On the Efficiency of Group Signatures Providing Information-Theoretic Anonymity

Lidong Chen[1] and Torben P. Pedersen[2]

[1] Mathematics Department, Texas A & M University, College Station, TX 77843 – 3368, USA, email: Lily.Chen@math.tamu.edu***

[2] Department of Comp. Sci., Aarhus University, Ny Munkegade, DK-8000 Århus C, Denmark, email: tppedersen@daimi.aau.dk†

Abstract. Group signatures, introduced by Chaum and van Heijst at Eurocrypt'91, allow members of a group to make signatures on behalf of the group while remaining anonymous. Furthermore, in case of disputes a designated group authority, who is given some auxiliary information, can identify the signer. Chaum and van Heijst presented four schemes, one of which protects the anonymity of the signer information-theoretically. However, this scheme as well as subsequent schemes with this property requires that the signer basically needs a new secret key for each signature and that the group authority secretly stores a very long string.

This paper analyses such group signature schemes and obtains lower bounds on the length of both the secret keys of the group members and the auxiliary information of the authority depending on the number of signatures each is allowed to make and the number of group members. These bounds are optimal as they are met by the scheme suggested by Chaum and van Heijst.

1 Introduction

Group signatures, introduced in [CH91], allow members of a group (e.g. a company or family) to make signatures on behalf of the group in such a way that

- only members can make signatures, and
- the actual member who made a given signature remains anonymous except that
- in case of dispute a designated authority (who is given some extra information) can identify the signer.

Such a signature scheme can, for example, be used in invitations to submit tenders. All companies submitting a tender then form a group and each company signs its tender anonymously using the group signature. Later, when the preferred tender has been selected, the winner can be identified, whereas the signers of all other tenders will remain anonymous. All submitters are bound to their tender by the signature, as the signer can be identified without his cooperation.

*** Work done while visiting Aarhus University

† Supported by Carlsbergfondet

L.C. Guillou and J.-J. Quisquater (Eds.): Advances in Cryptology - EUROCRYPT '95, LNCS 921, pp. 39-49, 1995.

1.1 Related Work

Group signatures should not be confused with the related notion of group oriented signatures first suggested in [Boy89b] and [CH89]. Here certain subsets of a group of people are allowed to sign on behalf of the group. Such schemes do not provide a method for identifying the (subset of the) members who actually made the signature (see [D93] for an overview). Another related concept is that of multi-signatures which require a digital signature from many persons (see [O88] and [OO93]).

Chaum and van Heijst present in [CH91] (see also [H92]) four group signature schemes: one protects the anonymity of the signer unconditionally, whereas the other three only give computational anonymity. The scheme giving information-theoretic anonymity is very simple and works as follows given any digital signature scheme. Each member chooses a pair of keys for the signature scheme and sends the public key secretly to the authority. When the authority has received all public keys, it forms the public key of the group as a list of all the individual public keys in random order. Each member can now sign a message using the secret key. The receiver verifies that the signature is valid with respect to one of the keys in the public key of the group. Only the authority, who knows the correspondence between public keys and group members, will be able to identify the originator of a given signature.

A serious drawback of this scheme is that if a member wants to sign many messages he needs a new key pair for each message (otherwise the signatures can be linked). The secret key of each group member, the auxiliary information and the public key of the group therefore get longer the more signatures a member is allowed to make. Other disadvantages are

- Each member, P, is only protected against framing (i.e., other persons making a signature for which the authority will identify P as the signer) under a cryptographic assumption. This problem can be remedied by replacing the digital signature scheme by unconditionally secure signatures (see [CR91]) or fail-stop signatures (see [WP90]).
- If a new person wants to be a member, all other members must select a new key-pair. Otherwise, it is easy to identify the public key of the new member. This problem has been solved in [CP94a].

A scheme solving both of these problems, while retaining unconditional anonymity is presented in [CP94b].

1.2 Results and Contents

Although, the scheme of Chaum and van Heijst has been improved in some ways, it has not been possible to construct a scheme which is more efficient in terms of the length of secret keys and auxiliary information. This paper explains that lack of efficiency by giving lower bounds on the sizes of these (see Section 3). These bounds say that the length of the secret key of each member grows as $T \log_2 n$, if each member can make T signatures and n is the number of members. Similarly, the length of the auxiliary information of the authority grows as $Tn \log_2 n$.

In order to obtain these lower bounds a definition of group signatures with information-theoretic anonymity is needed. This is given in Section 2.

