INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences

ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 708 (2009)

Stanisław Spież
Marian Srebrny
Jerzy Urbanowicz

Secret Sharing Matrices

Published as manuscript

Received 09 September 2009

Secret Sharing Matrices

Stanisław Spież* Marian Srebrny† Jerzy Urbanowicz‡

Abstract

We consider a secret sharing scheme given in terms of the secret sharing matrices which are introduced and investigated in this paper. The secret sharing matrices enable secret sharing with several secrets. The participants can use the same shares to recover more than one secret. We show that the secret sharing matrices provide a practical secret sharing scheme not necessarily determined by polynomial interpolation. Using Gaussian elimination we give some algorithms for constructing and extending all such matrices. The obtained scheme generalizes the original Shamir's scheme and its generalization due to Lai and Ding [5]. We also answer some of the questions of [5].

Key words. Secret sharing, key management, multiparty computation, threshold cryptography, polynomial interpolation, finite fields, generalized Vandermonde determinants, elementary symmetric polynomials, Gaussian elimination.

1 Introduction

Secret sharing, introduced by Shamir [11] and Blakley [2] independently in 1979, refers to methods for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. In a k-out-of-n scheme a dealer (or admin) gives some secret data (typically a cryptographic secret key) D to n players by dividing it into n shadow shares $D_0, D_1, \ldots, D_{n-1}$ and distributing one of them to each of the players in such a way that any group of k (threshold) or more players can collectively efficiently reconstruct the secret but no coalition of less than k players can get any information on D at all.

*Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland; spiez@impan.gov.pl

†Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland; M.Srebrny@ipipan.waw.pl

‡Institute of Computer Science, Polish Academy of Sciences, and Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland; J.Urbanowicz@ipipan.waw.pl; Corresponding author.

Let p be a large prime number and let $k \leq n < p$. The original secret sharing scheme introduced by Shamir [11] is based on the polynomial interpolation theorem in the field $\mathbb{F}_p$. Here we consider some secret sharing schemes based on an arbitrary finite field $\mathbb{F}$. One can think of Shamir's secret sharing scheme as determined by the standard polynomial basis $\mathcal{B}_{poly} = \{1, t, t^2, \ldots, t^{k-1}\}$ in the linear subspace of polynomials of degree $< k$ in the vector space $\mathbb{F}[t]$ over $\mathbb{F}$ and a set of n points in $\mathbb{F}^2$.

The admin of the system chooses a (pseudo)random sequence of coefficients $a_1, \ldots, a_{k-1} \in \mathbb{F}$ which (with given $a_0 = D$) can be identified with the polynomial $q(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_{k-1} t^{k-1}$ (a linear combination of the elements of $\mathcal{B}_{poly}$). Next he computes and distributes as the shares n points $D_0 = (t_0, y_0)$, $D_1 = (t_1, y_1)$, $\ldots$, $D_{n-1} = (t_{n-1}, y_{n-1})$ of the graph of q with non-zero pairwise different $t_0, t_1, \ldots, t_{n-1} \in \mathbb{F}$ applying the matrix equation

$$\begin{pmatrix} t_0^0 & t_0^1 & \ldots & t_0^{k-1} \\ t_1^0 & t_1^1 & \ldots & t_1^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n-1}^0 & t_{n-1}^1 & \ldots & t_{n-1}^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{pmatrix}.$$

In the original Shamir secret sharing scheme $\mathbb{F} = \mathbb{F}_p$ and the t_i's are integers such that $0 < t_0 < t_1 < \cdots < t_{n-1} < p$. Let $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ be an n-tuple over $\mathbb{F}$. The matrix $\mathbf{A}_{poly}(\mathbf{t}) = \left(t_i^j\right)_{0 \leq i \leq n-1,\, 0 \leq j \leq k-1}$ is uniquely determined by the standard polynomial basis $\mathcal{B}_{poly}$ and the tuple $\mathbf{t}$.

The shares in Shamir's secret sharing scheme can be also identified with the pairs $D_0 = (\mathbf{r}_0, y_0)$, $D_1 = (\mathbf{r}_1, y_1)$, $\ldots$, $D_{n-1} = (\mathbf{r}_{n-1}, y_{n-1})$, where $\mathbf{r}_i = (t_i^0, t_i^1, \ldots, t_i^{n-1})$ for $0 \leq i \leq n-1$) is the i-th row of $\mathbf{A}_{poly}(\mathbf{t})$. In this paper we generalize Shamir's scheme in such a way that the admin distributes as the shares the pairs $(\mathbf{r}_i, y_i)$, where $\mathbf{r}_i \in \mathbb{F}^k$ is the i-th row of a secret sharing matrix $\mathbf{A} = (\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n-1})^T$ introduced in the paper and $y_i = \mathbf{r}_i \cdot \mathbf{a}$ for $0 \leq i \leq n-1$.

By definition a secret sharing matrix is said to be at level i if one can use it to construct a secret sharing scheme with the secret placed as the i-th coefficient of the vector $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1})$ (Definition 1). If such a matrix allows placement of the secret as an arbitrary a_i $(0 \leq i \leq k-1)$, then we call it an all-level secret sharing matrix (Definition 2).

We show that if card($\mathbb{F}$) is sufficiently large the entries of a secret sharing matrix $\mathbf{A}$ can be chosen at random. On the other hand, we give fast deterministic algorithms for constructing such matrices based on Gaussian elimination. The shares can be also identified, as in Blakley's scheme [2], with some $(k-1)$-dimensional hyperplanes $\mathcal{H}_i = \{\mathbf{a} \in \mathbb{F}^k \colon \ \mathbf{r}_i \cdot \mathbf{a} = y_i\}$

$(0 \le i \le n-1)$ in $\mathbb{F}^k$. Since every k of the hyperplanes intersect at a specific point, the secret may be encoded as any single coordinate of the point of intersection. However, as one of the results of this paper, some of the coordinates may not be secure enough since in some cases less than k shares could be enough to reconstruct the secret.

Shamir's secret sharing matrix $\mathbf{A}_{poly}(\mathbf{t})$ for $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}^n$ is an example of a more general secret sharing matrix – the Shamir type secret sharing matrix $\mathbf{A}_{\mathcal{B}}(\mathbf{t})$ (Definition 4). This matrix is related to a basis $\mathcal{B} = \{v_0(t), v_1(t), \ldots, v_{k-1}(t)\}$ in the linear subspace of polynomials of degree $< k$ in the vector space $\mathbb{F}[t]$ over $\mathbb{F}$. We have $\mathbf{A}_{\mathcal{B}}(\mathbf{t}) = (\mathbf{r}_0(\mathbf{t}), \mathbf{r}_1(\mathbf{t}), \ldots, \mathbf{r}_{n-1}(\mathbf{t}))^T$, where $\mathbf{r}_i(\mathbf{t}) = (v_0(t_i), v_1(t_i), \ldots, v_{n-1}(t_i))$. Another example of the Shamir type secret sharing matrix is the matrix $\mathbf{A}_{binom}(\mathbf{t}) = \left(\binom{t_i}{j}\right)_{0 \le i \le n-1,\, 0 \le k \le k-1}$, corresponding to the binomial basis $\mathcal{B}_{binom} = \left\{\binom{t}{0}, \binom{t}{1}, \ldots, \binom{t}{k-1}\right\}$.

Generally, we have $\mathbf{A}_{\mathcal{B}}(\mathbf{t}) = \mathbf{A}_{poly}(\mathbf{t})\mathbf{M}$ with some $k \times k$ non-singular matrix $\mathbf{M}$ over $\mathbb{F}$ (which is the change-of-basis matrix of the bases $\mathcal{B}$ and $\mathcal{B}_{poly}$). For example, the change-of-basis matrices of the bases $\mathcal{B}_{poly}$ and $\mathcal{B}_{binom}$ consist of the Stirling numbers of the first or second kind. For more details see [10].

We also consider some secret sharing schemes related to the bases $\mathcal{B}$ of a k-dimensional vector subspace of polynomials of degree $< K$ (with some $K \ge k$) in the vector space $\mathbb{F}[t]$ over $\mathbb{F}$. Throughout the paper we denote this subspace by $\mathbb{F}[t]_{<K}$. An example of such a basis is $\mathcal{B}_{\mathbf{c}} = \{t^{c_0}, t^{c_1}, \ldots, t^{c_{k-1}}\}$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ is an increasing sequence of non-negative integers with $K = c_{k-1} + 1$. The secret sharing schemes corresponding to the bases $\mathcal{B}_{\mathbf{c}}$ with some special $\mathbf{c}$ were considered by Lai and Ding [5] who generalized Shamir's scheme using a more general polynomial $q(t) = a_0 t^{c_0} + a_1 t^{c_1} + \cdots + a_{k-1} t^{c_{k-1}}$, for some special $\mathbf{c}$.

In the sequel we write $\mathbf{e}_n$ for the standard n-th tuple $(0, 1, \ldots, n-1)$. Every coalition of k participants with the shares $D_{\rho_0} = (t_{\rho_0}, y_{\rho_0})$, $D_{\rho_1} = (t_{\rho_1}, y_{\rho_1})$, $\ldots$, $D_{\rho_{k-1}} = (t_{\rho_{k-1}}, y_{\rho_{k-1}})$ for a subsequence $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-1})$ of $\mathbf{e}_n$, can recover the secret because the determinant of the $k \times k$ submatrix of the matrix $\mathbf{A}_{poly}(\mathbf{t})$ consisting of the rows $\mathbf{r}_{\rho_0}(\mathbf{t})$, $\mathbf{r}_{\rho_1}(\mathbf{t})$, $\ldots$, $\mathbf{r}_{\rho_{k-1}}(\mathbf{t})$ is the classical Vandermonde determinant $\prod_{0 \le j < i \le k-1} \left(t_{\rho_i} - t_{\rho_j}\right)$, which is $\ne 0$ in $\mathbb{F}$ whenever $t_{\rho_i} \ne t_{\rho_j}$. This means that the $k \times k$ submatrix of $\mathbf{A}_{poly}(\mathbf{t})$ is non-singular and the matrix equation

$$\begin{pmatrix} t_{\rho_0}^0 & t_{\rho_0}^1 & \ldots & t_{\rho_0}^{k-1} \\ t_{\rho_1}^0 & t_{\rho_1}^1 & \ldots & t_{\rho_1}^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ t_{\rho_{k-1}}^0 & t_{\rho_{k-1}}^1 & \ldots & t_{\rho_{k-1}}^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} y_{\rho_0} \\ y_{\rho_1} \\ \vdots \\ y_{\rho_{k-1}} \end{pmatrix}$$

has the unique solution $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$.

