JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA) VOL. 2 NO. 2 (NOV 2019)
Available online at www.jfma.math.fsm.undip.ac.id

A SECRET SHARING SCHEME BASED ON MULTIVARIATE POLYNOMIALS

Ari Dwi Hartanto[1,*], Sutjijana[2]

[1,2]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Gadjah Mada*
Email: [1]ari@ugm.ac.id, [2]sutjijana@ugm.ac.id

Abstract. A Secret sharing scheme is a method for dividing a secret into several partial information. The secret can be reconstructed if a certain number of partial information is collected. One of the known secret sharing schemes is the Shamir's secret sharing scheme. It uses Lagrange interpolation (with one indeterminate) for reconstructing the secret. In this paper, we present a secret sharing scheme using multivariate polynomials with the secret reconstruction process using the multivariate interpolation formula derived by Saniee (2007). The resulted scheme can be considered as a generalization of the Shamir's secret sharing scheme.

Keywords: multivariate polynomial interpolation, secret sharing

I. INTRODUCTION

A secret sharing scheme is usually applied on a system to protect a secret from an individual or a group of people with less than a certain minimum number of members. For an illustration, suppose a company employs five senior financial staff. Each staff is not allowed to open the company's vault alone because of the regulation of the company. The vault is only allowed to be opened if at least two financial staffs simultaneous open the box. This rule anticipates the misuse of the access right of the vault key by each individual. Therefore, the company needs a system for the vault to accommodate the company regulation.

In 1979 Shamir introduced a secret sharing scheme called Shamir threshold scheme [2]. The scheme divides a secret that is put on the constant term of a polynomial of one indeterminate, and the partial information is taken in the form of points of the polynomial. Based on the theory of Lagrange interpolation, if we have $n + 1$ points of a polynomial of degree n then we can interpolate a unique polynomial of degree n that passes the points. This becomes the foundation of the Shamir threshold scheme (see [3]).

Tassa and Dyn [4] introduced bivariate Lagrange interpolation and stated its potential for designing a secret sharing scheme. They focused on how to design a multipartite access structure using bivariate interpolation. On the other hand, Saniee [1] derived a simple formula for multivariate Lagrange interpolation. In this paper, we intend to use the multivariate Lagrange interpolation formula for the secret sharing scheme.

The remainder of this paper is organized as follows. We start our presentation in Section 2 with Shamir's secret sharing scheme for providing a brief knowledge of the scheme. In Section 3, we give a brief explanation of the multivariate polynomial interpolation introduced by Saniee (2007). Furthermore, Section 4 contains the main discussion of this paper. Finally, we draw some concluding remarks in Section 5.

II. A SECRET SHARING SCHEME

Let ρ and r be two positive integers with $\rho \leq r$. A (ρ, r)-threshold scheme is a method to divide a secret K into r partial information and to distribute it to r participants such that every group of ρ participants can reconstruct the value of K but not for every group of participants with less than $\rho - 1$ members. The set of all participants that have the partial information of K denoted by $\mathcal{P} = \{P_1, P_2, \cdots, P_r\}$.

The value of K is chosen by a person called dealer, denoted by D, and we assume that $D \notin \mathcal{P}$. The value of K is only known by D and a system given authority by D for reconstructing K when ρ partial information is inputted on. The partial information of K provided by the dealer to each participant is called share. Shares are secretly distributed by the dealer such that each participant only knows his share and not know other shares.

One of the known (ρ, r)-threshold schemes is Shamir (ρ, r)-threshold scheme, or called Shamir Secret Sharing Scheme. The Shamir (ρ, r)-threshold scheme can be explained as follows.

(i). D chooses r distinct elements in the field $\mathbb{Z}_p$, i.e. $x_1, \cdots, x_r$. For all $i = 1, \cdots, r$, D distributes x_i to P_i.

(ii). Suppose D wants to divide a secret $K \in \mathbb{Z}_p$ into r shares. D choose secretly choose $\rho - 1$ elements in $\mathbb{Z}_p$, i.e. $a_1, \cdots, a_{\rho-1}$.

(iii). For all $i = 1, \cdots, r$, D calculates $y_i = a(x_i)$, with $a(x) = K + \sum_{j=1}^{\rho-1} a_j x^j \mod p$.

