JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Reviews on ECC cryptography

**Dr. Sushil Kumar Saini**
Associate Professor of Mathematics
Dronacharya Government College Gurugram

**Abstract:** Computer scientists have been studying elliptic curves over the past several decades, both geometrically and algebraically. As the name suggests, Elliptic Curve Cryptography (ECC) is a public-key cryptosystem. In comparison to RSA, ECC provides same security with the use of a smaller key, which reduces the amount of resources required and increases system performance. In order to provide hardware designers with a valuable reference for creating efficient ECC processors, we provide an overview of the different implementation options in this study. ECC Algorithm Process, Basic Protocols of ECC Algorithm, Different ECC Implementation and ECC Application are also discussed in this article.

**Keywords:** ECC, Public Key, Private Key, Secret Key

## I. Introduction

The integrity, security, and secrecy of today's data is ensured by cryptography. For encryption and decryption implementation, homomorphism in elliptic curve cryptography will reduce computing cost while maintaining the same degree of security as other techniques. Even tiny devices like mobile phones and pagers may be safeguarded in terms of data transit if the elliptic curve is approximated using ElGamal, Paillier and RSA. It is possible to find the most efficient ECC algorithm by comparing all of its distinguishing parameters. Streaming data will benefit from this endeavour in many sectors, even those where data is centralised. Due to the widespread usage of air as a communication channel these days, this research will aid in the development of a cryptographic system by providing an overview of the fundamentals and key players. Real-time applications like online voting, safe data transmission, and money transfer via end-to-end encryption will benefit from this kind of system in the future, since data is a crucial thing to manage and must be protected from various network threats. A lot of work has gone into spreading the word that combining Elliptic curve cryptography with some of the best current cryptosystems yields the best results possible.

The algebraic structure of elliptic curves over finite fields provides the basis for Elliptic Curve Cryptography (ECC), a public-key cryptosystem. Integer factorization and Discrete Logarithm algorithm families make use of ECC. Secured by the difficulty of solving DLPs over a collection of points on the ECC elliptic curve, the ECC is protected. Additionally, ECC offers the same degree of security as RSA or discrete logarithm systems, but with substantially shorter keys (about 160 to 3072 bits vs. 1024 to 1024 bits).

### 1.1 Various ECC Implementation

In today's digital age, the importance of small-scale gadgets cannot be overstated. It's a difficulty since such devices have a limited amount of memory, but they also need to be secure, which necessitates proper specification. ECC is the most suited cryptography for devices with limited memory, such as smartphones, palmtops, smartcards, etc., because of its low key size, minimal operation, and compact encryption and decryption parameters. Using RFID as an example, ECC has been implemented and has shown to be an effective security measure for communication and data access tagged memory. It also

reduces the storage space necessary for the key and backend system by simply storing the private key, which reduces the storage space required for both. Thus, the tag's commutation is reduced [14]. Moreover. ECC is a good public key cryptography for mobile or wireless environments [23].

## II. Literature Review

**Majumder et al. (2021),** Internet of Things (IoT) devices communicate via the Constraint Application Protocol (CoAP), an application layer-based protocol that is a compressed version of the HTTP protocol. The Representational State Transfer (RST) architecture underlies the CoAP protocol, which is often connected with the connectionless User Datagram Protocol (UDP). The Datagram Transport Layer Security (DTLS) protocol is used to create a secure session between different IoT devices and a remote server utilising existing techniques like Lightweight Establishment of Secure Session. In the DTLS layer, however, there are a number of restrictions on the management of keys, the establishment of sessions, and multi-cast message exchange. That's why IoT communication requires the creation of an efficient protocol for safe CoAP session setup. Thus, they have devised an efficient and secure communication technique to create a secure session key between IoT devices and a distant server using lightweight elliptic curve cryptography to solve the current restrictions related to key management and multicast security in CoAP (ECC). A CoAP implementation for IoT network authentication is referred to as ECC-CoAP in the proposed ECC-based CoAP. In order to verify the ECC-security, CoAP's a variety of well-known cryptographic attacks were studied and determined to be well protected. The ECC-CoAP performance study reveals that our method is light and secure.

