ECS Transactions

The Electrochemical Society
Advancing solid state & electrochemical science & technology

A Comprehensive Survey on Lightweight Asymmetric Key Cryptographic Algorithm for Resource Constrained Devices

To cite this article: Ananiah Durai Durai Sundararajan and Rajashree R 2022 *ECS Trans.* **107** 7457

View the article online for updates and enhancements.

ECS Transactions, 107 (1) 7457-7468 (2022)
10.1149/10701.7457ecst ©The Electrochemical Society

A Comprehensive Survey on Lightweight Asymmetric Key Cryptographic algorithm for Resource-Constrained Devices

[1]Rajashree .R, [2]Ananiah Durai .S*,

[1]SENSE, Vellore Institute of Technology, Chennai, India
[2]CNVD, Vellore Institute of Technology, Chennai, India, ananiahdurai.s@vit.ac.in

Elliptic Curve Cryptography, a popular lightweight asymmetric key cryptographic algorithm, widely adapted to meet the high-security requirement of resource-constrained devices especially for the popular IoT applications, is surveyed in this work. Further, ElGamal cryptosystem, Elliptic Curve Digital Signature Algorithm, and Elliptic Curve Diffie Hellman Key Exchange Algorithm have been comprehensively reviewed with its characteristics and preferred applications. In addition, a few related works are analyzed, and suggestions for suitable target applications were provided. Moreover, an earlier reported ECC cryptographic technique, is modeled using Vivado tool for target implementations on the few advanced FPGA devices. Strategies that enhance throughput, area and computation time that specifically caters to IoT applications were also reviewed. Design implementations on the advanced FPGA boards for IoT devices/similar applications were also analyzed and compared.

Keywords—Asymmetry key cryptography; Elliptic Curve Cryptography; Resource-constrained;

Introduction

Heterogeneous and high-speed applications utilizes the popular IoT platform enabled through the advanced network communication technologies. The devices involved in IoT for communication and networking are compact, low power and battery-operated devices. A device involved in realizing the IoT have a unique identifier, which automatically collects the data and exchanges the information over the network. The number of devices that interconnects the entire globe is increasing day by day and might reach 50 billion (1) soon. The unprotected networked devices are vulnerable to increased scrutiny resulting in security issues such as eavesdropping, hacking, data breaching etc. Cryptographic technique if employed over such unsecured communication backbone will ensure that the information sent over the network is illegible to the third party (1), thereby improving the security to a greater extend. Cryptography can be broadly classified into symmetric key cryptography and asymmetric key cryptography or public-key cryptography. The private key cryptography technique uses the same secret key between the sender and receiver for encrypting and decrypting the data. The private key cryptography techniques such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Triple-DES algorithm require separate private channels to share the key, and if one key is compromised, the eavesdropper will retrieve the data easily (1). Such issue in symmetric key cryptography is eliminated by the popular Public key cryptography algorithms such as Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC) and Hyperelliptic Curve Cryptography (HECC). The public key cryptography technique uses two keys such as a private key for encryption and a public key for decryption or vice versa (3). The above-mentioned cryptographic algorithms enable to secure the data and information against any internal or external attacks. It also provides security services and mechanisms such as data confidentiality, data integrity, access control, non-repudiation, and denial of service for resource-constrained devices (2). This paper surveys the reported public-key cryptographic algorithms that were developed and implemented for resource-constrained devices especially that are employed in IoT applications. It also compares the performance of the various work on lightweight asymmetric key cryptographic algorithms in the context of a resource-constrained application such as IoT.

This paper is organized as follows: Section II briefly explains the types of Public Key Cryptosystems with a respective illustration. Section III describes the mathematical background of ECC. Section IV relates the work done concerning applications of a lightweight cryptographic algorithm for resource-constrained devices. Section V provides FPGA implemented results of the various ECC design. Section VI gives detailed information about software and hardware specification to implement the cryptographic algorithm. Section VII various possible attacks on ECC are discussed with its countermeasures, and finally the article is concluded with a narrative on the best target implementation and prospective future research avenues.