Since the secret is placed as $D = a_0$ and $t_{\rho_i} \neq 0$, for all $0 \leq i \leq k-1$, to recover the secret by the polynomial interpolation formula we have to use all the shares y_{ρ_i} $(0 \leq i \leq k-1)$. This means that all the y_{ρ_i} $(0 \leq i \leq k-1)$ play essential role in recovering the secret and no coalition of less than k shareholders can recover it.

In the paper we study the above matrix equations for an arbitrary $n \times k$ secret sharing matrix $\mathbf{A} = (\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n-1})^T$ over $\mathbb{F}$ with the secret placed as $D = a_i$ for a fixed $0 \leq i \leq k-1$, both in a general case and in the case when $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(\mathbf{t})$ (in particular if $\mathbf{A} = \mathbf{A}_{poly}(\mathbf{t})$) (Theorems 1 and 2).

Our approach was inspired by Blakley [2] and Shamir [11], and by a short note in Koblitz [4], Chapter I, §5, p. 10. As for the other related work, in secret sharing the Chinese Remainder Theorem can also be used, as proposed by Asmuth and Bloom [1] and Mignotte [6]. In [1] the shares are generated by reduction of D modulo some n coprime positive integers $m_0, m_1, \ldots, m_{n-1}$ such that $D < \prod_{i=0}^{k-1} m_{\rho_i}$, for all subsequences $(\rho_0, \rho_1, \ldots, \rho_{k-1})$ of the sequence $(0, 1, \ldots, n-1)$. The secret is recovered by solving the system of k or more congruences using the Chinese Remainder Theorem in $\mathbb{Z}$ which provides a method to uniquely determine D modulo $\prod_{i=0}^{k-1} m_{\rho_i}$.

Asmuth-Bloom's arithmetical scheme and Shamir's polynomial scheme are special cases of a more general secret sharing scheme based on the Chinese Remainder Theorem in a ring A. See [7]. In the scheme of [1] $A = \mathbb{Z}$. In the scheme of [11] $A = \mathbb{F}_p[t]$. Then the Chinese Remainder Theorem is the Lagrange Interpolation Theorem on polynomials.

The paper is organized as follows. In section 2 we set up notation and terminology, and introduce the concept of secret sharing matrices which allow to extend Shamir's secret sharing scheme. In this section we also prove a natural intrinsic characterization of secret sharing matrices (Theorem 1). We pursue secret sharing matrices giving secret sharing schemes with the secret placed as the coefficient a_i for a fixed i, or for an arbitrary i $(0 \leq i \leq k-1)$. This enables a new feature of secret sharing that an authorized coalition can reconstruct not only one but up to k many different secrets, using the same shares.

In section 3 we consider Lai and Ding's generalization of Shamir's scheme. Answering their question, we use Theorem 1 to give necessary and sufficient conditions for placing the secret as any of the coefficients a_i for a fixed i, or for an arbitrary i (Theorem 2 with corollaries). That was an open problem of Lai and Ding [5]. To solve this problem we use some techniques concerning the generalized Vandermonde determinants and elementary symmetric polynomials.

In section 4 we give two algorithms for constructing or extending secret

sharing matrices at level i with a fixed $0 \leq i \leq k-1$ or all-level secret sharing matrices (Algorithms 4.1.1 and 4.2.1, respectively). In the algorithms we apply Gaussian elimination. All the secret sharing matrices can be constructed in this way.

In section 5 we show that not every secret sharing matrix corresponds to a basis of the vector space of polynomials of degree less than the threshold k. Thus the secret sharing matrices give some essentially new practical secret sharing schemes (Theorem 3). Making use of Theorem 1 and Lemma 2 we give examples of all-level secret sharing matrices of size $n \times k$ which are not of the Shamir type: with $n = 3$, $k = 2$, $\mathrm{char}(\mathbb{F}) > 3$ and the rows $\mathbf{r}_0 = (1, 1)$, $\mathbf{r}_1 = (1, 2)$, $\mathbf{r}_2 = (2, 3)$, or with $n = 5$, $k = 3$, $\mathrm{char}(\mathbb{F}) > 31$ and the rows $\mathbf{r}_0 = (1, 1, 1)$, $\mathbf{r}_1 = (1, 2, 4)$, $\mathbf{r}_2 = (1, 3, 9)$, $\mathbf{r}_3 = (1, 4, 16)$, $\mathbf{r}_4 = (2, 3, 1)$. Both the matrices are all-level secret sharing matrices (Theorem 1) and are not of the Shamir type (Lemma 2).

2 Secret sharing matrices

2.1 Terminology and notation

We follow the standard terminology and notation of [8]. Throughout the paper, let $\mathbb{F}$ be a (finite) field. Let n and k be natural numbers such that $k \leq n < \mathrm{card}(\mathbb{F})$. As described in the Introduction above the original secret sharing scheme of Shamir [11] can be viewed as given by a system of linear equations

$$\mathbf{A}\mathbf{a}^T = \mathbf{y}^T \tag{1}$$

with $\mathbf{A} = \mathbf{A}_{poly}(\mathbf{t})$, $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1})$, $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$.

We use the row notation for the vectors. For a vector $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ the column vector $\mathbf{c}^T$ denotes its transpose. We adhere to the convention that the indexing of rows and columns in the matrices starts with zero. We also apply this convention to the vectors.

Let $\mathbf{A}$ be an $n \times k$ matrix over $\mathbb{F}$ and let $m \in \mathbb{N}$ $(m \leq n)$, $s \in \mathbb{N}$ $(s \leq k)$. Given subsequences $\rho = (\rho_0, \rho_1, \ldots, \rho_{m-1})$ and $\gamma = (\gamma_0, \gamma_1, \ldots, \gamma_{s-1})$ of the sequences $\mathbf{e}_n$ and $\mathbf{e}_k$ respectively, we denote by $\mathbf{A}(\rho, \gamma)$ the matrix of size $m \times s$ obtained from $\mathbf{A}$ by removing all its r-th rows for $r \neq \rho_i$, $0 \leq i \leq m-1$ and all its l-th columns for $l \neq \gamma_j$, $0 \leq j \leq s-1$. In this notation, we have $\mathbf{A}(\mathbf{e}_n, \mathbf{e}_k) = \mathbf{A}$, and as usual $\mathbf{A}(i, j) = a_{ij}$ if $\mathbf{A} = (a_{ij})$. Applying the notation to the vector $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}^n$, we write $\mathbf{y}(\rho) = (y_{\rho_0}, y_{\rho_1}, \ldots, y_{\rho_{m-1}})$.

Given a sequence $\mathbf{u} = (u_0, u_1, \ldots, u_{s-1})$ and $0 \leq i \leq s-1$, denote by $\widehat{\mathbf{u}}_i$ the sequence obtained from $\mathbf{u}$ by deleting the term u_i. In particular by $\widehat{\mathbf{e}}_{s,i}$

we denote the subsequence of the sequence $\mathbf{e}_s$ with the term i deleted, and by $\mathbf{A}(\mathbf{e}_n, \widehat{\mathbf{e}}_{k,i})$ the matrix obtained from matrix $\mathbf{A}$ by deleting its i-th column.

Note that the submatrices of size $k \times k$ of the matrix $\mathbf{A} = \mathbf{A}_{poly}(\mathbf{t})$ have the form $\mathbf{A}(\rho, \mathbf{e}_k) = (t_{\rho_i}^j)_{0 \le i,j \le k-1}$, where $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-1})$ is a subsequence of the sequence $\mathbf{e}_n$. Then $\det(\mathbf{A}(\rho, \mathbf{e}_k))$ is the classical Vandermonde determinant. As in the Introduction above the submatrices are non-singular and form some consistent systems of linear equations

$$\mathbf{A}(\rho, \mathbf{e}_k)\mathbf{a}^T = (\mathbf{y}(\rho))^T\,, \tag{2}$$

with the unique solution $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}^k$.

Applying the classical Cramer and Laplace theorems to equation (2) gives

$$a_i = \frac{1}{\det(\mathbf{A}(\rho, \mathbf{e}_k))} \sum_{j=0}^{k-1} (-1)^{i+j} \det(\mathbf{A}(\widehat{\rho}_j, \widehat{\mathbf{e}}_{k,i}))y_{\rho_j}\,. \tag{3}$$

In fact formulas (3) boil down to the interpolating formulas. When the determinants of $\mathbf{A}(\widehat{\rho}_j, \widehat{\mathbf{e}}_{k,i})$ are $\neq 0$ for all $0 \le j \le k-1$, each participant's share (t_{ρ_j}, y_{ρ_j}) is clearly there and we can place the secret as the i-th coefficient a_i. This gives a characterization of such matrices.

2.2 Basic definitions

In Shamir's scheme any coalition of k or more shareholders can easily recover the secret D, but no $k-1$ or less shareholders can. The scheme is perfect and ideal; that is, knowing $k-1$ or fewer shares all values of the secret remain equally probable and the size of the shares is equal to the size of the secret. It is also extendable for new users. See [8], pp. 524–526.

The above properties of Shamir's scheme follow from the appropriate properties of the matrix $\mathbf{A}_{poly}(\mathbf{t})$. In this section we introduce some more general matrices which can be used to define a sharing scheme with the secret placed as $D = a_i$ for any $0 \le i \le k-1$ and with the same basic properties as the matrix $\mathbf{A}_{poly}(\mathbf{t})$.