**Dong et al. (2021),** An increase in GPU processing capacity is being spurred by the artificial intelligence and computer vision sectors. Particularly in embedded contexts such as mobile phones, gaming consoles, and vehicle-mounted systems, the NVIDIA Tegra K1/X1/X2 GPU platforms, which are also considered edge computing devices, are currently commonly employed to provide high-dimension display, auto-pilot, and so on. Meanwhile, the need for cryptographic operations for secure communications and authentications between edge computing nodes and IoT devices is growing as a result of the advent of the Internet of Things. Instead of using FPGAs, ASICs, and ARM CPUs to construct cryptographic algorithms, they provide an alternate approach using integrated GPU devices.

**Sadhukhan et al. (2021),** Smart-grid design has emerged in the recent few decades as a new power service provider capable of regulating power production while also monitoring customer power consumption behaviour and aiding in power system stability. As the delay-sensitive smart grid network develops, it will have to deal with a number of difficulties. This includes cyber-threats to the sent messages, control information for the smart-grid, and the protection of users' privacy while operating in the smart-grid environment. To combat these cyber-threats, it is critical that utility customers and service providers establish secure channels of communication. A unique mutual authentication technique between consumers and substations constructed on elliptic curve cryptography with trivial operations for a smart-grid context is explored in this work. In addition, a session key negotiation step is included in this design to reduce communication and computation costs while still ensuring secure communication. Security testing utilising widely used BAN-logic and mathematical security tests has shown our scheme's robustness against all relevant attacks. Furthermore, the AVISPA simulation results show that our suggested approach is safe. Finally, the suggested system is assessed using NS-2, a well-known network simulator, which reveals that the proposed method is efficient to be applied in a realistic setting.

**Mahto & Yadav (2018),** RSA and ECC, two of the most widely used public-key cryptosystems, are examined in this work (Elliptic Curve Cryptography). Since its introduction, RSA has been widely used as the first generation of public-key cryptography (PKC). ECC, on the other hand, has just lately begun to acquire traction. Additionally, the report claims that these cryptosystems are superior based on their testing, which is supported by the study and analysis. The results of the experiments with these cryptosystems and the various NIST-recommended modulus/key sizes are presented in the study. For RSA, the modulus/key sizes are 1024/2048/3072-bit, whereas for ECC, the modulus/key sizes are 160/224/256-bit. An ECC-based cryptosystem has been shown to be superior than RSA and its variations in terms of security for memory-constrained devices, while an RSA-based cryptosystem necessitates more sources. The paper's findings support this conclusion.

**Lara-Nino et al. (2020),** Certain Internet of Things (IoT) applications need public key cryptography (PKC) services such as authentication, encryption, signatures, and key agreements (such as healthcare, the government, military, etc). For these services, Elliptic curve cryptography (ECC) has been recommended as an efficient alternative. In an ECC-based system, the most expensive operation is scalar multiplication (kP). ECC must be properly implemented in IoT applications to fulfil the

needs of the application. For restricted devices, such as those in the IoT environment, an FPGA-based acceleration engine of the core ECC processes employing binary Edward curves is provided in this study. The suggested solution uses fewer than 1400 slices of Virtex-5 FPGA and provides security comparable to 128 bits while being lightweight and generic. The FPGA hardware requirements of the design detailed in the literature study are the least.

**Islam et al. (2020),** An area-time efficient hardware implementation of modular multiplication over five NIST-recommended prime fields is given in this research for light-weight elliptic curve cryptography (ECC). The temporal complexity of standard interleaved modular multiplication may be reduced using a new radix-2 interleaved method, which is being suggested. All four Xilinx FPGA platforms are used to implement the suggested multiplication algorithm individually. Only 1151, 1409, 1491, 2355, and 2496 look up tables (LUTs) are required for this design to run on the Virtex-7 FPGA, and it can perform single modular multiplication in 0.93 s, 1.18 s, 1.45 s, 2.80 s, and 4.69 s at clock frequencies of 207.1 MHz, 177.3 MHz, 137.6 MHz, and 111.2 MHz, respectively, over five NIST prime When compared to existing designs for modular multiplication, the suggested approach utilises hardware resources and area-delay products more efficiently than previous designs on the Virtex-6, Virtex-5, and Virtex-4 FPGAs.

