An Elliptic Curve Cryptography based Algebraic Structures for Security Provisioning using Algebraic Cryptography

Ravindra Babu Gudapati [1], Dr. Rajeev Jha [1]

[1] *Research Scholar, Department of Mathematics, Asian International University, Ghari, Imphal West, Manipur, India.* ravi.intv@gmail.com

[2] *Research Supervisor, Professor, Asian International University, Ghari, Imphal West, Manipur, India*

Abstract: In this day and age of pervasive computing, it is more important than ever to take measures to secure sensitive information. This is an especially important topic given that data is kept and sent in diverse places all over the world. The protection of information that has been stored relies heavily on the use of a number of different encryption methods, many of which may be traced back to algebraic cryptography. Using elliptic curve cryptography, we presented in this paper a way for producing algebraic codes over F q that are more resistant to cryptanalysis. The system's information rate as well as its level of security are both of the highest possible quality. It is easy to utilize this plan to construct a new scheme based on the existing one without recovering the secret. By doing so, it is possible to increase or decrease the number of shareholders, as well as widen the set of shares that may be used to retrieve the secrets.

Keywords: Algebraic Cryptography, Elliptic Curve Cryptography, Security Provisioning, and Security Provisioning.

1. INTRODUCTION

Nonetheless, the term "algebraic cryptography" is also often used in a narrower meaning. Algebraic encryption uses encoding and decoding, both of which are group homomorphisms. In cryptography, noncommutative algebra is seldom used. As noncommutative constructions are resistant to many standard cryptographic attacks, any new strategy is likely to garner a lot of interest. Yet, there are currently no security proofs in cryptography that would make it possible to rely on issues are highly assumptions when assessing the security of a cryptographic basic. As a result, investigating more flimsy ideas of safety is essential [1], [2]

With this stricter definition, algebraic cryptography is still] somewhat older than public-key cryptography. The first HMAC method, among the first known cryptosystems, was based on a cubic residual cryptography [3], [4], [5].

Public-key cryptography, makes heavy use of algebraic structures and has done so from the beginning. For example, determining an Euler totient is essential to constructing the RSA protocol, which is based on number theory (n). The security is based on the fact that it is difficult to factor into primes, or more particularly, to solve the so-called RSA problem, which is to find roots of a certain degree mod an integer n = pq, where both p and q are prime (this work may not be comparable to factoring).

- **Definition 1.** Suppose that there occurs an epimorphism f: G H, where H is a limited nonidentity group, and that G is a finite generated group. Suppose that there is an alphabet A, that there is a set of representations of right f in G denoted by R, and that there is a mapping P: A G such that Im(P) = ker(f) (f). If S = (R, A, P) satisfies all three conditions, then we say that it is symmetric over H with respect to f. The inversion of an item as well as the summation of two components may be calculated in a probability polynomial N time, where N represents the number of the models of G, H, and a. (in the set G or H); |R| = |H|, and the copy f(g) of each component g ∈ R as well as a matchless preimage g ∈ R such that f(g) = h of every element h ∈ H whose mappings P can be calculated in probabilistic exponential (in N) duration is referred to as a "backdoor function.

- **Definition 2.** Sharing a public key to encrypt data S consists of three procedures (G,E,D) that, in stochastic worst-case polynomial time, create keys, encrypt data, & decrypt data, respectively. G, a key-generation algorithm that takes inputs 1^n (is the security parameter) produces a pair $G(1^n) = (e, d)$ both overt and covert applications. The plaintext m and the shared key e are input into the encrypting algorithm E, which produces the ciphertext c.

$$E(e, m) = c$$

In conclusion, the decryption procedure D takes as input both the secret key d and the ciphertext c. D's output is a textual message

$$D(d, c) = m'$$

which may fail to equal the original message m when $E(e, m) = E(e, m')$. We refer to these occurrences as collisions, and we believe them to be very unusual.

