An Identity-Based Signature Scheme with Bounded Life-Span

Olivier Delos
Dept of Computer Sc. (INGI)
Place Sainte-Barbe, 2
B-1348 Louvain-la-Neuve, Belgium
E-mail: delos@info.ucl.ac.be
Fax: + 32 10 45 03 45

Jean-Jacques Quisquater
Dept of Elec. Eng. (DICE)
Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium
E-mail: jjq@dice.ucl.ac.be
Fax: +32 10 47 86 67

Abstract

The aim of this paper is to present a signature scheme in which the ability to sign messages of a signer is limited to a fixed number k of signatures. It is an identity-based signature scheme in which each signature can be used only once. We called such schemes "bounded life-span". It is based on mental games and it uses zero-knowledge tools. A validation center is needed to initialize this identity-based scheme. A credential center is used to insure the unicity and the bounded life-span aspects. It allows delegation and numerous practical applications.

1 Introduction

There are a lot of situations where the receiver of a message needs assurances concerning its non-alteration (accidental or voluntary), *i.e.* the authenticity (integrity) of the message and of its origin. The sender must be able to "sign" a message in such a way that any alteration of the message will be immediately revealed by the "signature". Furthermore, if the signature cannot be forged then this will also authenticate the sender.

Diffie and Hellman first introduced the concept of "digital signature" [DH76]. Since their paper, this concept has been the subject of numerous researches [GMR88]. We distinguish undeniable [CvA90], convertible [BCDP91], unconditionally secure, fail stop [WP90], blind, group [vH92], and multi-signatures [DF92, DQ94].

The aim of this paper is to present a signature scheme in which the ability to sign messages of a signer is limited to a fixed number k of signatures. It is an identity-based signature scheme in which each signature can be used only once. We called such schemes "bounded life-span". It is based on mental games [SRA81] and it uses zero-knowledge tools [Sh85, GMRa89, BGKW88].

Cryptography using one-time pad or key is known to be the most secure.

There exist similar aimed authentication schemes described in [dWQ90] but their signature adaptations are too complex. There exist also schemes based on non zero-knowledge techniques as described in [Vau93].

We combine a Guillou-Quisquater signature scheme [GQ89b, DQ94] with an instance of Lamport's scheme [L81]. Our scheme limits the signing power of users of the system to a fixed number of signatures.

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 83-94, 1994.

Our scheme may also be used as a delegation scheme as it is explained in this paper. Practical applications are easily derived from our scheme (*e.g.* to implement payment systems).

The one-time signature is an old concept attributed to Lamport-Diffie and improved in [Mer79]. Other versions which are Public Key Systems oriented are described in [GMR88, BM88, NY89]. Our contribution is to link the original idea of Lamport together with zero-knowledge schemes in an efficient way. It is a practical identity-based scheme whose goal is the limitation of the number of acknowledged signatures.

2 Bounded Life-span Signatures

We now outline our bounded life-span signature scheme, *i.e.* an identity-based signature scheme in which the right to produce acknowledged signatures is limited. Each user has a different but fixed identity I, which is validated once by the authority at the beginning of the system. The following desirable properties apply to such a scheme :

1. Signatures must be used only once, or it will be easily *detected* that a signature was reused,
2. Bounded life-span aspect should be revealed while sending out the signature.
3. No secret information should be revealed,
4. The representation of a user's identity must be fixed at all times, throughout his lifetime in the system.

2.1 Initialization of the System

2.1.1 First Step

A trusted center computes a public composite modulus $n = p \cdot q$ whose factors are strong primes. [1] These are kept secret. The center chooses also a public prime exponent v. The pair $(v\,;n)$ is made public.

Each user of the system has an identity I^*. [2] We assume that the identity string J is built from I^* with some added redundancy. This considerably enhances the intractability of an identity fraud. The center computes the secrets as follows : a redundancy function Red is applied to the original identity I^* such that the left and right parts of the result match a particular pattern. The Red identity J is then used to extract a secret number D using the signing function S of the center [GQ89b]. The center then issues the signer with this secret number $D \in Z_n$. [3] For modulus n and an identity I^* half the length of n, the center thus computes :

[1] A prime p is said to be *strong* if $p = 2\,p' + 1$ where p' is also a prime. A product of strong primes seems to be in general more difficult to factorize [McC90].

