International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Encryption and Decryption without any Cryptographic Algorithm

K Mani, R. Mahendran

Department of Computer Science Nehru Memorial College, Puthanampatti, Tiruchirappalli District, Tamil Nadu, India

ABSTRACT

In both symmetric and asymmetric cryptosystems key plays a vital role in performing both encryption and decryption. Symmetric-key encryption is very fast but key management is a major issue. Asymmetric or public-key encryption is slow in nature but key management is not a major issue because one key is derived from another. In both encryption algorithms the security of cryptographic algorithms depends on the size of the key. Normally, the key is shared in symmetric-key algorithm or derived in public-key algorithm, then encryption is performed using any one of the cryptographic algorithms. But, in this paper, a novel method is used in generating the key in terms of 1-1 function for encryption and the inverse of 1-1 function is used for decryption. For generating the key a multivariate polynomial, magic rectangle and Vandermonde Matrix are used. Based on 1-1 and inverse of 1-1 function encryption and decryptions are performed respectively without using any existing cryptographic algorithm

Keywords: Multivariate Polynomial, Magic Rectangle, Vandermonde Matrix, 1-1 function, Inverse function and Key

I. INTRODUCTION

A cryptographic system [1] consists of a plaintext message space M, a ciphertext message space C, an encryption key space K, and the decryption key space K′, an efficient key generation algorithm $G:N \mapsto K\times K'$, an efficient encryption algorithm $E:M\times K\mapsto C$ and an efficient decryption algorithm $D:C\times K^{-1}\mapsto M$. For $k\in K$ and $m\in M$, we denote by $C= E_{k_e}(m)$ and $m= D_{k_d}(C)$. There are two major classes of cryptosystems viz., private-key and public-key. In a private-key cryptosystem, encryption and decryption use the same key, i.e., $k_e= k_d$. But, in a public-key cryptosystem, encryption and decryption use different keys, i.e., for every $k_e\in K$, $\exists$ $k_d\in K'$ and $k_e\neq k_d$.

In symmetric-key cryptosystem, both sender and receiver must agree upon a key before any message is transmitted and key management is a major issue. In public key cryptosystem two keys are involved viz., private-key and public-key. Further, one key is derived from another key and key management is not a issue. Most public-key cryptosystems are based on integer factorization or discrete logarithms [2]. They suffered from major drawback, i.e., to maintain security. For that they must use very large key size which results in decreasing efficiency and large enough quantum computers can be built. To overcome this drawback, Multivariate Public Key Cryptosystem (MKPC) is normally used. MKPC uses multivariate polynomial system over finite field(F_p) which is an NP-complete problem. Several authors have proposed MKPC in which public map *P* or trapdoor one-way function is given as a set of *m* polynomial of a small degree *d* over *n* variables in a finite field F_p. If $d=2$, then it is called Multivariate Quadratic Public-key Cryptosystem (MQPC)[3]. An alternative to MKPC, a multivariate polynomial of

CSEIT1831284 | Received : 16 Feb 2018 | Accepted : 27 Feb 2018 | January-February-2018 [(3) 1 : 1709-1716]

degree *n* is proposed to generate the key in this work which uses Vandermonde Matrix (VM) and Magic Rectangle (MR). Once the multivariate polynomial of degree *n* generated it is converted into single variate polynomial which is used for encryption. The inverse of single variate polynomial is found which is then used for decryption.

The rest of the paper is organized as follows. Section 2 describes the related work. Mathematical background required for the proposed work is discussed in Section 3. Section 4 describes the proposed methodology used in this paper. An example of proposed methodology is discussed in Section 5. Finally, Section 6 ends with conclusion.