The probability quadratic technique (B) seems to exist for all probability - based polynomial methods (M and A), characteristics (h), and polynomials (Q), making it impossible to decode the secret key for sufficiently large k. Incorporating the three pillars of linguistically secure encryption into a single definition (G,E,D),

$$\Pr_r\left[A(1^k, c, e) = h(m) \mid (e, d) \quad \leftarrow^r G(1^k), m \leftarrow^r M(1^k), c \leftarrow^r E(e, m)\right] \leq \Pr_r\left[B(1^k) = h(m) \mid m \rightarrow^r M(1^k)\right] + \frac{1}{Q(k)}$$

An adversary who knows the message distributing M and is provided the encrypted messages and the public key will not be capable of decoding it with any more frequency than an algorithms that does not know anything but M. (M is required because, without it, an adversary would've been able to decode the message even if they knew the coding and the public key, as an example, just one message is broadcast constantly. The main problem is that this formulation uses probabilities that are based on the distribution of the messages that go into the cryptosystem. This makes sense as it is usually possible to crack a cryptosystem by just trying a small fraction of the possible inputs, rather than trying them all.

RSA is recognized as the de facto standard in the area of public-key cryptography, while ECC is viewed as an alternative to RSA in this field. The security of the RSA cryptosystem comes from the fact that it has been able to solve the Integer Factorization Problem (IFP), while the security of the Elliptic Curve Cryptosystem comes from having been able to solve the Elliptic Curve Discrete Logarithm Problem. The fact that the most well-known technique for solving the ECDLP takes whole exponential time as opposed to the sub-exponential time that is needed to solve the IFP of RSA is the fundamental reason why ECC is favoured over RSA. RSA requires entire exponential time to solve the IFP. When it comes to finding a solution to the ECDLP, the method known as Pollard's rho algorithm is the one that is the most effective. The complete exponential amount of time is required for this technique, and the expected running time is less than n/2. The most difficult ECDLP problem that could be solved using Pollard's rho approach as of the year 2003 used an elliptic curve that was specified over a 109-bit prime field. This problem was the largest one that had ever been attempted to be solved. The universal number field sieve developed by Pollard is perhaps the most well-known method for factoring generic integers (NFS). The heuristic expected run-time needed by the NFS to find a factor of the composite number n is denoted by the equation L[n] = [1/3, 1.923]. The RSA200 is the largest integer that could be factored using the NFS technique in a time that was less than sub-exponential. It is a 200-digit number with 665 bits, and it was factored in May of 2005 [16]. This indicates that ECC is capable of using parameters that are far smaller than those that RSA is capable of using while yet retaining the same level of security. An RSA-based cryptosystem, for example, requires a password with a length of 2048 bits to reach the secure communication of 112-bits, but an ECC-based cryptosystem requires a key with a size of 224 bits to achieve the same level of security. Both systems use a public key to encrypt and decrypt data. This work makes use of the RSA and ECC algorithms in order to show how these algorithms may be used by two parties that are communicating with one another.

2. ALGEBRAIC STRUCTURES

A set's algebraic structure is the relationship it has with the operations that can be carried out on its elements. In algebra, the most common types of organisation are groups, rings, and fields. The basic elements of algebra are the

algebraic structures known as groups, rings, fields, abstract algebra, and modules. It has uses in the fields of chemistry, physics, and Channel Coding in cryptography. It's like Groups, but for performing algebraic and numeric operations on closed sets. Similarities between two algebraic structures may be discovered and used.

Definition 3: As a non-empty set, Algebraic Structure has meaning. In the context of binary operations, S is said to be an algebraic structure (*) if the following postulates hold:

Prove: (a*b) goes to S for all a,b ∈ S.

Case: The preceding, on the other hand, does not constitute an acceptable algebraic structure.

S = {1,-1} is arithmetical construction under *

As

1*1 = 1;

1*-1 = -1;

-1*-1 = 1;

For all fallouts belong to S.

+ as 1+(-1) = 0 not goes to S.

Group

A non-empty set G, (G,*)

- Prove:(a*b) goes to G for all a, b ∈ G.
- Function: a*(b*c) = (a*b)*c ∀ a, b, c goes to G.
- Converses: ∀ a ∈ G there occurs a-1 ∈ G such that a*a-1 = a-1*a = e
- Variables: There occurs e ∈ G such that a*e = e*a = a ∀ a ∈ G

Summary:

- (Z,+) and Matrix multiplication is example of group.
- In addition to its arithmetical structure, a group is always composed of a monoid and a semigroup.

