Intern. J. Fuzzy Mathematical Archive
Vol. 23, No. 1, 2025, 13-30
ISSN: 2320 –3242 (P), 2320 –3250 (online)
Published on 1 June 2025
www.researchmathsci.org
DOI: http://dx.doi.org/10.22457/ijfma.v23n1a02248

Fuzzy-Based Performance Assessment of RSA and ECC in Digital Authentication

N. Ramya*[1], Hossein Rashmanlou[2], Farshid Mofidnakhaei[3], K. Hema Sri*[4]
and *N. Sikkander Asma*[4]*

[*1]Department of Mathematics, Vellalar College for Women, Erode. India
E-mail: jpramyamaths@gmail.com
[2]School of Physics, Damghan University, Damghan, Iran.
Email: Rashmanlou.1987@gmail.com
[3]Department of Physics, Sar. C., Islamic Azad University, Sari, Iran.
E-mail: Farshid.Mofidnakhaei@gmail.com
[*4]Department of Mathematics, Vellalar College for Women, Erode. India
[*]Corresponding author.

Received 12 April 2024; accepted 30 May 2025

Abstract. Digital signatures are essential for ensuring authenticity, integrity, and non-repudiation in electronic communications. This study presents a fuzzy logic-based comparative analysis of two widely used digital signature algorithms, RSA and Elliptic Curve Cryptography (ECC). While RSA offers strong security, its reliance on enormous key sizes increases computational load. ECC, on the other hand, provides equivalent security with significantly smaller keys, making it more suitable for ability-embarrassed environments such as IoT and mobile devices. The analysis incorporates fuzzy logic principles to evaluate the trade-offs in performance and security, offering practical guidance for selecting the optimal digital signature approach.

Keywords: Digital Signature, RSA Algorithm, Elliptic Curve Cryptography (ECC), Data Integrity.

AMS Mathematics Subject Classification (2010): 37N10

1. Introduction

Cryptography is a vital field concerned with safeguarding communication so that only the intended sender and receiver can interpret the memorandum. In practice, the security of such communication is not always binary (secure/insecure) but often lies on a spectrum influenced by multiple vague factors such as key strength, algorithm efficiency, and resource constraints, making fuzzy logic a suitable framework for analysis. Cryptographic systems typically operate using two primary key structures: symmetric and asymmetric keys. commensurate encryption, where the clone key is passed down for twain encryption and decryption, requires precise coordination and secure key exchange a task inherently vulnerable to leakage under uncertain conditions. Asymmetric encryption, by contrast, adoption a duo of analogous keys (a communal key and a independent key) and reduces the dependency on securely exchanging secrets, thus minimizing the risk of interception,

especially under fuzzy conditions of trust and network reliability. Digital signatures utility as fuzzy validators of authenticity, integrity, and non-repudiation in data transmission. They enable the recipient to assign a degree of belief to the claim that the memorandum originates from a specific sender and has not been tampered with crucial in environments where total certainty is rarely achievable. Among the various signature algorithms, RSA and Elliptic Curve Cryptography (ECC) are two dominant paradigms. RSA's surveillance is anchored in the hardness of factoring enormous accumulations, but its effectiveness degrades under fuzzily defined factors like quantum threat probability and computational resource growth. Consequently, RSA demands enormous key sizes to maintain a satisfactory level of security, leading to higher computational overhead. On the other hand, ECC leverages the mathematical complexity of elliptic curves and achieves commensurate security with significantly petite key sizes. This makes ECC a more efficient choice under fuzzy constraints such as narrow memory, processing power, and vitality consumption conditions typical in mobile devices and IoT systems. Through a fuzzy lens, the trade-off between RSA and ECC can be modeled using linguistic variables such as "high security," "moderate efficiency," or "low resource consumption," aiding in nuanced decision-making. Incorporating fuzzy logic into cryptographic evaluation allows practitioners to better navigate the uncertain, imprecise environments in which real-world security solutions are deployed.

