# Case Study Report-1

Akshay Hajare (SID 45756503)
ELEC8860 Engineering Unit
Macquarie University, NSW 2109 Australia
E-mail: akshay.hajare@students.mq.edu.au
5 MAY 2020

# New Efficient Architectures for Point Multiplication on Koblitz Curve

## Section-1:

This case study discusses elliptic curves and their use in cryptography. The emphasis is on the throughput advantages of using latest elliptic curve cryptography instead of a conventional cryptographic system like RSA and current cryptography systems like keys exchange algorithm to be obtained in the technical world. Unique applications are addressed for the secure data transfer and identity-based encryption. Fast reciprocals computation in F2n [1] using inversion operation is the key to the highly successful implementation mentioned in this report. Also, it discusses how this technique [1] outperforms the current hardware architectures in terms of processing time and memory wage.

To begin with, this technology made the public-key cryptography very reliable and much secure compared to the previous Elliptic curve systems. It requires small size key exchanges compare to the previous method which eased up the heavy tasks or calculations. With the reduction of key sizes, the data encryption between the two sides for various applications such as Key agreements, digital signatures have now been more rigid and fast. For e.g. in WhatsApp it takes a few seconds to decrypt the encrypted code through the use of personal keys without the interference of a third party. It has also made an important contribution to fast the calculation of large data inputs.

The key areas of contribution of this technology are
1) Mathematics of computing,
2) mathematical and numerical analysis
3) security and privacy
4) cryptography

Here, in this architecture the Gaussian Normal Basis (GNB) have been used over Normal Basis (NB) because it performs more straightforward and efficient multiplications compare to free squaring in architecture using cyclic shifts which makes multiplication more complex (NB). Choosing the coordinate system of curve and point is critical and has a major impact on the application of the elliptic curve. Many systems use Mixed and Projective co-ordinate systems which eases the inversion operations by performing fewer complex operations. But it adds more burden registers and control units which compromises the efficiency of the architecture. And also, the inversion operation should return to its final phase of ECC computations. For these reasons the Affine coordinates are used in this architecture to maximize the efficiency of the system.

The major contribution of Diffie-Hellman key exchange algorithm is, it tends to rely on exponentiation in a large group, and the group operation software implementation is generally computationally intensive. Efficient implementation would be for it to be widely distributed across a number of platforms, thus significantly improving Internet security by solving the question of key exchange for millions of host machines. According to Neal Koblitz [2] Elliptic curves are immune to Index calculus attack. It means same degree of security can be achieved for the Diffie-Hellman algorithm with the use of small numbers. This architecture uses fewer numbers while implementation than the originally proposed by Sun Microsystems Sun PRC. Utilization of small numbers helps saving the cost for computation and the computer gets faster. Since we assume no busy machine will invest more than a 0.l% of its cycles on key exchanges this architecture provides the same. The elliptic curve approach uses a group operation different than integers mod p multiplication. Instead, the operation is over the group of points on an elliptic curve, so the operation is more complicated arithmetically. The group size used in this implementation is roughly 2 to the power 115. And these group operations are implemented using Galois field (other finite field) F to the base2 to the power 155. Which offers more security than the working modulo a 512bit prime.

Changing the modulus from a 512-bit prime to a 1024 bit prime multiplies the cracking effort by a factor of 8 million in the discrete logarithm problem for modular arithmetic. In the elliptic curve example, requiring a corresponding increase in cracking effort involves adding just 46 bits to the field size. That would raise our field size to 201 bits from 155 bits.

Firstly, I selected this article because after reading both the papers I found this article is a complete package of knowledge. It contains 1) most recent research work which is the transient model shows how efficiently it reduces the cost and processing time of the machine with a simple algorithm.
2) advanced technology for the encryption and decryption. 3) Its applications over the wide areas of internet such as sending messages or emails and the main thing is how it actually works. 4) How the hardware systems are programmed to carry out specific task. 5) A glimpse how future technologies can replace this latest technology and what modifications we can do to achieve it [1]. 6) It describes the history of ECC how it all started from Neal Koblitz [2] to Transient method. 7) plenty of citations hence, more knowledge to gain. 8) The recent use of this technology in the form of crypto currency which on a bloom. 9) Detailed structure of the architecture and how it works.

Secondly, I am a big fond of cryptography I found out that this article discusses more about the hardware security as compare to the article “A HDL generator for flexible and efficient finite-field multipliers on FPGAs” which states more about the software. And my interest is in hardware field so that’s why I chose this article over other. Besides, this article is easy to understand compare to the other.

**List of the study and reviewing work done**:

1. Elliptic curve cryptography (ECC)
2. Key
3. Public-Key cryptography
4. Digital signatures
5. Key agreements
6. Security and Privacy in ECC

7. Mathematical and numerical analysis in ECC
8. Point multiplication
9. Affine coordinate
10. Diffie-Hellman key exchange algorithm
11. Transient mode
12. Koblitz curves
13. Galois field (Other finite field)

## Section-2:

1. Elliptic curve cryptography (ECC)

   It is the unique way to introduce Public-Key cryptography purely based on finite sets of identities (axioms) which is also called as algebraic structure on the curve which tends to be elliptic over a finite field. Each identity holds the information in the form of bits.

2. Key

   It is the essential part of the cryptography system which holds a specific value to encrypt or decrypt the information. It may be private or personal. For e.g. In an e-mail system the sender holds the public key while the receiver holds the private key.

3. Public-Key cryptography

   This cryptographic system comprised of a pair of keys mainly public and private. As the name says public keys are available to everyone while the private key is always hold by the owner. These keys can be generated by the special cryptographic algorithms. To maintain the security, one should not lose its private key.

