J. Integr. Sci. Technol.2025, 13(4), 1078

Article

Journal of Integrated
SCIENCE& TECHNOLOGY

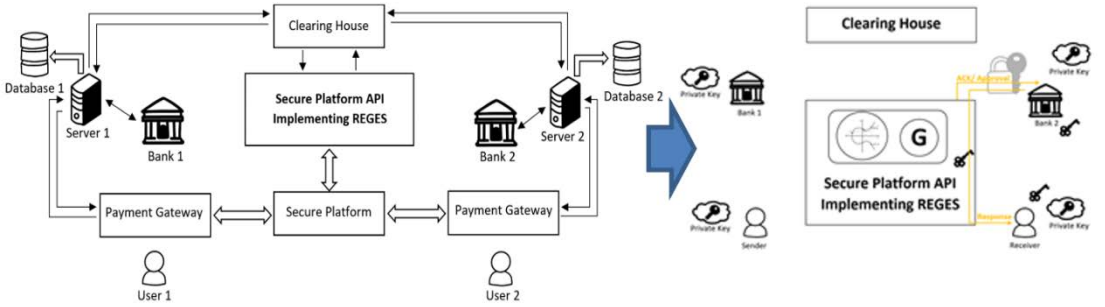
Novel protocol for secure funds transfer over the internet using rotating elliptic curve encryption standard

Dussa Lalith Kumar,[1] G.S.G.N. Anjaneyulu,[2*] V. Jalaja,[3] D. Aju[1]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore. India. [2]Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore. India. [3]Mathematics, Mohan Babu University (Erstwhile Sree Vidyanikethan Engineering College), Tirupathi. India.

Received on: 05-Sep-2024, Accepted: 28-Nov-2024 and Published on: 23-Jan-2025

ABSTRACT



The electronic fund transfer between financial institutions is known as EFT. The most common use of EFT is to have money deposited into an account electronically rather than receiving a paycheck and depositing it into a bank account. For years, cryptography has been used to protect electronic cash transactions. The existing algorithm required very large size key to achieve the optimal level of security and also more complexity in running time and this support minimum number of users, but the proposed algorithm enables superior levels of security while employing drastically small size private keys and can accommodate a large number of users with similar values for their first part of the private key, the naturally split private key enables users to store keys with ease, knowing that it's mathematically impossible to calculate second part of the private key, even when the first part is compromised and vice versa. This paper shows the mathematical model using which the algorithm can be implemented. The function and operation flow of the electronic money transfer process, as well as its security control system, are proposed in this work. This method is aimed at aiding highly secure electronic transactions between financial institutions, for instance transactions between banks, government reserves and other institutions, where such high levels of security are non-negotiable.

***Keywords**: Electronic fund transfer, Elliptic Curve, Public Key Cryptography, Three- dimensional graph, Dynamic private key.*

INTRODUCTION

Using Electronic Funds Transfer (EFT) networks, billions of dollars are transferred electronically between organizations and people every day. Transactions in EFT systems cannot be handled securely unless user identities can be verified and message transit between system nodes can be guaranteed. In today's competitive digital economy, information security is seen as one of the most pressing challenges. Electronic data interchange (EDI), direct marketing, and information retrieval are all made possible by web technologies. Electronic banking and financial services, in particular, offer enormous development potential over the Internet. Electronic money and digital cash are two of the most serious security concerns.[1] As more businesses launch interactive websites on the information superhighway, information security has become a major concern in the digital economy.[2] While the existing security protocols have been breached several times, we have developed a complete end to end protocol employing its own state of the art encryption standard and a new cryptography technique, essentially helping financial institutions make their transactions with utmost security against several cyber-attacks.[3] Cryptography is the science of keeping information private while communicating in hostile environments. Cryptography is becoming increasingly important in the modern era of information technologyand the proliferation of computer network connections.[4] To protect electronic fund transfers and classified conversations, cryptography is now commonly employed to protect data that must be conveyed and/or kept for

*Corresponding Author: G.S.G.N. Anjaneyulu
Tel: +91-9047288639; Email: anjaneyulu.gsgn@vit.ac.in

Cite as: *J. Integr. Sci. Technol., 2025, 13(4), 1078.*
URN:NBN:sciencein.jist.2025.v13.1078
DOI:10.62110/sciencein.jist.2025.v13.1078

lengthy periods of time.[5] Number theoretic or algebraic principles are used in current encryption approaches. Another paradigm that appears promisingis chaos. Chaos is a branch of nonlinear dynamics that has been extensively investigated. These unique nonlinear dynamics approach is being used to examine a wide range of applications in real systems, both man-made and natural. The chaotic behaviour of a nonlinear system is a subtle characteristic. It appears to be random. This unpredictability, on the other hand, has no stochastic cause. It is solely the consequence of the deterministic processes that define it. The extraordinary sensitivity of chaos to the system's beginning state is one of its most notable traits.

An elliptic curve has an aesthetic structure, these curves have been studied for a long time.They play a significant role in several mathematical domains today, including integer factorization,[6] number theory algorithms[7] and pseudorandom bit generation.[8] The elliptic curve cryptosystems set themselves apart from the systems based on a multiplicative group over a finite field or systems based on integer factorization because they do not employ a sub-exponential-time algorithm, for which we could find discrete logarithms in these groups.[9,10] The consequences of which are, the ability to use smaller key sizes, lower bandwidths, and quicker implementation while maintaining the same level of security, which give them a potential use in areas having limited circuit space such as mobile phones, wireless adapters, and any device employing nanochips.

The cryptosystems employ, Asymmetric cryptography, which is a cryptographic system thatuses keypairs, (a public key and a private key). The public key is shared with everyone, whilethe private key is kept a secret to an individual user. The method of asymmetric encryption allows the sender to send a message to the receiver without giving away any information abouttheir private key to the receiver and nothing about the message or the key to anyone else in theworld. Digital signatures are used to verify that a message has come from the owner of a certainprivate key and that the message (information) has not been tampered with in the journey. These asymmetric cryptosystems rely on one-way functions, which are mathematical functionsthat are easy to calculate in one direction and extremely difficult (nearly impossible) to calculate from the other direction.

As we are all aware Moore's law states that the number of transistors in a dense integratedcircuit doubles about every two years, this also gives us an insight into how fast these processors become with improving technology and more power encapsulated in the computers. These powerful computers make it possible for some one-way functions to be compromised, for example, the conventional RSA encryption using 256 bits, can be broken in a couple of hundred seconds using the modern computer, so we are having to resort to larger number of bits, which currently are around 2048 bits. These large number of bits cause slower operations, this is where the elliptic curve cryptography comes into the picture, accomplishing the task of encryption to similar extents while employing smaller key sizes.

The conventional elliptical curve systems, come with their complexities, where users cannotmake use of any random elliptic curve and any random point on it. Only some such elliptic curves can satisfy necessary conditions to be called safe and certain fixed points on these curvesare useful for encryption.[11] These include the choice of elliptic curve domain parameters such asunderlying finite field, field representation, elliptic curve, and algorithms for field arithmetic, elliptic curve arithmetic, and protocol arithmetic. These choices can be different based on the security requirements, application platform (including software, hardware and firmware), andthe constraints of the computing environment (speed of the processor, ROM, RAM, consumption of power). It is not an easy job to identify the perfect or most suitable choices, for any given scenario.

