On Partial Anonymity in Secret Sharing

Vanesa Daza and Josep Domingo-Ferrer

Rovira i Virgili University
UNESCO Chair in Data Privacy
Department of Computer Engineering and Mathematics
Av. Països Catalans, 26, E-43007 Tarragona, Catalonia
{vanesa.daza,josep.domingo}@urv.cat

Abstract. Anonymous secret sharing schemes allow a secret to be recovered from shares regardless of the identity of shareholders. Besides being interesting in its own right, this property is especially appealing to guarantee the anonymity of participants when secret sharing is used as a building block of more general distributed protocols (*e.g.* to anonymously share the secret key corresponding to a public key). However, current constructions of anonymous secret sharing schemes are not very efficient (because of the number of shares that every participant must hold) and existing bounds do not leave much room for optimism. In this paper we propose to weaken the anonymity condition to partial anonymity, where by partial anonymity we mean that the identity of the participant is not made public, but he is known to belong to some subset. That is, the search for a participant narrows down to one in a set of possible candidates. Furthermore, we propose a general construction of partial anonymous secret sharing schemes.

Keywords: Privacy, Protocols, Secret sharing.

1 Introduction

Anonymous secret sharing schemes allow a secret to be recovered from a set of shares without knowledge of which participants hold which shares. That is, in such schemes the computation of the secret can be carried out regardless the identities of shareholders. Beyond its intrinsic interest, anonymous secret sharing is particularly attractive to guarantee the anonymity of participants in more general distributed protocols. A typical application is anonymous sharing of the secret key corresponding to a certain public key. Unfortunately, the constructions of anonymous secret sharing schemes in the literature are not very efficient (in terms of the number of shares that every participant must hold) and existing bounds [4,16] do not leave much hope for forthcoming efficient constructions.

Anonymous secret sharing schemes were introduced in 1988 by Stinson and Vanstone [22]. Phillips and Phillips [17] proved that only some specific access structures can yield anonymous secret sharing schemes where the size of the shares given to each participant is equal to the size of the secret (smallest possible size). Later on, Blundo and Stinson [4] gave general constructions of anonymous secret sharing schemes. They also gave lower bounds on the size of the set

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 193–202, 2007.

of shares (as a function of the size of the secret) both for threshold and non-threshold access structures. However, their constructions are not very efficient and their lower bounds preclude substantially improved forthcoming constructions. Since then, some authors have proposed constructions of anonymous secret sharing schemes, but either they are quite inefficient or they are restricted to the particular $(2, n)$ threshold case.

1.1 Contribution and Plan of This Paper

The lack of efficient constructions for anonymous secret sharing motivates us to weaken the anonymity condition in quest of efficiency, measured in terms of the number of shares that must be held by any participant. In that sense, we introduce the notion of partial anonymity with the aim of providing a tradeoff between the level of anonymity achieved by a scheme and its efficiency. Roughly speaking, in partial anonymous secret sharing the identity of the participant is not made public, but he is known to belong to some subset. In other words, the search for a participant narrows down to one in a set of possible candidates. This principle bears some vague resemblance to k-anonymity [18] used for privacy in databases and k-anonymity to preserve privacy in communication protocols [23,24]. On the practical side, we propose an efficient construction of a scheme fulfilling the partial anonymity property.

The rest of the paper is organized as follows. We introduce some basic concepts on secret sharing schemes in Section 2. In Section 3 we review the notion of anonymous secret sharing schemes and we introduce the notion of partially anonymous secret sharing schemes. In Section 4 we provide some constructions of partially anonymous secret sharing schemes. Finally, we conclude in Section 5.

2 Secret Sharing

Secret sharing schemes were independently introduced by Shamir [19] and Blakley [2] in 1979. A secret sharing scheme is a method whereby a special entity D, usually called dealer, distributes a secret s among a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n players. The dealer secretly sends to every player P_i his share s_i of the secret s in such a way that only authorized subsets can recover the secret whereas non-authorized subsets obtain no information on the secret s.