4. Digital signatures

   It is a tool to verify the authenticity of the digital data (message or documents). It demonstrates the firmness of the security system weather the data is of a particular person’s or not.

5. Key agreements

   It is the protocol decided by two or more parties in such a way that any one of them can alter the outcome. Third parties cannot interfere in this agreement. Nowadays many key exchange systems are generated by a single party which can send the key to the other party, but that party won’t have the influence to change the agreements.

6. Security and Privacy in ECC

   This contains public-key techniques and its encryption which is done through the special cryptographic algorithms used to transfer keys from one party to another. The security is monitored by the digital signatures.

7. Mathematical and numerical analysis in ECC

   This field contains the computing of all the mathematical expression such as computations of polynomials, complexity and cryptography, and randomness geometry and discrete structure. With the help of latest inversion algorithm these tasks can be solved within a record time.

8. Point multiplication

   It can simply be calculated through repeated addition but in real time scheme equations are very lengthy and complex hence this method won't apply. For this Double and add method introduces as a successor to point multiplication.

   equation $y2 + zy = x3 + ax2 + b$.(e.g.)
   Here a and b are taken as constants from the finite field F2 to the power 155. Where b is a non-zero prime number. Variables x and y are also numbers from F2 to the power 155. Here first we add two points (x1,x2) and (y1,y2). Then we double the points (x,y). At last, we negate a point (x,y).

9. Affine coordinate

   It can be described by an ordered pair of non-collinear vectors (on a plane) e1 and e2 and a coordinate origin point O. The straight line which passes through origin point O and parallel to the basis vectors which are e1 and e2 is called affine coordinate. Vectors e1 and e2 show the positive direction of the coordinate axes. Axes which are parallel to e1 and e2 are also called as abscissa and ordinate axis.

   not(OM)=$xe_1+ye_2$.
   Here in this equation x is abscissa, and y is an ordinate axis.

10. Diffie-Hellman key exchange algorithm

    This algorithm can be implemented using group of points on an elliptic curve over a finite field by formula F2 to the power m. Where m is the prime number and, in this architecture, we used m as 155. It is used to start encrypted conversion between two parties which are unknowns. This algorithm suggested instead of using 192-bit modulus which is very risky and can be breached within 3 months developers should use 512-bit modulus. But it requires extra time to calculate hence this plan dropped out by Sun microsystems.

11. Transient mode

    It is a simple version of Diffie-Hellman key exchange algorithm. Here two parties select a random exponent e and interchange values of g (group element) to the power e. If a party selects a as an exponent and the other party selects b then the information exchange will result into g to the power(a*b). but its highly impossible. In this article at first, they tried to implement using ring Zp where p is 512 prime bits. Although this provides security, but its machine consumption ratio is more than 0.1% hence it slows the machine.

    This setback encouraged the developers and they managed to develop new algorithm which uses the size of a group as 2 to the power 155. And combining with Galois field it resulted

into F 2 to the power 155. This algorithmic value increases the computation speed and consumes less space.

12. Galois field (Other finite field)

    It is nothing but a finite field which comprises of finite sets of elements. Like other finite fields it is a set on which operations like multiplication, division, addition are defined and verified by a certain rule.

13. Koblitz curves

    Koblitz curves are a type of elliptic curves distinguished by their non-random construction that enables especially effective computation. This is different from the most widely used elliptic curves with a pseudo-random structure where a specified algorithm selects the parameters. Neil Koblitz [2] was first to introduced elliptic curves usefulness in a cryptography. This curve used to define binary anomalous curves over GF (2 to the power k). The process of selecting the recommended parameters associated with a Koblitz curve is by selecting repeatedly parameters that make an efficiently computable endomorphism until a prime order curve is found. The online cryptocurrency company name Bitcoin implemented this method. However, due to some security issues the company owner switched to non-random secp256k1 over pseudo-random secp256k1.

## Section-3:

**Ratings and Justification:**

**Tutorial – 8**

This is the idle tutorial which every student must read. It perfectly defines the research work, technology advancement, origin of the basic architecture, detailed theory, algorithms, future glimpse of the new technologies, present applications. However, some terms are very new and in complex language and most of the terms are unknown to me.

**Advance of Theory – 9**

In this article the new advanced theory has been proposed which overcomes all the current architecture technology in terms of efficiency, cost and speed configurations.

**Advance of Application – 6**

The proposed technology is fully capable of advancements in future applications, but the sources provided here are very limited and not too in detail. Less theory about general applications, hence difficult to understand.

**Presentation of Article – 8**

The presentation is great from headings to the citation everything is organized and in a good professional manner. But the language is somewhat difficult to understand.

**Future work and suggestion:**

In future I would suggest continuing with the “other finite fields” because it makes inversion implementation less costly and perfectly suited for ECC. And also, with slight modifications in its reciprocal algorithm we can compute reciprocals in ordinary integer modular arithmetic. 2 to the power A – 2 to the power B -1 is the basic algorithmic equation which can be used effectively with 2 to the power A - k2 to the power B – 1 for 32-bit k. The additional advantage of this is when reciprocal costs just a few multiplications, addition-subtraction chains can be used to quantify capacity, allowing for shorter chains more than recovering investment in reciprocal computing. Hence, by future perspective this method has a lot of potential to become a future trend.

## References:


[1] Reyhani-Masoleh, A., El-Razouk, H., Monfared, A.: New multiplicative inverse architectures using gaussian normal basis. IEEE Transactions on Computers 68(7), 991–1006 (2018)

[2] NEAL KOBLITZ, “Elliptic Curve Cryptosystems” , Mathematics of Computation, 48 n. 177 (1987), 203-209.