International Journal of Cryptology Research 11(2): 31 - 48 (2021)

An Empirical Attack on a Polynomial Reconstruction Problem Potential Cryptosystem

Siti Nabilah Yusof*[1] and **Muhammad Rezal Kamel Ariffin**[1]

[1] *Institute for Mathematical Research, Universiti Putra Malaysia, 43400, UPM Serdang, Selangor, Malaysia*

E-mail: sitinabilahyusof@gmail.com
**Corresponding author*

ABSTRACT

In this paper, we put forward an empirical strategy to show that the Polynomial Reconstruction Problem (PRP) cryptosystem by Ajeena et al. in 2013 is not secure. Our numerical strategy was able to reproduce the secret parameter α from the ciphertext. By obtaining this secret parameter α, the security of the ciphertext given by $CT = \mu + \alpha \times PK + e$ is now just reduced to $CT - \alpha \times PK = \mu + e$. Since e is an error vector with a particular Hamming weight, the error vector has many 0 vectors which might result in the equation $CT = \mu + \alpha \times PK + e$ to be vulnerable and potentially allowing an adversary to obtain the exact message, μ.

Keywords: Polynomial Reconstruction Problem, Post-Quantum Cryptography, Bivariate polynomial

1 INTRODUCTION

A good hard mathematical problem is need for a cryptosystem to be secured from any attack. As the technology evolved, the hard mathematical problem is evolving into a secured system from the attack of quantum computer. Shor's algorithm was delevoped in 1994 where this algo can solved Integer Factorization Problem (IFP) and Discrete Logarithm Problem (DLP) in polynomial time (Shor, 1994). The National Institute of Standards and Technology (NIST) had made a call for quantum resistant algorithm (Song and Zhao, 2017).

From the website Quantum Zoo Algorithm, there are many lists of good hard mathematical problem that are believed to be quantum resistant (Jordan, 2011). Post quantum cryptography objective is to creates schemes that can be safe from the attack of quantum computer (Gaborit et al., 2018). Hence, it is necessary for cryptographers to study new hard mathematical problem in order to establish a system that are quantum resistant (Imran et al., 2020). Besides that, cryptographers are also need to assure the security of cryptographic scheme by evaluating time complexity and memory needed for the attack (Kuwakado and Morii, 2010).

The PRP is one of the listed problem in (Jordan, 2011). The PRP was introduced in 1999 as a new hard mathematical problem for cryptographic design (Augot et al., 2003). When compared to the Reed-Solomon error correcting codes, the PRP has some similarity related to its formulation (Naor and Pinkas, 1999, Reed and Solomon, 1960). The reasons why PRP is highly suggested as a hard mathematical problem are because of evidence that PRP is quantum computer resistant and PRP has the advantages related to efficiency and effectiveness (Kiayias and Yung, 2004b).

The PRP can be solved in polynomial time if the weight of error,w is small such that $w \leq \frac{n-k}{w}$ where n is the number of element and k is the degree of the polynomial. This has been improved to $w \leq n - \sqrt{kn}$ (Venkatesan Guruswami, 1999). A cryptosystem based on PRP has been proposed in 2003 by Augot and Finiasz where we denote the cryptosystem as the AF-Cryptosystem (Augot and Finiasz, 2003). This cryptosystem utilized two types of PRP which are the first PRP concerns the definition in (Jordan, 2011) and the second PRP is a specially established PRP to assure decryption. We denote the second PRP as the Augot and Finiasz Solvable PRP (AF-SPRP) which define as follows,

Definition 1.1. ***(Augot and Finiasz Solvable PRP)*** *Given n, k, t and $(x_i, y_i)_{i=1,\cdots,n}$, output any polynomial p such that $deg < k$ and $p(x_i) = y_i$ for at least t values of i where $t = n - w$.*

The AF-Cryptosystem utilizes univariate polynomial (Kiayias and Yung, 2001, 2004a). The PRP based on Definition 1.1 is to ensure that decryption process can be done. That is, when one is given t points on a Cartesian plane, one needs to output a polynomial that fits all the points where t is the number of elements equal to zero in a vector. Lagrange interpolation is used in order to complete the decryption process.