A basic principle when designing secret sharing schemes is to minimize the amount of secret material. Therefore, the length of the shares should be as small as possible. In a secret sharing scheme the length of any share of a participant is greater than or equal to the length of the secret. When they are equal, the scheme is called ideal.

The family Γ of the subsets of shares authorized to recover the secret is called access structure. Any access structure is assumed to be monotone, that is, any superset of an authorized subset is also an authorized subset. A particular case is an access structure formed by those sets of players with at least t players, that is,

$$\Gamma = \{A \subset \mathcal{P} \mid\mid A \mid \geq t\}$$

Parameter t is usually called *threshold* and the corresponding access structure is a (t, n) threshold access structure (or t-out-of-n threshold access structure).

Shamir's secret sharing scheme [19] realizes an ideal (t, n) threshold access structure by means of Lagrange polynomial interpolation. Indeed, let $\mathbb{Z}_q$ be a finite field with $q > n$ and $s \in \mathbb{Z}_q$ the secret to be shared. The dealer picks a polynomial $p(x)$ of degree at most $t-1$, with free term the secret s, that is $p(0) = s$. The polynomial $p(x)$ can be written as $p(x) = s + \sum_{j=1}^{t-1} a_j x^j$, where $a_j \in \mathbb{Z}_q$ has been randomly chosen.

Every player P_i is univocally assigned a value $\alpha_i \in \mathbb{Z}_q$. Then, D privately sends to player P_i his share $s_i = p(\alpha_i)$, for $i = 1, \ldots, n$.

In this way, a set $A \subset \mathcal{P}$ of at least t players can recover the secret $s = p(0)$ by interpolating the set of shares they hold:

$$p(0) = \sum_{P_i \in A} s_i \lambda_i^A = \sum_{P_i \in A} s_i \left(\prod_{P_j \in (A \setminus P_i)} \frac{-\alpha_j}{\alpha_i - \alpha_j} \right),$$

where λ_i^A are the Lagrange coefficients.

On the other hand, it is not difficult to prove that less than t players do not have any option better than random guessing to find out the secret.

For the particular case of (n, n)-threshold access structures ($\Gamma = \mathcal{P}$), that is, where all participants must jointly co-operate to recover the secret, more efficient constructions exist. They are not only ideal, but the dealer's computations are simpler. In [15], Karnin, Greene and Hellman proposed the following (n, n)-threshold secret sharing scheme. To share a secret s among a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n players, the dealer selects at random $s_i \in \mathbb{Z}_q$, for any player P_i, for $i = 1, \ldots, n-1$ and secretly sends s_i to participants P_i as his secret share. Then, D computes the share of the participant P_n as follows: $s_n = s - \sum_{i=1}^{n-1} s_i \in \mathbb{Z}_q$ and sends s_n to P_n. Note that when all participants join their shares, they recover the secret s by simply adding their shares in $\mathbb{Z}_q$.

Although threshold access structures have been extensively studied and used in the literature not only for secret sharing schemes (see, for example, [3,6]) but also for more general protocols (see, for example, [8,20,7]), they correspond to quite peculiar situations where all players play exactly the same role. On the contrary, what usually happens in real situations is that different players play different roles. For example, some players can have some restrictions and other some special privileges, or players can be divided into different categories depending on some properties. This leads to access structures more general than thresholds. Ito, Saito and Nishizeki [14] proved that for any monotone access structure there always exists a secret sharing scheme realizing it. The main drawback of their construction is that the size of shares is exponential in the number of parties in the access structure.