(iv). For all $i = 1, \cdots, r$, D distributes share y_i to P_i secretly.

It is clear that $K = a(\bar{0})$. Therefore, the value of K can be known if the polynomial $a(x)$ is known. A polynomial of degree $\rho - 1$ over $\mathbb{Z}_p$ can be uniquely interpolated from ρ points using the Lagrange interpolation.

Based on the scheme above, each participant P_i has (x_i, y_i) which is a point on the polynomial $a(x)$. Next, we will discuss about how a group of ρ participants can reconstruct K using their shares. Let $\{P_{i_1}, \cdots, P_{i_\rho}\}$ be a group of ρ participants who want to reconstruct K. It means that share y_{i_j} and the value x_{i_j}, $j = 1, \cdots, \rho$, are collected. In fact, $y_{i_j} = a(x_{i_j})$, $j = 1, \cdots, \rho$, where $a(x) \in \mathbb{Z}_p[x]$ is a secret polynomial of order $\rho - 1$ that has been chosen by D. Using the points (x_{i_j}, y_{i_j}), $j = 1, \cdots, \rho$, we can interpolate polinomial $a(x)$ using Langrange interpolation formula:

$$a(x) = \sum_{j=1}^{\rho} \left(y_{i_j} \prod_{1 \leq k \leq \rho, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}} \right) \mod p.$$

Hence, the value of K is obtained, that is $K = a(\bar{0})$.

III. THE MULTIVARIATE LAGRANGE INTERPOLATION

Saniee (2007) discussed the multivariate polynomial interpolation over field $\mathbb{R}$. In this section, we will extend it to be a multivariate polynomial interpolation over arbitrary field F.

Let $F[X_1, \cdots, X_m]$ be a multivariate polynomial ring, where F is a field. A monomial of variable $X_1, \cdots, X_m$ is defined as a multiplication $X_1^{e_1} X_2^{e_2} \cdots X_m^{e^m}$, where $e_1, \cdots, e_m$ are non-negative integers. Let $\boldsymbol{e} = (e_1, \cdots, e_m)$ be an n-tuple of non-negative integers. Define $X^{\boldsymbol{e}} :=$

$X_1^{e_1} X_2^{e_2} \cdots X_m^{e^m}$. By this notation, every polynomial $f(X_1, \cdots, X_m) \in F[X_1, \cdots, X_m]$ can be written as a finite summation of monomials with coefficients in F, that is $f(X_1, \cdots, X_m) = \sum_{\boldsymbol{e}} \alpha_{\boldsymbol{e}} X^{\boldsymbol{e}}$. The element $\alpha_{\boldsymbol{e}}$ in F is called coefficient of the monomial $X^{\boldsymbol{e}}$, and $\alpha_{\boldsymbol{e}} X^{\boldsymbol{e}}$ is called term of $f(X_1, \cdots, X_m)$. Degree of $f(X_1, \cdots, X_m) = \sum_{\boldsymbol{e}} \alpha_{\boldsymbol{e}} X^{\boldsymbol{e}}$ is defined as the value of $\max_{\boldsymbol{e}} \boldsymbol{e}$. If $f(X_1, \cdots, X_m)$ is a polynomial of degree n then $f(X_1, \cdots, X_m)$ can be written as follow:

$$f(X_1, \cdots, X_m) = \sum_{\boldsymbol{e_i} \cdot \mathbf{1} \leq n} \alpha_{\boldsymbol{e_i}} X^{\boldsymbol{e_i}},$$

where $\boldsymbol{e_i} \cdot \mathbf{1} := \sum_{j=1}^{m} e_{i_j}$.