Given $0 \le i \le k-1$, we say that for a given $\mathbf{A}$ and $\mathbf{y}$ the equation $\mathbf{A}\mathbf{x}^T = \mathbf{y}^T$ has solutions with the i-th component as a free variable if for any $g \in \mathbb{F}$ there exists a solution $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1})$ with $x_i = g$. If the equation is consistent and the i-th components of any two of its solutions coincide then we say that it has a unique solution in the i-th component.

First we prove a theorem which will allow us to define the secret sharing matrices. The theorem is a consequence of the following two elementary facts from linear algebra.

Proposition. *Let $\mathbb{F}$ be a field and let $\mathbf{y} \in \mathbb{F}^m$. Set $m, m' \in \mathbb{N}$, $m < m'$. Assume that all matrices in the proposition are defined over the field $\mathbb{F}$. Then, we have*

(i) *for an $m \times m$ matrix $\mathbf{B}$, the equation $\mathbf{B}\mathbf{x}^T = \mathbf{y}^T$ has a unique solution in $\mathbf{x}$ if and only if $\mathbf{B}$ is non-singular;*

(ii) *for an $m \times m'$ matrix $\mathbf{B}$ with rank m and $0 \leq i \leq m' - 1$, the equation $\mathbf{B}\mathbf{x}^T = \mathbf{y}^T$ has solutions with the i-th component as a free variable if and only if $\mathrm{rank}(\mathbf{B}(\mathbf{e}_m, \widehat{\mathbf{e}}_{m',i})) = \mathrm{rank}(\mathbf{B})$.*

Theorem 1. *Let $\mathbf{A}$ be a matrix over $\mathbb{F}$ of size $n \times k$, $2 \leq k \leq n$, $\mathbf{a} = (a_0, \ldots, a_{k-1}) \in \mathbb{F}^k$, $0 \leq i \leq k-1$. Suppose*

$$\mathbf{y} = (\mathbf{A}\mathbf{a}^T)^T .$$

Then, all $k \times k$ submatrices of the matrix $\mathbf{A}$ and all $(k-1) \times (k-1)$ submatrices of the matrix $\mathbf{A}(\mathbf{e}_n, \widehat{\mathbf{e}}_{k,i})$ are non-singular if and only if

(i) *for each subsequence ρ of the sequence $\mathbf{e}_n$ of length k, the equation*

$$\mathbf{A}(\rho, \mathbf{e}_k)\mathbf{x}^T = (\mathbf{y}(\rho))^T$$

has a unique solution in the i-th component; i.e., if $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1})$ is a solution of the equation then $x_i = a_i$;

(ii) *for each subsequence ρ' of the sequence $\mathbf{e}_n$ of length $k-1$, the equation*

$$\mathbf{A}(\rho', \mathbf{e}_k)\mathbf{x}^T = (\mathbf{y}(\rho'))^T$$

has solutions with the i-th component as a free variable.

Proof. First, we observe that if all $k \times k$ submatrices of the matrix $\mathbf{A}$ are non-singular then by Proposition (i) for each subsequence ρ of the sequence $\mathbf{e}_n$, the equation $\mathbf{A}(\rho, \mathbf{e}_k)\mathbf{x}^T = (\mathbf{y}(\rho))^T$ has a unique solution in $\mathbf{x}$, which implies condition (i) of Theorem 1.

Next, we show that the conditions (i) and (ii) of Theorem 1 imply that all $k \times k$ submatrices of the matrix $\mathbf{A}$ are non-singular. Suppose, on the contrary, that there is a $k \times k$ submatrix $\mathbf{A}(\rho, \mathbf{e}_k)$ of the matrix $\mathbf{A}$ which is singular. Then, by (i) of Theorem 1, there exists a $(k-1) \times k$ submatrix $\mathbf{A}(\rho', \mathbf{e}_k)$ of the matrix $\mathbf{A}(\rho, \mathbf{e}_k)$, where ρ' is a subsequence of ρ such that the equation $\mathbf{A}(\rho', \mathbf{e}_k)\mathbf{x}^T = (\mathbf{y}(\rho'))^T$ has a unique solution in the i-th component, contrary to (ii) of Theorem 1.

It remains to show that, under the assumption that all $k \times k$ submatrices of $\mathbf{A}$ are non-singular, the condition (ii) of Theorem 1 is equivalent to the condition that all $(k-1)\times(k-1)$ submatrices of $\mathbf{A}(\mathbf{e}_n, \widehat{\mathbf{e}}_{k,i})$ are non-singular. This follows by applying part (ii) of the Proposition to $(k-1)\times k$ submatrices of $\mathbf{A}$. This completes the proof. □

We are now in a position to define the secret sharing matrices at any level i for $0 \leq i \leq k-1$.

Definition 1. *Let $\mathbf{A}$ be a matrix of size $n \times k$ over $\mathbb{F}$, where $k \leq n$, and let $0 \leq i \leq k-1$. We call $\mathbf{A}$ a secret sharing matrix at level i if and only if all $k \times k$ submatrices of the matrix $\mathbf{A}$ and all $(k-1)\times(k-1)$ submatrices of the matrix obtained from $\mathbf{A}$ by removing its i-th column are non-singular.*

By Theorem 1, the secret sharing matrix $\mathbf{A} = (\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n-1})^T$ at level i is a generic matrix of a sharing scheme with the secret placed as $D = a_i$. For each of such matrices $\mathbf{A}$, following Shamir's idea, we choose a random $(k-1)$-tuple $\widehat{\mathbf{a}}_i$. Then we determine the shares $(\mathbf{r}_0, y_0), (\mathbf{r}_1, y_1), \ldots, (\mathbf{r}_{n-1}, y_{n-1})$ from equation (1), and the secret $D = a_i$ can be determined from equation (2) by Gaussian elimination.

In the case when $i = 0$ or $k-1$ the matrix $\mathbf{A}_{poly}(\mathbf{t})$ for any sequence $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ with pairwise different t_i (and non-zero if $i = 0$) is a secret sharing matrix at level i in the sense of Definition 1. When $i \neq 0, k-1$ it is true for some special $\mathbf{t}$. For more details see [5] or the corollaries to Theorem 2 below. In the paper we also investigate secret sharing matrices at every level.

Definition 2. *Let $\mathbf{A}$ be a matrix of size $n \times k$ over $\mathbb{F}$, where $2 \leq k \leq n$. We call the matrix $\mathbf{A}$ an all-level secret sharing matrix if it is a secret sharing matrix at every level i for $0 \leq i \leq k-1$.*

An all-level secret sharing matrix $\mathbf{A}$ is a generic matrix of a secret sharing scheme with the secret placed as $D = a_i$, for arbitrary $0 \leq i \leq k-1$. In practice the matrices allow the admin to change the secret not changing the shares of users. They also allow to construct a secret sharing scheme in which the shareholders can use the same shares to recover more than one secret.

In the case of the original Shamir's scheme we shall characterize the sequences $\mathbf{t} \in \mathbb{F}^n$ such that $\mathbf{A}_{poly}(\mathbf{t})$ is a secret sharing matrix at a fixed level i, resp. at every level simultaneously.

3 Generalizations of Shamir's scheme

3.1 Lai-Dings's generalization of Shamir's scheme

As usual, for an r-tuple of indeterminates $\mathbf{x} = (x_0, x_1, \ldots, x_{r-1})$ and an r-tuple of increasing non-negative integers $\mathbf{c} = (c_0, c_1, \ldots, c_{r-1})$ we call $V_{\mathbf{c}}(\mathbf{x}) = \det\big((x_i^{c_j})_{0\le i,j\le r-1}\big)$ the generalized Vandermonde determinant. If $\mathbf{c} = \mathbf{e}_r$ it equals the classical Vandermonde determinant.

In this section we pursue Lai-Ding's scheme with a more general polynomial

$$q_{\mathbf{c}}(t) = a_0 t^{c_0} + a_1 t^{c_1} + \cdots + a_{k-1} t^{c_{k-1}},$$

where $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ is an increasing sequence of non-negative integers. Given such a polynomial and $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}^n$ we use the generalized Vandermonde determinants to prove necessary and sufficient conditions for coordinates $t_0, t_1, \ldots, t_{n-1}$ to determine secret sharing matrices.

Some special cases of the scheme based on the polynomial $q_{\mathbf{c}}(t)$ with $\mathbf{c} = (0, 1, \ldots, k-2, r)$, $r \ge k-1$ were considered in [5]. The Lai-Ding's scheme is determined by the basis $\mathcal{B}_{\mathbf{c}} = \{t^{c_0}, t^{c_1}, \ldots, t^{c_{n-1}}\}$ and the sequence $\mathbf{t}$ and can be viewed as given by equations (1) and (2) with $\mathbf{A} = \mathbf{A}_{\mathbf{c}}(\mathbf{t}) = (t_i^{c_j})_{0\le i\le n-1,\, 0\le j\le k-1}$.

Shamir's scheme is a special case of Lai-Ding's scheme related to the classical Vandermonde determinant. Then $\mathcal{B}_{poly} = \mathcal{B}_{\mathbf{e}_k}$, $\mathbf{A}_{poly}(\mathbf{t}) = \mathbf{A}_{\mathbf{e}_k}(\mathbf{t})$ and $i = 0$. In the paper we answer some interesting questions of [5] using relations between the generalized Vandermonde determinants and elementary symmetric polynomials (Lemma 1). We conclude this section with the definition of the Shamir type secret sharing matrices corresponding to some bases in k-dimensional subspaces of the space of polynomials over $\mathbb{F}$.

As usual the admin chooses a random vector of polynomial coefficients $\widehat{\mathbf{a}}_i$ for a fixed $0 \le i \le k-1$ and some appropriate elements $t_0, t_1, \ldots, t_{n-1}$ of $\mathbb{F}$, and next distributes as shares n points (t_0, y_0), (t_1, y_1), $\ldots$, (t_{n-1}, y_{n-1}) of the graph of polynomial q placing the secret as $D = a_i$. By finding the conditions on $t_0, t_1, \ldots, t_{n-1}$ (Theorem 2) we solve some open problems of Lai and Ding [5].