We describe next a general family of access structures that will be used in our proposal. It is the compartmented access structure, introduced by Simmons in [21]. There is a set of different compartments $C_1, \ldots, C_m$ in such a way that every participant is placed in a compartment, for some $i = 1, \ldots, m$. We

define $\psi : \{1, \ldots, n\} \rightarrow \{1, \ldots, m\}$ as the function assigning to each player P_i a compartment, denoted by $C_{\psi(i)}$. Then, given positive integers $t_1, \ldots, t_m$ and $t \geq \sum_{i=1}^{m} t_i$, the access structure consists of all subsets with at least t_i participants in C_i and a total of at least t participants. That is,

$$\Gamma = \{A \subset \mathcal{P} \mid\mid A \cap C_i \mid \geq t_i, \forall i = 1, \ldots, m \,, \mid A \mid \geq t\}.$$

Brickell [5] proved that there exist ideal secret sharing schemes realizing compartmented access structures. We review next the construction by [11], restricted to the particular case when $t = \sum_{i=1}^{m} t_i$. For the case $t > \sum_{i=1}^{m} t_i$, we refer the reader to [11,5].

The solution is based in Shamir's secret sharing schemes. The main idea is that the dealer shares a secret s by using an $(m-1)$-degree polynomial. Each compartment is related to a share of s. Then, to compute their share, at least t_i players in compartment C_i must join their shares. During the set-up phase, the dealer distributes the share of each compartment C_i among the players in the compartment by using a $(t_i, |C_i|)$-secret sharing scheme. Specifically D randomly selects an $(m-1)-$degree polynomial $P(x) \in \mathbb{Z}_q[x]$, such that $P(0) = s$. Let $s_i = P(\alpha_i)$, for $i = 1, \ldots, m$, where α_i is a public value associated with C_i. Then he distributes s_i among the players in compartment C_i using independent Shamir schemes. That is, he randomly selects a polynomial $F_i(x) \in \mathbb{Z}_q[x]$ of degree $t_i - 1$, for all $i = 1, \ldots, m$. Then, D secretly sends to every player P_i his share $F_{\psi(i)}(\beta_i)$, where β_i is the public value in $\mathbb{Z}_q$ associated to participant P_i.

Compartmented access structures are actually a special case of the more general multipartite access structure [13,9].

3 Anonymity and Partial Anonymity in Secret Sharing

Two kinds of anonymity in secret sharing are described in the literature. On the one hand, those schemes where shareholder identification is not required to successfully recover the secret, but the identity of the shareholder can be derived from the share. On the other hand, those schemes with the additional feature that players cannot be identified even when they show their shares. In other words, nobody can figure out the identity of a participant from the share he holds. The former category of schemes is usually called anonymous secret sharing (sometimes this anonymity is also referred to as submission anonymity). The latter category is usually called cryptographic anonymous secret sharing schemes [10,12]. The cryptographic notion of anonymity for secret sharing schemes is stronger than the submission notion. Some of the schemes satisfying submission anonymity do not offer cryptographic anonymity. This is because each share directly identifies the owner. In spite of this fact, submission anonymity in secret sharing remains especially interesting for example as a building block of some other distributed cryptographic protocols (*e.g.* distributed signature schemes). Then, when a participant publishes his partial information nobody is able to identify him because he does not directly publish his share but some information derived from it.

Several constructions have been published, both for submission anonymity [4,16,22] and for cryptographic anonymity [12]. However they are not very efficient and the most efficient ones have a small threshold ($t = 2$). Motivated by this fact, we introduce the concept of *partial anonymity* for secret sharing schemes. The main idea is to trade off anonymity and efficiency, by relaxing the anonymity condition to obtain more efficient schemes. This idea applies to both kinds of anonymity (submission and cryptographic) described before.

In order to define partial anonymity, we will lean on the definition of (t, n) anonymous threshold secret sharing in [1]. Let Σ be a (t, n) threshold secret sharing scheme on the set of participants $\mathcal{P} = \{P_1, \ldots, P_n\}$. For every secret s we note the set of shares as the vector $(s_1, \ldots, s_n)$, where s_i is the share (not necessarily a single value in $\mathbb{Z}_q$) held by player P_i.