II. RELATED WORK

In [4], Lih-Chung Wang et al., have proposed a new encryption scheme namely A Medium Field Multivariate Public-key encryption Scheme (MFE) belonging to MQ and provided a performance and security review. They presented the classical trapdoors central to PKCs like RSA and ElGamal were relatively slow due to modular exponentiation and discrete logarithm respectively and argued that MQ-Schemes based PKC were usually faster and no known assisted attack on them. In [5], Ding et al. proposed a high order linerarization equation attack and resisted HOLE attack on MFE multivariate PKC. Xin Wang[6] et al. have proposed some improved scheme for public-key polynomials of degree four and operated on smaller fields. The security analysis obtained from the proposed scheme proved that it was more security. Yun-Ju Huang [7] studied a new multivariate MQ assumption that could be used to construct public-key encryption schemes. For that they gave two directions viz., asymptotic formulation of MQ problems and provided empirical evidence to confirm the hardness. They proved that the proposed public-key encryption was efficient because only ciphertext length L+poly(K) was needed to encrypt a message M. In [8], Farshid et al. proposed a multivariate key pre-distribution scheme (MKPS), which was based on the category of threshold schemes for WSNs to improve the security in the MKPS. In that, they assigned *d* tuples of nonnegative integers to the sensor nodes as their IDs that were used to distribute the shares of multivariate polynomials. Once the network deployment has been done, nodes with *d-1* common keys were used to shares of polynomials stored in their memories. Rajesh[9] et al. proposed an efficient MKPC based on permutation *p*-polynomials over finite fields. They proved that decryption was much faster than other multivariate public-key cryptosystems and found that complexity encryption in the proposed MPKC was O(n^3) and for decryption it was O(n^2).

III. MATHEMATICAL BACKGROUND

The following mathematical preliminaries are required in performing encryption and decryption used in this paper

3.1 Definition (1-1 function)

A 1-1 function is said to be 1-1 in which no two elements of the domain *A* have the same image. In other words, a function *f* is said to be 1-1 (injective), iff whenever *f(x)=f(y)*, then ***x=y*** **.** For example, f(x) = 3x – 5, f(x)=18x^3+x^2+31x+9 etc., are 1-1 function.

3.2 Definition (Inverse function) Let *f* be a 1-1 function with domain *A* and range *B*. Then its inverse function, denoted as f^{-1}, has domain *B* and range *A* and is defined by $f^{-1}(y) = x$ iff *f(x)=y* for any *y* in *B*, i.e., the inverse of *f*, denoted by f^{-1}, is the unique function with domain equal to the range of *f* that satisfies $f(f^{-1}(x)) = x$, for all *x* in the range of f[10].

For example, (i) if y=f(x) = 3x – 5, then x=f^{-1}(y)=(y+5)/3

(ii) if y=f(x) =18x^3+x^2+31x+9, then

Then x= f^1(y) =	$-\frac{1}{54}\sqrt[3]{27\sqrt{3}\sqrt{8748x^2-147424x+2762219}-4374x+36856}+\frac{1673}{54\sqrt[3]{27\sqrt{3}\sqrt{8748x^2-147424x+2762219}-4374x+36856}}-\frac{1}{54}$

3.3 Definition (Vander monde matrix)

A Vandermonde matrix[11] is sometimes also called an alternant matrix. It is a type of matrix that arises in the polynomial least squares fitting. A Vandermonde matrix[12] of order is of the form

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} & x_1^n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} & x_{n-1}^n \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} & x_n^n \end{bmatrix} \text{ or } \begin{bmatrix} x_0^n & x_0^{n-1} & \dots & x_0^2 & x_0 & 1 \\ x_1^n & x_1^{n-1} & \dots & x_1^2 & x_1 & 1 \\ & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-1}^n & x_{n-1}^{n-1} & \dots & x_{n-1}^2 & x_{n-1} & 1 \\ x_n^n & x_n^{n-1} & \dots & x_n^2 & x_n & 1 \end{bmatrix}$$

Figure 1. Vandermonde Matrix **Figure 2.** Vandermonde Matrix

It is noted that in Vandermonde matrix shown in Figure 1 and Figure 2 are the same. The Vandermonde method can be generalized to interpolate multivariate real-valued function. But, this paper focuses on bivariate polynomials and again converted into univariate polynomial by replacing y as x.

