Some aspects of multi-variable secret sharing

Umadevi Ganugula and Prabal Paul

C. R. Rao AIMSCS,
University of Hyderabad campus, Gachibowli, Hyderabad-500046.
email: firstname DOT lastname AT gmail DOT com

Abstract. In this paper we introduce a technique that reduces a multi-variable polynomial to a single variable polynomial in such a way that it is easy to evaluate the multi-variable polynomial. Moreover, this single variable polynomial is optimal in certain cases. Based on this lemma, we propose a new optimal multi-variable secret sharing scheme. We improve upon some existing schemes. We propose a secret sharing scheme to realize a compartmental access structure scheme. Using the lemma, we prove that multi-variable secret sharing schemes are just a generalization of Shamir secret sharing scheme, which is based on single variable polynomials.

Keywords: Secret sharing, multi-variable polynomial, Shamir secret sharing scheme.

1 Introduction

A secret sharing scheme is a method where a trusted party called *the dealer* divides a secret s among a finite set of players $\mathbb{P}$ in such a way that a qualified subset of players can reconstruct the secret s. In a (k, n) secret sharing scheme [4, 8], the dealer distributes the secret s among n players as *shares*, such that when any k or more of these players give their shares correctly, the secret s can be uniquely reconstructed, and less than k players cannot get any information about the secret. The value k is usually referred to as the *threshold* of the scheme. A (k, n) secret sharing scheme is *perfect* [10] if k or more players can only reconstruct the secret and less than k players cannot get any information about the secret. The scheme is called *ideal* if the shares are taken from the same domain as that of the secret and size of share(s) is equal to the size of the secret(s). Secret sharing schemes are widely applied in tasks where the concurrence of at least threshold number of people is required like launching a missile, opening a bank vault, etc. In modern cryptography, secret sharing is well-studied as a primitive for *secure multiparty protocols* [9].

In [4], Shamir uses *single variable polynomials* for giving a secret sharing scheme whereas the works of [1, 5–7] use *bi-variable polynomials* for giving secret sharing schemes. In secret sharing, when *single variable polynomials* are used, a vandermonde matrix evolves during the reconstruction phase of the scheme, which through its non-singular property ensures that the polynomial is uniquely reconstructed. However, when *bi-variable* polynomials are used, the matrix that evolves in the reconstruction phase is not always a vandermonde matrix. In which case, its non-singular behavior cannot be easily verified and also the reconstruction of the polynomial need not be unique. If the polynomial is not uniquely reconstructed, then the secret cannot be retrieved. So, unique reconstruction of the polynomial in a polynomial-based secret sharing scheme is necessary. In this work, we give a technique by which a *multi-variable* polynomial can be converted to a *single variable* polynomial in such a way that, solving for the coefficients of the single variable polynomial is equivalent to that of solving for the multi-variable polynomial. Moreover, this transformation is optimal in certain cases. We use this technique to give a secret sharing scheme based on multi-variable polynomials. We use this technique to give *multi-variable multi-secret sharing schemes* and secret sharing schemes for *compartmented access structures* similar to the work of [7].

Organization of the paper. In section 2, we give some necessary definitions and outline some existing schemes [1, 3, 7]. In section 3, we give the lemma by which a *multi-variable* polynomial can be converted to a *single variable* polynomial. In section 4, we give new schemes for multi-variable secret sharing, multi-variable multi-secret sharing and a secret sharing scheme for *compartmented access structures*. In section 5, we compare our scheme with the existing schemes.

2 Preliminaries on secret sharing

We introduce notations used in this paper and give formal definitions for access structures, multi-secret sharing and compartmented access structures.

Definition 1 (Access Structure) Let $\mathbb{P} = \{p_1, p_2, \ldots, p_n\}$ be the set of players. A collection $\Gamma \subseteq 2^{\mathbb{P}}$ is referred to as *access structure*, when $\exists \mathcal{V} \in \Gamma$ such that players in $\mathcal{V}$ can reconstruct the secret and when $\exists \mathcal{V}' \notin \Gamma$ then players in $\mathcal{V}'$ cannot reconstruct the secret. An access structure is *monotone*, if $\mathcal{V} \in \Gamma$ and $\mathcal{V} \subseteq \mathcal{W}$ imply that $\mathcal{W} \in \Gamma$. Sets in Γ are authorized, and sets not in Γ are unauthorized.

Definition 2 (Multi-Secret Sharing Scheme) Let $\mathbb{S}=\{s_1, s_2, \ldots, s_m\}$ be a set of secrets chosen from a finite field $\mathbb{F}_q$, where q is a prime. The dealer shares the secrets from $\mathbb{S}$ among a finite set of players such that when k players give their shares, the secrets can be uniquely reconstructed, but less than k players cannot get any information about the secrets. In multi-secret sharing schemes, the player may get one or more shares. The ratio of number of the shares with each player and the number of secrets in $\mathbb{S}$ gives the *information rate* of the scheme. In the multi-secret sharing scheme given in [3], m secrets are shared among n players such that each player holds only one share.

Definition 3 (Compartmented Access Structure) We have taken the definition of compartmented access structure from [2, 7]. Given a situation where the player set $\mathbb{P}$ is divided into c compartments. If $k_i \in \mathbb{N}$ is the threshold for a compartment $\mathcal{C}_i$, $\forall\ 1 \leq i \leq c$ and $k \in \mathbb{N}$ is the threshold of the secret sharing scheme such that $k \geq \sum_{i=1}^{m} k_i$. Then the access structure Λ is defined as:

$$\Lambda = \{\mathcal{V} \subseteq \mathbb{P} : \exists \mathcal{W} \subseteq \mathcal{V} / |\mathcal{W} \cap \mathcal{C}_i| \geq k_i, 1 \leq i \leq c, and\ |\mathcal{W}| = k\}. \tag{1}$$

Such access structures are suitable for situations in which the size of an authorized subset must be at least some threshold k, but, in addition every compartment is represented by at least some number of participants in the authorized subset. In other situations, however, an opposite demand may occur: while the size of an authorized subset must be at least some threshold, we would like to limit the number of participants that represent each of the compartments, namely,

$$\Delta = \{\mathcal{V} \subseteq \mathcal{U} : \exists \mathcal{W} \subseteq \mathcal{V} / |\mathcal{W} \cap \mathcal{C}_i| \leq k_i, 1 \leq i \leq c, and\ |\mathcal{W}| = k\}. \tag{2}$$

where k_i,$k \in \mathbb{N}$ and $k \leq \sum_{i=1}^{m} k_i$.

