A Review on Elliptic Curve Cryptography for Big Data Transportation

Dr. Anil V Turukmane, Post Doc Research Scholar, Lincoln University College, Malaysia. E-mail: Anilturukmane@gmail.Com

Dr. Divya Midhunchakkaravarthy, Lincoln University College, Malaysia. E-mail: Divya@lincoln.edu.My

Abstract--- In the year 1985, Miller Victor and his partner Koblitz Neal brought forth the concept of Elliptic curvesin Cryptography. The evolution of the concept of Elliptic Curve Cryptography (ECC) has led to the development of Public Key Cryptography Systems. Distinct set of keys are used for encoding and decoding data in this system. The size of the larger key decides how strong the security will be as one of the keys involved in the encryption have to distributed publicly. Prime Factorization and Discrete Logarithm played a major role in PKC systems. With the advent of Elliptic Curve Cryptography, it has be enable to ensure the similar level of security as was favored in PKC systems by the use of proportionate magnitudes of small key. Elliptic Curve Cryptography solely involves the practice of Application Based Specific Systems and the gamut of research in this field does not lie out of this practice. Restrictions do exist in this kind of system such as Specific Domain CPU architecture which is used for Big Data Transportation in Network and the amount of processing speed and storage that can be used.

Keywords--- ECC Cryptographic Algorithms, Low Bandwidth, High Speed, High Security.

I. Introduction

There has been a huge boost in Data Privacy and Security Requirements. Myriad domains such as Banking on Smartphones, use of a wrist watch to monitor the health of a patient and working on the go by being connected to office networks employ Data Protection and Authentication.

Elliptic Curve Cryptography is a group of things having similar characteristics of a Public Key Crypto-system based on Rivest, Shamir, and Adelman. Still it is distinct from what Shamir, and Adelman professed. The fast-paced advancement capabilities of Cryptographic Algorithms present an appealing substitute to Researchers. Commensurate degree of security in keeping with the RSA can be ensured with the use of Minor Keys of Elliptic Curve Cryptography. Consider Ex. The 163-bit architecture of Elliptic Curve Cryptography is a great alternative to the 1024-bit offered by Rivest, Shamir and Adelman without compromising on security. The 163-bit architecture provides a seamless compatibility with various Wireless Communications such as Smartphone Signals, Sensor Networks and Smart Cards. Main selling point of ECC is the Multiplication Operation which appears to be more than competent when compared to RSA Exponentiation

II. Mathematical Functions

Elliptic curve does not literally mean the shape of ellipse, the concept involved in measuring the circumference of ellipses uses Qubic Equations which are the similar kind of equations used in Elliptical Curve Cryptography, Hence the name.

$$Y2+Fxy+Gy=X3+Hx2+Ix+J$$

Where X and Y change their values to The Real Numbers which are F, G, H, I and J.

The Elliptic Curve E expressed as the Weierstrass Equation:

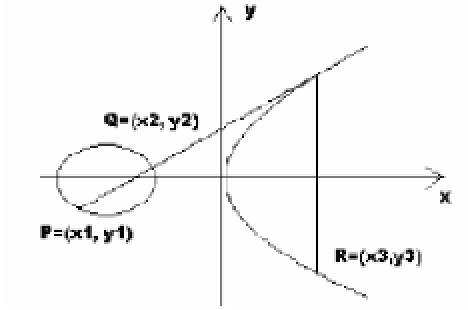
$$R2+Sy=S3+Tx2+H$$

Where S, R, T, H Єf2m,H≠0.

III. Point Addition

Point Addition: If B(P1,Ql) And D(P2,Q2) are points on the Elliptic Curve and If -Pi ≠P2 (Equally B≠-D),Then, S(P3,Q3)=B+D can be defined geometrically in the case B≠D,A Line intersecting the Curve at the points B And D must also intersect the Curve at a third point -S, And S(P3,Q3) is the answer, If B=D (Point Doubling),The Tangent Line is used

DOI: 10.5373/JARDCS/V11I12/20193218
ISSN 1943-023X
Received: 09 Oct 2019/Accepted: 12 Nov 2019

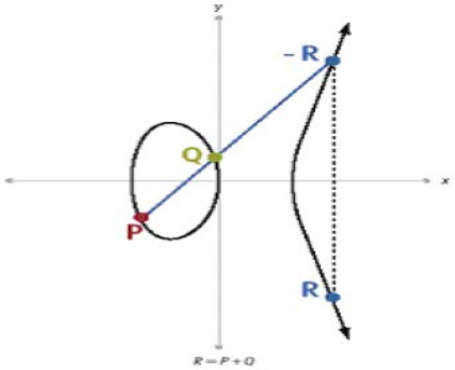


IV. Point Multiplication (Scalar Multiplication)

Point Multiplication also known as Scalar Multiplication is expressed by Repeated Addition.

