14

Threshold Secret Sharing Through Multivariate Birkhoff Interpolation

Vasileios E. Markoutis, Gerasimos C. Meletiou, Aphrodite N. Veneti, and Michael N. Vrahatis

Abstract Secret sharing schemes have been well studied and widely used in different aspects of real life applications. The original secret sharing scheme was proposed by Adi Shamir in 1979. A similar scheme was also invented independently in the same year by George Blakley. Shamir's scheme is based on Lagrange interpolation while Blakley's approach uses principles of hyperplane geometry. In 2007, Tamir Tassa proposed a hierarchical secret sharing scheme through univariate Birkhoff interpolation (a generalization of Lagrangian and Hermitian interpolation). In the contribution at hand we investigate the idea of generalizing Tassa's scheme through multivariate Birkhoff interpolation. We consider the problem of finding secret sharing schemes with multilevel structures and partially ordered sets of levels of participants. In order to ensure that our scheme meets the necessary requirements, we use totally nonsingular matrices.

Keywords: Secret sharing schemes • Multivariate Birkhoff interpolation • Hierarchies

V.E. Markoutis (✉)
Department of Mathematics, University of Patras, GR-26110 Patras, Greece
e-mail: billmarku@yahoo.gr

G.C. Meletiou
A.T.E.I. of Epirus, P.O. 110, GR-47100 Arta, Greece
e-mail: gmelet@teiep.gr

A.N. Veneti
Department of Informatics, University of Piraeus, 18534 Piraeus, Greece
e-mail: aveneti@unipi.gr

M.N. Vrahatis
Computational Intelligence Laboratory (CILab), Department of Mathematics, University of Patras, GR-26110 Patras, Greece
e-mail: vrahatis@math.upatras.gr

N.J. Daras, M.Th. Rassias (eds.), *Computation, Cryptography, and Network Security*, DOI 10.1007/978-3-319-18275-9_14

1 Introduction

A secret sharing scheme is a methodology to distribute appropriately a piece of information of a secret, called ***share***, to each element of a specific set, called ***participant***, so that the secret can be reconstructed after the revelation of the shares of specific subsets of the set of participants. Since these specific subsets of participants depend on the secret sharing problem that has to be solved, a plethora of different schemes have been proposed.

Secret sharing schemes are very important, since they are used in various significant applications including cryptographic key distribution and sharing, e-voting, secure online auctions, information hiding as well as secure multiparty computation, among others. Shamir in [20] and Blakley in [5] invented independently, in 1979, the idea of secret sharing schemes. Shamir's approach is based on Lagrange interpolation while Blakley's method uses principles of hyperplane geometry. Tassa in [22] generalized Shamir's construction for a hierarchical threshold secret sharing scheme. His approach solves the problem of an efficient hierarchical threshold secret sharing scheme with a totally ordered set of levels of participants and is based on univariate Birkhoff interpolation. Birkhoff interpolation is a generalization of the Hermite case, obtained by relaxing the requirement of consecutive derivatives at the nodes.

In the contribution at hand we investigate the idea of generalizing Tassa's scheme through multivariate Birkhoff interpolation. We consider the problem of finding secret sharing schemes with multilevel structures and partially ordered sets of levels of participants. In order to ensure that our scheme meets the necessary requirements, we use totally nonsingular matrices.

In Sect. 2 of the work at hand we present basic concepts and background material related to secret sharing and threshold secret sharing schemes. Also, we briefly describe Blakley's scheme as well as we present Shamir's scheme based on Lagrange interpolation. Subsequently, in Sect. 3 we give some basic definitions related to Birkhoff interpolation. Next, in Sect. 4 we give a brief description of Tassa's secret sharing scheme based on univariate Birkhoff interpolation. In Sect. 5 we detail our ideas for constructing partially ordered secret sharing schemes through multivariate Birkhoff interpolation, we discuss the obtained results and open up some perspectives for our future work. The chapter ends in Sect. 6 with a synopsis.

2 Secret Sharing and Threshold Secret Sharing Schemes

In this section, basic concepts and background material related to secret sharing and threshold secret sharing schemes are given. Also, Blakley's scheme is briefly described. Furthermore, Shamir's scheme based on Lagrange interpolation is presented.

2.1 Secret Sharing Schemes

Stinson in his survey article for secret sharing schemes [21] gives a detailed description of the basic concepts of a secret sharing scheme.

Let $\mathscr{P}$ be a set of n participants that a secret is distributed to and Γ be the set of subsets of $\mathscr{P}$ such as $\Gamma \subseteq 2^{\mathscr{P}}$. The set Γ contains every subset of participants that should be able to compute the secret. Thus, Γ is called an ***access structure*** and the subsets in Γ are called ***authorized*** subsets. An access structure must satisfy the ***monotonicity*** property. Suppose that $B \in \Gamma$ and $B \subseteq C \subseteq \mathscr{P}$. Then the subset C can determine the value of secret key K. Formally we can say that [3, 21]:

$$\text{if} \quad B \in \Gamma \quad \text{and} \quad B \subseteq C \subseteq \mathscr{P}, \quad \text{then} \quad C \in \Gamma.$$

If Γ is an access structure, then $B \in \Gamma$ is a minimal authorized subset of $A \notin \Gamma$ whenever $A \subset B$. The set of minimal authorized subsets of Γ is denoted by Γ_0 and is called the ***basis*** of Γ.

Let D be a participant, called ***dealer***, who does not belong to the set $\mathscr{P}$. The dealer chooses the value of the secret and distributes the shares of the secret secretly so that no participant knows the share given to another participant. Also, let $\mathscr{K}$ be the ***key set*** and $\mathscr{S}$ be the ***share set***. When the dealer D wants to share a ***secret key*** $K \in \mathscr{K}$ he gives each participant a share from $\mathscr{S}$.

A simple approach for the definition of a secret sharing scheme is given in [6]. Given a set of n participants and an access structure Γ, a ***secret sharing scheme*** for Γ is a method of distributing shares to each of the participants such that:

1. Any subset of the participants in Γ can determine the secret.
2. Any subset of the participants that does not belong in Γ cannot determine the secret.

The share of a participant refers specifically to the information that the dealer D sends in private to the participant. If any subset of participants that does not belong in Γ cannot determine any information about the secret, then the secret sharing scheme is said to be ***perfect***. Given a secret sharing scheme we define the ***information rate*** ρ of the scheme as follows:

$$\rho = \frac{\log_2 |\mathscr{K}|}{\log_2 |\mathscr{S}|}. \tag{1}$$

If $\rho = 1$, then the scheme is called ***ideal***.