Public Key Cryptography

Asymmetric key cryptography techniques make use of two keys for the information exchange. The public key is used for encryption, and a private key is used for decryption. Public key cryptography (PKC) based information transfer uses cryptographic algorithms such as RSA, DSA, and ECC. ECC has recently emerged as a preferred crypto style to replace the RSA algorithm due to its shorter key length and reduced power consumption while maintaining a similar level of security. High-speed design strategies on ECC are required for many hardware implementations, especially in IoT based resource-constrained environments such as sensor networks, biomedical, etc. The complex structure and mathematical computation involved in ECC promotes the construction of a cryptosystem that is highly challenging for the adversary to retrieve the data (1). The group points on elliptic curve that are determined using various number systems that yields a complex crypto style are discussed in the subsections.

Basics of Elliptic Curve Cryptography

ECC is one of the powerful public-key cryptographic techniques which has a shorter key size of only 160 bits. In these dual key techniques, the sender X utilizes the secret key, and the public key is assigned to the receiver Y for secured communication. ECC is widely used as the complexity in ECDLP (Elliptic curve discrete logarithm problem) proves to be tough enough that makes it hard for the adversary to determine the points from A = Q×B, where Q is the key and $A, B \in E_p(\alpha, \beta)$. p denotes prime number such that key-value Q must be less than the chosen p. In a real-time application, the value of Q is always kept large, so the determination of Q by the brute force method is impractical. Elliptic curves are described in general by the cubic equation as in [1] below;

$$y^2 + \alpha xy + \beta y = x^3 + \gamma x^2 + \Phi r + \mu \qquad [1]$$

Where x and y are the values of the points on the curve and α, β, γ, Φ and μ are the real numbers (4).

A typical illustration is considered here to determine points on the curve. If the message input is taken as character 'G,' its ASCII value will be 71, for which the plaintext 'm' can be considered as 71. Steps involved in computing the ciphertext are as follows (5);

- Step 1: The simplified form of [1] can be given as;

  $$y^2 mod\ p = (x^3 + \alpha x + \beta)\ mod\ p \qquad [2]$$

  If the prime number is considered to be 13 with $\alpha = \beta = 1$, then the equation '$4\alpha^3 + 27\beta^2 \neq 0$' must be satisfied (5).
- Step 2: The possible set of points (x, y) found from [2] can be given as below; ((0,1), (0,12), (1,4), (1,9), (4,2), (4,11), (5,1), (5,12), (7,0), (8,1), (8,12), (10,6), (10,7), (11,2), (11,11), (12,5) and (12,8)).
- Step 3: To transmit 'G' from the sender to the receiver using the above points, the message should be represented as message point 'Mp'. Therefore, message points must be calculated using the Koblitz method. The corresponding plaintext point x for the message can be computed from the relationship x = mk, according to the Koblitz method with 'm' being 71 and k chosen as 2.
- Step 3: If valid x is not found in the possible sets of step 2, then go for x = mk+1, x = mk+2 up till y exists. Once x is found, the corresponding value of that set is chosen as y, which constitutes Mp.
- The computed M_p is then used in to obtain the ciphertext point from the below equation;

  $$C_m = (Q * B, M_P + QP_Y) \qquad [3]$$

  Where Q is the Positive random integer, B is the Elliptic curve point from the group $E_p(\alpha, \beta)$, M_p, the message point in which 'G' is hidden, and P_Y is the Y's Public key.

In order to decrypt and get back the plaintext, the following computation must be performed.

$$M_P + QP_Y - n_Y(QB) = M_P + Q(n_Y * B) - n_Y(QB) = M_P \qquad [4]$$

Where Q = Positive random integer and $_{NY}$ is the receiver's private key.

Mathematical Background of ECC

A brief mathematical overview for the key generation considering prime field point sets on the elliptic curve is provided in this section. This enables better understanding on the complexity of the ECC cryptography for the beginners. The general equation for the elliptic curve E (α, β) based on cryptographic algorithms are very famous due to its Discrete Logarithmic Problem compared to integer factorization in RSA (6). An elliptic curve is classified into different types based on number systems such as real numbers, prime numbers and Galois (binary) fields. Figure 1 shows the block diagram of the classification.

