A Survey of the Elliptic curve cryptography attacks, advantages and Disadvantages

Dr. AMIT VERMA[1], KANWALPREET SINGH[2],BHARTI CHHABRA[3]
[1]*Professor and Head of Department and Professor, Department of computer Science, CEC Landran, Mohali, Punjab*
[2]*Mtech Research Scholar, Department of computer Science, CEC Landran, Mohali, Punjab*
[3]*Assitant Professor, Department of computer Science, CEC Landran, Mohali, Punjab*

Abstract- ECC is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of a RSA could be offered by 163 bit security strength of ECC. Other than this, ECC is particularly well suited for wireless communications, like mobile phones, PDAs, smart cards and sensor networks.EC point of multiplication operation is found to be computationally more efficient than RSA exponentiation. There have been many known cryptographic algorithms. The crux of any cryptographic algorithm is the "seed" or the "key" used for encoding/decrypting the material. Many of the cryptographic algorithms are available publicly, though some governments believe in having the procedure a secret. The general method is in using a publicly known algorithm while maintaining the key a secret.

Keywords- Ground water Detection, Swarm Optimization, Genetic Algorithm, Sensor Technology.

I. INTRODUCTION

ECC is the latest approach, and [1] measured as a wonderful method with low key size for the user, and has a solid exponential time challenge for a hacker to break into the system [2]. In ECC a 160-bit key offers the similar security as related to the out dated crypto system RSA with a 1024-bit key, thus lesser the computer power. Consequently, ECC gives significantly greater security for a given key size. Therefore, a key with small size makes it possible much more condensed executions for a given level of security which means faster cryptographic actions, running on smaller chips or more compact software. Additional, there are particularly efficient, compact hardware executions are available for ECC exponentiation operations, subscription potential reductions in application footprint even beyond those due to the shortest key length alone. Elliptic curve cryptography is not only appeared as an good-looking open key crypto-system for mobile or wireless atmosphere but also gives bandwidth savings. Elliptic curve cryptography is not easy to apprehend by attacker.

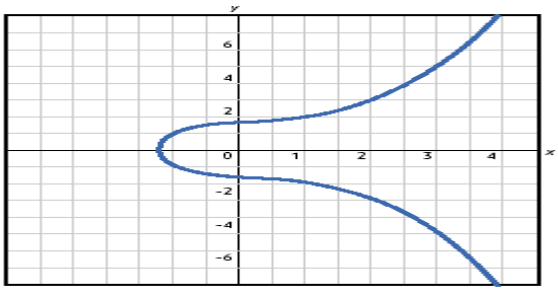

Fig.1: Elliptic Curve Cryptography

II. CRYPTOGRAPHIC METHODS

a) Symmetric ciphers,
b) Asymmetric ciphers and
c) Key exchanges

Symmetric ciphers are based on the extent of the key and the same keys are used to encrypt and decrypt data. Asymmetric ciphers consist of two dissimilar keys where one is the public key and private key. The refuge is based upon the component and the supporter used [3].

In general, symmetric key cryptosystems are favourite over public key systems due to the following factors:

1. Ease of computation
2. Reduced key length providing the same amount of security as compared to a larger key in Public key systems.

Hence the mutual method assumed is to use a public key system to securely transmit a "secret key". Once we have securely switched the Key, we then use this key for encryption and decryption using a Symmetric Key algorithm.

The idea of using Elliptic curves in cryptography was presented by Victor Miller and Neal Koblitz as an alternative to established public key organizations such as DSA and RSA. The Elliptical curve Discrete Log Problem makes it difficult to break an ECC as associated to RSA and DSA where the difficulties of factorization or the discrete log problem can be solved in sub-exponential time. This means that expressively smaller parameters can be used in ECC than in other

competitive organizations such as RSA and DSA. This helps in having smaller key size hence faster computations.

III. ADVANTAGE OF ECC

- ECC employs a relatively short encryption key a value that [6] must be fed into the encryption algorithm to decode an encrypted message.
- This short key is faster and requires less computing power than other first-generation encryption public key algorithms.