3.4 Definition (Bivariate Polynomial)

A polynomial in two variables with constant coefficients called bivariate polynomial is given by

$$p(x,y)=c_{nm}x^ny^m+\dots+c_{22}x^2y^2+c_{21}x^2y+c_{12}xy^2+c_{11}xy+c_{10}x+c_{01}y+c_{00} \qquad (1)$$

It is noted that if *p(x,y)* has degree *d*, then the number of terms which have exactly degree *d* is *d+1.* It is possible to find one polynomial which has a degree *(d-1)* passes through *d* points. Assuming the (x_i,y_i) where i=1,2,…,n pairs of values are unique. The number of interpolating polynomial must have *n* terms because there are *n* points and the form of interpolating polynomial may be varying. For example, if there are six points, then the interpolating polynomial is $p(x,y)=c_{21}x^2y+c_{12}xy^2+c_{11}xy+c_{10}x+c_{01}y+c_{00}$ [13]. For the sake of convenient, let p(x,y)= $p(x,y)=c_5x^2y+c_4xy^2+c_3xy+c_2x+c_1y+c_0$. Thus, *p(x,y)* has the maximum degree 3 and it covers all maximum 3, 2, 1 and constant term 2,1,2,1 respectively. Table 1 shows the degree of *p(x,y)* and the maximum number of terms for the corresponding degree. Suppose, the total number of terms in *p(x,y)=7* is needed, then from table 1, it is identified that *d(p(x,y))=4* because the total number of terms lie between $6 \le ctt_i \le 9$, and the upper value of ctt_i is taken. The number of term missing in *p(x, y) is* 9-7=2. Thus, *p(x,y)* in this case is

$$p(x,y)= c_{13}xy^3+c_{21}x^2y+c_{12}xy^2+c_{11}xy+c_{10}x+c_{01}y+c_{00} \quad (2)$$

Table 1. Total number of terms upto degree n.

d(p(x,y)) (d_i)	nterm= $nt_i=d_i-1$	tnterm tt_i=nti+3	ctnterm ctt_i
2	1	4	4
3	2	5	6
4	3	6	9
5	4	7	13
…	…	…	…
n	n-1	n+1	$\sum_{i=3}^{n-1}(ctt(i-1)+nti$
n+1	n	n+2	$\sum_{i=3}^{n}(ctt(i-1)+nti$

d-degree of p(x, y); nterm-number of terms in p(x, y) upto d tnterm- total nterm; ctnterm-cumulative tnterm

IV. PROPOSED METHODOLOGY

The proposed methodology consists of 3 steps viz., formation of bivariate p(x,y) using Vandermonde matrix [10] and magic rectangle, performing encryption and decryption.

4.1 Formation of Bivariate p(x,y)

In order to perform encryption, first either magic square of order m denoted as MS_m or magic rectangle of order m×n denoted as $MR_{m\times n}$ is generated based on magic sum of order m and starting number denoted as MSS_m and MRS respectively as proposed in [14]. Once MR is generated, it is converted into square matrix of order *m* denoted as SM_m for the entire matrix of MS or MR by taking modulus *p* where the value of *p* is determined on the basis of type of encoding used in the work. After obtaining SM, select a submatrix of order k×(k-1) denoted as $SSM_{k\times(k-1)}$ starting from SM(1,1) to SM(k,k-1).

Table 2. Rules for Making the SSM'_{kxk+1} to SSM_{kxk+1}

Rule	Description
1	Check the SSM(1,1) in SSM_{kxk-1} is odd or even
2	If SM(1,1) is odd, then make SSM(i, i),i=2,4,…(k-2) as even and SSM(i, i), i=3,5,…,(k-1) as odd. Also SSM(k, k)=1
3	Suppose SSM(i, i) is even then make SSM(i+1, i-1) and SSM(i-1, i+1) as odd, on the other hand if SSM(i, i) is an odd them make SSM(i+1,i-1) and SSM(i-1,i+1) as even

Form a dummy Vandermonde matrix by inserting 1 in kth column of $SSM_{k\times(k-1)}$ and now it becomes $VM'_{k\times k}$. Check $VM'_{k\times k}$ is invertible and gcd(det(VM'_k,p)) is odd. It is noted that in some cases, even if VM'_k is invertible, but det(VM'_k) may be an even number. In that case, modular inverse for VM is not possible. To make it possible, use the rules proposed in Table 2. Once det(VM'_k) becomes an odd number, the resultant is called correct VM and it is now used for generating the bivariate polynomial p(x,y). It is noted that the main difference between the existing Vandermonde interpolation and the proposed SM based VM is that in the existing method first a set of points $x=(x_1,x_2,x_3,\dots,x_n)$ and $y=(y_1,y_2,\dots,y_n)$ are accepted as input. Based on them, a bivariate polynomial p(x,y) is formed, the number of terms say *n* in p(x,y) depends on *(n-1)* number of points taken in *x* and *y* and the last term of p(x,y) is always a constant term. Once p(x,y) is formed, the coefficients of p(x,y) are determined on the basis of systems of linear equations where the RHS of linear equations are obtained by substituting x and y values in p(x,y) in the existing method. But in the proposed methodology, instead of taking the set of values *x* and *y*, the values are taken from SM, i.e., RHS of system of equations are again taken from SM.

