A review on Elliptic Curve Cryptography

[1]Gulivindala Suresh, [2]N.V.Lalitha
[1,2]Assistant Professor, Department of ECE,
[1,2]GMR Institute of Technology, Rajam, AP, INDIA.

Abstract: Elliptic curve cryptography (ECC) is basically a Public-Key Cryptography (PKC). EKC requires public and private key and also a group of operations linked with the keys to perform encryption. Its mechanism uses the algebraic arrangement of elliptic curves over finite fields. ECC is used for data encryption for real time applications and can be implemented through software or hardware**.** This study reviewed the implementation of Elliptic Curve Cryptography through both software and hardware.

***IndexTerms* – Elliptic curve cryptography, elliptic curve, public key.**

I. INTRODUCTION

Cryptography is the science of secret writing is an ancient art; the first documented use of cryptography in writing dates back to 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the internet. There are five primary functions of cryptography [1]: 1.Privacy/confidentiality, 2. Authentication, 3. Integrity, 4. Non-repudiation, 5. Key exchange.

II. TYPES OF CRYPTOGRAPHY

Cryptographic techniques are classified [2] based on keys used for encryption and decryption. These are classified into three types and are detailed below and shown in Figure 1.

i. Secret Key Cryptography (SKC): It employs a single key for both encryption and decryption; it is basically used for privacy and confidentiality.

ii. Public Key Cryptography (PKC): It adopts public key for encryption and secret key for decryption; therefore called asymmetric encryption. It is basically used for key exchange, non-repudiation and authentication.

iii. Hash Functions: It employs a mathematical transform to irrevocably "encrypt" data, providing a digital fingerprint. Primarily used to verify trustworthiness of the message [3].

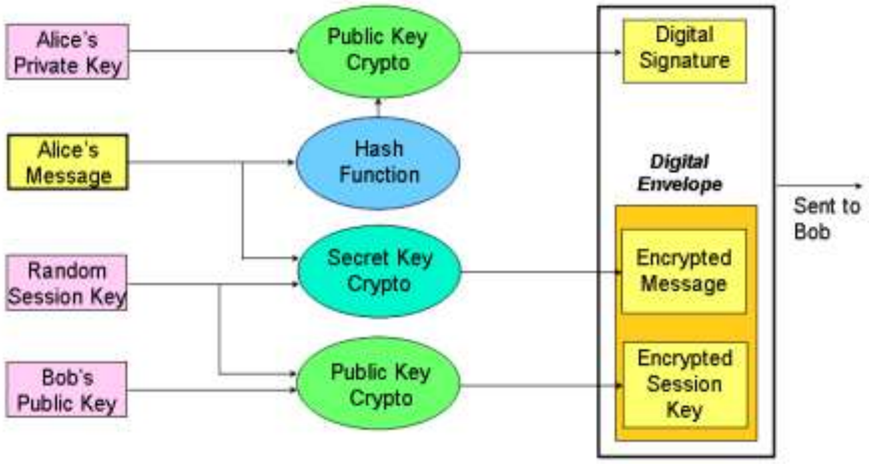

Figure.1: Different kinds of Cryptography

III. LITERATURE REVIEW

3.1 ELLIPTIC CURVE CRYPTOGRAPHY

In 1985, Victor Miller (IBM) and Neal Koblitz (University of Washington) proposed Elliptic Curve Cryptography (ECC) was proposed independently. Elliptic Curve Discrete Logarithm Problem (ECDLP) [4] is the base for the providing security in cryptosystems. ECC depends on difficulty of the ECDLP; the difficulty order magnitude is harder than others cryptosystems. This made ECC system more powerful than others. EKC requires public and private key and also a group of operations linked with the keys to perform encryption. Its mechanism uses the algebraic arrangement of elliptic curves over finite fields [4] as shown in figure 2.

One can refer to Lawrence C. Washington [5] for better understanding of elliptic curves and proofs for many theorems are also available. Jorko Teeriaho gave a very clear example implementation of ECC-DH key exchange, ECC encryption, Elliptic Curve Digital Signature using Mathematica [6]. Scott A. Vansfone provides an overview of current ECC standards and its application and advantages [7]. W. Stalling [8] has given a detailed explanation of various cryptographic techniques in his book “Cryptography and Network Security”.