Over the last few decades, there has been a considerable amount of research on the variousaspects of elliptic curve cryptography implementation.[12] Ullah shamsher et.al., presented the challenges and applications of elliptic curve cryptogaphy.[13] The contribution of this paper is a mathematical model, that deals with the 3-dimensional form of the elliptic curves over finite fields,[14] using concepts from the Diffie-Hellman key agreement protocol[15] and employing a naturally split private key, with static and dynamic implementation techniques that help enhance the security of the algorithm whilst keeping the key sizes considerably small.[16] The paper explains choosing safe curves for the implementation. The methodology proposed works on the graphical aspects of the curve and has arithmetic procedures that have been developed specifically to operate in this cryptosystem and the signature generation and verification using modified EDCSA.

ELLIPTIC CURVE CRYPTOSYSTEM

Discrete logarithmic cryptosystems are generally considered over a multiplicative group of integers module p, where p is a prime number. These systems can be modified using specific functions to be able to work as a group of points on an elliptic curve. To achieve the asymmetriccrypto system, the Diffie-Hellman key agreement protocol has been widely used over elliptic curves. We will be using the following notation, F_q refers to the finite field of q elements, $\hat{}F_q$ refers to the algebraic closure of F_q, I_n refers to the integers modulo n, and the cardinality of a set S is referred to as ^{c}S. Assume a finite field F_q of characteristic 3, and an elliptic curve E over F_q.

CURVE AND KEY AGREEMENTS

Let us consider Alice and Bob to be our sender and receiver respectively, now they decide upon an elliptic curve, and choose a random point on that elliptic curve, which acts as a key.Both Alice and Bob have to agree in advance over a method that both of them will be using to convert the points into an integer. (This is called symmetric encryption) for easy understating let's assume they agree to take the image of the point on the x- axis. (Following a simple map from F_q to the natural numbers).

Now, we have the elliptic curve E over F_q, and G is a point on the curve, that is mutuallyagreed upon and is publicly known to everyone. Alice chooses a number and keeps it a secret to herself, this will be her private key(k_a), and calculates the point $k_a.G$, Bob chooses a numberand keeps it a secret to himself, this will be his private key (k_b), and calculates the point $k_b.G$. Alice now sends her calculated $k_a.G$ to Bob and Bob sends his calculated $k_b.G$ to Alice, both of them use this information to calculate the common key $P = k_a.k_b.G$. Alice calculates the common key by multiplying her

private key with the value received from Bob, and similarly Bob calculates the common key by multiplying his private key with the value sent by Alice, thereby we get $k_a.k_b.G = k_b.k_a.G = P$. In this process Alice did not have to share her private key k_a and neither did Bob have to share his private key k_b.

Encryption and message transmission

Let us assume that message has been embedded in E using some method that is agreed by both parties. Now Alice wants to send a message $M \in E$. As Alice and Bob have already exchanged and generated the common key. Alice makes another random choice of an integer m and calculates m.G and m.(k_b.G), by multiplying the point G with her chosen random valueand the second point by multiplying the point G with the value received from Bob. She now sends the pair of points {(m.G), (M + m.(k_b.G))}.

Encrypted Message sent: {(m.G), (M + m.(k_b.G))}.

Decryption

Bob takes the pair of points he received and multiplies the first point by his private key k, Resulting in: m.G. k_b. He then subtracts this above-calculated value from the second point he received in the pair. Bob takes the pair of points he received, and multiplies the first point by his private key k_b, Resulting in: m.G. k_b, He then subtracts this above calculated value from the second point he received in the pair Resulting in: M + m.(k_b.G)) - m.G. k_b. Leaving us with: M. That is the message which was sent by Alice.

MATHEMATICAL BACKGROUND ON ELLIPTIC CURVES

We are presenting a paper, using the following concepts, discrete mathematics, number theory,and coordinate geometry, specifically pertaining to elliptic curves and 3-dimensional geometry. Knowledge of the concepts relating to prime numbers and their applications in cryptography, the arithmetic of points on an elliptic curve, theorems on public-key cryptography like Diffie-Helman (explained in Elliptic curve cryptosystems section. (Section 2)), and other theorems like Hasse's theorem would make the understanding of the paper smooth and effective.

Referring to the previously defined notation, F_q refers to the finite field of q elements, $\hat{}F_q$ refers to the algebraic closure of F_q, I_n refers to the integers modulo n, and the cardinality of a set S is referred to as ^{c}S. Assume a finite field F_q of characteristic 3, and an elliptic curve E over F_q, is the set of all solutions (x, y) $\hat{}F_q$ x $\hat{}F_q$, to an equation $y^2 = x^3 + ax + b$ (1) where a, b F_q, and $4a^3 + 27b^2 \neq 0$, and a point at infinity referred to as ∞. Let E be an elliptic curve over a finite field F_q, then E(F_q) will denote the points in E having both their coordinates in F_q, including the point ∞. E(F_q) would be an abelian group of rank 1 or 2. [7]. We have $E(F_q) \approx C_{n1}\ C_{n2}$, where C_n denotes the cyclic group of order n, n_2 divides n_1. A theorem of Hasse states that $^cE(F_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$. The curve E, therefore, issaid to be super singular if $t^2 = 0, q, 2q, 3q,$ or $4q$, otherwise the curve is called non-super singular.

If we consider q to be a power of 2 and E to be super singular, then $^cE(F_q)$ will be odd. If weconsider q to be a power of 2 and E to be non-super singular, then $^cE(F_q)$ will even. [8]. Therefore, if q is a prime number, then for each t satisfying $|t| \leq 2\sqrt{q}$ there exists at least one elliptic curve E defined over the finite field F_q with $^cE(F_q) = q + 1 - t$ if q is a power of 2, thenfor each odd number t, satisfying $|t| \leq 2\sqrt{q}$, there exists at least one non-super singular elliptic curve E defined over the finite field F_q with $^cE(F_q) = q + 1 - t$.

Consider the illustration, [12] where we take the elliptic curve E: $y^2 = x^3 + x + 1$, over I_{23}, now $^cE(I_{23}) = 28$, $E(I_{23})$ will be cyclic, and a generator of $E(I_{23})$ is P = (0, 1). The points in $E(I_{23})$ are as follows:
{P = (0, 1), 2P = (6, -4), 3P = (3, -10), 4P = (-10, -7), 5P = (-5, 3), 6P =(7, 11), 7P = (11, 3), 8P = (5, −4), 9P = (−4, −5), 10P = (12, 4), 11P = (1, −7), 12P = (−6, −3),
13P = (9, −7), 14P = (4, 0), 15P = (9, 7), 16P = (−6, 3), 17P = (1, 7), 18P = (12, −4), 19P =(−4, 5), 20P = (5, 4), 21P = (11, −3), 22P = (7 − 11), 23P = (−5, −3), 24P = (−10, 7), 25P =(3, 10), 26P = (6, 4), 27P = (0, −1), 28P = ∞}.

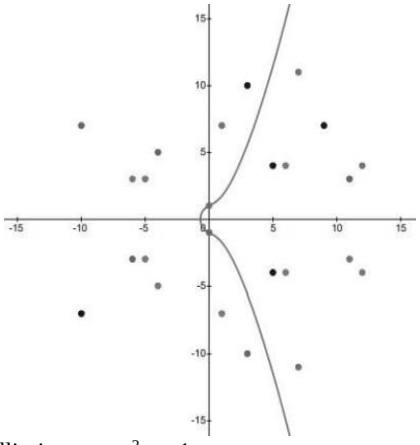


Figure 1. The elliptic curve x^3+x+1

We can now construct a group over elliptic curves. Where:

- the elements of the group are the points of an elliptic curve
- the identity element is the point ∞
- the inverse of a point P is the one symmetric about the x-axis
- addition is given by the rule: given 3 aligned, non-zero points P, Q, and R, their sumP+Q+R=0.