The advantage of the proposed scheme is that based on the order of VM matrix, p(x,y) is determined and the sender and receiver need not remember the set of *x* and *y* values. After forming the systems of equations, its matrix representation is VM×C=O where C is a coefficient matrix, VM is Vandermonde matrix and O is a output or RHS matrix with order n×n, n×1 and n×1 respectively, C is found as $C=VM^{-1}\times O$ using matrix inversion method. Once $C=[c_1,c_2,c_3,\dots,c_{n-1},c_n]^T$ is found, it is substituted in p(x,y) and now the p(x,y) contains two variables *x* and *y*. Replace *y* by *x* in p(x,y) and now p(x,y)=f(x) and check f(x) is either 1-1 or not. Suppose, if f(x) is not a 1-1 function, take an another $SSM_{k\times(k-1)}$ from SM and repeat the above process until f(x) is 1-1.

4.2 Perform Encryption

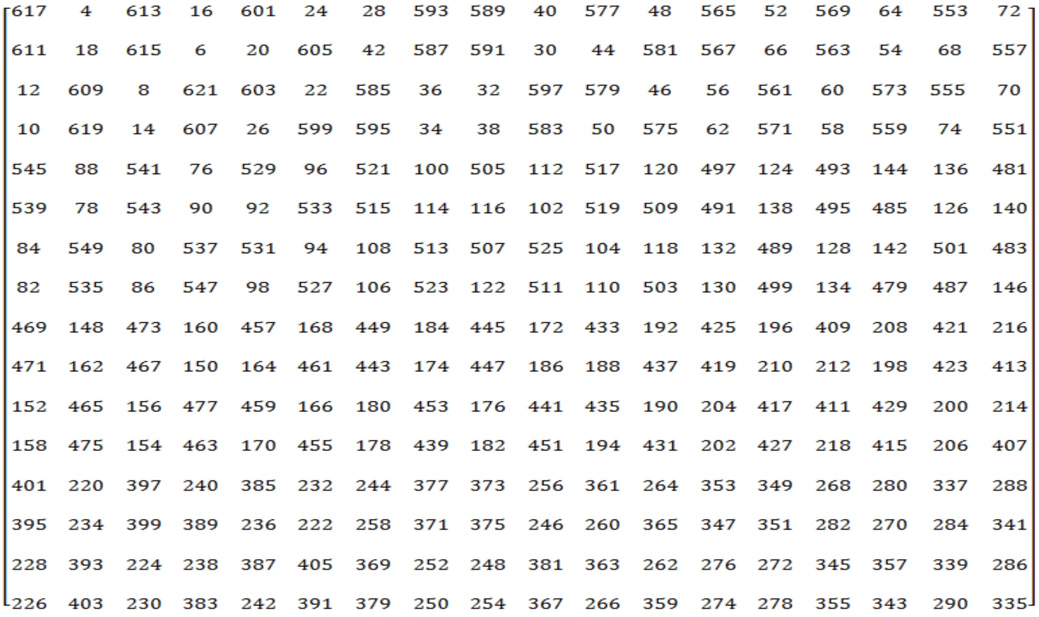
For each $x_i \in M$, find $y_i \in C$, $y_i=p(x_i)$ where x_i and y_i are plaintext and ciphertext respectively.

4.3 Perform Decryption

As c=y=p(x) is 1-1, definitely inverse exist. Find $m=x=p^{-1}(y)$.

