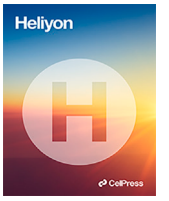
Heliyon 10 (2024) e25470

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

A failure in decryption process for bivariate polynomial reconstruction problem cryptosystem

Siti Nabilah Yusof [a], Muhammad Rezal Kamel Ariffin [a,b,*], Sook-Chin Yip [c,**], Terry Shue Chien Lau [d], Zahari Mahad [a], Ji-Jian Chin [e], Choo-Yee Ting [d]

[a] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia
[b] Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, Selangor, Malaysia
[c] Faculty of Engineering, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
[d] Faculty of Computing and Informatics, Multimedia University, Cyberjaya 63100, Selangor, Malaysia
[e] School of Engineering, Computing and Mathematics (Faculty of Science and Engineering), University of Plymouth, Drake Circus, Plymouth PL 48AA, UK

ARTICLE INFO

Keywords:
Polynomial reconstruction problem
Post-quantum cryptography
Decryption failure
Univariate polynomial
Bivariate polynomial

ABSTRACT

In 1999, the Polynomial Reconstruction Problem (PRP) was put forward as a new hard mathematics problem. A univariate PRP scheme by Augot and Finiasz was introduced at Eurocrypt in 2003, and this cryptosystem was fully cryptanalyzed in 2004. In 2013, a bivariate PRP cryptosystem was developed, which is a modified version of Augot and Finiasz's original work. This study describes a decryption failure that can occur in both cryptosystems. We demonstrate that when the error has a weight greater than the number of monomials in a secret polynomial, p, decryption failure can occur. The result of this study also determines the upper bound that should be applied to avoid decryption failure.

1. Introduction

A valid and secure cryptosystem can be designed using a good hard mathematical problem in cryptography. Cryptography is an important mechanism in data security where the cryptography algorithm makes communication possible in the presence of an adversary [8,30]. User's private data in embedded system needs to be protected and authenticated. It is essential for users to ensure that data consumed is valid [10,28]. Shor's algorithm has successfully solved classical problems such as the integer factorization problem (IFP) and the discrete logarithm problem (DLP) in polynomial time, where a quantum computer can attack cryptosystems that rely on such difficult mathematical problems [1,3,34]. Among the well-known cryptographic schemes that are algorithmically insecure in post quantum cryptography are RSA, El-Gamal, and Elliptic Curve Cryptosystem [7,22]. The National Institute of Standards and Technology (NIST) has called for a search for quantum-resistant algorithms [4,11,13,33].

Hence, this shows that post-quantum cryptography is preferable for information security purposes. Post-quantum cryptography is a cryptographic algorithm that is believed to be secure from the attack of quantum computer [21]. Post-quantum cryptography also consists of five major types which are lattice-based, code-based, isogeny-based, hash-based and multivariate-based cryptography [9,19]. The Quantum Algorithm Zoo website lists useful hard mathematical problems that may be immune to a quantum computing

* Corresponding author at: Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
** Corresponding author.
E-mail addresses: rezal@upm.edu.my (M.R. Kamel Ariffin), scyip@mmu.edu.my (S.-C. Yip).

https://doi.org/10.1016/j.heliyon.2024.e25470
Received 23 September 2023; Received in revised form 2 January 2024; Accepted 27 January 2024

Available online 1 February 2024

attack [20]. Thus, cryptographers must investigate diverse hard problems so that the new design cryptosystems are safe from the attack of quantum computers [18]. The evaluation of time intricacy and memory space for the attack is to ensure and validate the safety of the cryptosystems [26,27].

Quantum Algorithm Zoo introduced the PRP as a difficult mathematical problem in post-quantum cryptography [20]. This problem was introduced in 1999 when PRP developed a formulation equivalent to Reed-Solomon error-correcting codes [6,29,31]. The problem also contains the full intricacy against the quantum computers with the complexity of $\mathcal{O}(q)$ in which q contains n bits of prime. Besides that, a wide range of research on the PRP has been conducted based on the solvability and robustness [25].

This problem can be easily solved if the error's weight, w, is at most $\frac{n-k}{2}$. The parameter n represents the number of elements of the vector, while the parameter k represents the polynomial degree. This equation has been upgraded into $w \leq n - \sqrt{kn}$ [16]. Augot and Finiasz suggested a univariate PRP cryptosystem in 2003, where we call this scheme the AF-Cryptosystem. A univariate polynomial is used in the AF-Cryptosystem [23,24]. The AF-Cryptosystem also applied two PRP types: the first PRP is defined in [20], and the second PRP is built to guarantee the process of decryption. The second PRP is denoted as the Augot and Finiasz Solvable PRP (AF-SPRP), which is described below:

Definition 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 $t = n - w$.

