International Journal of Cryptology Research 4(1): 73 - 83 (2013)

Bivariate Polynomials Public Key Encryption Schemes

[1*] **Ruma Kareem Ajeena,** [1] **Hailiza Kamarulhaili and**
[2] **Sattar B. Almaliky**

[1]*School of Mathematical Sciences,*
Universiti Sains Malaysia, 11800 Minden, Penang, Malaysia

[2]*Computer Sciences School, Babylon University, Iraq*

E-mail: ruma_kareem@yahoo.com, hailiza@cs.usm.my and
Sattar-Almaliky@yahoo.com

*Corresponding author

ABSTRACT

One of the important fundamental problems in cryptography is a Polynomial Reconstruction Problem (PRP). There are several public key cryptographic systems constructed based on this problem. This paper provides an analytical study on a public key cryptosystem (*PKC*) that is based on bivariate polynomial Reconstruction Problem (*BPRP*) and takes into considerations the developments performed on the (*PKC*). A modification is proposed using bivariate polynomial instead of univariate polynomial which is used in the original Augot's system to enhance its security. The analysis concerned mainly the mathematical backgrounds related to bivariate polynomials and the operation, valid generally for these polynomials, especially in the finite fields $GF(q)$. The coding problem is included in the public key cryptosystem that considers the (*BPRP*). The Reed-Solomon Code is used in such type of (*PKC*) based on (*BPRP*).

Keywords: Polynomial Reconstruction Problem (PRP), cryptographic systems, Reconstruction Problem (*BPRP*), bivariate polynomials..

1. INTRODUCTION

Cryptography is one of the oldest fields of technical study. The records went back at least 4000 years. There are only 3 systems which is widely spread and remain hard enough to be broken and of real value. One of them takes too much space for most practical uses, another is too slow for most practical uses, and the third is widely believed to contain serious weaknesses. [1].

The Cryptography is a term which refers to the design of cryptosystems and cryptanalysis. This science Cryptology is divided into three parts; the cryptosystem designing part which is specialized in designing and constructing cryptosystems, the cryptanalysis part which is specialized in finding techniques and methods of transforming the cipher text to plain text, and the evaluation of the algorithms part which is specialized in calculating the complexities of these algorithms [2]. We consider a special class of Bose, Chaudhuri and Hocquenghem (BCH) codes and several important techniques available to enhance error correction capabilities. In particular, the well known Reed-Solomon Codes, is very widely used in mass storage systems to correct the burst errors associated with media defects. Reed Solomon error correction is a coding scheme which works by first constructing a polynomial from the data symbols to be transmitted and then sending an over-sampled plot of the polynomial instead of the original symbols themselves. Because of the redundant information contained in the over-sampled data, it is possible to reconstruct the original polynomial and thus the data symbols even in the face of transmission errors, up to a certain degree of error [3].

Electronic commerce requires at least the following fundamental cryptological primitives: one digital signature, one public-key encryption or key exchange scheme, and symmetric cipher. Currently most deployed PKCs involve the integer factoring problem or BPRP. We aim to introduce a new public-key encryption scheme that may be used for this problem. This is one of many schemes based on the difficulty of solving a system of bivariate polynomial equations. PKCs of this class are usually described as Bivariate (multivariate) or polynomial – based schemes [4].

2. MATHEMATICAL BACKGROUND

Definition 2.1: [5] A polynomial in two variables (that is a bivariate polynomial) with constant coefficients is given by

$$a_{nm}x^n y^m + \ldots + a_{22}x^2y^2 + a_{21}x^2y + a_{12}xy^2 + a_{11}xy + a_{10}x + a_{01}y + a_{00}. \qquad (1)$$

Definition 2.2: [5] The sum of two polynomials is obtained by adding together the coefficients sharing the same powers of variables (i.e., the same terms). For example,

$$(a_2x^2 + a_1x + a_0) + (b_1x + b_0) = a_2x^2 + (a_1 + b_1)x + (a_0 + b_0). \qquad (2)$$

This polynomial has order less than (in the case of cancellation of leading terms) or equal to the maximum order of the original two polynomials. Similarly, the product of two polynomials is obtained by multiplying term by term and combining the results, for example

$$\begin{aligned}(a_2x^2+a_1x+a_0)(b_1x+b_0)&=a_2x^2(b_1x+b_0)+a_1x(b_1x+b_0)+a_0(b_1x+b_0)\\&=a_2b_1x^3+(a_2b_0+a_1b_1)x^2+(a_1b_0+a_0b_1)x+a_0b_0,\end{aligned}\tag{3}$$

and has order equal to the sum of the orders of the two original polynomial [5].

