MATHEMATICAL SPECULATIONS ON CRYPTOGRAPHY

Anjali C B
Karnataka State Open University
Bangalore, 560066
anjalicb99@gmail.com

June 10, 2024

ABSTRACT

Abstract: The current cryptographic frameworks like RSA, ECC, and AES are potentially under quantum threat. Quantum cryptographic and post-quantum cryptography are being extensively researched for securing future information. The quantum computer and quantum algorithms are still in the early developmental stage and thus lack scalability for practical application. As a result of these challenges, most researched PQC methods are lattice-based, code-based, ECC isogeny, hash-based, and multivariate crypto schemes. In this paper, we explore other mathematical topics such as stereographic projection, Mobius transformation, change of basis, Apollonian circle, Binary Quadratic form equivalence, Gauss composition law, and its conjunctions. It fulfills preliminary conditions like bijection, primality, and np-hard problems, and the feasibility of one-way functions along with its interconnection. Thus allowing the exploration of new realms of mathematics for the development of secure protocols for future communication.

Keywords: RSA, ECC, AES, PQC, Stereographic Projection, Mobius Transformation, Apollonian Circle, Descartes Quadruple, Change of Basis, BQF Equivalence, Gauss Composition Law, Cryptography

1 Introduction

Cryptography is the method used for securing sensitive information using mathematical techniques and coding algorithms in a way that only authenticated users can decipher the information for the use of data. It ensures the information transmitted is secure, private, confidential, and accessible solely by intended recipients. The features of cryptography include confidentiality, integrity, authentication, non-repudiation, and key management. Cryptography should be efficient, flexible, resistant to attacks, and secure. Even though not mandatory, most modern cryptography frameworks are based on a way to function with a trapdoor. Thus, facilitating easy encryption and decryption for the user with knowledge of the trapdoor function and challenges in the absence of it.

2 Types of Cryptography

The three types of classification of cryptography are symmetric, asymmetric, and hash functions. Symmetric encryption is when both sender and receiver share the same secret key, there are mainly two types of symmetric encryption such as block ciphers and stream ciphers. The most used of these is AES, it is considered secure even against quantum attacks as of current knowledge if the key size is large enough. However, the disadvantage here is the need to transmit the secret key causing concerns of attacks. It is widely used for Bulk messages. Asymmetric encryption is one of the most used and reliable cryptography. The most used of these are RSA and ECC. They are efficient but currently under quantum threat. Hash functions are typically non-invertible conversions of data where the hashed functions are employed for data integrity verification and authentication.

3 Requirements of cryptography

The most used math in cryptography is modular arithmetic, number theory, and abstract algebra due to ease of solving, and extensive research availability. The current focus is also being shifted toward algebraic geometry. The security frameworks also encompass pre-image resistance, and collision resistance, maintain pseudo randomness, should be computationally complex to withstand attacks, and mathematically hard to crack. The conditions for the framework to be potentially sound for asymmetric encryption are it needs to be quantum attack resistant, mathematically hard, one-way function which is easier in one direction but computationally complex the other way without trapdoor function, bijective mapping, resistance against backdoor attacks, cryptanalysis resistant, efficient, secure and scalable.

4 Classical Cryptography

4.1 Advanced Encryption Standard

Advanced Encryption Standard [1] was published by NIST in 2001. It is a symmetric key algorithm that uses a block cipher. AES currently has 3 key lengths being used: 128 bits with 10 rounds, 192 bits with 12 rounds, and 256 bits with 14 rounds. The message is divided into 128-bit blocks and the key is further used to create 10 subkeys each of 128 bits. The four main steps involved are byte substitution where data is replaced by the data from the s-box, shift rows are left shifting the rows of the matrix, mix columns are multiplied by a standard AES specified matrix, add round key is done by XORing the array with 128-bit round key. All the operations are done in a finite field. As of current advancement increasing the key length of AES would make it withstand the quantum threat.