From Definition 1, the decryption process can occur in the AF-Cryptosystem. From the Cartesian plane, if we obtain t points, a polynomial is required to be yielded in which this polynomial consists of all the points where t is the zero element in a vector. The decryption process in the AF-Cryptosystem can be done using Lagrange interpolation.

Nevertheless, the AF-Cryptosystem was managed to be fully cryptanalyzed by Coron [12]. Next, a bivariate PRP cryptosystem was proposed in 2013 by Ajeena et al.; this cryptosystem is called the AAK-Cryptosystem [2]. The AAK-Cryptosystem is the modified version of the AF-Cryptosystem where they used bivariate polynomial and Vandermonde method. The creators of AAK-Cryptosystem mentioned that if the amount of variables increases, then the cryptosystem's security level can be improved.

Our contribution. In this paper, we analyze the decryption process for both cryptosystems, which is different from our published papers in [36,37]. In our published papers, we put forward results that discusses the AAK-Cryptosystem is not indistinguishable chosen plaintext attack (IND-CPA) secure and how to retrieve the private key from the AAK-Cryptosystem. While our findings in this paper indicate that decryption errors can occur in both cryptosystems if the weight of the big error vector E is greater than the number of monomials in the secret polynomial p.

Organization of the article. This paper's setup is as follows: in Section 2, we put forward the fundamentals of PRP, Lagrange interpolation, and Vandermonde method and outline both AF-Cryptosystem and AAK-Cryptosystem. In Section 3, we explain our propositions for decryption failure in both cryptosystems and give an example for this analysis. Finally, we discuss our result in Section 4 and we conclude our findings in Section 5.

2. Materials and methods

This section explains the fundamental knowledge about PRP, Lagrange interpolation, Vandermonde method, AF-Cryptosystem and AAK-Cryptosystem.

2.1. PRP

The PRP is known since the generalized Reed-Solomon list decoding problem has been reduced to it [32]. Next, we describe PRP based on [20], which shown down below:

Definition 2. ***(PRP from Quantum Zoo)*** Let $p(x) = a_k x^k + \cdots + a_1 x + a_0$ be a polynomial over finite field $\mathbb{F}_q$. One is given access to the oracle and query value of $x_i \in \mathbb{F}_q$ where $1 \leq i \leq k+1$ then output coefficients $a_k, \ldots, a_0$ to determine $p(x)$.

From Definition 2, this shows that when the oracle input $x \in \mathbb{F}_q$, then it will output $p(x)$. Then, this provides us the coefficients $a_k, \ldots, a_0$ [20]. Classically, we need $k+1$ queries to identify the number of coefficients. Therefore, the query complexity in PRP for a univariate polynomial with a degree equal to k is $\mathcal{O}\binom{k+1}{k}$.

2.2. Computational complexity of PRP

We know that $p(x)$ has a degree equal to k, and $p(x)$ contains $k+1$ coefficients, equivalent to $q-1$, hence $k = q-2$. Thus,

$$\mathcal{O}\binom{k+1}{k} = \mathcal{O}(q-1).$$

It is impractical for us to query input x if $q \approx 2^n$ is exponentially large. This shows that solving PRP would take exponential time, which is $\mathcal{O}(2^n)$.

2.3. Lagrange interpolation

The Lagrange interpolation method can identify a polynomial based on the observed value at each observed point. Besides that, Lagrange interpolation is regularly utilized in cryptography to share secret and coding computing [14]. The Lagrange interpolation is where we are provided n real values $x_1, x_2, x_3 \ldots, x_n$ and $y_1, y_2, y_3 \ldots, y_n$, then output a polynomial p that contains real coefficients which satisfies $p(x_i) = y_i$ where $i = 1, 2, 3, \ldots, n$ [17]. Polynomial p must have a degree less than the real values where degree$(p) < n$. The Lagrange interpolation formula with nth order is as follows,

$$f(x) = \frac{(x-x_1)(x-x_2)\ldots(x-x_n)}{(x_0-x_1)(x_0-x_2)\ldots(x_0-x_n)} \times y_0 + \frac{(x-x_0)(x-x_2)\ldots(x-x_n)}{(x_1-x_0)(x_1-x_2)\ldots(x_1-x_n)} \times y_1 + \ldots + \frac{(x-x_0)(x-x_1)\ldots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\ldots(x_n-x_{n-1})} \times y_n.$$

The AF-Cryptosystem utilized Lagrange interpolation in decryption process.

2.4. Vandermonde method

An interpolation polynomial with two or more dimensions is determined using the Vandermonde method. Given points that have two variables where $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, for each point, one must obtain the polynomial values $z_1, z_2, \ldots, z_n$, correspondingly. The two variables polynomial with the degree of $n-1$ can be obtained by using the following steps,

1. Formulate the formula of a polynomial with the degree $n-1$ where this polynomial contains two variables.
2. Calculate the polynomial at the given points.
3. Solve the system of linear equations.