Definition 2.3: The ***Reed- Solomon Code*** ($[n, k]$ RS_k code) of dimension k and length n over F_q is the following set of n - tuples (codeword)

$$RS_k=\{ev(f(x,y)):f\in F_q[x,y],\ \deg\ (f)<k\},\tag{4}$$

where $F_q[x,y]$ is the set of bivariate polynomials with coefficients in F_q. The set $(x_i,y_j),\quad i,j\in\{1,2,.....,n\}$ is called the Support of RS_k.

The Vandermonde Method

Suppose we have *4* 2D points (0, 1), (2, 5), (4, 3), and (6, 7) and we have values for each of these points, e.g., ((0, 1), 13), ((2, 5), 17), ((4, 3), 15), and ((6, 7), 18) and we want to fit a bivariate polynomial through these points. From the Vander monde method, it would make sense that we could find an interpolated bivariate polynomial with four terms, for example:

$$p(x,y)=c_1xy+c_2x+c_3y+c_4.\tag{5}$$

Thus, if we were to simply evaluate $p(x,y)$ at these four points, we get four equations:

$$\begin{aligned}p(0,1)&=c_1 0+c_2 0+c_3 1+c_4=13\\p(2,5)&=c_1 10+c_2 2+c_3 5+c_4=17\\p(4,3)&=c_1 12+c_2 4+c_3 3+c_4=15\\p(6,7)&=c_1 42+c_2 6+c_3 7+c_4=19\end{aligned}$$

This defines a system of linear equations which we may solve. In this case, the Vander monde matrix is the rather simple

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 10 & 2 & 5 & 1 \\ 12 & 4 & 3 & 1 \\ 42 & 6 & 7 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 13 \\ 17 \\ 15 \\ 19 \end{bmatrix}$$

where $c = (c_1, c_2, c_3, c_4)^T$.

Subsequently, the generalization can be drawn to n points

$$((x_1, y_1), z_1), ((x_2, y_2), z_2), \ldots, ((x_n, y_n), z_n). \qquad (2.6)$$

The polynomial $p(x, y)$ which passes through those points in equation (2.6) has degree n-1, and we can find it by the following steps.

i. Write down the formula of the general polynomial $p(x, y)$ of degree n-1;
ii. Evaluate the polynomial $p(x, y)$ at the points $((x_1, y_1), z_1)$, $((x_2, y_2), z_2)$,..., $((x_n, y_n), z_n)$, and
iii. Solve the system of linear equations.

Instead of execution all these operations, the problem easily can be written as Vc=Y where Y is the vector of y values, c represents the vector of coefficients, and v is the Vandermonde matrix.

Uniqueness

It is possible to find one polynomial which has a degree n-1 passes through n points. Assuming the (x_i, y_j), where $i = 1, ..., n$, pairs of values are unique. Since there are n points, the degree of the interpolating polynomial must have n terms. Thus, the form of the interpolating polynomial may be various, for example, given four points in a square, (0, 0), (0, 1), (1, 0), (1, 1), the logical choice is

$$p(x, y) = c_1xy + c_2x + c_3y + c_4.$$

Given nine points in a square, we could use,

$$p(x,y) = c_1x^2y^2 + c_2x^2y + c_3xy^2 + c_4x^2 + c_5y^2 + c_6xy + c_7x + c_8y + c_9.$$

Definition 2.4 (The Vandermonde matrix)

We define the *n* × *n* Vander monde matrix V by evaluating the *n* terms on each of the *n* points. We can generalize the Vandermonde method to interpolate multivariate real-valued functions. We will focus on bivariate polynomials, and the generalization is obvious.