Note: the order of the points is not essential, that is, as long as P, Q and R are aligned, P + (Q+ R) = Q + (P + R) = R + (P + Q) = 0. This says that we have proved that the addition operator is associative and commutative. Therefore, we are in an abelian group.

Geometric Addition

The explanation above proves the group to be abelian and hence we can use P + Q + R = 0, and P + Q = - R. This equation lets us derive the geometric method to perform the sum of twopoints P and

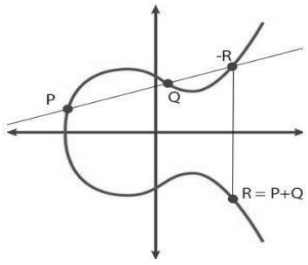


Figure 2: Addition of points on elliptic curves

Q. That is, on drawing a straight line passing through P and Q, this line will intersect the curve at a third point R. On taking the inverse of this point, we get -R (the symmetric point about the x-axis), which is the result of the addition performed. (Figure 2)

Let us now consider the edge cases:

- If P = 0 or Q = 0: We will not be able to draw a line, as 0 = ∞ is not on the xx-plane. Butas we have defined 0 as the identity element, P + 0 = P for every P.
- If P = -Q: We will have a vertical line and therefore intersect the curve in two points only.But as P is the inverse of Q, we can write P + Q = P + (-P)= 0.
- If P = Q: We will consider the tangent to the curve at that point because as we tend the points towards each other until they eventually collide the line, we get passing through them will satisfy all the conditions of being a tangent to that curve at that point. (Refer toFigure 1)

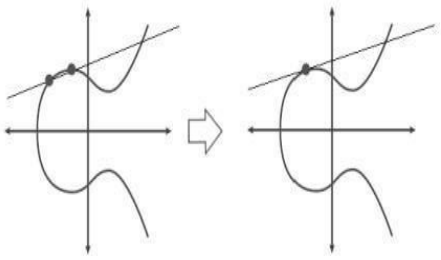


Figure 3. When the points collide (P = Q.)

If P ≠ Q and there is no third point R: We will have a tangential line in this case too, where the line passing through P and Q is a tangent to the curve. If we assume P to be the tangency point, then P + Q = -P, similarly if Q were to be the tangency point, then P+ Q = -Q.

Proof:

Let us assume (E) to be the equation and (L) to be the line passing through the points P and Q. (E) = $y^2 = x^3 + ax + b$ and (L) = $y = mx + n$. Let us take h to be a function differentiable in $x = x_p$, f is a function tangent to h in

$x = x_p$ if and only if, $f(x_p) = h(x_p)$

and hence $f'(x_p) = h'(x_p)$, now, supposing the line (L) passes only through P and Q and let h be the function of (E) and f be the function of (L): $h(x) = \pm \sqrt{(x^3 + ax + b)}$ and $f(x) = mx + n$, the intersection points are the solutions to h(x) = f(x) and therefore to

$h^2(x) = f^2(x)$ (2)

now as the intersection is supposed to happen in two points only, the cubic equation Eq.1 has a root a_1 and a double root a_2.

$$f^2(x) - h^2(x) = (x - a_1)^2(x - a_2),$$

On differentiating at a point x we get,

$$2f'(x)f(x) - 2h'(x)h(x) = (x - a_1)(2(x - a_2) + x - a_1)$$

(3)

On solving the above equation at $x = a_1$,

(1) If $h(a_1)$, $f(a_1) \neq 0$, then h is differentiable at $x = a_1$ and $f(a_1) = h(a_1)$ $f'(a_1) = h'(a_1)$

(2) If h(a) = f(a) = 0, then h is not differentiable at $x = a_1$, and we can also say that $\lim x \to a^{+}1\ h'(x) = \infty$ or $\lim x \to a^{-}1\ h'(x) = \infty$, finding the limit in (3), we get $\lim x \to a^{-}1 f'(x) = \infty$. which implies that (L) must be a vertical line at $x = a_1$, and as $h(a_1) = 0$ the curve (E) passes through the x-axis at $x = a_1$, as we already know that (E) is symmetric about thex-axis, we can conclude that (L) is a tangent to (E).

Algebraic addition

Let $P = (x_1, y_1)$ E and $Q = (x_2, y_2)$ E, and $Q \neq -P$, then $P + Q = (x_3, y_3)$. The slope of the line joining the points P and Q is given by $m = (y_2-y_1)/(x_2-x_1)$ and the equation of the line is given by $y = mx - mx_1 + y_1$, Substituting the line equation into the curve we get $(mx - mx_1 + y_1)^2 = x^3 + ax + b$, Sum of the roots = negation of the coefficient of x^2 is m^2, and hence $x_3 = m^2 - x_1 - x_2$, and the y-coordinate can be calculated by substituting into the equation of the line (PQ line), $y' = mx_3 - mx_1 + y_1$, on negating this third point (x_3, y'), which gives $y_3 = -mx_3 + mx_1 - y1$. Therefore, the sum, P + Q gives (x3, y3). where $(x_3, y_3) = (m^2 - x_1 - x_2, -mx_3 + mx_1 - y_1) \Rightarrow (x_3, y_3) = (m^2 - x_1 - x_2, (-x_3 + x_1)m - y_1)$

Scalar multiplication

We can define scalar multiplication as the repeated summation, where nP is given by, P + P +P + P +…..+ P (n times), Where n is a natural number. nP requires n additions, and if n has k digits, the operation would be $O(2^k)$ in time complexity. We use a faster method to accomplishthe same, called double and add. The double and add method essentially takes P, doubles it to get 2P and adds 2P to P, then doubles 2P to get 2^2P and so on… and add it to the result. We know that any natural number can be represented as the sum of powers of 2, thereby calculatingnP in lesser iterations while using the double and add method.

Selecting a safe elliptic curve

We realize from the discussion earlier that, not all elliptic curves are fit to be used in the elliptical cryptography. We now understand which kind of elliptic curves can be used for the sake of cryptography; we majorly require the elliptic curve E defined over a finite field F_q, to satisfy the given conditions:

- To be resistant against the Pollard ρ-attack.[17] $^cE(F_q)$ should be only by a large prime number p. (for instance, $p > 2^{150}$).
- To be resistant against the MOV reduction attack.[18] That is p should not divide q^{k-1} where $1 \leq k \leq W$, where W is sufficiently large enough to be computationallyinfeasible to find discrete logarithms in F_q.
- To be resistant to the anomalous attack[19,20] as given by Semaev, Smart, Satoh, thatsays $^cE(F_q) \neq q$.

We now discuss a few techniques for selecting safe elliptic curves.

Proposed Algorithm

Initial Setup

The following convention would be followed to present the proposed methodology, F_q refers to the finite field of q elements and $^{\wedge}F_q$ refers to the algebraic closure of F_q. I_n refers to the integers

∈

module n. The cardinality of a set S is referred to as ^{c}S, R is defined as all the real values in the range [0,180), excluding 180, and including 0. Let us assume that F_q has a characteristic greater than 3. An elliptic curve E defined over F_q, is the set of all solutions (x, y) $^{\wedge}F_q$ x $^{\wedge}F_q$ to an equation given by,

E: $y^2 = x^3 + ax + b$ (4)

where a, b belongs to F_q and $4a^3 + 27b^2 \neq 0$, and a point at infinity referred to as ∞.