The AF-Cryptosystem has been attacked by Coron where the plaintext managed to be retrieved in polynomial time (Coron, 2004). Next, Ajeena et al. proposed a modified AF-Cryptosystem where bivariate PRP and Vandermonde matrix are utilized in this system (Ajeena et al., 2013). We denote this modified cryptosystem as AAK-Cryptosystem. The designers for AAK-Cryptosystem assured that by increasing the number of variables can increase the security level against any attack.

Our contribution. This paper demonstrates a numerical example upon the AAK-Cryptosystem which we managed to obtain secret key, α. The motivation for this research is from the cryptanalysis done upon the AF-Cryptosystem by Coron. We use Berlekamp Welch algorithm and created a modified Coron cryptanalysis strategy and prove that we can construct a list of possible candidates of the AAK-Cryptosystem secret key, α.

The outline of this paper is shown as follows. In Section 2, we describe fundamental knowledge about PRP as well as Vandermonde method and outline AAK-Cryptosystem. In Section 3, we describe our numerical example on the AAK-Cryptosystem. Finally, we conclude in Section 4.

2 THE ATTACK

In this section, we show a numerical illustration on how we obtain secret key, α from (Ajeena et al., 2013) and also provide our own independent example following the AAK-Cryptosystem.

2.1 Cryptanalysis of AAK-Cryptosystem

This section presents a numerical illustration of how to obtain secret key, α from the example in (Ajeena et al., 2013). Given $n = 10$, $k = 3$, $w = 1$ and $W = 3$ in $\mathbb{F}_{11}$. Let $x = (2, 3, 3, 4, 5, 6, 7, 8, 9, 10)$ and $y = (4, 3, 6, 2, 1, 5, 7, 8, 9, 10)$. Let private polynomial,

$$p(x, y) = x^2y + xy^2 + 3xy + 5$$

and *E* be the big error vector,

$$E = (0, 0, 0, 10, 0, 7, 3, 0, 0, 0).$$

The public key is:

$$PK = C + E$$

where $C = ev(p(x, y))$. We compute C as follows:

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

Hence,

$$\begin{aligned} PK &= C + E \\ &= (0, 9, 1, 0, 6, 7, 2, 0, 1, 6) + (0, 0, 0, 10, 0, 7, 3, 0, 0, 0) \\ &= (0, 9, 1, 10, 6, 3, 5, 0, 1, 6). \end{aligned}$$

A message polynomial $\mu(x, y) = xy + 2x + 4y + 3$ is encoded into codeword μ which we know that $\mu = ev(\mu(x, y))$ then,

$$\mu(2,4) = 9,\ \mu(3,3) = 8,\ \mu(3,6) = 7,\ \mu(4,2) = 5,\ \mu(5,1) = 0$$

$$\mu(6,5) = 10,\ \mu(7,7) = 6,\ \mu(8,8) = 5,\ \mu(9,9) = 6,\ \mu(10,10) = 9.$$

Therefore, we have

$$\mu = (9, 8, 7, 5, 0, 10, 6, 5, 6, 9). \tag{1}$$

A private constant $\alpha = 3 \in \mathbb{F}_{11}$ and small error vector, e are chosed where

$$e = (0, 0, 0, 0, 0, 7, 0, 0, 0, 0) \tag{2}$$

with the weight of $w = 1$. The ciphertext *CT* is:

$$\begin{aligned}CT &= \mu + \alpha \times PK + e\\ &= (9, 8, 7, 5, 0, 10, 6, 5, 6, 9) + 3 \times (0, 9, 1, 10, 6, 3, 5, 0, 1, 6) + (0, 0, 0, 0, 0, 7, 0, 0, 0, 0)\\ &= (9, 8, 7, 5, 0, 10, 6, 5, 6, 9) + (0, 5, 3, 8, 7, 9, 4, 0, 3, 7) + (0, 0, 0, 0, 0, 7, 0, 0, 0, 0)\\ &= (9, 2, 10, 2, 7, 4, 10, 5, 9, 5).\end{aligned}$$