Semi Group

A non-empty set S, (S,*) if and only if the semigroup satisfies the following axiom:

- Prove:(a*b) have its place to S for all a, b ∈ S.
- Function: a*(b*c) = (a*b)*c ∀ a, b ,c have its place to S.

Summary: A semi-group is always an arithmetical construction.

Example: (Set of integers, +), and (Matrix ,*) are samples of semigroup.

Monoid

A non-empty set S, (S,*) if and only if the monoid axioms below are true:

- Prove:(a*b) goes to S for all a, b ∈ S.
- Function: a*(b*c) = (a*b)*c ∀ a, b, c goes to S.
- Variables: There occurs e ∈ S such that a*e = e*a = a ∀ a ∈ S

Summary: A monoid is always a semi-group and arithmetical construction.

Case:

(Set of integers,*) is the Variables and hence a monoid since 1 is an integer.

Due to the lack of an identity member, the set (Set of positive integers, +) is not Monoid. Nonetheless, this is a Semigroup.

Yet, 0 serves as the identity member of the monoid (Set of the whole numbers, +).

Commutative group / Abelian Group

A non-empty set S, (S,*) satisfies the following axiom, we say that it is an Abelian group:

- Prove:(a*b) goes to S for all a, b ∈ S.
- Variables: There occurs e ∈ S such that a*e = e*a = a ∀ a ∈ S
- Function: a*(b*c) = (a*b)*c ∀ a ,b ,c goes to S.
- Commutative: a*b = b*a for all a, b ∈ S
- Converses: ∀ a ∈ S there occurs a-1 ∈ S such that a*a-1 = a-1*a = e

Checking the axioms one at a time, beginning with the Prove condition, is the only certain method to determine the category to which a given set belongs.

This is an important finding among many others-

Table.1. Terminologies of Algebraic Cryptography

	Satisfaction with the Premises, Mandatory
Arithmetical Construction	Closing
Semi Collection	Closing, Associative
Monoid	Conclusion, Associative, Individuality
Collection	Conclusion, Associative, Individuality, Converse
Abelian Collection	Conclusion, Associative, Individuality, Converse, Commutative

Summary:

A group, monoid, semigroup, and abelian group describe every possible algebraic structure.

Several procedures on nonempty sets are compared in the table below:

N = Natural Numbers as a Group

Z = Integer Set

R = Group of True Numbers

E = Group of Twos and Ones

O = Group of Uneven Numbers

M = Matrix Collection

+,-,×,÷ are the processes.

Table.2. Process, and Groups of Algebraic Structures

Set, and Process	Monoid	Group	Abelian Group	Arithmetical Structure	Semi Group
N,+	A	A	A	Y	Y
N,-	A	A	A	A	A
N,×	Y	A	A	Y	Y
N,÷	A	A	A	A	A
Z,+	Y	Y	Y	Y	Y
Z,-	A	A	A	Y	A
Z,×	Y	A	A	Y	Y
Z,÷	A	A	A	A	A
R,+	Y	Y	Y	Y	Y
R,-	A	A	A	Y	A
R,×	Y	A	A	Y	Y
R,÷	A	A	A	A	A
E,+	Y	Y	Y	Y	Y
E,×	A	A	A	Y	Y
O,+	A	A	A	A	A
O,×	Y	A	A	Y	Y
M,+	Y	Y	Y	Y	Y
M,×	Y	A	A	Y	**Semi Group**

Rings

A ring R, occasionally represented by {R, +, A}, is a set of integers where all feasible configurations of a three numbers satisfy the axioms of binary multiplication and addition (a, b, c).

Typically, we merely add the outcomes of two procedures together, rather than employing the x sign for multiplication.

If and only if the axioms A1 through A5 hold, then R is indeed an atavistically abelian group. In an addition group, the element with symbol 0 is the Variables, while the element with symbol 1 is the anti-Variables.

Both a & b must belong to R for ab to be considered a member of that set.

- a(bc) = (ab)c for all a, b, c in R.
- a(b + c) = ab + ac for all a, b, c in R.
- (a + b)c = ac + bc for all a, b, c in R.

A ring may be considered to be a set wherein addition and subtraction can be performed [a b = a + (-b)], addition and multiplication within the set.