Remark 1. The first property implies that the shares given to an authorized subset uniquely determine the value of the secret. ***Accessibility*** and ***correctness*** are terms that are used alternatively to describe this property. The second property ensures that the shares given to an unauthorized subset reveal no information as to the value of the secret. ***Perfect security*** and ***privacy*** are terms that are used alternatively to describe this property.

The construction of a secret sharing scheme can be divided into the following three phases:

1. **Initialization phase:** The dealer chooses the secret key K.
2. **Secret sharing phase:** The dealer shares the secret key K among the set $\mathscr{P}$ of n participants giving each participant a share from $\mathscr{S}$ secretly.
3. **Secret reconstruction phase:** At a later time, a subset B of participants with $B \subseteq \mathscr{P}$ will pull their shares in an attempt to recompose the secret key K.

2.2 Threshold Secret Sharing Schemes

One of the most common class of secret sharing schemes is the class of threshold secret sharing schemes which implies that the reconstruction of the secret can be achieved by the contribution of a minimum number of participants of the set which we call ***threshold***.

Threshold secret sharing schemes were initially proposed for key management purposes. Let us recall an example from [21]:

Example 1. Assume that there is a vault in a bank that must be opened every day. The bank employs three senior tellers, but it is not desirable to entrust the combination to a unique person. We want to design a system whereby any two of the three senior tellers can gain access to the vault, but no individual can do so.

According to Shamir [20] a threshold secret sharing scheme can be defined as follows:

Definition 1. A (k, n) ***threshold secret sharing scheme*** is a method which gives efficient solution to the problem of the division of a piece of data K into n pieces $K_1, K_2, \ldots, K_n$ with the following two constraints:

1. K can be easily retrieved with the knowledge of k or more K_i pieces.
2. No information can be revealed about K with the knowledge of any $k-1$ or fewer K_i pieces.

Remark 2. In other words, a (k, n) threshold secret sharing scheme is a method of sharing a secret key K among a finite set $\mathscr{P}$ of n participants in such a way that any k participants can compute the value of K, but no one group of $k-1$ participants can do so.

A (k, n) threshold secret sharing scheme realizes the access structure:

$$\mathscr{A} = \{B \subseteq \mathscr{P} : |B| \geqslant k\}.$$

Such an access structure is called a ***threshold access structure***. It is obvious that in the case of a threshold access structure, the basis of the structure consists of all subsets of exactly k participants.

According to ***Blakley's scheme*** [5, 13] the secret is a point in a k-dimensional subspace over a finite field and the coefficients of the hyperplanes that intersect at this point are used to construct the shares. For the implementation of a (k, n) threshold secret sharing scheme, to each one of the n participants is given a hyperplane equation. In order to obtain the secret, a system of linear equations $Ax = y$ must be solved, where the matrix A and the vector y are derived from the hyperplane equations. When k participants come together, they can solve the system to find the intersection point of the hyperplanes in order to obtain the secret.

As we have mentioned before, Shamir [20] constructed a threshold secret sharing scheme using Lagrange interpolation. Also, Tassa [22] generalized Shamir's construction for a hierarchical threshold secret sharing scheme. His approach was based on univariate Birkhoff interpolation which solves the problem of an efficient hierarchical threshold secret sharing scheme with totally ordered set of levels of participants.

In our approach we investigate the construction of secret sharing schemes with the usage of multivariate Birkhoff interpolation. In this case, the structure that results is multilevel but the set of levels of participants is partially ordered.

Various threshold secret sharing schemes have been applied in many fields of information science [2] including threshold cryptography [10] and ad-hoc networks [1] among others.

2.3 Shamir's Scheme Through Lagrange Interpolation

As we have already mentioned, Shamir in [20] introduced the idea of a threshold secret sharing scheme through polynomial interpolation. His idea was based on Lagrange interpolation. More specifically, he exploited the fact that given k points on a 2-dimensional plane $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$ with distinct x_i, there exists one and only one polynomial $g(x)$ of $k-1$ degree such that $g(x_i) = y_i$ for all $i = 1, 2, \ldots, k$.

Thus, in order to divide and share a secret S he considered a random polynomial $g(x)$ of $k-1$ degree as following:

$$g(x) = a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} + S. \tag{2}$$

A polynomial interpolating value $g(x_i) = y_i$ is a share that can be given to a participant. A set of k shares are enough to define the unique polynomial $g(x)$ and obviously reveal S while $k-1$ or less shares do not suffice for the calculation of S.

Shamir's (k, n) threshold secret sharing scheme can be described by the following algorithm:

Algorithm 1

1. **Initialization phase:** The dealer chooses n distinct nonzero elements from a finite field $\mathbb{F}_q$, $\{x_1, x_2, \ldots, x_n\}$, and gives x_i to the i-th participant p_i. In other terms participant p_i is identified to the field element x_i.
2. **Secret sharing phase:** The dealer secretly chooses $k-1$ elements from $\mathbb{F}_q$, $\{a_1, a_2, \ldots, a_{k-1}\}$, and considers the following polynomial:

$$g(x) = \sum_{i=1}^{k-1} a_i x^i + S, \tag{3}$$

   where S is the constant term of the polynomial which represents the secret. The dealer computes the n shares $y_i = g(x_i)$ and gives each share to the corresponding participant.
3. **Secret reconstruction phase:** A subset B of k participants $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ will pull their shares and attempt to reconstruct S. Suppose that the k shares $y_{i_j} = g(x_{i_j})$, $1 \leqslant j \leqslant k$ are revealed. Then, the coefficients of polynomial $g(x)$ can be evaluated by Lagrange interpolation. Consequently secret S is obtained by the evaluation $S = g(0)$.

3 Birkhoff Interpolation

The problem of interpolating a function $f : \mathbb{R} \to \mathbb{R}$ by a univariate polynomial from the values of f and some of its derivatives on a set of sample points is one of the main questions in Numerical Analysis and Approximation Theory [18].

Birkhoff interpolation [4, 15, 17, 19] is a generalization of Lagrange and Hermite polynomial interpolation. It amounts to the problem of finding a polynomial $f(x)$ of degree $k-1$ such that certain derivatives have specified values at specified points:

$$f^{(n_i)}(x_i) = y_i, \quad \text{for} \quad i = 1, 2, \ldots, k, \tag{4}$$

where the data points (x_i, y_i) as well as the nonnegative integers n_i are given.

Remark 3. In contrast to Lagrange and Hermite interpolation problems which are well posed, Birkhoff interpolation problems do not always have unique solution.

