Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 26 (2023), No. 8, pp. 1815–1823
DOI : 10.47974/JIM-1660

Modified public key cryptosystem based on distance and geometry area in triangles

Maxrizal *
Department of Information Systems
Institut Sains Dan Bisnis Atma Luhur
Pangkalpinang 33172
Indonesia

Baiq Desy Aniska Prayanti
Department of Mathematics
Universitas Bangka Belitung
Pangkalpinang 33172
Indonesia

Abstract

Public key cryptosystems using commutative algebra are not safe from quantum algorithm attacks. For this reason, experts have developed non-commutative algebra applied to geometry-based public key cryptosystems. This study develops a public key cryptosystem using the concept of geometry on the area of a triangle. We can show that the proposed public key cryptosystem works well. Furthermore, mathematical hacking experiments carried out by hackers are complex because the public key cryptosystem works on a ring of real numbers.

Subject Classification: *(2010) 11T71, 14G50.*

Keywords: *Triangles of public-key cryptosystem, Cryptosystem triangles, Cryptosystem based on geometry.*

1. Introduction

Public key cryptosystems that use commutative algebra are not safe from quantum algorithm attacks. For this reason, experts have developed a public key cryptosystem based on non-commutative algebra. The proposed system includes a public key cryptosystem using non-

* *E-mail:* **maxrizal@atmaluhur.ac.id (Corresponding Author)**

commutative properties in ring matrices [1]–[7] and matrix polynomial decomposition [8], [9]. Experts also use special matrix forms to form public key cryptographic systems[10]–[13].

A public key cryptosystem that uses non-commutative algebra is also developed based on geometry. Experts use the Mobius plane [14], [15] or modify Elliptic Curve Cryptography (ECC) so that it is not vulnerable to quantum algorithm attacks [16]–[18]. Experts are also working on the Affine plane, modifying the Affine Hill Cipher to form public key cryptosystems [19]. As with ECC, experts also use discrete logarithms over group multiplication to construct public key cryptosystems [20].

For this reason, in this study, we propose a public key cryptosystem using the concept of triangular area. The proposed public key cryptosystem will work on a ring of real numbers ($\mathbb{R}$). We also carried out some experimental attacks that hackers might have done.

2. Geometry Distance and Area Analysis in Triangles

We take two points, $A(x_a, y_a) \in \mathbb{R}^2$ and $B(x_b, y_b) \in \mathbb{R}^2$. Then, we can form the equation of line

$$l_{AB} : \frac{(y-y_a)}{(y_b-y_a)} = \frac{(x-x_a)}{(x_b-x_a)} \tag{1}$$

If the gradient is $m = \frac{(y_B-y_A)}{(x_B-x_A)}$, then equation (1) becomes $l_{AB} : (y - y_A) = m(x - x_A)$.

Remark 2.1: Given two points, $A(x_a, y_a) \in \mathbb{R}^2$ and $B(x_b, y_b) \in \mathbb{R}^2$. We can use the Pythagorean equation to calculate the distance between points *A* and *B*.

$$d(A, B) = \sqrt{(x_b - x_a)^2 + (y_b - y_a)^2} \tag{2}$$

Next, we will calculate the distance of a point to an equation of a line.

Remark 2.2: If there is a point $C(x_c, y_c) \in \mathbb{R}^2$ and the equation of line $l_{AB} : ax + by + c = 0$, then the distance from point *C* to line l_{AB} is

$$d(C, l_{AB}) = \frac{|ax_c+by_c+c|}{\sqrt{a^2+b^2}} \tag{3}$$

Next, we will analyze an equation of a line to get information about the distance between its points.

Example 2.3: Given two points, $A(10, 4)$ and $B(2, 16)$. The equation of the line through AB is

$$l_{AB} : 12x + 8y - 152 = 0 \Leftrightarrow 3x + 2y - 38 = 0 \quad (4)$$

We get the distance AB is $d(A,B) = \sqrt{8^2+12^2} = 4\sqrt{13}$. Then, we investigate the denominator of equation (3), $\sqrt{a^2+b^2} = \sqrt{3^2+2^2} = \sqrt{13}$. So, we get $d(A,B) = 4\sqrt{a^2+b^2}$, which is $k = 4$.