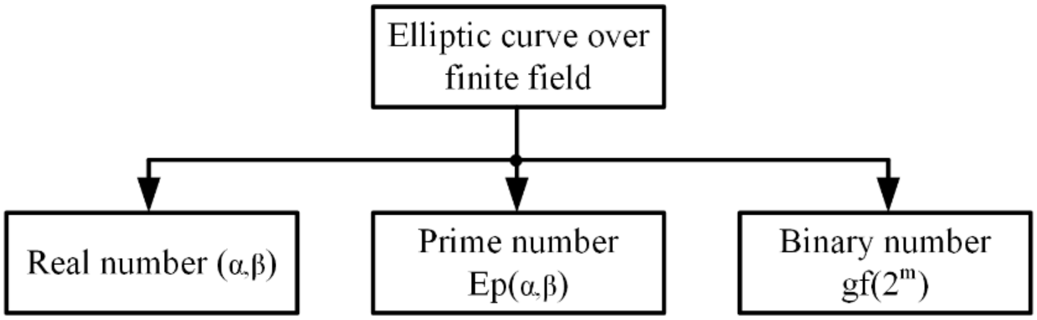

Figure 1. EC based on real numbers, prime number and Galois (binary) field (1)

Elliptic Curve over Prime Field

Consider (1) the Weierstrass equation for an elliptic curve over prime number E_p shown in [1], which was re-written [2]. Assume the value of α and β as (1, 1) with prime number p chosen as 13, Equation [2] is solved to obtain the set of points satisfying the elliptic curve over a prime field. The point addition formula is used to generate the ECC private key with the help of points set on the elliptic curve, as explained in the previous section. If point A = (r_A, s_A) and B = (r_B, s_B) belongs to elliptic curve E, then the addition of these point results in C = (r_C, s_C). ECC-based point addition and doubling used for adding two-point. Points on ECC are shown in equations [5], [6], [7], and [8] below.

$$x_C = (\Psi^2 - x_A - x_B)\ mod\ p \qquad [5]$$

$$y_C = (\Psi(x_A - x_C) - y_A) mod\ p \qquad [6]$$

$$\Psi = \left[\frac{y_B - y_A}{x_B - x_A}\right] mod\ p\ \ if\ A \neq B \qquad [7]$$

$$\Psi = \left[\frac{3x^2{}_A + \alpha}{2y_A}\right]^2 mod\ p\ if\ A = B \qquad [8]$$

Also, an elliptic curve, E: s^2 mod 97= (x^3 + 82x + 13) mod 97 defined over the prime field of a prime 97, is shown in Figure 2.

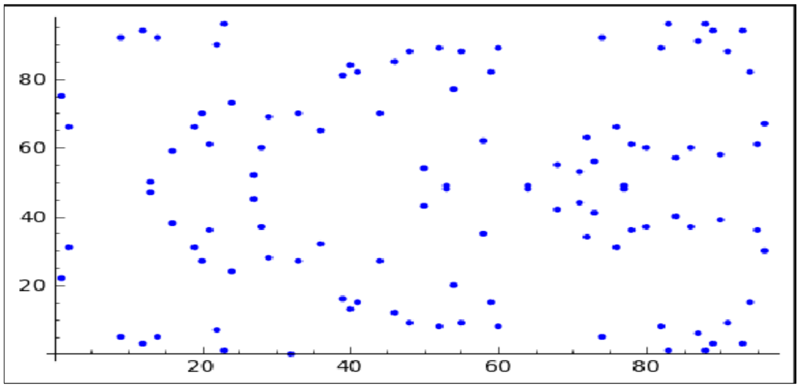

Figure 2. Elliptic Curve over prime field E: s^2 mod 97= (x^3 + 82x + 13) mod 97 (7)

Implementation Techniques of ECC

Implementation techniques of lightweight cryptography on various target devices and applications were discussed in the subsequent sections. IoT being the primary application on the various reported work is considered for review in this work. Reported designs on the basis of improved security levels and better shielding capability towards several attacks were considered for review. Further, specific designs on IoT irrespective of the target implementation were discussed in the first subsection. The second subsection primarily deals with the FPGA device as the target implementation device, with the area, time, throughput, and efficiency is the parameter of interest. Finally, in the end, advanced ECC techniques that utilize DNA computed encoding for enhanced security level is reviewed. The popularity of the application-specific design and implementation has driven this review on each specific context of parameter improvement.