2 Definitions

This section defines secure group signatures giving information-theoretic anonymity. Throughout this paper $\mathcal{M}$ denotes the message space.

As computational model we use Turing machines and interactive Turning machines as defined in [GMR89]. In protocols (specifically, in *gen* in Definition 1 below) it is assumed that each pair of participants can send secret messages to each other.

Definition 1. A group signature scheme for a group of n members $P_1, \ldots, P_n$ and an authority A is a tuple $(n, k, gen, sign, test, iden)$. Here k is the security parameter, *gen* is a protocol involving $n+1$ polynomially bounded participants and *sign*, *test*, *iden* are all polynomial time (in k) algorithms.

- On secret inputs (k, n, ρ_0) from A and ρ_i from P_i, $(i = 1, 2, \ldots, n)$, where each of $\rho_0, \rho_1, \ldots, \rho_n$ is a random bit-string, *gen* produces a common output, *pk*, secret output *aux* to A and secret output s_i to each P_i. Here, *pk* is the public key of the group, s_i is the secret key of P_i $(i = 1, 2, \ldots, n)$ and *aux* is the auxiliary information for A.
- *sign* is a *probabilistic* algorithm which on input s_i and $m \in \mathcal{M}$ outputs $sign(s_i, m)$. A string $\sigma \in \{0,1\}^*$ is called a *correct signature* on $m \in \mathcal{M}$, if there exists $i \in \{1, 2, \ldots, n\}$ such that $\sigma = sign(s_i, m)$.
- *test* is used to test signatures. On input *pk*, m, and a possible signature on m, it outputs *true* or *false*. A string σ is called an *acceptable signature* on m with respect to *pk* if $test(pk, m, \sigma) = true$.
- *iden* is used by A to identify the signer. On input *aux*, $m \in \mathcal{M}$ and an acceptable signature on m, it outputs $i \in \{1, 2, \ldots, n\} \cup \{?\}$ (the output ? indicates that *iden* could not identify the signer).

For any $i \in \{1, 2, \ldots, n\}$, and any $m \in \mathcal{M}$, the scheme must satisfy

$$test(pk, m, sign(s_i, m)) = true \qquad (1)$$

and

$$iden(aux, m, sign(s_i, m)) = i \qquad (2)$$

Remark. From (2) it immediately follows that different secret keys produce different signatures:

$$\forall i, j \in \{1, 2, \ldots, n\}\, \forall m \in \mathcal{M} : i \neq j \Rightarrow sign(s_i, m) \neq sign(s_j, m).$$

Remark. From (1) it follows that a correct signature is also acceptable (but an acceptable signature is not necessarily correct).

According to the informal description in the introduction a group signature scheme must

- be secure against forgeries;
- provide anonymity of the signer; and
- enable the authority to identify the signer.

Each of these properties will be defined in the following.

2.1 Security Against Forgeries

It must be infeasible to forge signatures in adaptively chosen message attacks (see [GMR88]). Let $\mathcal{F}$ be a polynomial time algorithm, which on input pk and possibly aux, works as follows.

1. Repeat the following:
   (a) Generate a message $m \in \mathcal{M}$ and $i \in \{1, 2, \ldots, n\}$;
   (b) Get $sign(s_i, m)$.
2. Output a message $m_0 \in \mathcal{M}$ different from all m's generated above and $\tilde{\sigma}(m_0)$.

Definition 2. Let a group signature scheme $(n, k, gen, sign, test, iden)$ and T, polynomial in k, be given. The scheme is *secure against forgeries* after signing T messages if the following holds: For any polynomial time $\mathcal{F}$ as above getting at most T signatures from each P_i, for all but a negligible fraction of the keys (distributed according to gen),

$$\begin{gathered}\forall c > 0, \exists k_0, \forall k > k_0 \\ Prob[test(pk, m_0, \tilde{\sigma}(m_0)) = true] \leq k^{-c},\end{gathered}$$

where $(m_0, \tilde{\sigma}(m_0))$ is the output of $\mathcal{F}$. The probability is over the random coins of signatures and the random coins of $\mathcal{F}$.

2.2 Anonymity

Every group member should be able to make signatures on behalf of the group without leaking any (Shannon) information about his identity — only the group authority must be able to link signatures to members. Thus in the definition of anonymity, the authority can be trusted, but some group members may try to identify other members. As we are interested in information-theoretic anonymity, these curious members may have unlimited computing power.