4.2 RSA Encryption

RSA [2] is classical cryptographic framework which was published in 1977. It is based on the difficulty of factoring large numbers. The mathematical formulation can be concisely given as:

$$n = p \times q \tag{1}$$

$$\phi(n) = (p-1) \times (q-1) \tag{2}$$

$$Choose\, e\, such\, that\, 1 < e < \phi(n) \tag{3}$$

$$\gcd(e, \phi(n)) = 1 \tag{4}$$

$$e \times d \equiv 1 \pmod{\phi(n)} \tag{5}$$

$$Cipher = Message^e n \tag{6}$$

$$Message = Cipher^d n \tag{7}$$

RSA is the most widely used algorithm currently due to its performance efficiency and simplicity. The key size is generally 1024 or 2048 bits. The process of period-finding using the Quantum Fourier Transform is used in Shor's algorithm. The Quantum Fourier transform takes some function f(x) and finds out the period of the function. This method is believed to be able to factor large numbers efficiently compared to classical algorithms but currently is not capable of scaling to potential due to qubit limitation.

4.3 Elliptic curve cryptography

ECC [5] is considered more secure along with the very short key size, the 256-bit ECC is said to be equivalent to the strength of a 3072-bit RSA key size but not over AES key size. This is very similar to the Diffie-Hellman discrete logarithm. ECC uses point addition of elliptic curve over finite field abelian group for encryption. It requires one-sixth of the computational effort of RSA to provide the same security and is 15 times faster than the same. ECDH and ECDSA are widely used in blockchain cryptography and others. The practical applicability of quantum algorithms is currently limited to quantum system scaling difficulties but concern about the future advancement exists.

5 Quantum Cryptography

Quantum computers [3] are believed to offer certain advantages over classical such as being able to compute certain specific classes of NP and NP-Hard problems in polynomial time due to their superposition, quantum parallelism, quantum entanglement, and other physical properties. Assuming fundamental principles of physics like superposition and entanglement are valid, it could be used efficiently in quantum cryptography for secure communication. QKD resists eavesdropping to an extent as it causes disturbance in the medium which could be detected, though it is not completely immune to eavesdropping the risks could be mitigated. Its no-cloning theorem which does not allow duplicate the unknown state to be copied perfectly is an added advantage. QKD [4] is considered very secure and implemented, extensive deployment is under research and is considered currently a very promising avenue.

6 Post-Quantum Cryptography

Post-quantum cryptography is the term coined to represent the crypto schemes that are capable of being secure under quantum and classical threats [6]. Numerous research is being done on exploring different possibilities to tackle the problem of quantum threats. The most prominent asymmetric encryptions are as follows

6.1 Lattice-based cryptography

The lattice is based on the shortest or closest vector problem which is considered np hard [7]. The problem on the lattice is considered np-hard but due to its periodic structure and Fourier transformation being the advantage of quantum computers, various methods are being researched to break it. An extension of Shor's algorithm is said to be capable of breaking the hardness of a few lattice problems. Due to its richness lattice is the most widely researched PQC method.

6.2 Code-based cryptography

It is also known as error-correcting code cryptography, is based on the error-correcting principle and difficulty of decoding random linear codes. For example, a 64-bit key is stored in 72-bit physical memory, it is designed in such a way that it would be system would be able to detect single-bit or double-bit errors and rectify them.

6.3 Hash-based cryptography

hash-based signature relies on the fact that the pre-image detection from the given hashed function is difficult. The conditions for using signatures are that it should not be repeated, the signer must know the function and thus the hashed function could be verified by the receiver. It should be a time function. Grover's algorithm does affect the hash-based function due to its search time reduction.

6.4 Multivariate quadratic polynomial cryptography

In the given finite field, finding a set of polynomials of n variables even for smaller degrees is difficult [9]. But checking if the function belongs to the set is easier but finding the solution of the function from the set is infeasible without the private key.

6.5 Super-singular ECC isogeny cryptography

Elliptic curves are a very rich field with a vast amount of research done. Elliptic curves are defined over a finite field with the ideal fractional class group that can act freely on them [10]. Using the relation between prime isogenies and ideal the protocol is built which is considered safe against quantum threats. The security relies on the isogeny path problem. Research in these areas to develop robust cryptographic schemes capable of withstanding quantum threats are being explored.