IV. APPLICATIONS OF ECC

Involving applications controlled channels; controlled channels are those, which are partial in memory, Processing and other resources. In some situations, following more pons of ECC and mainly useful.

1. Smaller keys
2. Smaller Signatures
3. Lesser certificates
4. Normal generation of key pair

Use of tokens and Smart card: development of smart card requires use of cryptography. Implementation ECC in such cases is essential

a) ***Smaller keys:*** smaller key sizes, Elliptic Curve Cryptography (ECC) [7] based signature schemes provide equivalent levels of security. ECC has additional advantages of being usable in environments that involve resource-constrained platforms. Like RSA, ECC based schemes are used for both digital signatures and encryption.

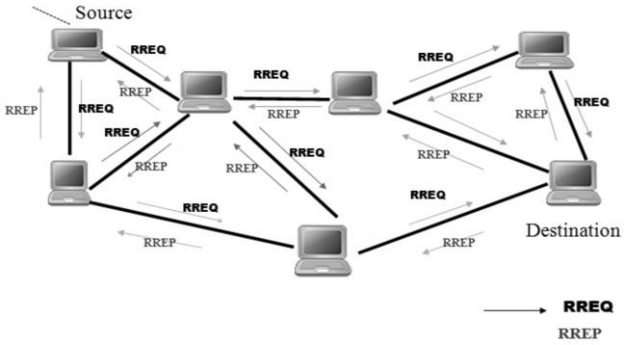

Fig.2 Architecture of the Network

V. RELATED WORK

Laiphrakpam Dolendro Singh et.al,2015 [4] described as elliptic curve cryptography has been a latest research area in the field of Cryptography. It offers higher level of security with smaller key size associated to other Cryptographic methods. A new method has been suggested in this paper where the standard procedure of planning the characters to affine points in the elliptic curve has been detached. The analogous ASCII values of the plain text are matching up. The opposite values serve as contribution for the Elliptic curve cryptography. This new method avoids the expensive operation of planning and the need to share the shared lookup table between the sender and the receiver. The procedure is intended in such a way that it can be used to encode or decrypt any type of writing with defined ASCII values.

K.S.Abitha et.al,2015[11] In this paper described as, protected data transmission using elliptic curve cryptography can be well-defined as transmission of data. This paper suggests a review about Secured data transmission using elliptic curve cryptography. The main problematic in present system is safety issues in transmitting data between foundation and the destination. After the review on various literature papers, they are concluding a new way that increases security deliberations of the network using AODV algorithm for transmission of data and to increment the efficiency of AODV algorithm using Elliptic Curve Cryptography.

D. Sravana Kumar et.al,2012 [12] described as Cryptography is the study of methods for confirming the privacy and authentication of the evidence. Public key encryption arrangements are secure only if the validity of the public key is guaranteed. Elliptic curve arithmetic can be used to progress a variety of elliptic curve cryptographic systems including key exchange, encryption and digital signature. The primary attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a reduced key-size, thereby reducing the dispensation overhead.

Tarun Narayan Shankar et.al,2009 [13] describes the simple idea of Elliptic Curve Cryptography and its execution through co-ordinate geometry for data encryption. Elliptic Curve Cryptography is an asymmetric key cryptography.

It contains

(i) Public Key group on the elliptic curve and its statement for data encryption and

(ii) Private Key group and its use in data decryption be contingent on the points on two dimensional elliptical curves.

Dr.R.Shanmugalakshmi et.al,2009 [14] The main reason of this paper to initiate the fast evolving cryptography investigators and to increase the security development in the arena of information refuge. In this article, a serious conversation about the comparison between ECC and other cryptography algorithms is tried to shape this article. Moreover, this piece explicates the role in the network

security. ECC's uses with smaller keys to deliver high security, high speed in a low bandwidth.

VI. ECC ATTACKS

A. Passive Attack

In practice, execution of an Elliptic Curve Scalar Multiplication can leak information [8] of k in many ways. The goal of the attacker is to retrieve the entire bit stream of k 1 using physical attacks. Physical attacks include mainly two types of attacks:

1) **Side Channel Analysis and**
2) **Fault Analysis**.