[2] To prevent misuse of authentications, we must append to the identity I a particular flag which restricts the use of I to either only authentication schemes, or only signature schemes [DQ94]. This gives I^*.

[3] This secret number D may be stored in a tamper-resistant device (Smart Card) [GUQ91].

$$I^* \longrightarrow J = Red(I^*) \longrightarrow D = S(J)$$
$$\text{where } D^v \cdot J \equiv 1 \mod n$$

Initialization:

$$\begin{tikzcd}
\text{Authority} \arrow[r, "\text{user}"] \arrow[d, "\text{public}"] & D : \; J \cdot D^v \equiv 1 \pmod n \\
(v\,;n) &
\end{tikzcd}$$

After the initialization of all users, the trusted center can be removed. It will not take part anymore in the system other than as a judge to settle eventual conflicts.

2.1.2 Second Step

Consider the following instance of the Lamport scheme [L81] :

Let $F(x) = x^v \mod n$. Here the function F is a one-way function with trapdoor the secret factors of the modulus n. From x_0 we get

$$x_i = F(x_{i-1}), \text{for } i = 1, 2, \ldots, k$$

That is, it is hard to compute x_{k-1} from x_k under the RSA assumption, *i.e.* if n is the product of two distinct primes p and q, and if v is coprime to $\phi(n)$, it is conjectured that extracting a v^{th} root modulo n is as difficult as factoring n. Clearly $x_i \equiv (x_0)^{v^i}$, $i = 1, 2, \ldots, k$. The number x_0 is chosen randomly, as long as the modulus n.

A "credential center" issues each signer with a different and unique (not already used) secret pair (x_k, x_0). Only the signer is able to compute the values $\{x_i\}_{1 \leq i < k}$ from the secret x_0 and nobody can compute x_{i-1} from x_i, unless one knows the secret factors of n.

The credential center registers in a public directory a pair (J, x_k) for each user having an identity I^* and wishing to take part in this system. The indexes i of the public x_i will be decreased each time a signature is registered. The x_i will be published in this directory in the decreasing order following their use by the signer.

$$\begin{tikzcd}
\begin{matrix}\text{Credential}\\ \text{Center}\end{matrix} \arrow[r, shift right, "(x_k, x_0)"'] \arrow[d] & \text{User} \arrow[l, shift right, "I^*"'] \\
\text{Public Directory : List of } (J, x_k) \text{ pairs} &
\end{tikzcd}$$

This secret distribution from the credential center to a legitimate user may be achieved by using a bi-authenticated secret message transmission as described in [DQ].

Secrets are stored in signer's smart card. No secret is needed by the verifier. There is only one modulus n and one exponent v in our scheme.

2.2 The Scheme

2.2.1 The Underlying Guillou-Quisquater Zero-Knowledge Proof

The underlying proof of the scheme is the following :

We describe a four round zero-knowledge bounded life-span variant of the Guillou-Quisquater proof [GQ89a, CP94, GK89] combined with an instance of the Lamport scheme [L81]. This scheme uses a public composite modulus $n = p \cdot q$, where the factors p and q are appropriate secret primes. It is a zero-knowledge proof of knowledge of v^{th} residues, where v is an appropriate public exponent [FFS88, GK89]. Its security is based on the RSA assumption if the exponent v is coprime to $\phi(n)$ [Bu93]. The prover and the verifier are respectively denoted by P and V. The prover has a current public pair (J, x_m) registered in the public directory :

GQ Bounded Life-span Zero-Knowledge Proof :

Input : $(J, x_m; v, n)$.

Language : $L_{c_1 c_2} = \{(J, x_m; v, n) \mid v$ is a prime, $c_1|n| < v < c_2|n|$
and J is a v^{th} residue in $Z_n\}$ with $0 < c_1 < c_2$.