The problem can be presented in the form $V \cdot c = Z$ where V is a Vandermonde matrix with the dimension of $n \times n$, also known as coefficients matrix [15,35]. Parameter Z contains z values, while parameter c is the coefficient vector. The AAK-Cryptosystem applied the Vandermonde method in the decryption process.

2.5. AF-cryptosystem

Augot and Finiasz introduced a univariate PRP cryptosystem which describes down below [5]. Considering that n is the number of elements in the vector and the AF-cryptosystem applied the following parameters in Table 1.

Table 1
Parameters.

Parameter	Remark
$\mathbb{F}_q$	A finite field of size q
n	The number of elements in the vector
k	Its dimension
W	The weight of big error vector, E where PRP is hard when, $W > \frac{n-k}{2}$ [2]
w	The weight of small error vector, e that enabling the PRP to decrypt the ciphertext when $w \leq \frac{n-k}{2}$ [12]

Remark 1. The parameter w is the vector's maximum number of nonzero elements.

Remark 2. The parameter $n - w$ is known as the number of zero elements of the vector.

The proposed AF-Cryptosystem is as follows:

Algorithm 1: Key generation process.

Input: Parameters (x_i, q, n, k, W, w)
Output: Public Key, PK and private key pair (C, E)
1: Generate $p(X)$ of degree k.
2: Generate big error vector E with the weight W.
3: Compute vector $C = ev(p(X)) = p(x_i)$ where $x_i \in \mathbb{F}_q$.
4: Computes $PK = C + E$.
5: Publish PK and (C, E).

Algorithm 2: Encryption process.

Input: Message, $\mu \in \mathbb{F}_q$
Output: Ciphertext, CT
1: Generate message polynomial $\mu(X)$ with length k.
2: Calculate $\mu = ev(\mu(X)) = \mu(x_i)$.
3: Generate $\alpha \in \mathbb{F}_q$.
4: Generate small error vector e with the weight w.
5: Calculate $CT = \mu + \alpha \times PK + e$.
6: Publish CT.

Algorithm 3: Decryption process.

Input: Ciphertext, CT
Output: Message polynomial, $\mu(X)$
1: **for** $i \leftarrow 1$ to n where $E_i = 0$ **do**
2: $\overline{CT} = \overline{\mu} + \alpha \times \overline{C} + \overline{e}$.
3: **end**
4: Correct $\overline{CT}$ and determine $\tilde{CT} = \tilde{\mu} + \alpha \times \tilde{C}$.
5: Computes $q(X)$ with the degree of k by applying Lagrange interpolation.
6: Determine leading coefficient of $q(X)$.
7: Calculate $\mu(X) = q(X) - \alpha p(X)$.

2.5.1. Proof of correctness

Proposition 1. *The message polynomial $\mu(x)$ can be obtained through the decryption algorithm in AF-Cryptosystem.*

Proof. Refer to Appendix A. □

2.6. AAK-cryptosystem

The AF-Cryptosystem was altered by Ajeena et al. to create the bivariate PRP cryptosystem that is described below [2]. The AAK-Cryptosystem applied the parameters in Table 1. The proposed modified cryptosystem is as follows:

Algorithm 4: Key generation process.

Input: Parameters $(x_i, y_i, q, n, k, W, w)$
Output: Public Key, PK and secret key pair (C, E)
1: Generate $p(X, Y)$ with degree of $k-1$ to both X and Y.
2: Generate big error vector with a weight of the W.
3: Compute vector $C = ev(p(X, Y)) = p(x_i, y_i)$ where $x_i, y_i \in \mathbb{F}_q$.
4: Compute $PK = C + E$.
5: Publish PK and (C, E).

Algorithm 5: Encryption process.

Input: Message, $\mu \in \mathbb{F}_q$
Output: Ciphertext, CT
1: Generate message polynomial $\mu(X, Y)$ with length $k+1$.
2: Calculate $\mu = ev(\mu(X, Y)) = \mu(x_i, y_i)$.
3: Generate $\alpha \in \mathbb{F}_q$.
4: Generate small error vector e with the weight w.
5: Calculate $CT = \mu + \alpha \times PK + e$.
6: Publish CT.

Algorithm 6: Decryption process.

Input: Ciphertext, CT
Output: Message polynomial, $\mu(X, Y)$
1: **for** $i \leftarrow 1$ to n where $E_i = 0$ **do**
2: $\overline{CT} = \overline{\mu} + \alpha \times \overline{C} + \overline{e}$.
3: **end**
4: Correct $\overline{CT}$ and determine $\tilde{CT} = \tilde{\mu} + \alpha \times \tilde{C}$.
5: Compute $q(X, Y)$ with the degree of $k-1$ by applying the Vandermonde method.
6: Determine leading coefficient of $q(X, Y)$.
7: Calculate $\mu(X, Y) = q(X, Y) - \alpha p(X, Y)$.