7 Mathematical Cryptography Core Ideas

In the vastness of mathematics, there are many more promising avenues than the previously listed one, which could be explored for utilization in post-quantum cryptography. A few of the topics which are listed below. Here, we try to summarize the topics related to algebraic geometry, linear algebra, and algebraic number theory and the intersection of the concepts along with the relation between them.

7.1 Change of Basis

Consider the transformation of matrix A from basis a1,a2 and matrix B in basis b1,b2. A transformation matrix can be used to transform data from one basis to another. Analogously, Alice represents matrix A, speaking a language only she understands, while Bob represents matrix B, speaking a different language that only he understands. The transformation matrix could be considered as the mathematical translator between Alice and Bob which could allow communication from Alice's basis to that of Bob. Similarly, its inverse allows communication from Bob back to Alice.

Definition 1: Let V be any vector space [11], and let $A = \{v_1, v_2, v_3, ..., v_n\}$ be a set of vectors in V. A is called a basis of V if A is linearly independent and V is the span of A. The vector a in V is represented as:

$$a = c_1v_1 + c_2v_2 + ... + c_nv_n$$

Scalars $c_1, c_2, ..., c_n$ are called coordinates of V relative to basis A, denoted by $[v]_A = [c_1, c_2, ..c_n]$.

Definition 2: If $A = \{v_1, v_2, \ldots, v_n\}$ is a basis of vector space V, then $A^* = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ is a basis of V^*. The functional $\varphi_i(c_1v_1 + \ldots + c_nv_n)$ is an element of the dual basis. A vector v belongs to V, where c_i are elements of F for $i = 1, \ldots, n$. i.e., $\varphi_i(v_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta. Any functional φ can be written as a linear combination of the dual basis vectors, i.e., $\varphi = \varphi(v_1)\varphi_1 + \varphi(v_2)\varphi_2 + \ldots + \varphi(v_n)\varphi_n$.

Definition 3: Let V be any vector space of dimension n over any field F. Let $A = (v_1, v_2, v_3, \ldots, v_n)$ and $B = (w_1, w_2, w_3, \ldots, w_n)$ be any two bases of V over F, and let $A^* = (\Phi_1, \Phi_2, \Phi_3, \ldots, \Phi_n)$ and $B^* = (\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n)$ be their respective dual bases of V^* over F.

Let P be the change of basis matrix [12] from the basis A to the basis B, and set $Q = P^{-1}$. Then $Q(\Phi_1, \Phi_2, \Phi_3, \ldots, \Phi_n) = (\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n)$.

$$QA^* = B^* \tag{8}$$
$$A^* = Q^{-1}B^* \tag{9}$$
$$A^* = PB^* \tag{10}$$
$$AA^* = APB^* \tag{11}$$
$$B \cdot C = (\sigma_1(c), \sigma_2(c), ..., \sigma_n(c)) \tag{12}$$
$$u = AA^* \cdot u \tag{13}$$
$$u = APA^* \cdot u \tag{14}$$
$$Public\,key\,:B^*, where\,u\,is\,plaintext. \tag{15}$$
$$\sigma^* = (\sigma_1(u), \sigma_2(u), ..., \sigma_n(u)) \tag{16}$$
$$Private\,key\,:AP\sigma^* \cdot u = u \tag{17}$$

This understanding of change of basis can be crucial in various cryptographic algorithms and mathematical frameworks for future exploration. But Matrix multiplication is considered computationally intensive if the number of matrices increases. Also, tensor which could be considered as n-dimensional matrices has many np-hard problems.

7.2 Stereographic Projection

Stereographic projection is a type of conformal linear transformation where circles from a sphere are mapped as circles or as straight lines on a tangent plane. The angles and cross ratios are preserved locally under the transformation but the distances are distorted [13]. Any point is its own harmonic conjugate concerning itself and any other point. The projection and inverse projection here are bijective, thus preventing pre-image resistance and collision resistance. The circle passing through the north pole is the only straight line in the plane. Stereographic projection of a complex plan onto a sphere constructs Mobius transformation [14]. It can be represented by

$$M(z) = \frac{az + b}{cz + d} \tag{18}$$

Inverse Mobius transformation:

$$M^{-1}(z) = \frac{dz - b}{-cz + a} \tag{19}$$

$$Given\,M_1(z) = \frac{a_1z + b_1}{c_1z + d_1}\,and\,M_2(z) = \frac{a_2z + b_2}{c_2z + d_2} \tag{20}$$

$$composition\,M = M_2 \circ M_1\,is\,: \tag{21}$$

$$M(z) = M_2\left(\frac{a_1 z + b_1}{c_1 z + d_1}\right) = \frac{a_2(a_1 z + b_1) + b_2(c_1 z + d_1)}{c_2(a_1 z + b_1) + d_2(c_1 z + d_1)} \tag{22}$$

