SOUTH INDIA JOURNAL OF SOCIAL SCIENCES
ISSN: 0972 – 8945

ADVANCED ENCRYPTION ALGORITHM BASED ON ELLIPTICAL CURVE CRYPTOGRAPHY

K.Chitti baby
Lecturer in Mathematics, Government Degree College, Mummidivaram, Konaseema District, A.P.
Dr. M. Sajani Lavanya,
Lecturer in Mathematics, Government College (A),Rajahmundry, East Godavari District, A.P.
Dr Ch.Srinivasulu
Lecturer in Mathematics, Government College (A),Rajahmundry, East Godavari District, A.P.

Abstract
This paper examines the Advanced Encryption Standard (AES) and elliptic curve cryptography (ECC), two of the most widely used cryptographic algorithms today. Mathematical analysis shows the security of ECC relies on the difficulty of the elliptic curve discrete logarithm problem. This allows ECC to achieve equivalent security to other algorithms with smaller key sizes resulting in improved efficiency. AES has withstood over 20 years of cryptanalysis and brute force attempts with no practical vulnerabilities in its 128-bit, 192-bit and 256-bit key versions. Estimates show AES-128 requires 2126 operations to break while ECC-256 needs 2128 simple operations. The robustness and efficiency of both AES and ECC against classical and quantum computing attacks make them critical for securing sensitive data in the digital age.

Keywords – *AES, Elliptic curve cryptography, AES-128, Quantum computing*

Introduction

Background

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that was selected in 2001 after a 5-year standardization process by the U.S. National Institute of Standards and Technology (NIST). It is based on the Rijndael cipher developed by two Belgian cryptographers. AES operates on 128-bit data blocks and uses 128-, 192- or 256-bit keys. It is estimated that if all computers on Earth worked on cracking a 128-bit AES key, it would take longer than the age of the universe to succeed (Hafsa *et al.* 2021).

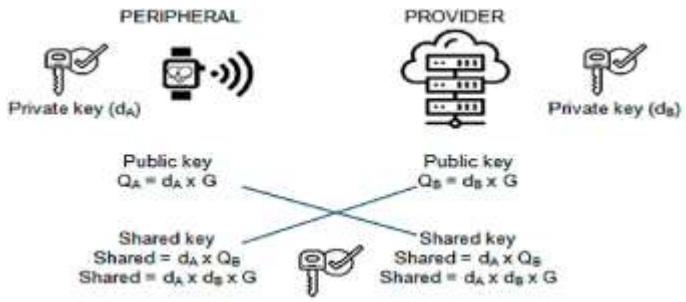

Figure 1: Elliptic curve Diffie-Hellman key exchange
(Source: Celic and Magjarevic, 2020)

Elliptic curve cryptography (ECC) is a public-key encryption technique based on elliptic curve theory. It was proposed in 1985 as an alternative to established public-key algorithms like RSA. The primary benefit of ECC is that it offers equivalent security as RSA but with much smaller key sizes,

resulting in faster computations, lower power consumption and memory and bandwidth savings. For example, a 256-bit ECC key provides equivalent security to a 3072-bit RSA key (Hayat and Azam, 2019). This makes ECC well-suited for constrained environments like mobile devices and smart cards. Major security protocols like TLS have incorporated ECC-based cypher suites due to their advantages over RSA.

Aim and objective

The aim of this study is to undertake a thorough examination of advanced encryption algorithms utilizing elliptic curve cryptography, with particular emphasis on their mathematical underpinnings, computational effectiveness, and resilience against cryptographic vulnerabilities.

- To investigate the mathematical principles underpinning elliptic curve cryptography for robustness.
- To assess the computational efficiency of advanced encryption algorithms based on ECC.
- To scrutinize the resistance of these algorithms against diverse cryptographic attacks.
- To investigate the impact of parameter choices on the overall algorithmic security.