Consider a polynomial $f(X_1, \cdots, X_m) = \sum_{\boldsymbol{e_i} \cdot \mathbf{1} \leq n} \alpha_{\boldsymbol{e_i}} X^{\boldsymbol{e_i}} \in F[X_1, \cdots, X_m]$ of degree n. Since $f(X_1, \cdots, X_m)$ is a polynomial with m variables and of degree n, there exist $\rho = \binom{n+m}{n}$ terms of $f(X_1, \cdots, X_m)$. Let $\boldsymbol{x_i} = (x_{i_1}, \cdots, x_{i_m}, f_i) \in F^{m+1}$, where $f_i = f(x_{i_1}, \cdots, x_{i_m})$, $i \in \{1, \cdots, \rho\}$, is ρ distinct points. By using these points, consider a system of linear equations $f_i = \sum_{\boldsymbol{e_j} \cdot \mathbf{1} \leq n} \alpha_{\boldsymbol{e_j}} \boldsymbol{x_i}^{\boldsymbol{e_j}}$, $i = 1, 2, \cdots, \rho$. The system has a unique solution if the sample matrix

$$M = \begin{pmatrix} \boldsymbol{x_1}^{\boldsymbol{e_1}} & \cdots & \boldsymbol{x_1}^{\boldsymbol{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{x_i}^{\boldsymbol{e_1}} & \cdots & \boldsymbol{x_i}^{\boldsymbol{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{x_\rho}^{\boldsymbol{e_1}} & \cdots & \boldsymbol{x_\rho}^{\boldsymbol{e_\rho}} \end{pmatrix}$$

is a non-singular matrix. On the other word, if the sample matrix is non-singular then there exists a unique $\alpha_{\boldsymbol{e_1}}, \cdots, \alpha_{\boldsymbol{e_\rho}}$ which meets the system of linear equations

$$f_i = \sum_{\boldsymbol{e_j} \cdot \mathbf{1} \leq n} \alpha_{\boldsymbol{e_j}} \boldsymbol{x_i}^{\boldsymbol{e_j}}, \quad i = 1, 2, \cdots, \rho. \tag{1}$$

To sum up, by using the ρ points, we can uniquely determine a multivariate polynomial of degree n.

In case the sample matrix M is singular, the system of linear equations (1) has either infinite number of solution or inconsistent. When the system of linear equations (1) has infinite number of solution, it means that the ρ points do not uniquely determine polynomial $f(X_1, \cdots, X_m)$.

Let $\boldsymbol{x_i} = (x_{i_1}, \cdots, x_{i_m}, f_i)$, $f_i = f(x_{i_1}, \cdots, x_{i_m})$, $i \in \{1, \cdots, t\}$ be t distinct points in F^{m+1}, $t < \rho$. The points form a system of linear equations $f_i = \sum_{\boldsymbol{e_j} \cdot \mathbf{1} \leq n} \alpha_{\boldsymbol{e_j}} \boldsymbol{x_i}^{\boldsymbol{e_j}}$, $i = 1, 2, \cdots, t$, where the number of equations is less than the number of variables. With this condition, it is clear that the system of linear equations has infinite solutions. It means that we do not have a unique polynomial that passes the points.

Similarly with the Lagrange interpolation for polynomial of one indeterminate, the formula of multivariate polynomial interpolation can also be determined. Define $\Delta = \det(M)$,

with

$$M = \begin{pmatrix} \boldsymbol{x_1^{e_1}} & \cdots & \boldsymbol{x_1^{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{x_i^{e_1}} & \cdots & \boldsymbol{x_i^{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{x_\rho^{e_1}} & \cdots & \boldsymbol{x_\rho^{e_\rho}} \end{pmatrix}$$

which is called sample matrix. For all $j = 1, \cdots, \rho$, define $\Delta_j(\boldsymbol{X}) = \det(M_j(\boldsymbol{X}))$, with

$$M_j(\boldsymbol{X}) = \begin{pmatrix} \boldsymbol{x_1^{e_1}} & \cdots & \boldsymbol{x_1^{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{X^{e_1}} & \cdots & \boldsymbol{X^{e_\rho}} \\ \vdots & & \vdots \\ \boldsymbol{x_\rho^{e_1}} & \cdots & \boldsymbol{x_\rho^{e_\rho}} \end{pmatrix} \leftarrow j^{th} \text{ row}$$