V. PROPOSED METHODOLOGY - AN EXAMPLE

To show the relevance of the work, let m=16, MSS_m=5000 and MRS=4. Based on methodology proposed in [14], MR_{16x18} is generated and it is shown in Figure 3.



$$\begin{bmatrix}
617 & 4 & 613 & 16 & 601 & 24 & 28 & 593 & 589 & 40 & 577 & 48 & 565 & 52 & 569 & 64 & 553 & 72 \\
611 & 18 & 615 & 6 & 20 & 605 & 42 & 587 & 591 & 30 & 44 & 581 & 567 & 66 & 563 & 54 & 68 & 557 \\
12 & 609 & 8 & 621 & 603 & 22 & 585 & 36 & 32 & 597 & 579 & 46 & 56 & 561 & 60 & 573 & 555 & 70 \\
10 & 619 & 14 & 607 & 26 & 599 & 595 & 34 & 38 & 583 & 50 & 575 & 62 & 571 & 58 & 559 & 74 & 551 \\
545 & 88 & 541 & 76 & 529 & 96 & 521 & 100 & 505 & 112 & 517 & 120 & 497 & 124 & 493 & 144 & 136 & 481 \\
539 & 78 & 543 & 90 & 92 & 533 & 515 & 114 & 116 & 102 & 519 & 509 & 491 & 138 & 495 & 485 & 126 & 140 \\
84 & 549 & 80 & 537 & 531 & 94 & 108 & 513 & 507 & 525 & 104 & 118 & 132 & 489 & 128 & 142 & 501 & 483 \\
82 & 535 & 86 & 547 & 98 & 527 & 106 & 523 & 122 & 511 & 110 & 503 & 130 & 499 & 134 & 479 & 487 & 146 \\
469 & 148 & 473 & 160 & 457 & 168 & 449 & 184 & 445 & 172 & 433 & 192 & 425 & 196 & 409 & 208 & 421 & 216 \\
471 & 162 & 467 & 150 & 164 & 461 & 443 & 174 & 447 & 186 & 188 & 437 & 419 & 210 & 212 & 198 & 423 & 413 \\
152 & 465 & 156 & 477 & 459 & 166 & 180 & 453 & 176 & 441 & 435 & 190 & 204 & 417 & 411 & 429 & 200 & 214 \\
158 & 475 & 154 & 463 & 170 & 455 & 178 & 439 & 182 & 451 & 194 & 431 & 202 & 427 & 218 & 415 & 206 & 407 \\
401 & 220 & 397 & 240 & 385 & 232 & 244 & 377 & 373 & 256 & 361 & 264 & 353 & 349 & 268 & 280 & 337 & 288 \\
395 & 234 & 399 & 389 & 236 & 222 & 258 & 371 & 375 & 246 & 260 & 365 & 347 & 351 & 282 & 270 & 284 & 341 \\
228 & 393 & 224 & 238 & 387 & 405 & 369 & 252 & 248 & 381 & 363 & 262 & 276 & 272 & 345 & 357 & 339 & 286 \\
226 & 403 & 230 & 383 & 242 & 391 & 379 & 250 & 254 & 367 & 266 & 359 & 274 & 278 & 355 & 343 & 290 & 335
\end{bmatrix}$$

Figure 3. $MR_{16\times 18}$ with MRcsum=5000 and MRrsum=5625

Suppose alphabetical encoding is used, then p=26. After taking modulus, i.e., p=26 for each element of Figure 3 and omitting last two columns, the resultant modulus form of Figure 3 is shown in Figure 4.