Let a non-empty subset $J \subseteq \{1, 2, \ldots, n\}$ be given. The members in J are assumed to be honest, but the members outside J may deviate from the prescribed methods (no assumption about computing power) — these members are denoted by $\tilde{P}_j$ for $j \notin J$. Consider an execution of gen by A, $(P_j)_{j \in J}$ and $(\tilde{P})_{j \notin J}$, and assume that this protocol ends with a public key, pk, of the group and secret keys sk_j of P_j for $j \in J$ (otherwise the group is not set up properly). Let $view_J$ denote the view (including pk) of the faulty participants (see [GMR89]), and let $SK(view_J)$ denote the set of possible secret keys of $(P_j)_{j \in J}$ given this view. This set is equipped with a distribution induced from the random coins of the authority and $(P_j)_{j \in J}$. In the following let $J = \{a_1, a_2, \ldots, a_{|J|}\}$. Then $SK(view_J)$ is a set of tuples $(sk_{a_1}, sk_{a_2}, \ldots, sk_{a_{|J|}})$.

For all positive integers t and L, $0 < L \leq |J|t$, define a subset of $J^L = J \times J \times \ldots \times J$ (L times) by

$$\mathcal{I}_J(t, L) = \{(i_1, \ldots, i_L) \in J^L \mid \forall j \in J : |\{l \in \{1, \ldots, L\} \mid i_l = j\}| \leq t\}.$$

Thus each $j \in J$ appears at most t times in $\underline{i} = (i_1, \ldots, i_L) \in \mathcal{I}_J(t, L)$. For $J = \{1, 2, \ldots, n\}$, $\mathcal{I}_J(t, L)$ will be denoted $\mathcal{I}(t, L)$.

If $\sigma(m_i)$ is a correct signature on $m_i \in \mathcal{M}$ for $i = 1, \ldots, L$, then $\sigma(\underline{m})$ denotes $(\sigma(m_1), \sigma(m_2), \ldots, \sigma(m_L))$. For every $\underline{i} \in \mathcal{I}_J(t, L)$, "$\sigma(\underline{m}) \Leftarrow \underline{i}$" denotes the event that there exists $(sk_{a_1}, sk_{a_2}, \ldots, sk_{a_{|J|}}) \in SK(view_J)$ such that for all $j \in \{1, 2, \ldots, L\}$:

$$sign(sk_{i_j}, m_j) = \sigma(m_j).$$

Definition 3. Let a group signature scheme $(n, k, gen, sign, test, iden)$ and T, polynomial in k, be given. The scheme provides *anonymity* for signing T messages if for any non-empty $J \subseteq \{1, 2, \ldots, n\}$ and any $\tilde{P}_{j \notin J}$ in the scenario described above, and for any $L \leq |J|T$ different messages

$$\underline{m} = (m_1, m_2, \ldots, m_L)$$

the following holds. Given correct signatures on these messages made by $(P_j)_{j \in J}$

$$\sigma(\underline{m}) = (\sigma(m_1), \sigma(m_2), \ldots, \sigma(m_L)),$$

where each P_j has made at most T signatures, then for any $\underline{i} \in \mathcal{I}_J(T, L)$,

$$Prob[\sigma(\underline{m}) \Leftarrow \underline{i}] = \frac{1}{|\mathcal{I}_J(T, L)|}.$$

The probability is over the choice of $(sk_{a_1}, sk_{a_2}, \ldots, sk_{a_{|J|}}) \in SK(view_J)$ and the random coins used in the signatures.

This definition can be generalised to allow the same message to be signed several times. However, we have chosen this definition as messages in practice will be unique (e.g., contain a time stamp) in order to prevent replay attacks.

2.3 Signer Identification

For any subset J of $\{1, 2, \ldots, n\}$, let $\mathcal{F}_J$ be a polynomial time algorithm, which works as follows:

1. Execute *gen* — the members not in J may deviate from the prescribed protocol.
2. Repeat the following:
   (a) Generate a message $m \in \mathcal{M}$, and a number $i \in J$;
   (b) Get $sign(s_i, m)$.
3. Output a message $m_0 \in \mathcal{M}$ different from all m's in 2 and an acceptable signature $\sigma(m_0)$ on m_0.