Definition 2. Let $\mathscr{X} = \{x_1, x_2, \ldots, x_n\}$ be an ordered set of real numbers such that $x_1 < x_2 < \cdots < x_n$ and $\mathscr{I} \subset \{1, 2, \ldots, n\} \times \{0, 1, \ldots, r\}$ be the set of pairs (i, j) such that the value $f_{i,j} = f^{(j)}(x_i)$ is known. The problem of determining the existence and uniqueness of a polynomial Q in $\mathbb{R}[X]$ of degree bounded by r such that:

$$\forall\, (i, j) \in \mathscr{I}, \quad Q^{(j)}(x_i) = f_{i,j}\,, \tag{5}$$

is called the ***Birkhoff interpolation problem***.

The multivariate Birkhoff interpolation problem is more complicated. A formal definition of this problem can be given as follows [8, 14]:

Definition 3. A ***multivariate Birkhoff interpolation scheme***, $(E, \mathbb{W}_s)$, consists of three components:

1. A **set of nodes** $\mathscr{Z}$:

$$\mathscr{Z} = \{z_t\}_{t=1}^{m} = \{(x_{t,1}, x_{t,2}, \ldots, x_{t,d})\}_{t=1}^{m} . \tag{6}$$

2. An **interpolation space** $\mathbb{W}_s$:

$$\mathbb{W}_s = \left\{W \ : \ W(z) = W(x_1, x_2, \ldots, x_d) = \sum_{i \in S} a_i x_1^{i_1}, \ldots, x_d^{i_d}\right\}, \tag{7}$$

where S is a lower subset of $\mathbb{N}_0^d$. A subset A of $\mathbb{N}_0^d$ is a lower set if $0 \leqslant j_k \leqslant i_k$, $k = 1, 2, \ldots, d$ and $i \in S$ implies that $j \in S$.

3. An **incidence** $(d+1)$**-dimensional matrix** E:

$$E = \{e_{t,\alpha}\}, \quad t = 1, 2, \ldots, m, \quad \alpha \in S, \tag{8}$$

where $e_{t,\alpha} = 0$ or $e_{t,\alpha} = 1$.

Given these components, the ***multivariate Birkhoff interpolation problem*** is, for given real numbers $c_{t,\alpha}$ for those t, α with $e_{t,\alpha} = 1$, to find a polynomial $W \in \mathbb{W}_s$ satisfying the interpolation conditions:

$$\frac{\partial^{\alpha_1+\alpha_2+\cdots+\alpha_d}}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \cdots \partial x_d^{\alpha_d}} W(z_t) = c_{t,\alpha} , \tag{9}$$

for those t, α with $e_{t,\alpha} = 1$.

Remark 4. The aforementioned schemes are interpolations over the real numbers. In cryptographic applications finite fields are used and derivatives (ordinary and partial) are replaced with formal derivatives of polynomials. Since we deal with polynomials it is always true that $\frac{\partial^2 f}{\partial x_1 \partial x_2} = \frac{\partial^2 f}{\partial x_2 \partial x_1}$.

4 Tassa's Scheme Through Univariate Birkhoff Interpolation

Tassa in [22] proposed a perfect and ideal secret sharing scheme for a multilevel totally ordered structure. His approach is based on univariate Birkhoff interpolation. Since Tassa's scheme is the basis of our scheme, we detail his following definition for a hierarchical threshold secret sharing scheme.

Definition 4. Let $\mathscr{P}$ be a set of n participants and assume that $\mathscr{P}$ is composed of levels, i.e., $\mathscr{P} = \cup_{i=0}^{m} \mathscr{P}_i$ where $\mathscr{P}_i \cap \mathscr{P}_j = \emptyset$ for all $0 \leqslant i < j \leqslant m$. Let $\boldsymbol{\kappa} = \{k_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers, $0 < k_0 < k_1 < \cdots < k_m$. Then, the $(\boldsymbol{\kappa}, n)$ ***hierarchical threshold access structure*** is given as follows:

$$\Gamma = \left\{B \subset \mathscr{P} : \ \left|B \cap \left(\cup_{j=0}^{i} \mathscr{P}_j\right)\right| \geqslant k_i , \quad \forall \ i \in \{0, 1, \ldots, m\}\right\}. \tag{10}$$

Algorithm 2

1. **Initialization phase:** The dealer chooses n distinct nonzero elements from a finite field $\mathbb{F}_q$, $\{x_1, x_2, \ldots, x_n\}$, and gives x_i to the i-th participant p_i. In other terms the dealer identifies each participant $p \in \mathscr{P}$ with an element of the field $\mathbb{F}_q$. For simplicity, the field element is also denoted by p.
2. **Secret sharing phase:** The dealer secretly chooses $k-1$ elements from $\mathbb{F}_q$, $\{a_1, a_2, \ldots, a_{k-1}\}$, and considers the following polynomial:

$$g(x) = \sum_{i=1}^{k-1} a_i x^i + S, \tag{11}$$

   where S is the constant term of the polynomial which represents the secret. Every participant p of the i-th level of the hierarchy receives the share:

$$y = \left(\frac{\mathrm{d}^{k_{i-1}} g}{\mathrm{d}x^{k_{i-1}}} \right)_p = g^{(k_{i-1})}(p),$$

   where $g^{(k_{i-1})}(p)$ is the k_{i-1}-th formal derivative of $g(x)$ at $x = p$ with $k_{-1} = 0$.
3. **Secret reconstruction phase:** An authorized subset B of k participants will pull their shares and attempt to reconstruct S. Then, the coefficients of polynomial $g(x)$ can be evaluated by univariate Birkhoff interpolation. Consequently secret S is obtained by the evaluation $S = g(0)$.

A corresponding $(\boldsymbol{\kappa}, n)$ ***hierarchical secret sharing scheme*** is a scheme that realizes the above access structure; namely, a method of assigning each participant $P_l \in \mathscr{P}$, with $0 \leqslant l < n$, a share $\sigma(P_l)$ of a given secret S such that authorized subsets $B \in \Gamma$ may recover the secret from the shares possessed by their participants, $\sigma(B) = \{\sigma(P_l) : P_l \in B\}$, while the shares of unauthorized subsets $B \notin \Gamma$ do not reveal any information about the value of the secret.

Remark 5. For the construction of a hierarchical threshold secret sharing scheme, Tassa used k-order derivatives and constructed shares for each level according to the order of the derivative. In this way he ensured that the participants of an upper hierarchically level possess more amount of information to their share than the participants of a lower level. The calculation of the polynomial coefficients during the secret reconstruction phase was based on the univariate Birkhoff interpolation.