We now continue to attack the ciphertext, CT. Let $M(\lambda)$ be the matrix of the system:

1. $M(\lambda)_{i,a,b} = (CT_i - \lambda \cdot PK_i) \cdot (x_i)^a \cdot (y_i)^b$
2. $M(\lambda)_{i,a,b} = -(x_i)^a \cdot (y_i)^b$

where $i \in \{1, \dots, 10\}$, $a \in \{0, 1, 2\}$ and $b \in \{0, 1, 2\}$ for (1) and (2). For the first half column of matrix $M(\lambda)$ we use (1). Hence, when $i = 1$, $a = 0$ and $b = 0$ then,

$$\begin{aligned} M(\lambda)_{1,0,0} &= (CT_1 - \lambda \cdot PK_1) \cdot (x_1)^0 \cdot (y_1)^0 \\ &= 9 - \lambda \cdot 0 \\ &= 9. \end{aligned}$$

When $i = 5$, $a = 1$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{5,1,1} &= (CT_5 - \lambda \cdot PK_5) \cdot (x_5)^1 \cdot (y_5)^1 \\ &= (7 - \lambda \cdot 6) \cdot 5 \cdot 1 \\ &= 2 - 8\lambda. \end{aligned}$$

When $i = 5$, $a = 2$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{5,2,1} &= (CT_5 - \lambda \cdot PK_5) \cdot (x_5)^2 \cdot (y_5)^1 \\ &= (7 - \lambda \cdot 6) \cdot 5^2 \cdot 1^1 \\ &= 10 - 7\lambda. \end{aligned}$$

For the second half column of matrix $M(\lambda)$ we use (2). When $i = 2$, $a = 2$ and $b = 2$ then,

$$\begin{aligned} M(\lambda)_{2,2,2} &= -(x_2)^2 \cdot (y_2)^2 \\ &= -(3^2) \cdot (3^2) \\ &= 7. \end{aligned}$$

When $i = 2$, $a = 2$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{2,1,1} &= -(x_2)^2 \cdot (y_2)^1 \\ &= -(3^2) \cdot (3^1) \\ &= 6. \end{aligned}$$

When all the entries in $M(\lambda)$ have been calculated then see Appendix A. From Appendix A, we can see that the dimension for $M(\lambda)$ is 10×18. Next, consider $M(\lambda)$ with $\lambda = 0$ and apply Gaussian elimination to calculate the rank of matrix $M(0)$. The rank for matrix $M(0)$ is 10, which the rank is equal to number of rows in matrix $M(\lambda)$ therefore we take column 9 until 18 to be a sub-square matrix for $M(\lambda)$. Then, the sub-square matrix denoted by $M'(\lambda)$ is a matrix with dimension 10×10 as follows:

$$M'(\lambda) = \begin{bmatrix} 4 & 10 & 7 & 6 & 9 & 3 & 1 & 7 & 6 & 2 \\ 8-3\lambda & 10 & 8 & 2 & 8 & 2 & 6 & 2 & 6 & 7 \\ 6-5\lambda & 10 & 5 & 8 & 8 & 4 & 2 & 2 & 1 & 6 \\ 7-2\lambda & 10 & 9 & 7 & 7 & 3 & 6 & 6 & 1 & 2 \\ 10-7\lambda & 10 & 10 & 10 & 6 & 6 & 6 & 8 & 8 & 8 \\ 3-5\lambda & 10 & 6 & 8 & 5 & 3 & 4 & 8 & 7 & 2 \\ 8-4\lambda & 10 & 4 & 6 & 4 & 6 & 9 & 6 & 9 & 8 \\ 9 & 10 & 3 & 2 & 3 & 2 & 5 & 2 & 5 & 7 \\ 1-5\lambda & 10 & 2 & 7 & 2 & 7 & 8 & 7 & 8 & 6 \\ 5-6\lambda & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{bmatrix}.$$