Dalal et al. [1] conduct a contingent analysis of RSA, ECC, and DH cryptographic algorithms aimed at optimizing security, highlighting the necessity for a thorough review of existing cryptographic techniques to identify their respective advantages and limitations. Yadav [2] emphasizes the importance of elliptic curve cryptography within blockchain-based IoT frameworks, advocating a contextual evaluation of ECC alongside RSA and other cryptosystems in emerging technological landscapes. Shankar et al. [3] introduce an enhanced multi signature protocol tailored for digital forensic applications, underscoring the need to survey existing signature schemes to validate the proposed method’s novelty and efficacy. Saho and Ezin [4] focus on securing documents using RSA and ECC digital signatures, necessitating an examination of the current landscape of digital signature implementations and associated security challenges. Suárez-Albela et al. [5] assess the performance and energy efficiency of RSA and ECC cipher suites for IoT devices, requiring a detailed appraisal of their suitability in fog and mist computing environments. Talebi et al. [6] investigate isomorphism concepts in vague graphs, demanding a foundational review of graph theory and fuzzy set literature to underpin their theoretical contributions. Shao et al. [7] apply vague graph theory to medical diagnosis problems, highlighting the importance of integrating fuzzy graph frameworks with practical healthcare analytics. Rashmanlou et al. [8] deliver an in-depth exploration of vague graphs, requiring a comprehensive survey of fuzzy graph theory principles and recent scholarly progress. Hussain et al. [9] employ interval intuitionistic neutron sophic sets for climate data analysis, emphasizing the significance of neutron sophic logic and its environmental applications. Shoaib et al. [10] delve into complex Pythagorean fuzzy graphs, necessitating an understanding of advanced fuzzy logic constructs and their computational implications. Kosari et al. [11] explore domination problems in vague graphs with biomedical applications, requiring a review of graph domination concepts and their use in modeling biological systems. Rashmanlou et al. [12] analyze product operations on interval-valued fuzzy graphs, calling for an examination of fuzzy graph algebra and its characteristics.