Lightweight Cryptography Algorithms

ECC and isogeny-based OTP generation method is proposed in (8) to authenticate the IoT devices in which a new key is shared between server and client. Here, the new key was evaluated and performed on both resource-constrained and non-constrained devices. It is not possible for the server to produce the key using the challenge-response, and it also does not rely on the counter/timestamp. For each communication session, a new OTP is generated and shared between the server and IoT devices which achieve low power and energy with the help of ECDH. Chiranjeevi (9) proposed a novel ECC-based lightweight architecture for IoT environments, which consists of a password management server, service provider server, and client PC. It helps to avoid insider attacks and also has a low computational cost to provide the authentication service with an increased level of security.

A new device control scheme is designed for the IoT environment by using the certificate and ECC-based key agreement protocol (10). It utilizes the one-way hash function and ECC features to offer secure data communication between the IoT devices. Here, both Real-Or-Random (ROR) model-based formal and informal security analysis techniques proved that the security level of the proposed certificate-based device control scheme is high. Khalid Mahmood (11) developed a Physically Unclonable Functions (PUF) based authentication protocol for multi-server D2D communication, which increases the difficulty level for the attackers to clone the credential used in the mobile devices. Random-Oracle-Model is introduced to fulfill the security need for multi-server infrastructure. It also exploits the features of ECC to devise the identity-based key agreement protocol for efficient data processing in D2D communication.

An ultra-lightweight ECC-based Multi-factor method authentication algorithm (12) is investigated for IoT application combining the benefits of ECC and linear congruential method to improve the security level. Here, time-sharing point multiplication is used to provide the highly secured key exchange and agreement protocol. As a result, it achieves secure communication with low overhead for IoT communication. The papers (13)(15)(16) presented about lightweight ECC-based RFID authentication scheme, and it provides security against many attacks such as impersonation attacks and server spoofing attacks by using the ECC features. It is claimed that this protocol can be further improved to prove the security against side-channel attacks. A secure framework is designed for IoT-based Medical Sensor Data (14) by adding biometric information for login credentials and increasing the security level by applying Substitution-Ceaser cipher and improved Elliptic Curve Cryptography. In this, ECC generated secret key reduces the computational cost, processing time, and average correlation coefficient.

FPGA Implementations of ECC

FPGA implementation with the area and time-efficient architecture for ECC-based modular multiplication over 5 NIST prime field values is proposed by Mainul Islam et al. (17). It reduces the time complexity by using modified radix -2 interleaved algorithms for modular multiplication. The design was implemented on Virtex 7, 6, 5, and 4. It occupies low memory and is computationally feasible due to its low processing time for modular multiplication. Finite Field (FF) based instruction set and proper interconnection of FF cores was proposed by Yu Zhang (18). The parallel algorithm for ECC point multiplication decreases the clock cycles and minimizes the critical path greatly and also supports data dependency. The Proposed Pseudo-multi-core architecture achieves shallow area compared to other algorithms and requires only 1428 cycles to implement ECC point multiplication.