The generic polynomial q in the scheme will be well-matched if and only if every coalition of $\ge k$ but not of $< k$ shareholders will be able to recover the secret. This means, by Theorem 1, that

$$\det(\mathbf{A}(\rho, \mathbf{e}_k)) = V_{\mathbf{c}}(\mathbf{t}(\rho)) \ne 0\,, \tag{4}$$

resp.

$$\det(\mathbf{A}(\rho', \widehat{\mathbf{e}}_{k,i})) = V_{\widehat{\mathbf{c}}_i}(\mathbf{t}(\rho')) \ne 0\,, \tag{5}$$

for any subsequence ρ of length k, resp. any subsequence ρ' of length $k-1$ of the sequence $\mathbf{e}_n$. Note that, by (3), the secret $D = a_i$ is a linear combination of y_{ρ_j} (write $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-1})$) for $0 \leq j \leq k-1$, with non-zero coefficients. The latter means that all the shares $y_{\rho_0}, y_{\rho_1}, \ldots, y_{\rho_{k-1}}$ have to participate in recovering the secret.

Remark. In the case of Shamir's scheme (recall that $i = 0$ then) (4) and (5) hold if and only if $t_0, t_1, \ldots, t_{n-1}$ are pairwise different and non-zero elements of $\mathbb{F}$. Note that if the admin would place in Shamir's scheme as the secret $D = a_{k-1}$ then (4) and (5) hold if and only if $t_0, t_1, \ldots, t_{n-1}$ are pairwise different. We need not assume that they are non-zero.

3.2 Generalized Vandermonde determinants

Let $\mathbf{x} = (x_0, x_1, \ldots, x_{k-1})$, where x_i $(0 \leq i \leq k-1)$ are indeterminates. As above, for $0 \leq i \leq k-1$ we denote by $\widehat{\mathbf{x}}_i$ the sequence obtained from the sequence $\mathbf{x}$ by striking out the indeterminate x_i. It is well-known that the polynomial $V_{\mathbf{c}}(\mathbf{x})$ is divisible by $V_{\mathbf{e}_k}(\mathbf{x})$ in the polynomial ring $\mathbb{Z}[\mathbf{x}]$, and their quotient is a homogeneous polynomial having exactly $V_{\mathbf{e}_k}(\mathbf{c})/V_{\mathbf{e}_k}(\mathbf{e}_k)$ non-negative "terms" (see [3] or [7]). In [9] the quotient was determined in terms of the elementary symmetric polynomials.

The elementary symmetric polynomial $\tau_r(\mathbf{x})$ of degree r $(0 \leq r \leq k)$ is the sum of all distinct products of r distinct variables out of $x_0, x_1, \ldots, x_{k-1}$. By convention we have $\tau_0(\mathbf{x}) = 1$. Moreover, $\tau_r(\mathbf{x}) = \tau_r(x_0, x_1, \ldots, x_{k-2}) + \tau_{r-1}(x_0, x_1, \ldots, x_{k-2})x_{k-1}$.

Definition 3. *Let $k, l \in \mathbb{N}$. For any tuples $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ and $\mathbf{d} = (d_0, d_1, \ldots, d_{l-1})$ we call the tuples $\mathbf{c}$ and $\mathbf{d}$ complementary with respect to the standard $(k+l)$-tuple $\mathbf{e}_{k+l}$ if*

$$\{0, 1, \ldots, k+l-1\} = \{c_o, c_1, \ldots, c_{k-1}\} \cup \{d_0, d_1, \ldots, d_{l-1}\}$$

and

$$\{c_0, c_1, \ldots, c_{k-1}\} \cap \{d_0, d_1, \ldots, d_{l-1}\} = \emptyset.$$

Remark. Let $0 \leq j \leq k-1$. Then the sequences $\mathbf{c} = \widehat{\mathbf{e}}_{k,j}$ and $\mathbf{d} = (j)$ are complementary with respect to the sequence $\mathbf{e}_k$.

Lemma 1. (See [9], Chapter XI, p. 334.) *Let $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ and $\mathbf{d} = (d_0, \ldots, d_{l-1})$ be some increasing sequences of non-negative integers. Let $\mathbf{x}$ be a k-tuple of indeterminates x_i. Assume that $\mathbf{c}$ and $\mathbf{d}$ are complementary with respect to the standard $(k+l)$-tuple $\mathbf{e}_{k+l}$ with $c_{k-1} = k+l-1$. Then we have*

$$V_{\mathbf{c}}(\mathbf{x}) = (-1)^{\lfloor k/2 \rfloor + \lfloor l/2 \rfloor} \det\big(\big(\tau_{k-d_i+j}(\mathbf{x})\big)_{0 \leq i,j \leq l-1}\big) V_{\mathbf{e}_k}(\mathbf{x})\,.$$

Corollary. (See [9], Chapter XI, p. 333.) *For fixed* $0 \leq i, j \leq k-1$ *we have*

$$V_{\mathbf{e}_{k,j}}(\widehat{\mathbf{x}}_i) = (-1)^{\lfloor k/2 \rfloor} \tau_{k-1-j}(\widehat{\mathbf{x}}_i) V_{\mathbf{e}_{k-1}}(\widehat{\mathbf{x}}_i)\,.$$

3.3 Some open problems of Lai-Ding's

Let $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ be an increasing sequence of non-negative integers and let $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ be an n-tuple over $\mathbb{F}$. Lai and Ding asked a question about restrictions for $\mathbf{t}$ which allow to use the polynomial $q_{\mathbf{c}}(t) = a_0 t^{c_0} + a_1 t^{c_1} + \cdots + a_{k-1} t^{c_{k-1}}$ as a generic polynomial for a secret sharing scheme. See [5], pp. 457-458. In Theorem 2, for a fixed $\mathbf{c}$ and for a fixed $0 \leq i \leq k-1$, we give some necessary and sufficient conditions for the matrix $\mathbf{A}_{\mathbf{c}}(\mathbf{t})$ to be a secret sharing matrix at level i.

Let $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ and $\mathbf{d} = (d_0, d_1, \ldots, d_{l-1})$ be complementary increasing sequences of non-negative integers with respect to the standard $(k+l)$-tuple $\mathbf{e}_{k+l}$ for some $l \geq 1$ and $c_{k-1} = k+l-1$. For a fixed $0 \leq i \leq k-1$, $\mathbf{d}$ is the concatenation of two sequences $\mathbf{d}_{1,i}$ and $\mathbf{d}_{2,i}$, where $\mathbf{d}_{1,i}$ consists of the terms less than c_{k-2} if $i = k-1$, and of the terms less than c_i otherwise. If $i \neq k-1$ the sequences $\widehat{\mathbf{c}}_i$ and $\mathbf{d}' = \mathbf{d}_{1,i} || c_i || d_{2,i}$ are complementary with respect to the sequence $\mathbf{e}_{k+l_i}$, where $l_i = l$. In the case when $i = k-1$ the sequences $\widehat{\mathbf{c}}_{k-1}$ and $\mathbf{d}' = \mathbf{d}_{1,k-1}$ are complementary with respect to the sequence $\mathbf{e}_{k+l_{k-1}}$, where $l_{k-1} = c_{k-2} - k + 1$.

The following theorem answers an open question of Lai and Ding [5].

Theorem 2. *Let* $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ *and* $\mathbf{d} = (d_0, d_1, \ldots, d_{l-1})$ *be complementary increasing subsequences of non-negative integers with respect to the standard* $(k+l)$*-tuple* $\mathbf{e}_{k+l}$*, for some* $l \geq 1$ *with* $c_{k-1} = k+l-1$*. Let* $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ *be an* n*-tuple over* $\mathbb{F}$ *with pairwise different coordinates. Fix* $0 \leq i \leq k-1$*. In the above notation, the matrix* $\mathbf{A}_{\mathbf{c}}(\mathbf{t})$ *related to the polynomial* $q_{\mathbf{c}}(t)$ *is a secret sharing matrix at level* i *if and only if for any subsequences* ρ *of length* k *and* ρ' *of length* $k-1$ *of the sequence* $\mathbf{e}_n$*,*

$$\det\big(\big(\tau_{k-d_s+u}(\mathbf{t}(\rho))\big)_{0 \leq s,u \leq l-1}\big) \neq 0$$

and

$$\det\big(\big(\tau_{k-d'_s+u}(\mathbf{t}(\rho'))\big)_{0 \leq s,u \leq l_i-1}\big) \neq 0,$$

where $\widehat{\mathbf{c}}_i$ *and* $\mathbf{d}' = (d'_0, d'_1, \ldots, d'_{l_i-1})$ *are complementary sequences with respect to the standard* $(k+l_i)$*-tuple* $\mathbf{e}_{k+l_i}$*.*

Proof. The theorem follows from Theorem 1, (4), (5) and Lemma 1. It follows from Theorem 1 that the matrix $\mathbf{A} = \mathbf{A}_{\mathbf{c}}(\mathbf{t})$ is a secret sharing matrix at level i if and only if (4) and (5) hold. Since $t_0, t_1, \ldots, t_{k-1}$ are pairwise different

elements of $\mathbb{F}$, we have in Lemma 1 $V_{\mathbf{e}_k}(\mathbf{t}(\rho)) \neq 0$ and $V_{\mathbf{e}_{k-1}}(\mathbf{t}(\rho')) \neq 0$. This completes the proof. □

The following corollary solves an open problem of Lai and Ding [5] related to Shamir's scheme.