**Faz-Hernández et al. (2019),** An efficient alternative to DSA and RSA, the elliptic curve cryptosystems have been developed. In recent years, Montgomery and Edwards elliptic curves have been employed to create cryptographic systems. Diffie-Hellman protocols X25519 and X448 were created using the elliptic curves Curve25519 and Curve448. The Edwards Digital Signature Algorithm's Ed25519 and Ed448 signature instances were derived by mapping these curves to twisted Edwards curves. Simultaneous SIMD parallel processing is used to implement these methods in a safe and effective manner. Techniques for using the Intel AVX2 vector instruction set to speed up prime field arithmetic and elliptic curve operations are presented in this paper As a consequence of our work, an AVX2-ready processor software library has been created. For Ed25519 and Ed448, our library computes digital signatures 19% and 29% quicker than earlier optimised versions, respectively. Our library also increases the execution time of X25519 and X448 by 10% and 20%, respectively.

**Hureib & Gutub (2020),** In order to prevent medical health data from being stolen, this study investigates ways for encrypting and concealing sensitive information [19]. Elliptic curve cryptography and picture steganography are used to accomplish this. Text would be decrypted using ECC in the first step. Stenography is employed to hide text inside images in the second step [2, 24]. When it comes to choosing a public key, selecting ECC, an algebraic structure of elliptic curves over finite fields, is seen as a desirable option. Furthermore, it may be employed in a variety of media, including CT and MRI scans, in the medical record system and in the field. Privacy information may be obscured by using Image Steganography, which is a method that many businesses and institutions use to conceal encrypted information. Anyone, any group, or any organisation may utilise this strategy to conceal and preserve their sensitive commercial information, national secrets, laboratory secrets, or other types of information of critical importance.

**Bos et al. (2014),** ECC, as it is currently implemented, is reviewed in this study to expose the distinct flaws and vulnerabilities that exist in implementations of ECC. Using this form of public-key cryptography, they examine four protocols that are widely used: Bitcoin (SSH), TLS, and the Austrian e-ID card. About one in ten computers support ECC via TLS and SSH, which is a good sign for the security community. ECC implementations, despite the high stakes in money, access, and resources they safeguard, have weaknesses identical to those of prior cryptographic systems, according to this research.

**Singh et al. (2016),** Computer scientists have been studying elliptic curves over the past several decades, both geometrically and algebraically. As the name suggests, Elliptic Curve Cryptography (ECC) is a public-key cryptosystem. In comparison to RSA, ECC provides same security with the use of a smaller key, which reduces the amount of resources required and increases system performance. This article explains the fundamentals of elliptic curves and related arithmetic. The advantages of elliptic curve cryptography over RSA in public key cryptosystems are also shown, with the help of our own experiments.

## III. ECC Application

When it comes to the actual world, ECC is used across a wide range of fields and technology. Here are a few examples.

### 3.1 Bitcoin

Using Bitcoin's encryption, payments must be made directly from one peer to another and not via a financial institution. In Bitcoin, the public block chain is a collection of daily transections. Chaining begins with the origin block, which contains a SHA-256 hash of every subsequent block in this group. In Bitcoin, the user's account is used as an ECDSA private secret key

to ensure that the ownership of the Bitcoin between the parties may be verified by linking the sender's ECDSA private key and receiver's ECDSA public key. As a result, a previous transaction's sender's public key might be used to verify the signature [2].