We follow these notations throughout the paper. Next we give outline of some of the existing schemes in [1, 3, 7].

2.1 Swarming secrets [1]

Let $\mathbb{P}$ be the set of players. A swarm set SW is defined as $SW \subseteq \mathbb{P}$ and is characterized by the tuple $(m, k, s_1, s_2, \ldots, s_m)$, where $s_1, \ldots, s_m$ are the m secrets that are shared among the players in SW according to a $(k, |SW|)$-secret sharing scheme, where $|SW|$ is the size of the swarm.

Each swarm is initiated by a *sharing* phase in which the dealer distributes m secrets among swarm members. The dealer knows the swarm members, the secrets $s_1, \ldots, s_m$ and the privacy threshold k. Each secret s_j is shared by a bivariate polynomial $\mathcal{P}(x, y)$ of degree k in each variable over field $\mathbb{F}$. $\mathcal{P}(x, y)$ is a random polynomial with the sole restriction that $\mathcal{P}(0, 0) = s_j$.

Secret Sharing Scheme (a): Deal(SW,s,k)

The dealer chooses $\mathcal{P}(x, y)$, a random bivariate polynomial of degree t in each variable over field $\mathbb{F}$ such that $P(0, 0) = s$.
For all $u \in SW$ do

- The dealer picks distinct $a_1, \ldots, a_{k+1} \in \mathbb{F}$ and sends $\mathcal{P}_u(a_1), \ldots, \mathcal{P}_u(a_{k+1})$ and $\mathcal{P}^*_u(a_1), \ldots, \mathcal{P}^*_u(a_{k+1})$ to u.

A player u in the swarm SW can compute two k-degree single variable polynomials. These polynomials are $\mathcal{P}^*_u(y) = \mathcal{P}(u, y)$ and $\mathcal{P}_u(x) = \mathcal{P}(x, u)$. Each such polynomial is of degree k due to the definition of $\mathcal{P}(x, y)$ and u receives the value of each polynomial at $k + 1$ points during the deal algorithm. Hence, u can compute the polynomials using Lagrange interpolation. For m secrets, the same sequence of instructions are executed m times (independently for each execution).

2.2 Recursive multi secret sharing scheme [3]

In [3],the secret sharing scheme is designed to recursively hide several secrets in a single variable polynomial. Each player gets one share on this polynomial such that when threshold number of players come together, the secrets can be recovered.

Secret Sharing Scheme (b):

$\mathbb{S}$=$\{s_1,s_2,\ldots,s_m\}$ is the set of m secrets from $\mathbb{F}_q$, the base field of characteristic p. There are n players and the scheme has a threshold k such that $k \leq n$ and the characteristic of the field $p \geq n$, then a (k, n) *multi-secret sharing scheme* is given as:

1. The dealer chooses a linear polynomial $\rho_1(x)$ with constant term s_1. He constructs $\rho_1(.)$ by choosing the coefficient of x to be a (non-zero) random finite field element. Then he evaluates ρ_1 at two other points to obtain $(\sigma_1^{(1)}, \omega_1^{(1)})$ and $(\sigma_2^{(1)}, \omega_2^{(1)})$, where $\sigma_1^{(1)}, \omega_1^{(1)}, \sigma_2^{(1)}, \omega_2^{(1)} \in \mathbb{F}_q$.
2. For each of the j^{th} secret, where $j \in \{2, 3, \ldots, m\}$, the dealer constructs $\rho_j(x)$ as follows:
   - $\rho_j(0) = s_j$,
   - $\rho_j(\sigma_1^{(j)})$=$\omega_1^{(j-1)}$,...,$\rho_j(\sigma_j^{(j)})$=$\omega_j^{(j-1)}$

   He interpolates these points to construct the polynomial $\rho_j(x)$. After $m-1$ iterations, all the m secrets are hidden and $\rho_m(x)$ is a m degree polynomial.
3. The dealer chooses $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$ as the public identities of the n players, such that $\alpha_r \neq \sigma_l^m$, $1 \leq r \leq n$, $1 \leq l \leq m$. He evaluates $\rho_m(x)$ at $\alpha_1, \alpha_2, \ldots, \alpha_n$ to generate the private shares $S_1, S_2, \ldots, S_n$.

We also give a small example of the scheme. Suppose $s_1 = 137$, $s_2 = 99$, $s_3 = 75$ are three secrets to be shared over the finite field $\mathbb{F}_p$ where $p = 157$. According to the scheme mentioned in [3], the three secrets can be hidden in a polynomial of degree 3 as follows:

1. The dealer constructs a degree 1 polynomial $\rho_1(x)$ to hide the first secret. For that, he puts the constant term in the resulting polynomial be s_1, so we get the point (0,137). The dealer randomly chooses another point from F_p as (1,43). Interpolating these two points, he constructs the polynomial $\rho_1(x)$= $63x + 137$. He evaluates this polynomial at two other points say, (2,106), (3, 12).
2. He hides s_2 and builds a degree 2 polynomial $\rho_2(x)$ whose constant is s_2. One point on $\rho_2(x)$ is (0,99). He stores $\rho_1(2)$, $\rho_1(3)$ as $\rho_2(1)$ and $\rho_2(2)$ respectively. The other points on $\rho_2(x)$ are (1,106), (2,12). He interpolates the polynomial $\rho_2(x)$=$28x^2 + 136x + 99$. He evaluates $\rho_2(x)$ at three other points, say, (3,131), (4,149), (5,66).
3. Similar to step 2,he generates $\rho_3(x)$ for the third secret s_3 as $68x^3 + 91x^2 + 54x + 75$. He chooses n identities for the players and gives the players shares on $\rho_3(x)$.