Talebi and Rashmanlou [13] propose novel domination set constructs in vague graphs, necessitating a review of related domination theories and fuzzy graph metrics. Ali et al. [14] investigate vertex relatedness in fuzzy graphs with applications to human trafficking networks, requiring insight into graph connectivity measures and social network analysis methodologies. Kosari et al. [15] examine topological indices in fuzzy graphs aimed at enhancing decision-making processes, demanding a thorough survey of fuzzy graph theory and multi-criteria evaluation methods. Rao et al. [16] analyze forcing parameters in cubic networks, necessitating familiarity with network theory and graph invariants. Rao et al. [17] introduce innovative concepts related to intuitionistic fuzzy trees, requiring review of fuzzy tree structures within computational intelligence domains. Chen et al. [18] develop video processing algorithms leveraging temporal intuitionistic fuzzy sets, emphasizing the relevance of fuzzy set theory in image and video analysis. Shao et al. [19] investigate fuzzy decision-making frameworks in medical diagnostics using vague sets, highlighting the need for literature on fuzzy decision systems and healthcare analytics. Shao et al. [20] introduce new categories of vague graphs with diverse applications, calling for comprehensive familiarity with the evolution of vague graph theory. Shao et al. [21] study regularity conditions in vague graphs, requiring a foundational understanding of graph regularity concepts and fuzzy graph properties. Kosari et al. [22] examine perfectly regular fuzzy graphs in psychological modeling, necessitating integration of fuzzy graph theory with psychological network analysis. Rao et al. [23] apply fuzzy Zagreb indices in multi-attribute decision-making contexts, demanding an exploration of fuzzy graph metrics alongside decision frameworks. Shao et al. [24] investigate strong and geodetic domination sets in graphs, underscoring the relevance of domination theory and combinatorial optimization. Shi et al. [25] employ QSPR modeling with topological indices to advance cancer treatment research, requiring literature on graph-based molecular modeling and chemo informatics. Rashmanlou et al. [26] study bipolar fuzzy graphs, necessitating an understanding of bipolar fuzzy set theory and its graph applications. Kosari [27] analyzes spectral radius and Zagreb Estrada indices in graphs, demanding familiarity with spectral graph theory and associated invariants. Rashmanlou et al. [28] explore unambiguous properties of bipolar fuzzy graphs, calling for review of fuzzy graph classification systems. Borzooei and Rashmanlou [29] examine domination in vague graphs, requiring insight into domination principles within fuzzy graph contexts. Rashmanlou and Jun [30] investigate integrated interval-valued fuzzy graphs, emphasizing interval fuzzy set theory and completeness properties. Borzooei et al. [31] analyze regularity aspects of vague graphs, necessitating exploration of fuzzy graph structural properties. Rashmanlou and Pal [32] discuss balanced interval-valued fuzzy graphs, calling for literature on balancing concepts in fuzzy graph theory. Ramya and Deivanayaki [33] simulate fluid flow over inclined surfaces through porous media, highlighting foundational fluid mechanics and porous medium modeling literature. Ramya et al. [34] study Lorentz force effects on nanofluid flow under fuzzy environments, emphasizing magnetohydrodynamic principles integrated with fuzzy system modeling. Ramya and Deivanayaki [35] investigate heat radiation influences on nanofluid flow considering heat and mass diffusion, requiring comprehensive heat transfer and nanofluid research review. Ramya and Deivanayaki [36] apply fuzzy logic to analyze Eckert number impacts on nanofluid flow with chemical reactions, highlighting fuzzy modeling and thermos fluid dynamics literature. Ramya and Deivanayaki [37] examine Soret and Dufour effects on Casson nanofluid flows within

magnetic fields, necessitating a review of coupled heat and mass transfer mechanisms in nanofluids. Ramya and Deivanayaki [38] assess thermophoresis and Brownian motion influences on ternary hybrid nanofluids containing microorganisms, demanding understanding of nanofluid dynamics and biofluid interactions. Ramya and Deivanayaki [39] explore microorganism effects on Carreau nanofluid flow through porous media in magnetohydrodynamic systems, requiring comprehensive knowledge of non-Newtonian fluid mechanics, porous media flow, and biofluid magnetohydrodynamics. Kosari et al. [40] examined a conjecture concerning the total domination subsidiary number in graphs. The study provided verification for specific graph classes and derived theoretical bounds, offering valuable insights into how edge subdivisions influence domination properties. Kou et al. [41] introduced the concept of quadruple Roman domination in trees, defining a new domination utility and investigating its behavior in tree structures. They established theoretical bounds and proposed algorithms for exact computation. Rao et al. [42] proposed the outer-independent double Roman domination parameter for graphs, exploring its structural characteristics, deriving key bounds, and discussing its applications in graph protection and defense modeling. Shaebani et al. [43] studied the restrained-rainbow reinforcement number in graphs—a novel parameter that integrates reinforcement strategies with restrained rainbow colorings. They provided complexity results and analyzed the parameter across various graph families. Finally, Kosari et al. [44] analyzed the complexity of the signed total-Roman domination problem in graphs. They proved the problem to be NP-complete and examined its computational behavior in specific graph classes, contributing to the broader study of signed and Roman domination variants. Lakdashti et al. [45] present a detailed study on edge irregular product operations within vague graphs, formulating new constructs and analyzing their mathematical behavior to advance applications in uncertain network modeling. Chen et al. [46] delve into the algebraic structure of elementary abelian coverings for the Wreath graph W (3, 2) and the foster graph F26A, offering comprehensive classifications that deepen the theoretical foundation of graph automorphisms and coverings. Talebi et al. [47] develop the framework of interval-valued intuitionistic fuzzy soft graphs, merging aspects of fuzzy logic and soft set theory to better accommodate ambiguity and imprecision in relational data systems. Talebi et al. [48] introduce and formalize the notion of regularity in interval-valued fuzzy graphs, presenting essential definitions and properties that support enhanced analysis in environments with graded uncertainties. Rashmanlou and Borzooei [49] investigate the fundamental characteristics of vague graphs, illustrating their potential through real-world applications where data ambiguity plays a critical role. Kosari et al. [50] define and analyze the restrained Roman reinforcement number, a novel graph invariant that combines defense strategy with domination theory to support optimal allocation of protective resources in networks. Kosari et al. [51] focus on the independent k-rainbow bondage number, quantifying the impact of edge removal on domination parameters and offering insights into structural vulnerabilities in complex networks. Kosari et al. [52] examine the computational difficulty of solving the signed total-Roman domination problem, establishing its NP-complete status and outlining implications for algorithm development in graph optimization. Ramya et al. [53] explore the thermal and flow behavior of micropolar nanofluids subjected to homogeneous–heterogeneous chemical reactions, utilizing the Cattaneo–Christov model to accurately capture non-Fourier heat conduction effects over exponentially stretching surfaces.