Let us define a curve Eq defined over F_q, is the set of all solutions (x, y, z)$^{\wedge}F_q$ x $^{\wedge}F_q$ xF_q to an equation given by,

Eq: $z^2 = x^3 + ax + b - y^2$ (5)where a, b F_q and $4a^3 + 27b^2 \neq 0$, and a point at infinity referred to as ∞. Let us now define a curve (Eq, θ) defined over F_q, which is the set of all solutions (x, y, z, θ) $^{\wedge}F_q$ x $^{\wedge}F_q$ x $^{\wedge}F_q$ x R to an equation given by

(Eq, θ): $z^2 = x^3 + ax + b - y^2$ (6)

where a, b F_q and $4a^3 + 27b^2 \neq 0$, θ is the angle through which the x-y plane has been rotated with respect to its initial position (θ R), and a point at infinity referred to as ∞. Refer to Figure4, where we have represented the general model of the curve plotted over the x-y-z plane, to get an understanding of the concepts discussed further in this article.

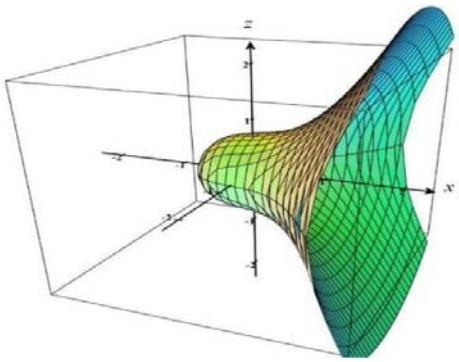


Figure 4: Representing (3) with θ at 0 degrees.

The Generator point(G):

The generator point (G) is a point of he form (x, y, 0, 0^0), of large prime order n, where(x, y) $^{\wedge}F_q$ x $^{\wedge}F_q$, where n is the max value, inside which, we will be considering our encryption valid

The Rotational dot product (‘.’)

The rotational dot product defined here is a modified version of the original dot product definedon the elliptical curve,[21] wherein we consider the numerical value (n), with an angle(θ), defined over a given curve (Eq, θ). The operation is performed by, rotating the x-y plane by anangle θ, in the anti-clockwise direction, having the x-axis as the hinge around which the rotation is performed, before dropping a dotted perpendicular onto the opposite side of the curve, fromthe point of intersection. (Similar to the original elliptical cryptography).

Graphical understanding*:* We get an elliptical curve from the point of view of the z-axis., Weperform rotation as shown in Figure 6, before dropping the dotted perpendicular from the current position of x’-y’ axis, here x’-y’ is the current position after the previous rotation has taken place.

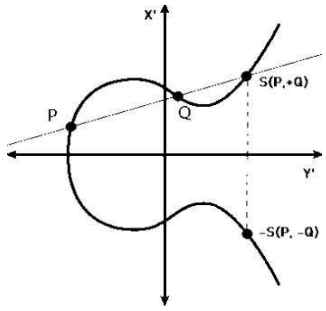


Figure 5: Representing how points are added on elliptic curves

We get a circle, from the x-axis point of view, and now we rotate x-y axis and effectively the point moves as shown below, before dropping a perpendicular.

The absence of θ can be considered as θ = 0, thereby denoting that the x-y plane is in its originalposition and has not been rotated. (In this case, all the rules of general elliptical curves and their multiplication apply as usual).[21]

Multiplication defined on rotational dot product:

Let us consider (n_a, θ_a) and (n_b, θ_b), where n_a, n_b Real numbers, and θ_a ,θ_b R. Now the rotational dot product between these points is defined as (n_a, θ_a)**.** (n_b, θ_b) = [(n_a x n_b),(θ_a + θ_b)].[21] That is the numerical value of the result is the arithmetic product or their individual numerical values and the angles get arithmetically added.

Some important properties of rotational dot product:

The rotational dot product is commutative, (n_a, θ_a)**.** (n_b, θ_b) = (n_b, θ_b)**.** (n_a, θ_a) = [(n_a xn_b),(θ_a + θ_b)].

Graphical understanding*:* The angles get added up while we perform the rotation every time,with the new numerical value, which is given by n_a x n_b, and the angle as shown below

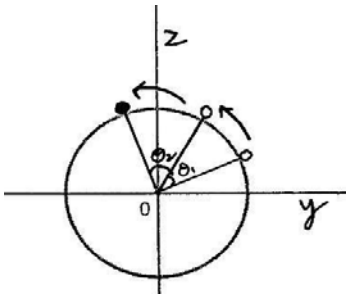


Figure 6. (Representing the angles getting added on point Multiplication)

The rotational dot product is associative, (n_a, θ_a)**.** [(n_b, θ_b)**.** (n_c, θ_c)] = [(n_a, θ_a)**.** (n_b,θ_b)]**.** (n_c, θ_c) = [(n_a x n_b x n_c),(θ_a + θ_b+ θ_c)], Where (n_c, θ_c) Real number x R.

The rotational dot product on a scalar, Let j be a scalar, where j real numbers, (n_a,θ_a)**.**j = ((n_a.j), θ_a).

real numbers, (n_a,θ_a)**.**j = ((n_a.j), θ_a).

PROPOSED CRYPTOSYSTEM

Key Generation

We are under the understanding that the curve has been defined over F_q, P is a point of primeorder N, in E(F_q); and that p is a prime number.

Private key generation (Privkey$_x$)

We employ a naturally split private key that has two distinct independent elements in it. Letus denote the key corresponding to a person x as Privkey$_x$, given by,

Privkey$_x$ = (n_x, θ) (8)

where nx [1, N-1] is the numerical part of the key, which corresponds to the number of times the iteration is performed. (Similar to the private key n used in the original elliptical curve cryptography), and θ is the angle (0, 99.99999999999999999^0) (99 followed by 17 9s in the decimal place) by which the x-y plane is rotated with the x-axis as the hinge after every iteration, in the anti-clockwise direction, here we restrict the angle to be using 19 bits and lie in the range 0 and 99.99999999999999999 both inclusive. The user chooses both values as pertheir choice, following the general rules of the cryptosystem they are following, that is making sure that they use enough bits for choosing the numerical value.

Note: θ can be used as a session dependent variable, depending on where the algorithm is beingimplemented, this would make the private key dynamic and naturally split.

Public key generation (Pubkey$_x$)

Let us denote the public key corresponding to a person x as Pubkey$_x$, given by,

Pubkey$_x$ = Privkey$_x$**.**G (Eq. 9),

that is

Pubkey$_x$ = (n_x, θ)**.**G (10)

The public key is calculated by applying the rotational dot product between the private key (n_x,θ) and the Generator point(G).