Tassa's $(\boldsymbol{\kappa}, n)$ hierarchical threshold secret sharing scheme with $\boldsymbol{\kappa} = \{k_i\}_{i=0}^m$ and $k = k_m$ can be described by the following algorithm:

5 The Proposed Approach

As we have already mentioned, in our approach we investigate the construction of secret sharing schemes with the usage of multivariate Birkhoff interpolation. In this case, the structure that results is multilevel but the set of levels of participants is partially ordered. In Tassa's scheme, the shares of two participants p_a and p_b of different levels have, by necessity, at least one of the following two properties:

(a) The share of p_a can substitute the share of p_b.
(b) The share of p_b can substitute the share of p_a.

In our case this is not always true due to the partial order of the levels of participants and this is the main difference with Tassa's scheme.

We illustrate our ideas through some examples and we propose a construction for the simple linear case of a threshold multilevel partially ordered secret sharing scheme. However, a generalized case of a partially ordered set should be an object of a much more complicated effort. At this point, it must be noted that a partially ordered secret sharing scheme is not hierarchical, since a hierarchical structure presupposes a totally ordered set of participants [11, 12].

5.1 The Main Idea of Our Approach

We consider the multivariate polynomial $g(x_1, x_2, \ldots, x_d)$ with coefficients from a finite field. The constant term of the polynomial denotes the ***secret*** S, that is $g(0, 0, \ldots, 0) = S$. Some participants receive ***shares*** of the following form:

$$y_t = g(x_{t,1}, x_{t,2}, \ldots, x_{t,d}) = g(z_t),$$

and they consist of the (top) level $\mathscr{P}_0$ (the d-tuples are nodes as they are described in Definition 3). Some participants receive shares of the form $\frac{\partial}{\partial x_1} g(z_t)$ and they belong to the level $\mathscr{P}_1$. In a similar way we define $\mathscr{P}_2, \mathscr{P}_3, \ldots$ The level $\mathscr{P}_{1,1}$ is related to the shares of the form $\frac{\partial^2}{\partial x_1^2} g(z_t)$ while the level $\mathscr{P}_{1,2}$ is related to the shares of the form $\frac{\partial^2}{\partial x_1 \partial x_2} g(z_t)$. Since $\frac{\partial^2}{\partial x_1 \partial x_2} g(z_t) = \frac{\partial^2}{\partial x_2 \partial x_1} g(z_t)$, the level $\mathscr{P}_{1,2}$ coincides with the level $\mathscr{P}_{2,1}$. Thus, an ordered set of levels is derived which have the form $\mathscr{P}_{j_1, j_2, \ldots, j_n}$.

For $d = 2$ and $d = 3$ the obtained multilevel structures are exhibited in Figs. 1 and 2, respectively.

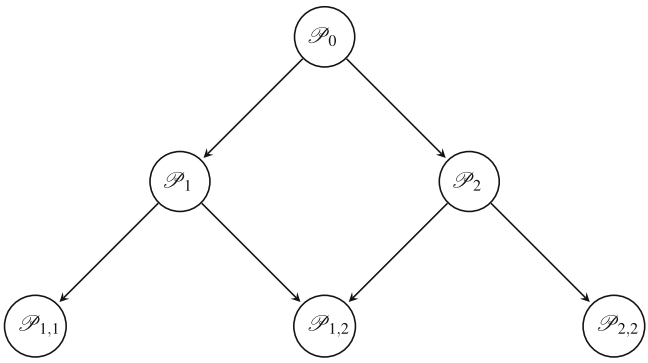

Fig. 1 The structure of a secret sharing scheme that can be constructed from a polynomial $g(x_1, x_2)$

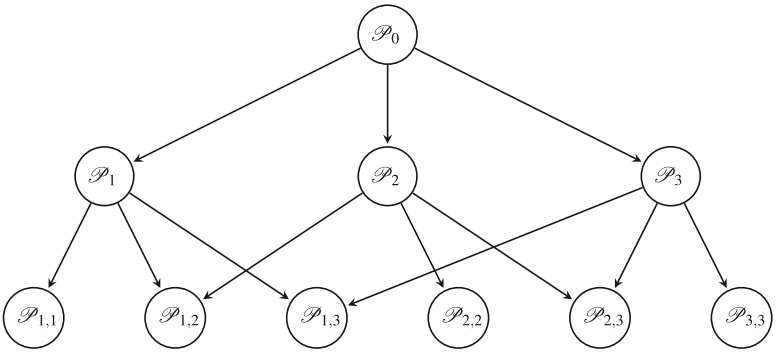

Fig. 2 The structure of a secret sharing scheme that can be constructed from a polynomial $g(x_1, x_2, x_3)$

Table 1 The distributed shares for the participants of the scheme that can be constructed from the polynomial g_1

Level of participant	Type of share
$\mathscr{P}_0$	$g_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2 + a_3x_1x_2 + S$
$\mathscr{P}_1$	$\frac{\partial g_1}{\partial x_1} = 2a_1x_1 + a_3x_2$
$\mathscr{P}_2$	$\frac{\partial g_1}{\partial x_2} = 2a_2x_2 + a_3x_1$
$\mathscr{P}_{1,1}$	$\frac{\partial^2 g_1}{\partial x_1^2} = 2a_1$
$\mathscr{P}_{1,2}$	$\frac{\partial^2 g_1}{\partial x_1 \partial x_2} = a_3$
$\mathscr{P}_{2,2}$	$\frac{\partial^2 g_1}{\partial x_2^2} = 2a_2$

Remark 6. In order to reconstruct S from the shares we have to tackle the multivariate Birkhoff interpolation problem. The set of levels is a partially ordered set, namely an upper semilattice. The level P is "greater" (or "higher") than the level Q, $P \succ Q$ means that a participant from P can replace a participant from Q.

The main idea of our approach is illustrated in the following examples.

5.2 Illustrative Examples

We consider the following polynomial:

$$g_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2 + a_3x_1x_2 + S. \tag{12}$$

By taking the first-order partial derivatives of the polynomial g_1 we get the polynomials that give the shares of the $\mathscr{P}_i$, $i = 1, 2$ level participants. Subsequently, by taking the second-order partial order derivatives we get the values of the shares of the $\mathscr{P}_{i,j}$, $i, j = 1, 2$ level participants. The shares that are distributed to the participants are exhibited in Table 1 while the consequent structure is the same as exhibited in Fig. 1.

Working in the same manner, we are able to construct a plethora of structures that represent the hierarchical relationship between participants in a secret sharing scheme. For example, we consider the following polynomial:

$$g_2(x_1, x_2, x_3) = a_1x_1x_2 + a_2x_2x_3 + a_3x_1x_3 + S. \tag{13}$$

The partial derivatives of the polynomial g_2 are used as the distributed shares of Table 2. The structure of the resulted secret sharing scheme is exhibited in Fig. 3.