Protocol : To prove that $(J, x_m; v, n) \in L_{c_1 c_2}$, we use the following four rounds :

- $V \rightarrow P : \{w_i = l_i^2 \bmod n\}_{i=1}^{c_1|n|}$, with $0 < l_i < n/2$.
- $P \rightarrow V : T_m = r_m^v \mod n$, where $r_m \in_R Z_n$. [4]
- $V \rightarrow P : \{l_i\}_{i=1}^{c_1|n|}$ and P constructs $d_m = [d_{m_1}, \ldots, d_{m_{c_1|n|}}]_2$, where $d_{m_i} = \frac{(l_i/n)+1}{2}$.
- $P \rightarrow V : t_m = r_m \cdot (D \cdot x_{m-1})^{d_m} \mod n$, where $D^v \cdot J \equiv 1 \pmod{n}$.

Verification: $T_m \overset{?}{\equiv} t_m^v \cdot (J \cdot x_m^{-1})^{d_m} \pmod{n}$ (and $T_m \neq 0$).

Note that we could use a three round bounded life-span variant of the Guillou-Quisquater proof but this protocol is not zero-knowledge though practically secure. Nevertheless a three round **zero-knowledge** bounded life-span variant of the Guillou-Quisquater proof can be obtained by iterating the protocol.

2.2.2 The Scheme

The security of the system is based on the RSA assumption, *i.e.* on the difficulty of factoring n (since v is coprime to $\phi(n)$).

[4] $a \in_R A$ means that the element a is selected randomly from the set A with uniform distribution.

The verifier has access to the public values n, v and to the public pairs (J, x_k) registered in the public directory.

Let us assume that $x_k, x_{k-1}, \ldots, x_{m+1}, x_m$ have already been used by the user having identity J, with $m \geq 1$. The corresponding public "key" of this user is now registered in the public directory as (J, x_{m+1}).

The protocol may be divided in the following steps. To send out a signature using x_{m-1} as a secret with bounded life-span, the signer performs the following :

Bounded Life-span Signature Protocol :

Input : $(J, x_{m+1}\,; v, n)$

Signer :

1. Reveals (J, x_m).
2. Picks $r_m \in_R Z_n$, and computes $T_m = r_m^v \mod n$.
3. Computes the hashing value $d_m = h(T_m, M|I^*)$, where $M|I^*$ is the message to be signed. [5]
4. Computes the final witness $t_m = r_m \cdot (D \cdot x_{m-1})^{d_m} \mod n$.
5. Sends the verifier the signature $\mathsf{Sgn}(T, t, M|I^*)$. [6]

Verifier :

6. Knows $(J, x_{m+1}\,; v, n)$ and (J, x_m) and checks that :
   1. $x_{m+1} \overset{?}{=} x_m^v \mod n$, [7]
   2. $d_m \overset{?}{=} h(t_m^v \cdot (J \cdot x_m^{-1})^{d_m} \mod n, M|I^*)$.

   It is easy to see that if the signer follows the protocol, the verification will be valid. Indeed,

$$\begin{aligned} t_m^v \cdot (J \cdot x_m^{-1})^{d_m} &= (r_m^v \cdot D^{d_m v} \cdot x_{m-1}^{d_m v}) \cdot J^{d_m} \cdot x_m^{-d_m} \mod n \\ &= r_m^v \cdot (D^v\, J)^{d_m} \cdot (x_{m-1}^v \cdot x_m^{-1})^{d_m} \mod n \\ &= r_m^v \mod n \end{aligned}$$