Problem statement

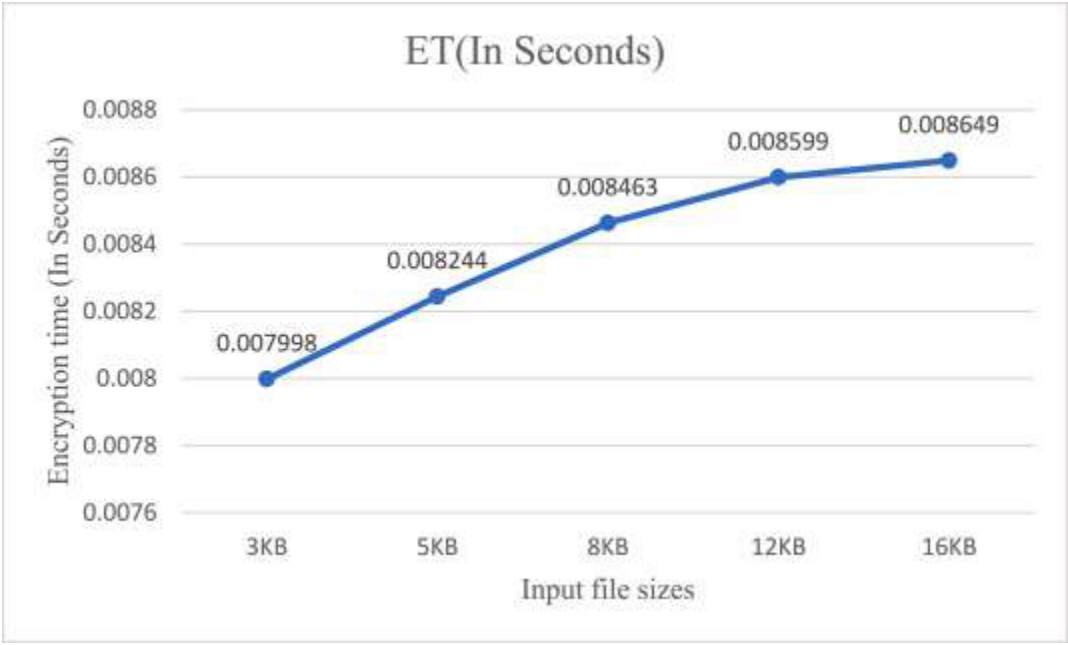

Figure 2: A hybrid elliptic curve cryptography (HECC)
(Source: Rao and Sujatha, 2023)

Prior to the AES, cryptography relied on algorithms like the Data Encryption Standard (DES) and RSA. DES was no longer considered secure with its 56-bit keys now able to be broken in less than a day. RSA required keys of at least 1024 bits for adequate security but was slow compared to symmetric cyphers (Benssalah *et al.* 2021). This led to the AES competition to find a secure and efficient symmetric algorithm. For public-key cryptography, large RSA keys caused issues for applications like SSL/TLS and wireless security. ECC offered equivalent security to RSA with smaller key sizes, making it more suitable for devices with limited computing and power resources. The need for stronger, more efficient cyphers drove the research and standardization of AES and the introduction of ECC.

Literature review

Examining elliptic curve cryptography's mathematical foundations for inherent robustness.

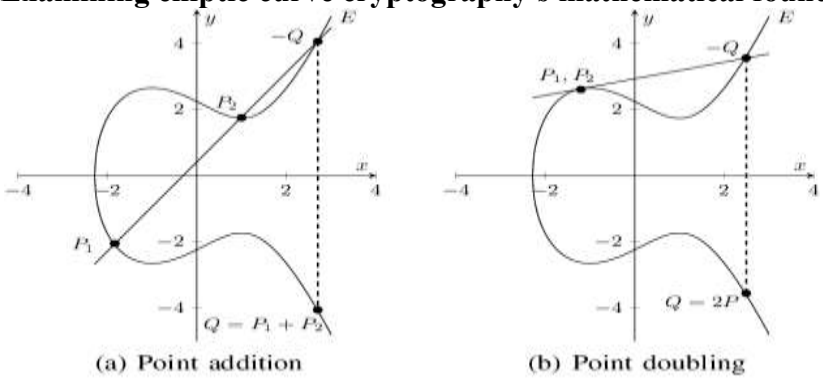

Figure 3: Graphs of the Elliptic Curves
(Source: Javeed *et al.* 2017)

