied with the wares obtained or until a court has made a decision.

If desired, the rules described for preventing unjustified loss of interest can be adapted to this case accordingly.

4. Comparison of the two approaches

The advantages (+) and disadvantages (–) of the two approaches are summarized in Table 1.

Security by Identification of Perpetrators in Cases of Detected Fraud	**Security Between Absolutely Anonymous Parties by Active Participation of a Trustee**
+ Only in the case of fraud is active participation of the authenticating third party needed while the values are exchanged.	– The trustee must always be active while the values are exchanged.
– Who should ensure that the identities of the parties exchanging values are revealed by the authenticating third party only in the assigned cases?	+ The parties exchanging values are completely anonymous.
	+ No confidence in the trustee's service is necessary, since the trustee can be controlled by the parties exchanging values and brought to court if frauds or irregularities are ascertained.
– Uncovered claims may arise because it is never verified that the parties can pay and identification of such parties does not help very much (see Section 4. (1) of ref. [2]).	+ All charges from one party exchanging values to the other may be called in by recourse to the values deposited with the trustee.

Table 1: Advantages and disadvantages of the two approaches

To come to a final judgement, let us consider how the disadvantages can be moderated, especially by the expected progress of information technology.

Keeping identities secret requires both organizational and technical means. Regrettably, humans (and therefore organizations as well) are not always honest. The same is true with respect to the design of computers, where the possibility of Trojan Horses leaking data cannot be excluded. Using a fault and sabotage tolerant chain of authenticating third parties (hopefully diverse with respect to humans in the roles both of operators and designers of computers) as mentioned in Section 2.2 helps greatly and moderates this disadvantage considerably. Technical progress enables ever longer and thereby more secure chains. But it does not help the parties exchanging values to ensure that their identities are not compromised.
Without a third party which is active while the values are exchanged we cannot imagine how to avoid uncovered claims. But society as a whole seems to have learned to live with them.
The active trustee can easily be implemented by a computer thereby avoiding any performance problems, if the problem of checking informal properties of the ware is excluded. This checking is in general a time and human labor consuming task irrespective of how the value exchange is organized. If this problem is excluded, postal and telecommunications services or value-added network providers may offer a fully computerized additional service to act as trustees using some standard contracts for value exchange.

After weighing these arguments against each other, we prefer the second approach to provide security and anonymity for unobservable value exchange.

Acknowlegements

We cordially thank Birgit Pfitzmann, Manfred Böttger and an anonymous referee for their comments on this paper.

References

[1] Michael Ben-Or, Oded Goldreich, Silvio Micali, Ronald L. Rivest: A Fair Protocol for Signing Contracts; Automata, Languages and Programming (ICALP), 12th Colloquium, Nafplion, Greece, July 15-19, 1985, Winfried Bauer (ed.), LNCS 194, Springer Verlag, Heidelberg, pp. 43-52

[2] Holger Bürk, Andreas Pfitzmann: Payment Systems Enabling Security and Unobservability; Computers & Security Vol. 8, No. 5, August 1989, pp. 399-416

[3] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM Vol. 24, No. 2, February 1981, pp. 84-88

[4] Dorothy Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading, Mass.; 1982

[5] Shimon Even, Oded Goldreich, Abraham Lempel: A Randomized Protocol for Signing Contracts; Communications of the ACM Vol. 28, No. 6, June 1985, pp. 637-647

[6] Oded Goldreich: On Concurrent Identification Protocols; Laboratory for Computer Science, Massachusetts Institute of Technology, MIT/LCS/TM-250, December 1983

[7] Oded Goldreich: On Concurrent Identification Protocols; Advances in Cryptology, Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of Cryptographic Techniques, April 9-11, 1984, Paris, France, T. Beth, N. Cot, I. Ingemarsson (eds.), Lecture Notes in Computer Science LNCS 209, Springer-Verlag Heidelberg, 1985, pp. 387-396

[8] S. Herda: Authenticity, Anonymity and Security in OSIS. An Open System for Information Services; Proc. 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, P.P.Spies (ed.), Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg 1985, pp. 35-50

[9] Andreas Pfitzmann: How to implement ISDNs without user observability - Some remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 14/85