It is easy to prove that $\det(M_j(\boldsymbol{x_i})) = 0_F$ if $i \neq j$, and $\det(M_j(\boldsymbol{x_j})) = \Delta$. Next, define

$$l_i(\boldsymbol{X}) = \frac{\Delta_j(\boldsymbol{X})}{\Delta},$$

for all $j = 1, \cdots, \rho$. With the notations above, we get the formula of Lagrange interpolation for multivariate case as follow:

$$f(\boldsymbol{X}) = \sum_{j=1}^{\rho} f_j l_j(\boldsymbol{X}).$$

Example 3.1 Consider points

$$(1, 0, -1), (0, 1, -7), (2, 1, 3), (-1, 1, -6), (-3, 2, 1), (-2, -1, 11)$$

in $z = f(x, y)$ $(m = 2)$, where $f(x, y)$ is a multivariate polynomial of degree $n = 2$ over $\mathbb{R}$. we will interpolate a multivariate polynomial of degree 2 with 2 variables, namely, $z = f(x, y) = \alpha_1 x^2 + \alpha_2 xy + \alpha_3 y^2 + \alpha_4 x + \alpha_5 y + \alpha_6$, using the $\rho = \binom{2+2}{2} = 6$ points. First, create a system of linear equations as follow, and check whether its sample matrix is non-singular.

$$\left.\begin{array}{rcccccccccccc} -1 &=& \alpha_1 & & & & & + & \alpha_4 & & & + & \alpha_6 \\ -7 &=& & & & & \alpha_3 & & & + & \alpha_5 & + & \alpha_6 \\ 3 &=& 4\alpha_1 & + & 2\alpha_2 & + & \alpha_3 & + & 2\alpha_4 & + & \alpha_5 & + & \alpha_6 \\ -6 &=& \alpha_1 & - & \alpha_2 & + & \alpha_3 & - & \alpha_4 & + & \alpha_5 & + & \alpha_6 \\ 1 &=& 9\alpha_1 & - & 6\alpha_2 & + & 4\alpha_3 & - & 3\alpha_4 & + & 2\alpha_5 & + & \alpha_6 \\ 11 &=& 4\alpha_1 & + & 2\alpha_2 & + & \alpha_3 & - & 2\alpha_4 & - & \alpha_5 & + & \alpha_6 \end{array}\right\} \quad (2)$$

The sample matrix of (2) is

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 9 & -6 & 4 & -3 & 2 & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix}.$$

Since $\det(M) = -120 \neq 0$, the six points above define uniquely a multivariate polynomial of degree 2. Define:

$$M_1(x,y) = \begin{pmatrix} x^2 & xy & y^2 & x & y & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 9 & -6 & 4 & -3 & 2 & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix} \quad M_2(x,y) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ x^2 & xy & y^2 & x & y & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 9 & -6 & 4 & -3 & 2 & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix}$$

$$M_3(x,y) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ x^2 & xy & y^2 & x & y & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 9 & -6 & 4 & -2 & 2 & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix} \quad M_4(x,y) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ x^2 & xy & y^2 & x & y & 1 \\ 9 & -6 & 4 & -3 & 2 & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix}$$

$$M_5(x,y) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ x^2 & xy & y^2 & x & y & 1 \\ 4 & 2 & 1 & -2 & -1 & 1 \end{pmatrix} \quad M_6(x,y) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 2 & 1 & 2 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 \\ 9 & -6 & 4 & -3 & 2 & 1 \\ x^2 & xy & y^2 & x & y & 1 \end{pmatrix}.$$

Then,

$$\begin{aligned} \Delta_1(x,y) &= 12y^2 + 36xy - 36x + 72y - 84 \\ \Delta_2(x,y) &= 60x^2 - 240y^2 - 60x + 120y \\ \Delta_3(x,y) &= -20x^2 - 20xy + 40y^2 - 60y + 20 \\ \Delta_4(x,y) &= -40x^2 - 16xy + 248y^2 + 96x - 192y - 56 \\ \Delta_5(x,y) &= 12xy - 36y^2 + 24y - 12x + 12 \\ \Delta_6(x,y) &= -12xy - 24y^2 + 12x + 36y - 12. \end{aligned}$$

Therefore, we have

$$\begin{aligned} f(x,y) &= -\frac{\Delta_1(x,y)}{\Delta} - 7\frac{\Delta_2(x,y)}{\Delta} + 3\frac{\Delta_3(x,y)}{\Delta} - 6\frac{\Delta_4(x,y)}{\Delta} + \frac{\Delta_5(x,y)}{\Delta} + 11\frac{\Delta_6(x,y)}{\Delta} \\ &= 2x^2 + xy - 4y - 3. \end{aligned}$$