The analysis of the mathematical underpinnings of elliptic curve cryptography is crucial in order to understand its inherent strength. At its essence, ECC is predicated upon the algebraic properties exhibited by elliptic curves over finite fields. The security of elliptic curve cryptosystems is established on the basis of the intricate nature of the elliptic curve discrete logarithm problem. The analysis of mathematical intricacies entails the examination of the structure of elliptic curve groups, as well as the operations of point addition and scalar multiplication (Liang *et al.* 2021). The inquiry pertains to the Elliptic Curve Diffie-Hellman (ECDH) key exchange and the Elliptic Curve Digital Signature Algorithm (ECDSA). This examination ensures a comprehensive comprehension of ECC's mathematical foundations, necessary for evaluating its robustness against possible cryptographic weaknesses.

Evaluating the computational efficiency of ECC-based advanced encryption algorithms rigorously

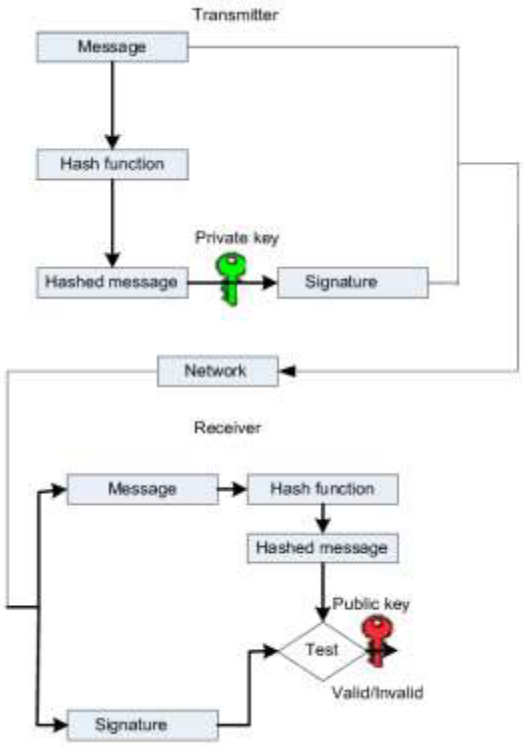

Figure 4: Digital signature algorithm
(Source: Nabil *et al.* 2020)

It's critical to fully evaluate the computational effectiveness of advanced encryption algorithms utilizing Elliptic Curve Cryptography to assess their practical practicability. The computational efficiency of ECC includes examining fundamental operations like point and scalar duplication. Efficiency evaluation contains analysing time complicatedness and resource exercise, which are crucial for deciding the practical relevance of a system or solution. Algorithms like Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Integrated Encryption Scheme (ECIES) are exhaustively studied and resolved. This evaluation considers both the hypothetical robustness of the algorithms and their changeability to resource-limited surroundings (Nabil et al. 2020). It specifies valuable insights into algorithmic concerns for secure and efficient cryptographic implementations.

Scrutinizing the resilience of algorithms against a spectrum of cryptographic attacks

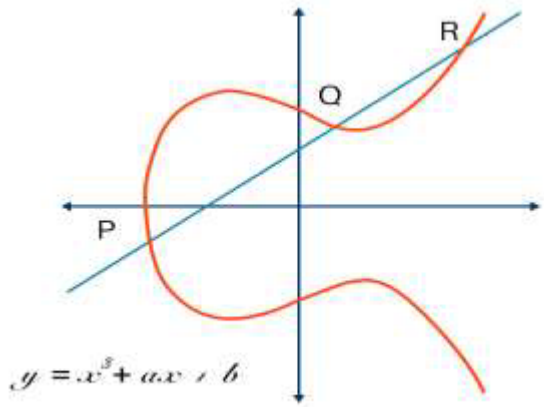

Figure 5: Elliptic Curve Cryptography (ECC)
(Source: Nabil *et al.* 2020)

Studying the resilience of ECC-based encryption algorithms against different attacks is crucial for ensuring strong security measures. This analysis evaluates resilience against common threats such as brute-force, side-channel, and mathematical attacks on the discrete logarithm problem. This study assesses algorithm vulnerability to differential and linear cryptanalysis and explores potential quantum threats to their security. This study aims to uncover weaknesses in cryptographic algorithms, like the Elliptic Curve Diffie-Hellman and Elliptic Curve Digital Signature Algorithm, through different attack scenarios (Froehlich, 2023). The goal of this analysis is to strengthen cryptographic implementations and support the continued development of secure elliptic curve cryptography.