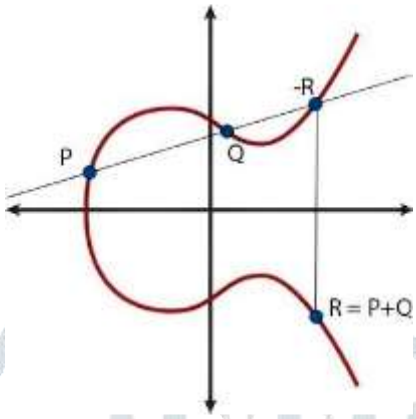

Figure.2: Elliptic Curve

3.2 ELLIPTIC CURVE CRYPTOSYSTEMS ON SOFTWARE

Over the past 15 years, numerous works have been written on various aspects of ECC software implementation. Most of these works does not consider all the factors, which contribute towards an efficient implementation. Elliptic curve cryptosystems have been extensively studied not only by the research community but also by industry. In particular, there are several standards involving ECC, namely IEEE P1363. The main scope of software implementation is to find the execution time of the algorithm. Normally, execution time refers to the time that an algorithm takes to complete a particular task. Some of the ECC works implemented in software are reviewed and given in Table 1.

Table 1. Review of Elliptic Curve Cryptosystems on Software

S.No	Reference	Approach	Remarks
1	[9]	Cryptographic transformation, arithmetic operation in elliptic curve point group and CPU commands, implemented in JAVA	Moderate speed and high accuracy Limited physical security and storage
2	[10]	Sliding window algorithm	Fast and portable
3	[11]	Montgomery multiplier, implemented in assembly languages	Execution is fast and it is 11.3 nsec
4	[12]	Elliptic curve operations and binary field arithmetic	Fast and efficient
5	[13]	Projective coordinates system and uniform addressing technique	High performance
6	[14]	Mixed coordinate system	Fast and effective

3.3 ELLIPTIC CURVE CRYPTOSYSTEMS ON HARDWARE

The swift advancement in technology and computational effort may doubt the strength of security of ECC. Mostly, security of the practical cryptosystems is mainly depends on computational assumptions. Mathematically, it is possible to decipher the secret information without knowing the secret key and this occurs normally in hardware implementations. Hardware implementations are vulnerable to side channel attacks, though hardware executes the algorithm through the design architecture [15]. Many works addressed this issue especially for ECC and also provided countermeasures to these side channel attacks. Table 2 illustrates the review of elliptic curve cryptosystems on hardware.

Table 2. Review of Elliptic Curve Cryptosystems on Hardware

S.No	Reference	Approach	Remarks
1	[16]	Optimized version of Montgomry’s method on non-super singular elliptic curves	Requires less memory and fast
2	[17]	Carry free Montgomery invrsion approach implemented on CMOS technology	Faster and requires less area
3	[18]	Employed an ALU for ECC field arithmetic	Low power, compact and low cost
4	[19]	Specific type of addition chains for addition and multiplication	Fast and secure

5	[20]	Elliptic curve point operation on modified Jacobian coordinates	Low power, low area
6	[21]	Sunar-Koc multiplication	Low power, low area
7	[22]	Karatsuba method for multiplication	Low power, low area
8	[23]	Recursive Karatsuba-Offman multiplier is employed	Low power, low area
9	[24]	Fuzzy modular arithmetic on AT89C51 microcontroller	Low power, low area
10	[25]	Pipelining concept for multiplication	Fast, low area

IV. CONCLUSION

Cryptography is the art of encrypting the data. Various types of cryptography are discussed and presented the process of Elliptic Curve Cryptography. ECC can be used for data encryption for real time applications. ECC can be implemented using software and implemented on hardware. This study reviewed the implementation of Elliptic Curve Cryptography on software and hardware.

REFERENCES

[1] Gary C. Kesssler, “An Overview of Cryptography”, February 2018.

[2] Diffie, Whitfield; Hellman, Martin"Multi-user cryptographic techniques", AFIPS Proceedings. 45: 109–112, Foreign Affairs.

[3] Kahn, David (Fall 1979). "Cryptology Goes Public". Foreign Affairs. 58 (1): 153. doi:10.2307/20040343.

[4] Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, 1996. ISBN 0-471-11709-9.