In terms of addition and multiplication, the collection of all n2 multiplications over actual figures is a ring. The ring is said to be commutative if and only if the following additional condition holds:

Commutativity of exponentiation: ab = ba for all a, b in R.

To provide an example, let's say that S is the collection of all even integers (both positive and negative, plus zero) that can be added and multiplied without producing a remainder. The ring S is characterised by symmetry. As shown above, the set among all n2 squares matrix is not linked.

As a result, we define an integral domain to be a distributed ring that meets the following conditions:

- For any numbers an in the set R, there exists an element 1 such that a1 = 1a = a. This is called a multiplicative identity.
- If a and b are in R and ab equals zero, then either an or b must be zero.

Let S denote the collection of integer that includes positive and negative numbers as well as 0. S is a domain of integrals.

Fields

A field F, sometimes denoted by {F, +, x}, is a set of integers where addition and multiplication are the only allowed operations, and the following axioms hold for all three numbers (a, b, and c) in F:

- F meets axioms A1 though A5 & M1 though M6; so, F is an integrated domain.
- There's an object a-1 in F so that aa for any an in F other than 0-1 = (a-1)a = 1.

Simply put, a field is any set in which we may perform arithmetic operations (addition, subtraction, multiplication, and division) without ever having to leave the set. The following rule describes division: a/b = a(b-1). The real numbers, the actual values, and the complex numbers are only few of the fields that may be used. The collection of all prime numbers does not constitute a field because not every member in the set has a second derivative among the integers; in fact, only the components 1 and -1 possess multiplying Converses in the integers.

3. EXAMPLE FOR ALGEBRAIC CRYPTOGRAPHY

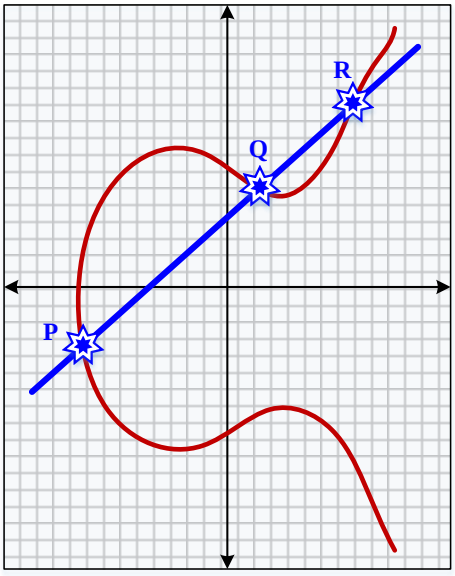

Fig.1. Elliptic curve

Definition 4: Example for Algebraic Structure- Elliptic Curves over Prime Fields

An elliptic E over F, for some field F other than 2 or 3, is defined by the equation $y^2 = x^3 + ax + b$, where $a, b \in F$ and $4a^3 + 27b^2 \neq 0$. Points with rational values on the set E over F, indicated by E(F), are

$$E(F) = \{(x, y) \in F^2 : y^2 = x^3 + ax + b\} \cup \{O\},$$

The equation is closed under the projective space O $y^2 = x^3 + ax + b$. The point O represents infinity and is referred to as such. It's a property $4a^3 + 27b^2 \neq 0$ guarantees that the polynomial $x^3 + ax + b$ is not a polynomial over F. Set of logically valid points with some arithmetic operations and infinity serving as the zero element, the commutative group structure of E(F). Let q denote a prime > 3. Consider the elliptic curve E over the prime field GF to be finite (q). The map of multiplication by m for all positive integers m $[m]: E \to E$ defined by

$$[m]: P \mapsto mP = P + \cdots + P$$

is a specified endomorphism of E over $GF(q)$. Now let $G \in E(GF(q))$ be an N-point, where N is a positive integer. $m, 1 < m < N - 1$, set $P = [m]G$. Given $GF(q), E, G$, and P, the Elliptical Surface Integer determination using the Discrete Logarithm Problem m. Let $\Delta \equiv 0,1(\mathrm{mod}4)$ consist of a negative number that doesn't constitute a square. Discriminant's Imaginary Quadratic Order Δ is defined to be,

$$\mathcal{O}_\Delta = \mathbb{Z} + \omega\mathbb{Z}$$

where

$$\omega = \begin{cases} \sqrt{\frac{\Delta}{4}}, & \text{if } \Delta \equiv 0 \pmod 4, \\ \frac{1+\sqrt{\Delta}}{2}, & \text{if } \Delta \equiv 1 \pmod 4. \end{cases}$$