2.6.1. Proof of correctness

Proposition 2. *The proof of the decryption algorithm in AAK-Cryptosystem is correct.*

Proof. Refer to Appendix B. □

3. The decryption failure

This section explains how decryption failure can occur in the AF-Cryptosystem and AAK-Cryptosystem. A numerical illustration is also provided.

3.1. Decryption failure in AF-cryptosystem

Proposition 3. *If the weight of nonzero element in big error E is $W > k + 1$, then the decryption process in AF-Cryptosystem cannot occur.*

Proof. Refer to Appendix C. □

3.1.1. Numerical illustration for Proposition 3

In this section, inline with Proposition 3, we put forward a numerical example where the system owner incorrectly sets the system parameters such that $n - W < k + 1$ which would lead to the system owner unable to decrypt the ciphertext.

Example 1. Let $n = 7$, $k = 2$, $w = 2$ and $W = 5$ in $\mathbb{F}_{11}$. Given $x = (9, 8, 7, 6, 5, 4, 3)$. We start with the key generation process by taking the private polynomial,

$$p(x) = x^2 + 2x + 6$$

and big error vector E,

$$E = (1, 2, 3, 4, 5, 0, 0).$$

The public key is:

$$PK = C + E.$$

Vector C is obtained by the evaluation of $p(x)$ where:

$$p(9) = 6,\ p(8) = 9,\ p(7) = 3,\ p(6) = 10,$$

$$p(5) = 8,\ p(4) = 8,\ p(3) = 10.$$

Hence, $C = (6, 9, 3, 10, 8, 8, 10)$. Then, compute PK as follows,

$$\begin{aligned} PK &= C + E \\ &= (6, 9, 3, 10, 8, 8, 10) + (1, 2, 3, 4, 5, 0, 0) \\ &= (7, 0, 6, 3, 2, 8, 10). \end{aligned}$$

Next, in encryption process, we evaluate $\mu(x) = x + 5$ codeword μ which shown as follows,

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

$$\mu(5) = 10,\ \mu(4) = 9,\ \mu(3) = 8.$$

Thus, we have

$$\mu = (3, 2, 1, 0, 10, 9, 8).$$

Next, we generate a constant $\alpha = 2 \in \mathbb{F}_{11}$ and a small error vector, e where

$$e = (6, 7, 0, 0, 0, 0, 0).$$

Observe that the weight for the small error vector is $w = 2$. Then, the CT is:

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

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

In the decryption process, based on the AF-Cryptosystem, we need to consider the position of zero elements in E where $n - W = 2$. From E, we have

$$E_6 = E_7 = 0.$$

Therefore, we obtain two shadows $\overline{CT} = CT_6 = CT_7 = (3,6)$. Next, Lagrange interpolation is applied to find $q(x)$. The degree of polynomial $q(x)$ must be $k = 2$. From $\overline{CT}$, we have

$$q(4) = 3 \text{ and } q(3) = 6$$

Hence, the unique polynomial $q(x)$ is as follows,

$$\begin{aligned} q(x) &= \frac{(x - x_7)}{(x_6 - x_7)}(CT_6) + \frac{(x - x_6)}{(x_7 - x_6)}(CT_7) \\ &= \frac{(x-3)}{(4-3)}(3) + \frac{(x-4)}{(3-4)}(6) \\ &= 3x - 9 - 6x + 24 \bmod 11 \\ &= 8x + 4. \end{aligned}$$

As we can see here, $q(x)$ has a degree of 1, which is smaller than $p(x)$. Therefore, we cannot identify $\mu(x)$ due to the small size of $q(x)$. Hence, the decryption process is a failure.

3.2. Decryption failure in AAK-cryptosystem

This section presents the scenario where the decryption process in AAK-Cryptosystem is a failure. A larger size of W, will make it difficult to determine the message polynomial, $\mu(x,y)$.

Proposition 4. *If the weight of nonzero element in big error E is larger than number of monomial of secret polynomial $p(x,y)$, then the decryption process in AAK-Cryptosystem cannot occur.*

Proof. Refer to Appendix D. □

3.2.1. Numerical illustration of Proposition 4

In this section, inline with Proposition 4, we put forward a numerical example where the system owner incorrectly sets the system parameters such that $n - W < k^2$ which would lead to the system owner unable to decrypt the ciphertext.