2.3 Multipartite secret sharing using bivariate interpolation [7]

In [6] and [7], secret sharing schemes are proposed realizing compartmental access structures. Let $\mathbb{P}$ be the set of players divided into compartments. Let there be c compartments such that k_i is the threshold and u_{ij} is the j^{th} player of the compartment C_i. Given a reasonably large finite field $\mathbb{F}_q$ of characteristic p, the dealer chooses c distinct elements $x_1, x_2, \cdots, x_c$ from $\mathbb{F}_q$. He defines

$$L_i(x) = \prod_{1 \leq j \leq c, j \neq i} \frac{x - x_j}{x_i - x_j}.$$

He chooses $\mathcal{P}_i(y)$, a polynomial of degree $k_i - 1$. He defines,

$$\mathcal{P}(x, y) = \sum_{i=1}^{c} \mathcal{P}_i(y) L_i(x) = \sum_{i=1}^{c} \sum_{j=0}^{k_i - 1} a_{i,j} y^j L_i(x).$$

Then according to definition 3, when threshold $k \geq \sum_{i=1}^{c} k_i$, the scheme is given as follows:

Secret Sharing Scheme (c):

1. The secret is $s = \sum_{i=1}^{c} \sum_{j=0}^{k_i-1} a_{i,j}$.
2. Each player $u_{i,j}$ from compartment C_i will be given a unique point $(x_i, y_{i,j}), y_{i,j} \neq 1$ and his private share is the value of $\mathcal{P}(x, y)$ at that point.

It is proved in [7], that when k_i players from the i-th compartment come together, they can recover $\mathcal{P}_i(y)$. When threshold k players come together, $\mathcal{P}(x, y)$ can be reconstructed and secret s can be recovered.

When the secret is $S = a_{1,0} = a_{2,0} = \cdots = a_{c,0}$, then $\mathcal{P}_i(y)$ has the property that $\mathcal{P}_1(0) = \mathcal{P}_2(0) = \cdots = \mathcal{P}_c(0)$ and $k \leq \sum_{i=1}^{c} k_i$, the secret sharing scheme can be given as follows:

Secret Sharing Scheme (d):

1. The dealer gives each player $u_{i,j}$ from compartment C_i a unique point $(x_i, y_{i,j}), y_{i,j} \neq 1$ and his private share is the value of $\mathcal{P}(x, y)$ at that point.

The significance of outlining these schemes is that; we improve some of the schemes found in [1, 3] and also give a scheme similar to that of [7].

3 Background

In this section, we state and prove some results that we require in our schemes. The following lemma is the most important result of the paper. We give an example for better understanding of this lemma. The corollary followed by the lemma is trivial from the lemma.

Lemma 1. *Let $F(x_1, \cdots, x_n)$ be a polynomial in n variables $x_1, \cdots, x_n$ over a finite field $\mathbb{F}_q$ of characteristic p, where p is reasonably large. Without loss of generality, let the highest degree monomial of F is $x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n}$ with the property that the highest degree of x_i in F is t_i for all $i = 1, \cdots, n$. Then it is possible to get a single variable polynomial f of degree $(t_1+1)(t_2+1)\cdots(t_n+1)-1$ such that solving the co-efficient of f is equivalent to solve the co-efficients of F with the added property that there is an one one correspondence between the co-efficients of F and f.*

Proof. Consider the following quotient rings: $F_{n-1} = \mathbb{F}_q[x_1, \cdots, x_n]/ < x_n - x_{n-1}^{t_{n-1}+1} >$, $F_{n-2} = F_{n-1}/ < x_{n-1} - x_{n-2}^{t_{n-2}+1} >, \cdots$, $F_1 = F_2/ < x_2 - x_1^{t_1+1} >$. Let $f(x_1)$ be a polynomial in $\mathbb{F}_q[x_1]$ such that $\overline{f(x_1)} = \overline{F(x_1, x_2, \cdots, x_n)}$ in F_1. If possible, let $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$ be two monomials of F such that $\overline{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}} = \overline{x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}}$ in F_1. Without loss of generality, let $i_1 \leq j_1$. Then, $i_1 + (t_1+1)i_2 + (t_1+1)(t_2+1)i_3 + \cdots + (t_1+1)(t_2+1)\cdots(t_{n-1}+1)i_n = j_1 + (t_1+1)j_2 + (t_1+1)(t_2+1)j_3 + \cdots + (t_1+1)(t_2+1)\cdots(t_{n-1}+1)j_n$ implies $(i_1 - j_1) = (t_1+1)(j_2 + (t_2+1)j_3 + \cdots + (t_2+1)\cdots(t_{n-1}+1)j_n - (i_2 + (t_2+1)i_3 + \cdots + (t_2+1)\cdots(t_{n-1}+1)i_n))$. So, $(t_1+1)|(i_1 - j_1)$. Hence, $i_1 = j_1$. In a similar fashion, one can easily obtain that $i_2 = j_2, \cdots, i_n = j_n$. Hence, a contradiction to the assumption that distinct monomials have same degree.

With some elementary calculations, it is easy to check that the degree of f is $(t_1+1)(t_2+1)\cdots(t_n+1)-1$. Let $A = \{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} | 0 \leq i_j \leq t_j - 1, 1 \leq j \leq n\} \subseteq \mathbb{F}_q[x_1, \cdots, x_n]$ and $B = \{x_1^k | 0 \leq k < (t_1+1)(t_2+1)\cdots(t_n+1)\} \subseteq F_1$. Clearly, $|A| = |B| = (t_1+1)(t_2+1)\cdots(t_n+1)$. Consider a mapping $g : A \to B$ as follows: $g(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}) = x_1^{i_1 + (t_1+1)i_2 + (t_1+1)(t_2+1)i_3 + \cdots + (t_1+1)(t_2+1)\cdots(t_{n-1}+1)i_n}$.
One can easily calculate that $0 \leq i_1 + (t_1+1)i_2 + (t_1+1)(t_2+1)i_3 + \cdots + (t_1+1)(t_2+1)\cdots(t_{n-1}+1)i_n \leq (t_1+1)(t_2+1)\cdots(t_n+1)-1$. Hence g is well defined. From the first part, one can say that g is injective. Since $|A| = |B|$ and it is finite, therefore, g is surjective.