If Δ_1 is square free, then $\mathcal{O}_{\Delta_1}$ is the highest possible order in the space of quadratic numbers $\mathbb{Q}(\sqrt{\Delta_1})$ and Δ_1 is called a essential discriminant. The non-maximal order of conductor $p > 1$ with (non-fundamental) discriminant $\Delta_p = \Delta_1 p^2$ is denoted by $\mathcal{O}_{\Delta_p}$. The conductance p is assumed to be prime. Discriminatory (whether basic or not) criteria shall be referred to without subscripts.

Let E be an elliptic curve well-defined over $GF(q)$, and $\mathcal{O}_\Delta$ consist of its endomorphism ring. Let's pretend $\mathcal{O}_\Delta$ is a maximal order. Let $\pi \in \mathcal{O}_\Delta$ mean that E is endomorphic to the Frobenius group, and $\bar{\pi}$ is its conjugate. As a result, under Theorem 3 of [14] of E is $|E(GF(q))| = q + 1 - t$, where $t = \pi + \bar{\pi}$.

If E is defined by the equation $y^2 = x^3 + ax + b$Furthermore, if d is a residue that is not a square root of p, then the twist $\tilde{E}$ related to the elliptic curve The equation [[What does E mean?]] (independent of the choice of d) $y^2 = x^3 + d^2ax + d^3b$.

4. RELATED WORK

For each finite field F q, q > 2, we prove that any known q ordinary bipartite algebraic network A (n, q) on 2 q n nodes has girth 2 n or 2 n + 2. This result is extended to the case of graph A (n, K) formed over any commutative ring K. Extremal graph theory and Algebraic Graph Cryptography are discussed as a result [11]. The authors of [12] offer two generalised algebraic cryptographic systems. Finally, it's demonstrated that a first generic scheme encompasses a wide range of systems & protocols that have been studied in the literature and that make use of two-sided multiplications. The second overarching approach we offer may be understood in terms of algebraic systems including automorphisms or endomorphisms. Algebraic cryptography was also investigated in light of the membership search problem. Then, the study shows how both methods are vulnerable by proving that highlighted membership search problem is effectively decidable on the chosen algebra system. Both nonlinear as well as linear decomposition techniques are used in the attacks; they work together to great effect. The author then presents two standard examples of protocol and systems that use one of the two cryptanalysis methods outlined. These protocols serve as examples for other popular cyphers in algebra, including as Diffie-Hellman, Massey-O'Murray, and ElGamal. Without fixing the fundamental computational difficulties that underlie the techniques, they are easy to circumvent [12]. The "linguistics" application of algebraic geometry has found value in both diplomacy & defence. The Pharaohs were supposed to have been the first to arrange a meeting of the army. He said that the Arabs had already attempted encryption. The Chinese used a broad array of means of communication during times of strife. The objective was to create confusion about what was really being said. There are thanks, a message, and an overview of the topic of scientific (word) searches as it relates to different techniques in English linguistics in this work. Topographic graphic password (Topsnut-gpws) were shown to be both quick and easy to recall in the research. Researchers have examined algebraic groups built using Topsnut-gpws for possible use in network encryption. The presence of particular algebraic groups is now determined by the new brand activation of our graphs. Generating longer, more complex text-based passwords is now a breeze thanks to algebraic groups and modern graph labelings. For straightforward networks, the authors provide the network-gpws encryption approach. This results in new mathematical problems to solve [14]. The creation of these new cryptographic primitives is based on group invariants, making them more secure than their predecessors. Verifiable breaks, which are far less powerful than traditional cryptographic breaks, are also introduced. The modified version adds the need of proof of successful decryption by

an adversary. Unless NP = RP [15], it is shown that matrix group consistent cryptosystems are secure, as is a key agreement technique for modular groups that is analogous to Anshel-Anshel-Goldfeld. The writers of [16] examine cryptography's history in try to better understand its origins. The writers began with the very basics of encryption and skipped all the way to today's cutting-edge techniques. After outlining the drawbacks of traditional encryption methods, the authors offer chaos-based cryptography. Because chaos theory & cryptography are so intrinsically linked, nonlinearities are often used in the creation of novel cryptographic protocols. As chaotic maps are very sensitive to initial conditions, this makes sense, since chaotic signals are often indistinguishable from background noise. Given their sensitivity to initial conditions and the spreading nature of their trajectories throughout the whole period, they appear to fit a model that satisfies the standard Shannon criterion of confusion and diffusion.