Common key generation(K)

Let us denote the common key corresponding to a set of sender and receiver as,

K$_{sender\text{-}receiver}$ = Privkey$_{sender}$**.**

Pubkey $_{receiver}$ = Privkey$_{receiver}$**.**

Pubkey$_{sender}$(11)

On simplification, using (8), we get

K$_{sender\text{-}receiver}$ = Privkey$_{sender}$**.**(Privkey$_{receiver}$**.**G) (11)

= Privkey$_{receiver}$**.**(Privkey$_{sender}$**.**G) (12)

On simplification, using (8) and (10),

K$_{sender\text{-}receiver}$ = (n_{sender}, θ_{sender})**.** ($n_{receiver}$, $\theta_{receiver}$)**.**G and hence K$_{sender\text{-}receiver}$ =(n_{sender},.$n_{receiver}$)**.**G**.**(θ_{sender} + $\theta_{receiver}$)

The common key is used to encrypt the message that the sender is trying to send to the receiver. The sender and receiver exchange their public keys, and each of them calculates the common key used for the communication between them. The sender has their private key anduses the public key of the receiver and performs a rotational dot product to calculate the common key. Similarly, the receiver has their private key and uses the public key of the senderand performs rotational dot product to calculate the common key. For simplicity of use, we will refer to the common key between a set of receiver and sender as (K).

Encryption

Let us define the process of encryption on the sender end, making use of the values and operations we have described so far, We have to generate a cipher value (the value of themessage, post encryption, which will be sent to the receiver).[22]

Process (On the sender end):

Consider the Generator point(G) and the Common key(K) corresponding to the pair ofreceiver and sender, and perform the rotational dot product between these values.

Common key(K)**.** Generator point(G) = K**.**G (13)This would act as the first part of the tuple. The point (K**.**G) can be expressed as (x_1, y_1, z_1),as we are performing this with respect to the three-dimensional system we have considered.

Consider the Public key of the receiver (Pubkey$_{receiver}$), and the Common key(K) corresponding to the pair of receiver and sender, and perform the rotational dot productbetween these values.

Public key(Pubkey$_{receiver}$)**.**Common key(K) = Pubkey$_{receiver}$**.**K (14)

Consider the message(M) to be encrypted and sent, and the above-calculated value (Eq.8);choose a mutually agreed method between the sender and receiver and add these values.

Message(M) + (Pubkey$_{receiver}$**.**K) (15)

This would act as the second part of the tuple. The point (M + Pubkey$_{receiver}$**.**K) can be expressed as (x_2, y_2, z_2), as we are performing this with respect to the three-dimensionalsystem we have considered.

Generating the Ciphertext, we couple tuple values from (13) and (15),

Cipher text = {(K**.**G), (M + Pubkey$_{receiver}$**.**K)} (16)

This will encrypt message; the sender will be sending to the receiver.

Decryption

Let us define the process of decryption on the receiver end, We are given the ciphertext, andhave to decipher the message that the sender has sent, from (16), We have,

{(K.G), (M + Pubkey$_{receiver}$**.**K)}

Process (On the receiver end):

Consider the first tuple in the ciphertext (K**.**G) and the private key of the receiver(Privkey$_{receiver}$), and perform a rotational dot product between these values.

(K.G)**.** (Privkey$_{receiver}$) (17)

Consider the second tuple in the cipher text (M + Pubkey$_{receiver}$**.**K) and the above calculated value (K**.**G)**.** (Privkey$_{receiver}$) (11), and subtract the latter from the former,

(M + Pubkey$_{receiver}$**.**K) - (K.G)**.** (Privkey$_{receiver}$)

Using associative property of the rotational dot product as discussed earlier, we can simplifythe above equation to be, (M + Pubkey$_{receiver}$**.**K) - K**.**(G**.** Privkey$_{receiver}$). Using the equation from (9) we get,(M + Pubkey$_{receiver}$**.**K) - K**.**(Pubkey$_{receiver}$)

Using commutative property of the rotational dot product as discussed earlier, we can simplifythe above equation to be,

(M + Pubkey$_{receiver}$**.**K) – (Pubkey$_{receiver}$)**.**K ,

On simplification,

M + (Pubkey$_{receiver}$**.**K – Pubkey$_{receiver}$**.**K)

We are left with, M. The message has been successfully decrypted.

Signature Generation

To sign a message M, sender performs the following (Similar to ECDSA).

We are under the understanding that the curve has been defined over F_q, and P is a point ofprime order N, in $E(F_q)$; and that p is a prime number.

(1) Select a random integer a that lies in the range [1, N - 1].
(2) Calculate the value $aP = (x_1, y_1, z_1)$, let $r = x_1$, mod N (here x_1, will be considered aninteger between 0 and q -1). If r = 0, then we perform step 1 again.
(3) Calculate a^{-1} mod N.
(4) Calculate $s = a^{-1}\{h(M) + nr\}$ mod N, where h is the Secure Hash Algorithm.[23]
(5) The signature for the message M is the pair of the values (r, s).

Signature Verification

To verify sender's signature (r, s) on the message M, the receiver must follow the below steps.(Similar to ECDSA),[21]

(1) Get the Public key corresponding to the sender $Pubkey_{sender}$.
(2) Check to see if both the integers received (r, s) lie in the range [1, N-1].
(3) Calculate $w = s^{-1}$ mod N and h(M).
(4) Calculate $u1 = h(M)w$ mod N and $u2 = rw$ mod N.
(5) Calculate $u_1P + u_2\ Pubkey_{sender} = (x_2, y_2, z_2)$ and $v = x_2$ mod N.
(6) Validate the signature only if v = r, else reject it.

Proposed Architecture

The protocol implements a 2FA (2 factor authentication), to log the users in. The protocol suggests the first authentication level to be a digital password scheme employing strong passwords, of a minimum length of 8 consisting of a sequence of alpha-numeric characters andsymbols. The second level of authentication is to be an email OTP system, where the email OTP is triggered right after the password level has been cleared. The user can successfully log onto the secure funds transfer platform only on having cleared the 2FA.

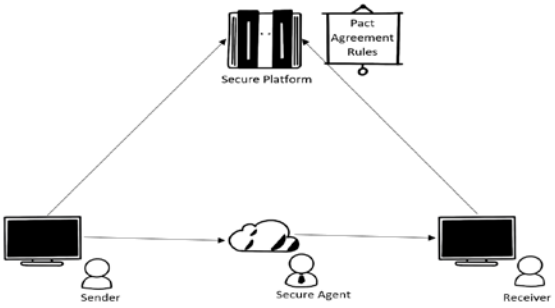


Figure 7. (A high-level view of the pact agreement.)

The Figure 8 shows the overall flow of the protocol, at a user level. The users view the protocol to be the way its shown here, Once both the sender and receiver agree to a Pact set by either of them, which is overlooked by an agent from the secure funds transfer platform.

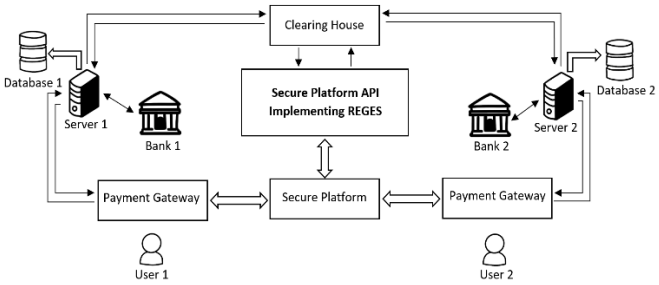


Figure 8. The Architecture diagram

The Figure 8 shows the information flow in the proposed protocol implementing REGES, wherethe platform acts as in intermediary in every step, encrypting the data using the novel cryptosystem proposed here. The detailed explanation of the process is explained in the furthersections.

