# A Secret Sharing Scheme Based on Exponentiation in Galois Fields

Clara M. Gallardo, Leandro Tortosa, Jose F. Vicent, Antonio Zamora

***Abstract*—** To provide more efficient and flexible alternatives for the applications of secret sharing schemes, this paper describes a threshold sharing scheme based on exponentiation of matrices in Galois fields. A significant characteristic of the proposed scheme is that each participant has to keep only one master secret share which can be used to reconstruct different group secrets according to the number of threshold values.

***Keywords*—** Computer security, cryptography, public-key cryptography, threshold schemes, prepositioned secret sharing.

## I. Introduction

Secret-sharing schemes are a tool used in many cryptographic protocols. The motivation for secret sharing is secure key management [1]. In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (e.g. the person who knows the key becomes unavailable, or the computer which stores the key is destroyed), then all the important files become inaccessible A secret sharing scheme involves a dealer who has a secret, a finite set of *n* participants, and a collection *A* of subsets of the set of participants called the access structure.

A perfect secret sharing scheme for *A* is a method by which the dealer distributes shares to the parties such that: (1) any subset in *A* can reconstruct the secret from its shares, and (2) any subset not included in *A* can never reveal any partial information on the secret (in the information theoretic sense). Secret sharing schemes were first introduced by Blakley [4] and Shamir [22] for the threshold case, that is, for the case where the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold. Secret sharing schemes for general access structures were introduced by Ito, Saito, and Nishizeki [14]. They tried to realize the general access structure by using the multiple shadows assignment approach. Later Benaloh and Leichter [3] proposed a simpler method of developing a secret sharing scheme by translating the access structure into a monotone formula. They also stated that there exists access structures for which any generalized secret sharing must give some trustee shares which are from a domain larger than that of the secret. However, this conclusion may only applied to those secret sharing schemes without cryptographic assumption.

*This work was partially supported by the Spanish grants GVPRE/2008/363*

J.F. Vicent. Ciencia de la Computación e Inteligencia Artificial. Universidad de Alicante. Campus de San Vicente del Raspeig, Ap. Correos 99, E-03080, Alicante. SPAIN. (+34 96 590 3400 x 2990; fax: +34 96 590 3902; jvicent@dccia.ua.es)
C. Gallardo. Ciencia de la Computación e Inteligencia Artificial. Universidad de Alicante. Campus de San Vicente del Raspeig, Ap. Correos 99, E-03080, Alicante. SPAIN. (c.gallardo.calero@gmail.com)
L. Tortosa. Ciencia de la Computación e Inteligencia Artificial. Universidad de Alicante. Campus de San Vicente del Raspeig, Ap. Correos 99, E-03080, Alicante. SPAIN. ( tortosa@dccia.ua.es)
A. Zamora. Ciencia de la Computación e Inteligencia Artificial. Universidad de Alicante. Campus de San Vicente del Raspeig, Ap. Correos 99, E-03080, Alicante. SPAIN. ( zamora@dccia.ua.es)

In general, the ability to redistribute shares of secrets between different sets of shareholders is useful for a wide range of applications. Consider the following examples:

- Multiparty signature schemes. Business organizations may use digital signature schemes to sign legal documents they exchange with counterparties. Such schemes are typically asymmetric: an organization generates signatures with a *private* key known only to itself, and the counterparties verify signatures with a corresponding *public* key. To prevent a single rogue agent from signing documents without proper authorization, the organization may require multiple agents to generate signatures with a multiparty signature scheme [10]-[11]-[12]-[13]-[19] that distribute shares of the private key to the agents. Over time, the organization will need to give shares of the private key to agents who join, and invalidate the shares of agents who leave. Changing the private key each time agents join or leave would require revocation of the well-known public key. A better solution would be to redistribute shares of the private key in a way that invalidates old shares and obviates the need for public key revocation.
- Distributed key servers**:** Recent distributed storage systems, such as [2]-[6]-[9]-[20]-[24]-[25], use disk space on (potentially) untrusted storage devices to store data. Clients may encrypt data before handing it off to the storage system. One way for clients to store their encryption keys is to employ threshold sharing schemes to distribute shares of the keys to a set of *key servers*. Of course, since clients must store keys for as long as they store the encrypted data, a mobile adversary may have a large window of opportunity to compromise multiple key servers, and thus obtain enough shares to reconstruct the keys. To counter the adversary, the uncompromised key

servers could periodically redistribute shares of the keys to new, uncompromised servers. The adversary would then need to restart the process of compromising servers, assuming that old shares cannot be combined with new shares to reconstruct the secret.

Both of these applications must support dynamic shareholder membership, and protect secrets from mobile adversaries. In the multiparty signature system, gents may join or leave the organization, while in the storage system, key servers may be added or removed for maintenance or security purposes. It may also be advantageous to change the threshold value of the underlying sharing scheme to accommodate new policies. In both applications, the system needs to retain the original secrets when generating new shares and invalidating old shares. More importantly, to prevent faulty old shareholders from corrupting the shares of new shareholders, new shareholders must be able to verify the validity of their shares after redistribution (i.e., that their shares can be used to reconstruct the secret).

Originally the secret sharing scheme are motivated by the problem of secure information storage but secret sharing schemes have found numerous other applications in cryptography and distributed computing, secure multiparty computations, threshold cryptography, access control, and attribute based encryption [5]-[7]-[14]-[15]-[16].

For example a (*n, k*)-threshold image secret sharing scheme [23], where $k \leq n$, divided a secret image into *n* shadow images (known as the shadows) in the way that requires at least *k* shadows for the secret reconstruction.

A major problem with secret sharing schemes is that the shares' size in the best known secret sharing schemes realizing general access structures is exponential in the number of parties within the access structure. Thus, the known constructions for general access structures are impractical. This is true even for explicit access structures (e.g. access structures whose characteristic function can be computed by a small uniform circuit). On the other hand, the best known lower bounds on the shares' size for sharing a secret with respect to an access structure are far from the above upper bounds.