$$\begin{bmatrix}
19 & 4 & 15 & 16 & 3 & 24 & 2 & 21 & 17 & 14 & 5 & 22 & 19 & 0 & 23 & 12 & 7 & 20 \\
13 & 18 & 17 & 6 & 20 & 7 & 16 & 15 & 19 & 4 & 18 & 9 & 21 & 14 & 17 & 2 & 16 & 11 \\
12 & 11 & 8 & 23 & 5 & 22 & 13 & 10 & 6 & 25 & 7 & 20 & 4 & 15 & 8 & 1 & 9 & 18 \\
10 & 21 & 14 & 9 & 0 & 1 & 23 & 8 & 12 & 11 & 24 & 3 & 10 & 25 & 6 & 13 & 22 & 5 \\
25 & 10 & 21 & 24 & 9 & 18 & 1 & 22 & 11 & 8 & 23 & 16 & 3 & 20 & 25 & 14 & 6 & 13 \\
19 & 0 & 23 & 12 & 14 & 13 & 21 & 10 & 12 & 24 & 25 & 15 & 23 & 8 & 1 & 17 & 22 & 10 \\
6 & 3 & 2 & 17 & 11 & 16 & 4 & 19 & 13 & 5 & 0 & 14 & 2 & 21 & 24 & 12 & 7 & 15 \\
4 & 15 & 8 & 1 & 20 & 7 & 2 & 3 & 18 & 17 & 6 & 9 & 0 & 5 & 4 & 11 & 19 & 16 \\
1 & 18 & 5 & 4 & 15 & 12 & 7 & 2 & 3 & 16 & 17 & 10 & 9 & 14 & 19 & 0 & 5 & 8 \\
3 & 6 & 25 & 20 & 8 & 19 & 1 & 18 & 5 & 4 & 6 & 21 & 3 & 2 & 4 & 16 & 7 & 23 \\
22 & 23 & 0 & 9 & 17 & 10 & 24 & 11 & 20 & 25 & 19 & 8 & 22 & 1 & 21 & 13 & 18 & 6 \\
2 & 7 & 24 & 21 & 14 & 13 & 22 & 23 & 0 & 9 & 12 & 15 & 20 & 11 & 10 & 25 & 24 & 17 \\
11 & 12 & 7 & 6 & 21 & 24 & 10 & 13 & 9 & 22 & 23 & 4 & 15 & 11 & 8 & 20 & 25 & 2 \\
5 & 0 & 9 & 25 & 2 & 14 & 24 & 7 & 11 & 12 & 0 & 1 & 9 & 13 & 22 & 10 & 24 & 3 \\
20 & 3 & 16 & 23 & 4 & 15 & 5 & 18 & 14 & 17 & 25 & 2 & 16 & 12 & 7 & 19 & 1 & 0 \\
18 & 13 & 22 & 19 & 8 & 1 & 15 & 16 & 20 & 3 & 6 & 21 & 14 & 18 & 17 & 5 & 4 & 23
\end{bmatrix}$$

Figure 4. SM_{16x16} after taking modulus p=26 of $MR_{16\times 18}$

Let a submatrix of order 6×5 denoted as SSM_{6x5} shown in Figure 5 is taken from MR_{16x16} starting from MR(1,1). Fill 1 in sixth column, then the VM' matrix corresponding to SSM_{6x5} is VM'_{6x6} which is shown in Figure 6.

$$\begin{pmatrix} 19 & 4 & 15 & 16 & 3 & 19 \\ 13 & 18 & 17 & 6 & 20 & 13 \\ 12 & 11 & 8 & 23 & 5 & 12 \\ 10 & 21 & 14 & 9 & 0 & 10 \\ 25 & 10 & 21 & 24 & 9 & 25 \\ 19 & 0 & 23 & 12 & 14 & 19 \end{pmatrix}$$

Figure 5. VM'_{6x5}

$$\begin{pmatrix} 19 & 4 & 15 & 16 & 3 & 1 \\ 13 & 18 & 17 & 6 & 20 & 1 \\ 12 & 11 & 8 & 23 & 5 & 1 \\ 10 & 21 & 14 & 9 & 0 & 1 \\ 25 & 10 & 21 & 24 & 9 & 1 \\ 19 & 0 & 23 & 12 & 14 & 1 \end{pmatrix}$$

Figure 6. VM'_{6x6}

$$\begin{pmatrix} 19 & 4 & 15 & 17 & 3 & 1 \\ 13 & 18 & 18 & 6 & 19 & 1 \\ 11 & 11 & 7 & 24 & 5 & 1 \\ 10 & 20 & 13 & 10 & 1 & 1 \\ 25 & 10 & 21 & 24 & 9 & 1 \\ 19 & 0 & 23 & 12 & 14 & 1 \end{pmatrix}$$

Figure 7. VM_{6x6}

Now, $\det(VM'_{6x6})$=-364416 mod 26 =0 and hence inverse is not possible. After applying the proposed rule shown in table 2, VM'_{6x6} becomes VM_{6x6} which is shown Figure 7.