In this section, we briefly recap the known SCA also known as passive attacks on an ECC implementation. Most SCA attacks are based on power consumption leakage. Most often, electromagnetic radiation is considered as an extension of the power consumption leakage and the attacks/countermeasures are applied without change. For the sake of simplicity, we will only mention power traces as the side-channel to describe the known attacks. However, it is important to point out that EM radiation can serve as a better leakage source since radiation measurements can be made locally.

1) Simple Power Analysis

Simple power analysis attacks make use of distinctive key-dependent patterns shown in the power traces. when double and-add algorithm is used for a point multiplication, the value of scalar bits can[9] be revealed if the adversary can distinguish between point doubling and point addition from a power trace.

a) Template Attacks

A template attack requires access to a fully controllable device, and proceeds in two phases. In the first phase, the profiling phase, the attacker constructs templates of the device. In the second phase, the templates are used for the attack. The feasibility of this type of attacks on an implementation of the ECDSA algorithm. In a template attack on a masked Montgomery ladder implementation is presented.

b) Differential power analysis

DPA attacks use statistical techniques to pry the secret information out [10] of the measurements. DPA sequentially feeds the device with N input points Pi, i ∈ {1, 2, .., N}. For each point multiplication, kPi, a measurement over time of the side-channel is recorded and stored. The attacker then chooses an intermediate value, which depends on both the input point Pi and a small part of the scalar k, and transforms it to a hypothetical leakage value with the aid of a hypothetical leakage model. The attacker then makes a guess of the small part of the scalar. For the correct guess, there will be a correlation between the measurements and the hypothetical leakages. The whole scalar can be revealed incrementally using the same method.

c) Comparative Side-Channel Attacks

Comparative SCA resides between a simple SCA and a differential SCA. Two portions of the same or different leakage trace are compared to discover the reuse of values. The first reported attack belonging to this category is the doubling attack. The doubling attack is based on the assumption that even if the attacker does not know what operation is performed, he can detect when the same operations are performed twice. For example, for two point doublings, 2P and 2Q, the attacker may not know what P and Q are, but he can tell if P = Q. Comparing two power traces, one for kP and one for k(2P), it is possible to recover all the bits of k.

d) Zero-Value Point Attack

A zero-value point attack (ZPA) [1] is an extension of RPA. Not only considering the points (i.e. R[1] and R[0]) generated at step i, a ZPA also considers the value of auxiliary registers. For some special points P, some auxiliary registers will predictably have zero value at step i under the assumption of processed bits of the scalar. The attacker can then use the same procedure of RPA to incrementally reveal the whole scalar.

e) Carry-Based Attack

The carry-based attack is designed to attack Coron's first countermeasure (also known as scalar randomization). Instead of performing kP, Coron suggested to perform (k + r#E)P where r is a random number. The crucial observation here is that, when adding a random number a to a fixed number b, the probability of generating a carry bit c = 1 depends solely on the value of b (the carry-in has negligible impact [18]). If (k + r#E) is performed with a w-bit adder, where w is the digit size, the attacker can learn k digit by digit from the distribution of the carry bit.

2) Fault Attacks

Besides passive side-channel analysis, adversaries can actively disturb the cryptographic devices to derive the secret. Faults on the victim device can be induced with a laser beamer, glitches in clock, a drop of power supply and so on. Readers who are interested in these methods are referred to [34]. In

this section, we give a short description of the known fault analysis on ECC. Based on the scalar recovery method, we divide fault attacks on ECC into three categories, namely, safe-error based analysis, weak-curve based analysis and differential fault analysis

.***Safe-Error Analysis***

Basically these are two types: C safe-error and M safe-error

1) **C safe-error:** The C safe-error attack exploits dummy operations which are usually introduced to achieve SPA resistance. Taking the add-and-double-always algorithms [14, Alg. 1] as an example, the dummy addition in step 3 makes safe error possible. The adversary can induce temporary faults during the execution of the dummy point addition. If the scalar bit ki = 1, then the final results will be faulty. Otherwise, the final results are not affected. The adversary can thus recover ki by checking the correctness of the results.
2) **M safe-error**: The M safe-error attack exploits the fact that faults in some memory blocks will be cleared. To attack RSA. However, it also applies to ECSM. Assuming that R[ki] in Alg. 1 is loaded from memory to registers and overwritten by 2R[ki], then faults in R[1] will be cleared only if ki = 1. By simply checking whether the result is affected or not, the adversary can reveal.