Next, we present two additional illustrative examples by considering the polynomials:

$$g_3(x_1, x_2, x_3) = \lambda(x_1^2 + x_2^2 + x_3^2) + a_1x_1 + a_2x_2 + a_3x_3 + S, \tag{14}$$

and

$$g_4(x_1, x_2) = ax_1^3 + bx_1^2 + cx_1 + ax_2^2 + dx_2 + S. \tag{15}$$

Table 2 The distributed shares for the participants of the scheme that can be constructed from the polynomial g_2

Level of participant	Type of share
$\mathscr{P}_0$	$g_2(x_1, x_2, x_3) = a_1x_1x_2 + a_2x_2x_3 + a_3x_1x_3 + S$
$\mathscr{P}_1$	$\frac{\partial g_2}{\partial x_1} = a_1x_2 + a_3x_3$
$\mathscr{P}_2$	$\frac{\partial g_2}{\partial x_2} = a_1x_1 + a_2x_3$
$\mathscr{P}_3$	$\frac{\partial^2 g_2}{\partial x_3} = a_2x_2 + a_3x_1$
$\mathscr{P}_{1,2}$	$\frac{\partial^2 g_2}{\partial x_1 \partial x_2} = a_1$
$\mathscr{P}_{2,3}$	$\frac{\partial^2 g_2}{\partial x_2 \partial x_3} = a_2$
$\mathscr{P}_{1,3}$	$\frac{\partial^2 g_2}{\partial x_1 \partial x_3} = a_3$

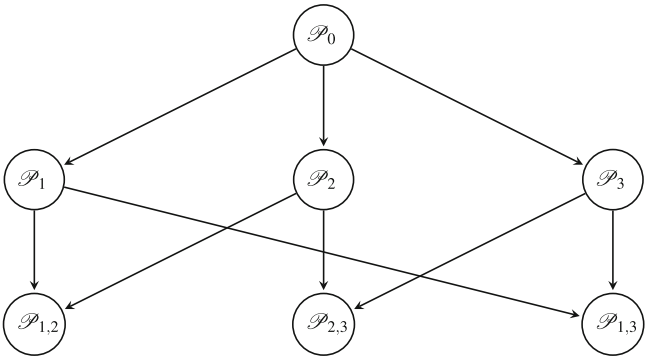

Fig. 3 The structure of a secret sharing scheme that can be constructed from the polynomial g_2

Table 3 The distributed shares for the participants that can be constructed from the polynomial g_3

Level of participant	Type of share
$\mathscr{P}_0$	$g_3(x_1, x_2, x_3) = \lambda(x_1^2 + x_2^2 + x_3^2) + a_1x_1 + a_2x_2 + a_3x_3 + S$
$\mathscr{P}_1$	$\frac{\partial g_3}{\partial x_1} = 2\lambda x_1 + a_1$
$\mathscr{P}_2$	$\frac{\partial g_3}{\partial x_2} = 2\lambda x_2 + a_2$
$\mathscr{P}_3$	$\frac{\partial g_3}{\partial x_3} = 2\lambda x_3 + a_3$
$\mathscr{P}_{xx} = \mathscr{P}_{1,1} = \mathscr{P}_{2,2} = \mathscr{P}_{3,3}$	$\frac{\partial^2 g_3}{\partial x_1^2} = \frac{\partial^2 g_3}{\partial x_2^2} = \frac{\partial^2 g_3}{\partial x_3^2} = 2\lambda$

Table 4 The distributed shares for the participants that can be constructed from the polynomial g_4

Level of participant	Type of share
$\mathscr{P}_0$	$g_4(x_1, x_2) = ax_1^3 + bx_1^2 + cx_1 + ax_2^2 + dx_2 + S$
$\mathscr{P}_1$	$\frac{\partial g_4}{\partial x_1} = 3ax_1^2 + 2bx_1 + c$
$\mathscr{P}_{11}$	$\frac{\partial^2 g_4}{\partial x_1^2} = 6ax_1 + 2b$
$\mathscr{P}_2$	$\frac{\partial g_4}{\partial x_2} = 2ax_2 + d$
$\mathscr{P}' = \mathscr{P}_{1,1,1} = \mathscr{P}_{2,2}$	$\frac{\partial^3 g_4}{\partial x_1^3} = 3\frac{\partial^2 g_4}{\partial x_2^2} = 6a$

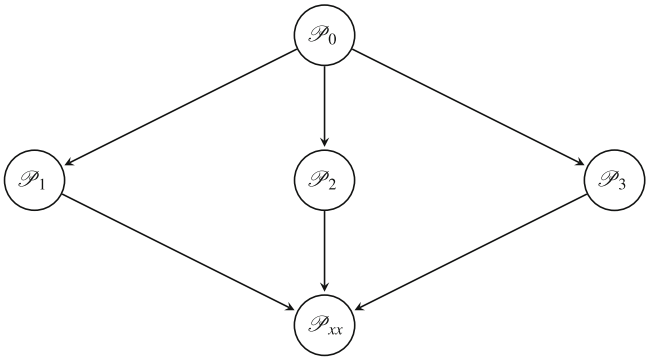

Fig. 4 The structure of a secret sharing scheme that can be constructed from the polynomial g_3

In Tables 3 and 4 we present, respectively, the shares that are distributed to the participants. The corresponding structures are exhibited in Figs. 4 and 5.

5.3 The Linear Polynomial Case

In this subsection we present a ***threshold*** $(n + 1)$***-level partially ordered secret sharing scheme***. To this end, we consider the scheme that is derived from an n-variable linear polynomial of the following form:

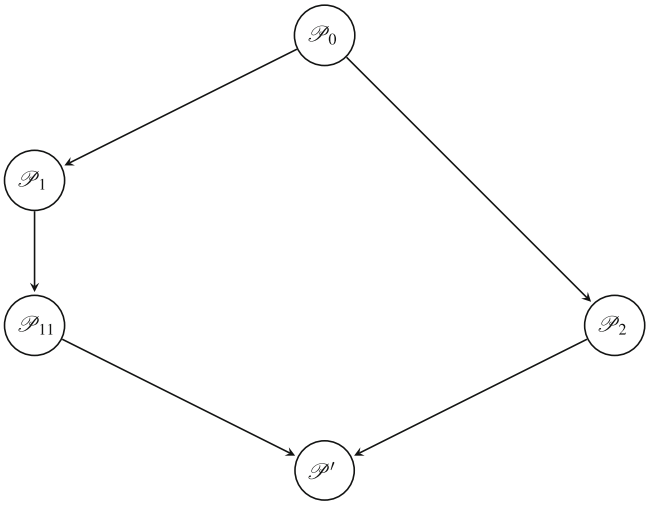

Fig. 5 The structure of a secret sharing scheme that can be constructed from the polynomial g_4