Definition 1. *[Beimel-Franklin] A secret sharing scheme Σ realizing a (t, n) threshold access structure is said to be anonymous if, for every secret s, every vector of shares $(s_1, \ldots, s_n)$ and every permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$, the vector $(s_1, \ldots, s_n)$ is a vector of shares for the secret s if and only if the vector $(s_{\pi(1)}, \ldots, s_{\pi(n)})$ is a vector of shares for s.*

The above definition captures the idea that the reconstruction of the secret can be performed from the shares without knowing the identities of the parties holding those shares. That is, if a vector of shares is possible given a secret s, then every possible permutation in the order of the coordinates in this vector is possible given the secret s.

Note that this situation does not happen in Shamir's (t, n) threshold secret sharing scheme described in Section 2 whenever $1 < t < n$. Indeed, the Lagrange coefficients λ_i^A of a participant P_i depend on the set A to reconstruct the secret. However, when $t = n$, Shamir's scheme fulfills Definition 1 (and also Karnin, Greene and Hellman's scheme, see Section 2), although the identity of the participants arises implicitly from the access structure (as it is known that all participants take part in the protocol).

In Definition 1, a permutation is applied to the whole set of shares to guarantee anonymity of the shareholders. We do not propose to apply a permutation to the whole set of shares, but to divide the set of participants into different groups and to fulfill Definition 1 within each group to guarantee anonymity of a participant inside its group.

More specifically, let $G_1, \ldots, G_m \subset \mathcal{P}$ be subsets of participants in such a way that every participant P_i is placed in one and only one subset $G_1, \ldots, G_m$. Let $\psi : \{1, \ldots, n\} \to \{1, \ldots, m\}$ be the mapping that assigns each participant to a group, so that participant P_i will be placed in group $G_{\psi(i)}$. Let n_i be the cardinality of each set G_i and let t_i be a threshold assigned to set G_i, for all $i = 1, \ldots, m$. Then, we require that Definition 1 be satisfied for each of the sets G_i to guarantee that, locally, the participant is anonymous within his group and, globally, the only partial information that is obtained is that the participant is a member of a specific group.

Let Σ_i be a (t_i, n_i) secret sharing scheme for the set of participants in G_i. For every secret s we note the set of shares in Σ_i as the vector $(s^i_{j_1}, \ldots, s^i_{j_{n_i}})$, where s^i_j

is the share (not necessarily a single value in $\mathbb{Z}_q$) held by player P_j and we assume that the set of players in G_i is $P_{j_1}, \ldots, P_{j_{n_i}}$, where $\{j_1, \ldots, j_{n_i}\} \in \{1, \ldots, n\}$ for every j. Then, if at least t_i participants in G_i pool their shares, they can directly recover the secret s and the only information that is leaked is that they are participants in the set G_i.

However, it may be the case that the secret is not recoverable by players in each set G_i or maybe it is not desirable that members of a unique set can recover the secret. For example, in the former situation, to satisfy the secrecy condition, each threshold t_i must be at least t (a general threshold set related to the overall number of participants n) but the cardinality n_i of G_i may be smaller than t. A way to circumvent this problem of small sets is to require a threshold t_i for each set G_i in such a way that the sum of all the thresholds is at least t. In this way, the threshold t_i can be adapted to the size of G_i. Then, the resulting access structure is a $(G_1, \ldots, G_m)$ compartmented access structure (see Section 2 above).

Let Σ be a secret sharing scheme realizing a $(G_1, \ldots, G_m)$ compartmented access structure on the set of participants $\mathcal{P}$ with thresholds $t_1, \ldots, t_m, t = \sum_{i=1}^{m}$. For every secret s we note the set of shares as the vector $(s_1, \ldots, s_n)$, where s_i is the share (not necessarily a single value in $\mathbb{Z}_q$) held by player P_i. Then a $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme realizing a $(G_1, \ldots, G_m)$ compartmented access structure can be defined as follows:

Definition 2. *[Partial anonymous secret sharing] A secret sharing scheme Σ is said to be $(t_1, \ldots, t_m)$-partially anonymous if, for every secret s, every vector of shares $(s_1, \ldots, s_n)$ and every permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $\pi(G_i) = G_i$ (*e.g.* for every $P_j \in G_i$, $P_{\pi(j)} \in G_i$) for all $i = 1, \ldots, m$, the vector $(s_1, \ldots, s_n)$ is a vector or shares for the secret s if and only if $(s_{\pi(1)}, \ldots, s_{\pi(n)})$ is a vector of shares for s.*

Note that for $m = 1$, the new Definition 2 is equivalent to Definition 1 by [1].

4 Some Constructions

In this section we provide a general construction of $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme from different anonymous secret sharing schemes. The key point is that anonymous secret sharing schemes used as a building block have smaller thresholds, so *the share length of the $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme is considerably smaller that the one in a (t, n) anonymous secret sharing scheme* (remember that $t = \sum_{i=1}^{m} t_i$ and $n = \sum_{i=1}^{m} n_i$).

To begin with, let us describe the very particular case $t_1 = \ldots = t_m = 1$. That is, we assume the secret is recovered if at least one participant in each of the compartments G_i pool their shares. Note that in this case we are considering $m = t$. Similar reasonings apply if the threshold considered is less than m (at least $t < m$ participants from t different compartments are required to recover the secret).

Example 1. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of players and let $G_1, \ldots, G_m$ be compartments such that any set in $\mathcal{P}$ is placed exactly in one compartment, in such a way that no compartment remains empty. Let us construct a $(1, \ldots, 1)$-partially anonymous secret sharing scheme as follows. The dealer picks at random a polynomial $p(x)$ of degree at most $m-1$, whose free term is the secret s he wants to share. Let $p(x)$ be $p(x) = s + \sum_{j=1}^{m-1} a_j x^j$, where $a_j \in \mathbb{Z}_q$ has been randomly chosen, for $j = 1, \ldots, m-1$.

Every compartment G_i is univocally associated a value $\alpha_i \in \mathbb{Z}_q$. Then, D privately sends to each player in G_i his share $s_i = p(\alpha_i)$, for $i = 1, \ldots, m$.

Therefore, a set $A \subset \mathcal{P}$ with at least one player from every compartment can recover the secret $s = p(0)$ by interpolating the set of shares they hold. The main difference with Lagrange interpolation in the usual Shamir scheme is that now the participants do not have to publish their value α_i but only the compartment G_i they belong to. So, the only information that an outsider can derive is that the participant belongs to G_i.

It is easy to check that such a secret sharing scheme fulfills Definition 2 because the shares of all players in G_i are the same, for any $i = 1, \ldots, m$.

This construction can also use Karnin, Greene and Hellman's scheme instead of Shamir's scheme. □

The above construction can be generalized to obtain a $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme using as building blocks both (t_i, n_i)-anonymous secret sharing schemes and compartment secret sharing constructions. We detail this idea below.

Theorem 1. *Let $G_1, \ldots, G_m$ be disjoint compartmented subsets of players such that $G_1 \cup \cdots \cup G_m = \mathcal{P}$. Let Σ_i be a (t_i, n_i) anonymous secret sharing schemes on the set of players G_i, for $i = 1, \ldots, m$. Then, there exists a $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme Σ realizing a $(G_1, \ldots, G_m)$ compartmented access structure. Furthermore, the share length of scheme Σ is lower-bounded by the maximum of the share lengths of schemes Σ_i.*