Next, we need to find determinant $f(\lambda)$,

$$f(\lambda) = \text{det}\ (M'(\lambda)) = 74877540\lambda - 42937040.$$

The highest degree for polynomial $f(\lambda)$ is 1. This coincides with the fact that $M'(\lambda)$ has 1 columns that contain λ. Upon factoring $f(\lambda)$ modulo $q = 11$ we obtain the following:

$$f(\lambda) = \lambda - 3.$$

We take $\lambda = 3$ as the secret key where $M'(3)$ is indeed a non-invertible matrix. To see this fact, we calculate the nullspace of $M'(3)$, which is the column matrix Y. The column matrix Y is given by:

$$Y = \begin{bmatrix} 9 \\ 1 \\ 4 \\ 0 \\ 5 \\ 5 \\ 3 \\ 7 \\ 9 \\ 1 \end{bmatrix}.$$

Observe that $M'(3) \cdot Y = 0$.

Remark 2.1. *Observe that*

$$\begin{aligned} CT - 3 \times PK &= (9,8,7,5,0,6,6,5,6,9) \\ &= (9,8,7,5,0,10,6,5,6,9) + (0,0,0,0,0,7,0,0,0,0,0). \end{aligned}$$

Since the error vector has many zeros according to the prescribed Hamming weight, the vector $(9,8,7,5,0,6,6,5,6,9)$ *leaks information on the message,* μ*. As such, the AAK-Cryptosystem is not secure.*

2.2 Independent Example

This section provides another numerical illustration on how to obtain secret key, α based on an example that we generated independently from AAK-Cryptosystem algorithm. Given $n = 10$, $k = 3$, $w = 1$ and $W = 3$ in $\mathbb{F}_{11}$. Let $x = (5,4,3,2,1,10,9,8,7,6)$ and $y = (2,4,6,8,10,1,3,5,7,9)$. Let private polynomial,

$$p(x,y) = x^2y + xy^2 + 2xy + 3x + 4y + 5$$

and *E* be the big error vector,

$$E = (1,2,3,0,0,0,0,0,0,0).$$

The public key is:

$$PK = C + E$$

where $C = ev(p(x,y))$. We compute C as follows:

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

Therefore,

$$\begin{aligned} PK &= C + E \\ &= (8,6,5,4,2,4,4,0,2,9) + (1,2,3,0,0,0,0,0,0,0) \\ &= (9,8,8,4,2,4,4,0,2,9). \end{aligned}$$

A message polynomial $\mu(x,y) = xy + 3x + 9y + 6$ is encoded into codeword μ which we know that $\mu = ev(\mu(x,y))$ then,

$$\mu(5,2) = 5,\ \mu(4,4) = 4,\ \mu(3,6) = 10,\ \mu(2,8) = 1,\ \mu(1,10) = 10$$

$$\mu(10,1) = 0,\ \mu(9,3) = 10,\ \mu(8,5) = 5,\ \mu(7,7) = 7,\ \mu(6,9) = 5.$$

Therefore, we have

$$\mu = (5,4,10,1,10,0,10,5,7,5). \tag{3}$$

A constant $\alpha = 2 \in \mathbb{F}_{11}$ which is a private key and small error vector, e are chosed where

$$e = (5,0,0,0,0,0,0,0,0,0) \tag{4}$$

with the weight of $w = 1$. The ciphertext *CT* is:

$$\begin{aligned}
CT &= \mu + \alpha \times PK + e \\
&= (5,4,10,1,10,0,10,5,7,5) + 2 \times (9,8,8,4,2,4,4,0,2,9) + (5,0,0,0,0,0,0,0,0,0) \\
&= (5,4,10,1,10,0,10,5,7,5) + (7,5,5,8,4,8,8,0,4,7) + (5,0,0,0,0,0,0,0,0,0) \\
&= (6,9,4,9,3,8,7,5,0,1).
\end{aligned}$$