Corollary. *In the above notation, let* $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ *be an* n*-tuple over* $\mathbb{F}$ *with pairwise different coordinates. In the original Shamir's scheme the secret can be placed as* $D = a_i$ *for a fixed* $0 \leq i \leq k-1$ *(or in other words the matrix* $\mathbf{A}_{poly}(\mathbf{t})$ *is a secret sharing matrix at level* i*) if and only if for every subsequence* ρ *of length* $k-1$ *of the sequence* $\mathbf{e}_n$*,*

$$\tau_{k-1-i}(\mathbf{t}(\rho)) \neq 0\,. \tag{6}$$

The matrix $\mathbf{A}_{poly}(\mathbf{t})$ *is an all-level secret sharing matrix if and only if* (6) *holds for every* $0 \leq i \leq k-1$*.*

Proof. The corollary is a consequence of Theorem 2 and the corollary to Lemma 1. □

Remarks. (i) Here a question is whether there exists some $\mathbf{t} \in \mathbb{F}^n$ with pairwise different coordinates such that (6) holds for any subsequence ρ of length $k-1$ of the sequence $\mathbf{e}_n$ with a fixed $1 \leq i \leq k-2$, resp. with all $0 \leq i \leq k-1$. This means that the matrix $\mathbf{A}_{poly}(\mathbf{t})$ is a secret sharing matrix at level i, resp. an all-level secret sharing matrix. We can extend this question to more general matrices $\mathbf{A}_{\mathbf{c}}(\mathbf{t})$ with $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$.
(ii) In particular, if $\mathbb{F} = \mathbb{F}_q$ a question is whether (6) holds for sufficiently large q with $k \leq n < q$ and $0 \leq i \leq k-1$. For $i = 0$ or $i = k-1$, the answers to the question are positive for any q and any $\mathbf{t}$ with pairwise different (and non-zero if $i = 0$) coordinates.

Corollary. (Cf. [5].) *Given an* n*-tuple* $\mathbf{t}$ *over* $\mathbb{F}$ *with pairwise different coordinates, the secret in Shamir's scheme can be placed as* $D = a_{k-1}$*, and if the coordinates are non-zero also as* $D = a_0$*. (In other words the matrix* $\mathbf{A}_{poly}(\mathbf{t})$ *is a secret sharing matrix at level* $k-1$ *and* 0*, respectively then.)*

Proof. If $i = k-1$, the left hand side of (6) equals 1 (and is not equal to 0), and if $k = 0$, it equals $\prod_{j=0}^{k-1} t_{\rho_j} \neq 0$, and hence the corollary follows at once. □

Corollary. (Cf. [5]). *The secret in the Shamir scheme can be placed as* $D = a_{k-2}$ *for some pairwise different* $t_0, t_1, \ldots, t_{n-1} \in \mathbb{F}$*, if and only if for every subsequence* $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-2})$ *of the sequence* $\mathbf{e}_n$*,*

$$t_{\rho_0} + t_{\rho_1} + \cdots + t_{\rho_{k-2}} \neq 0\,.$$

Proof. If $i = k-2$ then $\tau_{k-i-1} = \tau_1$, and the corollary follows easily from the previous one. □

It is easy to see that not always the secret in Shamir's scheme can be placed as $D = a_{k-2}$.

Example. Let $\mathbb{F} = \mathbb{F}_7$, $n = 5$, $k = 3$ and $q(t) = a_0 + a_1 t + a_2 t^2$. If we place the secret as $D = a_1$ and use $\mathbf{t} = (1, 2, 3, 4, 5)$, a coalition of 2 participants can reconstruct the secret. Then $D_i = q(t_i) = q(i+1)$. Then $D_2 = q(3) = a_0 + 3a_1 + 2a_2$ and $D_3 = q(4) = a_0 + 4a_1 + 2a_2$. Hence $a_1 = D_3 + 6D_2$. Similarly $D_1 = q(2) = a_0 + 2a_1 + 4a_2$ and $D_4 = q(5) = a_0 + 5a_1 + 4a_2$. Hence $a_1 = 2D_1 + 5D_4$. Note that if $D = a_0$ or a_2, the secret can be reconstructed by 3 but not by 2 shareholders. Note that for the subsequence $(3, 4)$ of the sequence $(1, 2, 3, 4, 5)$ we have $3 + 4 = 0$, and the corollary above shows that the secret cannot be placed as $D = a_1$.

3.4 Secret sharing schemes related to bases

As in the Introduction we generalize Shamir-Lai-Ding's secret sharing schemes by using more general bases $\mathcal{B} = \{v_0(t), v_1(t), \ldots, v_{k-1}(t)\}$ in a k-dimensional vector subspace of the vector space $\mathbb{F}[t]_{<K}$ with some $K \geq k$.

In this section, a secret sharing scheme is given by a generic matrix of the form $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(\mathbf{t}) = (v_s(t_u))_{0 \leq u \leq n-1,\, 0 \leq s \leq k-1}$ and $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ over $\mathbb{F}$. An example of such a matrix is Shamir's matrix $\mathbf{A}_{poly}(\mathbf{t})$. Another (more general) example is Lai-Ding's matrix $\mathbf{A}_{\mathbf{c}}(\mathbf{t})$ defined for increasing sequences $\mathbf{c} = (c_0, c_1, \ldots, c_{k-1})$ of non-negative integers. Shamir's matrix is related to the basis $\mathcal{B}_{poly}$ and Lai-Ding's to the basis $\mathcal{B}_{\mathbf{c}}$.

The matrix $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(\mathbf{t})$ is a secret sharing matrix at level i, for a fixed $0 \leq i \leq k-1$, if and only if it satisfies conditions (i) and (ii) of Theorem 1. These conditions give some additional assumptions on the $\mathbf{t}$ similar to those in Theorem 2.

It is clear that for a given secret sharing matrix $\mathbf{A}$ and sufficiently large K, there exists a basis $\mathcal{B}$ of the vector space $\mathbb{F}[t]_{<K}$ such that $\mathbf{A} = \mathbf{A}_{\mathcal{B}}$. We shall show in section 5 that the assertion is false for $K = k$. For illustration, see two examples of secret sharing matrices not corresponding to any polynomial basis in $\mathbb{F}[t]_{<k}$, which are given in the Introduction.

Now we are ready to define the Shamir type secret sharing matrices.

Definition 4. *An $n \times k$ secret sharing matrix $\mathbf{A}$ is said to be the Shamir type secret sharing matrix if there exists a basis $\mathcal{B}$ of the vector space of polynomials of degree $< k$ in $\mathbb{F}[t]$ such that $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(\mathbf{t})$ for some $\mathbf{t} \in \mathbb{F}^n$.*

Example. A non-trivial example of a polynomial basis in $\mathbb{F}[t]_{<k}$ is the binomial basis. Given $r \in \mathbb{N}$ with $r!$ not divisible by $\mathrm{char}(\mathbb{F})$, we define a polynomial $\binom{t}{r} \in \mathbb{F}[t]$ of degree r by $\binom{t}{r} = \frac{t(t-1)\cdots(t-r+1)}{r!}$ (by convention $\binom{t}{0} = 1$). This polynomial equals 0 at $t = 0, 1, \ldots, r-1$ and 1 at $t = r$.

Assume that $(k-1)!$ is not divisible by $\mathrm{char}(\mathbb{F})$. Consider the basis $\mathcal{B}_{binom} = \left\{\binom{t}{0}, \binom{t}{1}, \ldots, \binom{t}{k-1}\right\}$ of the linear space $\mathbb{F}[t]_{<k}$ over $\mathbb{F}$. Let $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}^n$. The secret sharing matrix related to this basis is given by $\mathbf{A}_{binom}(\mathbf{t}) = (\binom{t_i}{j})_{0\le i\le n-1,\, 0\le j\le k-1}$. All the k-order minors of the matrix are the classical Cauchy determinants $C(\mathbf{t}(\rho)) = \det((\binom{t_{\rho_i}}{j})_{0\le i,j\le k-1})$, and so differ from the classical Vandermonde determinants by the factor $\left(\prod_{i=0}^{k-1} i!\right)^{-1}$. Thus if $t_0, t_1, \ldots, t_{n-1}$ are pairwise different (recall that by assumption $(k-1)!$ is not divisible by $\mathrm{char}(\mathbb{F})$), the minors are $\neq 0$. Under this assumptions, the matrix $\mathbf{A}_{binom}(\mathbf{t})$ satisfies condition (i) of Theorem 1.

The matrix $\mathbf{A}_{binom}(\mathbf{t})$ satisfies condition (ii) of Theorem 1 with $i = k-1$ and $i = 0$ under the same assumptions on the tuple $\mathbf{t}$ as in Shamir's scheme (and under the same assumptions on $\mathrm{char}(\mathbb{F})$) as in the case of condition (i) of Theorem 1. Indeed, for any subsequence ρ of the sequence $\mathbf{e}_n$ and every $0 \le s \le k-1$, the determinants of the matrices $\mathbf{A}(\widehat{\rho}_s, \mathbf{e}_{k-1}) = (\binom{t_{\rho_i}}{j})_{0\le i\le k-1, 0\le j\le k-2, i\ne s}$ and $\mathbf{A}(\widehat{\rho}_s, \widehat{\mathbf{e}}_{k,0}) = (\binom{t_{\rho_i}}{j})_{0\le i\le k-1, 1\le j\le k-1, i\ne s}$ are the classical Cauchy determinants. They differ from the classical Vandermonde determinant by the factor $\left(\prod_{s=0}^{k-2} s!\right)^{-1}$ if $i = k-1$ and by the factor $\left(\prod_{0\le i\le k-1,\, i\ne s} t_{\rho_i}\right) \cdot \left(\prod_{i=1}^{k-1} i!\right)^{-1}$ if $i = 0$. Thus the matrices are non-singular because by assumption $(k-1)!$ is not divisible by $\mathrm{char}(\mathbb{F})$.

If we place the secret as $D = a_i$ for $i \ne 0, k-1$, conditions (i) and (ii) of Theorem 1 generate some other assumptions on the sequence $\mathbf{t}$ just as in Shamir's scheme.

4 Algorithms for constructing secret sharing matrices

In this section we describe two algorithms for constructing secret sharing matrices. One algorithm is for secret sharing matrices at a fixed level i $(0 \le i \le k-1)$, and the other is for all-level secret sharing matrices. The algorithms allow to determine all such matrices both in the case of secret sharing matrices at level i and in the case of all-level secret sharing matrices.

First we recall some notation and basic facts related to Gaussian elimination, which will be the main tool of the section. The Gaussian elimination algorithm is a well-known efficient algorithm for solving systems of linear equations; we refer the reader to [12], section 15.4, p. 326.

A matrix over a field $\mathbb{F}$ is said to be in reduced row echelon form if the following conditions hold:

(i) All non-zero rows are above any zero rows.

(ii) The first non-zero entry of a non-zero row is 1 and it is always strictly to the right of the leading coefficient of the row above it. It is called a leading 1 or a pivot.