Proof. In order to prove the theorem, we will explicitly construct the scheme Σ from $\Sigma_1, \ldots, \Sigma_m$. Without loss of generality, we can assume that

$$G_1 = \{P_1, \ldots, P_{n_1}\}$$

$$G_2 = \{P_{n_1+1}, P_{n_1+2}, \ldots, P_{n_1+n_2}\}$$

$$\ldots$$

$$G_i = \{P_{n_1+\ldots+n_{i-1}+1}, P_{n_1+\ldots+n_{i-1}+2}, \ldots, P_{n_1+\ldots+n_{i-1}+n_i}\}$$

$$\ldots$$

$$G_m = \{P_{n_1+\ldots+n_{m-1}+1}, P_{n_1+\ldots+n_{m-1}+2}, \ldots, P_n\}$$

Then, to share a secret s, the dealer chooses at random a polynomial $P(x)$ of degree $m-1$. Let $s^i = P(\alpha_i)$ be the share of compartment G_i, for $i = 1, \ldots, m$,

where $\alpha_i \in \mathbb{Z}_q$ is publicly associated to compartment G_i. Then, to distribute s^i (for every $i = 1, \ldots, m$) among the players in G_i he uses the anonymous secret sharing scheme Σ_i. Let

$$s_{n_1+\ldots+n_{i-1}+1}, s_{n_1+\ldots+n_{i-1}+2}, \ldots, s_{n_1+\ldots+n_{i-1}+n_i}$$

be the set of shares for players

$$P_{n_1+\ldots+n_{i-1}+1}, P_{n_1+\ldots+n_{i-1}+2}, \ldots, P_{n_1+\ldots+n_{i-1}+n_i}$$

respectively. Then, D privately sends $s_{n_1+\ldots+n_{i-1}+j}$ for $j = 1, \ldots, n_i$.

In this way, by construction it is easy to check that Σ realizes a $G_1, \ldots, G_m$ compartmented access structure (see Section 2). Thus, a subset not in the $G_1, \ldots, G_m$ compartmented access structure obtains no information on the secret, even if they join all their shares.

It only remains to prove that Σ is, in fact, a $(t_1, \ldots, t_m)$-partially anonymous secret sharing scheme. To do so, we need to check that Definition 2 is fulfilled. Indeed, for any secret s and any permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $\pi(G_i) = G_i$

$$(s_1, \ldots, s_{n_1}, \ldots, s_{n_1+\ldots+n_{i-1}+1}, \ldots, s_n)$$

is a set of shares for s if and only if

$$(s_{\pi(1)}, \ldots, s_{\pi(n_1)}, \ldots, s_{\pi(n_1+\ldots+n_{i-1}+1)}, \ldots, s_{\pi(n)})$$

is a set of shares of s. This easily follows from the fact that the schemes Σ_i are anonymous secret sharing schemes; that is, $(s_{n_1+\ldots+n_{i-1}+1}, \ldots, s_{n_1+\ldots+n_{i-1}+n_i})$ is a set of shares for s^i if and only if $(s_{\pi(n_1+\ldots+n_{i-1}+1)}, \ldots, s_{\pi(n_1+\ldots+n_{i-1}+n_i)})$ is a set of shares for s^i.

By construction, the length of the shares in Σ is lower-bounded by the maximum length of the shares of Σ_i. □

By [4], the lower bound on the size of the share domain depends multiplicatively on the amount $n - t$ for a (t, n) threshold access structure. Then, by Theorem 1, if $G_1, \ldots, G_m$ and $t_1, \ldots, t_m$ are chosen in a way that $\max_{i=1,\ldots,m} \{n_i - t_i\} < (n - t)$, the domain of shares of the resulting $(t_1, \ldots, t_m)$-partially anonymous secret sharing schemes is lesser than the domain of shares of the (t, n) threshold secret sharing scheme.

5 Conclusion

Anonymous secret sharing schemes allow a secret to be recovered from shares regardless of the identity of shareholders. Beyond their intrinsic interest, anonymous secret sharing allows anonymous participation in more general cryptographic protocols. A typical application is to make it possible for several parties to anonymously share the secret key corresponding to a public key.

Since current constructions of anonymous secret sharing schemes are not very efficient, we have introduced the notion of partial anonymous secret sharing schemes in an attempt to relax anonymity requirements to obtain more efficient constructions. A general construction for such partially anonymous schemes has also been described.