Based on Example 2.3., we know that, generally, $d(A,B) \neq \sqrt{a^2+b^2}$.

Remark 2.4: We take the equation of line $l_{AB} : ax + by + c = 0$. We take two points $H, G \in \mathbb{R}^2$ on line l_{AB}. Notice that $d(H,B) = k\sqrt{a^2+b^2}$, with $k \in \mathbb{R}$.

Next, we will calculate the area of the triangle.

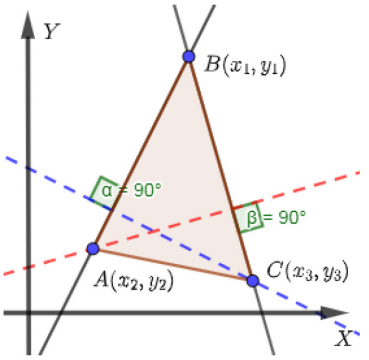

Figure 1

Height lines on each side of the triangle

In triangle ABC, we can always find the altitude of each vertex, according to Figure 1.

Remark 2.5: Given a point $A(x_a, y_a), B(x_b, y_b), C(x_c, y_c) \in \mathbb{R}^2$. We symbolize the heights of triangle ABC, namely $d(C, l_{AB}), d(A, l_{BC})$ and $d(B, l_{AC})$. The area of triangle ABC can be calculated by

$$2L_{\Delta ABC} = d(A,B)d(C,l_{AB}) = d(B,C)d(A,l_{BC}) = d(A,C)d(B,l_{AC}) \quad (5)$$

Next, from the equations of the two intersecting lines, we can find the cosine of the angle formed by the two lines.

Remark 2.6: Given the lines l_{AB} and l_{BC} equations that intersect at point B. We choose points H and G to form the vectors $BH = \vec{u}$ and $BG = \vec{v}$. We can calculate $\cos\alpha = \frac{u.v}{|u|\,|v|}$, where $|u|$ is the length of the vector u.

Once we have the cosine D, we can calculate a triangle's area.

Remark 2.7: We were given point $A(x_a, y_a), B(x_b, y_b), C(x_c, y_c) \in \mathbb{R}^2$. We symbolize $\angle ABC = \beta$, $\angle CAB = \alpha$, and $\angle BCA = \gamma$. The area of the ABC triangle can be calculated by

$$2L_{\Delta ABC} = d(A,B).d(B,C)\sin\beta = d(B,C).d(C,A)\sin\gamma = d(C,A).d(A,B)\sin\alpha \tag{6}$$

3. Proposed Public Key Cryptosystem Algorithm

In this study, we will modify the public key cryptosystem using the concept of distance and geometric area in triangles. We will use the point parameters on $\mathbb{R}^2$, the point distance, and the area of the triangle ABC.

3.1 *Key Generation Algorithm*

Let us say that Alice and Bob will send a secret message. Alice and Bob agree to choose any point $B(x_b, y_b) \in \mathbb{R}^2$. They agree to choose any two points $A(x_a, y_a), C(x_c, y_c) \in \mathbb{R}^2$. They form the equations of the lines l_{AB} and l_{BC}. All these parameters are public.

(1) Alice will determine any point $H(x_h, y_h) \in \mathbb{R}^2$ that lies on the equation of the line l_{AB}. She chooses any x_h so that $H(x_h, y_h)$ is obtained, which is private. She counted $d(H,B)$ and kept it a secret. Alice also calculates $d(H, l_{BC})$ and sends it to Bob.

(2) Bob will determine any point $G(x_g, y_g) \in \mathbb{R}^2$ that lies on the equation of the line l_{BC}. He chooses any x_g so that $G(x_g, y_g)$ is obtained, which is private. He counted $d(G,B)$ and kept it a secret. Bob also calculates $d(G, l_{AB})$ and sends it to Alice.