Hence, solving F is equivalent to solving f. □

The following corollary is trivial from the above lemma.

Corollary 1. *Let $F(x_1, \cdots, x_n)$ be a polynomial in n variables $x_1, \cdots, x_n$ over a finite field $\mathbb{F}_q$ of characteristic p, where p is reasonably large. Let the highest degree of x_i in F be t_i for all $i = 1, \cdots, n$. Then it is possible to get a single variable polynomial f of degree less than or equal to $(t_1+1)(t_2+1)\cdots(t_n+1)-1$ such that solving the co-efficient of f is equivalent to solving the co-efficients of F.*

As we have mentioned before, we give the following example for readers better understanding.

Example 1. Let $F(x,y,z) = \sum_{i=0}^{1}\sum_{j=0}^{2}\sum_{k=0}^{3} c_{i,j,k}x^iy^jz^k$. Now let $f(x)$ be the polynomial obtained from F by putting $z = y^3, y = x^2$. Then $f(x) = c_{1,2,3}x^{23} + c_{0,2,3}x^{22} + c_{1,1,3}x^{21} + c_{0,1,3}x^{20} + c_{1,0,3}x^{19} + c_{0,0,3}x^{18} + c_{1,2,2}x^{17} + +c_{0,2,2}x^{16} + c_{1,1,2}x^{15} + c_{0,1,2}x^{14} + c_{1,0,2}x^{13} + c_{0,0,2}x^{12} + c_{1,2,1}x^{11} + c_{0,2,1}x^{10} + c_{1,1,1}x^9 + c_{0,1,1}x^8 + c_{1,0,1}x^7 + c_{0,0,1}x^6 + c_{1,2,0}x^5 + c_{0,2,0}x^4 + c_{1,1,0}x^3 + c_{0,1,0}x^2 + c_{1,0,0}x + c_{0,0,0}$. Hence by interpolating f, one can completely solve F.

4 Our schemes

4.1 Multi-variable Secret Sharing Scheme

Let $\mathcal{P}(x_1, \cdots, x_l)$ be a polynomial in $l(\geq 1)$ variables $x_1, \cdots, x_l$ over a finite field $\mathbb{F}_q$ of characteristic p, where p is large. Let the highest degree monomial of $\mathcal{P}$ be $x_1^{t_1}x_2^{t_2}\cdots x_l^{t_l}$ with the property that the highest degree of x_i in $\mathcal{P}$ is t_i for all $i = 1, \cdots, l$ and value of $\mathcal{P}$ at $x_1{=}x_2{=}\ldots{=}x_l{=}0$ is the secret s to be shared. When there are n players and threshold $k = (t_1+1)\cdots(t_l+1)$ such that $k \leq n$ and the characteristic of the field $p \geq n$, then a (k,n) *perfect secret sharing scheme* is given as:

Secret Sharing Scheme 1

- The dealer randomly chooses n distinct elements $\alpha_1, \cdots, \alpha_n$ from $\mathbb{F}_q$ and computes $\mathcal{S}_i{=}\mathcal{P}(\alpha_i, \alpha_i^{(t_1+1)}, \cdots, \alpha_i^{(t_1+1)(t_2+1)\cdots(t_{l-1}+1)})$ and gives $(\alpha_i,\mathcal{S}_i)$ as private share to the i-th player and publishes $t_1, t_2, \cdots, t_l$.

Lemma 2. *When $k = (t_1+1)\cdots(t_l+1)$ distinct players come together and give their private shares correctly, then secret s can be uniquely constructed. And the scheme is perfect.*

Proof. Let k players come together to reveal the secret from $\mathcal{P}(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$. Let the i-th player have $(\alpha_{1,i}, \alpha_{2,i}, \cdots, \alpha_{n,i})$ and $\mathcal{P}(\alpha_{1,i}, \alpha_{2,i}, \cdots, \alpha_{n,i})$ as his private share. According to the lemma 1, $\alpha_{j,i}$'s should satisfy the following conditions:

$$\alpha_{j,i} = \alpha_{j-1,i}^{t_{j-1}+1} \text{ for all } 2 \leq j \leq n, 1 \leq i \leq k$$

To reconstruct the secret i.e. the polynomial, it is sufficient to compute the co-efficients of the single variable polynomial of degree $k-1$ according to lemma 1 and hence, when k players come together and compute the co-efficients of $\mathcal{P}$ and reconstruct the secret as $\mathcal{P}(0, \cdots, 0)$.

When less than k players come, they cannot unconditionally reconstruct the secret as the number of co-efficients in F and f are k. Thus, this is a *perfect* scheme. □

Corollary 2. *This scheme can be a (t,n) secret sharing scheme for any $t|(t_1+1)(t_2+1)\cdots(t_l+1)$, by giving $\frac{(t_1+1)(t_2+1)\cdots(t_l+1)}{t}$ private shares to each player.*

4.2 Secret Sharing for Compartmented Access Structures

When the player set $\mathbb{P}$ is divided into c compartments, such that k_i is the threshold of the compartment C_i, $\forall\ 1 \leq i \leq c$. We give a secret sharing scheme, which satisfies the compartmented access structure Λ given in definition 3.