Disclaimer and Acknowledgments

The authors are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization. This work was partly supported by the Spanish Ministry of Education through project SEG2004-04352-C04-01 "PROPRIETAS" and by the Government of Catalonia under grant 2005 SGR 00446.

References

1. Beimel, A., Franklin, M.: Weakly-private secret sharing. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 253–272. Springer, Heidelberg (2007)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, American Federation of Information, Processing Societies Proceedings, vol. 48, pp. 313–317 (1979)
3. Blundo, C., Giorgia Gaggia, A., Stinson, D.R.: On the dealer's randomness required in secret sharing schemes. Designs, Codes and Cryptography 11, 107–122 (1997)
4. Blundo, C., Stinson, D.R.: Anonymous secret sharing schemes. Discrete Applied Mathematics 77, 13–28 (1997)
5. Brickell, E.F.: Some ideal secret sharing schemes. J. Math. Combin. Comput. 6, 105–113 (1989)
6. Carpentieri, M.: A perfect threshold secret sharing scheme to identify cheaters. Designs, Codes and Cryptography 5, 183–188 (1995)
7. Cramer, R., Damgård, I., Nielsen, J.: Multiparty computation from threshold homomorphic encryption. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 280–299. Springer, Heidelberg (2001)
8. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990)
9. Farràs, O., Martí-Farré, J., Padró, C.: Ideal multipartite secret sharing schemes. In: Eurocrypt 2007. LNCS, Springer, Heidelberg (to appear, 2007)
10. Gehrmann, C.: Topics in Authentication Theory, Ph.D. Thesis, Lund University (1997)
11. Ghodosi, H., Pieprzyk, J., Safavi-Naini, R.: Secret sharing in multilevel and compartmented groups. In: Boyd, C., Dawson, E. (eds.) ACISP 1998. LNCS, vol. 1438, pp. 367–378. Springer, Heidelberg (1998)
12. Guillermo, M., Martin, K.M., O'Keefe, C.M.: Providing anonymity in unconditionally secure secret sharing schemes. Designs, Codes and Cryptography 28, 227–245 (2004)
13. Herranz, J., Sáez, G.: New results on multipartite access structures. IEE Proceedings of Information Security 153-4 (December 2006)
14. Ito, M., Saito, A., Nishizeki, T.: Secret sharing scheme realizing any access structure. In: Proc. IEEE Globecom'87, pp. 99–102 (1987)

15. Karnin, E.D., Greene, J.W., Hellman, M.E.: On secret sharing systems. IEEE Transactions on Information Theory 29(1), 35–41 (1983)
16. Kishimoto, W., Okada, K., Kurosawa, K., Ogata, W.: On the bound for anonymous secret sharing schemes. Discrete Applied Mathematics 121(1-3), 193–202 (2002)
17. Phillips, S.J., Phillips, N.C.: Strongly ideal secret sharing schemes. Journal of Cryptology 5, 185–191 (1992)
18. Samarati, P., Sweeney, L.: Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Tech. rep., SRI International (1998)
19. Shamir, A.: How to share a secret. Communications of the ACM 22, 612–613 (1979)
20. Shoup, V.: Practical threshold signatures. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 207–220. Springer, Heidelberg (2000)
21. Simmons, G.J.: How to (really) share a secret. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 390–448. Springer, Heidelberg (1990)
22. Stinson, D.R., Vanstone, S.A.: A combinatorial approach to threshold schemes. SIAM J. Disc. Math. 1, 230–236 (1988)
23. von Ahn, L., Bortz, A., Hopper, N.J.: k-anonymous message transmission. In: Proc. of the 10th ACM Conference on Computer and Communications Security, pp. 122–130. ACM Press, New York (2003)
24. Xu, S., Yung, M.: k-anonymous secret handshakes with reusable credentials. In: Proc. of the 11th ACM Conference on Computer and Communications Security, pp. 158–167. ACM press, New York (2004)