(3) After the exchange of $d(H, l_{BC})$ and $d(G, l_{AB})$ (according to Remark 2.5), Bob and Alice can form the same private key i.e.

$$K_{Alice} = \left\lfloor d(H,B)d(G,l_{AB}) \right\rfloor = \left\lfloor 2L_{\Delta ABC} \right\rfloor = \left\lfloor d(G,B)d(H,l_{BC}) \right\rfloor = K_{Bob} \tag{7}$$

3.2 *Message Encryption and Description*

Alice and Bob can use any operation for the encryption and decryption process. However, the focus of the proposed algorithm is on the security of the key generation algorithm.

4. Hacking Attack Analysis

Hackers can use the information from the lines $l_{AB}: a_1x + b_1y + c_1 = 0$ and $l_{BC}: a_2x + b_2y + c_2 = 0$ equations. They can also calculate $d(H,B) = k_1\sqrt{a_1^2+b_1^2}$ and $d(G,B) = k_2\sqrt{a_2^2+b_2^2}$ with $k_1, k_2 \in \mathbb{R}$.

4.1 Case 1

Hacker counts $K_{Alice} = \lfloor d(H,B)d(G,l_{AB}) \rfloor = k_1\sqrt{a_1^2+b_1^2}.d(G,l_{AB})$ or $K_{Bob} = \lfloor d(G,B)d(H,l_{BC}) \rfloor = k_2\sqrt{a_2^2+b_2^2}.d(H,l_{BC})$. Note that hackers may know $d(G,l_{AB})$ or $d(H,l_{BC})$. However, k_1 or k_2 is unknown, so hackers must do a brute force attack step.

4.2 *Case 2*

Hacker working on $d(H,l_{BC})$ and $d(G,l_{AB})$. Let us suppose a hacker does $d(H,l_{BC})$. It knows that $d(H,l_{BC}) = \frac{|a_2x_h+b_2y_h+c_2|}{\sqrt{a_2^2+b_2^2}}$. Notice that $d(H,l_{BC})$ and $\sqrt{a_2^2+b_2^2}$ are known, but the hacker still has a hard time guessing the point $H(x_h, y_h)$. The same thing happens if the hacker works on $d(G,l_{AB})$.

4.3 *Case 3*

Hackers find the angle formed by l_{AB} and l_{BC} intersecting at point $B(x_b, y_b) \in \mathbb{R}^2$. They use point $A(x_a, y_a), C(x_c, y_c) \in \mathbb{R}^2$ to form vectors $BA = \vec{u}$ and $BC = \vec{v}$. Next, the hacker calculates $\cos\alpha = \frac{u.v}{|u|\ |v|}$.

Using the Pythagorean equation, hackers can find $\sin\alpha$. Hacker can calculate

$$K = \lfloor 2L_{\Delta} \rfloor = d(H,B).d(G,B)\sin\alpha = k_1k_2\sqrt{a_1^2+b_1^2}\sqrt{a_2^2+b_2^2} \tag{8}$$

Hacker cannot find *K* because there are still unknown variables k_1 and k_2.

5. A Toy Example

Alice and Bob agree to choose any point $B(-1,5)$. They agree to choose any two points $A(3,-1)$ and $C(-2,1)$. They form the equations of the lines $l_{AB}: 3x+2y-7=0$ and $l_{BC}: 4x-y+9=0$. All these parameters are public.

(1) Alice will determine any point $H \in \mathbb{R}^2$ that lies on the equation of the line $l_{AB}: 3x+2y-7=0$. She chooses any $x_h = 1055$ so that $H(1055;-1579)$ is obtained, which is private. She counted $d(H,B) = \sqrt{(-1-1055)^2+(5+1579)^2} = 1903,731$ and kept it a secret. Alice also calculates $d(H,l_{BC}) = \frac{|4.(1055)-(-1579)+9|}{\sqrt{4^2+(-1)^2}} = 1408,647$ and sends it to Bob.

(2) Bob will determine any point $G \in \mathbb{R}^2$ that lies on the equation of the line $l_{BC}: 4x-y+9=0$. He chooses any $x_g = -345$ so that $G(-345;-1371)$ is obtained, which is private. He counted $d(G,B) = \sqrt{(-1+345)^2+(5+1371)^2} = 1418,348$ and kept it a secret. Bob also calculates $d(G,l_{AB}) = \frac{|3.(-345)+2(-1371)-7|}{\sqrt{3^2+2^2}} = 1049,493$ and sends it to Alice.