F=Dg=G+G+.... +G (D times addition)

Elliptic Curve Discrete Logarithm Problem (ECDLP), upon which the Security of ECC is based is elaborated below. Given an Elliptic and a Point on it, to determine Df rom the F=Dg was, Where F and G are Points on the Curve and Dg means Gadded itself D Times. It is easy to get F From -H And G, Especially for thelarge Numbers.



V. Existing Surveys

Putting forth the current surveys which are accessible to us in Elliptic Curve Cryptography/Elliptic Curve Digital Signature Algorithm. The focal point of this survey is to study the varied facets of Elliptic Curve Cryptography / Elliptic Curve Digital Signature Algorithm. Starting with the point as to how our research varies extensively with the current available research. Listing various contemporary studies in Elliptic Curve Cryptography/Elliptical Curve Digital Signature Algorithm. Let us first deal with Efficiency and Performance Hardware implementation in the ECC algorithm has been analyzed for Flexibility and Performance with the help of Accelerators. Different aspects concerning Hardware implementations for ECC were put forth like Group Law, Selecting Curves, Selection of Coordinates and Pm Algorithms. It was highlighted that the efficiency of hardware implementation relies heavily on the Architecture of Multiple Scalar Multiplication in Ecdsa's verification. Ton of research exists confirming that the use of Hardware's Accelerators results in high performance, but it comes at a cost, it inhibits the flexibility feature, to enhance flexibility feature we take the help of Reduction Circuits. Likewise, Driessen Et Al. contrasted various signature schemes (ECDSA, XTR-DSA, And NTR Using) on different criteria such as, Performance, Memory, Energy Consumption, Keys Length and Signature. Though much testing Memory and Performance were a standout feature in the NTRU Sing algorithm. But what the NtruSing Algorithm makes up in memory and performance lacks in terms of security leaving it vulnerable to attacks. Hence the exhaustive study focusing on Attacks and Countermeasures named Security and Countermeasures in Ecc Algorithm is professed. By dividing the Attacks as Passive and Active the Authors theorized that the Countermeasures set in place for attacks may itself be vulnerable to attacks. In selecting countermeasures, the authors recommended studies. Surveys dealing with Public Cryptography Algorithms concerning problems that are hard in nature such as Discrete Logarithm Problem (DLP), Integer Factorization Problem (IFP), Lattices and Error Correcting Codes and their computation in Classical as well

DOI: 10.5373/JARDCS/V11I12/20193218
ISSN 1943-023X

Received: 09 Oct 2019/Accepted: 12 Nov 2019

as Quantum Computers were put forward. They as well quoted studies from Error-Correcting Code (Mceliece Cryptography) Rabin, RSA, ECDSA, ELGAMAL, ECDH and Lattices (NTRU), specifying that only ECC comes with a superior measure of security when compared to other Crypto-systems; It also comes with added benefits such as Less Storage, Small Keys Sizes and High Speed. When evaluating the physical attacks the authors distinguished them into two sets, Fault Attacks (FA) and Side Channel Analysis (SCA) in the study ECC Algorithm and Physical Attacks. Counter measures like the Differential Power Analysis (DPA), Fault Attack (Fa) and Simple Power Analysis (SPA) were also strongly favored also qualities that Add Randomness which makes dealing with Implementation and Countermeasures Selection easy were preferred.

VI. Applications and Implementation

Wireless Sensor Networks (WSNS) were scrutinized regarding the Security Techniques. The study focused on three aspects Key Management System, Secure Routing System and Authentication System. The situational analysis highlighted that for Constrained-Resource Devices ECC suited the most. In conjunction, a survey detailing the various strategies applied during attacks when dealing with bit coin and ethereum was presented in relation to Elliptic Curve cryptography and Elliptic Curve Digital Signature Algorithm. The Author argued that there exists distinct ideals for Curves (Ieee P1363,Safe Curves and Ansi X9.63) In comparison our Survey elaborated on Safe Curves while employing Secp256k1 with the help of ECDSA, confirming that Safe Curves has robust Curve ideals. Key methodologies to prevent future attacks on ECC were suggested by the author.