Since we have know the matrix M of which the entries are coefficients of the system (2), we

can also do an interpolation by solving the system (2) as follow:

$$\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\\ \alpha_5\\ \alpha_6\end{pmatrix} = M^{-1}\begin{pmatrix}-1\\ -7\\ 3\\ -6\\ 1\\ 11\end{pmatrix} = \begin{pmatrix}2\\ 1\\ 0\\ 0\\ -4\\ -3\end{pmatrix}.$$

Hence,

$$\begin{aligned} f(x,y) &= \alpha_1 x^2 + \alpha_2 xy + \alpha_3 y^2 + \alpha_4 x + \alpha_5 y + \alpha_6 \\ &= 2x^2 + xy - 4y - 3. \end{aligned}$$

IV. A SECRET SHARING SCHEME USING MULTIVARIATE POLYNOMIALS

In this section, we give a secret sharing scheme based on multivariate polynomials. Suppose D wants to divide a secret $K \in \mathbb{Z}_p$ into r partial information and to distribute it to participants $P_1, \cdots, P_r$. The scheme is given as follow:

(i). The dealer D secretly chooses a multivariate polynomial $f(X_1, \cdots, X_m)$ of degree n in $\mathbb{Z}_p[X_1, \cdots, X_m]$, where $\binom{n+m}{n} \leq r$ and its constant term is K.
(For simplicity, $\binom{n+m}{n}$ is denoted by ρ.)

(ii). The dealer D secretly chooses r distinct points on $z = f(X_1, \cdots, X_m)$, namely,

$$(x_{1_i}, \cdots, x_{m_i}, f_i) \in \mathbb{Z}_p^{m+1}, \text{ with } f_i = f(x_{1_i}, \cdots, x_{m_i}), \;\; i = 1, \cdots, r,$$

such that every ρ points of the r points, its sample matrix is non-singular.

(iii). For all $i = 1, \cdots, r$, D distributes share $(x_{1_i}, \cdots, x_{m_i}, f_i)$ to P_i secretly.

Suppose a group of participants $\{P_{i_1}, P_{i_2}, \cdots, P_{i_\rho}\} \subseteq \{P_1, \cdots, P_r\}$ wants to reconstruct the secret K using their shares: $(x_{i_j}, \cdots, x_{i_j}, f_{i_j}), \;\; j = 1, 2, \cdots, \rho$. Note that each share is a point in the multivariate polynomial $f(X_1, \cdots, X_m)$. Therefore, once they successfully obtain the multivariate polynomial $f(X_1, \cdots, X_m)$, they get $K = f(\bar{0}, \cdots, \bar{0})$.

In the secret sharing scheme using multivariate polynomials, determining the number of variable and the degree of the polynomial depends on threshold parameter (the parameter ρ). The value of ρ should not be less than 3 since $\rho = 2$ is only associated to a polynomial with $m = 1$ variable (not a multivariate polynomial).

For all threshold parameters, there exists a multivariate polynomial that associates with. Suppose a dealer wants to divide K using threshold parameter $\rho_0 \geq 3$ and r_0. It means that the partial information of K will be given to r_0 participants, and K can only be reconstructed if at least ρ_0 participants are gathered. The dealer can choose a multivariate polynomial with $m = \rho_0 - 1$ variable and of degree $n = 1$ since $\binom{n+m}{n} = \binom{(\rho_0 - 1)+1}{1} = \binom{\rho_0}{1} = \rho_0$.

One of the weakness of this scheme is in determining the number of variable and the degree of multivariate polynomial is not flexible when the threshold parameter has been determined

first. For instance, if a dealer wants to divide a secret K using threshold parameter $\rho = 5$ then the only choice for the number of variable on polynomial is $m = 4$ and the degree of polynomial is $n = 1$. There is no other m and n such that $\binom{n+m}{n} = 5$.