Expanding the terms, we have:

$$M(z) = \frac{(a_2 a_1 + b_2 c_1)z + (a_2 b_1 + b_2 d_1)}{(c_2 a_1 + d_2 c_1)z + (c_2 b_1 + d_2 d_1)}$$

(23) Thus, the composed transformation $M(z) = M_2(M_1(z))$ has the form:

$$M(z) = A_1 z + \frac{B_1}{C_1 z + D_1} \tag{24}$$

where:

$$A_1 = a_2 a_1 + b_2 c_1 \tag{25}$$

$$B_1 = a_2 b_1 + b_2 d_1 \tag{26}$$

$$C_1 = c_2 a_1 + d_2 c_1 \tag{27}$$

$$D_1 = c_2 b_1 + d_2 d_1 \tag{28}$$

Set of non-singular Mobius transformation forms group under composition. Unique Mobius transformation of sending 3 points (q, r, s) to other 3 (q', r', s') points is given as:

$$M(z) = \frac{(w - q')(r' - s')}{(w - s')(r' - q')} = \frac{(z - q)(r - s)}{(z - s)(r - q)} \tag{29}$$

$$Where[w, q', r', s'] = [z, q, r, s] \tag{30}$$

For a given hyperbolic Mobius transformation M, The multiplier associated with ξ_+ is a real number $m = \rho$.

$$M'(z') = \rho z' \tag{31}$$

If A' and B' are any origin-centered circles:

$$\frac{r_B}{r_A} = \frac{radius\,of\,B'}{radius\,of\,A'} = \sqrt{\rho} \tag{32}$$

$$M' = I_{B'} \cdot I_{A'} \tag{33}$$

where $I_{A'}$ and $I_{B'}$ are inversion transformations. From the symmetry principle:

$$M = I_B \cdot I_A \tag{34}$$

To pick a pair of circles C_2 corresponding to the value of ρ, we use circles of Apollonius with limit points ξ_+ and ξ_-. For a group of Apollonian circles limit points are symmetric with respect to each of its circles.

7.3 Apollonian Circle

A fractal-like recursive arrangement [18] of four mutually tangent circles with integer curvature which obeys Descartes equation can be considered as integral Apollonius circle packing. If the given curvatures are (a, b, c, d) here $a = \pm\frac{1}{r}$ where r is the radius of the circle. The Descartes equation is given by:

$$a^2 + b^2 + c^2 + d^2 = \frac{1}{2}(a + b + c + d)^2 \tag{35}$$

Thus called as Descartes quadruple.Descartes quadruple $v = (a, b, c, d)$ with $L(v) = a + b + c + d > 0$ is a root quadruple if

$$(a \leq 0 \leq b \leq c \leq d) \, and \, (a + b + c \geq d). \tag{36}$$

The Apollonian root quadruples $(\pm n, x, y, z)$ with $\pm n \leq 0 \leq x \leq y \leq z$ is in bijection with positive definite IBQF of discriminant $-4n^2$ having a non-negative middle coefficient. The reduced BQF $[A, B, C]$ associated with it is given by:

$$[A, B, C] = [-n + x, \frac{1}{2}(-n + x + y - z), -n + y] \tag{37}$$

Primitive root quadruples are equivalent to reduced BQF in the $GL(2, \mathbb{Z})$ having a non-negative middle coefficient. A positive definite form $[A, B, C]$ is considered to be reduced if the following conditions are satisfied:

$$0 \leq |2B| \leq A \leq C \tag{38}$$

$$(-n, x, y, z) \, is \, a \, root \, quadruple \tag{39}$$

Primitivity condition $gcd(-n, x, y, z) = 1$ transforms to $gcd(A, B, C) = 1$, vice versa

Reduced forms list form classes under $GL(2, \mathbb{Z})$-action when $B \geq 0$. Circle packing is one of the NP-hard problems. Few Diophantine equations are also considered hard to solve.