Since the order of VM matrix is 6, and its corresponding bivariate polynomial is $p(x,y)=c_{21}x^2y+c_{12}xy^2+c_{11}xy+c_{10}x+c_{01}y+c_{00}$. For simplicity, let $p(x,y)= c_5x^2y+c_4xy^2+c_3xy+c_2x+c_1y+c_0$. Let the output of VM matrix is also taken from 6th column of SM_{16x16}. Now $C=VM^{-1}×O$ where V is VM Matrix and O is its output matrix.

$$\begin{pmatrix} 9 & 4 & 15 & 17 & 3 & 1 \\ 13 & 18 & 18 & 6 & 19 & 1 \\ 11 & 11 & 7 & 24 & 5 & 1 \\ 10 & 20 & 13 & 10 & 1 & 1 \\ 25 & 10 & 21 & 24 & 9 & 1 \\ 19 & 0 & 23 & 12 & 14 & 1 \end{pmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 24 \\ 7 \\ 22 \\ 1 \\ 18 \\ 13 \end{bmatrix} \qquad \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{pmatrix} 19 & 4 & 15 & 17 & 3 & 1 \\ 13 & 18 & 18 & 6 & 19 & 1 \\ 11 & 11 & 7 & 24 & 5 & 1 \\ 10 & 20 & 13 & 10 & 1 & 1 \\ 25 & 10 & 21 & 24 & 9 & 1 \\ 19 & 0 & 23 & 12 & 14 & 1 \end{pmatrix}^{-1} \begin{bmatrix} 24 \\ 7 \\ 22 \\ 1 \\ 18 \\ 13 \end{bmatrix}$$

$V\,M \times C = O$ $\qquad$ $C = VM^{-1} \times O$

Now, $\det(V^{-1})$= -278217 mod 26=9. Thus modular inverse is possible because gcd(9,26)=1. To find, VM^{-1} mod 26, we have

$$\begin{pmatrix} 56078/278217 & 8464/92739 & -2302/30913 & -25567/278217 & 633/30913 & -40972/278217 \\ -7136/278217 & 1946/92739 & -427/30913 & 6766/27827 & 1207/30913 & -12488/278217 \\ -56102/278217 & -9913/92739 & -160/36913 & 31204/278217 & 1683/30913 & 40930/278217 \\ -10717/92739 & -1730/30913 & 1806/30913 & 1610/92739 & 1483/30913 & 4430/92739 \\ -1700/278217 & 5558/92739 & 782/30913 & -18038/278217 & -111/30913 & -2975/278217 \\ 211492/92739 & 17217/30913 & 14798/30913 & -12449/92739 & -67168/30913 & -845/92739 \end{pmatrix} \bmod 26$$

To find c_i, i=0,2,…,5

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} \begin{pmatrix} 12 & 4 & 14 & 1 & 7 & 14 \\ 10 & 10 & 11 & 8 & 15 & 24 \\ 8 & 11 & 4 & 14 & 7 & 8 \\ 19 & 14 & 14 & 18 & 25 & 14 \\ 4 & 2 & 24 & 8 & 7 & 7 \\ 6 & 21 & 22 & 7 & 10 & 13 \end{pmatrix} \begin{bmatrix} 24 \\ 7 \\ 22 \\ 1 \\ 18 \\ 13 \end{bmatrix} = \begin{bmatrix} 933 \\ 1142 \\ 601 \\ 1541 \\ 863 \\ 1131 \end{bmatrix} \bmod 26 = \begin{bmatrix} 23 \\ 24 \\ 3 \\ 7 \\ 5 \\ 13 \end{bmatrix}$$

This gives result, $c_5=13, c_4=5, c_3=7, c_2=3, c_1=24, c_0=23$ and therefore interpolating polynomial is $p(x,y)= 13x^2y+5xy^2+7xy+3x+24y+23$. To perform encryption, replace y by x in p(x,y), then $f(x)=18x^3+7x^2+27x+23$.
Let the message to be encrypted is M='KANNANBABA'. When alphabet encoding (A=1, B=2, C=3,…,Z=26) is used then x={11,1,14,14,1,14,2,1,2,1}. Table 2 shows the encrypted form of M.

Table 3. Encryption of "KANNANBABA", using $f(x)= 18x^3+7x^2+27x+23$

i	1	2	3	4	5	6	7	8	9	10
$m_i \in M$	K	A	N	N	A	N	B	A	B	A
x_i	11	1	14	14	1	14	2	1	2	1
$y_i=f(x_i)$	25125	75	51165	51165	75	51165	249	75	249	75
y_i mod 26	9	23	23	23	23	23	15	23	15	23
$c_i \in C$	I	W	W	W	W	W	O	W	O	W

Thus the message M="KANNANBABA" is converted into C= "IWWWWWOWOW"
To perform decryption, since p(x) is 1-1, inverse exists and $y=p^{-1}(x)$ is

$$f^{-1}(y)= -\frac{1}{54}\sqrt[3]{27\sqrt{3}\sqrt{8748y^2-342544y+4632275}-4374y+85636}+\frac{1409}{54\sqrt[3]{27\sqrt{3}\sqrt{8748y^2-342544y+4632275}-4374y+85636}}-\frac{7}{54}$$

The decryption process is shown in Table 4.