Definition 4. Let a group signature scheme $(n, k, gen, sign, test, iden)$ and T, polynomial in k, be given. The scheme provides ***signer identification*** for signing T messages if the following holds: For any subset J of $\{1, 2, \ldots, n\}$, and for any polynomial time algorithm $\mathcal{F}_J$ as above getting at most T signatures from each P_i $(i \in J)$,

$$\forall d > 0, \exists k_0, \forall k > k_0$$
$$Prob[iden(aux, m_0, \sigma(m_0)) \in \{1, 2, \ldots, n\} \setminus J] \geq 1 - k^{-d},$$

where $(m_0, \sigma(m_0))$ is the output of $\mathcal{F}_J$. The probability is over the random coins of $\mathcal{F}_J$, and the random coins used in *gen* and *sign*.

There are two aspects of this definition. Firstly, if $|J| = n - 1$ the signer must be identified by the authority with overwhelming probability. Secondly, it says that no subset of (polynomially bounded) group members can frame a member outside this subset.

Remark. If the dishonest members (i.e., those outside J) are allowed unlimited computing power, this definition gives unconditional security against framing.

2.4 Secure Group Signatures

The preceding three definitions give

Definition 5. A group signature scheme is *secure* for signing T messages, if it is secure against forgery and provides both anonymity and signer identification after each member has made at most T signatures.

Remark. The definition easily generalises to let P_i sign T_i messages, $i = 1, 2, \ldots, n$.

3 Lower Bounds

Based on the definition given above this section shows that the length of the secret keys and auxiliary information grows by the number of signatures and group members. In the following it is assumed that all members and the authority participates honestly when generating the keys, since we want to give lower bounds on correct keys.

3.1 Secret Keys

The main idea in the proof of the lower bound of the secret keys is to partition the set of possible secret keys of each member into nonempty, disjoint subsets. Then the number of possible secret keys is bounded by the number of subsets.

A public key pk, produced by gen, corresponds to a set of possible secret keys defined as

$$\begin{aligned} SK(pk) = \{(sk_1, sk_2, \dots, sk_n) \mid \exists aux, \rho_0, \rho_1, \dots, \rho_n : \\ gen(n, k, \rho_0, \rho_1, \dots, \rho_n) = (pk, (sk_1, sk_2, \dots, sk_n), aux)\}. \end{aligned}$$

We will omit pk in the following. The set $SK^{(i)}$ is defined as all possible secret keys of P_i, $i = 1, 2, \dots, n$, i.e. $SK^{(i)}$ is the projection of SK on the i'th coordinate. If $s_i \in SK^{(i)}$ denotes the actual secret key of P_i, then

$$(s_1, s_2, \dots, s_n) \in SK.$$

For a t-tuple $\underline{i} = (i_1, i_2, \dots, i_t) \in \{1, 2, \dots, n\}^t$ and t different messages $\underline{m} = (m_1, m_2, \dots, m_t)$ define for every $r, 1 \leq r \leq n$

$$SK_{\underline{i}}^{(r)}(\underline{m}) = \{sk \in SK^{(r)} | sign(sk, m_j) = sign(s_{i_j}, m_j), j = 1, 2, \dots, t\},$$

where s_i is the secret key of P_i ($i = 1, 2, \dots, n$). $SK_{\underline{i}}^{(r)}(\underline{m})$ is the set of possible keys of P_r which will give P_{i_j}'s signature on m_j for $j = 1, 2, \dots, t$.

Lemma 6. *If a group signature scheme $(n, k, gen, sign, test, iden)$ provides anonymity for signing T messages, then for any $t \leq T$, the following holds: For all $\underline{i} = (i_1, i_2, \dots, i_t)$, and any t different messages $\underline{m} = (m_1, m_2, \dots, m_t)$,*

$$SK_{\underline{i}}^{(r)}(\underline{m}) \neq \emptyset \qquad \textit{for } r = 1, 2, \dots, n.$$