We present a new $(n,k)$ verifiable secret distribution protocol for Shamir's threshold sharing scheme, which is based on the powers of square matrices in Galois fields and a scheme proposed by Charnes, Pieprzyk and Safari-Naini (see [8]). The security of the scheme proposed is guaranteed since it is based in the well known discrete logarithm problem in *GF*(*q*). The use of Galois fields of the form *GF*(2*l*), called *binary extension fields*, is ubiquitous in a variety of areas ranging from cryptography to storage system reliability. These algebraic structures are used to compute codewords in linear erasure codes, evaluate and interpolate polynomials in Shamir's secret sharing algorithm, compute algebraic signatures over variable-length strings of symbols [21] and encrypt blocks of data in Rijndael's cipher. These applications typically perform computation in either *GF*(28) or *GF*(216).

We have considered to present the secret sharing scheme as an $(n,\ k)$ scheme, that is, we divide the secret into *n* parts and *k* of them are needed to recover the secret.

## II. MATHEMATICAL BACKGROUND

The field $GF(2^l)$ is defined by a set of $2^l$ unique elements that is closed under both addition and multiplication, in which every non-zero element has a multiplicative inverse and every element has an additive inverse. Addition and multiplication in a Galois field are associative, distributive and commutative. The Galois field $GF(2^l)$ may be represented by the set of all polynomials of degree at most $l-1$, with coefficients from the binary field *GF*(2) (the field defined over the set of elements 0 and 1). Thus, the 4-bit field element $a = 0111$ has the polynomial representation $a(x) = x^2+x+1$.

In contrast to finite fields defined over an integer prime, the field $GF(2^l)$ is defined over an irreducible polynomial of degree *l* with coefficients in *GF*(2). An irreducible polynomial is analogous to a prime number in that it cannot be factored into two non-trivial factors. Addition and subtraction in *GF*(2) is done with the bitwise XOR operator, and multiplication is the bitwise AND operator. It follows that addition and subtraction in $GF(2^l)$ are also carried out using the bitwise XOR operator, while multiplication turns out to be more complicated. In order to multiply two elements $a(x) \cdot b(x) \in GF(2^1)$*;* we perform polynomial multiplication of $a(x) \cdot b(x)$ and reduce the product modulo an *l*-degree irreducible polynomial over *GF*(2). Division among field elements is computed in a similar fashion using polynomial division. The *order* of a non-zero field element ord(α) is the smallest positive *i* such that $\alpha^i = 1$. If the order of an element $\alpha \in GF(2^1)$ is $2l-1$, then α is primitive. In this case, α generates $GF(2^1)$ *i. e.*, all non-zero elements of $GF(2^1)$ are powers of α. For a detailed and rigorous explanation of finite fields, please refer to [17].

## III. RESULTS OBTAINED

We assume that we have a set of all secrets *K*. The set of all shares is *S* and the set of all participants is *P* (|*K*| = n). Secret sharing schemes consists of two algorithms. The first is called the dealer, is generates and distributes shares among the participants. The second is called the combiner, it collects shares from the participants and recomputes the secret only for sets of shares belonging to the access structure. The formal definition is given below.

**Definition 1:** A secret sharing scheme is a collection of two algorithms. The first (the dealer) is a probabilistic mapping

$$D : K \rightarrow S_1 \times S_2 \times \ldots \times S_n$$

where $S_i \subset S\ (i = 1,2,\ldots,n)$ and $S_i$ is a subset which is used to generate a share for the participants $P_i \in P$. The second (the combiner) is a function

$$C : S_{i_1} \times S_{i_2} \times \ldots \times S_{i_t} \to K$$

Such that if the corresponding subset of participants $\{P_{i_1} \times P_{i_2} \times \ldots \times P_{i_t}\}$ belongs to the access structure Π, it produces the secret $\mathrm{K} \in K$. The combiner fails to recomputed the secret if the subset of participants does not belong to the access structure Π.

A perfect secret sharing scheme is called ideal if the length of each participants share is equal to the length of the secret.

An example of a perfect and ideal scheme is the Shamir *(t,n)* threshold scheme. In this scheme any subset of *t* out of *n* participants can recreate the secret. In this scheme the dealer selects at random a polynomial of degree *(t-1)* over a *GF(q)*. The polynomial has the following form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{t-1} x^{t-1}$$

where the coefficients $a_i \ for\ i = 0,1,\ldots,t-1$ are chosen randomly and uniformly from *GF(q)*.

The secret key is *k = f(0)* and the *i-th* participant's share is

$$p_i \to s_i = f(i)$$

for all $p_i \in P$.

The combiner takes shares from the participants and determines f(x). This always succeeds if the combiner has at least t different shares, but fails if the number of shares is less than t.

We define a conditionally secure Shamir secret scheme using exponentiation in Galois fields. This scheme can withstand the lost of polynomials bounded number of shares. A covert channel cannot occur in a conditionally secure Shamir scheme unless the discrete logarithm problem is solvable in polynomial time.

## IV. Case one

In this scheme we establish that the base of the exponentiation is an integer and the exponent is a matrix. More exactly, the base is an element belonging to $GF(8)$ and, consequently, is a polynomial. With the aim to simplify the computations, we will take its numerical representation, as we will show in case one example.

Let us consider a generator $g$ of $GF(8)$, which is known by all the participants. Let

$$f(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3 + \ldots + A_{k-1} x^{k-1},$$

the function where

$$A_r \in M_{t\times t}(9_7) \text{ for } r = 0 \ldots k-1$$

and consider the secret $s = f(0) = A_0 \in M_{t\times t}(9_7)$.

To begin with, we compute the initial conditions $c_i = f(i)$ that the dealer will distribute among all the participants, using a public channel. Remark that $c_i \in M_{t\times t}(9_7)$ for $i = 1 \ldots n$.

In the next step, each of the participants will compute a part of the secret by means of $s_i = g^{c_i}$. As we can see, this computation consists of raising a polynomial to a matrix. This type of computation motivates the following definition.