Example 2. Let $n = 10$, $k = 2$, $w = 1$ and $W = 7$ in $\mathbb{F}_{11}$. Given $x = (4,3,2,1,2,1,2,3,4,3)$ and $y = (1,1,2,2,3,3,4,4,3,0)$. We start with the key generation process by taking the secret polynomial,

$$p(x,y) = xy + 2x + y + 1$$

and big error vector E,

$$E = (1,2,3,4,1,2,3,0,0,0).$$

The public key is:

$$PK = C + E.$$

Vector C is obtained where the $p(x,y)$ is evaluated down below:

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

Thus, $C = (3,0,0,7,3,9,6,1,2,7)$. Then, the PK is as follows,

$$\begin{aligned} PK &= C + E \\ &= (3,0,0,7,3,9,6,1,2,7) + (1,2,3,4,1,2,3,0,0,0) \\ &= (4,2,3,0,4,0,9,1,2,7). \end{aligned}$$

Next, in encryption process, we evaluate $\mu(x, y) = 2x + 4y + 5$ codeword μ which shown as follows,

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

Hence, we obtain

$$\mu = (4,2,4,2,8,6,1,3,1,9).$$

Next, we generate a secret value $\alpha = 3 \in \mathbb{F}_{11}$ and a small error vector, e such that

$$e = (2,0,0,0,0,0,0,0,0,0).$$

Observe that the weight for the small error vector is $w = 1$. Then, CT is:

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

In the decryption process, based on the AAK-cryptosystem, we need to consider the position of zero elements in E where $n - W = 3$. From E we have

$$E_8 = E_9 = E_{10} = 0.$$

Thus, we contain three shadows $\overline{CT} = CT_8 = CT_9 = CT_{10} = (6,7,8)$. The next step is to find a unique polynomial $q(x, y)$ using the Vandermonde method. Polynomial $q(x, y)$ must be with the degree of $k - 1 = 1$ for X and Y. Let $q(X, Y) = q_1xy + q_2x + q_3y + q_4$, we have,

$$q(3,4) = q_1(1) + q_2(3) + q_3(4) + q_4 = 6$$
$$q(4,3) = q_1(1) + q_2(4) + q_3(3) + q_4 = 7$$
$$q(3,0) = q_1(0) + q_2(3) + q_3(0) + q_4 = 8.$$

We need to determine the coefficients for $q(X, Y)$ by using Gaussian elimination,

$$\begin{bmatrix} 1 & 3 & 4 & 1 \\ 1 & 4 & 3 & 1 \\ 0 & 3 & 0 & 1 \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \\ q_3 \\ q_4 \end{bmatrix} = \begin{bmatrix} 6 \\ 7 \\ 8 \end{bmatrix}.$$

Then, the equation of the system is

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 2 & 3 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 & 0 \end{array}\right].$$

As we can see here, the system shows that q_4 is a free variable and is not a unique solution. Hence, we cannot identify $q(x, y)$. From $\overline{CT} = (6,7,8)$, we have insufficient information to identify unique polynomial $q(x, y)$. Hence, the decryption process cannot be done.

4. Discussion

Based on the results, we need to ensure the weight of big error vector W, is less than the number of monomials of the secret polynomial p, for both AF-Cryptosystem and AAK-cryptosystem. The users of these cryptosystems need to take into consideration information regarding the boundary value for W, to prevent decryption failure from occurring.

5. Conclusion

This paper presents that decryption failure can occur in AF-Cryptosystem and AAK-Cryptosystem. When W is greater than the number of monomials of secret polynomial p, then we cannot determine unique polynomial q. Hence, we cannot decrypt the ciphertext, CT, to identify the message polynomial, μ. Thus, the recommended weight for big error vector, E to be used in AF-Cryptosystem and AAK-Cryptosystem are $\frac{n-k}{2} < W \leq k + 1$ and $\frac{n-k}{2} < W \leq k^2$ respectively so that decryption process can occur.

For the future works, we would suggest an investigation into whether the size of the message polynomial that is used in both cryptosystems could also contribute towards decryption failure.

Availability of data and materials

Not applicable.

Consent of publication

Not applicable.

CRediT authorship contribution statement

Siti Nabilah Yusof: Writing – original draft, Methodology, Formal analysis, Conceptualization. **Muhammad Rezal Kamel Ariffin:** Writing – review & editing, Validation, Supervision, Funding acquisition. **Sook-Chin Yip:** Writing – review & editing, Funding acquisition. **Terry Shue Chien Lau:** Formal analysis. **Zahari Mahad:** Formal analysis. **Ji-Jian Chin:** Funding acquisition, Formal analysis. **Choo-Yee Ting:** Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The results of Terry Shue Chien Lau were supported by Multimedia University Postdoc (MMUI/230164). We also acknowledged the support from the Ministry of Higher Education, Malaysia through the Fundamental Research Grant Scheme with reference code FRGS/1/2019/STG06/UPM/02/8, which gives us the opportunity to do this research.