Entering the Pact

The user, either the sender or the receiver when chooses to transfer funds should enter the pact,wherein they trigger an OTP to the other party by selecting them and the type of transaction. The other party will be notified about the invite and can choose to agree or deny, considering the other party agrees to the pact, they agree and enter, triggering an OTP to the initial party. These OTPs triggered are sent by phone, and the timer on the screen dies out after a certain limit. Making sure both the parties are active and in front of the screen while the deal takes place. On entering the right OTPs received on their phones, they have successfully entered the Pact.

The users can now transfer the funds over the internet using REGES (Rotating elliptic graph encryption Standard), this protocol is new and being proposed in this paper, using a novel cryptography method, which employs a naturally split dynamic private key, making it a perfectuse for the electronic funds transfer over the internet.

The Pact is overlooked by a human on the secure platform, or an automated service based on the type of the pact generated by the users. The platform makes sure the service or goods have been successfully exchanged before agreeing to transfer the funds. Once the agreement is received, the users and their respective banks undergo the transaction employingthe REGES.

The respective elliptic curve(E) and the Generator point(G) are given by the platform to both the users and both their banks, so they can generate their respective public keys. The encryption protocol requires the exchange of public keys in order to calculate the common keythat is used to encrypt the data. There are 3 exchanges that take place.[24]

- Between the sender and their respective bank.
- Between the sender's bank and the receiver's bank.
- Between the receiver and their respective bank.

We implement a handshake protocol, to make sure a connection is established first and then, their respective public keys are exchanged.

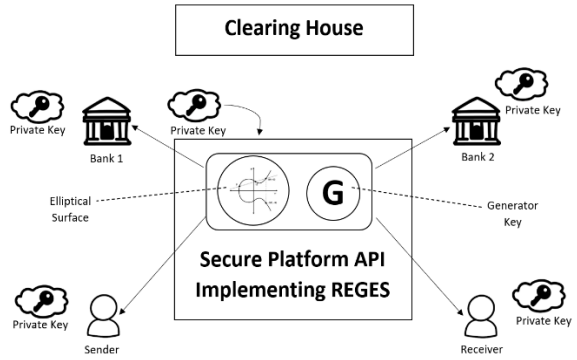


Figure 9. Broadcasting Elliptic surface and Generator point)

The private keys of each party here are session dependent as the second part of the private key is dynamic and should be chosen at the time of the transaction, the users can choosetheir private key's second part right before entering the pact, and the banks can choose to use a pseudo random algorithm to generate random values for the second part of the private key.

There are 3 communications that will take place now, based on the REGES, the communication between the sender and their bank is carried out with the secure platform's APIat its centre, wherein the authenticity of the transaction message is kept secure as the protocoldemands REGES, which is technically infeasible to break or intercept as, without being able to decrypt all the 3 private keys any hacker cannot intercept the transaction or modify anything.A message acknowledgment is always sent back to the secure platform post every communication attempt to recheck the integrity of the messages, as the secure platform has both the public keys, the platform performs a membership check and signature checking of themessages being transferred.

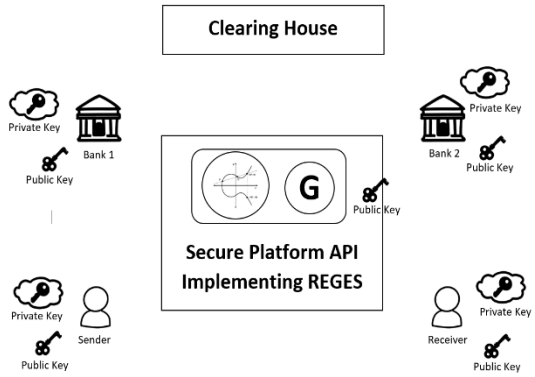


Figure 10. Entities in the transaction

The first message is transferred between the sender and their bank, through the secure platform, the user accesses their bank and sends a request to transfer a certain amount of fundsto the desired destination account. The secure platform crosschecks the data, the amount and the destination by signature verification and lets the message pass through or deny.

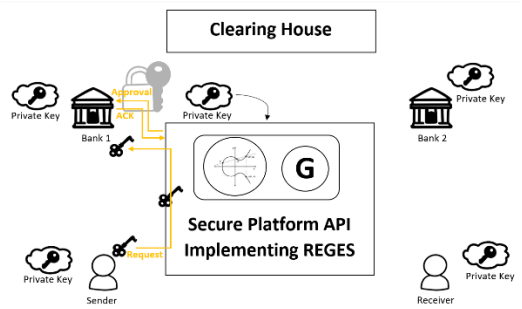


Figure 11. Transaction between sender and sender's bank

The second message is transferred between the sender's bank and the receiver's bank, through the secure platform, the message is sent, and an acknowledgment is sent back to the secure platform, the platform on verifying the messages sends an agreement message back to the bank servers to agree to the request. The banks can now process the transaction. The happens with the clearing house as in intermediate, the agreement response is directly sent to the clearing house.

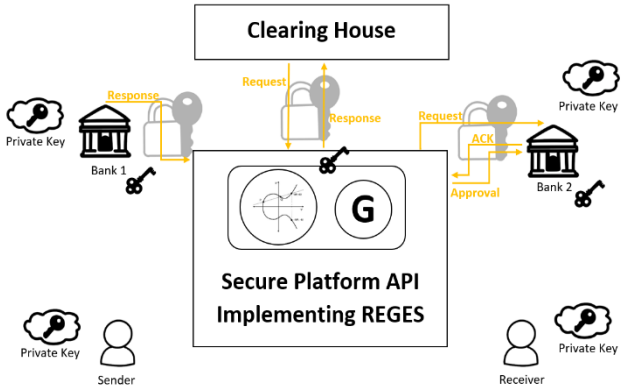


Figure 12. Transaction between sender's bank and receiver's bank.

The third message is transferred between the receiver and the receiver's bank, the receiver then gets a notification about the amount being transacted and then anacknowledgment is sent back to the secure platform, where the final amount is cross-checked as per the pact signed and is verified and is processed, the receiver has no say to deny this request, as they have already signed the pact. The funds transaction approval is sent to the bank.

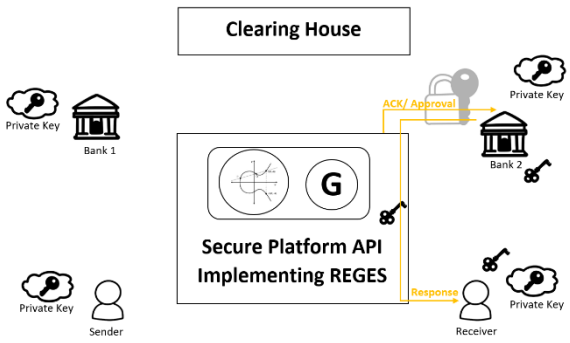


Figure 13. Transaction between receiver's bank and receive

The secure transaction is now complete.

Exiting the Pact

The transaction once completed, and the Pact successfully kept. The users can exit the session,their public keys are deleted from the secure platform, and they can choose a new value for their secondary part of their own private keys. The elliptic surface generated, and the Generatorpoint are discarded by the platform. The transaction is written onto a ledger, which is publiclyvisible to everyone (the values are encrypted using REGES). The ledger is updated and the session is terminated once and for all.

SECURITY ANALYSIS

Let us discuss how our proposed method stands strong against some very well know attacks performed by hackers and attackers. Let us also consider a situation where, we are implementing the algorithm using its dynamic version of the private key, that implies after every session [a session is a time frame between two parties used in online communication], the θ can be reset to a new value, giving the hacker absolutely no power over the next session, even if they somehow got their hands onthe previous version of the private key. Let us assume a key size of n for the following section.Listed below are few of these attacks.

