Verifiable Secret Sharing for Monotone Access Structures

Thomas Beth Hans-Joachim Knobloch Marcus Otten*

Universität Karlsruhe
European Institute for System Security
Am Fasanengarten 5
D–76128 Karlsruhe
Germany

Abstract

Several verifiable secret sharing schemes for threshold schemes based on polynomial interpolation have been presented in the literature. Simmons and others introduced secret sharing (also called shared control) schemes based on finite geometries, which allow istributing a secret according to any monotone access structure.

In this paper we present a verifiable secret sharing scheme for a class of these geometry-based secret sharing schemes, which thus provides verifiable sharing of secrets according to general monotone access structures.

Our scheme relies on the homomorphic properties of the discrete exponentiation and therefore on the cryptographic security of the discrete logarithm. The version based on Simmons' scheme is non-interactive.

1 Introduction

The first and well-known examples for secret sharing schemes are the threshold schemes based on polynomial interpolation introduced by Shamir and Blakley [Sham79, Blak80]. In these schemes a trustworthy party, often called the *dealer*, distributes shares of a secret among N different parties in such a way that any k of them can recover the secret, whereas less than k shareholders can not.

*Marcus Otten has been supported by "Deutsche Forschungsgesellschaft, Graduiertenkolleg Beherrschbarkeit Komplexer Systeme, Universität Karlsruhe" under contract number Vo 287 / 5-1.

1st Conf.- Computer & Comm. Security '93-11/93 -VA,USA
© 1993 ACM 0-89791-629-8/93/0011...$1.50

Later, new secret sharing schemes for more general access structures, in which different shareholders may have different status, became a topic of research [ItSN87, BeLe88, Simm88, SiJM91]. The most general access structures for which practicable secret sharing schemes (often also called shared control schemes) exist are the general *monotone access structures*, in which arbitrary subsets of the set of participants may be designated. These designated subsets of shareholders and all their supersets, however no other set of participants, shall be able to cooperatively reveal the secret.

Another problem is, what can be done if there is not a commonly trusted dealer. In [InSi90] a scheme was presented that needs no trusted dealer. However this and other protocols (e.g. for multiparty computation or mental game problems) incorporate steps, in which one of the participants distributes a partial secret, which he knows, among other participants using a secret sharing scheme. If this "sub"-dealer is possibly not trustworthy, *verifiable secret sharing schemes* (VSS schemes) can be used.

Several VSS schemes have been published, which allow verification of some basic premises about the secret sharing scheme by the shareholders, even if the dealer is dishonest [CGMA85, Feld87, BrSt88, RaOr89, Pede91]. All these schemes are verifiable threshold schemes.

In this contribution we present a verification scheme for the secret sharing scheme presented in [SiJM91], where a construction is given to share a secret according to any general monotone access structure. Our verification scheme is non-interactive. There exists a generalization of the verification scheme presented here, which can deal with a slightly larger class of geometrical schemes. This scheme can be found in [Otte92].

The rest of the paper is organized as follows. In section 2 we briefly recall the geometry based secret sharing scheme which underlies our protocol. In section 3 we give a description of our approach. Section 4 contains security and efficiency considerations. Generalizations

and open problems are discussed in section 5.

2 The Geometrical Secret Sharing Scheme

The geometrical secret sharing scheme which underlies our verification scheme is that of [SiJM91]. For the convenience of the reader we will recall this scheme in the following few paragraphs.

The participants of the scheme are a dealer P_0 and shareholders P_i, $1 \leq i \leq N$. The access structure is

$$\mathcal{Z} = \{Z \subseteq \{P_1, \ldots, P_N\} \mid R(Z)\}$$

where $R(Z)$ shall denote that the members of Z are allowed to reconstruct the secret. An access structure is called monotone, if for every $Z \in \mathcal{Z}$ and $Z' \supseteq Z$ $Z' \in \mathcal{Z}$ holds. This means that when a set Z is allowed to initialize the controlled action, then also every superset Z' of Z is allowed to do so.