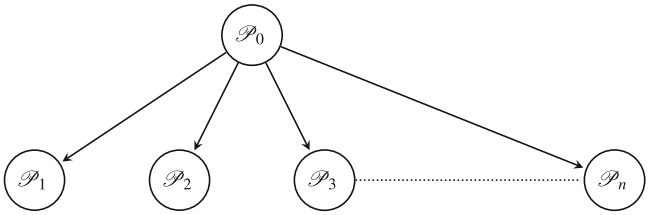

Fig. 6 The structure of a partially ordered $(\boldsymbol{\kappa}, 2n+1)$ threshold secret sharing scheme with $\boldsymbol{\kappa} = (1, n+1)$

$$g(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n + S, \tag{16}$$

where $a_1, a_2, \ldots, a_n$ are the coefficients of the polynomial g and S is the constant term of the polynomial that represents the secret key. The partial order which is defined has the structure exhibited in Fig. 6.

The information piece (share) for participants from $\mathscr{P}_0$ is unique. Therefore, without loss of generality we assume that $\mathscr{P}_j$ has exactly one participant $|\mathscr{P}_j| = 1$. Also, without loss of generality we assume that $\mathscr{P}_0$ contains $n+1$ participants, which determines the minimal number for reconstructing the secret S.

The specific structure has two important properties:

(a) None of the participants of a level $\mathscr{P}_j, j \neq 0$ can replace a participant of a level $\mathscr{P}_i, i \neq 0, j$. Thus, we say that we have a ***partially ordered structure***.
(b) ***Participants of the level $\mathscr{P}_0$ can replace whichever participant*** of the structure such that an authorized subset can be constructed.

The following algorithm describes the corresponding secret sharing scheme:

Algorithm 3

1. **Initialization phase:** The dealer selects the following polynomial:

$$g(x_1, x_2, \ldots, x_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n + S, \tag{17}$$

where a_i are elements that are chosen randomly from a finite field $\mathbb{F}_q$ and q is a large prime power. The participants are identified by the dealer so that each participant from $\mathscr{P}_0$ is identified with the n-tuple $(x_{1,k}, x_{2,k}, \ldots, x_{n,k}) \in \mathbb{F}_q^n$ after a suitable selection of the $x_{i,k}$ and each participant from $\mathscr{P}_j$, $1 \leqslant j \leqslant n$ is identified with the index j.

2. **Secret sharing phase:** The dealer distributes the shares so that each participant from $\mathscr{P}_0$ receives the value:

$$y_k = g(x_{1,k}, x_{2,k}, \ldots, x_{n,k}) \in \mathbb{F}_q, \tag{18}$$

and each participant from $\mathscr{P}_j$ receives the value:

$$a_j = \frac{\partial g}{\partial x_j}. \tag{19}$$

3. **Secret reconstruction phase:** A subset B of participants will pull their shares and attempt to reconstruct S. This can be done by solving a system of linear equations. The unknowns are the coefficients a_i as well as the element S. The participants from $\mathscr{P}_0$ will pull their equation:

$$y_k = \sum_{i=1}^{n} a_i x_{i,k} + S. \tag{20}$$

The participants from $\mathscr{P}_j$, $1 \leqslant j \leqslant n$ will pull the value:

$$a_j = \frac{\partial g}{\partial x_j}. \tag{21}$$

If the $x_{i,k}$ with $1 \leqslant i \leqslant n$ and $1 \leqslant k \leqslant n+1$ are suitably chosen from a finite field, then a unique solution exists for S if B is an authorized subset, $|B| \geqslant n+1$.

Next, we define a class of matrices on which our scheme is based.

Definition 5. An $n \times n$ matrix is called a ***principally nonsingular matrix*** if every principal submatrix is nonsingular. Also, an $n \times n$ matrix is said to be a ***totally nonsingular matrix*** if all its square submatrices are nonsingular.

Remark 7. This class of matrices contains the ***totally negative matrices***, whose the determinant of the corresponding minors is strictly negative, and the ***totally positive matrices*** whose the determinant of the corresponding minors is strictly positive. If we allow the existence of null minors, these classes can be extended to the ***totally nonpositive matrices*** as well as to the ***totally nonnegative matrices***.

The following theorem gives necessary and sufficient conditions for accessibility and perfect security of the scheme:

Theorem 1. *Consider the following* $(n+1)\times(n+1)$ *matrix:*

$$X_1 = \begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{n,1} & 1 \\ x_{1,2} & x_{2,2} & \cdots & x_{n,2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{1,n} & x_{2,n} & \cdots & x_{n,n} & 1 \\ x_{1,n+1} & x_{2,n+1} & \cdots & x_{n,n+1} & 1 \end{pmatrix}. \tag{22}$$

Then, the accessibility and perfect security are satisfied iff the matrix X_1 *is totally nonsingular.*

Proof. Let us denote by X the following matrix:

$$X = \begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{n,1} \\ x_{1,2} & x_{2,2} & \cdots & x_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,n} & x_{2,n} & \cdots & x_{n,n} \\ x_{1,n+1} & x_{2,n+1} & \cdots & x_{n,n+1} \end{pmatrix}. \tag{23}$$

We consider the following cases:

Case 1: *All participants belong to the level* $\mathscr{P}_0$.

According to the assumptions of the theorem all the rows of X and X_1 are linearly independent. Retrieving the secret S amounts to the solution of the following system:

$$\sum_{i=1}^{n} a_i x_{i,j} + S = y_j, \quad j = 1, 2, \ldots, n+1. \tag{24}$$

The matrix X_1 is the coefficient matrix of the system and the elements $a_1, a_2, \ldots, a_n, S$ are the unknowns. The condition $\det(X_1) \neq 0$ implies existence of a unique solution and the secret S can be retrieved. Thus, the **accessibility is satisfied**.

Let B be a set of participants with $|B| = n$. It corresponds to a set of n rows of X, namely $\{(x_{1,j_k}, x_{2,j_k}, \ldots, x_{n,j_k})\}$, $k = 1, 2, \ldots, n$. The unknown S can be treated as a parameter. For any randomly chosen value S_0 of S we derive the following linear system:

$$\sum_{i=1}^{n} a_i x_{i,j_k} = y_{j_k} - S_0, \quad k = 1, 2, \ldots, n. \tag{25}$$

Its coefficient matrix is an $n \times n$ minor of X. According to the assumptions it has exactly one solution for all S_0, therefore no information can be revealed about S. Thus, the **perfect security is satisfied**.