Appendix A. The proof of Proposition 1

Proof. Based on the ciphertext CT, the message polynomial $\mu(x)$ can be recovered where:

$$\begin{aligned} CT &= \mu + \alpha \times PK + e \\ &= \mu + \alpha \times (C + E) + e. \end{aligned} \tag{A.1}$$

Consider $E_i = 0$, which is the shortened code of Reed-Solomon code of dimension k, $\overline{RS_k}$. Given that $\overline{\mu}$, $\overline{C}$, $\overline{e}$ and $\overline{CT}$ are the shortened code for μ, C, e and CT respectively then E is disappeared. Now, (A.1) turns into

$$\overline{CT} = \overline{\mu} + \alpha \times \overline{C} + \overline{e}. \tag{A.2}$$

From (A.2), $\overline{\mu} + \alpha \times \overline{C} \in \overline{RS_k}$. Given that the weight of e is smaller than error correction capacity $\overline{RS_k}$ then correct $\overline{CT}$ and determine $\tilde{\mu} + \alpha \times \tilde{C}$. By applying Lagrange interpolation, calculate $q(x)$ which has the degree equals to k such that

$$ev(q(x_i)) = \tilde{\mu}_i + \alpha \times \tilde{C}_i \tag{A.3}$$

for $i \in \{1, 2, \ldots, n\}$. Since $ev(q(x_i))$ is the evaluation of $q(x_i)$, vector $\tilde{C} = ev(p(x_i))$ is the evaluation of $p(x_i)$ and vector $\tilde{\mu} = ev(\mu(x_i))$ is the evaluation of $\mu(x_i)$ then

$$\begin{aligned} q(x_i) &= \mu(x_i) + \alpha p(x_i) \\ \mu(x_i) &= q(x_i) - \alpha p(x_i). \end{aligned} \tag{A.4}$$

Based on (A.4), the $\mu(x)$ has been recovered. Thus, the proof is terminated. □

Appendix B. The proof of Proposition 2

Proof. Based on the ciphertext CT, the message polynomial $\mu(x, y)$ can be recovered where:

$$\begin{aligned} CT &= \mu + \alpha \times PK + e \\ &= \mu + \alpha \times (C + E) + e. \end{aligned} \tag{B.1}$$

The position $E_i = 0$ is considered the shortened code of Reed-Solomon of dimension k, $\overline{RS_k}$. Given that $\overline{\mu}$, $\overline{C}$, $\overline{e}$ and $\overline{CT}$ are the shortened code for μ, C, e and CT respectively then E is disappeared. Now, (B.1) turns

$$\overline{CT} = \overline{\mu} + \alpha \times \overline{C} + \overline{e}. \tag{B.2}$$

From (B.2), $\overline{\mu} + \alpha \times \overline{C} \in \overline{RS_k}$. Given that e is with the weight less than error correction capacity $\overline{RS_k}$ then correct $\overline{CT}$ and determine $\tilde{\mu} + \alpha \times \tilde{C}$. By applying Vandermonde method, compute $q(x, y)$ which has the degree equals to $k - 1$ where

$$ev(q(x_i, y_i)) = \tilde{\mu}_i + \alpha \times \tilde{C}_i \tag{B.3}$$

for $i \in \{1, 2, \ldots, n\}$. Since $ev(q(x_i, y_i))$ is the evaluation of $q(x_i, y_i)$, vector $\tilde{C} = ev(p(x_i, y_i))$ is the evaluation of $p(x_i, y_i)$ and vector $\tilde{\mu} = ev(\mu(x_i, y_i))$ is the evaluation of $\mu(x_i, y_i)$, hence

$$\begin{aligned} q(x_i, y_i) &= \mu(x_i, y_i) + \alpha p(x_i, y_i) \\ \mu(x_i, y_i) &= q(x_i, y_i) - \alpha p(x_i, y_i). \end{aligned} \tag{B.4}$$

Based on (B.4), the $\mu(x, y)$ can be recovered. □

Appendix C. The proof of Proposition 3

Proof. Based on Table 1, Alice generates $p(x)$ with a degree equal to k, and during the key generation process, E with weight W is generated by Alice. Given that $p(x)$ be as follows,

$$p(x_i) = x^k + \ldots + a_2 x^2 + a_1 x^1 + a_0.$$

Thus, $p(x)$ has $k+1$ coefficients. Suppose that Alice chooses the weight E as $W > k+1$. The position of zero and nonzero elements in E can vary. The ciphertext, CT contains n vector elements given by,

$$CT_i = \mu_i + \alpha \cdot PK_i + e_i \quad \forall\ 1 \leq i \leq n.$$

In the decryption process, the position of zero elements is important, and there are $n - W$ zero elements. The decryption process will acquire $\overline{CT}$ where $\overline{CT}$ contains $n - W$ elements. Next, the unique polynomial $q(x)$ with degree k can be determined by applying Lagrange interpolation. Polynomial $q(x)$ must have $k + 1$ coefficients which are the same as the secret polynomial $p(x)$.