(iii) Every leading coefficient is the only non-zero entry in its column.

It is well known that the Gaussian elimination algorithm involving elementary row operations reduces any matrix to a matrix in reduced row echelon form. We denote by $R(\mathbf{A})$ the (unique) matrix in reduced row echelon form corresponding to the matrix $\mathbf{A}$.

If the rank of an $n \times k$ matrix $\mathbf{A}$ is equal to r then the matrix $R(\mathbf{A})$ has exactly r non-zero rows (so exactly r pivots), and hence it has exactly $k - r$ columns which do not contain a pivot. Note that these columns and their numbers determine the matrix $R(\mathbf{A})$. In the algorithms below we determine the number $n(\mathbf{A})$ of the first column of $R(\mathbf{A})$ which does not contain a pivot and the vector $\mathbf{c}(\mathbf{A})$ which consists of the first $n(\mathbf{A})$ entries of this column. (Recall that in the paper the rows and columns in the matrices are numbered as from zero.)

4.1 Algorithm for constructing or extending a secret sharing matrix at level i

In this subsection we describe an algorithm of finding a secret sharing $n \times k$ matrix over $\mathbb{F}$ at level $i = k-1$. By using a column permutation one can get an algorithm for finding a secret sharing $n \times k$ matrix at level i for arbitrary $0 \leq i \leq k-1$.

We adopt the notation of the previous section. The algorithm gives a method of constructing a secret sharing matrix or appending some additional rows to a given secret sharing matrix at level $i = k-1$. Both the cases differ by an initializing matrix $\mathbf{A}_0$, and in both we append some additional rows to $\mathbf{A}_0$.

We start with $\mathbf{A}_0$ as an $n \times k$ secret sharing matrix $\mathbf{A}$ when we extend $\mathbf{A}$ to a larger secret sharing matrix at level $i = k-1$, and with $\mathbf{A}_0$ as an arbitrary $(k-1) \times k$ matrix over $\mathbb{F}$ such that its $(k-1) \times (k-1)$ submatrix obtained by removing its $(k-1)$-th column is non-singular when we construct a secret sharing matrix at level $i = k-1$ from the outset. Here any such matrix can be obtained from a $(k-1) \times k$ matrix over $\mathbb{F}$ such that its first

$k-1$ columns form the identity $(k-1)\times(k-1)$ matrix (and the last column is arbitrary) by performing elementary row operations. The size of the matrix $\mathbf{A}_0$ is $m \times k$, where $m = n$ and $m = k-1$ respectively.

In steps 2-5 in the algorithm below we make use r times of a subprocedure computing a vector $\mathbf{v} = (v_0, v_1, \ldots, v_{k-1}) \in \mathbb{F}^k$ extending the $m \times k$ matrix $\mathbf{A}_0$ to an $(m+1)\times k$ secret sharing matrix at level $i = k-1$. The components v_t $(0 \leq t \leq k-1)$ of the vector $\mathbf{v}$ are determined by induction on t.

4.1.1 Algorithm for constructing or extending secret sharing matrices at level $i = k-1$

INPUT: positive integers n, k, r $(2 \leq k \leq n)$, and an $m \times k$ matrix $\mathbf{A}_0$.

OUTPUT: an $(m+r) \times k$ secret sharing matrix $\mathbf{B}$ at level $i = k-1$ extending the matrix $\mathbf{A}_0$.

SUMMARY: r additional rows are appended to the matrix $\mathbf{A}_0$.

1. (*Initializing*) $\mathbf{B} \leftarrow \mathbf{A}_0$.
2. (*Computing* $v_0, v_1, \ldots, v_{k-2}$) Compute the first $k-1$ components v_0, v_1, …, v_{k-2} of the vector $\mathbf{v}$ as follows.
   - 2.1. (*Computing* n_ρ *and* $\mathbf{c}_\rho$) For all increasing subsequences ρ of length $k-2$ of the sequence $\mathbf{e}_m$ do the following:
     - 2.1.1. Use Gaussian elimination to compute $R(\mathbf{B}(\rho, \mathbf{e}_k))$.
     - 2.1.2. Set $n_\rho \leftarrow n(\mathbf{B}(\rho, \mathbf{e}_k))$.
     - 2.1.3. Set $\mathbf{c}_\rho \leftarrow \mathbf{c}(\mathbf{B}(\rho, \mathbf{e}_k))$.
   - 2.2. (*Computing* $\mathcal{S}_l$) For $l = 0$ to $k-2$ do the following:
     - 2.2.1. Set $\mathcal{J}_l$=the set of all subsequences ρ of length $k-2$ of the sequence $\mathbf{e}_m$ such that $n_\rho = l$.
     - 2.2.2. Set $S_0 \leftarrow \emptyset$ if $\mathcal{J}_0 = \emptyset$ and $S_0 \leftarrow \{0\}$ otherwise.
     - 2.2.3. For $1 \leq l \leq k-2$ set $\mathcal{S}_l \leftarrow \{(v_0, v_1, \ldots, v_{l-1}) \cdot \mathbf{c}_\rho\colon \ \rho \in \mathcal{J}_l\}$.
     - 2.2.4. Select as v_l an arbitrary element of $\mathbb{F} \setminus \mathcal{S}_l$.
3. (*Computing* $\mathcal{S}$ *and* v_{k-1}) Compute the component v_{k-1} of vector $\mathbf{v}$ as follows.
   - 3.1. (*Computing* $\mathbf{c}^*_\rho$) For all increasing subsequences ρ of length $k-1$ of the sequence $\mathbf{e}_m$ do the following:
     - 3.1.1. Use Gaussian elimination to compute $R(\mathbf{B}(\rho, \mathbf{e}_k))$.

3.1.2. Set $\mathbf{c}^*_\rho$=the last column of $R(\mathbf{B}(\rho, \mathbf{e}_k))$.

3.2. Set $\mathcal{J}$=the set of all subsequences ρ of length $k-1$ of the sequence $\mathbf{e}_m$.

3.3. Set $\mathcal{S} \leftarrow \{(v_0, v_1, \ldots, v_{k-2}) \cdot \mathbf{c}^*_\rho \colon \ \rho \in \mathcal{J}\}$.

3.4. Select as v_{k-1} an arbitrary element of $\mathbb{F} \setminus \mathcal{S}$.

4. Set $\mathbf{v} \leftarrow (v_0, v_1, \ldots, v_{k-1})$.

5. Update $\mathbf{B}$ by appending r additional rows repeating r times steps 2-4.

6. Return $\mathbf{B}$.

Remarks. (i) In step 2.2.4, note that such an element exists whenever $\binom{m}{k-2} < \mathrm{card}(\mathbb{F})$. Similarly, in step 3.4, such an element exists whenever $\binom{m}{k-1} < \mathrm{card}(\mathbb{F})$. In practise, $\mathbb{F}$ is a finite field and $\mathrm{card}(\mathbb{F})$ is very large, much greater than $\max\{\binom{m}{k-1}, \binom{m}{k-2}\}$. Therefore with a high probability any extension of a non-singular matrix chosen at random gives a secret sharing matrix at level i for an arbitrary i. In fact, the probability that any extension of a given secret sharing matrix at level i, by appending a (pseudo)random row-vector, is a secret sharing matrix at level i too is greater than

$$\Big(1 - \frac{\binom{m}{k-2}}{\mathrm{card}(\mathbb{F})}\Big) \cdot \Big(1 - \frac{\binom{m}{k-1}}{\mathrm{card}(\mathbb{F})}\Big)$$

because

$$\mathrm{card}(\mathbb{F} \setminus \mathcal{S}_l) = \mathrm{card}(\mathbb{F}) - \mathrm{card}(\mathcal{S}_l) \geq \mathrm{card}(\mathbb{F}) - \mathrm{card}(\mathcal{J}_l)\,,$$

and hence

$$\prod_{l=0}^{k-2} \Big(1 - \frac{\mathrm{card}(\mathcal{J}_l)}{\mathrm{card}(\mathbb{F})}\Big) \geq 1 - \frac{\sum_{l=0}^{k-2} \mathrm{card}(\mathcal{J}_l)}{\mathrm{card}(\mathbb{F}} = 1 - \frac{\binom{m}{k-2}}{\mathrm{card}(\mathbb{F})}\,.$$

In typical situation, when $k, m \leq 10$, $\mathbb{F} = \mathbb{F}_p$ and p is a several-dozen-bit prime number, this probability is close to certainty.
(ii) Note that to find n_ρ and c_ρ we need only to apply the Gaussian elimination algorithm until we find the first column which does not contain a pivot. We also may assume that n_ρ and c_ρ (or only n_ρ), which have been already computed in the preceding steps, are stored in the memory. To save the memory, we may slightly modify the above algorithm assuming that only the numbers n_ρ are remembered. Then we additionally need to compute c_ρ, for each $\rho \in \mathcal{J}_l$.

4.1.2 Proof of correctness of Algorithm 4.1.1

It suffices to show that the algorithm produces a secret sharing matrix at level $i = k-1$ in the case when $r = 1$. Thus let $\mathbf{B}$ be the matrix obtained from $\mathbf{A}_0$ by appending the row $\mathbf{v} = (v_0, v_1, \ldots, v_{k-1})$ defined in the step 4 as the $(m+1)$st row of $\mathbf{B}$. Note that we need only to show that all $(k-1)\times(k-1)$ submatrices of $\mathbf{B}(\mathbf{e}_{m+1}, \mathbf{e}_{k-1})$ which contain the last row of $\mathbf{B}(\mathbf{e}_{m+1}, \mathbf{e}_{k-1})$ and all $k \times k$ submatrices of $\mathbf{B}$ which contain the last row of $\mathbf{B}$ are non-singular.