Definition 2.5 (Bivariate Interpolation) [6]

Let $f(x, y)$ be a function defined for a surface. Given points $((x_1, y_1), z_1)$, $((x_2, y_2), z_2)$, ..., $((x_n, y_n), z_n)$. To find an interpolating polynomial, we simply substitute the points into the bivariate polynomial, and obtained naturally a system of linear equations in the coefficients which may then be solved using Gaussian elimination or LU decomposition.

Example 2.2: Find the polynomial which interpolates the points ((3, 3), -1), ((3, 4), 2), ((5, 3), 1). Because there are three points, the interpolating polynomial could be of the form $p(x,y) = c_1x + c_2y + c_3$. Thus, we define the Vander monde matrix

$$\begin{bmatrix} 3 & 3 & 1 \\ 3 & 4 & 1 \\ 5 & 3 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}$$

and solve the system $V_c = Z$, where $Z = (-1,2,1)^T$. This gives the result $c = (1,3,-13)^T$ and therefore the interpolating polynomial is $p(x,y) = x + 3y - 13$.

Example 2.3: Find the polynomial which interpolates the points ((3, 3), 5), ((3, 4), 6), ((4, 3), 7), ((4, 4), 9). Because there are four points, the interpolating polynomial could reasonably be of the form $p(x) = c_1xy + c_2x + c_3y + c_4$. Thus, we define the Vander monde matrix

$$\begin{bmatrix} 9 & 3 & 3 & 1 \\ 12 & 3 & 4 & 1 \\ 12 & 3 & 4 & 1 \\ 16 & 4 & 4 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 5 \\ 6 \\ 7 \\ 9 \end{bmatrix}$$

and solve the system $V_c = Z$ where $Z = (5,6,7,9)^T$. This gives the result $c = (1,-1,-2,5)^T$ and therefore the interpolating polynomial is $p(x, y) = xy - x - 2y + 5$.

3. CRYPTOGRAPHIC SYSTEM BASED ON BPRP

Augot and Finiasz (2003) proposed the first public key encryption scheme based on the (PRP). This section will present discussion of the performances and state the parameters that are required to reach the desired security level from such scheme. Let us consider the following parameters:

- F_q is a finite field, q is the size of F_q.
- n is the length of the Reed –Solomon code used by this scheme.
- k its dimension.
- W is the weight of a large error E, so that the PRP for n, k, W is believed to be hard, or it must have $W > (n - k) / 2$ which need to be verified.
- w is the weight of a small error e, such that $w \leq (n - k) / 2$

Key Generation Process

Let us consider that we have two parties ***A*** and ***B***. Then want to have their communication using modified cryptosystem based on the bivariate polynomial.

A secretly does the followings:

- Choose the sets x and y.
- Generates a monic (unitary) bivariate polynomial $p(x, y)$ of degree equal to k -1**,** with respect x and of degree equal to k-1 with respect y.
- Generates an error vector E of dimension n with the weight W, where W is exactly non zero coordinates.
- Computes the codeword $C = ev(p(X, Y)) = p(x_i , y_j)$ of RS_k, $\exists$ $x_i = i$ and $y_j = j$ for $i = 1,2,\ldots\ldots,n$ and $j = 1,2,\ldots\ldots,n$.
- Computes

$$Pk = C + E, \tag{6}$$

where Pk is the public-key, while C and E are kept secret or the secret-key is (C, E).

Example 3.1: Let us have Modified Augot's Cryptosystem, n = 10, k =3, and $F_q = F_{11}$. Then it is required to generate the public-key. Let x = (2, 3, 3, 4, 5, 6, 7, 8, 9, 10), y = (4, 3, 6, 2, 1, 5, 7, 8, 9, 10).