The secret to be shared is a point p in an affine or projective finite geometry of dimension n over GF(q) (for the remaining sections we will use the case of an affine geometry AG(n, q)). Let $\langle s \rangle$ denote the affine subspace spanned by the points in the set $s \subseteq$ AG(n, q). The dealer publishes a domain variety V_d which includes p. There exists an indicator variety V_i such that

$$\langle V_d \cup V_i \rangle = \text{AG}(n, q) \quad (1)$$

$$V_d \cap V_i = \{p\} \quad (2)$$

The share $s_i \subset S = \{p_0, \ldots, p_m\}$ of any shareholder P_i is a set of points of AG(n, q). The shares and the set S have to satisfy the following conditions:

$$S \cap V_d = \emptyset \quad (3)$$

$$\langle S \rangle = V_i \quad (4)$$

$$\forall Z \in \mathcal{Z} : \bigcup_{P_i \in Z} s_i = S \quad (5)$$

$$\forall C \notin \mathcal{Z} : \bigcup_{P_i \in C} s_i \neq S \quad (6)$$

Next we show how to construct the two varieties V_i and V_d according to Simmons, Jackson and Martin [SiJM91]. Suppose a given monotone access structure $\mathcal{Z}$. We now construct a monotone boolean formula

$$\Gamma = \Gamma(b_1, \ldots, b_n)$$

in disjunctive normal form (DNF) for which the following condition holds:

$$\Gamma(b_1, \ldots, b_n) = 1 \Leftrightarrow Z \in \mathcal{Z}$$

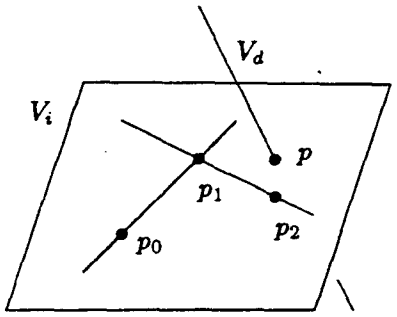

Figure 1: Realization of $\Gamma = AB \vee AC \vee BC \vee D$.

$$\text{with} \quad b_i = \begin{cases} 1 & P_i \in Z \\ 0 & \text{else} \end{cases}$$

It is easy to see that each monotone access structure has a unique boolean formula Γ in DNF and that to each monotone DNF formula there exits exactly one monotone access structure. Therefore each access structure can be identified by its DNF formula and vice versa. For any monotone Γ we define the formula Γ^* to be the logical expression obtained by interchanging the AND and OR in Γ written in DNF.

We now show how to derive the set S of points from AG(n, q). Let the two formulas Γ and Γ^* be given:

$$\Gamma(b_1, \ldots, b_n) = C_0 \vee C_1 \vee \cdots \vee C_r$$

$$\Gamma^*(b_1, \ldots, b_n) = S_0 \vee S_1 \vee \cdots \vee S_m$$

Choose $m + 2$ points $\{W, p_0, p_1, \ldots, p_{m-1}, p_m\}$ on a m-dimensional hyperplane of AG(n, q) such that no $m + 1$ points lie on a hyperplane of dimension $m - 1$. Let $p = W$ be the secret point and $S = \{p_0, \ldots, p_m\}$ (this means $V_i = \langle p_0, \ldots, p_m \rangle$). To decide which point p_i is given to which participant you define the mapping (the so called *cumulative scheme*)

$$\alpha : \{P_1, \ldots, P_n\} \rightarrow 2^S$$

$$\alpha(P_i) = s_i := \{p_j \mid b_i \text{ appears in } S_j\}$$

As a last step select a domain variety V_d of dimension r which intersects V_i at the secret point d. To illustrate the method we give a brief **example**. We want to design an access control system for four participants, in which any two out of the first three participants or the fourth participant on its on are allowed to determine the secret. The monotone DNF formula for this access structure is (for notational convenience we let $b_1 = A$, $b_2 = B$ and so on):

$$\Gamma(A, B, C, D) = AB \vee AC \vee BC \vee D$$

As a next step we determine the corresponding Γ^*:

$$\Gamma^*(A, B, C, D) = (A \vee B)(A \vee C)(B \vee C)D$$

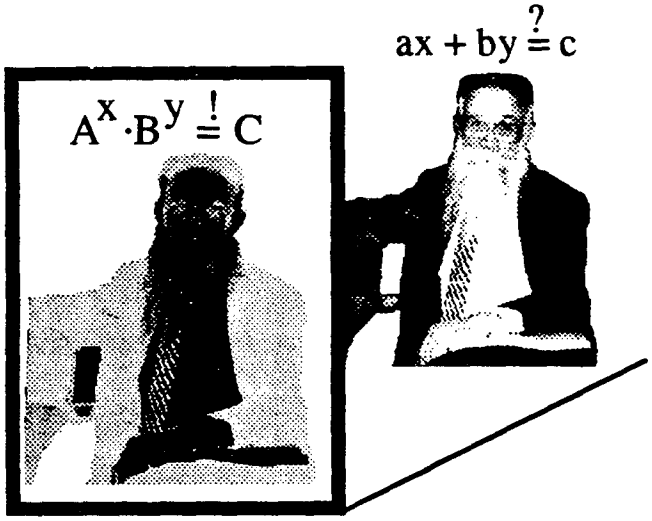

Figure 2: Computing by homomorphic images.

$$= ABD \vee ACD \vee BCD$$
$$= S_0 \vee S_1 \vee S_2$$

So the dimension of V_i is $m = 2$. The first point p_0 is given to participants P_1, P_2 and P_4. P_1, P_3 and P_4 get the point p_1, whereas p_2 is given to P_2, P_3 and P_4. Figure 1 shows a realization of this scheme where the dimension of the publicly known variety V_d was chosen to be 1. In the rest of the paper let $m = \dim(V_i)$ and $r = \dim(V_d)$.

3 The Verification Scheme

3.1 Prerequisites

The goal of the verification scheme is to allow the shareholders to verify the conditions (1) to (6) without giving them more information about p than they can already derive from s_i.

For this purpose we use the homomorphic properties of the discrete exponentiation and thus rely on the cryptographic security of the discrete logarithm assumption (see e.g. [Beth91]). The main and often used idea is to check equations after applying a proper one way function to the values involved. See figure 2 for an example where the secret values a, b and c are protected by a discrete exponentiation with results A, B and C whereas the validity of the linear combination can be checked if x and y are public.

Notation: For any point $x = [x_1, \ldots x_n]^T \in \mathrm{AG}(n, q)$ and for any $g \in GF(q)$ by g^x we denote the component wise exponentiation $[g^{x_1}, \ldots, g^{x_n}]^T$. By $\frac{g^x}{g^y}$ for $x, y \in \mathrm{AG}(n, q)$ we denote the vector $g^{x-y} = [\frac{g^{x_1}}{g^{y_1}}, \ldots, \frac{g^{x_n}}{g^{y_n}}]^T$.

Lemma 1 Let q be a prime and $\bar{q}$ a prime power with $q|\bar{q}-1$ (this means $dq = \bar{q}-1$) and $q^2 \nmid \bar{q}-1$, h a generator of $\mathrm{GF}(\bar{q})^*$ and $g = h^d = h^{(\bar{q}-1)q^{-1}}$ (therefore g is a generator of a cyclic subgroup of $\mathrm{GF}(\bar{q})$ of order q). Then the following equivalence holds for arbitrary elements $x, y, z, \lambda, \rho \in \mathrm{GF(q)}$

$$\lambda x + \rho y = z \text{ in } \mathrm{GF(q)} \Leftrightarrow g^{\lambda x} g^{\rho y} = g^z \text{ in } \mathrm{GF}(\bar{q}) \quad (7)$$