**Definition 2:** Let $A = (a_{ij}) \in M_{t\times t}(\mathrm{Z}_7)$ and $n \in GF(8)$. We define the power function $\zeta$ as

$$\zeta(n, A) = n^A = (n^{a_{ij}}) \in M_{t\times t}(GF(8)).$$

So, $s_i = g^{c_i} = \zeta(g, c_i) \in M_{t\times t}(GF(8))$. (1)

To recover the secret, we choose *k* parts in a random way. As

$$A_0 + A_1 i + A_2 i^2 + A_3 i^3 + \ldots + A_{k-1} i^{k-1}$$

and

$$s_i = g^{c_i} = g^{f(i)} = g^{A_0 + A_1 i + A_2 i^2 + A_3 i^3 + \ldots + A_{k-1} i^{k-1}}$$

are matrices, we need to use the above definition. We can say that the element $(j, p)$ of the matrix $s_i$ is as follows

$$g^{a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \ldots + a_{k-1,jp} i^{k-1}} \quad (2),$$

where $a_{r,jp}$ is the element $(j, p)$ of $A_r$.

We use the following notation

$$f_{jp}(i) = g^{a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \ldots + a_{k-1,jp} a^{k-1}}$$

so that

$$s_i = \begin{pmatrix} f_{11}(i) & f_{12}(i) & \cdots & f_{1t}(i) \\ f_{21}(i) & f_{22}(i) & \cdots & f_{2t}(i) \\ \vdots & \vdots & & \vdots \\ f_{t1}(i) & f_{t2}(i) & \cdots & f_{tt}(i) \end{pmatrix} \text{with } i = 1,\ldots n$$

Starting from the expression (2) and performing a break down for all the elements of the matrix (remark that the last step represents a change in the notation to simplify it)

$$f_{jp}(i) = g^{a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \ldots + a_{k-1,jp} i^{k-1}} =$$

$$g^{a_{0,jp}} g^{a_{1,jp} i} g^{a_{2,jp} i^2} \cdots g^{a_{k-1,jp} i^{k-1}} =$$

$$g^{a_{0,jp}} (g^{a_{1,jp}})^i (g^{a_{2,jp}})^{i^2} \cdots (g^{a_{k-1,jp}})^{i^{k-1}} =$$

$$g_{0,jp} (g_{1,jp})^i (g_{2,jp})^{i^2} \cdots (g_{k-1,jp})^{i^{k-1}}.$$

Applying again this break down the matrix $s_i$ is:

$$s_i = \begin{pmatrix} g_{0,11}(g_{1,11})^i \cdots (g_{k-1,11})^{i^{k-1}} & \cdots & g_{0,1t}(g_{1,1t})^i \cdots (g_{k-1,1t})^{i^{k-1}} \\ g_{0,21}(g_{1,21})^i \cdots (g_{k-1,21})^{i^{k-1}} & \cdots & g_{0,2t}(g_{1,2t})^i \cdots (g_{k-1,2t})^{i^{k-1}} \\ \vdots & & \vdots \\ g_{0,t1}(g_{1,t1})^i \cdots (g_{k-1,t1})^{i^{k-1}} & \cdots & g_{0,tt}(g_{1,tt})^i \cdots (g_{k-1,tt})^{i^{k-1}} \end{pmatrix} \quad (3).$$

Now, we substitute $i$ for the index of the participants that are included in the authorized set. We suppose, without introducing any restriction, that the $k$ authorized participants are labeled as 1, 2, …, $k$.

We obtain $s_i$ as a numerical matrix $t \times t$ in $(1)$ and we also obtain a matrix $t \times t$ with $kt^2$ unknowns in $(3)$. Equating the two expressions for each of the participants, we obtain $t^2$ systems of $k$ equations, with $k$ unknowns each one. These systems may be solved by means of logarithms and they are compatible with a unique solution, since the determinant of the coefficients has the structure of the Vandermonde determinant.

From the solutions of the systems we can compute the coefficients of the matrices, taking logarithms of $A_r$ in base $g$. From the set of these coefficients, we select some of them, that is $A_0$. This constitutes the original secret that has been recovered.

## V. Case One: Example

Let us consider $g = 2$ as a generator of $GF(8)$, and let

$$f(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3$$

with

$$A_1 = \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 2 & 5 \\ 1 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} 1 & 0 \\ 6 & 3 \end{pmatrix},$$

whose coefficients are in $Z_7$ and consider the secret

$$\mathrm{s} = f(0) = A_0 = \begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}.$$

The administrator computes the initial conditions

$$c_i = f(i)$$

$$c_1 = f(1) = \begin{pmatrix} 5 & 3 \\ 1 & 5 \end{pmatrix},$$

$$c_2 = f(2) = \begin{pmatrix} 1 & 0 \\ 4 & 2 \end{pmatrix},$$

$$c_3 = f(3) = \begin{pmatrix} 6 & 0 \\ 4 & 2 \end{pmatrix},$$

$$c_4 = f(4) = \begin{pmatrix} 5 & 3 \\ 2 & 2 \end{pmatrix},$$

$$c_5 = f(5) = \begin{pmatrix} 4 & 2 \\ 6 & 6 \end{pmatrix},$$

$$c_6 = f(6) = \begin{pmatrix} 2 & 4 \\ 3 & 4 \end{pmatrix},$$

and distributes them to the participants throughout a channel that perhaps is not secure.

