PAYMENT SYSTEMS AND CREDENTIAL MECHANISMS WITH PROVABLE SECURITY AGAINST ABUSE BY INDIVIDUALS

(Extended Abstract)

Ivan Bjerre Damgård[1]

Aarhus University, Mathematical Institute,
Ny Munkegade,
DK 8000 Aarhus C,
Denmark.

Summary

Payment systems and credential mechanisms are protocols allowing individuals to conduct a wide range of financial and social activities while preventing even infinitely powerful and cooperating organizations from monitoring these activities. These concepts were invented and first studied by David Chaum.

Clearly, such systems must also be secure against abuse by individuals (prevent them from showing credentials that have not been issued to them, etc.). In this work, we present constructions for which we can prove, that no individual can cheat successfully, unless he possesses an algorithm that contradicts a single plausible intractability assumption. This can be done while maintaining the unconditional security against abuse by organizations.

Our construction will work using any general two-party computation protocol with unconditional privacy for one party, and any signature scheme secure against adaptive chosen message attacks (these concepts are explained in more detail later). From the signature scheme by Bellare and Micali [BeMi] and the multiparty computation protocol by Chaum, Damgård and van de Graaf [ChDaGr], it will be clear that both requirements can be met if pairs of claw free functions and trapdoor one-way permutations exist. This, in turn, is satisfied, for example if factoring Blum integers is a hard problem.

For credential mechanisms, we obtain an additional advantage over one earlier proposals [ChEv], where a center trusted by the organizations (but not by individuals) was needed. This center possessed a "master" secret allowing it to issue all types of credentials supported by the system. Moreover, the center had to be on-line permanently. In our construction, only an off-line center is needed, which only has to be trusted as far as validating the identity of each individual is concerned. Only organizations authorized to issue a given type of credential have the ability to compute them.

---

[1]This research was supported by the Danish Natural Science Research Council.

S. Goldwasser (Ed.): Advances in Cryptology - CRYPTO '88, LNCS 403, pp. 328-335, 1990.

1. Related Work

In earlier work, Chaum [Ch] and Chaum and Evertse [ChEv] have proposed ways to implement payment systems and credential mechanisms, and have established their security against infinitely powerful organizations by information theoretic arguments. While these constructions were quite practical, they left some open questions with regard to the security against abuse by individuals: For payment systems, this security depended on the assumption that RSA used for signatures, along with some redundancy scheme or one way function, is secure against a chosen message attack. So far, no one has been able to reduce this to some widely accepted intractability assumption, and in fact many proposed redundancy schemes have subsequently been broken. For credential mechanisms, the security could only be proved in a restricted, formal model, where potentially bad interaction between RSA and the one way function used was abstracted away. Moreover, an assumption about a very powerful center was needed, as outlined in the summary above (note, however, that Chaum [Ch2] has later modified the construction to do without this last assumption).

Chaum [Ch3] has also designed a credential mechanism which has provable security, but is based on the specific homomorphic properties of RSA. This protocol is much slower than [ChEv], although not completely unresonable in practice.

By contrast, our work is of mainly theoretical interest: while the protocols constructed are probably not practical in the forseeable future, the main purpose of our work is to establish the existence of credential mechanisms and payment systems with respect to as weak an intractability assumption as possible.

In independent work, Chaum [Ch2] has designed a protocol construction with some properties quite similar to ours, in terms of feasibility, the intractability assumption needed, and the problems that can be solved by the protocols. Chaum's solution uses interactive proofs, and not multiparty computations. Compared to our work, the process of creating a credential is simplified, while the process of showing one is slightly more complicated.

2. Basic Results

A pair of functions (f_0, f_1) is called *claw free* if

- $\mathrm{Im}(f_0) = \mathrm{Im}(f_1)$.
- Both functions are t to 1 mappings for some constant t.
- Both f_0 and f_1 are easy to compute, but it is hard to find *a claw*, i.e. r, s, such that $f_0(r) = f_1(s)$.