This study presents a fuzzy-based comparative analysis of RSA and ECC digital signature algorithms. By evaluating the adaptability of key generation, signing, and verification operations under varying conditions, the research acknowledges that performance and security do not exist in binary absolutes but along a continuum influenced by device capabilities, network conditions, and threat levels. The analysis captures the nuanced trade-offs between computational overhead, key size, and cryptographic strength using fuzzy descriptors such as "low," "moderate," and "high" for resource consumption and security assurance. The study's novelty lies in its empirical assessment approach, which translates theoretical cryptographic robustness into practical performance metrics, enabling flexible, fuzzy-informed decision-making suited for environments with ambiguous or evolving security requirements.

2. Mathematical analysis

RIVEST-SHAMIR-ADLEMANN(RSA) Algorithm

RSA (Rivest–Shamir–Adleman) is one of the oldest and most commonly rampant communal-key cryptographic algorithms, refined in 1977. As a foundational cryptosystem, RSA plays a crucial though context-dependent role in digital signature frameworks by enabling both encryption and signature verification. However, its practical application often lies in a fuzzy spectrum of trade-offs between security strength and computational demands. Digital signatures, inherently uncertain in environments prone to tampering or interception, use RSA to establish authenticity and authenticate memorandum integrity with a degree of confidence rather than absolute certainty. RSA operates using a duality of mathematically combined keys: a communal key for encryption and an independent key for decryption. The separation between these keys introduces a layer of security that depends on the computational complication of factoring enormous composite commercial. In fuzzy terms, the "difficulty" of this task scales with the bit-length of the primes involved, translating into linguistic variables such as "very strong," "moderate," or "weak" encryption strength depending on the key size and attacker capability. The independent key must remain confidential, while the communal key is distributed freely. This asymmetry enables secure memorandum transmission but also introduces fuzzy thresholds of risk where shorter keys may be "potentially vulnerable" and longer keys are considered "computationally robust." The effectiveness of RSA thus varies across systems with differing security tolerances, computational resources, and anticipated threat levels. In scenarios where efficiency is critical and power constraints exist such as mobile and embedded systems the RSA algorithm may fall into a "less favorable" fuzzy category due to its high computational cost relative to alternatives like ECC.

RSA Key Generation

- Select amphibian opposing prime commercial p and q. These suffer be enormous and random.
- Gauge $n = p \times q$.This is the modulus for twain the communal and independent keys.
- Gauge Euler's totient utility:

$$\varphi(n) = (p-1)\,(q-1)$$

- This represents the number of positive accumulations less than n that are coprime to n.
- Choose an accumulation e such that 1 < e < φ(n) and e is coprime to $\varphi(n)$, i.e.,

$$gcd(e, \varphi(n)) = 1$$

This is the communal key proponent.