Let $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-2})$ be a subsequence of the sequence $\mathbf{e}_{m+1}$ with $\rho_{k-2} = m$ and let $\rho' = (\rho_0, \rho_1, \ldots, \rho_{k-3})$. By the assumptions on $\mathbf{A}_0$, the the rank of $\mathbf{B}(\rho', \mathbf{e}_{k-1})$ is equal to $k-2$. It follows that column $n_{\rho'} = n(\mathbf{B}(\rho', \mathbf{e}_{k-1}))$ of $R(\mathbf{B}(\rho', \mathbf{e}_{k-1}))$ is the only column of this matrix without pivot. By step 2, $v_{n_{\rho'}} \neq (v_0, v_1, \ldots, v_{n_{\rho'}-1}) \cdot \mathbf{c}_{\rho'}$, where $\mathbf{c}_{\rho'} = \mathbf{c}(\mathbf{B}(\rho', \mathbf{e}_{k-1}))$. It follows that the vector $(v_0, v_1, \ldots, v_{k-2})$ is not a linear combination of the rows of $R(\mathbf{B}(\rho', \mathbf{e}_{k-1}))$, so $\mathbf{B}(\rho, \mathbf{e}_{k-1})$ is non-singular.

Now, let $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-1})$ be a subsequence of the sequence $\mathbf{e}_{m+1}$ with $\rho_{k-1} = m$ and let $\rho' = (\rho_0, \rho_1, \ldots, \rho_{k-2})$. By the assumptions on $\mathbf{A}_0$, the the rank of $\mathbf{B}(\rho', \mathbf{e}_{k-1})$ is equal to $k-1$. It follows that $R(\mathbf{B}(\rho', \mathbf{e}_{k-1}))$ is the identity matrix. By step 3, $v_{k-1} \neq (v_0, v_1, \ldots, v_{k-2}) \cdot \mathbf{c}^*_{\rho'}$, where $\mathbf{c}^*_{\rho'}$ is the last column of $R(\mathbf{B}(\rho', \mathbf{e}_k))$. By similar arguments as above we deduce that $\mathbf{B}(\rho, \mathbf{e}_k)$ is non-singular.

4.1.3 Efficiency of Algorithm 4.1.1

The main ingredient of the algorithm is Gaussian elimination which requires at most $\binom{m}{k-2}(k-2)k^2$ operations in $\mathbb{F}$ in step 2.1 and at most $\binom{m}{k-1}(k-1)k^2$ operations in step 3.1 (see [12], p. 327), and so a total of $m\binom{m}{k-2}k^2$ operations in $\mathbb{F}$.

Indeed the loop in step 2.1 is executing $\binom{m}{k-2}$ times, and in step 3.1 $\binom{m}{k-1}$ times. Therefore the step 2.2.3 requires at most $(k-2)\binom{m}{k-2}$ operations and the step 3.2 at most $(k-1)\binom{m}{k-1}$ operations, so a total of $m\binom{m}{k-2}$ operations in $\mathbb{F}$. Hence the whole algorithm performs a total of $\Phi(m,k) = m\binom{m}{k-2}(k^2+1)$ operations in $\mathbb{F}$.

In typical situation, when $k-1 \leq m \leq 10$, an easy computation shows that $10 \leq \Phi(m,2) \leq 50$, $40 \leq \Phi(m,3) \leq 1000$, $153 \leq \Phi(m,4) \leq 7650$, and $416 \leq \Phi(m,5) \leq 31200$.

4.2 Algorithm for constructing an all-level secret sharing matrix

In this subsection we give an algorithm, which is a slight modification of that from the previous section, for finding or extending an all-level secret sharing matrix. The algorithm gives a method for constructing an all-level secret sharing matrix or gives the same but extending a given all-level secret sharing matrix. Again we introduce an initializing matrix $\mathbf{A}_0$ and construct the matrices by appending some additional rows to $\mathbf{A}_0$.

We start with $\mathbf{A}_0$ as an $n \times k$ all-level secret sharing matrix $\mathbf{A}$ if we want to extend $\mathbf{A}$, or with $\mathbf{A}_0$ as an arbitrary $(k-1) \times k$ matrix over $\mathbb{F}$ such that all its $(k-1) \times (k-1)$ submatrices are non-singular otherwise. Here any such matrix $\mathbf{A}_0$ can be obtained by performing elementary row operations, from a $(k-1) \times k$ matrix over $\mathbb{F}$ such that its first $k-1$ columns form the identity $(k-1) \times (k-1)$ matrix and all components of its k-th column are non-zero.

The size of the matrix $\mathbf{A}_0$ is again $m \times k$, where $m = n$ or $m = k-1$. In the algorithm we apply r times a similar inductive subprocedure computing a vector $\mathbf{v} \in \mathbb{F}^k$ extending the $m \times k$ matrix $\mathbf{A}_0$ to an all-level $(m+1) \times k$ secret sharing matrix.

4.2.1 Algorithm for constructing or extending all-level secret sharing matrices

INPUT: positive integers n, k, r $(2 \leq k \leq n)$, and an $m \times k$ matrix $\mathbf{A}_0$.

OUTPUT: an all-level $(m+r) \times k$ secret sharing matrix $\mathbf{B}$ extending the matrix $\mathbf{A}_0$.

SUMMARY: r additional rows are appended to the matrix $\mathbf{A}_0$.

1. (*Initializing*) $\mathbf{B} \leftarrow \mathbf{A}_0$.
2. (*Computing* $v_0, v_1, \ldots, v_{k-2}$) Compute the first $k-1$ components v_0, v_1, ..., v_{k-2} of the vector $\mathbf{v}$ as in steps 2.1-2.2 of Algorithm 4.1.1. and set $\mathbf{v}' \leftarrow (v_0, v_1, \ldots, v_{k-2})$.
3. (*Computing* v_{k-1}) Compute the component v_{k-1} of the vector $\mathbf{v}$ as follows
   - 3.1. (*Computing* $\mathcal{S}_i$) For all increasing subsequences ρ of length $k-2$ of the sequence $\mathbf{e}_m$ and for each $0 \leq i \leq k-2$ do the following:
     - 3.1.1. Use Gaussian elimination to compute $R(\mathbf{B}(\rho, \widehat{\mathbf{e}}_{k,i}))$.

3.1.2. Set $c^*_{\rho,i}$=the last column of $R(\mathbf{B}(\rho, \widehat{\mathbf{e}}_{k,i}))$.

3.1.3. Set $\mathcal{J}_i$=the set of all ρ such that $c^*_{\rho,i}$ does not contain a pivot.

3.1.4. Set $\mathcal{S}_i \leftarrow \{\widehat{\mathbf{v}'}_i \cdot \mathbf{c}^*_{\rho,i} \colon \ \rho \in \mathcal{J}_i\}$.

3.2. (*Computing* $\mathcal{S}$) Compute the set $\mathcal{S}$ as in steps 3.1-3.3 of Algorithm 4.1.1.

3.3. Select as v_{k-1} an arbitrary element of $\mathbb{F} \setminus \left(S \cup \bigcup_{i=0}^{k-2} \mathcal{S}_i\right)$.

4. Set $\mathbf{v} \leftarrow (v_0, v_1, \ldots, v_{k-1})$.

5. Update $\mathbf{B}$ by appending r additional rows repeating r times steps 2-5.

6. Return $\mathbf{B}$.

Remark. In step 3.3, note that such an element exists whenever

$$\binom{m}{k-1} + (k-1)\binom{m}{k-2} < \mathrm{card}(\mathbb{F})\,.$$

Following the first remark to Algorithm 4.1.1, with a high probability any extension of a non-singular matrix chosen at random gives an all-level secret sharing matrix. In typical situation, when $m, k \leq 10$, $\mathbb{F} = \mathbb{F}_p$ and p is a several-dozen-bit prime number this probability is close to certainty again.

4.2.2 Proof of correctness of Algorithm 4.2.1

As before, it suffices to show that the algorithm produces an all-level secret sharing matrix in the case when $r = 1$. Let $\mathbf{B}$ be the matrix obtained from $\mathbf{A}_0$ by appending the row $\mathbf{v} = (v_0, v_1, \ldots, v_{k-1})$ defined in the step 4 as the $(m+1)$st row of $\mathbf{B}$.

By the same argument as in the proof in subsection 4.1.2, all $(k-1) \times (k-1)$ submatrices of $\mathbf{B}(\mathbf{e}_{m+1}, \mathbf{e}_{k-1})$ all $k \times k$ submatrices of $\mathbf{B}$ are non-singular. Thus it remains to show that that for each i, $0 \leq i \leq k-2$, all $(k-1) \times (k-1)$ submatrices of $\mathbf{B}(\mathbf{e}_{m+1}, \widehat{\mathbf{e}}_{k,i})$ which contain the last row of $\mathbf{B}(\mathbf{e}_{m+1}, \widehat{\mathbf{e}}_{k,i})$ are non-singular. Notice that the rank of any $(k-1) \times (k-2)$ submatrix of $\mathbf{B}(\mathbf{e}_{m+1}, \widehat{\mathbf{e}}_{k-1,i})$ is equal to $k-2$.

Let $\rho = (\rho_0, \rho_1, \ldots, \rho_{k-2})$ be a subsequence of the sequence $\mathbf{e}_{m+1}$ with $\rho_{k-2} = m$. By the assumptions on $\mathbf{A}_0$, the rank of $\mathbf{B}(\rho', \widehat{\mathbf{e}}_{k,i})$, where $\rho' = (\rho_0, \rho_1, \ldots, \rho_{k-3})$, is equal to $k-2$. It follows that $R(\mathbf{B}(\rho', \widehat{\mathbf{e}}_{k,i}))$ has exactly one column without a pivot. If the last column of $R(\mathbf{B}(\rho', \widehat{\mathbf{e}}_{k,i}))$ contains a pivot then, by applying the Gaussian elimination algorithm, we obtain that $R(\mathbf{B}(\rho, \widehat{\mathbf{e}}_{k,i}))$ is the identity matrix since the rank of $R(\mathbf{B}(\rho, \widehat{\mathbf{e}}_{k-1,i}))$ is equal to $k-2$. Suppose now that the last column of $R(\mathbf{B}(\rho', \widehat{\mathbf{e}}_{k,i}))$ does

not contain a pivot. By step 4, $v_{k-1} \neq \widehat{\mathbf{v}'}_i \cdot \mathbf{c}^*_{\rho',i}$, where $\mathbf{c}^*_{\rho',i}$ is the last column of $R(\mathbf{B}(\rho', \widehat{\mathbf{e}}_{k,i}))$. Consequently, by applying the Gaussian elimination algorithm, we obtain again that $R(\mathbf{B}(\rho, \widehat{\mathbf{e}}_{k,i}))$ is the identity matrix.