We now continue to attack the ciphertext, CT. Let $M(\lambda)$ be the matrix of the system:

1. $M(\lambda)_{i,a,b} = (CT_i - \lambda \cdot PK_i) \cdot (x_i)^a \cdot (y_i)^b$
2. $M(\lambda)_{i,a,b} = -(x_i)^a \cdot (y_i)^b$

where $i \in \{1, \ldots, 10\}$, $a \in \{0, 1, 2\}$ and $b \in \{0, 1, 2\}$ for (1) and (2). We use (1) for the first half column of matrix $M(\lambda)$. Hence, when $i = 1$, $a = 0$ and $b = 0$ then,

$$\begin{aligned} M(\lambda)_{1,0,0} &= (CT_1 - \lambda \cdot PK_1) \cdot (x_1)^0 \cdot (y_1)^0 \\ &= 6 - \lambda \cdot 9 \\ &= 6 - 9\lambda. \end{aligned}$$

When $i = 5$, $a = 1$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{5,1,1} &= (CT_5 - \lambda \cdot PK_5) \cdot (x_5)^1 \cdot (y_5)^1 \\ &= (3 - \lambda \cdot 2) \cdot 1 \cdot 10 \\ &= 8 - 9\lambda. \end{aligned}$$

When $i = 5$, $a = 2$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{5,2,1} &= (CT_5 - \lambda \cdot PK_5) \cdot (x_5)^2 \cdot (y_5)^1 \\ &= (3 - \lambda \cdot 2) \cdot 1^2 \cdot 10^1 \\ &= 8 - 9\lambda. \end{aligned}$$

Next, we use (2) for the second half column of matrix $M(\lambda)$. When $i = 2$, $a = 2$ and $b = 2$ then,

$$\begin{aligned} M(\lambda)_{2,2,2} &= -(x_2)^2 \cdot (y_2)^2 \\ &= -(4^2) \cdot (4^2) \\ &= 8. \end{aligned}$$

When $i = 2$, $a = 2$ and $b = 1$ then,

$$\begin{aligned} M(\lambda)_{2,1,1} &= -(x_2)^2 \cdot (y_2)^1 \\ &= -(4^2) \cdot (4^1) \\ &= 2. \end{aligned}$$

After finishing calculating all the entries in $M(\lambda)$ then see Appendix B where we can see that the dimension for $M(\lambda)$ is 10×18. Next, by considering $M(\lambda)$ with $\lambda = 0$ and Gaussian elimination is applied to calculate the rank of matrix $M(0)$. The rank for matrix $M(0)$ is 10, which the rank is equal to number of rows in matrix $M(\lambda)$ therefore we take column 9 until 18 to be a sub-square matrix for $M(\lambda)$. Then, the sub-square matrix denoted by $M'(\lambda)$ is a matrix with dimension 10×10 as follows:

$$M'(\lambda) = \begin{bmatrix} 2-3\lambda & 8-\lambda & 5-2\lambda & 10-4\lambda & 7-5\lambda & 3-10\lambda & 6-9\lambda & 10 & 9 & 7 \\ 1-7\lambda & 3-10\lambda & 1-7\lambda & 4-6\lambda & 1-7\lambda & 4-6\lambda & 5-2\lambda & 10 & 7 & 6 \\ 1-2\lambda & 1-2\lambda & 6-\lambda & 3-6\lambda & 3-6\lambda & 7-3\lambda & 9-7\lambda & 10 & 5 & 8 \\ 4-3\lambda & 7-8\lambda & 1-9\lambda & 8-6\lambda & 3-5\lambda & 2-7\lambda & 5-\lambda & 10 & 3 & 2 \\ 3-2\lambda & 3-2\lambda & 8-9\lambda & 3-2\lambda & 3-2\lambda & 8-9\lambda & 3-2\lambda & 10 & 1 & 10 \\ 8-4\lambda & 3-7\lambda & 3-7\lambda & 3-7\lambda & 8-4\lambda & 8-4\lambda & 8-4\lambda & 10 & 10 & 10 \\ 8-3\lambda & 8-3\lambda & 2-9\lambda & 6-5\lambda & 6-5\lambda & 7-4\lambda & 10-\lambda & 10 & 8 & 2 \\ 4 & 7 & 2 & 10 & 1 & 5 & 3 & 10 & 6 & 8 \\ -10\lambda & -3\lambda & -10\lambda & -4\lambda & -10\lambda & -4\lambda & -6\lambda & 10 & 4 & 6 \\ 4-3\lambda & 6-10\lambda & 10-2\lambda & 2-7\lambda & 3-5\lambda & 5-\lambda & 1-9\lambda & 10 & 2 & 7 \end{bmatrix}.$$