Md. Mainul Islamet, al., proposed a novel hardware architecture for twisted Edward curve group operation such as point addition and point doubling. The Montgomery ladder algorithm was used for Elliptic Curve Point Multiplication design to provide fast computation with high SCA resistance. The proposed radix-2 interleaved modular multiplier, and projective coordinate-based representation of Edward curve-based hardware architecture provides high throughput of 173.2 kbps with a processing time of 1.48 ms by offering a high level of security with a 256-bit key size (19). The fixed-base comb method proposed in (13) for ECC point multiplication employs a single two-stage pipelined karatsuba-ofman multiplier for low complexity; further two single-stage pipelined karatsuba-ofman multiplier was implemented to achieve low latency. The resultant hardware architecture provided high efficiency compared with existing architecture for both Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) implementations. The pre-computation method has been performed before regular point multiplication that does not occupy more area. Choi et.,al. (20) implemented a partial modular reduction based on low complexity ECC processor by using different FPGAs. It proves that it requires very low processing and achieves high throughput compared with the ECC processor's traditional full modular reduction technique over the NIST prime field. Shahroodi et., al.; describe modified binary differential additional chain-based point multiplication algorithm for Elliptic Curve Cryptosystem over GF(2^{163}), GF(2^{233}), and GF(2^{283}) (21). The proposed double point multiplication architecture for ECC consists of three phases such as pre-computation, initialization, and point multiplication phases. It improves efficiency, provides better processing time, and consumes less energy than previous work.

K.C. Cinnati et., al. (22) presented a novel architecture for two finite field arithmetic blocks such as multiplier block and addition/subtraction/reduction block to perform all arithmetic operations. Also, the design supports both prime and binary fields without reconfiguring hardware. The proposed architecture improves timing performance by involving the pipeline balancing concept, and also reduction step is separated from the polynomial multiplication step of the finite field multiplication. The proposed ECC coprocessor improves the system's efficiency by exploiting the advantages of DSP48E slices in Xilinx Vertex-5 FPGA. Zia-Uddin et., al. (23) describes area optimized and high throughput based architecture for ECC processor, consisting of novel Most Significant Digit based serial multiplier for arithmetic operation. Also distributed RAM-based memory unit is utilized to lower the read and write time. It also utilizes the Itoh-Tsujii inversion algorithm for inversion purposes to reduce the area occupancy. High-speed operation is obtained by using a finite-state machine-based control unit.

DNA Computing based Elliptic Curve Cryptography

P Vijayakumar et., al.; improved the existing DNA computing-based cryptography technique by encoding the message using a DNA mapping table. The encoded message is then encrypted by using the ECC encryption algorithm. Such mapping techniques will provide a greater level of security. Also, it offers features such as few numbers of bits for transmission and low computational overhead (24).

Salma et., al. (25) introduced the image encryption techniques by using ECC and DNA computing techniques. In this, the initial pixel value of the plain image is encrypted by the ECC encryption algorithm, and the resultant image is allowed to map with a DNA sequence. It achieves two levels of security and resists cryptanalyst attacks.

ECC Implementation Platforms

The choice of ECC implementation platforms are enormous that provides flexibility for the designer to opt for an application specific tools to develop the engine. Such platforms exploits the advanced computer-aided tools available in the market. Choice of both software and hardware tools drives versatile implementation of ECC. This section explores on few software CAD tools that are reportedly utilized for the development of ECC. Also a brief overview that summarizes the hardware tool such as Vivado by Xilinx and Quartos II by Altera is provided.

Software platforms

AVISPA Automated Validation of Internet Security Protocols and Applications (AVISPA) is a tool that helps to validate the Internet security-sensitive protocols and their application automatically. It also provides a modular and expressive formal language to specify the security protocol and its properties. It integrates the different back ends, which implements the novel automatic analysis techniques such as authentication, integrity checking, and error detection. In (26), the utilized AVISPA tool evaluated the performance of different IoT-based ECC authentication protocols. The obtained results show that the tool accurately determined the resistance level of the protocol against many vulnerabilities.

Python. Python (27) is a powerful object-oriented and high-level programming language. Python uses the tinyec library file to generate ECC-based private and public key pairs for the end-users. It also helps to derive a secret shared key and ciphertext public key for the encryption algorithm and Elliptic Diffie-Hellmann key exchange algorithm. Python libraries tinyec and pycryptodome are used for ECC-based hybrid encryption and decryption.