Table 4. Decryption of "IWWWWWOWOW", using $x= f^{-1}(y)$

i	1	2	3	4	5	6	7	8	9	10
$c_i \in C$	I	W	W	W	W	W	O	W	O	W
y_i	25125	75	51165	51165	75	51165	249	75	249	75
$x_i=f^{-1}(y_i)$	11	1	14	14	1	14	2	1	2	1
$m_i \in M$	K	A	N	N	A	N	B	A	B	A

VI. CONCLUSION

An alternative to MKPC has been proposed without using existing standard PKC available in the existing literature. The proposed method uses MR and VM matrix to generate a multivariate polynomial which was then converted into univariate polynomial. This univariate polynomial is used to perform encryption and its inverse was used for decryption. The proposed schemes may provide more security because the degree of multivariate polynomial is only known to sender and receiver. Further, MR is used to generate the Vandermonte matrix but the numbers in the MR are generated only based on order of matrix, magic sum and seed number where these three values are only known to sender and receiver. As the entire key generation is based on multivariate polynomial which is based on VM matrix and its output is again taken from MR, the eavesdropper cannot easily be cracked the original message which results in enhancing the security. The idea used in this paper is unique and innovative.

VII. REFERENCES

[1]. Introduction to Cryptography: Principles and Applications, Book by Hans Delfs and Helmut Knebl, Springer, third edition, 2002.

[2]. A.J. Menezes, P.C. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Ration, Florida, USA, 1997.

[3]. Multivariate Cryptography precision.moscito.org / by-publication /recent/00421-multivariate.pdf.

[4]. Lih-Chung Wang, Bo-Yin Yang, Yu-Hua Hu, and Feipei Lai "A Medium-Field Multivariate Public-Key Encryption Scheme", 2015.

[5]. Ding, J., Hu, L. High order linearization equation (hole) attack on multivariate public key cryptosystems, Lecture Notes in Computer Science, 4450: 233–248, 2007.

[6]. Xin Wang , Feng Feng, Xinmei Wang, Qi Wang, "A More Secure MFE Multivariate Public Key Encryption Scheme", International Journal of Computer Science and Applications Technomathematics Research Foundation Vol. 6, No. 3, pp. 1-9 , 2009.

[7]. Yun-Ju Huang, Feng-Hao Liu, Bo-Yin Yang, "Public-Key Cryptography from New Multivariate Quadratic Assumptions", May 15, 2012.

[8]. Farshid Delgosha, Erman Ayday, Faramarz Fekri , MKPS: A Multivariate Polynomial Scheme for Symmetric Key-Establishment in Distributed Sensor Networks.

[9]. Rajesh P. Singh, B. K. Sarma, A. Saikia, "Public key cryptography using Permutation P-Polynomials over Finite Fields".

[10]. Jean-Paul Tremblay, R. Manohar "Discrete Mathematical Structures with Applications to Computer Science", February 2nd 2001 , McGraw Hill Education.

[11]. Douglas Wilhelm Harder The Vandermonde Method, University of Waterloo, Onrario,Canada N2L 3GI, https://ece.uwaterloo.ca/~dwharder/Numerical Analysis/05 Interpolation/Vandermonde.

[12]. Wikipedia Vandermonde Matrix, https://en.wikipedia.org/wikiVander monde_matrix.

[13]. Ruma Kareem Ajeena, Hailiza Kamarulhaili and Sattar B. Almaliky, "Bivariate Polynomials Public Key Encryption Schemes" , International Journal of Cryptology Research 4(1): 73 – 83, 2013.

[14]. Mani. K, Viswambari. M, "Enhancing the Security in Cryptosystems Based on Magic Rectangle", International Journal of Computer Network and Information Security (IJCNIS), Vol. 9, No.4, 2017.