Man in the Middle Attack (Replay)

This attack happens when the hacker places themselves between the communication of the receiver and the sender. Specifically, the Relay attack occurs when an attacker attempts to intercept and save old messages and tries to send them later, impersonating one of the parties.We have the Signature verification algorithm, using which both the parties can be very sure that the message has been signed by the right person and can easily figure out if the signature verification fails. If we choose to consider the dynamic key approach, it becomes even harderfor the attacker to be able to forge signatures, as all his work would go to vein, when a new session is initiated.

Parameters targeted: Cipher text => {(K.G), (M + $Pubkey_{receiver}$.K)}

Statistical Strength: Attacker needs to decode n elements of the key in the conventional approach. If we implement the dynamic key approach, the attacker on having decoded the (n-19) still has to decode the 19 bits that correspond to the theta(θ), which keep changing post every session. Technically this gives the attacker no possible way to confirm that the (n-19) bits he has decoded are valid, as the key can only be used as a whole (using all n bits).On somehow decoding the (n-19) bits, the attacker still has to decode out of 19^9 possibilities.

Brute Force Attack

This is a type of password attack, where the attacker uses the methos of rando guessing to try different private keys and hope to succeed. We have an immense number of possibilities, to brute force all keys, but the inherent implementation of the algorithm requires the interventionof both the parties to get your messages encrypted, so unless the attacker gets access to at leastone of the parties or is acting at the party themselves, it would still be very difficult to try out so many passwords involving the other to be agreeing to keep validating multiple attempts of wrong signature verifications. On considering the dynamic approach, this approach to hack into the system becomes even more difficult as the attack would have to go through all this effort just to find out the new θ all over again.

Parameters targeted: Private key => $Privkey_x = (n_x, \theta)$

Statistical Strength: Attacker on stealing one part of the private key has no theoretically possible way to mathematically compute the other part of the key (either the n_x from θ or vice versa), making it extremely secure. The dynamic approach keeps the attacker continuously making attempts for every new session which is infeasible as it would take around 7 years to compute the 19 bits of θ. (19^9 possibilities).

Dictionary Attack:

This is a type of password attack, where an attempt is made to copy an encrypted file that contains the private key and apply the same encryption to a dictionary of commonly used private keys and compare the results. The implemented of the algorithm does not allow for such an attack, even if the attacker gets a file having the encrypted private keys, they cannot perform the encryption with only a single party involving in the process, now assuming the private key has been stored using a differently encrypted file, the attacker will still have to findtwo parts of the private key, that can no correlation whatsoever, so even on compromising a part of it, the attack is rendered useless. On considering the dynamic key approach, the attackerwould have no control over the system, even after an element of the key has been compromisedas the user would use a session dependent θ, and hence the attack has no control over it.

Parameters targeted: Cipher text => {(K.G), (M + $Pubkey_{receiver}$.K)}

Eavesdropping Attack

This attack occurs through interception of network traffic, and the attacker can passively, or actively grab information to gain valuable information. We have a system where there is a dependency between the sender and receiver before they can successfully exchange messages,therefore the hacker should be able to get valuable information from both parties to make use of it, because the common key used to encrypt the data has elements of the both parties' private keys involved in it, and considering active eavesdropping, the attack still has to find two distinct and independent elements of the key of a user to be able to use that information. On consideringthe dynamic key approach, the attacker is rendered helpless as his information is invalid once the session ends, and the attacker must go through the process to get access to the new key, while the session lasts, this is very difficult as both the parties are active and using the protocol,they would easily spot any suspicious activity.

Parameters targeted: The modified EDSCA signature generation and verification protocol.

Birthday Attack

This attack involves a message processed by a hash function and produce a message digest offixed length. Now the attack involves finding two different messages generating the same digest. We have a method, that has immensely high avalanche effect and we are working on a3-dimensional curve giving us a lot of surface area to work with, the process involved makes the generation of cipher texts very random and placed very far apart on a 3-dimensional curve,the possibility of collision is reduced to nearly impossible.

Parameters targeted: Cipher text => {(K.G), (M + $Pubkey_{receiver}$.K)}

SECURITY PROOF AND COMPLEXITY ANALYSIS:

The proposed cryptosystem and digital signature both are based on elliptic curve discrete logarithm along with commutative property of the rotational dot product.

Therefore, the security of the protocol depends on the elliptic curve discrete logarithm connecting with associative and commutative property of the rotational dot product. Hence algorithm is more secured as long as ECDLP is unbreakable. Since all the equations is either in cryptosystem and digital signature are in linear form over elliptic curve then the order of complexity is 'n' over elliptic curve and hence time to execute the algorithm is less when we compare with the existing algorithm.

STRENGTH AND SOUNDNESS OF THE ALGORITHM

The algorithm proposed has several strengths and advantages, let us shine a light on a few of them,

- Extremely high degree of security, with just four extra bits in the key. This is possibleas the extra bits accounts for an angle referred to as 'theta'(θ), that is responsible forthe rotation of the x-y plane in an anti-clockwise direction post every iteration in theprocess of encryption. This process creates a high degree of uncertainty, which accounts for the superior levels of security. This also accounts for significant extremeavalanche effect.
- Naturally split private key, a numerical value, and an angle(θ). The angle 'theta(θ)' is the second part of the private kay that the user gets to choose, with the numerical value as in other conventional encryption algorithms. As opposed to other key splitting mechanisms where, a single key is split using mathematical procedures, which sometimes are back trackable, if a few of the split pieces are found, thereby compromising on the security, this model proposes the usage of two values, which have no interrelation whatsoever, and hence making it theoretically impossible to deduce the second using the first or vice versa.
- Ability to accommodate more private keys with the same numerical value, given a different angle. The naturally split private key, enables multiple users to have the same numerical value with different theta(θ) values, which would effectively make it a different private key. This allows the model to accommodate multiple keys, whicheffectively only differ by four bits.
- Extremely sophisticated trapdoor function. (Practically impossible to backtrack) The mathematical model, which is based on a protocol, that has a 3-dimensional surface,with an element of rotation, makes it extremely difficult to backtrack or brute force, as its understandable that, even the slightest ever change in any of the elements of theprivate key, will cause significantly profound change in the produced cipher text, the3-dimensional aspect provides exceptional security.
- Ability to achieve a very high degree of security, while using smaller key sizes. Theintroduction of the second element of the private key, provides and accounts for the most amount of security apart from the conventional methods, therefore the first element in the private key can be smaller and the security is still not compromised.
- The algorithm, when implemented using the dynamic private key approach, can immensely change the security aspects of the method, the usage of sessions is common in multiple communication systems, therefore effectively using a new private key to hash the messages corresponding to every new session, makes it very difficult for attackers, as they should be able to find the key in while the communication is active on both ends and the information gained will be rendered not so useful in the next session.

Statistical Analysis

The algorithm proposed will be compared the original elliptical curve cryptography. We understand that elliptical curve cryptography already uses a low number of bits in its keys to achieve respectable amount of security, on the other hand other encryption methods like the RSA, would consume a lot of bits to achieve a very high level of security, lets now discuss howwe fair against them,

Let us consider a key size of n, using the elliptical curve cryptography the attacker has to gothrough, K^n possibilities, where K is the number possible values each bit in the key of size n can take. Considering the methodology suggested by the paper, assuming similar number of bits used, which is n. The key now has, the numerical value which uses n-19 bits and an angle that uses 19 bits.