Proof. Assume there exist $t \leq T$ different messages $\underline{m} = (m_1, \dots, m_t)$, and $\underline{i} = (i_1, i_2, \dots, i_t)$, such that

$$SK_{\underline{i}}^{(r_0)}(\underline{m}) = \emptyset,$$

for some r_0. Let $\sigma(m_j) = sign(s_{i_j}, m_j)$, $j = 1, 2, \dots, t$ and $\underline{i}_0 = (r_0, r_0, \dots, r_0)$. Then

$$Prob[\sigma(\underline{m}) \Leftarrow \underline{i}_0] = 0,$$

which contradicts the definition of anonymity. □

Theorem 7. *Let a group signature scheme $(n, k, gen, sign, test, iden)$ be given. If it provides anonymity for signing T messages, then for any $r \in \{1, 2, \dots, n\}$,*

$$|SK^{(r)}| \geq n^T.$$

Proof. First, for any $t \leq T$ different messages $\underline{m} = (m_1, m_2, \ldots, m_t)$, if

$$\underline{i} = (i_1, i_2, \ldots, i_t) \neq (i'_1, i'_2, \ldots, i'_t) = \underline{i}',$$

then

$$SK^{(r)}_{\underline{i}}(\underline{m}) \cap SK^{(r)}_{\underline{i}'}(\underline{m}) = \emptyset.$$

Otherwise there exists

$$sk \in SK^{(r)}_{\underline{i}}(\underline{m}) \cap SK^{(r)}_{\underline{i}'}(\underline{m}),$$

such that for some $j \in \{1, 2, \ldots, n\}$, $i_j \neq i'_j$,

$$sign(sk, m_j) = sign(s_{i_j}, m_j) \quad \text{and} \quad sign(sk, m_j) = sign(s_{i'_j}, m_j),$$

which contradicts Definition 1 (see the remark following that definition).

Second, by Lemma 6, for any t different messages $\underline{m} = (m_1, \ldots, m_t)$, and any t-tuple $\underline{i} = (i_1, i_2, \ldots, i_t) \in \{1, 2, \ldots, n\}^t$,

$$|SK^{(r)}_{\underline{i}}(\underline{m})| \geq 1.$$

Finally, for any t different messages $\underline{m} = (m_1, m_2, \ldots, m_t)$

$$|SK^{(r)}| \geq \sum_{\underline{i} \in \{1,2,\ldots,n\}^t} |SK^{(r)}_{\underline{i}}(\underline{m})| \geq n^t,$$

for any $t \leq T$. □

Thus each member must have a secret key chosen from a set of at least n^T possible secret keys. In other words, at least $T \log n$ bits are needed to represent some of the secret keys of each group member. Thus, the length of secret keys grows linearly in the number of signatures.

3.2 Auxiliary Information

In this section, we consider the length of the auxiliary information held by the authority. Let $(n, k, gen, sign, test, iden)$, T and an integer L, $0 < L \leq nT$ be given. Consider the following experiment given L different messages $m_1, m_2, \ldots, m_L$:

1. Generate $(pk, (s_1, \ldots, s_n), aux)$ correctly using gen.
2. Choose $(i_1, i_2, \ldots, i_L) \in \mathcal{I}(T, L)$ uniformly at random.
3. Let an (L, T)-history $hist_L(\underline{m}) = (pk, (m_1, \sigma_1), \ldots, (m_L, \sigma_L))$ be defined by

$$\sigma_j = sign(s_{i_j}, m_j) \qquad \text{for } j = 1, \ldots, L.$$

Let AUX be the random variable of the authority's auxiliary information (defined on the probability space induced by gen). Let ID be the uniformly distributed random variable taking the value $(i_1, i_2, \ldots, i_L) \in \mathcal{I}(T, L)$.

The following lemma follows immediately from the definition of unconditional anonymity.

Lemma 8. *If the group signature scheme $(n, k, gen, sign, test, iden)$ provides anonymity for signing T messages, then for any (L,T)-history $hist_L(\underline{m})$, ID is uniformly distributed on $\mathcal{I}(T, L)$. Especially, the conditional entropy of ID given $hist_L(\underline{m})$ is*

$$H(ID \mid hist_L(\underline{m})) = \log_2 |\mathcal{I}(T, L)| = \log_2 \left(\frac{(Tn)!}{(T!)^n}\right).$$

Theorem 9. *If the group signature scheme $(n, k, gen, sign, test, iden)$ provides anonymity for signing T messages and signer identification, then*

$$H(AUX) \geq Tn(\log n - 1).$$

Proof. Let $L = Tn$, and consider an (L,T)-history, $h = hist_L(\underline{m})$. The entropy of AUX can be written

$$\begin{aligned} H(AUX) &\geq H(AUX \mid h) \\ &= H(AUX, ID \mid h) - H(ID \mid AUX, h) \\ &= H(AUX|ID, h) + H(ID \mid h) - H(ID|AUX, h). \end{aligned}$$