Once each participant receives the initial condition everyone computes the corresponding part of the secret, obtaining $s_i = g^{c_i} = \zeta(g, c_i)$,

$$s_1 = g^{c_1} = \begin{pmatrix} 7 & 3 \\ 2 & 7 \end{pmatrix},$$

$$s_2 = g^{c_2} = \begin{pmatrix} 2 & 1 \\ 6 & 4 \end{pmatrix},$$

$$s_3 = g^{c_3} = \begin{pmatrix} 5 & 1 \\ 6 & 4 \end{pmatrix},$$

$$s_4 = g^{c_4} = \begin{pmatrix} 7 & 3 \\ 4 & 4 \end{pmatrix},$$

$$s_5 = g^{c_5} = \begin{pmatrix} 6 & 4 \\ 5 & 5 \end{pmatrix},$$

$$s_6 = g^{c_6} = \begin{pmatrix} 4 & 6 \\ 3 & 6 \end{pmatrix}.$$

Suppose now that the participants 1, 2, 3 and 4 constitute an authorized set and they join their parts in order to recover the whole secret. The administrator performs the required tasks and obtains $s_i$

$$s_i = \begin{pmatrix} g_0 g_1^i g_2^{i^2} g_3^{i^3} & g_4 g_5^i g_6^{i^2} g_7^{i^3} \\ g_8 g_9^i g_{10}^{i^2} g_{11}^{i^3} & g_{12} g_{13}^i g_{14}^{i^2} g_{15}^{i^3} \end{pmatrix}.$$

Replacing i by 1, 2, 3 and 4 and equalizing the resulting matrices with the numerical contribution of each participant, that is

$$s_1 = \begin{pmatrix} g_0 g_1 g_2 g_3 & g_4 g_5 g_6 g_7 \\ g_8 g_9 g_{10} g_{11} & g_{12} g_{13} g_{14} g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 2 & 7 \end{pmatrix},$$

$$s_2 = \begin{pmatrix} g_0 g_1^2 g_2^4 g_3 & g_4 g_5^2 g_6^4 g_7 \\ g_8 g_9^2 g_{10}^4 g_{11} & g_{12} g_{13}^2 g_{14}^4 g_{15} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 6 & 4 \end{pmatrix},$$

$$s_3 = \begin{pmatrix} g_0 g_1^3 g_2^2 g_3^6 & g_4 g_5^3 g_6^2 g_7^6 \\ g_8 g_9^3 g_{10}^2 g_{11}^6 & g_{12} g_{13}^3 g_{14}^2 g_{15}^6 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 6 & 4 \end{pmatrix},$$

$$s_4 = \begin{pmatrix} g_0 g_1^4 g_2^2 g_3 & g_4 g_5^4 g_6^2 g_7 \\ g_8 g_9^4 g_{10}^2 g_{11} & g_{12} g_{13}^4 g_{14}^2 g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 4 & 4 \end{pmatrix}.$$

At last, the administrator must perform the comparison between matrices (the comparison is element by element). The outcome of this process is that we have four systems of four equations. We illustrate with an example of the element $(1,1)$

$$\left.\begin{aligned} g_0 g_1 g_2 g_3 &= 7 \\ g_0 g_1^2 g_2^4 g_3 &= 2 \\ g_0 g_1^3 g_2^2 g_3^6 &= 5 \\ g_0 g_1^4 g_2^2 g_3 &= 7 \end{aligned}\right\}.$$

As we have already mentioned theoretically, the system has a unique solution since we arrive to a Vandermonde type determinant. Consequently, we can solve these four systems with no compatibility problem. The solutions for our example are:

$$g_0 = 7,\ g_1 = 6,\ g_2 = 4,\ g_3 = 2,$$
$$g_4 = 4,\ g_5 = 3,\ g_6 = 7,\ g_7 = 1,$$
$$g_8 = 2,\ g_9 = 1,\ g_{10} = 2,\ g_{11} = 4,$$
$$g_{12} = 1,\ g_{13} = 2,\ g_{14} = 2,\ g_{15} = 3.$$

As $g = 2$, we can easily compute the coefficients of the initial matrices. More detailed, from $g_0$, $g_4$, $g_8$ and $g_{12}$ we can compute the coefficients $A_0$ and recover the original secret:

$$g_0 = 7 \rightarrow \log_2 7 = 5$$
$$g_4 = 4 \rightarrow \log_2 4 = 2$$
$$g_8 = 2 \rightarrow \log_2 2 = 1$$
$$g_{12} = 1 \rightarrow \log_2 1 = 0$$

and, therefore

$$A_0 = s = \begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}.$$

## VI. Case Two

In this scheme, we have taken a matrix as the base for the exponentiation and an integer as the exponent. Certainly, the base is a matrix whose elements are in $GF(8)$ so it is a polynomial matrix. To work with, we choose its numerical representation. Let us consider $G \in M_{t\times t}(GF(8))$ a square matrix whose elements are generators of $GF(8)$, and which is known by all the participants. Let the function

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_{k-1} x^{k-1},$$

where

$$a_r \in 9_7 \text{ for } r = 0,\ldots,k-1$$

and consider the secret

$$s = G^{f(0)} = G^{a_0} \in M_{t\times t}(GF(8)).$$

As we have seen in case 1 we begin computing $c_i = f(i) \in 9_7$ for $i = 0 \ldots n$, that is, the initial conditions that will be distributed to all the participants using a public channel.

Then, each of the participants computes the corresponding part of the secret, as $s_i = G^{c_i}$. As we see, the operation involved in this step consists of a power of matrices, although we are not going to perform the usual power of matrices, but the power of each of the elements of the matrix. That specific operation leads us to the following definition:

**Definition 3:** Let $A = (a_{ij}) \in M_{t\times t}(GF(8))$, and $n \in 9_7$. We define the power function $\psi$ as

$$\psi(A,n) = A^n = (a_{ij}^n) \in M_{t\times t}(GF(8)).$$

Then, $s_i = \psi(G, c_i)$ (4) and each participant obtains a part of the secret, which is a matrix of $M_{t\times t}(GF(8))$.

To recover the secret, we choose *k* parts in a random way. As $G$ is a matrix and

$$a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \ldots + a_{k-1} i^{k-1} \in Z_7,$$

we need use the definition (2) to compute

$$s_i = G^{c_i} = G^{f(i)} = G^{a_0 + a_1 i + a_2 i^2 + a_3 i^3 + \ldots + a_{k-1} i^{k-1}}$$

where the element $(j,p)$ of $s_i$ is as follows

$$g_{jp}^{a_0 + a_1 i + a_2 i^2 + \ldots + a_{k-1} i^{k-1}},$$

and $g_{jp}$ is the element $(j,p)$ of the matrix $G$.