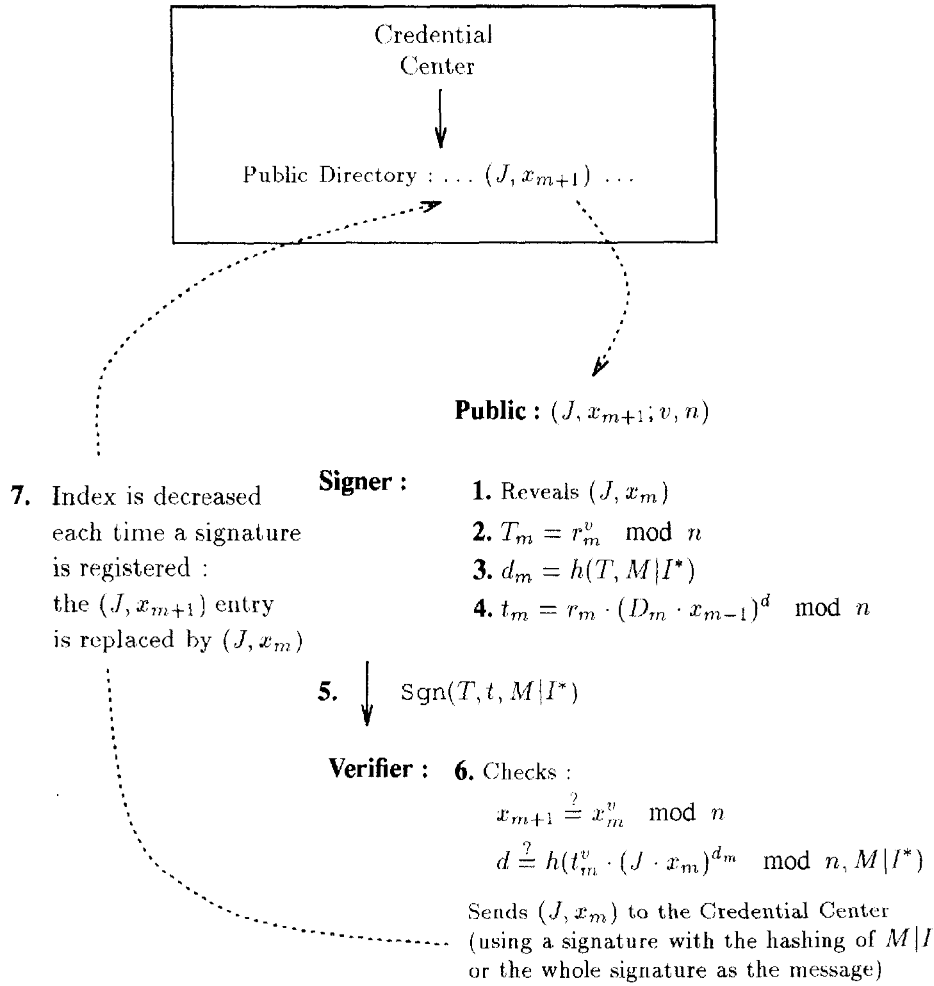
   Using this protocol the verifier is convinced with overwhelming probability that the signer knows $D = S(J)$ (and thus is an authorized entity) and that he knows the secret x_{m-1}. This x_{m-1} which is used but not revealed at the end of the protocol will be actually revealed during the next signing operation.
7. The verifier sends the revealed (J, x_m) with the corresponding signature to the credential center in order to update the public directory.

[5] In this paper, $a|b$ means that a is concatenated with b.

[6] Note that x_m may be revealed as a part of the signature. **Sgn** may merely denote concatenation.

[7] Actually, x_{m+1} is obtained from the public directory.

Schematically,



Credential Center

Public Directory : . . . (J, x_{m+1}) . . .

Public : $(J, x_{m+1}; v, n)$

Signer :

1. Reveals (J, x_m)

2. $T_m = r_m^v \mod n$

3. $d_m = h(T, M|I^*)$

4. $t_m = r_m \cdot (D_m \cdot x_{m-1})^d \mod n$

5. $\mathrm{Sgn}(T, t, M|I^*)$

Verifier : 6. Checks :