(3) After exchanging $d(H,l_{BC})$ and $d(G,l_{AB})$, Alice generates the private key

$$\begin{aligned} K_{Alice} &= \lfloor d(H,B)d(G,l_{AB}) \rfloor \\ &= \lfloor (1903,731).(1049,493) \rfloor \\ &= \lfloor 1997952,358 \rfloor \\ &= 1997952 \end{aligned} \tag{9}$$

and Bob generates

$$\begin{aligned} K_{Bob} &= \lfloor d(G,B)d(H,l_{BC}) \rfloor \\ &= \lfloor (1418,348).(1408,647) \rfloor \\ &= \lfloor 1997951,655 \rfloor \\ &= 1997952 \end{aligned} \tag{10}$$

Let's say that Alice has a message $P = [12 \quad 12345 \quad 5 \quad 123]$.. Alice and Bob agree to use encryption $C = E(P) = P + K$ and decryption

$P = D(C) = C - K$. Bob and Alice's encryption and decryption are very easy to do.

6. Hacking Experiment

Hackers can use the information from the lines $l_{AB} : 3x + 2y - 7 = 0$ and $l_{BC} : 4x - y + 9 = 0$ equations. They can also calculate $d(H,B) = k_1\sqrt{13}$ and $d(G,B) = k_2\sqrt{17}$ with $k_1, k_2 \in \mathbb{R}$.

6.1 *Case 1*

Hacker counts $K_{Alice} = \lfloor d(H,B)d(G,l_{AB}) \rfloor = k_1\sqrt{13}.(1049,493)$ or $K_{Bob} = \lfloor d(G,B)d(H,l_{BC}) \rfloor = k_2\sqrt{17}.(1408,647)$. However, k_1 or k_2 is unknown, so hackers must do a brute force attack step.

6.2 *Case 2*

Hacker working on $d(H,l_{BC})$ and $d(G,l_{AB})$. Let us suppose a hacker does $d(H,l_{BC})$. It knows that $d(H,l_{BC}) = \frac{|4x_h - y_h + 9|}{\sqrt{17}} \Leftrightarrow 1408,647\sqrt{17} = |4x_h - y_h + 9|$. Notice that $d(H,l_{BC})$ and $\sqrt{a_2^2 + b_2^2}$ are known, but the hacker still has a hard time guessing the point $H(x_h, y_h)$. The same thing happens if the hacker works on $d(G,l_{AB})$.

6.3 *Case 3*

Hackers find the angle formed by l_{AB} and l_{BC} intersecting at point $B(-1,5)$. They use point $A(3,-1)$ and $C(-2,1)$ to form vectors $BA = \vec{u} = \begin{pmatrix} -6 \\ 4 \end{pmatrix}$ and $BC = \vec{v} = \begin{pmatrix} -4 \\ -1 \end{pmatrix}$. Next, the hacker calculates $\cos\alpha = \frac{u.v}{|u||v|} = \frac{20}{2\sqrt{13}\sqrt{17}}$ $\Leftrightarrow \sin\alpha = \frac{22}{2\sqrt{13}\sqrt{17}}$.

Hacker can calculate

$$K = \lfloor 2L_{\Delta} \rfloor = d(H,B).d(G,B)\sin\alpha = k_1k_2\sqrt{13}\sqrt{17}\,\frac{22}{2\sqrt{13}\sqrt{17}} = 11k_1k_2 \qquad (11)$$

Hacker cannot find K because there are still unknown variables k_1 and k_2.

7. Conclusion

This study develops a public key cryptosystem using the concept of geometry on the area of a triangle. We can show that the proposed public key cryptosystem works well. Furthermore, mathematical hacking experiments carried out by hackers are complex because the public key cryptosystem works on a ring of real numbers.

Disclosure statement

The author reported no potential conflict of interest.

References

[1] D. Ezhilmaran and V. Muthukumaran, "Key Exchange Protocol Using Decomposition Problem In Near Ring," *Gazi Univ. J. Sci.*, vol. 29, no. 1, pp. 123–127 (2016).