To simplify we use the following notation

$$f_{jp}(i) = g_{jp}^{a_0 + a_1 i + a_2 i^2 + \ldots + a_{k-1} a^{k-1}}$$

so that

$$s_i = \begin{pmatrix} f_{11}(i) & f_{12}(i) & \cdots & f_{1t}(i) \\ f_{21}(i) & f_{22}(i) & \cdots & f_{2t}(i) \\ \vdots & \vdots & & \vdots \\ f_{t1}(i) & f_{t2}(i) & \cdots & f_{tt}(i) \end{pmatrix} \text{with } i = 1,\ldots n$$

.(4)

Now, we perform a similar break down as we used in the case before, for all the elements of the matrix

$$f_{jp}(i) = g_{jp}^{a_0 + a_1 i + a_2 i^2 + \ldots + a_{k-1} i^{k-1}} =$$
$$g_{jp}^{a_0} g_{jp}^{a_1 i} g_{jp}^{a_2 i^2} \cdots g_{jp}^{a_{k-1} i^{k-1}} = (g_{jp}^{a_0})(g_{jp}^{a_1})^i (g_{jp}^{a_2})^{i^2} \cdots (g_{jp}^{a_{k-1}})^{i^{k-1}} \quad (5)$$

and we apply a change in the notation $g_{jp}^{a_r} = g_{jp,r}$ obtaining the expression

$$(g_{jp,0})(g_{jp,1})^i (g_{jp,2})^{i^2} \cdots (g_{jp,k-1})^{i^{k-1}}.$$

We use the previous break down for the expression $(5)$ and, as we have already mentioned, we choose the participants numbered as 1, 2, …*k*.

We obtain $s_i$ as a numerical matrix $t \times t$ in $(4)$ and we also obtain a matrix $t \times t$ with $kt^2$ unknowns in $(5)$. Equating the two expressions for each of the participants, we obtain $t^2$ systems of *k* equations, with *k* unknowns each one. These systems may be solved by means of logarithms and they are compatible with a unique solution, since the determinant of the coefficients has the structure of the Vandermonde determinant.

Selecting the solutions that differ in *k*, and composing the matrix $G^{a_0} = k$ we can recover the secret.

## VII. Case two: Example

Let

$$G = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix} \in M_{2\times 2}(GF(8)),$$

and

$$f(x) = 5 + 4x + 2x^2 + x^3$$

the function with coefficients in $Z_7$ with the secret

$$s = G^{f(0)} = G^5 = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix} \in M_{2\times 2}(GF(8))$$

The administrator computes the initial conditions

$$c_i = f(i) \in 9_7$$

and distributes them

$$c_1 = f(1) = 5,\ c_2 = f(2) = 1,$$
$$c_3 = f(3) = 6,\ c_4 = f(4) = 5,$$
$$c_5 = f(5) = 4,\ c_6 = f(6) = 2,$$

among all the participants throughout a channel that perhaps is not secure.

Once each participant receives the initial condition, everyone computes the corresponding part of the secret

$$s_i = G^{c_i} = \psi(G, c_i) \in GF(8),$$

obtaining

$$s_1 = G^{c_1} = G^5 = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix},$$
$$s_2 = G^{c_2} = G^1 = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix},$$
$$s_3 = G^{c_3} = G^6 = \begin{pmatrix} 4 & 6 \\ 2 & 6 \end{pmatrix},$$
$$s_4 = G^{c_4} = G^5 = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix},$$
$$s_5 = G^{c_5} = G^4 = \begin{pmatrix} 2 & 7 \\ 5 & 7 \end{pmatrix},$$
$$s_6 = G^{c_6} = G^2 = \begin{pmatrix} 4 & 5 \\ 7 & 5 \end{pmatrix}.$$

Suppose now that the participants 1, 2, 3 and 4 constitute an authorized set and they join their parts in order to recover the whole secret. The administrator performs the required tasks and obtains

$$s_i = \begin{pmatrix} g_0 g_1^i g_2^{i^2} g_3^{i^3} & g_4 g_5^i g_6^{i^2} g_7^{i^3} \\ g_8 g_9^i g_{10}^{i^2} g_{11}^{i^3} & g_{12} g_{13}^i g_{14}^{i^2} g_{15}^{i^3} \end{pmatrix}.$$

Replacing *i* by 1, 2, 3 and 4 and equalizing the resulting matrices with the numerical contribution of each participant, that is,

$$s_1 = \begin{pmatrix} g_0 g_1 g_2 g_3 & g_4 g_5 g_6 g_7 \\ g_8 g_9 g_{10} g_{11} & g_{12} g_{13} g_{14} g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix},$$
$$s_2 = \begin{pmatrix} g_0 g_1^2 g_2^4 g_3 & g_4 g_5^2 g_6^4 g_7 \\ g_8 g_9^2 g_{10}^4 g_{11} & g_{12} g_{13}^2 g_{14}^4 g_{15} \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix},$$
$$s_3 = \begin{pmatrix} g_0 g_1^3 g_2^2 g_3^6 & g_4 g_5^3 g_6^2 g_7^6 \\ g_8 g_9^3 g_{10}^2 g_{11}^6 & g_{12} g_{13}^3 g_{14}^2 g_{15}^6 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 2 & 6 \end{pmatrix},$$
$$s_4 = \begin{pmatrix} g_0 g_1^4 g_2^2 g_3 & g_4 g_5^4 g_6^2 g_7 \\ g_8 g_9^4 g_{10}^2 g_{11} & g_{12} g_{13}^4 g_{14}^2 g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix}.$$

At last, the administrator must perform the comparison between matrices (the comparison is element by element). The outcome of this process is that we have four systems of four equations. We illustrate with an example

$$\left.\begin{aligned} g_0 g_1 g_2 g_3 &= 7 \\ g_0 g_1^2 g_2^4 g_3 &= 2 \\ g_0 g_1^3 g_2^2 g_3^6 &= 5 \\ g_0 g_1^4 g_2^2 g_3 &= 7 \end{aligned}\right\}.$$

As we have already mentioned theoretically, the system has a unique solution since we arrive to a Vandermonde type determinant. Consequently, we can solve these four systems with no compatibility problem. The solutions for our example are

$$g_0 = 7,\ g_1 = 6,\ g_2 = 4,\ g_3 = 2,$$
$$g_4 = 2,\ g_5 = 7,\ g_6 = 5,\ g_7 = 3,$$
$$g_8 = 4,\ g_9 = 3,\ g_{10} = 7,\ g_{11} = 5,$$
$$g_{12} = 2,\ g_{13} = 7,\ g_{14} = 5,\ g_{15} = 3.$$

As we can check, $g_0$, $g_4$, $g_8$ and $g_{12}$ are the elements of the matrix

$$G^{a_0} = G^5 = s = \begin{pmatrix} 7 & 2 \\ 4 & 2 \end{pmatrix}$$

and we have already recovered the secret.