$$x_{m+1} \overset{?}{=} x_m^v \mod n$$

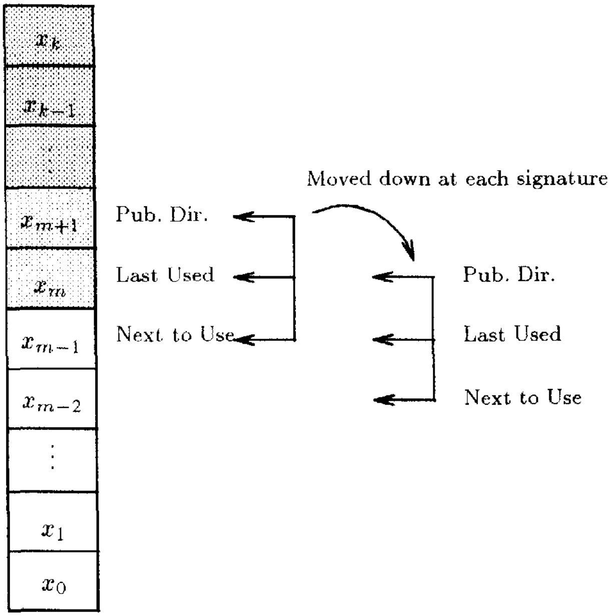
$$d \overset{?}{=} h(t_m^v \cdot (J \cdot x_m)^{d_m} \mod n, M|I^*)$$

Sends (J, x_m) to the Credential Center (using a signature with the hashing of $M|I^*$ or the whole signature as the message)

7. Index is decreased each time a signature is registered : the (J, x_{m+1}) entry is replaced by (J, x_m)

The verifier sends the new public pair (J, x_m) to the credential center as an update request of the public directory. This request is composed of the new entry and either the hashing of the signed message concatenated with the identity string I^* of the signer or the whole signature. This request is signed by the verifier using a classical Guillou-Quisquater signature scheme using D as the secret number.

The bounded life-span secrets x_i may be related to one exclusive credential center (service provider, *etc*). But this deals with management.



Actually the number of available signatures is $k - 1$ if x_0 is used and $k - 2$ if not.

3 Analysis and Remarks

3.1 What Happens if a Signature is Replayed ?

Using for a second time the same value x_m to produce a signature implies a second verification. If the previous verifier was honest the public directory was updated and the second signature will be rejected. At the same time of sending the signature, the signer may publish the value x_m to prevent a reusing by the verifier.

A crooked signer could sign different messages with the same Lamport secret number to different verifiers. But only one signature, the one which will be registered by the corresponding credential center, will be accepted by the verifier.

How could a judge settle an *a posteriori* conflict between two signatures using the same secret(s) but involving two different messages ? If two verifiers are involved in the conflict, the answer is simple : positive decision in favour of the (first) verifier who has signed the update request of the Public Directory. The same solution is adopted if there is only one verifier involved in the conflict since the signed update request of the Public Directory contains the (hashing of the) involved message.

The (J, x_{m+1}) entry in the Public Directory means that the secrets $x_k, x_{k-1}, \ldots, x_m$ have already been used and x_{m-1} is the next secret to be used. Excepted the credential center, nobody can successfully request the update of the Public Directory without the help of the legitimate user.

3.2 Refreshment

Refreshment of "exhausted signatures" is easy, practical and does not require the manufacture of a new card. It consists in loading the card with a new secret pair (x'_k, x'_0) by repeating the second step of the initialization. Our scheme is fully compatible with multi-application smart cards.

3.3 Delegation Scheme

A user may wish to delegate to some trusted entity his capability of signing for a limited time and/or for a restricted number of signatures. The user's smart card can construct and sign time-stamped delegation certificates [ABKL93] to the trusted entity. These delegation certificates enable the delegated entity to convince others that he acts on the behalf of the user. However the time-stamp solution requires a secure time source. This can pose problems for battery-less cards. A possible solution is nevertheless to use the Haber-Stornetta technique to time-stamp a digital document [HS91].

An interesting characteristic of our scheme is its extension to a *delegation signature scheme*. Each user can become a credential "sub-center" accepted (recognized) by the main credential center. When x_{m-1} is the next secret Lamport number to be used, a user, acting as a "sub-center", can delegate his signature power by giving to another user a secret x_i with $1 \leq i \leq m-1$ (using [DQ]). The delegation may concern either any legitimate user or a particular user having an identity string J related to the identity string of the "sub-center" (J contains a particular pattern class introduced by the redundancy function) *without endangering* neither his secret number D nor the secrets x_l, with $1 \leq l < i$.