[5] Lawrence C. Washington, “Elliptic Curves Number Theory and Cryptography”, Taylor & Francis Group, Second Edition 2008.

[6] Jorko Teeriaho, “Cyclic Group Cryptography with Elliptic Curves”, Brasov, May (2011).

[7] Scott A. Vansfone, “Elliptic Curve Cryptography-The Answer to Strong, Fast Public-Key Cryptography for Securing Constrained Environments, Information Security Technical Report”, 1997, IEEE vol. 2, no. 2, pp. 78–87.

[8] Williams Stallings, “Cryptography and Network Security”, Prentice Hall, 4th Edition, 2000.

[9] V. Miller, “Use of Elliptic Curves in Cryptography”, April 1986, Advances in Cryptology - Crypto '85 proceedings, Lecture Notes in Computer Science, Springer-Verlag Berlin, Vol. 218/1986, pp. 417-426.

[10] N. Koblitz, “Elliptic Curve Cryptosystems”, Mathematics of Computation, June 1987, Vol. 48, No. 177, pp. 203-209.

[11] R. Kodali and H. Budwal, “High performance scalar multiplication for ecc,” in International Conference on Computer Communication and Informatics (ICCCI), 2013, Jan 2013, pp. 1–4.

[12] R. Kodali, S. Karanam, K. Patel, and H. Budwal, “Fast elliptic curve point multiplication for wsns,” in TENCON Spring Conference, 2013 IEEE, April 2013, pp. 194–198. [8] B. Sunar and C. K. Koc¸, “An efficient optimal normal basis type ii multiplier,” July 2001, IEEE Transactions on Computers, vol. 50, no. 1, pp. 83–87.

[13] Khabbazian, Majid, B.Sc., "Software elliptic curve cryptography.", 2004.

[14] Zhou, Yongbin & Feng, DengGuo. 2005. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing.. IACR Cryptology ePrint Archive. 2005. 388.

[15] Dan, Y., Zou, X., Liu, Z. et al. J. Zhejiang Univ. Sci. A 2009 10: 301. https://doi.org/10.1631/jzus.A0820024

[16] E. Savas, "A carry-free architecture for Montgomery inversion," Dec. 2005, in IEEE Transactions on Computers, vol. 54, no.12, pp. 1508-1519.

[17] Batina, Lejla & Mentens, Nele & Sakiyama, Kazuo & Preneel, Bart & Verbauwhede, Ingrid. 2006. Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks. ESAS 2006. 6-17. 10.1007/11964254_3.

[18] Nicolas, Meloni. 2006. Fast and Secure Elliptic Curve Scalar Multiplication Over Prime Fields Using Special Addition Chains.. IACR Cryptology ePrint Archive. 2006. 216.

[19] Jiahong, Zhang & Tinggang, Xiong & Xiangyan, Fang. 2010. A Fast Hardware Implementation of Elliptic Curve Cryptography. 1519 - 1522. 10.1109/ICISE.2009.29.

[20] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, “Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks”, ESAS 2006, LNCS 4357, pp. 6–17.

[21] A. Karatsuba and Y. Ofman, “Multiplication of multidigit numbers on automata,” in Soviet physics doklady, vol. 7, 1963, p. 595.

[22] Z. Ge, G. Shou, Y. Hu, and Z. Guo, “Design of low complexity gf (2ˆm) multiplier based on karatsuba algorithm,” in 13th International Conference on Communication Technology (ICCT), 2011, pp. 1018–1022.

[23] Gopinath Ganapathy and K. Mani, “Maximization of Speed in Elliptic Curve Cryptography Using Fuzzy Modular Arithmetic over a Micro-controller based Environment”, June 2009, Proceedings of the World Congress on Engineering and Computer Science, vol. 1.

[24] Lo’ai Tawalbeh, Moad Mowafi and Walid Aljoby, “Use of Elliptic Curve Cryptography for Multimedia Encryption, IET Information Security”, December 2012 vol. 7, issue 2, pp. 67–74.

[25] H. Marzouqi, M. Al-Qutayri, K. Salah, D. Schinianakis and T. Stouraitis, "A High-Speed FPGA Implementation of an RSD-Based ECC Processor," Jan. 2016 in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 1, pp. 151-164.