JAVA. Java (28) is a high-level, robust class-based object-oriented and secure programming language developed by Sun microsystem. Java is used to demonstrate different ECC-based processes such as key agreement, key generation, signature generation. This programming language helps to perform the Elliptic Curve Cryptography with a MIR key device using the standard SunPKCS11 provider. NIST curves such as secp252r1 and secp384r1 are supported by java language to generate ECC key pairs and general ECC curve parameters.

Scyther**.** Scyther (29) is a widely used tool for automatically verifying security protocol with an unbounded number of sessions and nonces. It can characterize and supports the representation of all the protocol's execution behaviour and security properties. Scyther tools can also be used to find new multi-protocol attacks on many conventional protocols and analyse the ISO/IEC 9798 family of authentication algorithms. ECC-based mutual authentication protocols are widely implemented and analysed using this tool due to its versatile adaptability. It also has features to identify such security protocol's security requirements and vulnerabilities. The model algorithm that analysis the protocol behaviour examines resistance against potential attacks.

Hardware Platforms. The ECC processor is widely implemented on the hardware devices such as ASIC and FPGA. Implementations on FPGA devices became popular due to their reconfigurability options. Xilinx ISE design suite (17) and vivado tool are used for such implementations. The target implementations devices are mostly advanced devices such as Virtex 6 and Virtex 7. Certain authentication implementation also utilizes Maple software.

Performance analysis and attacks on ECC

The main operation involved in Elliptic Curve Cryptosystem is point addition, point doubling, modular multiplication and scalar point multiplication. These operations are implemented using Vivado tool, and its performance is analysed using different FPGA devices such as Virtex 6 and Virtex 7. The following parameters are analysed to determine the performance of the proposed ECC processor in terms of clock cycles, number of LUT's, maximum frequency and processing time. Table 1 shows different implementation results and its performances of ECC.

Elliptic curve design on Virtex 7 by (19) has achieved a maximum frequency of 177.7 MHz compared to the design implemented on similar target devices. From the simulation result achieved in (17), it is inferred that time taken to process the operations involved in Elliptic Curve Cryptosystem is 1.45µs which is very less compared to other works carried out by the researchers. Similarly, number of LUT's used by the design mentioned in (30) is 96.9, which is very less compared to other design system. Finally, compared to other design work mentioned in Table 1, Virtex 7 (17) with lesser number of LUT's as 1491 by utilizing 257 clock cycles operates at 177.3 MHz achieves less processing time of 1.45 µs.

TABLE 1: Performance comparison of the reported implementation results

Work	Target Device	Number of LUTs	Clock Cycles	Max. Frequency (MHz)	Time
(17)	Virtex 7	1491	257	177.3	1.45 µs
(17)	Virtex 6	1551	257	160.7	1.60 µs
(19)	Virtex 7	32781	262650	177.7	1.48 ms
(19)	Virtex 6	33238	262650	161.1	1.63 ms
(30)	Virtex 7	96.9	215.9	72.9	2.96 ms
(30)	Virtex 6	154.8	215.9	64.4	3.35 ms

Attacks on ECC and countermeasures

Many attacks on ECC were reported over the decade, which poses severe security breaches. The research work to shield the crypto engine from such attacks is rising to enhance the security. Few Prominent countermeasures that have proved to counter the major threats effectively are discussed below.

Side-Channel Attack

The unintentional leakage of information that happened during data processing is called a side-channel attack in ECC. For example, the critical operation in ECC is computing $Q = k \times P$, and if the value of k is retrieved by the eavesdropper, then the Q value can be easily computed. Thus, ECC is found to be more vulnerable to various side-channel attacks. Enormous techniques to countermeasure and increase the security of the cryptosystem have been reported recently (1).

Power Analysis Attacks

Implementation of ECC in resource constrained network such as wireless sensor network, Mobile Adhoc Network, Vehicular Adhoc Network, Internet of Things is more vulnerable to power analysis attacks because exploitation of information about power consumption from the running cryptographic devices reveals the secret key of the network, it will help to acquire the entire network by the eavesdropper. Techniques such as charge sharing, structural implementation to reduce power spikes and ASIC implementation using adiabatic logic styles will enable to counter the attack.