Proof:

$$g^{\lambda x} g^{\rho y} \equiv g^z$$
$$\Leftrightarrow g^{\lambda x + \rho y \bmod |\mathrm{GF}(\bar{q})^*|} \equiv g^{z \bmod |\mathrm{GF}(\bar{q})^*|}$$
$$\Leftrightarrow h^{d(\lambda x + \rho y) \bmod |\mathrm{GF}(\bar{q})^*|} \equiv h^{dz \bmod |\mathrm{GF}(\bar{q})^*|}$$

in $\mathrm{GF}(\bar{q})$. Because h is a generator of $\mathrm{GF}(\bar{q})^*$ and $|\mathrm{GF}(\bar{q})^*| = \bar{q}-1$ the following holds:

$$\Leftrightarrow \quad d(\lambda x + \rho y) \equiv dz \bmod dq$$

With $gcd(d, q) = 1$ (here we need $q^2 \nmid \bar{q}-1$) and the Chinese Remainder Theorem this is equivalent to

$$\Leftrightarrow \quad d(\lambda x + \rho y) \equiv dz \bmod q \quad \text{and}$$
$$d(\lambda x + \rho y) \equiv dz \bmod d$$
$$\Leftrightarrow \lambda x + \rho y \equiv z$$

in $\mathrm{GF(q)}$. □

This is one of several well-known methods to allow the use of field axioms in the exponent of a discrete exponentiation (see e.g. [DeFr91]).

Another fact we will use in our scheme is that in a variety V of $\mathrm{AG}(n, q)$ with dimension d and $V = \langle\{y_0, \ldots, y_d\}\rangle$ every point of V can be represented in a form $y_0 + \sum_{i=1}^{d} \lambda_i (y_i - y_0)$.

Lemma 2 The intersection of two varieties

$$V_1 = \langle x_0, \ldots, x_d \rangle \quad \text{and} \quad V_2 = \langle y_0, \ldots, y_e \rangle$$

of dimensions d and e will consist of exactly one point, if and only if there exist unique coefficient vectors $(\lambda_1, \ldots, \lambda_d)$ and $(\rho_1, \ldots, \rho_e)$ such that

$$x_0 + \sum_{i=1}^{d} \lambda_i (x_i - x_0) = y_0 + \sum_{j=1}^{e} \rho_j (y_j - y_0) \quad (8)$$

Proof: "⇒": Let $V_1 \cap V_2 = \{p\}$. Then there exist parameters λ_i and ρ_j satisfying equation (8) for the point p in the intersection of V_1 and V_2. Because the vectors $(x_i - x_0)$ and $(y_j - y_0)$ are bases for the affine subspaces V_1 and V_2 the parameters are unique.

"$\Leftarrow$": Assume there is only one solution

$$(\lambda_1, \ldots, \lambda_d, \rho_1, \ldots, \rho_e)$$

for the inhomogeneous linear equation

$$\sum_{i=1}^{d} \lambda_i (x_i - x_0) - \sum_{j=1}^{e} \rho_j (y_j - y_0) = y_0 - x_0$$

The solution space of the above equation has dimension 0, hence the solution space contains exactly one point p. Therefore p is the only element in the intersection of the two affine subspaces V_1 and V_2. □

3.2 Distribution of Verification Information

1. The dealer P_0 chooses g and $\bar{q}$ according to lemma 1 and points $y_0, \ldots, y_r$ such that $V_d = \langle \{y_0, \ldots, y_r\} \rangle$ and publishes the chosen values as well as index sets $\bar{s}_i = \{j | p_j \in s_i\}$.

2. P_0 publishes

$$(a_0, \ldots, a_m, a_{m+1}) = (g^{p_0}, \ldots, g^{p_m}, g^p).$$

3. P_0 determines $(\rho_1, \ldots, \rho_r)$ such that

$$p = y_0 + \sum_{i=1}^{r} \rho_i (y_i - y_0) \quad (9)$$

in GF(q) and publishes $g^{\rho_1}, \ldots, g^{\rho_r}$.

4. P_0 publishes $(\lambda_1, \ldots, \lambda_m)$ for which

$$p = p_0 + \sum_{i=1}^{m} \lambda_i (p_i - p_0) \quad (10)$$

in GF(q) holds.

5. For any unit vector e_l in AG(n, q) the dealer determines all the parameters $(\lambda_{l,1}, \ldots, \lambda_{l,m})$ and $(\rho_{l,1}, \ldots, \rho_{l,r})$ which fulfil the equations

$$e_l = \sum_{i=1}^{m} \lambda_{l,i} (p_i - p_0) + \sum_{j=1}^{r} \rho_{l,j} (y_j - y_0) \quad (11)$$

in GF(q). Then $(\lambda_{l,1}, \ldots, \lambda_{l,m})$ and $g^{\rho_{l,1}}, \ldots, g^{\rho_{l,r}}$ are published.