Propose Algorithm

Step 1: A field size q, which is a large odd prime,$q \approx 2^{160}$ bit integer.

Step 2: Two parameters a,b ε F_q to define the equation of elliptic curve E over F_q,

Step 3: 3: A **f**inite point B = **$(x_B, y_B,)$** whose order is a large (160-bit) prime number in $E(F_q)$, where B is a point in $E(F_q)$

Step 4: The order of B = t.

Step 5. For

{

$1 \leq i \leq n$,

Select original signer A_i

for

{

$1 \leq d_i \leq t - 1$

//as private key, and computes the

//corresponding public key $Q_i = d_i$ X B = (x_{Q_i}, y_{Q_i}),

}

}

Step 6. Let h( ) be a public collision-resistant hash function that must be secure.

Step 7. Select Private Key (corresponds to A_i and Public Key Q_p)

V. CONCLUSION

In this paper concluding a new way, that increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of algorithm using ECC(Elliptic Curve Cryptography). Efficiency, and reliability will be increased for each transmission of data, While enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification, we are concluding that the Secured data transmission using elliptic curve cryptography provide a efficiency higher than vector when compared with ad-hoc. Any node in between source and destination can try to view the information. So the data which is transmitted has to be encrypted and decrypted so that the security issues will be eliminated and with the usage of the resources and effective delivery to the user, hence the proposed method will provide an effective solution that may help the source and destination to transfer data in a secured manner using encryption and decryption.

VI. REFERENCES

[1]. B.Schneier. Applied Cryptography. John Wiley and Sons, second edition, 1996
[2]. V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology - CRYPTO'85, LNCS 218, pp.417-426, 1986.
[3]. R. Schroppel, H. Orman, S. O'Malley and O. Spatscheck, "Fast key exchange with elliptic key systems", Advances in Cryptography, Proc. Crypto'95, LNCS 963, pp. 43-56, Springer-Verlag, 1995.
[4]. Singh, Laiphrakpam Dolendro, and Khumanthem Manglem Singh. "Implementation of Text Encryption using Elliptic Curve Cryptography."Procedia Computer Science 54 (2015): 73-82.
[5]. Kani, Ernst. "The State Of The Art Of Elliptic Curve Cryptography." Queen's University.
[6]. +Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. "Elliptic curve cryptography." Ubiquity 2008.May (2008): 7.
[7]. Afreen, Rahat, and S. C. Mehrotra. "A review on elliptic curve cryptography for embedded systems." arXiv preprint arXiv:1107.3631 (2011).
[8]. Gupta, Vipul, et al. "Performance analysis of elliptic curve cryptography for SSL." Proceedings of the 1st ACM workshop on Wireless security. ACM, 2002.

[9]. Chen, Tzer-Shyong, Yu-Fang Chung, and Gwo-Shiuan Huang. "Efficient proxy multisignature schemes based on the elliptic curve cryptosystem."Computers & Security 22.6 (2003): 527-534.

[10]. Li, Fengying, and Qingshui Xue. "Two improved proxy multi-signature schemes based on the elliptic curve cryptosystem." Computing and Intelligent Systems. Springer Berlin Heidelberg, 2011. 101-109.

[11]. K.S.Abitha et.al ," Secured Data Transmission Using Elliptic Curve Cryptography",International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 3, March 2015.

[12]. Kumar, D. Sravana, C. H. Suneetha, and A. Chandrasekhar. "Encryption of data using Elliptic Curve over finite fields." arXiv preprint arXiv:1202.1895(2012).

[13]. Shankar, Tarun Narayan, and G. Sahoo. "Cryptography with Elliptic Curves."International Journal Of Computer Science And Applications 2.1 (2009): 0974-1003.

[14]. Shanmugalakshmi, R., and M. Prabu. "Research issues on elliptic curve cryptography and its applications." International Journal of Computer Science and Network Security 9.6 (2009): 19-22.