5. PERFORMANCE ANALYSIS OF ECC

The purpose of this experiment was to examine the efficacy of the aforementioned techniques on the basis of the following characteristics on the local system while using a variety of input sizes. Described in this part are the platforms, experimental settings, and critical management of empirical procedures.

a) Assessment Criteria and Criteria: While evaluating the effectiveness of a cryptographic algorithms, the following factors should be taken into consideration.

- Encryption Time: The duration that an encryption scheme takes to create an encrypted message from an original message is referred to as the encryption time.
- Decryption Time: The amount of time it takes for a decryption algorithm to create an original message from an encrypted message is what is referred to as the decrypt time.

b) Platforms for Evaluative Assessment: The effectiveness of the encryption technique is analyzed with the accompanying configuration taken into consideration.

- Software Specification: Experimental assessment running on Eclipse JEE Mars with Java Development Kit 8 Update 65, version 2014 of Matlab, and Windows 8.1 Professional 64-bit Operating System.
- The hardware specifications include a one terabyte hard drive, four gigabytes of random-access memory, and an Intel Core i5 CPU from the fourth generation running at 2.40 gigahertz.

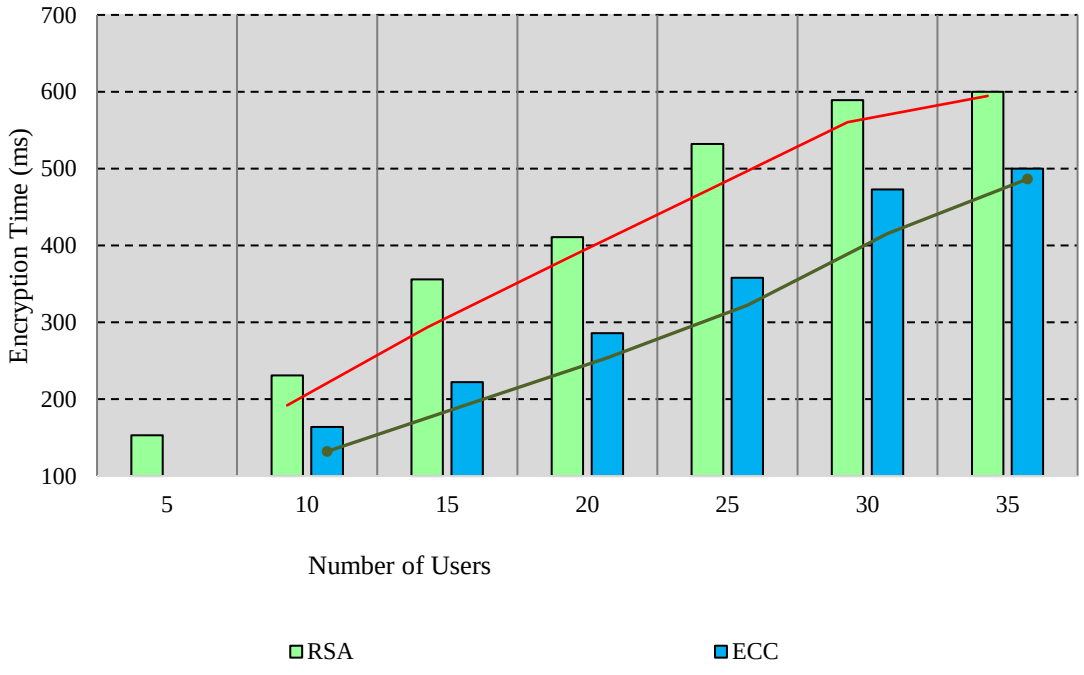

Fig.2. Encryption Time vs. Number of Users

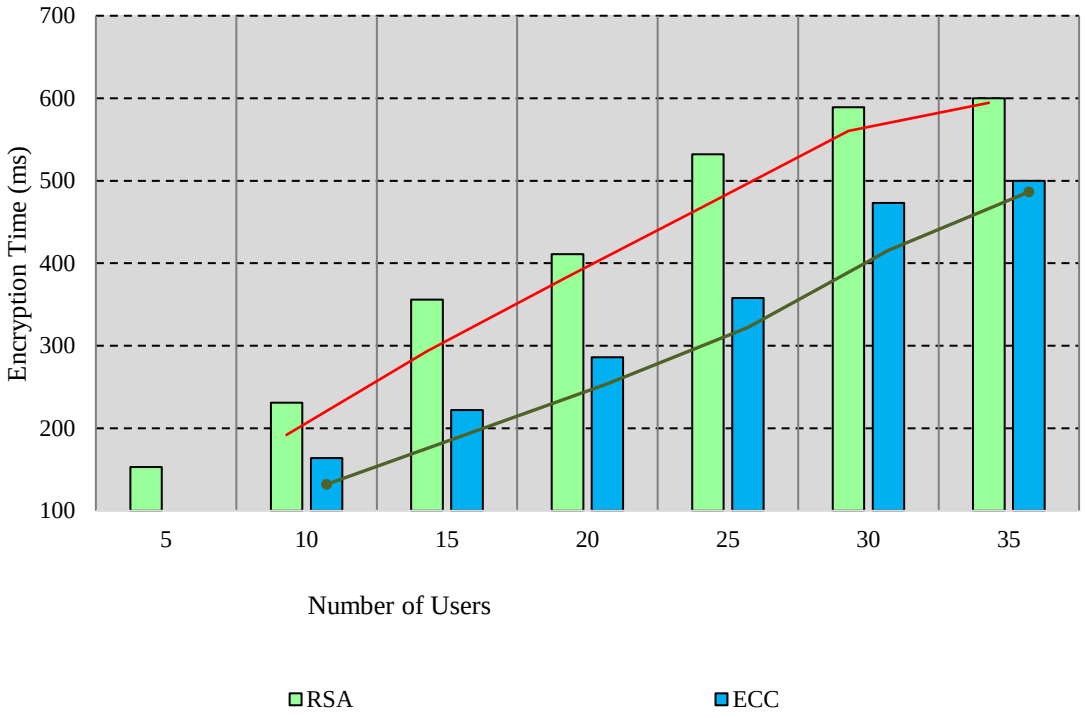

Fig.3. Decryption Time vs. Number of Users

6. ATTACKS AGAINST ALGEBRAIC CRYPTOGRAPHY

Examining potential vulnerabilities in a brand-new cryptosystem or set of cryptosystems is standard operating procedure. Here, we take a look at several attacks against fafsa cryptosystems and offer advice on how to counter them. The attack model and the defend model is presented in Fig.4. The defend mechanism provides that the proposed work achieves better security against this type of threats. In this model, the main intention of the attack is to derive private keys from the public key. In general, RSA private keys can be hacked from the public keys through factorization. To defend this, attack the derived public and private keys must be secure and must be generated from the largest prime numbers.