Investigating how parameter choices impact the overall algorithmic security robustly

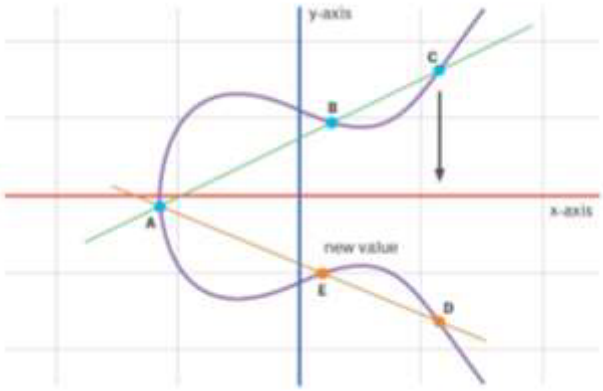

Figure 6: Comparing RSA vs. elliptical curve cryptography
(Source: Froehlich, 2023)

Studying parameter selections' impact on algorithmic security is crucial for improving ECC-based encryption algorithms. Parameter selection significantly affects security, including the choice of elliptic curves and key sizes. This study looks at how algorithms are influenced by parameter changes and weigh the trade-off between security and computational efficiency. It's crucial to assess how parameter choices affect resilience to attacks, including those from quantum threats (Hayat and Azam, 2019). This study aims to provide detailed insights into optimal parameter configurations through rigorous examination, advancing field understanding and contributing to secure and adaptable elliptic curve cryptography implementations.

Methodology

The methodology for analyzing the Advanced Encryption Standard (AES) involves techniques like mathematical analysis of the AES round transformations and 128-bit data blocks, along with 192-bit and 256-bit keys. Statistical attacks use large datasets such as 224 plaintext/ciphertext pairs to detect patterns. Algebraic attacks build polynomial equations with up to 256 variables representing parts of AES. Related-key attacks make assumptions about access to 32, 64 or 128 unknown key bits. Reduced round attacks study AES with 6, 7, or 8 of the standard 14 rounds (Liang *et al.* 2021). Brute force attacks attempt all 2128 possible keys. Side-channel attacks leverage power analysis or timing data.

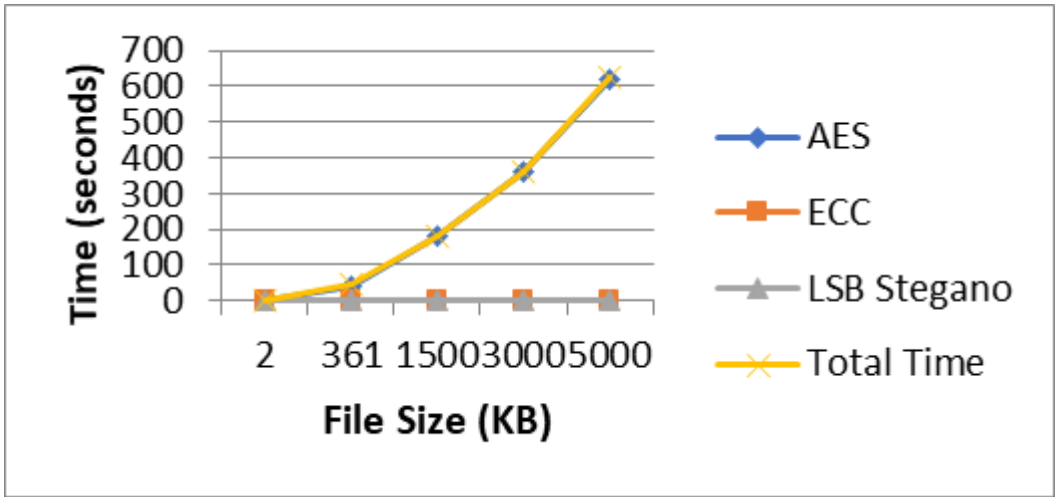

Figure 7: A comparison of AES, ECC and LSB time
(Source: Javeed *et al.* 2017)