The identity of the delegate could be related to the delegator. Either the delegator sends an update request to the credential center concerning the identity of its public entry : (J, x_{m+1}) becoming (J, J', x_{m+1}). Or at the initialization of the system, identity classes have been designed on the basis of the identity of candidate delegators. The first solution gives a better protection against stolen secrets (though this should not be a problem by using smart cards).

This delegation scheme is transitive and "suspensive" in the sense that the sub-center must wait the use of x_i before using x_{i-1} otherwise the delegate could not use his available signature. However this revocation possibility gives a full control to the delegator.

3.4 General Remarks

- Actually the credential center is **not** an authority or a trusted center in the sense that he does not (need to) know the factorization of the modulus n. The only part he plays in this scheme is to issue secret Lamport pairs (x_k, x_0) and to manage the Public Directory. Trust is then limited to his application.
- To prevent the fraudulent use of values of k greater than the maximal authorized value, a kind solution is to insert this value in one "field" of the redundant identity J which is signed by the Authority.

- The credential center (and the sub-center or delegator in a delegation scheme) is able to revoke "licenses", signature power, the ability to sign of the signer, once granted.
- How to choose the Lamport numbers :
  A new Lamport pair must never have been used before. Since there could exist many independent credential centers, such numbers should include a particular redundant pattern related to the credential center. Or the simple fact that "registration" is the key word suffices : the credential center is the only entity mastering the **public** directory; this implies a control from the users.
- Performances : From the signer point of view, the costs are roughly the same than for a classic Guillou-Quisquater signature scheme. The verification process is roughly 50% more expansive.
- The protocol is on-line. An off-line version would be possible provided we could have confidence in smart cards.
- Note that this scheme simplifies and generalizes the scheme presented in [dWQ90].
- Would not it be more simple to use a Guillou-Quisquater signature in parallel with an instance of the Lamport scheme, as $F(x) : x^v \mod n$. Doing this we loose the interconnection between the Lamport values and the user's secret $S(J)$. It prevents unauthorized, illegitimate Lamport instances; x_0 must be chosen and validated by the credential center.
  Moreover acting this way the secret numbers must be disclosed before the approval of the signature and then before using the service granted by this approval. In case of (server) (communication) failure some odd instances of secret numbers may be reused. On the other hand, in our scheme, secret numbers are revealed the next time a signature is performed. This also provide the verifier with a proof that the service was granted.
  No secret information is revealed during transactions; when x_{m-1} is revealed it may be public.

3.5 Applications

3.5.1 Pre-payment Cards

One type of application leads to the following setting : there is one credential center which is the only one verifier. That means practically that any seller can manage his own payment system allowing his clients to use prepaid cards to buy food, things or services (including computer network services).

When the credential center is also the only one verifier, it may fix an appropriate lifetime to individual signature, *i.e.* it may allow replays of a signature for a fixed period of time or a fixed number of occurrences.

A similar or derived application may allow several verifiers to be connected to the same credential center : prepaid cards for parking in private areas, or prepaid access to services.

3.5.2 Electronic Cash

Another application deals with the possibility to withdraw money thanks to banking cards. A banking card could be loaded at a bank counter with the equivalent of a fixed number of bank notes. This loading operation could occur regularly or only a single time on the same card. The physical bank notes could then be withdrawn at any ATM in connection with the bank (even abroad). A practical application could be a (nice) alternative to traveller's checks.

3.5.3 Pay-TV

Another type of implementation may be achieved by means of an hierarchization of the management performed by the credential center. The setting is as follows : One main application center, say a cable TV organization, is the only authority able to load smart cards [8] with (x_k, x_0) secret pairs related to one particular (set of) user(s) and the user's decoder. The decoder plays both the role of the verifier and of the public directory manager described in our scheme.

Only a particular set of users are allowed to use a particular decoder. This set may be distinguished from the others by using a special class of redundancy in I^* identity strings.

Or in an original setting, the decoder sends request to the main application center which manages the public directory and delegation allows any card user to use any decoder.