## VIII. Case three

We have considered in this scheme than the base as the exponent both are matrices. The base is a matrix with elements in $GF(8)$ and therefore a polynomial matrix, but like in the previous cases, we choose his numeric representation.

This scheme begins different that second case, but it takes place to one point in the process where it follows a similar way and it resolve in the same way.

Let be $G \in M_{t\times t}(GF(8))$ a square matrix know for all of participants whose elements are generators of *GF(8)*. Let be a function

$$f(x) = A_0 + A_1 x + A_2 x^2 + \cdots + A_{k-1} x^{k-1},$$

where

$$A_r \in M_{t\times t}(Z_p) \text{ for } r = 0,\ldots,k-1$$

and let be a secret value $s = f(0) = A_0$.

This scheme begins when administrator computes the initial conditions $c_i = f(i)$ and he distribute them between the participants using a public channel. Note than

$$c_i \in M_{t\times t}(Z_p), \text{ with } i = 1,\ldots,n.$$

Each participant computed his part of the secret $s_i = G^{c_i}$. As we can be observed, this operation involves a matrix to the power of matrix, and therefore the following definition becomes necessary:

**Definition 4:** Let be $A = (a_{ij}) \in M_{t\times t}(GF(8))$, and $B = (b_{ij}) \in M_{t\times t}(9_7)$. We defined the power function $\gamma$ like this

$$\gamma(A,B) = A^B = (a_{ij}^{b_{ij}}) \in M_{t\times t}(GF(8)).$$

In order to recover the secret, we randomly choose $k$ parts. On the one hand, we have than

$$s_i = G^{c_i} = G^{f(i)} = G^{A_0 + A_1 i + A_2 i^2 + \cdots + A_{k-1} i^{k-1}}$$

and, for another one, the element of the matrix

$$A_0 + A_1 i + A_2 i^2 + \cdots + A_{k-1} i^{k-1}$$

have the form

$$a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \cdots + a_{k-1,jp} i^{k-1}$$

where $a_{r,jp}$ is the element $(j,p)$ of the matrix $A_r$ with $r = 0,\ldots,k-1$.

If we join both expressions and apply the definition 3, we obtain

$$s_i = \begin{pmatrix} f_{11}(i) & f_{12}(i) & \cdots & f_{1t}(i) \\ f_{21}(i) & f_{22}(i) & \cdots & f_{2t}(i) \\ \vdots & \vdots & & \vdots \\ f_{t1}(i) & f_{t2}(i) & \cdots & f_{tt}(i) \end{pmatrix} \text{ with } i = 1,\ldots n,$$

(6)

where

$$f_{jp}(i) = g_{jp}^{a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \cdots + a_{k-1} i^{k-1}}$$

and $g_{jp}$ is the element $(j,p)$ of the matrix $G$ for $j,p = 1,\ldots t$.

Now, we perform a similar break down as we used in the case before, for all the elements of the matrix

$$\begin{aligned} f_{jp}(i) &= g_{jp}^{a_{0,jp} + a_{1,jp} i + a_{2,jp} i^2 + \ldots + a_{k-1,jp} i^{k-1}} \\ &= g_{jp}^{a_{0,jp}} g_{jp}^{a_{1,jp},i} g_{jp}^{a_{2,jp} i^2} \cdots g_{jp}^{a_{k-1,jp} i^{k-1}} \\ &= (g_{jp}^{a_{0,jp}})(g_{jp}^{a_{1,jp}})^i (g_{jp}^{a_{2,jp}})^{i^2} \cdots (g_{jp}^{a_{k-1,jp}})^{i^{k-1}} \end{aligned} \quad (7)$$

and we apply a change in the notation

$$g_{jp}^{a_{r,jp}} = g_{jp,r}$$

obtaining the expression

$$(g_{jp,0})(g_{jp,1})^i (g_{jp,2})^{i^2} \cdots (g_{jp,k-1})^{i^{k-1}}.$$

We use the previous break down for the expression (7) and, as we have already mentioned, we choose the participants numbered as 1, 2, …, *k*.

We obtain $s_i$ as a numerical matrix $t\times t$ in (6) and we also obtain a matrix $t\times t$ with $kt^2$ unknowns in (7). Equating the two expressions for each of the participants, we obtain $t^2$ systems of *k* equations, with *k* unknowns each one. These systems may be solved by means of logarithms and they are compatible with a unique solution, since the determinant of

the coefficients has the structure of the Vandermonde determinant.

Selecting the solutions that differ in $k$, and composing the matrix $G^{a_0} = k$ we can recover the secret.