Let $\mathcal{P}(x_1, x_2)$ be a bi-variable polynomial over a finite field $\mathbb{F}_q$ of characteristic p with the property that the highest degree of x_2 in $\mathcal{P}$ is $c-1$. Let $\mathcal{P}(x_1, x_2) = \sum a_{i_1,i_2}x_1^{i_1}x_2^{i_2}$. Randomly choose $b_{0,0}, b_{0,1}, \cdots, b_{0,c-1}$ from $\mathbb{F}_q$. $\mathcal{P}$ can be re-written as:

$$\mathcal{P}(x_1,x_2) = \mathcal{P}_0(x_1)+\mathcal{P}_1(x_1)x_2+\mathcal{P}_2(x_1)x_2^2+\cdots+\mathcal{P}_{c-1}(x_1)x_2^{c-1}+[(a_{0,0}-b_{0,0})+(a_{0,1}-b_{0,1})x_2+\cdots+(a_{0,c-1}-b_{0,c-1})x_2^{c-1}]$$

where $\mathcal{P}_i(x_1) = b_{0,i} + a_{1,i}x_1 + a_{2,i}x_1^2 + \cdots + a_{k_i-1,i}x_1^{k_i-1}$, for all $i = 0, 1, \cdots, c-1$ and $\mathcal{P}_c(x_2) = (a_{0,0} - b_{0,0}) + (a_{0,1} - b_{0,1})x_2 + \cdots + (a_{0,c-1} - b_{0,c-1})x_2^{c-1}$. Here k_i is the threshold of the compartment C_i and the threshold of the scheme by definition 3 is $k \geq \sum_0^{c-1} k_i$. And also, $\mathcal{P}$ is chosen in such a way that $k_0 \leq k_1 \leq k_2 \leq \cdots \leq k_{c-1}$.

Secret Sharing Scheme 2:

1. Let the secret be $s = a_{0,0} + a_{0,1} + \cdots + a_{0,c-1}$.
2. The dealer gives each player $u_{i,j}$ from compartment C_i $(0 \leq i \leq c-1)$ a unique point $y_{i,j}, y_{i,j} \neq 0$ and his private share is $\mathcal{P}_i(y_{i,j})$.
3. The dealer chooses c distinct points from $\mathbb{F}_q^2$ and publishes the values of $\mathcal{P}$ at these points.

Lemma 3. *When k players come together, such that at least k_i players from compartment C_i take part in the reconstruction, the secret s can be uniquely reconstructed. And the scheme is perfect.*

Proof. In the above scheme, when k_i people from the i-th compartment come together, then they can reconstruct $\mathcal{P}_i(x_1)$. Using i, $\mathcal{P}_i$ (for all $0 \leq i \leq c-1$) and the c public values, $\mathcal{P}$ can be reconstructed and the secret s can be obtained. Since the number of unknowns in $\mathcal{P}$ is $k_0 + k_1 + k_2 + \cdots + k_{c-1} + c$, when less than k number of players come together, they will not be able to reconstruct the secret. Hence the scheme is perfect. □

It can be easily verified that this scheme can also be used for nested compartments, that is compartments of compartments using three variables.

4.3 Operators $\mathbb{I}$ & $\mathbb{D}$

Formal derivatives and integration

Let $\mathbb{F}_q$ be a finite field with characteristic p. Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ (where $n < p$). Then the formal derivative denoted by $f'(x)$ and is defined by $f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. The reverse process is known as the formal integration. We refer to formal derivative by operator $\mathbb{D}$ and formal integration by $\mathbb{I}$.

4.4 Multi-variable Multi-Secret Sharing Schemes

In multi-secret sharing schemes, the dealer shares more than one secret among the set of players $\mathbb{P}$. Let $\{s_1, s_2, \ldots, s_m\}$ be m secrets chosen from a finite field $\mathbb{F}_q$, where q is a prime. The dealer shares these m secrets among n players, such that $k(\leq n)$ players can get together and reconstruct the secrets. In [3], a $(m+1, n)$ multi-secret sharing scheme with m secrets is given. The scheme of [3] is outlined in the preliminaries section.

One limitation of scheme (b) is that, for a given set of m secrets, the threshold is fixed as $m+1$. However, when the desired threshold(k) for the secret sharing scheme is greater or less than the number of secrets to be hidden (m), this scheme can not be used. In this section, we use lemma 1 and scheme (b) to give (k, n) secret sharing schemes, where the threshold k is not fixed by m. In brief, for a given set of m secrets from $\mathbb{F}_q$:

1. We give multi-secret sharing schemes where threshold k can take some values from the range $[2m, (m/2+1)^2]$ $\cup \{m+1\}$, when $m \geq 1$.
2. When operators $\mathbb{I}, \mathbb{D}$ are used, we give multi-secret sharing schemes where threshold $k \leq n$ can take any value from the range $[2, \infty)$ for any $k \leq n$.

Lemma 4. *Given secret sharing scheme(b) from section 2, when threshold $k = m+1$ distinct players come together and give their private shares correctly, the m secrets $\{s_1, s_2, \ldots, s_m\}$ can be uniquely reconstructed. And the scheme is perfect.*

Proof. When $m+1$ distinct players give their shares correctly, using interpolation techniques (α_k, S_{α_k}), $1 \leq k \leq m+1$, the dealer constructs $\rho_m(x)$ and retrieves the m^{th} secret, $s_m = \rho_m(0)$. For reconstructing the other j secrets, where $m-1 \leq j \leq 1$,

- $\omega_1^{(j)} = \rho_{j+1}(\sigma_1^{(j+1)}), \ldots, \omega_{j+1}^{(j)} = \rho_{j+1}(\sigma_{j+1}^{(j+1)})$,
- He interpolates $(\sigma_1^{(j)}, \omega_1^{(j)}), \ldots, (\sigma_j^{(j)}, \omega_j^{(j)})$ to get $\rho_j(x)$, $s_j = \rho_j(0)$.