3.3 Verification

Every shareholder P_i performs the following checks and, if one of them fails, announces a failure.

1. P_i uses s_i to check that he got all necessary points and all the $\bar{s}_j$ to check conditions (5) and (6) and $(y_0, \ldots, y_r)$ to check that none of his points is in V_d.

2. (*Correctness of the* a_j) P_i checks

$$a_j = g^{p_j} \quad (12)$$

in GF($\bar{q}$) for all $p_j \in s_i$.

3. (*Correctness of* $p \in V_d$) P_i checks in GF($\bar{q}$)

$$a_{m+1} = g^{y_0} \prod_{j=1}^{r} \frac{(g^{\rho_j})^{y_j}}{(g^{\rho_j})^{y_0}} \quad (13)$$

4. (*Correctness of* $p \in V_i$) P_i checks in GF($\bar{q}$)

$$a_{m+1} = a_0 \cdot \prod_{j=1}^{m} \left(\frac{a_j}{a_0}\right)^{\lambda_j} \quad (14)$$

5. (*Correctness of* $\dim(V_i \cup V_d) = n$) P_i checks for $1 \le l \le n$

$$g^{e_l} = \prod_{j=1}^{m} \left(\frac{a_j}{a_0}\right)^{\lambda_{l,j}} \cdot \prod_{k=1}^{r} (g^{\rho_{l,k}})^{(y_k - y_0)} \quad (15)$$

in GF($\bar{q}$).

If none of the shareholders announced a failure, they are convinced that their shares are valid according to conditions (1) to (6).

4 Security and Efficiency

4.1 Correctness of the Verification

We have to show that the conditions (1) to (6) of section 2 are fulfilled if no shareholder complains during the verification phase. Condition (3) is explicitly checked in the first step of the verification, condition (4) is not really a condition, but rather the definition of V_i. The fact that no shareholder complains implies the validity of condition (5) (note that the index sets $\bar{s}_i$ are public).

To check the remaining conditions we prove the following

Lemma 3 Under the assumption that no honest shareholder complains during the verification the following equation holds unconditionally:

$$\langle s_0, \ldots, s_m \rangle \cap \langle y_0, \ldots, y_r \rangle = \{p\}$$

Proof: The validity of the equations (13) and (14) asserts the relations $p \in \langle s_0, \ldots, s_m \rangle$ and $p \in \langle y_o, \ldots, y_r \rangle$ using lemma 1.

Since equation (15) holds for each unit vector e_l together with lemmas 1 and 2 it follows straightforward that the vectors $\{s_1 - s_0, \ldots, s_m - s_0, y_1 - y_0, \ldots, y_r - y_0\}$ form a basis of the affine space $\mathrm{AG}(n, q)$. The dimension formula

$$\dim(\mathrm{AG}(n,q)) = n = \dim(V_i) + \dim(V_d) - \dim(V_i \cap V_d)$$

and the equality $n = m + r$ imply $\dim(V_i \cap V_d) = 0$, therefore $V_i \cap V_d = \{p\}$. □

The last lemma directly ensures the validity of condition (1) and condition (2). Since $\langle S \cup V_d \rangle = \mathrm{AG}(n, q)$ and $\dim(\langle S \rangle) = m$, no proper subset $S' \subset S$ intersects with V_d. Therefore condition (6) holds.

4.2 Security of the Shares and Secret

With respect to the secrecy the dealer must be considered honest, since otherwise he obviously can give the secret p privately to any arbitrary participant without being detected by any means.

First we consider the information released by the dealer when broadcasting the values $a_i = g^{p_i}$, $a = g^p$ and g^{ρ_j} in steps 2 and 3 of the distribution phase respectively. Computing p, p_i or ρ_j from the distributed values would mean breaking the discrete logarithm assumption. The determination of a coefficient vector $(\rho_1, \ldots, \rho_r)$ according to equation (9) without breaking the discrete logarithm is nothing else but exhaustive search in V_d. The same is valid for determining the p_i with respect to the set $\mathrm{AG}(n, q) \setminus V_d$ (the set of all possible points for the shares p_i).