Requirement (2) of Definition 1 implies that $H(ID|AUX, h) = 0$ and thus

$$H(AUX) \geq H(ID \mid h) + H(AUX|ID, h) \geq H(ID \mid h).$$

From the lemma above,

$$H(ID \mid h) = \log \frac{(Tn)!}{(T!)^n}.$$

Stirlings Formula

$$n! \approx e^{-n} n^n \sqrt{2\pi n}$$

gives

$$\log \frac{(Tn)!}{(T!)^n} \approx Tn \log n + \log \sqrt{2\pi Tn} - n \log \sqrt{2\pi T} \geq Tn(\log n - 1).$$

This completes the proof. □

This bound can be interpreted as follows. The authority needs some information corresponding to each signature that each member is allowed to make — in total nT pieces. Each of these must be unique for the member — this requires $\log n$ bits.

3.3 Comparison with Upper Bound

In the construction of Chaum and van Heijst the length of the auxiliary information is

$$\log\left(\frac{(Tn)!}{(T!)^n}\right).$$

This is exactly the bound which was obtained above.

Furthermore, if a secret key of the digital signature scheme used in this construction requires K bits then the length of the secret key of each member is KT bits. This should be compared with the bound $T\log_2 n$. Since all secret keys must be different, $K \geq \log_2 n$. Thus, except for the length of the secret keys of the given digital signature scheme (which we have only bounded by $\log_2 n$) the upper and lower bounds meet.

4 Conclusion

A detailed definition of group signatures with information-theoretic anonymity has been given, and it has been shown that in such schemes the length of the secret keys and the auxiliary information grows linearly in the number of signatures. These bounds only require anonymity and that the authority can identify signers of correct signatures, but the definitions of security against forgery and signer identification are not used.

On the one hand these bounds say that the scheme of Chaum and van Heijst is optimal, on the other they imply that such group signature schemes have some limits which might make them less attractive in some applications.

Some group signature schemes offering only computational anonymity have been suggested (e.g., see [CH91] and [CP94a]), but it is still an open problem to construct efficient such schemes, which can be proved secure under a "common cryptographic assumption".

References

[Boy89b] C. Boyd. Digital Multisignatures. In *Cryptography and Coding*, pages 241 – 246, 1989.

[CH91] D. Chaum and E. van Heijst. Group Signatures. In *Advances in Cryptology - proceedings of EUROCRYPT 91*, Lecture Notes in Computer Science #547, pages 257-265. Springer-Verlag, 1991.

[CR91] D. Chaum and S. Roijakkers Unconditionally Secure Digital Signatures In *Advances in Cryptology - proceedings of CRYPTO 90.* Lecture Notes in Computer Science #537, pages 206–214, 1991.

[CP94a] L. Chen and T. P. Pedersen New Group Signature Schemes. In *Advances in Cryptology - Proceedings of Eurocrypt '94.*

[CP94b] L. Chen and T.P. Pedersen. Group Signatures: Unconditional Security for Members. Technical Report DAIMI PB – 481, Aarhus University, September 1994.

[CH89] R. A. Croft and S. P. Harris. Public-Key Cryptography and Reusable Shared Secrets. In *Cryptography and Coding*, pages 189 – 201, 1989.

[D93] Y. Desmedt. Threshold Cryptosystems. In *Advances in Cryptology - proceedings of AUSCRYPT 92*, Lecture Notes in Computer Science #718, pages 3–14, 1993.

[GMR88] S. Goldwasser, S. Micali, and R. L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen Message Attack. *SIAM Journal on Computing*, 17(2):281 - 308, April 1988.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof-Systems. *SIAM Journal of Computation*, 18(1):186–208, 1989.

[H92] E. van Heijst. *Special Signature Schemes*. PhD thesis, CWI, 1992.

[O88] T. Okamoto. A Digital Multisignature Scheme Using Bijective Public-Key Cryptosystems. *ACM Trans. on Comp. Sys.*, 6(8):432 – 441, 1988.

[OO93] K. Ohta and T. Okamoto. A Digital Multisignature Scheme Based on the Fiat-Shamir Scheme. In *Advances in Cryptology - proceedings of ASIACRYPT 91*, Lecture Notes in Computer Science #739, pages 139 – 148. Springer-Verlag, 1993.

[WP90] M. Waidner and B. Pfitzmann. The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability In *Advances in Cryptology - proceedings of Eurocrypt 89*. Lecture Notes in Computer Science #434, page 690, 1990.