Example 4.1 Suppose a dealer D wants to divide a secret $K = \overline{234} \in \mathbb{Z}_{313}$ into $r = 10$ shares and to distribute it to participants $P_1, \cdots, P_{10}$. The dealer wants to design a system in order that K can be reconstructed if there exist at least $\rho = 6$ participants who are gathered. Secretly D choose a multivariate polynomial of degree 2 and with 2 variable (see Table 1.):

$$f(x, y) = \overline{37}x^2 + \overline{12}xy + \overline{13}y^2 + \overline{11}x + \overline{5}y + \overline{234} \in \mathbb{Z}_{313}[x, y]$$

and choose 10 points on the polynomial:

$$\begin{array}{llll} \boldsymbol{s_1} = (\overline{3}, \overline{103}, \overline{12}), & \boldsymbol{s_2} = (\overline{121}, \overline{3}, \overline{20}), & \boldsymbol{s_3} = (\overline{10}, \overline{33}, \overline{103}), & \boldsymbol{s_4} = (\overline{23}, \overline{210}, \overline{78}), \\ \boldsymbol{s_5} = (\overline{300}, \overline{5}, \overline{280}), & \boldsymbol{s_6} = (\overline{100}, \overline{27}, \overline{186}), & \boldsymbol{s_7} = (\overline{18}, \overline{40}, \overline{118}), & \boldsymbol{s_8} = (\overline{92}, \overline{22}, \overline{178}), \\ \boldsymbol{s_9} = (\overline{75}, \overline{32}, \overline{117}), & \boldsymbol{s_{10}} = (\overline{42}, \overline{113}, \overline{266}). & & \end{array}$$

Every six points of the points above results a non-singular sample matrix. Therefore, the ten points above can be used by the dealer as shares. Next, for all $i = 1, \cdots, 10$, the dealer distributes $\boldsymbol{s_i}$ to P_i.

Suppose six participants $P_1, P_4, P_5, P_7, P_9, P_{10}$ wants to reconstruct K using their shares, i.e. $\boldsymbol{s_1}, \boldsymbol{s_4}, \boldsymbol{s_5}, \boldsymbol{s_7}, \boldsymbol{s_9}, \boldsymbol{s_{10}}$. They have the sample matrix

$$M = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix}.$$

and $\Delta = \det(M) = 290$. Define:

$$M_1(x, y) = \begin{pmatrix} x^2 & xy & y^2 & x & y & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix}, \quad M_2(x, y) = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ x^2 & xy & y^2 & x & y & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix},$$

$$M_3(x, y) = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ x^2 & xy & y^2 & x & y & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix}, \quad M_4(x, y) = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ x^2 & xy & y^2 & x & y & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix},$$

$$M_5(x,y) = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ x^2 & xy & y^2 & x & y & \overline{1} \\ \overline{199} & \overline{51} & \overline{249} & \overline{42} & \overline{113} & \overline{1} \end{pmatrix}, \quad M_6(x,y) = \begin{pmatrix} \overline{9} & \overline{309} & \overline{280} & \overline{3} & \overline{103} & \overline{1} \\ \overline{216} & \overline{135} & \overline{280} & \overline{23} & \overline{210} & \overline{1} \\ \overline{169} & \overline{248} & \overline{25} & \overline{300} & \overline{5} & \overline{1} \\ \overline{11} & \overline{94} & \overline{35} & \overline{18} & \overline{40} & \overline{1} \\ \overline{304} & \overline{209} & \overline{85} & \overline{75} & \overline{32} & \overline{1} \\ x^2 & xy & y^2 & x & y & \overline{1} \end{pmatrix}.$$

Then,

$$\begin{aligned} \Delta_1(x,y) &= \overline{302}x^2 + \overline{141}xy + \overline{138}y^2 + \overline{90}x + \overline{76}y + \overline{226} \\ \Delta_2(x,y) &= \overline{69}x^2 + \overline{63}xy + \overline{143}y^2 + \overline{215}x + \overline{107}y + \overline{196} \\ \Delta_3(x,y) &= \overline{212}x^2 + \overline{80}xy + \overline{57}y^2 + \overline{227}x + \overline{207}y + \overline{201} \\ \Delta_4(x,y) &= \overline{177}x^2 + \overline{84}xy + \overline{273}y^2 + \overline{144}x + \overline{247}y + \overline{33} \\ \Delta_5(x,y) &= \overline{63}x^2 + \overline{293}xy + \overline{207}y^2 + \overline{96}x + \overline{88}y + \overline{275} \\ \Delta_6(x,y) &= \overline{116}x^2 + \overline{278}xy + \overline{121}y^2 + \overline{167}x + \overline{214}y + \overline{298}. \end{aligned}$$