7.4 Binary Quadratic Form Equivalence

Binary quadratic forms are represented as $ax^2 + bxy + cy^2$. Two binary quadratic forms f and g are said to be equivalent if the following conditions are satisfied: if they can be transformed into each other and the discriminant of them is similar [15]. IBQF is properly equivalent if g, which is a rational number, belongs to $SL(2, \mathbb{Z})$, $f^2 = g \cdot f$, here f is the positive definite form with $disc < 0$, $a \geq 0$. It is reduced if any of these qualities are true: $|B| \leq A \leq C$ or if $b \geq 0$. Both equivalences are equivalent to a single reduced form.

Gauss composition law: which states

$$f_1(x_1, y_1) \cdot f_2(x_2, y_2) = f_3(X, Y), \tag{40}$$

the group defined by Gauss can be obtained simply by considering the free group generated [16] by all primitive quadratic forms of a given discriminant D, modulo the relation $Q_{id,D} = 0$ and modulo all relations of the form

$$QA_1 + QA_2 + QA_3 = 0, where \, QA_1, QA_2, QA_3 \tag{41}$$

form a triplet of primitive quadratic forms arising from a cube A of discriminant D. Bhargava's cube as an extension of Gauss composition law:

$$A_1, A_2, A_3, B_1, B_2, B_3 \tag{42}$$

are 2×2 matrices of opposite pairs of vertices. Bhargava constructed three IBQFs as follows:

$$Q_1 = -det(A_1x + B_1y), Q_2 = -det(A_2x + B_2y), Q_3 = -det(A_3x + B_3y). \tag{43}$$

Bhargava established the following result connecting a Bhargava cube with the Gauss composition law: If a cube A gives rise to three primitive BQF Q_1, Q_2, Q_3, where Q_1, Q_2, Q_3 with identical discriminant also the product of the three forms is the identity within the Gauss composition group. Alternatively, if Q_1, Q_2, and Q_3 are any three primitive BQF of the identical discriminant whose product is the identity within the Gauss composition group then there exists a cube A producing Q_1, Q_2, Q_3.

The multiplicativity of invertible O-ideals induces a group structure on the equivalence classes of primitive integral forms. The corresponding groups are called class groups. All the equivalent reduced forms can be found in each class group and are unique. There are several existing proposals for digital signatures using quadratic forms like BR93, FS87, etc. There are a few intractable problems using BQF along with Diffie Hellman and principle ideal classes mentioned in [17]. Imaginary quadratic order and many other problems related to lattice [17] BQF are widely explored along with the potential application in multivariate polynomial frameworks in the field of post-quantum cryptography.

8 Methodology

To summarize the mutual relationship of the above-listed mathematical concepts concerning cryptography, consider an Apollonian quadruple Q1 which is composed of 4 circles c1,c2,c3, and c4 with radius r1,r2,r3, and r4 with curvatures as k1,k2,k3, and k4 respectively. They follow Descartes's equation, are primitive, and they follow conditions mentioned in eqn (35),(36),(37). When Mobius transformation with respect to a point is considered on the condition that Z must be an integer value. Mobius transformation has special properties that map circles to circles, along with the preservation of circles and angles, it also preserves tangency. Mobius transformation thus maps Q1 to Q2 in such a way that it is related by transformation T(z) as in eqn(18), whose inverse can be as given in eqn(19). Thus we get 2 quadruples Q1 and Q2 which are similar, have BQF equivalency, and also are in reduced form as they meet the necessary condition in eqn(38). Now if we were to use a simple change of basis shown in sec 7.1 where the change of basis on the transformation matrix T(z) takes place. We get a secure framework, but the applicability, and security must be rigorously analyzed. Thus combining the different concepts mentioned allows a variety of protocol options due to the richness of the topics involved and interception of these concepts along with the availability of np-hard problems and scope for one-way trapdoor function opens a realm of opportunities for further research, thus allowing us to also check the integration of various concepts of math from algebraic geometry, number theory and abstract algebra along with lattices, elliptic curves, and other conventional methods .