Hence, all the m secrets can be uniquely reconstructed. When less than k number of players come together, they can not unconditionally reconstruct the polynomial $\rho_m(x)$ uniquely and hence the secrets can not be recovered. Hence, the scheme is *perfect*. □

Secret Sharing Scheme 3

Let $f(x_1, x_2, \ldots, x_l) \in \mathbb{F}_q[x_1, x_2, \ldots, x_l]$ be a polynomial such that the highest degree of x_i in f is $k_i - 1$. Without loss of generality, let $k_1 \leq k_2 \leq \cdots \leq k_l$. Also let $x_1^{k_1-1} x_2^{k_2-1} \ldots x_l^{k_l-1}$ be a monomial in f. Then f can be written as

$$f(x_1, x_2, \ldots, x_l) = \sum_{j=2}^{l} \sum_{i_j=0}^{k_j-1} f_{i_2,\ldots,i_l}(x_1) x_2^{i_2} x_3^{i_3} \ldots x_l^{i_l}$$

where each $f_{i_2,\ldots,i_l}(x_1)$ is a polynomial of degree atmost $k_1 - 1$.

When the dealer uses $f(x_1, x_2, \ldots, x_l)$, he can hide a total of $k = \Pi_{i=1}^{l} k_i - k_1$ secrets by using scheme (b) and hiding $k_1 - 1$ secrets in each of $f_{i_2,\ldots,i_l}(x_1)$ where $0 \leq i_j \leq k_j - 1$ and $0 \leq j \leq l$. However, when the dealer has m secrets and he wants to design a (k, n) secret sharing scheme with threshold k and n players.

- When $m \leq (\Pi_{i=1}^{l} k_i) - k_1$: Using scheme (b), the dealer hides each of the $k_1 - 1$ secrets in first $\lfloor (\frac{m}{k_1-1}) \rfloor$ of $f_{i_2,\ldots,i_l}(x_1)$ where $0 \leq i_j \leq k_j - 1$ and $2 \leq j \leq l$. He hides the remaining secrets and some random values in the next $f_*(x_1)$. And he fills the remaning $f_*(x_1)$s with random values for the coefficients. By following lexicographic ordering on variables $x_2, x_3, \ldots, x_l$, this step is made deterministic.

- When $m \geq (\Pi_{i=1}^{l} k_i) - k_1$: The dealer divides the m secrets into $d = \Pi_{i=2}^{l} k_i$ groups of size $t_1, t_2, \ldots, t_d$. He applies the scheme (b) on each of these groups and constructs i polynomials of degree of degree t_i, where $0 \leq i \leq d$. Applying operator $\mathbb{D}$ on each of these d polynomials, he reduces their degree to $k_1 - 1$. The coefficients that are lost while applying operator $\mathbb{D}$ are stored as public information. Once this is done, he uses the resulting polynomials as $f_{i_2,\ldots,i_l}(x_1)$ where $0 \leq i_j \leq t_j - 1$ and $2 \leq j \leq l$ and constructs $f(x_1, x_2, \ldots, x_l)$.

- The dealer chooses n identities for the players and using scheme 1 and polynomial $f(x_1, x_2, \ldots, x_l)$, he gets the private shares for the players. The dealer publishes the values of $k_1, k_2, \ldots, k_l$ and $t_1, t_2, \ldots, t_d$.

Lemma 5. *When k players come together, give their private shares and use the public information correctly, then the secrets can be uniquely recovered. And the scheme is perfect.*

Corollary 3. *For any value of k and for any given set of m secrets, it is clearly evident that this scheme can be a (k, n) multi-secret sharing scheme.*

Secret Sharing Scheme 4

Let $\mathbb{S}$=$\{s_1, s_2, \ldots, s_m\}$ be m secrets from $\mathbb{F}_q$, the base field of characteristic p. Let the number of players be n and the threshold k, such that $k \leq n$ and the characteristic of the field $p \geq n$, then a (k, n) *multi-secret sharing scheme* is given as:

1. The dealer groups $\mathbb{S}$ as $\mathbb{S}_1 \cup \mathbb{S}_2$, such that $\mathbb{S}_1$=$\{s_1\}$ and $\mathbb{S}_2$=$\{s_2, \ldots, s_m\}$.
2. For the set of secrets in $\mathbb{S}_1$, the dealer uses scheme (b) of section 2 and constructs a polynomial $\rho_1(x)$. For the set of secrets in $\mathbb{S}_2$, he uses scheme (b) to construct $\rho'_{m-1}(y)$. He multiplies these two polynomials and gets $\rho_m(x, y)$=$\rho_1(x)$*$\rho'_{m-1}(y)$.
3. The dealer chooses $\alpha_1, \alpha_2, \ldots, \alpha_n$ as the public identities of the n players similar to step 3 in scheme (b). Using scheme 1, he evaluates $\rho_m(x, y)$ at $\alpha_1, \alpha_2, \ldots, \alpha_n$ to generate the private shares $S_1, S_2, \ldots, S_n$ of the n players.

Lemma 6. *When $k = 2m$ distinct players come together and give their private shares correctly, the m secrets $\{s_1, s_2, \ldots, s_m\}$ can be uniquely reconstructed.*

Proof. When $2m$ distinct players give their shares correctly, using interpolation on (α_k, S_{α_k}), $1 \leq k \leq 2m$, the dealer constructs $\rho_m(x, y)$. The uniqueness of interpolation follows from lemma 1. $\rho_m(x, y)$ can be split into $\rho_1(x)$ and $\rho'_{m-1}(y)$. Using lemma 4, the secrets can be uniquely reconstructed from $\rho_1(x)$, $\rho'_{m-1}(y)$. Hence all the m secrets can be uniquely recovered. □

Corollary 4. *This scheme is a (k, n) multi-secret sharing scheme for sharing m secrets with $k = (m/2 + 1)^2$, when $\mathbb{S}$ as $\mathbb{S}_1 \cup \mathbb{S}_2$ and $\mathbb{S}_1$=$\{s_1, \ldots, s_{m/2}\}$ and $\mathbb{S}_2$=$\{s_{m/2}, \ldots, s_m\}$.*

Corollary 5. *This scheme is a (k, n) multi-secret sharing scheme for sharing m secrets where k can take some values from the range $[2m, (m/2 + 1)^2] \cup m + 1$.*

4.5 Other Multi-variable Multi-Secret Sharing Schemes

Secret Sharing Scheme 5

Let $\mathbb{S}$=$\{s_1, s_2, \ldots, s_m\}$ be m secrets from $\mathbb{F}_q$, the base field of characteristic p. When operators $\mathbb{I}$ and $\mathbb{D}$ are used, then (k, n) *multi-secret sharing schemes*, with n players and threshold k such that $k \leq n$ and k taking any value in $[2, \infty)$ are given as:

Step 1.