Hence,

$$\begin{aligned} f(x,y) &= \overline{12}\frac{\Delta_1(x,y)}{\Delta} + \overline{78}\frac{\Delta_2(x,y)}{\Delta} + \overline{280}\frac{\Delta_3(x,y)}{\Delta} + \overline{118}\frac{\Delta_4(x,y)}{\Delta} + \overline{117}\frac{\Delta_5(x,y)}{\Delta} + \overline{266}\frac{\Delta_6(x,y)}{\Delta} \\ &= \overline{37}x^2 + \overline{12}xy + \overline{13}y^2 + \overline{11}x + \overline{5}y + \overline{234}. \end{aligned}$$

With other way, for determining the coefficient $f(x,y) = \alpha_1 x^2 + \alpha_2 xy + \alpha_3 y^2 + \alpha_4 x + \alpha_5 y + \alpha_6$, they can also use the invers of the sample matrix M.

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \end{pmatrix} = M^{-1} \begin{pmatrix} \overline{12} \\ \overline{78} \\ \overline{280} \\ \overline{118} \\ \overline{117} \\ \overline{266} \end{pmatrix} = \begin{pmatrix} \overline{191} & \overline{310} & \overline{18} & \overline{142} & \overline{215} & \overline{63} \\ \overline{198} & \overline{215} & \overline{119} & \overline{78} & \overline{205} & \overline{124} \\ \overline{307} & \overline{21} & \overline{120} & \overline{97} & \overline{304} & \overline{90} \\ \overline{173} & \overline{222} & \overline{99} & \overline{89} & \overline{268} & \overline{88} \\ \overline{160} & \overline{77} & \overline{304} & \overline{207} & \overline{37} & \overline{154} \\ \overline{31} & \overline{182} & \overline{209} & \overline{53} & \overline{233} & \overline{232} \end{pmatrix} \begin{pmatrix} \overline{12} \\ \overline{78} \\ \overline{280} \\ \overline{118} \\ \overline{117} \\ \overline{266} \end{pmatrix} = \begin{pmatrix} \overline{37} \\ \overline{12} \\ \overline{13} \\ \overline{11} \\ \overline{5} \\ \overline{234} \end{pmatrix}$$

Hence, $K = \overline{234}$.

Note:
We used MAGMA (http://magma.maths.usyd.edu.au/) for doing the calculation above. The program script can be found in the Appendices.

V. CONCLUSION

The secret sharing scheme based on multivariate polynomials can be constructed by adopting the Shamir's secret sharing scheme. However, when the dealer wants to divide the secret K with threshold parameter (ρ_0, r_0), the choice of the number of variables (m) and the degree (n) for the polynomial used in the scheme are not flexible. For example, if he has decided to determine $\rho = 4$ then the only choice of the parameters are $m = 3$ and $n = 1$ (see Table 1.). This becomes a weakness of the scheme.

In our scheme, the parameter m should be greater than or equal to 2 in order that the used polynomial is multivariate. If $m = 1$ then the polynomial used on the scheme is a polynomial with one indeterminate. Because our scheme is adopted from Shamir's secret sharing scheme, our scheme is equal to the Shamir's scheme when $m = 1$. Therefore, we can conclude that our scheme can be considered as a generalization of Shamir's secret sharing scheme.

Table 1. Some threshold parameters ρ

m	n	$\rho = \binom{n+m}{n}$	m	n	$\rho = \binom{n+m}{n}$	m	n	$\rho = \binom{n+m}{n}$
2	1	3	4	1	5	6	1	7
2	2	6	4	2	15	6	2	28
2	3	10	4	3	35	6	3	84
2	4	15	4	4	70	6	4	210
2	5	21	4	5	126	6	5	462
3	1	4	5	1	6	7	1	8
3	2	10	5	2	21	7	2	36
3	3	20	5	3	56	7	3	120
3	4	35	5	4	126	7	4	330
3	5	56	5	5	252	7	5	792

REFERENCES

[1] K. Saniee, "A simple expression for multivariate lagrange interpolation," *SIAM*, vol.1, no.1, pp.1–9, 2007.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol.22, pp.612–613, 1979.