4 Conclusion

We outlined a signature scheme which limits the right of the signer to produce acknowledged signatures. It is based on the Guillou-Quisquater zero-knowledge proof and Lamport authentication scheme. It is practical and flexible. Our scheme allows delegation and refreshment is easy.

A trusted center initializes the system and will not take part any more other than as a judge to settle eventual conflicts.

A credential center issues each signer with a different and unique (not already used) set of k bounded life-span secrets which are to be used to produce signatures. This center manages the bounded life-span property of the signature scheme.

Actually the credential center is **not** an authority or a trusted center in the sense that he does not (need to) know the factorization of the modulus n.

The credential center (and the sub-center or delegator in a delegation scheme) is able to revoke "licenses", signature power, the ability to sign of a user, once granted.

5 Acknowledgments

We would like to thank Mike V. D. Burmester for discussions and comments about this work.

[8] Multi-applications smart cards.

References

[ABKL93] M. Abadi, M. Burrows, C. Kaufman and B. Lampson. Authentication and delegation with smart cards. *Science of Computer Programming*, N ° 21, pp. 93–113, Elsevier, 1993.

[BM88] M. Bellare and S. Micali. How to sign given any trapdoor function. *Proceedings of the 20^{th} Symposium on Theory of Computing, STOC'90*, pp. 427–437.

[Bu93] M. V. D. Burmester. Recent developments in efficient Zero-Knowledge proofs. *Talk given at the Université Catholique de Louvain*, June 1993.

[BCDP91] J. Boyar, D. Chaum, I. Damgard and T. Pedersen. Convertible Undeniable Signatures. *Advances in cryptology, Proceedings of CRYPTO '90, Lecture Notes in Computer Science*, N° 537, pp. 189–205, Springer-Verlag, 1991.

[BD89] M. V. D. Burmester and Y. G. Desmedt. Remarks on Soundness of Proofs. *Electronic letters*, pp. 1509–1510, Vol. 25, N ° 22, 26th October 1989.

[BGKW88] M. Ben-Or, S. Goldwasser, J. Killian and A. Wigderson. Multi-prover interactive proofs : How to remove intractability assumptions. *Proceedings of the twentieth annual ACM Symp. Theory of Computing, STOC'88*, pp. 113–131, May 2–4, 1988.

[CP94] G. do Crescenzo and G. Persiano. Round-optimal perfect zero-knowledge proofs. *Information Processing Letters*, pp. 93–99, Vol. 50, N ° 2, 22 April 1994.

[CvA90] D. Chaum and H. van Antwerpen. Undeniable Signatures. *Advances in cryptology, Proceedings of CRYPTO '89, Lecture Notes in Computer Science*, N ° 435, pp. 212–216, Springer-Verlag, 1990.

[DF92] Y. Desmedt and Y. Frankel. Shared Generation of Authenticators and Signatures. *Advances in cryptology, Proceedings of CRYPTO '91, Lecture Notes in Computer Science*, N ° 576, pp. 457–469, Springer-Verlag, 1992.

[DH76] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, Vol. IT-22, N° 6, pp. 644–654, 1976.

[DQ94] O. Delos and J.-J. Quisquater. Efficient multi-signature schemes for cooperating entities. *Proceedings of French-Israeli Workshop on Algebraic Coding, Lecture Notes in Computer Science*, N° 781, pp. 63–74 , Springer-Verlag, 1994.

[DQ] O. Delos and J.-J. Quisquater. Biauthentication and secret message transmission. *Manuscript UCL 1994.*

[dWQ90] D. de Waleffe and J.-J. Quisquater. Better login protocols for computer networks. *Proceedings of ESORICS '90*, pp. 163–172, October 1990.

[FFS88] U. Feige, A. Fiat and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2), pp. 77–94, 1988.

[GDQ89] L. C. Guillou, M. Davio and J.-J. Quisquater Public-key techniques: Randomness and Redundancy. *Cryptologia*, Vol. 13, N° 2, pp. 167–189, April 1989.