## IX. Case three: example

Let

$$G = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix} \in M_{2\times 2}(GF(8))$$

and the function

$$f(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3$$

With

$$A_0 = \begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix},\ A_1 = \begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 2 & 5 \\ 1 & 1 \end{pmatrix},$$

$A_3 = \begin{pmatrix} 1 & 0 \\ 6 & 3 \end{pmatrix}$, with coefficients in $9_7$ and let be the secret

$$s = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}} = \begin{pmatrix} 7 & 5 \\ 5 & 1 \end{pmatrix}.$$

The administrator computes the initial conditions

$$c_i = f(i)$$

and distributes them

$$c_1 = f(1) = \begin{pmatrix} 5 & 3 \\ 1 & 5 \end{pmatrix},$$

$$c_2 = f(2) = \begin{pmatrix} 1 & 0 \\ 4 & 2 \end{pmatrix},$$

$$c_3 = f(3) = \begin{pmatrix} 6 & 0 \\ 4 & 2 \end{pmatrix},$$

$$c_4 = f(4) = \begin{pmatrix} 5 & 3 \\ 2 & 2 \end{pmatrix},$$

$$c_5 = f(5) = \begin{pmatrix} 4 & 2 \\ 6 & 6 \end{pmatrix},$$

$$c_6 = f(6) = \begin{pmatrix} 2 & 4 \\ 3 & 4 \end{pmatrix}$$

among all the participants throughout a channel that perhaps is not secure.

Once each participant receives the initial condition, everyone computes the corresponding part of the secret

$$s_i = G^{c_i} = \gamma(G, c_i),$$

obtaining the following parts

$$s_1 = G^{c_1} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 5 & 3 \\ 1 & 5 \end{pmatrix}} = \begin{pmatrix} 7 & 4 \\ 5 & 2 \end{pmatrix},$$

$$s_2 = G^{c_2} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 1 & 0 \\ 4 & 2 \end{pmatrix}} = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix},$$

$$s_3 = G^{c_3} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 6 & 0 \\ 4 & 2 \end{pmatrix}} = \begin{pmatrix} 5 & 1 \\ 3 & 5 \end{pmatrix},$$

$$s_4 = G^{c_4} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 5 & 3 \\ 2 & 2 \end{pmatrix}} = \begin{pmatrix} 7 & 4 \\ 7 & 5 \end{pmatrix},$$

$$s_5 = G^{c_5} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 4 & 2 \\ 6 & 6 \end{pmatrix}} = \begin{pmatrix} 6 & 5 \\ 2 & 6 \end{pmatrix},$$

$$s_6 = G^{c_6} = \begin{pmatrix} 2 & 3 \\ 5 & 3 \end{pmatrix}^{\begin{pmatrix} 2 & 4 \\ 3 & 4 \end{pmatrix}} = \begin{pmatrix} 4 & 7 \\ 6 & 7 \end{pmatrix}.$$

Suppose now that the participants 1, 2, 3 and 4 constitute an authorized set and they join their parts in order to recover the whole secret. The administrator performs the required tasks and obtains $s_i$

$$s_i = \begin{pmatrix} g_0 g_1^i g_2^{i^2} g_3^{i^3} & g_4 g_5^i g_6^{i^2} g_7^{i^3} \\ g_8 g_9^i g_{10}^{i^2} g_{11}^{i^3} & g_{12} g_{13}^i g_{14}^{i^2} g_{15}^{i^3} \end{pmatrix}.$$

Replacing $i$ by 1, 2, 3 and 4 and equalizing the resulting matrices with the numerical contribution of each participant, that is,

$$s_1 = \begin{pmatrix} g_0 g_1 g_2 g_3 & g_4 g_5 g_6 g_7 \\ g_8 g_9 g_{10} g_{11} & g_{12} g_{13} g_{14} g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 4 \\ 5 & 2 \end{pmatrix},$$

$$s_2 = \begin{pmatrix} g_0 g_1^2 g_2^4 g_3 & g_4 g_5^2 g_6^4 g_7 \\ g_8 g_9^2 g_{10}^4 g_{11} & g_{12} g_{13}^2 g_{14}^4 g_{15} \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix},$$

$$s_3 = \begin{pmatrix} g_0 g_1^3 g_2^2 g_3^6 & g_4 g_5^3 g_6^2 g_7^6 \\ g_8 g_9^3 g_{10}^2 g_{11}^6 & g_{12} g_{13}^3 g_{14}^2 g_{15}^6 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 3 & 5 \end{pmatrix},$$

$$s_4 = \begin{pmatrix} g_0 g_1^4 g_2^2 g_3 & g_4 g_5^4 g_6^2 g_7 \\ g_8 g_9^4 g_{10}^2 g_{11} & g_{12} g_{13}^4 g_{14}^2 g_{15} \end{pmatrix} = \begin{pmatrix} 7 & 4 \\ 7 & 5 \end{pmatrix}.$$

At last, the administrator must perform the comparison between matrices (the comparison is element by element). The outcome of this process is that we have four systems of four equations.

$$\left.\begin{aligned} g_0 g_1 g_2 g_3 &= 7 \\ g_0 g_1^2 g_2^4 g_3 &= 2 \\ g_0 g_1^3 g_2^2 g_3^6 &= 5 \\ g_0 g_1^4 g_2^2 g_3 &= 7 \end{aligned}\right\}.$$

As we have already mentioned theoretically, the system has a unique solution since we arrive to a Vandermonde type determinant. Consequently, we can solve these four systems with no compatibility problem, obtaining:

$$g_0 = 7,\ g_1 = 6,\ g_2 = 4,\ g_3 = 2,$$

$$g_4 = 5,\ g_5 = 4,\ g_6 = 2,\ g_7 = 1,$$

$$g_8 = 5,\ g_9 = 1,\ g_{10} = 5,\ g_{11} = 2,$$

$$g_{12} = 1,\ g_{13} = 3,\ g_{14} = 3,\ g_{15} = 4.$$

As we can check, $g_0$, $g_4$, $g_8$ and $g_{12}$ are the elements of the matrix

$$G^{A_0} = \mathrm{G}^{\begin{pmatrix} 5 & 2 \\ 1 & 0 \end{pmatrix}} = s = \begin{pmatrix} 7 & 5 \\ 5 & 1 \end{pmatrix}$$

and we have already recovered the secret.

## X. Conclusion

The main idea of this paper is to develop a secret sharing scheme based on power of matrices in Galois fields. The previous work of Shamir [22] and Charnes, Pieprzyk and Safari-Naini [8] have been a reference for the construction of our two schemes.