[3] D. Stinson, *Cryptography: Theory and Practice, Third Edition*, CRC Press, Inc., Florida, 2006.

[4] T, Tassa, T., N. Dyn, "Multipartite secret sharing by bivariate interpolation," *Journal of Cryptology*, vol.22, no.2, pp.227–258, 2006.

APPENDICES

Program Script: Secret Sharing Scheme Based on Multivariate Polynomials

```
//Defining some parameters
r := 10; //number of participant
n := 2; //degree of the secret polynomial
m := 2; //number of the secret polynomial variable
p := 313; //a prime number (as order of the finite field Zp)

rho := Binomial(n+m,n);

//Defining a finite field of order p and a polynomial ring
FF := GF(p);
F<x,y> := PolynomialRing(FF,m,"glex");

//a secret K and a secret polynomial
K := 234;
p := 37*x^2 + 12*x*y + 13*y^2 + 11*x +5*y + K;

//r choosen points (W) ==============
S := Matrix(FF,r,m+1,

            [3, 103, 0,
            121, 3, 0,
            10, 33, 0,
            23, 210, 0,
            300, 5, 0,
            100, 27, 0,
            18, 40, 0,
            92, 22, 0,
            75, 32, 0,
            42, 113, 0]
);

mon := MonomialsOfWeightedDegree(F, n);
for i in [n-1..0 by -1] do
    mon := mon join MonomialsOfWeightedDegree(F, i);
end for;

w := ZeroMatrix(FF,1,r*rho);
w := Eltseq(w);
k := 0;
for i in [1..r] do
    s := Submatrix(S,i,1,1,m);
    S[i,m+1] := Evaluate(p, Eltseq(s));

    for j in [1..#mon] do
        k := k+1;
        w[k] := Evaluate(mon[j], Eltseq(s));
    end for;
```

```
end for;
W := Matrix(FF,r,rho,w);
//==================================


//Checking whether the r points can be used for shares
comb := Subsets({1..r},rho);
Comb := SetToSequence(comb);
for i in [2..#Comb] do
    idM := SetToSequence(Comb[1]);
    M := Submatrix(W,idM[1],1,1,rho);
    for j in [2..rho] do
        M := VerticalJoin(M,Submatrix(W,idM[j],1,1,rho));
    end for;
    if Determinant(M) eq 0 then
    M;
        print "The following points can not be used for shares.";
        S;
        status := 0;
        break;
    else
        status := 1;
    end if;
end for;

if status eq 1 then
    print "The following points can be used for shares:";
    S;
end if;
```

Program Script: Reconstructing A Key

```
//Defining some parameters
r := 10; //number of participant
n := 2; //degree of the secret polynomial
m := 2; //number of the secret polynomial variable
p := 313; //a prime number (as order of the finite field Zp)

rho := Binomial(n+m,n);

//Defining a finite field of order p and a polynomial ring
FF := GF(p);
F<x,y> := PolynomialRing(FF,m,"glex");

//shares ==============
S := Matrix(FF,rho,m+1,
            [3, 103, 12,
            23, 210, 78,
            300, 5, 280,
            18, 40, 118,
```

```
            75, 32, 117,
            42, 113, 266]
);

mon := MonomialsOfWeightedDegree(F, n);
for i in [n-1..0 by -1] do
    mon := mon join MonomialsOfWeightedDegree(F, i);
end for;

w := ZeroMatrix(FF,1,rho*rho);
w := Eltseq(w);
k := 0;
for i in [1..rho] do
    s := Submatrix(S,i,1,1,m);

    for j in [1..#mon] do
        k := k+1;
        w[k] := Evaluate(mon[j], Eltseq(s));
    end for;
end for;
W := Matrix(F,rho,rho,w);
//===================================

D := Determinant(W);
"Delta =",D,"\n";

P := 0;
for i in [1..rho] do
    M := W;
    mo := SetToSequence(mon);
    InsertBlock(~M, Matrix(F,1,rho,mo), i,1);
    d := Determinant(M);
    "Delta",i,"=",d;

    p := p + S[i,m+1]*(d/D);
end for;
C := Coefficients(p);

"\n The secret polynomial:\n p =",p;
"\n The secret:\n K =", C[#C];
```