- Generate a monic bivariate polynomial $p(x, y) = x^2y + xy^2 + 3xy + 5$.
- Generate a random 10 - dimension vector E of weight W =3, is exactly non zero coordinates, E = (0,0,0,10,0,7,3,0,0,0), since $W \geq \lfloor (n-k)/2 \rfloor = 3.$ That is, W =3.
- Compute the codeword $C = ev(p(X,Y))$ of RS_k. That is, $C = p(x_i, y_j) \bmod q, \exists \ x_i = i$ and $x_j = j$ for i = 1,2,……,n and $j = 1,2,\ldots,\ldots,n.$

  $p(2 , 4) = 0$, $p(3, 3) = 9$, $p(3, 6) =1$, $p(4, 2) = 0$, $p(5, 1) = 6$, $p(6, 5)$= 7, $p(7, 7)$ = 2, $p(8, 8)$ = 0, $p(9,9)$ =1, $p(10,10)$ =6. Then C = (0,9,1,0,6,7,2,0,1,6).

The public-key is $Pk = C+E$ = (0, 9, 1, 10, 6, 3, 5, 0, 1, 6).

Encryption Process

Let us consider that ***B*** wishes to send a message to ***A***. The message m_0 of length k +1 over the alphabet F_q. The following steps will be performed:

- Generates the m_0 bivariate polynomial of length k +1, where m_0 = $m_{0,0}$, …….., $m_{0,\ k+1}$ is seen as the polynomial :

$$m_0(X,Y) = m_{0,0} + m_{0,1}Y + m_{0,2}X + \ldots\ldots + m_{0,k-2}X^{k-2}Y^{k-2} \qquad (7)$$

- The message is firstly encoded using (Reed-Solomon Code) into a codeword m in RS_{k-1}.
- Randomly generates a primitive element $\alpha \in F_q$.
- Randomly generates an error pattern vector e of dimension n with the weight w, where w is exactly nonzero coordinates.
- Compute the cipher text

$$CT = m + \alpha \times Pk + e. \qquad (8)$$

- Transmits CT to ***A***.

Example 3.2: Let us have Modified Augot's Cryptosystem, n = 10, k =3 , and $F_q = F_{11}$ and Pk = (0,9,1,10,6,3,5,0,1,6). Then it is required to compute the encrypted message. The encryption of the message can be computed as follows:

Let $m_0(X, Y) = xy + 2x + 4y + 3$, that length k +1= 4, deg (m_0) = 1 with respect x and deg (m_0) = 1 with respect y, and the coefficients 2, 4 and 3 $\in F_{11.}$

Compute m_s for s = 1, 2, ……., 10.

$m_1 = m_0(2, 4) = 9$, $m_2 = m_0(3, 3) = 8$, $m_3 = m_0(3, 6) = 7$, $m_4 = m_0(4, 2) = 5$, $m_5 = m_0(5, 1) = 0$, $m_6 = m_0(6, 5) = 10$, $m_7 = m_0(7, 7) = 6$, $m_8 = m_0(8, 8) = 5$, $m_9 = m_0(9, 9) = 6$, $m_{10} = m_0(10, 10) = 9$.

That is m = (9, 8, 7, 5, 0, 10, 6, 5,6,9), let α $=3 \in F_{11}$ and since $w \leq \lfloor (n-k)/2 \rfloor = 3$, let w = 1, then e = (0, 0, 0, 0, 0, 7, 0, 0,0,0), where e has exactly w =1 non zero coordinates.

The cipher text is $CT = m + \alpha \times Pk + e$, that is CT_s for s = 1,2,……,10.

$CT_1 = m_1 + \alpha \times Pk_1 + e_1 = 9$, $CT_2 = 2$, $CT_3 = 10$, $CT_4 = 2$, $CT_5 = 7$, $CT_6 = 4$, $CT_7 = 10$,
$CT_8 = 5$, $CT_9 = 9$, $CT_{10} = 5$. Then CT = (9, 2, 10, 2, 7, 4, 10, 5, 9, 5).

Decryption Process

We proposed a modification to this system by using Vander monde interpolation Method instead of Berlekamp-Welch Interpolation that was used in the original Augot system. Hence we will describe the steps of the proposed decryption process.