9 Conclusion

when the necessary conditions are satisfied, the primitive given reduced BQF is related to the stereographic projection and the Mobius transformation, which has a subtype hyperbolic Mobius transformation related to the Apollonian circle. Thus interlinking the mathematical concepts mentioned in the paper. The theoretically proposed protocol combines the strength of the transformation from the different compositions of Mobius, BQF equivalence, and change of basis. The vastness, and abundance of the insights and their interconnection allow us to explore the potential use of mathematical insights from the above concepts. Another example is if the quadruples are plotted onto the sphere and the antipodal points of the center of circles are considered where the centers to center form a cube shape, thus allowing us to apply Bharghav's cube law. The discriminant remains the same and therefore when plotted in 2d the other point is not visible. Suppose this is the case when BQF equivalence is merged with a change of basis as mentioned. Is it possible to get another cryptographic protocol? Is there any other possibility of utilizing the combinations of the above mathematical topics? In-depth investigation and extensive study are required for further exploration and gaining more insights into the potential of these concepts.

References

[1] Dworkin, M. J. (2023). Advanced Encryption Standard (AES). Retrieved from `https://doi.org/10.6028/NIST.FIPS.197-upd1`

[2] Rivest, R. L., Shamir, A., & Adleman, L. (n.d.). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.

[3] Gokhale, P. (2015, November 16). How does Shor's algorithm work in layman's terms? Retrieved from `https://example.com`

[4] An overview of Quantum Cryptography and Shor's Algorithm. (2020). *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5), 7487–7495. Retrieved from `https://doi.org/10.30534/ijatcse/2020/82952020`

[5] Hankerson, D., Menezes, A. (2021). Elliptic Curve Cryptography. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. Retrieved from `https://doi.org/10.1007/978-3-642-27739-9_245-2`

[6] Lanzagorta, M., & Uhlmann, J. (2008). Quantum Computer Science. *Synthesis Lectures on Quantum Computing*, 1(1), 1–124. Retrieved from `https://doi.org/10.2200/s00159ed1v01y200810qmc002`

[7] Micciancio, D., & Regev, O. (n.d.). Lattice-based Cryptography.

[8] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. In Nature (Vol. 549, Issue 7671, pp. 188–194). Nature Publishing Group. Retrieved from `https://doi.org/10.1038/nature23461`

[9] Goubin, L., & Yang, B.-Y. (n.d.). Multivariate Cryptography.

[10] de Feo, L. (2017). Mathematics of Isogeny Based Cryptography. Retrieved from `http://arxiv.org/abs/1711.04062`

[11] JIN, X.-Q., LIU, W.-H., LIU, X., & ZHAO, Z. (2022). An Introduction to Linear Algebra. Science Press, EDP Sciences. Retrieved from `https://doi.org/10.1051/978-2-7598-3044-2`

[12] Sharma, R.K., Shukla, W., & Ramasamy, S. (2009). A public key cryptography from linear algebra. *Shekar(New Series) INTERNATINAL JOURNAL OF MATHEMATICS*, 1(1), 23–37.

[13] Coxeter, H. S. M. (1987). Projective geometry (2nd ed.).

[14] Needham, T. (1997). Visual Complex Analysis. Oxford University Press Inc, 160–180.

[15] Bhargava, M. (2004). Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. In *Annals of Mathematics*, 159.

[16] Hartung, R. (n.d.). Computational Problems of Quadratic Forms: Complexity and Cryptographic Perspectives.

[17] Cohen, A. M., Cohen, H., Eisenbud, D., Singer, M. F., & Sturmfels, B. (n.d.). *Algorithms and Computation in Mathematics* (Vol. 20).

[18] Graham, R. L., Lagarias, J. C., Mallows, C. L., Wilks, A. R., & Yan, C. H. (2003). Apollonian circle packings: Number theory. *Journal of Number Theory*, *100*(1), 1–45. `https://doi.org/10.1016/S0022-314X(03)00015-5`