[2] A. V. N. Krishna, A. H. Narayana, and K. M. Vani, "A Novel Approach with Matrix Based Public Key Cryptosystems," *J. Discret. Math. Sci. Cryptogr.*, vol. 20, no. 2, pp. 407–412 (2017).

[3] M. Andrecut, "A Matrix Public Key Cryptosystem," *https://arxiv.org/abs/1506.00277v1*, pp. 1–18 (2015).

[4] Z. Y., E. Luy, and B. Gonen, "Public Key Cryptosystem based on Matrices," *Int. J. Comput. Appl.*, vol. 182, no. 42, pp. 47–50 (2019).

[5] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public Key Exchange Using Matrices Over Group Rings," *Groups, Complexity, Cryptol.*, vol. 5, no. 1, pp. 97–115 (2013).

[6] M. Yumman, T. Shah, and I. Hussain, "Asymmetric Cryptosystem on Matrix Algebra over a Chain Ring," *Symmetry (Basel).*, vol. 13, no. 1, pp. 1–11 (2021).

[7] M. Zeriouh, A. Chillali, and A. Boua, "Cryptography Based on the Matrices," *Bol. Soc. Paran. Mat*, vol. 3, no. 3, pp. 75–83 (2019).

[8] J. Liu, H. Zhang, and J. Jia, "Cryptanalysis of Schemes Based on Polynomial Symmetrical Decomposition," *Chinese J. Electron.*, vol. 26, no. 6, pp. 1139–1146 (2017).

[9] J. Liu, H. Zhang, J. Jia, H. Wang, S. Mao, and W. Wu, "Cryptanalysis of an Asymmetric Cipher Protocol Using a Matrix Decomposition Problem," *Sci. China Inf. Sci.*, vol. 59, no. 5 (2016).

[10] P. M. Sree Parvathi and C. Srinivasan, "Matrix Lie Group as an Algebraic Structure for NTRU Like Cryptosystem," *J. Discret. Math. Sci. Cryptogr.*, vol. 23, no. 7, pp. 1455–1464 (2020).

[11] M. Maxrizal, "Public Key Cryptosystem Based on Singular Matrix," *Trends Sci.*, vol. 19, no. 3, p. 2147 (2022).

[12] M. Helal Ahmed, J. Tanti, and S. Pushp, "A Public Key Cryptosystem Using Cyclotomic Matrices," *Coding Theory - Recent Adv. New Perspect. Appl. [Working Title]*, pp. 1–9 (2021).

[13] M. Kumari, "A model of Public key cryptography using multinacci matrices," https://arxiv.org/abs/2003.08634v1, pp. 1–12 (2020).

[14] Christoph Capellaro, "Design of Ciphers based on the Geometric Structure of the Laguerre and Minkowski Planes," https://arxiv.org/abs/2103.04428v1, pp. 1–20 (2021).

[15] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi, and R. M. Zulqarnain, "A Novel Image Encryption Technique Based on Mobius Transformation," *Comput. Intell. Neurosci.*, pp. 1–14 (2021).

[16] A. Dua and A. Dutta, "A study of applications based on elliptic curve cryptography," *Proc. Int. Conf. Trends Electron. Informatics, ICOEI 2019*, vol. 0, no. Icoei, pp. 249–254 (2019).

[17] L. D. Singh and K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography," *Procedia Comput. Sci.*, vol. 54, no. 1, pp. 73–82 (2015).

[18] D. Di Tullio and A. Pal, "A New Method For Geometric Interpretation Of Elliptic Curve Discrete Logarithm Problem," https://arxiv.org/abs/1909.08901v1, pp. 1–10 (2019).

[19] P. Sundarayya and G. Vara Prasad, "A public key cryptosystem using Affine Hill Cipher under modulation of prime number," *J. Inf. Optim. Sci.*, vol. 40, no. 4, pp. 919–930 (2019).

[20] C. Meshram and X. Li, "New efficient key authentication protocol for public key cryptosystem using DL over multiplicative group," *J. Inf. Optim. Sci.*, vol. 39, no. 2, pp. 391–400 (2018).

Received September 2022