For a set B of m participants, $|B| = m \leqslant n$ the same technique can be used. The corresponding set of rows of X is $\{(x_{1,j_k}, x_{2,j_k}, \ldots, x_{n,j_k})\}$, $k = 1, 2, \ldots, m$, which are linearly independent due to the assumption. The following linear system of m equations:

$$\sum_{i=1}^{n} a_i x_{i,j_k} = y_{j_k} - S_0, \quad k = 1, 2, \ldots, m, \tag{26}$$

has exactly q^{n-m} solutions (where q is the cardinality of the finite field $\mathbb{F}_q$) and no information can be obtained about S.

For the inverse part of the proof, let us assume that the conditions of accessibility and perfect security are satisfied. On the contrary, assume that $\det(X_1) = 0$. Also, let us assume that the linear system (24) has more than one solutions and a unique value can be found for the unknown S, which is possible. This implies that at least one of the equations of the system (24) can be removed and that n or less than n participants can reveal the secret S, which is a contradiction to the assumption of perfect security. Therefore, the rows of X_1 are linearly independent.

Again, on the contrary, assume that m rows of X, $m < n + 1$ are linearly dependent, namely the rows $\{(x_{1,j_k}, x_{2,j_k}, \ldots, x_{n,j_k})\}$, $k = 1, 2, \ldots, m$. However the corresponding rows $\{(x_{1,j_k}, x_{2,j_k}, \ldots, x_{n,j_k}1, 1)\}$, $k = 1, 2, \ldots, m$ of X_1 are linearly independent and S can be retrieved from m participants which is a contradiction to the assumption of perfect security.

We conclude that matrix X_1 is invertible and that all submatrices $n \times n$ minors of X are invertible.

Case 2: *Some of the participants belong to the levels* $\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_n$.

This case can be treated as the Case 1. Assume that r participants, $r \leqslant n$, belong to the levels $\mathscr{P}_{t_1}, \mathscr{P}_{t_2}, \ldots, \mathscr{P}_{t_r}$, where $\{t_1, t_2, \ldots, t_r\} \subseteq \{1, 2, \ldots, n\}$ and that the remaining $n + 1 - r$ participants belong to the level $\mathscr{P}_0$. The share of the participant of the level $\mathscr{P}_{t_l}$, $1 \leqslant l \leqslant r$, is $a_{t_l} = \frac{\partial g}{\partial x_{t_l}}$ and the t_l-th column has to be deleted from the matrix X_1. The new obtained matrix X_1' has $n + 1 - r$ rows corresponding to the $n + 1 - r$ participants from $\mathscr{P}_0$, and $n + 1 - r$ columns after the deletion of r columns. The new matrix X' is $(n + 1 - r) \times (n - r)$. The rest of the proof is similar to the Case 1.

Thus the theorem is proved. □

Remark 8. Obviously, the scheme is also ***ideal***, since every participant receives a field element, just like the secret.

Remark 9. For the implementation of the scheme a totally nonsingular matrix is required which can be obtained from a totally positive matrix [7] over the reals. The well-known ***Hilbert matrix***:

$$H = \begin{pmatrix} 1 & \frac{1}{2} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n} & \frac{1}{n+1} & \cdots & \frac{1}{2n-1} \end{pmatrix}, \tag{27}$$

is totally positive [16]. Also, totally nonsingular matrices can be derived from the ***Vandermonde matrix*** under specific conditions [9].

Next, we present an illustrative example. To this end, we consider the structure exhibited in Fig. 7 with which we represent a $(\boldsymbol{\kappa}, 7)$ four-level threshold partially ordered secret sharing scheme with $\boldsymbol{\kappa} = (1, 4)$. In order to construct the scheme we use the Hilbert matrix. For this case the corresponding algorithm of our approach is the following:

5.4 Perspectives for Future Work

Multivariate Birkhoff interpolation over large degree polynomials is a challenge to build multilevel threshold secret sharing schemes with partially ordered sets of levels. The ordered set, exhibited in Fig. 8, represents the structure of a multilevel partially ordered threshold secret scheme.

Observing this special structure a general question has to be answered: *Given a scheme with a partially ordered set of levels as above, is it always feasible to find a multivariate polynomial, such that the order is derived from the polynomial ?*

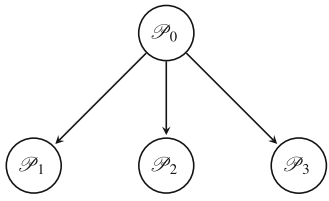

Fig. 7 The structure of a partially ordered $(\boldsymbol{\kappa}, t)$ four-level threshold secret sharing scheme with $\boldsymbol{\kappa} = (1, 4)$

Algorithm 4

1. **Initialization phase:** The dealer selects a polynomial of the form:

$$g(x_1, x_2, x_3) = \sum_{i=1}^{3} a_i x_i + S, \tag{28}$$

where a_i are chosen randomly over a finite field $\mathbb{F}_q$. Let us assume that $a_1 = 2, a_2 = 4, a_3 = 5$ and $q = 11$. Suppose further that the secret S is 8. Participants are identified by the dealer so that each participant from $\mathscr{P}_0$ is identified with the first 3 elements of a row of the 4×4 matrix which has been resulted after the transformation, with row multiplication, of the last column of the 4×4 Hilbert matrix to a vector of ones, and each participant from $\mathscr{P}_j$, $1 \leqslant j \leqslant 3$ with the index j.

2. **Secret sharing phase:** The dealer distributes the shares so that each participant from $\mathscr{P}_0$ receives the value:

$$y_k = g(x_{1,k}, x_{2,k}, x_{3,k}) \in \mathbb{F}_{11}, \tag{29}$$

and each participant from $\mathscr{P}_j$ receives the value:

$$a_j = \frac{\partial g}{\partial x_j}. \tag{30}$$

The distributed shares are shown in Table 5.