Next, determine determinant $f(\lambda)$ where,

$$\begin{aligned} f(\lambda) &= \text{det}\ (M'(\lambda)) \\ &= 11120000\lambda^7 - 26304000\lambda^6 - 456701360\lambda^5 - 1567046420\lambda^4 \\ &\quad - 287411880\lambda^3 + 501086980\lambda^2 - 274221820\lambda + 7042420. \end{aligned}$$

The highest degree for polynomial $f(\lambda)$ is 7. This coincides with the fact that $M'(\lambda)$ has 7 columns that contain λ. Upon factoring $f(\lambda)$ modulo $q = 11$ we obtain the following:

$$f(\lambda) = \lambda(\lambda - 2)(\lambda - 3)(\lambda^4 + 8\lambda^3 + 7\lambda^2 + 4\lambda + 3).$$

We take $\lambda = 2$ as the secret key where $M'(2)$ is indeed a non-invertible matrix. To see this fact, we calculate the nullspace of $M'(2)$, which is the column matrix Y. The column matrix Y is given by:

$$Y = \begin{bmatrix} 3 \\ 3 \\ 8 \\ 4 \\ 10 \\ 9 \\ 7 \\ 5 \\ 5 \\ 1 \end{bmatrix}.$$

Observe that $M'(2) \cdot Y = 0$.

Next, we take $\lambda = 3$ as the secret key where $M'(3)$ is indeed a non-invertible matrix. To see this fact, we calculate the nullspace of $M'(3)$, which is the column matrix Y. The column matrix Y is given by:

$$Y = \begin{bmatrix} 10 \\ 7 \\ 1 \\ 2 \\ 0 \\ 6 \\ 9 \\ 9 \\ 7 \\ 1 \end{bmatrix}.$$

Observe that $M'(3) \cdot Y = 0$.

Remark 2.2. *Observe that*

$$CT - 2 \times PK = (10, 4, 10, 1, 10, 0, 10, 5, 7, 5)$$

and

$$CT - 3 \times PK = (1, 7, 2, 8, 5, 7, 6, 5, 5, 7)$$

In this case, there are 2 vectors to choose from by the adversary. But, this is trivial. This is because, the AAK-Cryptosystem is an asymmetric encryption and in general transports the symmetric key for the symmetric encryption. The adversary can test both cases, and the case where he manages to obtain meaningful information from the ciphertext encrypted by the symmetric encryption, will indicate he has utilized the correct vector. As such, the AAK-Cryptosystem is not secure.

3 CONCLUSION

In this paper, we present a cryptanalysis on AAK-Cryptosystem as outlined in (Ajeena et al., 2013) as well as a cryptanalysis on our own example where the attack is resourced from strategies found in (Coron, 2004). In the end, we are able to provide empirical evidence that we can obtain a list of possible values of the secret key, α. Therefore, AAK-Cryptosystem is not safe to be used.

ACKNOWLEDGMENTS

The research was supported by Ministry of Education of Malaysia with Fundamental Research Grant Scheme (FRGS/1/2019/STG06/UPM/02/8).