1. When the desired threshold k is a prime: Using scheme (b), the dealer constructs a m-degree polynomial $\rho_m(x)$ hiding the m secrets.
   - When $k > m$, the dealer applies operator $\mathbb{I}$ on $\rho_m(x)$ for $k - m - 1$ times and increases the degree of $\rho_m(x)$ to $k - 1$. Each time operator $\mathbb{I}$ is applied on $\rho_m(x)$, the constant is replaced by a random value from $\mathbb{F}_q$ to get a polynomial $\mathcal{P}(x)$ with k unknowns.
   - When $k < m$, the dealer applies the operator $\mathbb{D}$ on $\rho_m(x)$ for $m - k - 1$ times and decreases the degree of $\rho_m(x)$ to $k - 1$. Each time operator $\mathbb{D}$ is applied on $\rho_m^i(x)$ where $\rho_m^1(x) = \rho_m(x)$, the constant $\rho_m^i(x)$ is preserved as public information $\rho_m^i(a)$, evaluating $\rho_m^i(.)$ at a random value a, for $1 \leq i \leq m - k - 1$. Let $\mathcal{P}(x)$ be the resulting polynomial with k unknowns.

2. When the desired threshold k is composite:
   (a) If k is even and $k = 2 * t$: The dealer divides m secrets into two groups and using scheme 4 constructs two polynomials $\rho_1(x)$ and $\rho_{m-1}^{'}(y)$.
   - When $t < (m - 1)$, he applies operator $\mathbb{D}$ on $\rho_{m-1}^{'}(y)$ for $m - t$ times. He preserves the additional information of $\rho_{m-1}^{'}(y)$ as public information similar to case 1. Then, he multiplies these two polynomials to get the polynomial $\mathcal{P}(x, y)$.
   - When $t > (m - 1)$, he applies operator $\mathbb{I}$ on $\rho_{m-1}^{'}(y)$ for $t - m$ times. He multiplies these two polynomials to get the polynomial $\mathcal{P}(x, y)$.

   (b) If k is odd and can be written as $p_1^{a_1}.p_2^{a_2} \ldots p_l^{a_l}$.
   - When $l < m$, then in the setting of scheme 4, the dealer groups $\mathbb{S}$ as $\mathbb{S}_1 \cup \mathbb{S}_2 \cup \ldots \mathbb{S}_l$, such that $\mathbb{S}_i$=$\{s_i\}$,$\forall\ 1 \leq i \leq l - 1$ and $\mathbb{S}_l$=$\{s_l, s_{l+1}, \ldots, s_m\}$. He constructs l polynomials $\rho_1(x_1), \ldots, \rho_l(x_l)$. He applies operator $\mathbb{I}$ and raises the degree of $\rho_i(.)$ to the power $p_i^{a_i} - 2$, for all $i \in \{1, 2, \ldots, l - 1\}$ and $\rho_l(.)$ to the power $p_l^{a_l} - m + l$. Multiplying the resulting polynomials, he gets the polynomial $\mathcal{P}(.)$.
   - When $l > m$, then in the setting of scheme 4, the dealer groups $\mathbb{S}$ as $\mathbb{S}_1 \cup \mathbb{S}_2 \cup \ldots \mathbb{S}_m$, such that $\mathbb{S}_i$=$\{s_i\}$,$\forall\ 1 \leq i \leq m$. He constructs m polynomials $\rho_1(x_1), \ldots, \rho_m(x_m)$. He applies operator $\mathbb{I}$ and raises the degree of $\rho_i(.)$ to the power $p_i^{a_i} - 2$, for all $i \in \{1, 2, \ldots, m - 1\}$ and $\rho_m(.)$ to the power $p_m^{a_m} \ldots p_l^{a_l} - 2$. He multiplies all these polynomials to get the polynomial $\mathcal{P}(.)$.

Step 2.
The dealer picks the final polynomial $\mathcal{P}(.)$ and n identities of the players and uses scheme 1 to get the (k, n) multi-secret sharing scheme for the desired threshold k.

Lemma 7. *When m is known, if k number of players come together and give their private shares correctly, then all the secrets can be uniquely recovered.*

Proof. When k players come together, then the polynomial $\mathcal{P}$ can be reconstructed. When m and step 1 of the scheme is known to the players, using the respective technique, $\rho_m(.)$ can be reconstructed. Using schemes (b) and 3, the m secrets can be recovered. □

Note. It is only to ensure that the retrieval of secrets be done in a deterministic way, the scheme expects that each of the first $(l-1)$ groups (in the odd case) have a single secret while constructing the polynomial using scheme (b). On contrary, different groups can have different number of secrets and the secret retrieval phase can be altered accordingly.

We give a small example to explain the working of this secret sharing scheme.

Example.

It is explained in section 2 how a polynomial can be used to hide three secrets and using the resulting polynomial, a $(4, n)$ secret sharing scheme can be given, where the number of players is n and the threshold $k = 4$. In this example, we explain how step 1 can actually be used in obtaining the polynomial $\mathcal{P}(.)$. We show for $k = 1, 2, \ldots, 9$ and this k can be any other value from $\mathbb{N}$. This example is an extension of example 2.2 where the number of secrets $m = 3$.