Upon receipt of $CT = m + \alpha \times Pk + e$. **A** will perform the following steps:

- Considers only the positions where $E_{\text{i}} = 0$.
- Considers the shortened code of length n-W which is also a Reed Solomon Code of dimension k, $(\overline{RS_k})$.
- Solve the equation $\overline{m} + \alpha \times \overline{C} + \overline{e} = \overline{CT}$, where $\overline{m}$, $\overline{C}$, $\overline{e}$ correspond to the shortened versions of m, C, e. And E has disappeared, $\overline{m} + \alpha \times \overline{C} \in \overline{RS_k}$.

- Computes by using Vander monde interpolation Method, the unique polynomial *q*(*X*, *Y*) of degree *k* -1 such that $ev(q(X,Y)) = \overline{m} + \alpha \times \overline{C}$.
- Computes $q(X,Y) - \alpha p(X,Y) = m_0(X,Y)$, where *α* leading coefficient of *q*(*X*, *Y*), $\overline{C}$ = *ev*(*p*(*X*, *Y*)) and *p*(*x*, *y*) has degree $k-1, \deg(m_0) \leq k-2$.

Example 3.3: Let us have Modified Augot's Cryptosystem based on bivariate polynomial, *n* = 10, *k* =3 , and $F_q = F_{11}$, *Pk* = (0,9,1,10,6,3,5,0,1,6) and *CT* =(9, 2, 10, 2, 7, 4,10, 5,9,5). Then it is required to apply the decryption process and recover the message.

The decryption of the cipher text and recover the message can compute by the steps:
Firstly, compute *n-W* =7. That is, $E_1 = E_2 = E_3 = E_5 = E_8 = E_9 = E_{10}$=0, and $\overline{CT}$ = (CT_1, CT_2, CT_3, CT_5, CT_8, CT_9, CT_{10}) = (9, 2, 10, 7, 5, 9, 5).

By using Vander monde interpolation Method, we can compute the unique bivariate polynomial *q*(*X*, *Y*) of degree *k* -1= 2 with respect *x* and *y* such that *ev*(*q*(*X*, *Y*)) $= \overline{m} + \alpha \times \overline{C}$. Since $\overline{CT} = \overline{m} + \alpha \times \overline{C} + \overline{e}$, where $\overline{m} + \alpha \times \overline{C} \in \overline{RS_k}$, and $\overline{e} < \overline{w} \leq$ (*n-W-k*)/2. Then $\overline{CT}$ = *ev*(*q*(*X*, *Y*)) $= \overline{m} + \alpha \times \overline{C}$, that is, $CT_1 = q(2, 4) = 9$, $CT_2 = q(3, 3) = 2$, $CT_3 = q(3, 6) = 10$, $CT_5 = q(5, 1) = 7$, $CT_8 = q(8, 8) = 5$.

Now, applying the Vander monde interpolation method to find a bivariate polynomial *q*(*X*, *Y*). Since x = 2, 3, 3, 4, 5, 6, 7, 8,9,10 and y = 4, 3, 6, 2, 1, 5, 7, 8,9,10 then we get seven shadows: CT_1, CT_2, CT_3, CT_5, CT_8, CT_9 ,CT_{10} , we can construct *q*(*X*, *Y*) from four of the shadows: CT_1, CT_2, CT_3, CT_8 ,CT_9 ,CT_{10}.

Let $q(X, Y) = q_1 x^2 y + q_2 x y^2 + q_3 xy + q_4 x + q_5 y + q_6$, we have,

$$9 = q_1(16) + q_2(32) + q_3(8) + q_4(2) + q_5(4) + q_6$$
$$2 = q_1(27) + q_2(27) + q_3(9) + q_4(3) + q_5(3) + q_6$$
$$10 = q_1(54) + q_2(108) + q_3(18) + q_4(3) + q_5(6) + q_6$$
$$5 = q_1(512) + q_2(512) + q_3(64) + q_4(8) + q_5(8) + q_6$$
$$9 = q_1(729) + q_2(729) + q_3(81) + q_4(9) + q_5(9) + q_6$$
$$5 = q_1(1000) + q_2(1000) + q_3(100) + q_4(10) + q_5(10) + q_6$$