If Alice takes $W > k + 1$, it will result in the polynomial $q(x)$, which contains less number of coefficients in $\overline{CT}$. This is because $n - W < k + 1$. From here, by using Lagrange interpolation, the $q(x)$ that will be acquired contains degree $n - W - 1$, which is less than k. One must compute $q(x) - \alpha \cdot p(x)$ in order to recover $\mu(x)$. Since $q(x)$ is smaller than $p(x)$, we will recover $\mu(x)$ with a degree less than $p(x)$. Hence, the decryption process is a failure due to the weight of the big error vector, E. □

Appendix D. The proof of Proposition 4

Proof. Based on the parameters in Table 1, we start with the key generation process, where Alice has a private polynomial $p(x, y)$ of degree $k - 1$ for both x and y and a big error vector E its weight is W. Given that $p(x, y)$ is as follows,

$$p(x_i, y_i) = x^{k-1} y^{k-1} + \ldots + a_{1,1} x^1 y^1 + a_{1,0} x^1 + a_{0,1} y^1 + a_{0,0}.$$

Then, $p(x, y)$ has k^2 coefficients. Suppose that Alice chooses the weight E as $W > k^2$. The position of zero and nonzero elements in E can vary. The ciphertext, CT contains n vector elements given by,

$$CT_i = \mu_i + \alpha \cdot PK_i + e_i \quad \forall\ 1 \leq i \leq n$$

In the decryption process, the position of zero elements is essential, and there are $n - W$ zero elements. The decryption process will obtain $\overline{CT}$, with $n - W$ elements in $\overline{CT}$. Next, by using the Vandermonde method, we can determine $q(x, y)$ with degree $k - 1$ where $q(x, y)$ contains k^2 coefficients which are the same as the secret polynomial $p(x, y)$.

If Alice selects W to be more than k^2, it will result in $q(x, y)$ containing less number of coefficients in $\overline{CT}$. This is because $n - W < k^2$. Using the Vandermonde method, the solution we will obtain is not unique. This would lead to a situation where we have to calculate a system of equations where the number of equations is less than the number of variables. Therefore, matrix V is not a square matrix. Upon solving such systems, we would arrive at the following situations:

i) infinitely many solutions
ii) no solution

The $\mu(x, y)$ can be recovered by calculating $q(x, y) - \alpha \cdot p(x, y)$. Since $q(x, y)$ can be i) or ii), then we cannot calculate $q(x, y) - \alpha \cdot p(x, y)$. Thus, the decryption process is a failure due to the weight of the big error vector, E. □