ECC may be used in the SSH protocol in a variety of areas. Use of a host key for authentication between server and client is an option that may aid with self-authentication. The server key is supplied to the client by the server at the moment of key exchange so that the client may verify that the fingerprint matches the stored value. Afterwards, the server authenticates itself by signing a copy of the exchange key and using ECDSA as the key. As a last option, clients may choose to employ ECDSA public keys for authentication.

### 3.2 Austrian e-ID

Physical smart cards are one of the most used methods for granting access to users as physical security. Embedded in the smart cards are cryptographic hardware modules that store a private key needed for encryption and signatures in order to execute the cryptographic calculations. ECC is a viable alternative for this kind of application because to its short key size and low computational cost. ECDSA public keys may be used to produce legally binding digital signatures [24].

### 3.3 Transport Layer Security (TLS)

It is possible to use EC in a variety of ways throughout the protocol. All RFC cypher suites employ the ECDH key exchange. It is possible that the server's ECDSA public key is included in the TLS certificate. Using an extra set of cypher suites, TLS included ECC into the client and server greeting messages. Key exchange, encryption, message authentication techniques, and identity varication are all supported by the suites. A list of available elliptic curves and cypher suites is supplied by the client, and the server has the option of answering with a single cypher suite from the list if it does not enhance any cypher suites. Otherwise, the connection is cancelled. Only one ECC curve type with a key or signature is supplied in the server if ECC is required by the suite. As a result, a client must utilise many TLS sessions to offer alternative sets of curves in order to learn about the server's support for ordered preference [24].

## IV. Conclusion and Future Work

Over the last few decades, computer scientists have been investigating elliptic curves from both a geometric and an algebraic perspective. Elliptic Curve Cryptography (ECC) is a public-key cryptosystem that, as its name implies, uses elliptic curves. Comparing ECC to RSA, ECC delivers the same level of security while using a lower key size, which minimises the number of resources needed and improves the overall system efficiency. As part of this research, we present an overview of the various implementation alternatives for ECC processors in order to serve as a beneficial reference for hardware designers when developing efficient ECC processors. The ECC Algorithm Process, the ECC Algorithm Basic Protocols, the Different ECC Implementations, and the ECC Application are all covered in detail in this article.

## References


1. Majumder, S., Ray, S., Sadhukhan, D., Khan, M. K., & Dasgupta, M. (2021). ECC-CoAP: Elliptic curve cryptography-based constraint application protocol for internet of things. *Wireless Personal Communications*, *116*(3), 1867-1896.
2. Dong, J., Zheng, F., Lin, J., Liu, Z., Xiao, F., & Fan, G. (2021). EC-ECC: Accelerating Elliptic Curve Cryptography for Edge Computing on Embedded GPU TX2. *ACM Transactions on Embedded Computing Systems (TECS)*, *21*(2), 1-25.
3. Sadhukhan, D., Ray, S., Obaidat, M. S., & Dasgupta, M. (2021). A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. *Journal of Systems Architecture*, *114*, 101938.
4. Mahto, D., & Yadav, D. K. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. *Int. J. Netw. Secur.*, *20*(4), 625-635.
5. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2020). Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Networks*, *103*, 102159.
6. Islam, M. M., Hossain, M. S., Shahjalal, M. D., Hasan, M. K., & Jang, Y. M. (2020). Area-time efficient hardware implementation of modular multiplication for elliptic curve cryptography. *IEEE Access*, *8*, 73898-73906.
7. Faz-Hernández, A., López, J., & Dahab, R. (2019). High-performance implementation of elliptic curve cryptography using vector instructions. *ACM Transactions on Mathematical Software (TOMS)*, *45*(3), 1-35.
8. Hureib, E. S., & Gutub, A. A. (2020). Enhancing medical data security via combining elliptic curve cryptography and image steganography. *Int. J. Comput. Sci. Netw. Secur.(IJCSNS)*, *20*(8), 1-8.

9. Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014, March). Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security* (pp. 157-175). Springer, Berlin, Heidelberg.
10. Singh, S. R., Khan, A. K., & Singh, T. S. (2016, September). A critical review on elliptic curve cryptography. In *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)* (pp. 13-18). IEEE.