It is well known that claw free pairs of permutations exist, for example if factoring a Blum-integer is hard. A Blum-integer is an integer $n = pq$, where p and q are primes congruent to 3 modulo 4. As an easy example, consider

$$f_0(x) = x^2 \bmod n, \quad \text{and} \quad f_1(x) = (a \cdot x)^2 \bmod n,$$

where a has Jacobi symbol -1. It is elementary to prove that these functions permute the set of quadratic residues modulo n, and that knowledge of a claw immediately implies

knowledge of the factors of n. If the functions are easy to invert, given some extra information, they are called *trapdoor*. The example above clearly has this property: knowledge of the factors of n suffices to extract square roots modulo n. Although more details would be required for a formal definition, the above will do for this abstract. Details on claw-free functions and their cryptographic applications can be found in [Da].

Our protocols are based on the following two results:

Theorem 1. [BeMi]
If one-way trapdoor permutations exist, then there exists a signature scheme which is secure against an adaptive chosen message attack □

Here, "secure" means that an enemy will not be able to produce even a single message m and a valid signature for it, if he has not seen a signature for m produced by the real signer. This signature system will be called "The BM signature scheme" in the following.

Theorem 2. [ChDaGr]
If clawfree pairs of functions exist, and trapdoor one-way permutations exist, then there exists a protocol allowing parties A and B to carry out any (probabilistic) computation with private input, such that the secrets of A are unconditionally protected, and the secrets of B are protected, if A cannot invert the one way trapdoor permutation used □

This protocol can easily be generalized such that also the output is kept secret to one party. Note also that the unconditional protection of one party is essential to the "unconditional untraceability", that we want from the systems constructed in the following. Therefore other general computation protocols [Ya], [GoMiWi] cannot be used.

One of the main ideas in this protocol is that, using a pair (f_0, f_1) of claw free functions, it is possible for participant A to *commit* to a choice of a bit, without giving away any Shannon information about her choice: having chosen $b \in \{0,1\}$, A chooses uniformly $x \in domain(f_b)$, and computes the *commitment*, $f_b(x)$. If she chooses to do so, A can later *open* the commitment by revealing x, this will convince everybody about her original choice.

Since both functions are t to 1 mappings, even an infinitely powerful receiver will not be able to compute anything about b from the commitment; and by the claw freeness, a polynomially bounded A will not be able to open a commitment in more than one way. Note, however, that any method for establishing such commitments can be used by the protocol, and that the existence of pairs of claw free functions is not a necessary condition for the existence of bit commitment schemes.

In the protocols considered in this paper, we have two kinds of participants: individuals with limited (polynomially bounded) computing power, and organizations, which may have unlimited computing power, but are not required to use it in the protocols. Given organization O and individual A, consider the following interaction:

1) O chooses an instance of the BM signature scheme, and sends the public key to A.

2) A chooses some message m.

3) A and O use the protocol from Theorem 2 to compute O's signature on m. The protocol is set up, such that A is unconditionally protected and enters m as private output, while O enters the secret key to the signature scheme. Also, the signature is private output for A.

4) Steps 2) and 3) are repeated a number of times, polynomial in the security parameter.

Let us remark that the security parameter is simply an integer that measures the work that has to be done in the protocol, and the cryptographic security.

Theorem 3.
After the above interaction, the following hold:

i) O has no information in the Shannon sense about the m's chosen by A.

ii) A is not able to compute O's signature on any message with non negligible probability, unless it has been chosen in step 2) at some point.

Proof (sketch).
i) is clear from Theorem 2.
Assume ii) is false. Then the following procedure will break the BM scheme under an adaptive chosen message attack, contradicting Theorem 1:
We simply run A's algorithm, and each time A has executed step 2), we use the chosen message attack to obtain a valid signature on the m that was chosen. With this information, we can simulate A's interaction with O in step 3) without knowing the secret key. By the minimum-knowledge property of the computation protocol, the messages sent in the simulated interaction have a distribution which is polynomially indistinguishable from those sent in a conversation with the real O. In particular, this means that A's probability of outputting a new, signed message is essentially the same in the simulation as in the actual interaction with O □

3. Payment Systems

In a payment system, we have one special participant called the bank (B). In addition, we have a set of individuals, and a set of organizations.

Each individual can do a special interaction with B called a *withdrawal* (one can think of this as the individual withdrawing money from his account). If B is willing to participate, then after completion of the withdrawal, the individual can compute one element in a set of numbers called EC. A number in EC is called an *electronic coin* (*ec*). Each individual can submit the *ec*'s he possesses to organizations as payment. The organization will then, possibly by interacting with B, decide whether to accept the payment. The purpose of a payment system is to ensure that:

1) Each *ec* can be submitted and accepted as payment exactly once.