Attacks on resource-constrained devices

Implementation of ECC in resource-constrained networks such as wireless sensor networks, Mobile Adhoc Networks, Vehicular Adhoc Networks, Internet of Things is more vulnerable to various attacks. Among them, power analysis attack is prominent. The exploitation of information about the power consumption of running cryptographic devices reveals the secret key. Thus eavesdropper can take control the entire network.

Further other attacks such as man in the middle attack, fault attack, and birthday attack were also widely reported. Countermeasures for these attacks have also been found to shield such attacks (1) effectively.

Conclusion

Reported research work on Lightweight Cryptosystems were reviewed elaborately with its merits and demerits. ECC based cryptosystem was the primary focus of this review article. The key generation, encryption, and decryption algorithm were dealt in detail. Explanation on the tools utilized for ECC point addition, point doubling, and Elliptic Curve Scalar Point Multiplication were also provided. Finally, performance analyses of different ECC-based Scalar point architectures were analysed and compared. Also, the types of attacks on ECC and its countermeasure were briefed. Performance analysis in terms of parameter such as processing time, Number of LUT's, Clock cycle and operating frequency are compared. From the results, its proves that Virtex 7 achieves better processing time compared with other system design. In the future, the performance of the crypto processor can be further improved by implementing hybrid ECC and genetic algorithm techniques to cater for the requirement of IoT applications.

References

1. Alsharari, Talal & Alresheedi, Shayem & Fatani, Abdulaziz & Maolood, Ismail., Significant role of internet of things (IoT) for designing smart home automation and privacy issues. *International Journal of Engineering & Technology* (2020).
2. Stallings, W., & Stallings, W. *Cryptography and network security: Principles and practice*. Upper Saddle River, N.J: Prentice-Hall, pp.396, (1999).
3. Jena, D., & Jena, S. K. A novel and efficient cryptosystem for large message encryption. *International Journal of Information and Communication Technology*, 3(1), pp.32, (2011).
4. D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer-Verlag,(2004).
5. Padma, Bh & Chandravathi, D. & P.Prapoorna, Roja,Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method. *International Journal on Computer Science and Engineering.* Vol. 02, No. 05, 1904-1907,(2010).
6. Lynn Margaret Batten, "Bibliography," in *Public Key Cryptography: Applications and Attacks*, IEEE,pp.195-198, (2013).
7. Liew, Khang Jie & Kamarulhaili, Hailiza,Comparison Study on Point Counting Algorithms of Elliptic Curves Over Prime Field. *European Journal of Scientific Research*, 61,538-548,(2011)..
8. B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, *A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT),* in IEEE Systems Journal, vol. 14, no. 3, pp. 3440-3450,(2020).