Key = numerical value (n-19 bits) + angular value (19 bits)

Now the total possibilities a hacker must try before succeeding goes up exponentially in the power of 19. We will have all possible numerical values of size n-19, for every single angle, the angle can take a maximum value of 99.99999999999999999 (a part of the semi-circle in each iteration). Every such angle can have all possibilities of numeric values there by making it, = $19^{(n-19)}$ extra possibilities corresponding to each of their starting points (taking the floor value of 99.99999999999999999, for easy calculation). Therefore, giving it an extra factor of 99 which now becomes,

= $19^{(n-19)}$ x 99 extra possibilities

The total possibilities for a hacker to check becomes,

= K^{n-19} x $19^{(n-19)}$ x 9 x 9^{19} possibilities

Where the last element '9^{19}' corresponds to the number of possible angles we can choose in each case, as we have 19 bits to fill, and each of them has 9 possibilities. Thereby this exponential increase in the security makes this a highly secure algorithm

Time taken to crack the $Privkey_x$: (n_x, θ), for n_x. Let us assume in any other system it takestime (T) to crack the password by brute forcing it. For every such n_x, the attacker would now have to calculate the corresponding θ, which is mathematically unrelated to n_x, and every attempt tobrute force θ would cost the attacker 7 years in 2022. [time taken to brute force 19 bits of data.] (Source: security.org), thereby (T x 7) years, making is extremely difficult to crack. Given the possibility on implementing the algorithm using the dynamic private key approach the attacker would have to recalculate the θ for every new session, which would give the attacker absolutely no power over the communication, as no session would last as long as 7 years, and it is advised that users constantly

refresh (restart) their sessions, and therefore making it impossible to crack the Private key. Making the algorithm extremely secure and a best fit for highly secure transactions.

CONCLUSION

The protocol proposed is one of a kind, and the first ever one to implement a naturally split dynamic key encryption standard. The architecture and the mathematical model proposed are the first in their kind, the first ever 3-dimensional curve based, rotating encryption, where the private key has two naturally split distinct and independent elements to it. The 3-dimensional approach gives the algorithm a lot of geometric places to play with, achieving a very high avalanche effect and a near zero possibility of a collision in the cipher text values generated for different messages. This protocol is essentially aimed at enabling highly secure transactions between financial institutions, though it can also be implemented at lower levels of security based on the need, the level of security it could achieve is extremely high if the complete protocol suggested is followed end to end. We have discussed the possibility of a dynamic implementation of the algorithm where the second part of the private key can dynamically change for every session, and this would make the system resistant to most types of cyber-attacks as we have discussed in the paper. This could be the basis for further research, and improvisations. The architecturesuggested could act as the base for developing and implementing some of the most secure encryption algorithms ever made, without compromising on the space needed to store the keys,or fear of having compromised a part of the key.

ACKNOWLEDGEMENT

There is no funding support for the above work.

CONFLICT OF INTEREST STATEMENT

Authors do not have a financial support for this work and thus, no influence on this work. No conflict of interest exists.

REFERENCES

1. D. Zhu. Security Control in Inter-Bank Fund Transfer. *J. Electron. Commer. Res.* **2002**, 3 (1), 15–22.
2. R. Banerjee. Confidentiality and data protection in the electronic fund transfer. *Int. J. Law 203 Int. J. Law www.lawjournals.org* **2020**, 6, 203–206.
3. U. Mardiyev. Using of R parameter in a Massey-Omura protocol on elliptic curves. In *International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021*; **2021**; pp 1–3.
4. J. Yao, C. Yan, T. Zhang. Elliptic Curve Cryptography Algorithm Against Energy Attack. In *2021 IEEE Conference on Telecommunications, Optics and Computer Science, TOCS 2021*; **2021**; pp 224–227.
5. O. Ahmedova, Z. Khudoykulov, U. Mardiyev, A. Ortiqboyev. Conversion of the Diffie-Hellman Key Exchange Algorithm Based on Elliptic Curve Equations to Elliptic Curve Equations with Private Parameters. In *International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2021*; **2021**; pp 1–4.
6. H.W. Lenstra. Factoring Integers with Elliptic Curves. In *The Annals of Mathematics*; **1987**; Vol. 126, p 649.
7. S. Goldwasser, J. Kilian. Almost all primes can be quickly certified. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*; **1986**; pp 316–329.
8. B.S. Kaliski. A pseudo-random bit generator based on elliptic logarithms. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer-Verlag, **1987**; Vol. 263 LNCS, pp 84–103.
9. B. Mazur. Modular curves and the eisenstein ideal. *Publ. Mathématiques L'Institut des Hautes Sci.* **1977**, 47 (1), 33–186.
10. F. Morain. Building cyclic elliptic curves modulo large primes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer-Verlag, **1991**; Vol. 547 LNCS, pp 328–336.
11. M. Soeten. Hasse's Theorem on Elliptic Curves with an extension to hyperelliptic curves of genus 2; Master Thesis Mathematics, University of Groningen, **2013**.
12. Z.-M. V. Zadorozhnyi, V. V. Muravskyi, O.A. Shevchuk. Management Accounting of Electronic Transactions With the Use of Cryptocurrencies. *Financ. Credit Act. Probl. theory Pract.* **2018**, 3 (26), 169–177.
13. S. Ullah, J. Zheng, N. Din, et al. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Comput. Sci. Rev.* **2023**, 47, 47.
14. G.J. Lay, H.G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer-Verlag, **1994**; Vol. 877 LNCS, pp 250–263.
15. A.F.X. Ametepe, A.S.R.M. Ahouandjinou, E.C. Ezin. Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks. *Wirel. Networks* **2022**, 28 (3), 991–1001.
16. C.H. Meyer, S.M. Matyas, R.E. Lennon. Required cryptographic authentication criteria for electronic funds transfer systems. *Proc. - IEEE Symp. Secur. Priv.* **2012**, 1981 (1981), 89–98.
17. J.M. Pollard. Monte Carlo Methods for Index Computation (mod p). *Math. Comput.* **1978**, 32 (143), 918.
18. G. Frey, H.-G. Ruck. A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves. *Math. Comput.* **1994**, 62 (206), 865.
19. T. Satoh, K. Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math Univ St Pauli* 47 (1), 81–92.
20. P. Zode, R. Deshmukh. Side channel attack resistant architecture for elliptic curve cryptosystem. In *Cyber-Physical Systems*; **2018**; Vol. 4, pp 205–215.
21. A.J. Menezes, S.A. Vanstone. Elliptic curve cryptosystems and their implementation. *J. Cryptol.* **1993**, 6 (4), 209–224.
22. V.K. Sharma, P. Mathur, D.K. Srivastava. Secure Electronic Fund Transfer Model based on Two level Authentication. In *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*; IEEE, **2018**; pp 1338–1342.
23. X. Huang, P.G. Shah, D. Sharma. Protecting from attacking the man-in-middle in wireless sensor networks with elliptic curve cryptography key exchange. In *Proceedings - 2010 4th International Conference on Network and System Security, NSS 2010*; **2010**; pp 588–593.
24. K. Yesodha, M. Krishnamurthy, K. Thangaramya, A. Kannan. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. *J. Supercomput.* **2024**, 80 (13), 18866–18899.