A THE FULL MATRIX $M(\lambda)$ FOR NUMERICAL ILLUSTRATION OF CRYPTANALYSIS ON AAK-CRYPTOSYSTEM IN (AJEENA ET AL., 2013)

$$M(\lambda) = \begin{bmatrix} 9 & 3 & 1 & 7 & 6 & 2 & 3 & 1 & 4 & 10 & 7 & 6 & 9 & 3 & 1 & 7 & 6 & 2 \\ 2-9\lambda & 6-5\lambda & 7-4\lambda & 6-5\lambda & 7-4\lambda & 10-\lambda & 7-4\lambda & 10-\lambda & 8-3\lambda & 10 & 8 & 2 & 8 & 2 & 6 & 2 & 6 & 7 \\ 10-\lambda & 5-6\lambda & 8-3\lambda & 8-3\lambda & 4-7\lambda & 2-9\lambda & 2-9\lambda & 1-10\lambda & 6-5\lambda & 10 & 5 & 8 & 8 & 4 & 2 & 2 & 1 & 6 \\ 2-10\lambda & 4-9\lambda & 8-7\lambda & 8-7\lambda & 5-3\lambda & 10-6\lambda & 10-6\lambda & 9-\lambda & 7-2\lambda & 10 & 9 & 7 & 7 & 3 & 6 & 6 & 1 & 2 \\ 7-6\lambda & 7-6\lambda & 7-6\lambda & 2-8\lambda & 2-8\lambda & 2-8\lambda & 10-7\lambda & 10-7\lambda & 10-7\lambda & 10 & 10 & 10 & 6 & 6 & 6 & 8 & 8 & 8 \\ 4-3\lambda & 9-4\lambda & 1-9\lambda & 2-7\lambda & 10-2\lambda & 6-10\lambda & 1-9\lambda & 5-\lambda & 3-5\lambda & 10 & 6 & 8 & 5 & 3 & 4 & 8 & 7 & 2 \\ 10-5\lambda & 4-2\lambda & 6-3\lambda & 4-2\lambda & 6-3\lambda & 9-10\lambda & 6-3\lambda & 9-10\lambda & 8-4\lambda & 10 & 4 & 6 & 4 & 6 & 9 & 6 & 9 & 8 \\ 5 & 7 & 1 & 7 & 1 & 8 & 1 & 8 & 9 & 10 & 3 & 2 & 3 & 2 & 5 & 2 & 5 & 7 \\ 9-\lambda & 4-9\lambda & 3-4\lambda & 4-9\lambda & 3-4\lambda & 5-3\lambda & 3-4\lambda & 5-3\lambda & 1-5\lambda & 10 & 2 & 7 & 2 & 7 & 8 & 7 & 8 & 6 \\ 5-6\lambda & 6-5\lambda & 5-6\lambda & 6-5\lambda & 5-6\lambda & 6-5\lambda & 5-6\lambda & 6-5\lambda & 5-6\lambda & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{bmatrix}.$$