9. S. Rajamanickam, S. Vollala, R. Amin and N. Ramasubramanian, *Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC,* in IEEE Systems Journal, vol. 14, no. 2, pp. 1972-1983,(2020)
10. A.K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, *Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment*, in IEEE Access, vol. 7, pp. 55382-55397,(2019).
11. Khalid Mahmood, Salman Shamshad, Minahil Rana, AkashaShafiq, Shafiq Ahmad, Muhammad ArslanAkram,and Ruhul Amin, *PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication*, Journal of Information Security and Applications, vol.61 pp. 2214-2126,(2021).
12. Aswathy, R.H.,and Malarvizhi, N. *A design of lightweight ECC based cryptographic algorithm coupled with linear congruential method for resource constraint area in IoT*. J Ambient Intell Human Compute. (2021).
13. Khalid, Madiha; Mujahid, Umar; Najam-ul-Islam, and Muhammad, *Cryptanalysis of ultra-lightweight mutual authentication protocol for radio frequency identification enabled Internet of Things networks.* International Journal of Distributed Sensor Networks, 14(8),(2018).
14. S. Gabsi, Y. Kortli, V. Beroulle, Y. Kieffer, A. Alasiry and B. Hamdi, *Novel ECC-Based RFID Mutual Authentication Protocol for Emerging IoT Applications*, in IEEE Access, vol. 9, pp. 130895-130913,(2021).
15. ManashaSaqib, Bhat Jasra, Ayaz and Hassan Moon, *A lightweight three factor authentication framework for IoT based critical applications*, Journal of King Saud University - Computer and Information Sciences,1319-1578,(2021).
16. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, *A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data*, in IEEE Access, vol. 8, pp. 52018-52027.,(2020).
17. M. M. Islam, M. S. Hossain, M. Shahjalal, M. K. Hasan and Y. M. Jang, *Area-Time Efficient Hardware Implementation of Modular Multiplication for Elliptic Curve Cryptography*, in IEEE Access, vol. 8, pp. 73898-73906,(2020).
18. Yu Zhang, Dongdong Chen, Younhee Choi, Li Chen, and Seok-Bum Ko, *A high performance ECC hardware implementation with instruction-level parallelism over GF(2163)*, Microprocessors and Microsystems, Volume 34, Issue 6,Pages 228-236,(2010).
19. M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal and Y. M. Jang, *FPGA Implementation of High-Speed Area-Efficient Processor for Elliptic Curve Point Multiplication Over Prime Field*, in IEEE Access, vol. 7, pp. 178811-178826, (2019).
20. R. Salarifard, S. Bayat-Sarmadi and H. Mosanaei-Boorani, *A Low-Latency and Low-Complexity Point-Multiplication in ECC*, in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 65, no. 9, pp. 2869-2877,(2018).
21. P. Choi, M. Lee, J. Kim and D. K. Kim, *Low-Complexity Elliptic Curve Cryptography Processor Based on Configurable Partial Modular Reduction Over NIST Prime Fields*, in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 65, no. 11, pp. 1703-1707,(2018).
22. T. Shahroodi, S. Bayat-Sarmadi and H. Mosanaei-Boorani, *Low-Latency Double Point Multiplication Architecture Using Differential Addition Chain Over GF(2^m)* , in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 4, pp. 1465-1473,(2019).

23. Z. Khan and M. Benaissa, *Throughput/Area-efficient ECC Processor Using Montgomery Point Multiplication on FPGA*, in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 62, no. 11, pp. 1078-1082,(2015).
24. P Vijayakumar, V Vijayalakshmi and G Zayaraz, *Article: DNA Computing based Elliptic Curve Cryptography*, International Journal of Computer Applications 36(4):pp.18-21,(2011).
25. Bendaoud, Salma & Amounas, Fatima & el hassan, el kinani. *A New Image Encryption Scheme Based on Enhanced Elliptic Curve Cryptosystem Using DNA Computing.* NISS19: Proceedings of the 2nd International Conference on Networking, Information Systems & Security. Pp.1-5(2019).
26. Zargar, S., Shahidinejad, A., Ghobaei and Arani, M. *A lightweight authentication protocol for IoT-based cloud environment,* International Journal of Communication Systems. doi:10.1002/dac.4849, (2021).
27. Asep Saepulrohman, Teguh Puja Negara. (2020). Implementation of Elliptic Curve Diffie-Hellman (ECDH) for Encoding Messages Becomes a Point on the GF(p). *International Journal of Advanced Science and Technology*, *29*(06), 3264 – 3273,(2020).
28. Gayoso Martínez, Víctor & Sánchez Ávila, Carmen & Garcia, J. & Hernandez Encinas, Luis. (2005). Elliptic curve cryptography: Java implementation issues. 238 – 241(2005).
29. Huihui Huang, Xuyang Miao, Zehui Wu, Qiang Wei, "An Efficient ECC-Based Authentication Scheme against Clock Asynchronous for Spatial Information Network", *Mathematical Problems in Engineering*, vol. 2021, Article ID 8811970, 14 pages, (2021).
30. Asif, S., Hossain, M. S., & Kong, Y, *High-throughput multi-key elliptic curve cryptosystem based on residue number system.* IET Computers & Digital Techniques, 11(5), 165–172., (2017).