2) At some point of time, consider the set Ω of successful withdrawals. Let Δ be the set of *ec* 's accepted by organizations. Assuming that 1) holds, Δ must correspond in a natural way to a subset of Ω, i.e. there is an injective map, $f : \Delta \rightarrow \Omega$, such that when $f(\delta) = \omega$, then ω is exactly the withdrawal which enabled that individual to later transmit δ to some organization. We now require, that at each point of time, no matter which strategy the organizations (including the bank) follow, and no matter how much computing power they have, the probability distribution on f they can compute will be the uniform distribution over all injective mappings from Δ to Ω.

Based on Theorem 3., a payment system is easily designed: Assume individual A has an account in bank B. The bank chooses an instance of the BM-signature scheme, and we fix the rule that any number signed with this instance is an *ec*.

When A wishes to conduct a withdrawal, he chooses a random number R and gets the bank's signature on it by doing the computation protocol from Theorem 2 with the bank. Since R is entered as private input from A, B gets no information on the numbers signed. After this, the bank deducts the corresponding amount from A's account. When A wants to spend his money, say in shop S, he gives R and the signature to S. S will send this to B, who will check if R has been submitted before, and whether the signature is valid. The bank then puts money on the account of S and informs S about acceptance of the payment.

It follows easily from Theorem 3 that A will not be able to spend money without receiving it from the bank first, and that the bank will not be able to trace any number it receives, back to a particular individual, i.e. condition 2) above is satisfied, and condition 1) holds relative to our intractability assumption.

In contrast with the credential mechanism to be outlined later, this system needs an on-line participant, namely the bank. This seems to be an inherent property in systems were numbers are worth money, and you want to prevent individuals from using a number more than once.

4. Credential Mechanisms

For this, we need the concept of unconditionally secure *bit commitments*, as explained in Section 2.

What we are looking for is a method allowing organization O to transmit personal information about individual A, say, to some other organization. Typically, this information takes the form of a *credential*, i.e. a message saying that a given individual satisfies some "predicate": he can drive a car, passed an exam, etc. At the same time, we want to prevent organizations from building complete records on the behavior of an individual, i.e. find out which credentials he possesses, who he shows them to, etc. Following the ideas of [ChEv], we will let each individual represent himself by different *pseudonyms* with different organizations. Assume that some unique bit string $ID(A)$ (name, address, etc.) is attached to each individual A. Then a pseudonym in our case will be a set of unconditionally secure bit commitments to the bits in $ID(A)$. A will compute one such set for each organization, he interacts with.

In order for a credential mechanism to be useful, it has to satisfy 2 basic properties:

1) No individual can show a credential to anyone, unless it has been properly issued to him.

2) The credential mechanism reveals no Shannon information about which pseudonyms apply to the same individual.

Property 2) must be stated a little more precisely before it can be formally proved, but it will do for the informal reasoning in this abstract.

A more complete and formal definition of the concept of a credential mechanism can be found in [ChEv].

To set up our construction, we need one special organization, called Z, which will be used to validate once and for all each individual in the system. Z starts by choosing its own instance of the BM scheme and sending the public key to all participants.

The following protocol is executed for each individual A:

a) A sends $ID(A)$ to Z, and Z checks this against A. Z also makes sure that A has not entered the system before.

b) The following steps c)-d) are executed for each organization O, that A wants to interact with later:

c) A chooses a random bitstring R_O, which must contain as many bits as is needed as random input to the computation of A's pseudonym with O.

d) A and Z do a computation protocol, where Z signs a bitstring which is the concatenation of $ID(A)$, $ID(O)$ and R_O. A is unconditionally protected, and enters R_O as private input, while $ID(A)$ and $ID(O)$ are public. Z enters its secret key to the signature scheme as private input. The resulting signature is given to A as private output.