(k,n) Scheme k-Threshold	Secrets $\mathbb{S}$	Polynomial by scheme (b)	Operations on Polynomials	Public Information	Shares on Polynomial
(2,n)	$\{s_1,s_2,s_3\}$	g(x) degree: 3	$g_1(x) = \mathbb{D}(g(x))$ $g_2(x) = \mathbb{D}(g_1(x))$	(r,g(r)) $(r_1, g_1(r_1))$	$g_2(x)$
(3,n)	$\{s_1,s_2,s_3\}$	g(x) degree: 3	$g_1(x) = \mathbb{D}(g(x))$	(r,g(r))	$g_1(x)$
(4,n)	$\{s_1,s_2,s_3\}$	g(x) degree: 3			$g(x)$
(5,n)	$\{s_1,s_2,s_3\}$	g(x) degree: 3	$g_1(x) = \mathbb{I}(g(x))$		$g_1(x)$
(6,n)	$\{\{s_1\},\{s_2,s_3\}\}$	g(x),h(y) degree(g): 1 degree(h): 2			$g(x) * h(y)$
(7,n)	$\{s_1,s_2,s_3\}$	g(x) degree: 3	$g_1(x) = \mathbb{I}^3(g(x))$		$g_1(x)$
(8,n)	$\{\{s_1\},\{s_2,s_3\}\}$	g(x),h(y) degree(g): 1 degree(h): 2	$h_1(y) = \mathbb{I}(h(y))$		$g(x) * h_1(y)$
(8,n)	$\{\{s_1\},\{s_2\},\{s_3\}\}$	g(x),h(y),i(z) degree(g): 1 degree(h): 1 degree(i): 1			$g(x) * h(y) * i(z)$
(9,n)	$\{\{s_1\},\{s_2,s_3\}\}$	g(x),h(y) degree(g): 1 degree(h): 2	$g_1(x) = \mathbb{I}(g(x))$		$g_1(x) * h(y)$

Table 1. Example for Scheme 5

5 Comparison of our scheme with other schemes

In this section, we explain how the schemes given in this paper are better than some existing schemes [1] and how they are similar to some existing schemes [7].

5.1 Comparison with [1]

The secret sharing scheme of [1] is outlined in subsection 2.1. The scheme uses $P(x, y)$, a bi-variate polynomial of degree t in each variable whose constant term is the secret. A $(t + 1, n)$ secret sharing scheme where each player has $2(t + 1)$ values is introduced. When $(t + 1)$ players come together, the total information available for reconstructing the secret is $2(t+1)^2$. However, the total number of co-efficients in P is only $(t+1)^2$. It is evident

that the scheme can be improved. When corollary 2 of scheme 1 is used, $(t+1)$ players can come together and each player has only $(t+1)$ values, the secret can be reconstructed. Moreover, our algorithm is not heuristic and we prove clearly that the secret can be determined uniquely.

5.2 Comparison with [7] and Scheme 2

The secret sharing scheme of [7] is outlined in subsection 2.3. We compare the scheme (c), scheme 1 and scheme 2. Both schemes (c) and 2 are quite similar and try to give secret sharing schemes for compartmented access structures. In scheme (c), when t_i players from the i-th compartment come together, they can reconstruct $\mathcal{P}_i(y)$. While in scheme 2, when the required number of people from the ith compartment come together, they can reconstruct the polynomial $\mathcal{P}_i(x_1)$. When the threshold number of people come together, they can reconstruct all the monomials of $\mathcal{P}$ except the co-efficients of $\mathcal{P}_c(x_2)$, which they can reconstruct by using the public information. Though the secret is not the same in scheme (b) and scheme 2, they can be made the same by choosing appropriate values of $b_{0,0}, b_{0,1}, \cdots, b_{0,c-1}$. Moreover, in both cases, the information stored at the participants is the same and also, less than threshold number of participants cannot reconstruct the secret. It can be easily verified that scheme 2 along with scheme 1 works equally well as scheme (c) only when there is same threshold on all compartments.

6 Conclusion

In this paper we introduced a technique that reduces a multi-variable polynomial to a single variable polynomial such that evaluation of the multi-variable polynomial is made easier. However, this single variable polynomial is optimal in certain cases only. Based on this lemma, we gave a new optimal multi-variable secret sharing scheme. We improve existing scheme [3] and show that this scheme along with operators $\mathbb{I}, \mathbb{D}$ can be transformed into a secret sharing scheme with any desired threshold. We propose a secret sharing scheme to realize a compartmental access structure scheme similar to [7]. We also show that our scheme 1 performs better than the scheme in [1]. And finally prove that multi-variable secret sharing schemes are just a generalization of Shamir secret sharing scheme [4] based on single variable polynomial.

References

1. Shlomi Dolev, Juan Garay and Niv Gilboa and Vladimir Kolesnikov; Swarming secrets. Allerton'09: Proceedings of the 47th annual Allerton conference on Communication, control, and computing, IEEE Press, pp. 1438-1445, 2009.
2. E.F. Brickell; Some ideal secret sharing schemes. Journal of Combinatorial Mathematics and Combinatorial Computing, vol 9, pp.105-113, 1989.
3. Abhishek Parakh,Subhash Kak; Recursive secret sharing for distributed storage and information hiding. IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems (ANTS), pp.1-3, 2009.
4. Adi Shamir; How to share a secret. Communications of ACM, Vol. 22, pp. 612-613, 1979.
5. Douglas R. Stinson; An Explication of Secret Sharing Schemes. Designs, Codes and Cryptography, Vol. 2, pp. 357-390, 1992.
6. Tamir Tassa and Nira Dyn; Multipartite Secret Sharing by Bivariate Interpolation. Proceedings of ICALP, pp.288-299 , 2006.
7. Tamir Tassa and Nira Dyn; Multipartite Secret Sharing by Bivariate Interpolation. Journal of Cryptology, 22, pp. 227-258, 2009.
8. G.R.Blakley; Safeguarding cryptographic keys. AFIPS Conference proceedings, AFIPS Press, pp. 313317, 1979.
9. O.Goldreich, S.Micali and A.Wigderson; How to play any mental game. Proceedings of the nineteenth annual ACM symposium on Theory of computing, STOC, pp. 218-229, 1987.
10. Marco Carpentieri; A perfect threshold secret sharing scheme to identify cheaters. Designs, Codes and Cryptography, pp. 183-187, 1995.