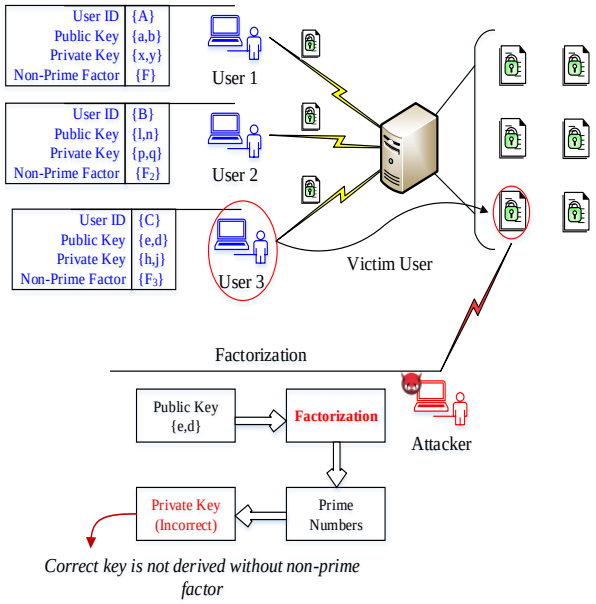

Fig.4. Attacks in ECC

7. CONCLUSION

The information security that has been saved depends primarily on the use of a bunch of alternative encryption techniques, the origins of many of which may be traced back to the field of algebraic cryptography. In this research, we developed a method for constructing algebraic codes over F q that are more secure against cryptanalysis by using elliptic curve cryptography. These codes are more difficult to break. Both the information rate of the system and its degree of security are of the very best conceivable grade. Using this method to build a new scheme that is based on the present one is straightforward and does not need retrieving the secrets. It is possible to expand or reduce the number of shareholders by doing so, and doing so also makes it possible to extend the set of shares that may be utilized to recover the secrets. Algebraic functions employed in cryptographic algorithms are now thought of as having an essential cryptography property: resistance against algebraic attacks and quick algebraic assaults. These two attacks are very potent analytical ideas that may be used against symmetric cryptographic algorithms like those employed in cryptographic algorithms.

8. REFERENCES

[1] S Hofheinz, D. (2016). Algebraic Partitioning: Fully Compact and (almost) Tightly Secure Cryptography. IACR Cryptol. ePrint Arch., 2015, 499.
[2] O'Neill, M.E. (2009). The Genuine Sieve of Eratosthenes. J. Funct. Program., 19, 95-106.
[3] Abdullah, D., Rahim, R., Apdilah, D., Efendi, S., Tulus, T., & Suwilo, S. (2018). Prime Numbers Comparison using Sieve of Eratosthenes and Sieve of Sundaram Algorithm. 2nd International Conference on Computing and Applied Informatics.
[4] Atkin, A.O., & Bernstein, D.J. (2003). Prime sieves using binary quadratic forms. Math. Comput., 73, 1023-1030.
[5] Joye, M., Paillier, P., & Vaudenay, S. (2000). Efficient Generation of Prime Numbers. CHES.
[6] Joye, M., & Paillier, P. (2006). Fast Generation of Prime Numbers on Portable Devices: An Update. CHES.
[7] Makkaoui, K.E., Hssane, A.B., Ezzati, A., & El-Ansarib, A. (2017). Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing. EUSPN/ICTH.
[8] Herranz, J. (2014). Attribute-based signatures from RSA. Theor. Comput. Sci., 527, 73-82.
[9] Mathur, S., Gupta, D., Goar, V., & Choudhary, S. (2018). Implementation of Modified RSA Approach for Encrypting and Decrypting Text Using Multi-power and K-Nearest Neighbor Algorithm. Networking Communication and Data Knowledge Engineering, 229-237.
[10] Thangavel, M., Varalakshmi, P., Murrali, M., & Nithya, K. (2015). An Enhanced and Secured RSA Key Generation Scheme (ESRKGS). J. Inf. Sec. Appl., 20, 3-10.
[11] Ustimenko, V. (2022). New results on algebraic graphs of large girth and their impact on Extremal Graph Theory and Algebraic Cryptography. IACR Cryptol. ePrint Arch., 2022, 1489.
[12] Roman'kov, V. (2018). Two general schemes of algebraic cryptography. Groups Complexity Cryptology, 10, 83 - 98.
[13] Kasm, N.Y., & Hamad, Z.A. (2019). Applications of Algebraic Geometry in Cryptography. Modern Applied Science.
[14] Yao, B., Mu, Y., Sun, H., Zhang, X., Wang, H., Su, J., & Ma, F. (2018). Algebraic Groups for Construction of Topological Graphic Passwords in Cryptography. 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2211-2216.
[15] Grigoriev, D., Kojevnikov, A., & Nikolenko, S.I. (2009). Algebraic cryptography: New constructions and their security against provable break. St Petersburg Mathematical Journal, 20, 937-953.
[16] Ariffin, K., & Rezal, M. (2008). Chaos Based Cryptography An Alternative to Algebraic Cryptography.

DOI: https://doi.org/10.15379/ijmst.v10i4.2360