B THE FULL MATRIX $M(\lambda)$ FOR NUMERICAL ILLUSTRATION OF OUR INDEPENDENT EXAMPLE

$$M(\lambda) = \begin{bmatrix}
6-9\lambda & 1-7\lambda & 2-3\lambda & 8-\lambda & 5-2\lambda & 10-4\lambda & 7-5\lambda & 3-10\lambda & 6-9\lambda & 10 & 9 & 7 & 6 & 1 & 2 & 8 & 5 & 10 \\
9-8\lambda & 3-10\lambda & 1-7\lambda & 3-10\lambda & 1-7\lambda & 4-6\lambda & 1-7\lambda & 4-6\lambda & 5-2\lambda & 10 & 7 & 6 & 7 & 6 & 2 & 6 & 2 & 8 \\
4-8\lambda & 2-4\lambda & 1-2\lambda & 1-2\lambda & 6-\lambda & 3-6\lambda & 3-6\lambda & 7-3\lambda & 9-7\lambda & 10 & 5 & 8 & 8 & 4 & 2 & 2 & 1 & 6 \\
9-4\lambda & 6-10\lambda & 4-3\lambda & 7-8\lambda & 1-9\lambda & 8-6\lambda & 3-5\lambda & 2-7\lambda & 5-\lambda & 10 & 3 & 2 & 9 & 6 & 4 & 7 & 1 & 8 \\
3-2\lambda & 8-9\lambda & 3-2\lambda & 3-2\lambda & 8-9\lambda & 3-2\lambda & 3-2\lambda & 8-9\lambda & 3-2\lambda & 10 & 1 & 10 & 10 & 1 & 10 & 10 & 1 & 10 \\
8-4\lambda & 8-4\lambda & 8-4\lambda & 3-7\lambda & 3-7\lambda & 3-7\lambda & 8-4\lambda & 8-4\lambda & 8-4\lambda & 10 & 10 & 10 & 1 & 1 & 1 & 10 & 10 & 10 \\
7-4\lambda & 10-\lambda & 8-3\lambda & 8-3\lambda & 2-9\lambda & 6-5\lambda & 6-5\lambda & 7-4\lambda & 10-\lambda & 10 & 8 & 2 & 2 & 6 & 7 & 7 & 10 & 8 \\
5 & 3 & 4 & 7 & 2 & 10 & 1 & 5 & 3 & 10 & 6 & 8 & 3 & 4 & 9 & 2 & 10 & 6 \\
-4\lambda & -6\lambda & -9\lambda & -6\lambda & -9\lambda & -8\lambda & -9\lambda & -8\lambda & -\lambda & 10 & 4 & 6 & 4 & 6 & 9 & 6 & 9 & 8 \\
1-9\lambda & 9-4\lambda & 4-3\lambda & 6-10\lambda & 10-2\lambda & 2-7\lambda & 3-5\lambda & 5-\lambda & 1-9\lambda & 10 & 2 & 7 & 5 & 1 & 9 & 8 & 6 & 10
\end{bmatrix}.$$

REFERENCES

Ajeena, R. K., Kamarulhaili, H., and Almaliky, S. B. (2013). Bivariate polynomials public key encryption schemes. *International Journal of Cryptology Research*, 4(1):73–83.

Augot, D. and Finiasz, M. (2003). A public key encryption scheme based on the polynomial reconstruction problem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 229–240. Springer.

Augot, D., Finiasz, M., and Loidreau, P. (2003). Using the trace operator to repair the polynomial reconstruction based cryptosystem presented at eurocrypt 2003. *Cryptology ePrint Archive*.

Coron, J.-S. (2004). Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem. In *International Workshop on Public Key Cryptography*, pages 14–27. Springer.

Gaborit, P., Otmani, A., and Kalachi, H. T. (2018). Polynomial-time key recovery attack on the faure–loidreau scheme based on gabidulin codes. *Designs, Codes and Cryptography*, 86(7):1391–1403.

Imran, M., Abideen, Z. U., and Pagliarini, S. (2020). An experimental study of building blocks of lattice-based nist post-quantum cryptographic algorithms. *Electronics*, 9(11):1953.

Jordan, S. (2011). `https://quantumalgorithmzoo.org/`.

Kiayias, A. and Yung, M. (2001). Polynomial reconstruction based cryptography. In *International Workshop on Selected Areas in Cryptography*, pages 129–133. Springer.

Kiayias, A. and Yung, M. (2004a). Cryptanalyzing the polynomial-reconstruction based public-key system under optimal parameter choice. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 401–416. Springer.

Kiayias, A. and Yung, M. (2004b). Directions in polynomial reconstruction based cryptography. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 87(5):978–985.

Kuwakado, H. and Morii, M. (2010). Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *2010 IEEE International Symposium on Information Theory*, pages 2682–2685. IEEE.

Naor, M. and Pinkas, B. (1999). Oblivious transfer and polynomial evaluation. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 245–254.

Reed, I. S. and Solomon, G. (1960). Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee.

Song, B. and Zhao, Y. (2017). Provably secure identity-based identification and signature schemes from code assumptions. *Plos one*, 12(8):e0182894.

Venkatesan Guruswami, M. S. (1999). Improved decoding of reed-solomon and algebraic-geometry codes.