3. **Secret reconstruction phase:** Suppose now that we have an authorized set which consists of 2 participants of the level $\mathscr{P}_0$ and 2 participants of the levels $\mathscr{P}_j$, $1 \leqslant j \leqslant 3$. For example we assume that we have the subset $\{p_0^1, p_0^3, p_1, p_2\}$. Since p_1, p_2 are elements of the specific subset, a_1 and a_2 are the coefficients that we can obtain directly. Due to the presence of participants p_0^1 and p_0^3 in the set, we obtain the following linear system:

$$a_1 x_{1,1} + a_2 x_{2,1} + a_3 x_{3,1} + S = y_1,$$

$$a_1 x_{1,3} + a_2 x_{2,3} + a_3 x_{3,3} + S = y_3,$$

$$a_1 = 2,$$

$$a_2 = 4.$$

By substituting $x_{i,k}$ with the corresponding elements of the transformed Hilbert and y_j with the values of the shares, we rewrite the system as follows:

$$4a_1 + 2a_2 + 5a_3 + S = 5,$$

$$2a_1 + 7a_2 + 10a_3 + S = 2,$$

$$a_1 = 2,$$

$$a_2 = 4.$$

By computing the inverses over finite field $\mathbb{F}_{11}$ we finally get $S = 8$ which is the correct value.

Table 5 The distributed shares for the participants of the scheme of Fig. 7

Participant	Value of share
p_0^1	5
p_0^2	3
p_0^3	2
p_0^4	9
p_1	2
p_2	4
p_3	5

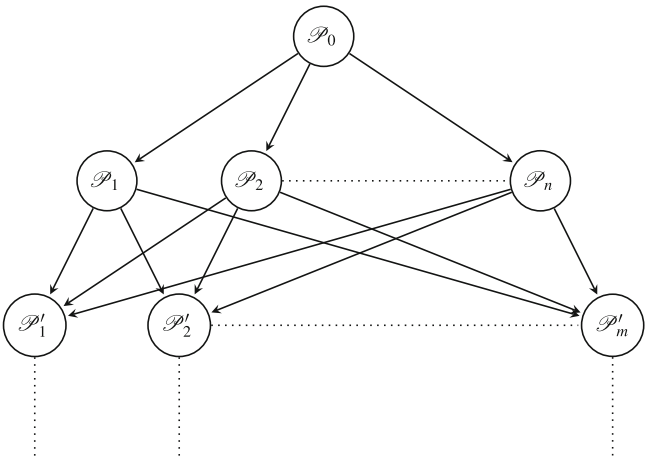

Fig. 8 The structure of a partially ordered threshold secret sharing scheme

6 Synopsis

In the work at hand, we investigated the adaptation of multivariate Birkhoff interpolation problem for the construction simple secret sharing schemes. The resulted structures consist of partially ordered levels of participants. For a simple linear polynomial with n variables, the secret sharing scheme that can be constructed is perfect with the usage of totally nonsingular matrices which ensure both correctness and perfect security.

Finally we posed the analogous generalized problem, which implies the construction of specific structures with polynomials through the multivariate Birkhoff interpolation problem.

References

1. Ballico, E., Boato, G., Fontanari, C., Granelli, F.: Hierarchical secret sharing in ad hoc networks through Birkhoff interpolation. In: Elleithy, K., Sobh, T., Mahmood, A., Iskander, M., Karim, M. (eds.) Advances in Computer, Information, and Systems Sciences, and Engineering, pp. 157–164. Springer, Dordrecht (2006)
2. Beimel, A.: Secret-sharing schemes: a survey. Lect. Notes Comput. Sci. **6639**, 11–46 (2011)
3. Benaloh, J.C., Leichter, J.: Generalized secret sharing and monotone functions. Lect. Notes Comput. Sci. **403**, 27–36 (1990)
4. Birkhoff, G.D.: General mean value and remainder theorems with applications to mechanical differentiation and quadrature. Trans. Am. Math. Soc. **7**, 107–136 (1906)
5. Blakley, G.R.: Safeguarding cryptographic keys. In: Proceedings of the 1979 AFIPS National Computer Conference, vol. 48, pp. 313–317. AFIPS Press, Montvale, NJ (1979)
6. Brickel, E.F.: Some ideal secret sharing schemes. J. Combin. Math. Combin. Comput. **6**, 105–113 (1989)
7. Carnicer, J.M.: Interpolation shape control and shape properties. In: Peña, J.M. (ed.) Shape Preserving Representations in Computer-Aided Geometric Design, Chapter 2, pp. 15–43. Nova Science Publishers, Commack, NY (1999)
8. Crainic, M., Crainic, N.: Pólya conditions for multivariate Birkhoff interpolation: from general to rectangular sets of nodes. Acta Math. Univ. Comenianae **79**(1), 9–18 (2010)
9. Demmel, J., Koev, P.: The accurate and efficient solution of a totally positive generalized Vandermonde linear system. SIAM J. Matrix Anal. Appl. **27**(1), 142–152 (2005)
10. Desmedt, Y., Frankel, Y.: Shared generation of authenticators and signatures. Lect. Notes Comput. Sci. **576**, 457–469 (1992)
11. Farràs, O., Padró, C.: Ideal hierarchical secret sharing schemes. Lect. Notes Comput. Sci. **5978**, 219–236 (2010)
12. Farràs, O., Padró, C.: Ideal hierarchical secret sharing schemes. IEEE Trans. Inform. Theory **58**(5), 3273–3286 (2012)
13. Hei, X.-L., Du, X.-J., Song, B.-H.: Two matrices for Blakley's secret sharing scheme. In: Proceedings of the 2012 IEEE International Conference on Communications (ICC), pp. 810–814. IEEE (2012)
14. Lorentz, R.A.: Multivariate Birkhoff Interpolation. Lecture Notes in Mathematics Series, vol. 1516. Springer, Berlin/Heidelberg (1992)
15. Lorentz, G.G., Jetter, K., Riemenschneider, S.D.: Birkhoff Interpolation. Encyclopedia of Mathematics and Its Applications, vol. 19. Addison-Wesley, Reading (1982)
16. Peña, J.M.: Stability and error analysis of shape preserving representations. In: Peña, J.M. (ed.) Shape Preserving Representations in Computer-aided Geometric Design, Chapter 5, pp. 85–97. Nova Science Publishers, Commack, NY (1999)
17. Pólya, G.: Bemerkung zur Interpolation und zur Naherungstheorie der Balkenbiegung. Z. Angew. Math. Mech. **11**, 445–449 (1931)
18. Rouillier, F., El Din, M.S., Schost, E.: Solving the Birkhoff interpolation problem via the critical point method. Lect. Notes Artif. Intell. **2061**, 26–40 (2001)
19. Schoenberg, I.J.: On Hermite-Birkhoff interpolation. J. Math. Anal. Appl. **16**, 538–543 (1966)
20. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
21. Stinson, D.R.: An explication of secret sharing schemes. Designs Codes Cryptogr. **2**(4), 357–390 (1992)
22. Tassa, T.: Hierarchical threshold secret sharing. J. Cryptol. **20**(2), 237–264 (2007)