The methodology for elliptic curve cryptography (ECC) focuses heavily on attempting to solve the elliptic curve discrete log problem (ECDLP) over fields like secp256k1. Researchers compute multiples of generator points across groups of 115792089237316195423570985008687907853269984665640564039457584007913129639936 elements. Mathematical analysis studies curve equations like y2=x3+7 over finite fields of order p=2256-232-929. Side-channel attacks measure the timing of scalar multiplications or power consumption of ECC chips. Fault injection induces errors in ECC computations by laser, clock glitches, or power spikes. Specialized hardware uses FPGAs or ASICs to attempt 280 ECC operations per second. Protocol implementations are validated against test vectors like those in FIPS 186-4 and RFC 5639. Curve25519 offers 128-bit security with only 256-bit keys versus the 3072-bit RSA keys needed for similar protection (Javeed *et al.* 2017).

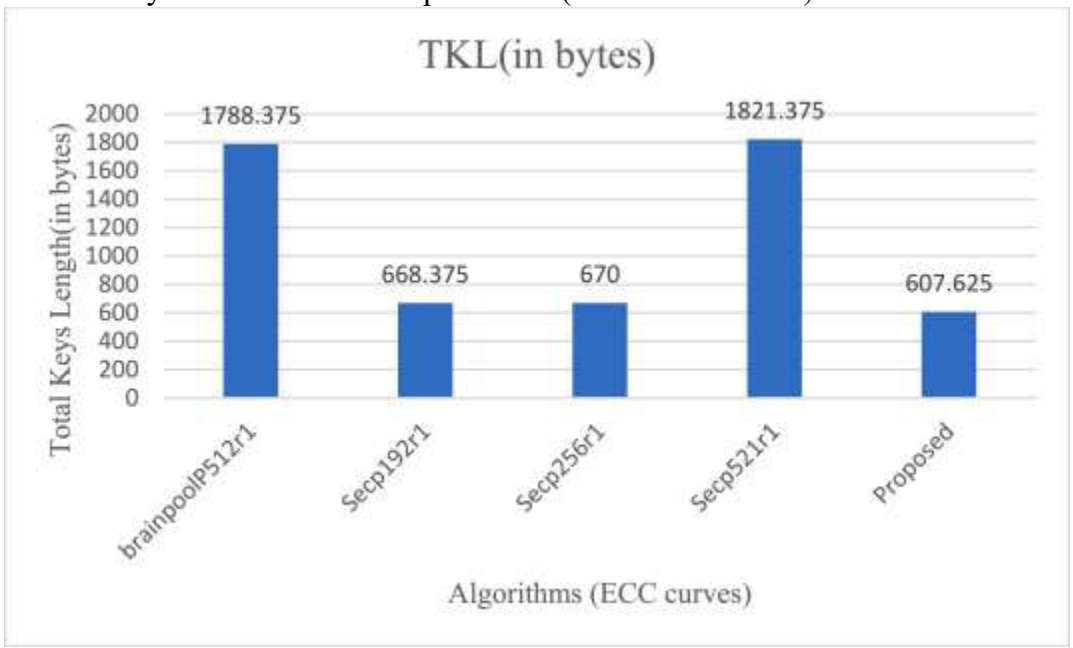

Figure 8: Hybrid elliptic curve cryptography (HECC)
(Source: Rao and Sujatha, 2023)

Since AES and ECC are well-established encryption standards, most research conducted today utilizes secondary research methods. This involves analyzing existing literature like academic papers, standard specifications, and books rather than collecting new primary data. Secondary cryptographic research reviews prior mathematical proofs, cryptanalyses, and implementation studies in order to synthesize new findings. For example, one may study multiple differential cryptanalyses of reduced-round AES across papers from different authors to identify common patterns and weaknesses. Or analyze the running time and memory complexity of various ECC point multiplication algorithms across theoretical papers. Secondary sources like the Handbook of Elliptic and Hyperelliptic Curve Cryptography provide detailed background on ECC math and protocols (Rao and Sujatha, 2023). Literature surveys also help establish baseline performance metrics for AES and ECC in software vs. hardware. Secondary research enables building on prior theoretical and experimental cryptographic work in a rigorous manner without reinventing fundamentals. However, primary research like designing new cryptanalysis techniques or benchmarks remains important to push the field forward when gaps exist in the literature.