Contrasting of the ECC with RSA was carried out by Kim and Harkanson they came to the conclusion that ECC Algorithm grants the highest level of output if not more but Equivalent amount of security to the RSA. They illustrated that ECC Algorithm use makes up 69% of websites, whereas only 3% used RSA and the remaining used different Algorithms. Describing the real world applications of ECC in the field of E-Health, Iris Pattern Recognition and Vehicular Communication. Nonetheless, they discovered that there was a corollary between the Application and Implementation. When we take the example of RFID, a technology which is employed for the Implementation of a specific Application. My Survey elaborates upon the study of ECC Algorithm and in itself is quite distinct when compared to preceding research. First of all we assimilate three facets (Applications, Efficiency and Security) into single search

VII. ECC Algorithms for Enhanced Optimization and Performance

Varied Algorithms to enhance Performance and Optimization in Elliptic Curve Squaring, Point Multiplication and Multiplication Etc. are discussed below

Karatsuba Multiplication

The technique established by Of man and Karastuba allows for a reduction in Polynomial mathematical Equation replacing it for an incremental Number of Additions. As Long as the Time Ratio for executing a Multiplication Vs. an Addition is High, this back and for this more Efficient.

Consider the Example of Two Degree-1 Polynomials, 1 0 *E*(*Y*) = *EY*+ *E* And 1 0 *G*(*Y*) = *G Y* + *G*.

For the existing Method, We must calculate the product of each possible Pair of Coefficients.

H0 = E0 G0
H1 = E0 G1
H2= G1 G0
H3 = A1 G1

And then calculating the Product:

D(Y) = E(Y). G(Y) is:
D(*Y*)*= H3 Y+* (*H2 + H1) Y+ H0*

The Karatsuba multiplication Method Begins By Taking The Same Two Polynomials, And Calculating The Three Products

B0 = E0 G0
B= E 1g1
B2= (*E0 + E1) (G0 + G1)*

These we use the equation to assemble the Result

DOI: 10.5373/JARDCS/V11I12/20193218
ISSN 1943-023X
Received: 09 Oct 2019/Accepted: 12 Nov 2019

$D(Y) = E(Y).\ G(Y);$

$D(Y) = B1\ Y + (B2 - B1 - Be)\ Y + B0$

Check the above result if they are Equal. The existing Method needs 1 Addition and 4 multiplication, While the Karatsuba Method requires 3 Multiplications and 4 Additions. Thus Karatsuba multiplication procedure has1 Multiplication For 3 Additions. If the Cost to Multiply on the Target Platform is at least 3 times the Cost for Addition, then the Method is effective. While this basic form of Karatsuba has been presented in the original research Paper, there are a number of ways this Method may be expanded to handle larger Degree Polynomials. This is shown where the Authors give an In-Depth Study of this Method and its Variations..

VIII. Conclusion

This paper elaborates upon the Mathematical Functions prominently employed in ECC Algorithm. These Functions help in enhancing the Security, Performance and also aims to deliberate upon the Optimization of ECC Algorithm for future uses.

References

[1] I. Biehl, B. Meyer, And V. MUller. Di_Erential Fault Attacks On Elliptic Curve Cryptosystems, 2000.

[2] Bitcoincard.Org. Sample Transaction. 2012

[3] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, And B. Moeller., 2006.

[4] D. Boneh And I. Shparlinski. On The Unpredictability Of Bits Of The Elliptic Curve Di_E{Hellman Scheme.. Springer, 2001.

[5] E. Brier, M. Joye, And T. E. D. Win. Weierstra Elliptic Curves And Side-Channel Attacks. In Public Key Cryptography Pkc 2002, Volume 2274 Of Lncs, Pages 335{345. Springer, 2002.

[6] B. B. Brumley, M. Barbosa, D. Page, And F. Vercauteren. Practical Elimination and reliazation of An Eccrelated Software Bug Attack. Springer, 2012.

[7] B. B. Brumley And R. M. Hakala. Cache-Timing Template Attacks. In M. Matsui, Editor Springer, 2009.

[8] Bureau Of Engraving And Printing {U.S. Department Of The Treasury. Damaged currency. Http://Moneyfactory.Gov/Uscurrency/Damagedcurrency.Html, 2013.

[9] Bushing", H. M. Cantero, S. Boessenkool, And S. Peter. Ps3 Epic Fail. Http://Events.Ccc.De/Congress/2010/Fahrplan/Attachments/1780_27c3_Console_Hacking_2010.Pdf, 2010.

DOI: 10.5373/JARDCS/V11I12/20193218
ISSN 1943-023X

Received: 09 Oct 2019/Accepted: 12 Nov 2019