$$\begin{bmatrix} 5 & 10 & 8 & 2 & 4 & 1 \\ 5 & 5 & 9 & 3 & 3 & 1 \\ 10 & 9 & 7 & 3 & 6 & 1 \\ 6 & 6 & 9 & 8 & 8 & 1 \\ 3 & 3 & 4 & 9 & 9 & 1 \\ 10 & 10 & 1 & 10 & 10 & 1 \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \end{bmatrix} = \begin{bmatrix} 9 \\ 2 \\ 10 \\ 5 \\ 9 \\ 5 \end{bmatrix}$$

By using Gaussian Elimination we can find the coefficients $q_1 = 3$, $q_2 = 3$, $q_3 = 10$, $q_4 = 2$, $q_5 = 4$, $q_6 = 7$.Then $q(X, Y) = 3\,x^2y + 3xy^2 + 10xy + 2x + 4y + 7$. The leading coefficient of $q(X, Y) = 3 = \alpha$. Then the message is

$$\begin{aligned} m_0(X, Y) &= q(X, Y) - \alpha\ p(X, Y). \\ &= 3\,x^2y + 3xy^2 + 10xy + 2x + 4y + 7 - 3(x^2y + xy^2 + 3xy + 5) \\ &= (xy + 2x + 4y - 8) \bmod 11 \\ &= xy + 2x + 4y + 3. \end{aligned}$$

4. SECURITY IMPLICATIONS

In our modified scheme based on bivariate polynomial, we have managed to apply the scheme on key generation process, encryption and decryption processes of the cryptosystem. This improvement has increased the security level compared with the original cryptosystem which was based on a univarate polynomial. The adversaries will have to solve for two variables equation systems instead of just a single variable in the univarate version. This in return will give more running time to attack the bivariate polynomial cryptosystem based.

We can summarize the security level with the simple values:

n	*W*	*n-W*	*k*	Deg(*q*)	Number of shadows	Number of attempts to find *q*(*x*, *y*)
10	3	7	3	2	6	7
15	6	9	3	2	6	84
20	8	12	3	2	6	924
25	11	14	3	2	6	3003
30	13	17	3	2	6	12376
100	48	52	3	2	6	20358520
150	73	77	3	2	6	237093780
160	78	82	3	2	6	350161812
180	88	92	3	2	6	713068356
200	98	102	3	2	6	1.3465e+009

5. CONCLUSION

Giving the public-key and cipher text, we can recover the corresponding plaintext in bivariate polynomial. The proposed modified Cryptosystem based on BPRP and using Vander monde interpolation method is comparable with the original system. The use of polynomials with two variables instead of polynomials with one variable, help us to increase security level and resistance against many attacks. This work can be further extended to multivariate polynomials, where we can generalize the modified cryptosystem by using multivariate polynomials.

REFERENCES

[1] Wikipedia, History of Cryptography, the free encyclopedia en.wikipedia.org/wiki/History_of_cryptography, 17 January 2013.

[2] W. Diffie and M. E. Hellman. 1976. New Directions in Cryptography. *IEEE Trans. Inform. Theory*. **IT-22**.

[3] L-C. Wang, B-Y. Yang Y-H Hu, and F. Lai. 2006. A Medium-Field Multivariate Public key encryption scheme.

[4] D. Augot and M. Finiasz. 2003. A public key encryption scheme bases on the Polynomial Reconstruction Problem. *Proceedings of Euro crypt2003*.

[5] Wikipedia, Bivariate Polynomials, the free encyclopedia, en.wikipedia.org/wiki/Polynomial _function, 19 January 2013.

[6] Douglas Wilhelm Harder. The Vandermonde Method. University of Waterloo, Ontario, Canada N2L 3G1. https://ece.uwaterloo. ca/~dwharder/NumericalAnalysis/05Interpolation/ andermonde/.