In this work we describe a secret sharing scheme with disenrollment capability and which resists cheating. Our schemes are secure assuming that calculating the discrete logarithm in *GF(q)* is "difficult" and they use not secure channels to distribute to the participants "initial conditions" – the shares of the secret key. The updated shadows are now used to recover the secret key, which remains the same for subsequent updates of shares.

Our modified shadows are related to the original shadows via the discrete logarithm. So the participants need to secure only one secret key – the initial conditions. If some of the modified shadows are acquired by unauthorized users, the initial conditions are still secure and new shares are easily generated without compromising the security of the system.

We have developed three different cases. In the first case, the base of the powers is an integer and the coefficients of the exponent function are matrices. In the second case the base is a matrix and the exponent is an integer. Finally in the third case the base and the exponent are both matrices.

*References:*


[1] Abascal, P. *Compartir secretos mediante Códigos Correctores.* Thesis of Degree.

[2] Álvarez, R, Tortosa, L., Vicent, J., Zamora, A. "Block Upper Triangular Matrices for Authentication and Integrity". Proceedings of the WSEAS Transactions on Mathematics. Tenerife. Canary Island, Spain 2005.

[3] Benaloh, J. and Leichter, I., "Generalized Secret Sharing and Monotone Functions", Procedings Crypto '88 (1988), pp. 27-35.

[4] Blakley, G.R., "*Safeguarding Cryptography Keys".* Proceedings AFIPS Conference. (1979), 48, pp. 313-317.

[5] Blanco, M.F., "*Construcción afín de un esquema de secreto compartido".* Proceedings of IV Reunión Española sobre Criptología (1996), pp. 67-74.

[6] Bolosky, W.J., Douceur, J.R., Ely, D. and Theimer, M. "Feasibility of a serverless distributed file system deployed on an existing set of desktop PCs". In *Proc. of SIGMETRICS 2000, the Intl. Conf. On Measurement and Modeling of Computing Systems*, pp. 34–43. June 2000.

[7] Cao, C. J., Ma, J.F., **"**Identity-based Constant Round Group Key Exchange Protocol via Secret-Share". Proceedings of WSEAS TRANSACTIONS on SYSTEMS. January 2008

[8] Charnes, C., Pieprzyk, J. & Safari-Naini, R., "*Conditionally Secure Secret Sharing Schemes with Disenrolment Capability".* Proc. ACM Conference on Computer and Communications Security (1994), pp. 89-95.

[9] Dabek, F., Kaashoek, M.F., Karger, D., Morris, R. and Stoica, I. "Wide-area cooperative storage with CFS". In *Proc. of the 18th Symp. on Operating Systems Principles*, pp. 202–215. Oct. 2001.

[10] Frankel, Y., Gemmell,P., MacKenzie, P.D. and Yung, M., "Optimal resilience proactive public-key cryptosystems". In *Proc. of the 38th IEEE Ann. Symp. on Foundations of Computer Science*, pp. 384–393.Oct. 1997.

[11] Frankel, Y., Gemmell, P., MacKenzie, P.D. and Yung, M. "Proactive RSA". In *Proc. of CRYPTO 1997, the 17th Ann. Intl. Cryptology Conf.*, vol. 1294 of *Lecture Notes in Computer Science*, pp. 440–454. Aug. 1997.

[12] Gennaro, R., Jarecki, S., Krawczyk,H., and Rabin, T. "Robust threshold DSS signatures". In *Proc. Of EUROCRYPT 1996, the Intl. Conf. on the Theory and Application of Cryptographic Techniques*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 354–371. May 1996.

[13] Herzberg, A., Jakobsson,M.,.Jarecki, S., Krawczyk, H. and Yung, M. "Proactive public key and signature systems". In *Proc. of the 4th ACM Intl. Conf. on Computer and Communications Security*, pp. 100–110.Apr. 1997.

[14] Ito, M., Saito, A. & Nishizeki, T., "*Secret sharing schemes realizing general access structures".* Proc. IEEE Globecom '87 (1987), pp. 99-102.

[15] Karnin, E.D., Greene, J.W. & Hellman, M., "*On secret sharing systems".* IEEE Transactions on Information Theory (1982), 29, pp. 35-41.

[16] Kim, S.J., Ahn, G.B., Kim, H.J., Won, D.H., "Safe Protocol providing Authentication and Secret Sharing Peer to Peer Computing". Proceedings of WSEAS Transactions and Communications. January 2003

[17] Lidl, R and Niederreiter, H.,. "*Introduction to finite fields and their applications"*. Cambridge University Press, New York, NY, USA, 1986.

[18] Rabin, T. "A simplified approach to threshold and proactive RSA". In *Proc. of CRYPTO 1998, the 18th Ann. Intl. Cryptology Conf.*, vol. 1462 of *Lecture Notes in Computer Science*, pp. 89–104. Aug. 1998.

[19] Rowstron, A. and Druschel, P." Storage management and caching in PAST, a large-scale, persistent peerto- peer storage utility". In *Proc. of the 18th Symp. on Operating Systems Principles*, pp. 188–201. Oct. 2001.

[20] Schwarz, T., Miller, L.. "Store, forget, and check: Using algebraic signatures to check remotely administered storage". *Proceedings of the 26th International Conference on Distributed Computing Systems (ICDCS '06)*, Lisboa, Portugal, July 2006. IEEE.

[21] Shamir, A., "*How to share a secret"*. Communication of the ACM (1979), Vol. 22, pp. 612-613.

[22] Thien, C.C. and Lin, J.C., "Secret image sharing", *Computers & Graphics*, Vol. 26, pp.765–770, 2002.

[23] Wylie, J.J., Bakkaloglu, M., Pandurangan, V., Bigrigg, M.W., Oguz, S., Tew, K., Williams, C., Ganger, G.R. and Khosla, P.K.. "Selecting the right data distribution scheme for a survivable storage system". Tech. Rep. CMU-CS-01-120, Sch. of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, May 2001.

[24] Wylie, J.J., Bigrigg, M.W., Strunk, J.D., Ganger, G.R., Kiliccote, H. and Khosla, P.K. "Survivable information storage systems". *IEEE Computer*, pp. 61–68, Aug. 2000.