After this, A can compute his pseudonym with O, $PS_O(A)$, based on R_O. When he starts interacting with O, he must first convince O that he knows Z's signature on a string which is the concatenation of $ID(A)$, $ID(O)$ and a string R_O, and also that this string has the property that computing a pseudonym for $ID(A)$ based on R_O leads to the pseudonym $PS_O(A)$ that A wants to use with O. Using the general computation protocol with no private input from O, this can be done while revealing no information to O about $ID(A)$ or R_O.

Lemma 1

The above ensures that each individual is represented by at most 1 pseudonym with each organization, and that different individuals have different pseudonyms with the same organization.

Proof.

Assume the first statement is false, and let A be an individual with 2 pseudonyms representing him with O. Since $PS_O(A)$ is uniquely determined by $(ID(A), R_O)$, this means that A must have Z's signature on at least two strings of the form $(ID(A), ID(O), R_O)$, $(ID(A), ID(O), R'_O)$. But since Z only signs 1 string starting with

$ID(A)$, $ID(O)$, this contradicts Theorem 3. If the second statement is false, this trivially implies that some conspiracy of individuals has been able to find a claw for the pair of functions used in computing commitments. But this contradicts the basic assumption on claw freeness □

Now, for each type of credential, an instance of the BM scheme is chosen, and each organization authorized to issue that type is assumed to have a copy of the secret key. We then fix the rule that a given type of credential applies to A, if he possesses a signature in the corresponding signature scheme on $ID(A)$.

O can now issue a credential to A by doing a computation protocol with him, where O signs $ID(A)$. During this protocol, it is checked by using the commitments in $PS_O(A)$ that A really enters the correct ID-string as private input.

A can show this credential to O' by convincing O' that he knows a signature in the relevant signature scheme on the string committed to in $PS_O(A)$. As before, this can be done while revealing no information about $ID(A)$ or the signature.

Theorem 4.
The credential mechanism outlined above satisfies properties 1) and 2).

Proof.
1): By correctness of the computation protocol, it is clear that A cannot show a credential, unless he really knows the relevant signature on $ID(A)$. By Lemma 1, he cannot pretend being someone else, and in that way fool an organization into computing this signature for him. Thus, if he did not receive the credential from an organization, the only possibility is that he computed the signature himself, which contradicts Theorem 3.
2): follows easily from the fact that all individuals are unconditionally protected in all interactions with organizations □

It might be argued that this system, like any system that identifies people by numbers, does not protect against different *physical* persons sharing the same *digital* identity (see for example [De]). A solution to this would of course have to deal with the problem of checking the physical identity of a person. Numerous solutions using tamper resistant devices, photos, hand-written signatures and the like can be developed. Note that such a solution does not have to violate condition 2) above (the untraceability), because the identity check does not have to be executed by the organizations themselves, but could be done e.g. by an independent tamper resistant device.

Acknowledgement

The author would like to thank David Chaum for many inspiring and helpful discussions on credential mechanisms in general, and on this work in particular.

References

[BeMi] Bellare and Micali: "How to Sign Given any Trapdoor Function", these proceedings.

[Ch] Chaum: "Privacy Protected Payments", Preprint., available from author.

[Ch2] Chaum: Private communication.

[Ch3] Chaum: "Elections with Unconditionally Secret Ballots and Disruption Equivalent to Breaking RSA", to appear in Proc. of EuroCrypt 88.

[ChDaGr] Chaum, Damgård and van de Graaf: "Multiparty Computations Ensuring Privacy of each Party's Input and Correctness of the Result", Proc. of Crypto 87, Springer.

[ChEv] Chaum and Evertse: ''A Secure and Privacy Protecting Protocol for Transmitting Personal Information Between Organizations", Proc. of Crypto 86, Springer.

[Da] Damgård: "The Application of Claw Free Functions in Cryptography; Unconditional Protection in Cryptographic Protocols", phd.-thesis, Aarhus University, 1988.

[De] Desmedt: "Special Uses and Abuses of the Fiat-Shamir Passport Protocol", Proc. of Crypto 87, Springer.

[GoMiRi] Goldwasser, Micali and Rivest: "A Paradoxical Solution to the Signature Problem", Proc. of FOCS 84, pp.441-448.

[GoMiWi] Goldreich, Micali and Wigderson: "How to Play Any Mental Game", proc. of FOCS 87.

[Ya] Yao: "How to Generate an Exchange Secrets", proc. of FOCS 86.