[GK89] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. Technical Report N° 570 of Technion, 1989.

[GMR88] S. Goldwasser, S. Micali and R. Rivest. A digital signature scheme secure against adaptative chosen-message attacks. *Siam J. Comput.*, 1988, Vol. 17, pp. 281–308.

[GMRa89] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *Siam J. Comput.*, 1989, Vol. 18, N° 1, pp. 186–208.

[GQ88a] L. C. Guillou and J.-J. Quisquater. Efficient digital public-key signatures with shadow. *Advances in cryptology, Proceedings of CRYPTO '87, Lecture Notes in Computer Science*, N° 304, p. 223, Springer-Verlag, 1988.

[GQ89a] L.C. Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In C. G. Günther, editor, *Advances in Cryptology, Proceedings of EUROCRYPT '88, Lecture Notes in Computer Science*, N° 330, pp. 123–128, Springer-Verlag, 1988.

[GQ89b] L.C. Guillou and J.-J. Quisquater. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. *Advances in Cryptology, Proceedings of CRYPTO '88, Lecture Notes in Computer Science*, N ° 403, pp. 216–231, Springer-Verlag, 1989.

[GUQ91] L. C. Guillou, M. Ugon and J.-J. Quisquater. The Smart Card: A Standardized Security Device Dedicated to Public Cryptology. *Contemporary Cryptology : The Science Information Integrity*, edited by G. J. Simmons, IEEE Press, 1991.

[HS91] S. Haber and W.S. Stornetta. How to Time-Stamp a Digital Document. *Advances in Cryptology, Proceedings of CRYPTO '90, Lecture Notes in Computer Science*, N ° 537, pp. 437–455, Springer-Verlag, 1991.

[L81] L. Lamport. Password Authentication With Insecure Communication. *Comm. of ACM*, Vol. 24, N° 11, pp. 770–772, Nov. 1981.

[McC90] K. Mc Curley. Odd and ends from cryptology and computational number theory. *Cryptology and computational number theory*, edited by C. Pomerance, AMS short course, pp. 145–166, 1990.

[Mer79] R. C. Merkle. A Certified Digital Signature. *Advances in Cryptology, Proceedings of CRYPTO '89, Lecture Notes in Computer Science*, N ° 435, pp. 218–238, Springer-Verlag, 1989.

[NY89] M. Naor and M. Yung. Universal One-way Hash Functions and their Cryptographic Applications. *Proceedings of the 21 st Symposium on Theory of Computing, STOC'89*, pp. 33-43, 1989.

[Q87] J.-J. Quisquater. Secret distribution of keys for public-key system. *Advances in cryptology, Proceedings of CRYPTO '87, Lecture Notes in Computer Science*, N ° 293, pp. 203–208, Springer-Verlag, 1987.

[R80] M. O. Rabin. Probabilistic algorithms for testing primality. *Journal on Number Theory*, Vol. 12, pp. 128–138, 1980.

[Sh85] A. Shamir. Identity-based cryptosystems and signatures schemes. *Advances in cryptology, Proceedings of CRYPTO '84, Lecture Notes in Computer Science*, N ° 196, pp. 47–53, Springer-Verlag, 1985.

[SRA81] A. Shamir, R. Rivest and L. Adleman. Mental Poker. *The Mathematical Gardner*, edited by D. A. Klarner, Wadsworth International, 1981.

[Vau93] S. Vaudenay. Mémoire de Magistère de Mathématiques Fondamentales et Appliquées et d'Informatique. GRECC, Laboratoire d'Informatique de l'Ecole Normale Supérieure, Paris, 1993.

[vH92] E. van Heijst. Special Signature Schemes. Thesis for the degree of Doctor at the Eindhoven University of Technology (The Netherlands), July 1992.

[WP90] M. Waidner and B. Pfitzmann. The Dining Cryptographers in the Disco : Unconditional Sender and Recipient Untraceability with computationally Secure Serviceability. *Advances in cryptology, Proceedings of EUROCRYPT '89, Lecture Notes in Computer Science*, N ° 434, p.690, Springer-Verlag, 1990.