Next we have to consider the additional information contained in the parameters λ_i that are distributed in step 4. For that we consider a maximum set of cheating shareholders knowing all but one of the p_i to construct V_i and all λ_i. Then the following holds:

Lemma 4 Under the assumption that the dealer is honest even for a maximum set of cheating shareholders the coefficient vector $(\lambda_1, \ldots, \lambda_m)$ contains no additional information.

Proof: Without loss of generality let p_m be the point unknown to the cheating shareholders. Then the equation (10) can be simplified to a form

$$p = \lambda p_m + d \tag{16}$$

with known coefficient λ and vector d. It has to be shown, that for any point $p' \in V_d$ there exists a unique solution p'_m for the equation $p' = \lambda p'_m + d$. This p'_m must be shown to be neither in V_d nor in $\langle S \setminus \{p_j\} \rangle$. Let $p'_m := \lambda^{-1}(p' - d)$ for an arbitrary $p' \in V_d$. If $p'_m \in \langle S \setminus \{p_j\} \rangle$ then the intersection of $\langle S \setminus \{p_j\} \rangle$ and V_d would not be empty which contradicts with the honest-dealer-assumption. $p'_m \in V_d$ together with $p' \in V_d$ implies $d \in \langle y_1 - y_0, \ldots, y_r - y_0 \rangle$. This is a contradiction to $d \in \langle p_1 - p_0, \ldots, p_{m-1} - p_0 \rangle$. □

Now consider the information published by P_0 in step 5 of the distribution phase in section 3.2, namely the matrix

$$M = \begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,m} & g^{\rho_{1,1}} & \cdots & g^{\rho_{1,r}} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,m} & g^{\rho_{n,1}} & \cdots & g^{\rho_{n,r}} \end{pmatrix} \tag{17}$$

Recall that $r \geq 1$, since a V_d of dimension 0 would instantly reveal the secret p. If the $\rho_{i,j}$ were given directly, this would constitute a basis conversion matrix M' (to the standard orthonormal base), which could be used to compute p efficiently. However, this computation involves an inversion of M'. Since at least one column of M is completely undetermined, M^{-1} is also undetermined.

4.3 Robustness against Cheating Shareholders during the Recombination

If none of the shareholders indicates a failure during the verification phase, their shares are fixed by the values $a_0, \ldots, a_m$ and the secret p is fixed by a_{m+1}. During an attempted recombination of the secrets a shareholder can no longer try to cheat by misrepresenting his share, since a recombination device can compare the shares to the witnesses a_i before doing any other computations.

The validity of the result of the recombination can also be checked using the witness a_{m+1}. Thus a shared control device does not need to store the secret in clear as reference value for a comparison.

4.4 Efficiency

The presented verification scheme is non-interactive. The additional communication from the dealer to the shareholders is $O(n^2 \log \bar{q})$ bits. The computational effort of the dealer is $O(n^3)$ operations in $\mathrm{GF}(\bar{q})$, the required additional effort of the shareholders is $O(n^2)$ operations in $\mathrm{GF}(\bar{q})$.

5 Generalizations and Open Problems

The verifiable secret sharing scheme presented in section 3 can be generalized for a wider class of geome-

try based secret sharing methods. The method shown here relies on the fact that the secret sharing schemes described in [SiJM91] are *cumulative*: each designated subset of shareholders constructs the same indicator variety V_i. Non-cumulative schemes allow the construction of different varieties V_i', each of them having properties $V_d \cap V_i' = \{p\}$ and $\dim(V_i') = m$. A modified form of our scheme can deal with such schemes whenever interaction between the dealer and the shareholders is allowed and can be found in [Otte92].

When dealing with general geometry-based secret sharing schemes two further problems arise. The first one is the construction of non-interactive verification for non-cumulative schemes. The second problem is dropping the requirement $\dim(V_i') = m$ in non-cumulative schemes which is essential in our generalized verification scheme.

The existence of a VSS scheme for general monotone access structures maybe allows the use of non-threshold secret sharing schemes in the construction of multiparty computation protocols.