References

[1] N.A.S. Abdul Jamal, M.R. Kamel Ariffin, S.H. Sapar, K. Abdullah, New identified strategies to forge multivariate signature schemes, Symmetry 14 (11) (2022) 2368.
[2] R.K. Ajeena, H. Kamarulhaili, S.B. Almaliky, Bivariate polynomials public key encryption schemes, Int. J. Cryptol. Res. 4 (1) (2013) 73–83.
[3] A.A. Agarkar, H. Agrawal, LRSPPP: lightweight R-LWE-based secure and privacy-preserving scheme for prosumer side network in smart grid, Heliyon 5 (3) (2019).
[4] A. Li, D. Liu, C. Zhang, X. Li, S. Yang, X. Liu, J. Lu, X. Zhou, A. Hu, T. Ni, A flexible and high-performance lattice-based post-quantum crypto secure coprocessor, IEEE Trans. Ind. Inform. 19 (2) (2022) 1874–1883.
[5] D. Augot, M. Finiasz, A public key encryption scheme based on the polynomial reconstruction problem, in: International Conference on the Theory and Applications of Cryptographic Techniques, 2003, pp. 229–240.
[6] D. Augot, M. Finiasz, P. Loidreau, Using the Trace Operator to Repair the Polynomial Reconstruction Based Cryptosystem Presented at Eurocrypt 2003, International Association for Cryptologic Research 209, 2003.
[7] M.B. Begum, N. Deepa, M. Uddin, R. Kaluri, M. Abdelhaq, R. Alsaqour, An efficient and secure compression technique for data protection using Burrows-Wheeler transform algorithm, Heliyon (2023).
[8] A. Bhatia, A. Kumar, A. Jain, A. Kumar, C. Verma, Z. Illes, M.S. Raboaca, Networked control system with MANET communication and AODV routing, Heliyon 8 (11) (2022).
[9] A.C. Canto, J. Kaur, M.M. Kermani, R. Azarderakhsh, Algorithmic security is insufficient: a comprehensive survey on implementation attacks haunting post-quantum security, arXiv preprint, arXiv:2305.13544, 2023.
[10] S. Chen, J. Chen, Lattice-based group signatures with forward security for anonymous authentication, Heliyon 9 (4) (2023).
[11] A. Cintas-Canto, M. Mozaffari-Kermani, R. Azarderakhsh, K. Gaj, CRC-oriented error detection architectures of post-quantum cryptography Niederreiter key generator on FPGA, in: 2022 IEEE Nordic Circuits and Systems Conference (NorCAS), 2022, pp. 1–7.
[12] J.S. Coron, Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem, in: International Workshop on Public Key Cryptography, 2004, pp. 14–27.
[13] R. Elkhatib, R. Azarderakhsh, M. Mozaffari-Kermani, Accelerated RISC-V for SIKE, in: 2021 IEEE 28th Symposium on Computer Arithmetic (ARITH), 2021, pp. 131–138.
[14] A. Fu, X. Zhang, N. Xiong, Y. Gao, H. Wang, J. Zhang, VFL: a verifiable federated learning with privacy-preserving for big data in industrial IoT, IEEE Trans. Ind. Inform. 18 (5) (2020) 3316–3326.
[15] G. Patanè, Fourier-based and rational graph filters for spectral processing, IEEE Trans. Pattern Anal. Mach. Intell. (2022) 7063–7074.
[16] V. Guruswami, M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, IEEE Trans. Inf. Theory (1999) 1757–1767.
[17] D. Huang, Q. Gan, X. Wang, M.R. Ogiela, X.A. Wang, Privacy preserving IoT-based crowd-sensing network with comparable homomorphic encryption and its application in combating COVID19, Int. Things 20 (2022).
[18] M. Imran, Z.U. Abideen, S. Pagliarini, An experimental study of building blocks of lattice-based NIST post-quantum cryptographic algorithms, Electronics 9 (11) (2020) 1953.
[19] N.A.S.A. Jamal, M.R. Kamel, Novel forgery mechanisms in multivariate signature schemes, Comput. Sci. 18 (3) (2023) 451–461.
[20] S. Jordan, Quantum algorithm zoo, https://quantumalgorithmzoo.org/, 2011.
[21] J. Kaur, A.C. Canto, M.M. Kermani, R. Azarderakhsh, A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard, arXiv preprint, arXiv:2304.06222, 2023.
[22] M.M. Kermani, R. Azarderakhsh, Lightweight hardware architectures for fault diagnosis schemes of efficiently-maskable cryptographic substitution boxes, in: 2016 IEEE International Conference on Electronics, Circuits and Systems (ICECS), 2016, pp. 764–767.
[23] A. Kiayias, M. Yung, Polynomial reconstruction based cryptography, in: International Workshop on Selected Areas in Cryptography, 2001, pp. 129–133.
[24] A. Kiayias, M. Yung, 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, 2004, pp. 401–416.
[25] A. Kiayias, M. Yung, Directions in polynomial reconstruction based cryptography, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 87 (5) (2004) 978–985.
[26] H. Kuwakado, M. Morii, Quantum distinguisher between the 3-round Feistel cipher and the random permutation, in: IEEE International Symposium on Information Theory, 2010, pp. 2682–2685.
[27] C.Y. Lin, J.L. Wu, Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintext related permutation and diffusion, Entropy 22 (5) (2020) 589.
[28] M. Mozaffari Kermani, R. Azarderakhsh, M. Mirakhorli, Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education, 2016.
[29] M. Naor, B. Pinkas, Oblivious transfer and polynomial evaluation, in: Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, 1999, pp. 245–254.
[30] A. Razaq, G. Alhamzi, S. Abbas, M. Ahmad, A. Razzaque, Secure communication through reliable S-box design: a proposed approach using coset graphs and matrix operations, Heliyon 9 (5) (2023).
[31] I.S. Reed, G. Solomon, Polynomial codes over certain finite fields, J. Soc. Ind. Appl. Math. 8 (2) (1960) 300–304.
[32] S.B. Sadkhan, K.H. Ruma, Evaluation of polynomial reconstruction problem using Lagrange interpolation method, in: 2nd International Conference on Information and Communication Technologies, 2006, pp. 1399–1403.
[33] A. Sarker, M.M. Kermani, R. Azarderakhsh, Efficient error detection architectures for postquantum signature Falcon's sampler and KEM SABER, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 30 (6) (2022) 794–802.
[34] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
[35] T. Jahani-Nezhad, M.A. Maddah-Ali, Berrut approximated coded computing: straggler resistance beyond polynomial computing, IEEE Trans. Pattern Anal. Mach. Intell. 45 (1) (2022) 111–122.
[36] S.N. Yusof, M.R. Kamel Ariffin, An empirical attack on a polynomial reconstruction problem potential cryptosystem, Int. J. Cryptol. Res. 11 (2021) 31–48.
[37] S.N. Yusof, M.R. Kamel Ariffin, T.S.C. Lau, N.R. Salim, S.C. Yip, T.T.V. Yap, An IND-CPA analysis of a cryptosystem based on bivariate polynomial reconstruction problem, Axioms 12 (3) (2023) 304.