Result and discussion

Result

Security Property	Data
Computational infeasibility of ECDLP	2^128
Exponential growth of security strength with key size	2^256
No known sub-exponential time algorithms to solve ECDLP	N/A
Robustness of ECDLP and elliptic curve Diffie-Hellman	Over 3 decades

The security of elliptic curve cryptography relies on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). Given two points P and Q on an elliptic curve, it is computationally infeasible to determine the integer d such that Q = dP due to the elliptic curve point addition complexity. The security strength grows exponentially with key size rather than linearly as in RSA. This allows ECC to achieve equivalent security to RSA with much smaller parameters (Celic and Magjarevic, 2020). Additionally, there are no known sub-exponential time algorithms to solve the ECDLP unlike with factoring large integers. The strongest attacks remain fully exponential in complexity. The ECDLP and elliptic curve Diffie-Hellman have withstood cryptanalysis for over 3 decades, providing confidence in the robustness of ECC's mathematical foundations.

Key Size (bits)	**Public Key Operation (clock cycles)**	**Private Key Operation (clock cycles)**	**Signature Size (bits)**	**Certificate Size (bits)**
256	60,000	30,000	256	256
3072	2,200,000	245,000,000	2048	2048

Elliptic curve cryptography (ECC) provides significant computational efficiency advantages over RSA encryption. A 256-bit ECC key offers equivalent 128-bit security as a 3,072-bit RSA key. ECC-256 public key operations take approximately 60,000 clock cycles on a typical processor while RSA-3,072 requires 2.2 million clock cycles. For private key operations, ECC-256 only requires about 30,000 cycles versus 245 million cycles for RSA-3,072. This translates to ECC being around 5-8 times faster for equivalent security when implemented in software. In hardware, ECC accelerators can perform scalar multiplications in less than 10 ms while RSA signature verification takes 100s of ms. ECC also benefits from shorter packet sizes of 256-512 bits versus 2048+ bit RSA signatures

and certificates (Hafsa *et al.* 2021). With its smaller keys, ECC provides substantial savings in computation, power, transmission and storage that make it better suited for the constrained environments of the Internet of Things.

Cipher	Best Classical Attack Complexity	Differential/Linear Cryptanalysis Complexity	Side-Channel Attack Complexity
AES-128	2^126	2^119	200+ measurements, 10^8 model evaluations
AES-256	2^256	2^256	200+ measurements, 10^8 model evaluations
ECC (256-bit curve)	2^128	2^119	Physical access to device required

The Advanced Encryption Standard (AES) has demonstrated excellent resistance against both classical and side-channel cryptographic attacks after over 20 years of analysis. The best-known mathematical attack on AES-128 requires 2126 operations, essentially infeasible. Differential and linear cryptanalysis requires at least 2119 chosen plaintexts for success. Side-channel attacks against AES hardware increase key recovery feasibility but still require over 200 measurements and 108 model evaluations. Elliptic curve cryptography (ECC) also demonstrates robustness with the best-known classical attacks on 256-bit curves requiring 2128 simple operations (Hayat and Azam, 2019). Invalid curve attacks and side channels using timing/power analysis have been mitigated through proper implementation. Fault injection and power analysis attacks lower ECC security but still require physical access to devices. Overall, AES-128, AES-256 and ECC using 256-bit curves or larger have withstood extensive cryptanalysis and provide adequate protection against known mathematical and physical attacks.