4.2.3 Efficiency of Algorithm 4.2.1

Similarly as in the previous algorithm, the main ingredient of the algorithm is Gaussian elimination performed in steps 2 and 3. Some similar loops are also executed. We leave it to the reader to compare the numbers of operations in $\mathbb{F}$ in both the above algorithms in typical situation $m, k \leq 10$.

5 The Shamir type secret sharing matrices

In this section we prove that a secret sharing matrix need not be the Shamir type secret sharing matrix. See Definition 4 in section 3. A set of vectors $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{s-1}\}$ in the vector space $\mathbb{F}^k$ is said to be in general position if no l of them are linearly dependent, for each $l \leq k$. An example of vectors in general position in $\mathbb{F}^k$ are the rows in a secret sharing matrix. In the original Shamir secret sharing scheme the rows lie on the curve $\mathbf{s}\colon \mathbb{F} \to \mathbb{F}^k$ given by

$$\mathbf{s}(t) = (1, t, \ldots, t^{k-1}) .$$

They are of the form $\mathbf{s}(t_0), \mathbf{s}(t_1), \ldots, \mathbf{s}(t_{n-1})$ for some $t_0, t_1, \ldots, t_{n-1} \in \mathbb{F}$. We have $q(t) = \mathbf{s}(t) \cdot \mathbf{a}$, where q is Shamir's generic polynomial and $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1})$.

More generally, in the secret sharing scheme related to a basis $\mathcal{B} = \{v_0(t), v_1(t), \ldots, v_{k-1}(t)\}$ of a k-dimensional vector subspace of the space $\mathbb{F}[t]_{<K}$ (for some $K \geq k$) the rows lie on the curve $\mathbf{v}\colon \mathbb{F} \to \mathbb{F}^k \subseteq \mathbb{F}^K$ given by

$$\mathbf{v}(t) = (v_0(t), v_1(t), \ldots, v_{k-1}(t)) .$$

Lemma 2 yields some crucial information about the rows of the secret sharing matrix $\mathbf{A}_\mathcal{B}$ related to a basis $\mathcal{B}$ of the vector space $\mathbb{F}[t]_{<k}$ over $\mathbb{F}$ (in the case when $K = k$).

Lemma 2. *Let $2 \leq k \leq n$ be natural numbers and let $\mathcal{B}$ be a basis of the vector space $\mathbb{F}[t]_{<k}$ over $\mathbb{F}$. Let $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1})$ be an n-tuple over $\mathbb{F}$ with pairwise different $t_0, t_1, \ldots, t_{n-1}$. Assume that $\mathbf{A} = \mathbf{A}_\mathcal{B}(\mathbf{t})$. Let $\mathbf{r}_i$ $(0 \leq i \leq n-1)$ denote the i-th row of $\mathbf{A}$. Then each $\mathbf{r}_i$ is a unique linear combination of $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{k-1}$ with some coefficients which sum up to 1. Consequently, if the first components of the rows $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{k-1}$ are equal then the first components of all the rows $\mathbf{r}_0, \mathbf{r}_1, \ldots, \mathbf{r}_{n-1}$ are equal.*

Proof. Let $\mathcal{B} = \{v_0(t), v_1(t), \ldots, v_{k-1}(t)\}$. Then $\mathbf{r}_i = \mathbf{v}(t_i)$, where $\mathbf{v}(t) = (v_0(t), v_1(t), \ldots, v_{k-1}(t))$. Note that there exists a non-singular $k \times k$ matrix $\mathbf{M}$ with coefficients in $\mathbb{F}$ such that

$$\mathbf{v}(t) = \mathbf{s}(t)\mathbf{M}\,.$$

Thus, $\mathbf{r}_i = \mathbf{v}(t_i) = \mathbf{s}(t_i)\mathbf{M}$, and

$$\mathbf{A} = \mathbf{A}_{poly}(\mathbf{t})\mathbf{M}\,.$$

Note that the rows $\mathbf{s}(t_0), \mathbf{s}(t_1), \ldots, \mathbf{s}(t_{n-1})$ of the matrix $\mathbf{A}_{poly}(\mathbf{t})$ have the property that each $\mathbf{s}(t_j)$ is a unique linear combination of the rows $\mathbf{s}(t_0), \mathbf{s}(t_1), \ldots, \mathbf{s}(t_{k-1})$ with some coefficients which sum up to 1. Therefore, the first assertion of the theorem follows, since the multiplication of a vector in $\mathbb{F}^k$ by $\mathbf{M}$ induces a linear isomorphism $\mathbb{F}^k \to \mathbb{F}^k$. The second assertion is a direct consequence of the first one. □

Note that for any $n \times k$ matrix $\mathbf{A}$ over $\mathbb{F}$, where $n < \mathrm{card}(\mathbb{F})$, there exists a basis $\mathcal{B}$ of a k-dimensional vector subspace of the space $\mathbb{F}[t]_{<K}$ over $\mathbb{F}$ and pairwise different $t_0, t_1, \ldots, t_{n-1} \in \mathbb{F}$ such that $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(t_0, t_1, \ldots, t_{n-1})$ for sufficiently large K.

Here a question is whether for a given $n \times k$ matrix $\mathbf{A}$ over $\mathbb{F}$, where $n \leq \mathrm{card}(\mathbb{F})$, which is a secret sharing matrix at level i $(0 \leq i \leq k-1)$ (or more specifically an all-level secret sharing matrix), there exists a basis $\mathcal{B}$ of the vector space $\mathbb{F}[t]_{<k}$ over $\mathbb{F}$ and pairwise different $t_0, t_1, \ldots, t_{n-1} \in \mathbb{F}$ such that $\mathbf{A} = \mathbf{A}_{\mathcal{B}}(\mathbf{t})$. Lemma 2 provides a negative answer to the above question.

Theorem 3. *Let $2 \leq k < n$ be natural numbers. There exists a secret sharing $n \times k$ matrix $\mathbf{A}$ at level i for a fixed $0 \leq i \leq k-1$ (or an all-level secret sharing matrix) such that $\mathbf{A} \neq \mathbf{A}_{\mathcal{B}}(\mathbf{t})$ for any basis $\mathcal{B}$ of the k-dimensional vector space $\mathbb{F}[t]_{<k}$ over $\mathbb{F}$ and any tuple $\mathbf{t} \in \mathbb{F}^n$ with pairwise different coordinates.*

Proof. By using the algorithm of subsection 4.1 (resp. 4.2), we construct a secret sharing $(k+1) \times k$ matrix $\mathbf{A}$ at level i over $\mathbb{F}$ for a fixed $0 \leq i \leq k-1$ (resp. an all-level secret sharing matrix over $\mathbb{F}$) such that all its entries, except for the last one in the first column are equal. W can do it under assumption

$$\max\Big(\frac{k(k+1)}{2}, \frac{(k-1)k(k+1)}{6}\Big) < \mathrm{card}(\mathbb{F})$$

(resp.

$$\frac{k(k+1)(k^2-2k+4)}{6} < \mathrm{card}(\mathbb{F})).$$

Consequently, by Lemma 2, the rows of the matrix $\mathbf{A}$ do not satisfy the condition for the rows of matrices $\mathbf{A}_{\mathcal{B}}(\mathbf{t})$, where $\mathcal{B}$ is a basis of the vector space $\mathbb{F}[t]_{<k}$, which is the desired conclusion. □

6 Conclusion

We have proposed a new secret sharing scheme which has all the features of the original Shamir's scheme, and some new features too. In general in Shamir's polynomial interpolation secret sharing scheme the secret cannot be placed at any level. We have showed that the secret can be placed at level i if we give some additional assumptions on the values of elementary symmetric polynomials of $t_0, t_1, \ldots, t_{n-1}$. The assumptions define an n-tuple $\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) \in \mathbb{F}^n$ such that the matrix $\mathbf{A}_{poly}(\mathbf{t})$ is a secret sharing matrix at level i.

Corollary 1 to Theorem 2 (formula (6)) specifies where the secret can be placed for a fixed n-tuple $\mathbf{t}$; i.e., as what coefficient. Our scheme, based on an arbitrary secret sharing matrix, allows placement of the secret at any level; i.e., as any of the coefficients $a_0, a_1, \ldots, a_{k-1}$. It results in an option of applying our scheme not only to a single secret but to up to k many secrets with the same shares, and with the same threshold.

7 Acknowledgement

The authors gratefully acknowledge insightful conversations with Dr. Artur Jakubski and his constructive suggestions concerning Shamir's secret sharing scheme and secret sharing matrices.

References

[1] C.A. Asmuth and J. Bloom, A modular approach to key safeguarding, *IEEE Trans. on Information Theory* **29** (1983), 208—210.

[2] G.R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proc.* **48** (1979), 313–317.

[3] R.J. Evans and I.M. Isaacs, Generalized Vandermonde determinants and roots of unity of prime order, *Proc. Amer. Math. Soc.* **58** (1976), 51–54.

[4] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, New York Berlin Heidelberg, 1998.

[5] C.-P. Lai and C. Ding, Several Generalizations of Shamir's Secret Sharing Scheme, *Internat. J. Found. Comput. Sci.* **15** (2004), 445–458.

[6] M. Mignotte, How to share a secret, In: Beth T. (Ed.), *Cryptography Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, Springer-Verlag *Lecture Notes in Computer Science* **149** (1983), 371–375.

[7] O.H. Mitchell, Note on determinants of powers, *Amer. J. Math.* **4** (1881), 341–344.

[8] A.J. Menezes, P. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[9] T. Muir, *A treatise on the theory of determinants*, Dover Publ., New York 1960.

[10] A.M. Robert, *A Course in p-adic Analysis*, Springer-Verlag, New York Berlin Heidelberg, 2000.

[11] A. Shamir, How to share a secret, *Communications of the ACM* **22** (1979), 612–613.

[12] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, Cambridge New York, 2005.