6 Conclusion

We have shown how the homomorphic properties of the discrete exponentiation function can be used to verify the correct distribution of shares in some geometry-based secret sharing schemes. This property could also be used in verification schemes for other geometry-based protocols like [Simm88, Simm89, Beut89].

References

[BeLe88] J. Benaloh, J. Leichter: *Generalized Secret Sharing and Monotone Functions*, Crypto '88, Advances in Cryptology, LNCS Vol. 403, Springer, Berlin, 1990, pp. 27–35

[Beth91] Th. Beth: *Keeping Secrets a Personal Matter or: The Exponential Security System*, Proc. IMA Workshop on Cryptography and Coding, Cirencester, December 1991

[Beut89] A. Beutelspacher: *How to say "No"*, Eurocrypt '89, Advances in Cryptology, LNCS Vol. 434, Springer, Berlin, 1990, pp. 491–498

[Blak80] G. R. Blakley: *Security Proofs for Information Protecting Systems*, Proc. of the 1980 Symposium on Security and Privacy, IEEE Comp. Soc. Press, 1981, pp. 79–88

[BrSt88] E. F. Brickell, D. R. Stinson: *The Detection of Cheaters in Threshold Schemes*, Crypto '88, Advances in Cryptology, LNCS Vol. 403, Springer, Berlin, 1990, pp. 564–577

[ChEG87] D. Chaum, J.-H. Evertse, J. van de Graaf: *An Improved Protocol for Demonstrating Possession of a Discrete Logarithm and Some Generalizations*, Eurocrypt '87, Advances in Cryptology, LNCS Vol. 304, Springer, Berlin, 1988, pp. 127–141

[CGMA85] B. Chor, O. Goldwasser, S. Micali, B. Awerbuch: *Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults*, Proc. of the 26th FOCS, IEEE 1985, pp. 383–395

[DeFr91] Y. Desmedt, Y. Frankel: *Threshold Cryptosystems*, Crypto '91, Advances in Cryptology, LNCS Vol. 576, Springer, Berlin, 1992, pp. 307–315

[Feld87] P. Feldman: *A Practical Scheme for Non-Interactive Verifiable Secret Sharing*, Proc. of the 28th FOCS, IEEE 1987, pp. 427–437

[InSi90] I. Ingemarsson, G. J. Simmons: *A Protocol to Set Up Shared Secret Schemes Without the Assistance of a Mutually Trusted Party*, Eurocrypt '90, Advances in Cryptology, LNCS Vol. 473, Springer, Berlin, 1991, pp. 266–282

[ItSN87] M. Ito, A. Saito, T. Nishizeki: *Secret Sharing Schemes Realizing General Access Structures*, IEEE Globecom 1987, IEEE Communication Society Press, Washington, D.C., 1987, pp. 99–102

[Otte92] M. Otten: *Mehrparteienprotokolle und Korrektes Verteilen von Geheimnissen*, Diplomarbeit, Universität Karlsruhe, European Institute for System Security, 1992

[Pede91] T. P. Pedersen: *Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing*, Crypto '91, Advances in Cryptology, LNCS Vol. 576, Springer, Berlin, 1991, pp. 129–140

[RaOr89] T. Rabin, M. Ben-Or: *Verifiable Secret Sharing and Multiparty Protocols with Honest Majority*, Proc. of the 21st STOC, ACM 1989, pp. 73–85

[Sham79] A. Shamir: *How to Share a Secret*, Comm. of the ACM, Vol. 22, No. 11, November 1979, pp. 612–613

[SiJM91] G. J. Simmons, W.-A. Jackson, K. Martin: *The Geometry of Shared Secret Schemes*, Bulletin of the Institute of Combinatorics, Winnipeg Canada, January 1991

[Simm88] G. J. Simmons: *How To (Really) Share a Secret*, Crypto '88, Advances In Cryptology, LNCS Vol. 403, Springer, Berlin, 1990, pp. 390–448

[Simm89] G. J. Simmons: *Robust Shared Secret Schemes*, Congressus Numerantium, Vol. 68, May 1989, pp. 215–248