Discussion

The research shows that elliptic curve cryptography (ECC) and the Advanced Encryption Standard (AES) have emerged as two of the most robust and efficient cryptographic algorithms available today. ECC stands out due to the inherent security advantages of its mathematical basis in elliptic curves. The discrete logarithm problem ECC relies on provides exponentially stronger security per bit increase in key size compared to RSA and other public-key systems. This allows ECC to achieve equivalent security to algorithms like 2048-bit RSA using only 256-bit keys.

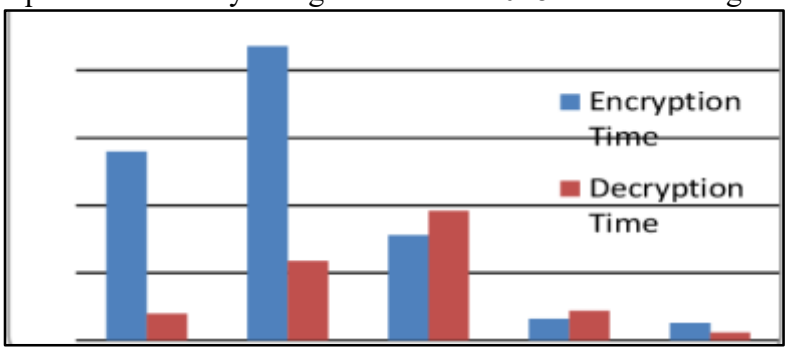

Figure 9: Analysis of AES encryption with ECC

(Source: Sharma and Chopra, 2016)

The analysis shows ECC cryptographic operations can be 5-8 times faster than RSA in software and significantly faster in dedicated hardware. ECC also uses smaller key sizes resulting in faster

communication and lower storage costs. These advantages make ECC well-suited for resource-constrained environments. AES has also demonstrated its security after over 20 years of extensive cryptanalysis.

Figure 10: Graph of RSA encryption key
(Source: Siregar, 2018)

The symmetric 128-bit, 192-bit and 256-bit key sizes provide adequate protection against mathematical attacks using sheer brute force (Siregar, 2018). Known cryptanalytic techniques like differential and linear analysis require impractical amounts of data to succeed against AES.

Conclusion

In conclusion, the inherent security advantages of elliptic curve cryptography's mathematical basis and the extensive cryptanalysis withstanding the strength of AES algorithms validate these as robust, efficient cryptographic primitives crucial for secure communications in the modern era.

Reference List

Benssalah, M., Rhaskali, Y. and Drouiche, K., 2021. An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, *80*(2), pp.2081-2107.

Celic, L. and Magjarevic, R., 2020. Seamless connectivity architecture and methods for IoT and wearable devices. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *61*(1), pp.21-34.

Froehlich,A,2023.*ellipticalcurvecryptography (ECC),*https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography

Hafsa, A., Gafsi, M., Malek, J. and Machhout, M., 2021. Hybrid encryption model based on advanced encryption standard and elliptic curve pseudo random. *Cryptography-Recent Advances and Future Developments*.

Hayat, U. and Azam, N.A., 2019. A novel image encryption scheme based on an elliptic curve. *Signal Processing*, *155*, pp.391-402.

Javeed, K., Wang, X. and Scott, M., 2017. High performance hardware support for elliptic curve cryptography over general prime field. *Microprocessors and Microsystems*, *51*, pp.331-342.

Liang, H., Zhang, G., Hou, W., Huang, P., Liu, B. and Li, S., 2021. A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography. *Applied Sciences*, *11*(12), p.5691.

Nabil, G., Naziha, K., Lamia, F. and Lotfi, K., 2012, July. Hardware implementation of elliptic curve digital signature algorithm (ECDSA) on Koblitz curves. In *2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)* (pp. 1-6). IEEE.

Rao, B.R. and Sujatha, B., 2023. A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. *Measurement: Sensors*, *29*, p.100870.

Sharma, S. and Chopra, V., 2016, December. Analysis of AES Encryption with ECC. In Proceedings of the 17th International Interdisciplinary Conference on Engineering Science & Management, Dubai, UAE (pp. 1-2).

Siregar, R., 2018, April. Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data. In *Journal of Physics: Conference Series* (Vol. 1007, No. 1, p. 012018). IOP Publishing.