- Gauge d such that

$$d \cdot e \equiv 1(mod\varphi(n))$$

This is the independent key proponent.

The communal key is (n, e), and the independent key is (n, d).

Example Calculation of RSA Algorithm

The RSA digital signature scheme is stationed on modular arithmetic and the frustration of factoring enormous prime commercial.

Step 1: Key Generation

- Choosing two enormous prime commercials

$$p = 61, \quad q = 53$$

- To gauge the modulus

$$N = p \times q = 61 \times 53 = 3233$$

- To gauge Euler's totient utility

$$\varphi(n) = (p-1) \times (q-1) = (61-1) \times (53-1) = 60 \times 52 = 3120$$

- Choosing a communal exponent e such that it is coprime to φ(n)

A valid e must satisfy

$$1 < e < \varphi(N)$$
$$gcd(e, \varphi(N)) = 1$$

so that it has an inverse

$$e = 17$$
$$gcd(17, 3120) = 1$$

- To acquisition the independent key exponent d, we solve for d in

$$d \equiv e^{-1} \pmod{\varphi(N)}$$

where,

$$e = 17, \varphi(N) = 3120$$

This means acquisitioning d such that

$$e \cdot d \equiv 1 \, mod \, \varphi(N)$$
$$17 \cdot d \equiv 1(mod 3120)$$

This means we are looking for d as the modular inverse of 17 modulo 3120, Using the Extended Euclidean Algorithm, where The **Extended Euclidean Algorithm (EEA)** builds upon the standard Euclidean Algorithm, which regulate the greatest common divisor (GCD) of two accumulations. In addition to computing the GCD, the extended version also identifies the coefficients that satisfy Bézout's identity

$$ax + by = gcd(a, b)$$
$$17d + k(3120) = 1$$

We use the Euclidean algorithm to acquisition gcd (e, φ(N)), ensuring that an inverse exists

$$3120 \div 17 = 183, 3120 - (17 \times 183) = 9$$
$$17 \div 9 = 1, 17 - (9 \times 1) = 8$$
$$9 \div 8 = 1, 9 - (8 \times 1) = 1$$
$$8 \div 1 = 8, 8 - (1 \times 8) = 0$$

Since the detritus is 0, we stop here. The greatest common divisor (GCD) is 1, meaning 17 and 3120 are coprime. Since the greatest common divisor (gcd) is 1, the commercial are coprime, and an inverse exists. We express 1 as a linear combination of e and φ(N) by back-substituting from the previous equations

$$1 = 9 - 1 \times 8$$

Substitute $8 = 17 - 1 \times 9$

$$1 = 9 - 1 \times (17 - 1 \times 9) = 2 \times 9 - 1 \times 17$$

Substitute $9 = 3120 - 183 \times 17$

$$1 = 2 \times (3120 - 183 \times 17) - 1 \times 17$$

$$1 = 2 \times 3120 - 367 \times 17$$

Thus, we get

$$1 = 2(3120) - 367(17)$$

Taking mod 3120 on both sides

$$-367 \times 17 \equiv 1 \, mod \, 3120$$

Since d must be positive, we adjust

$$d = 3120 - 367 = 2753$$

$$d = 2753$$

Communal Key: (e, N) = (17, 3233)
Independent Key: (d, N) = (2753, 3233)

Step 2: Signing a Memorandum

- Hash the memorandum to get a numerical representation

$$M = 123$$

- Gauge the signature S using the independent key

$$S = M^d \, mod \, N$$

$$S = 123^{2753} \, mod \, 3233$$

- Using modular exponentiation, we get

$$S = 2746$$

The sender transmits (M, S) to the receiver.

Step 3: Signature Verification

To authenticate the signature, the receiver

- Gauges M' using the communal key

$$M' = S^e \, mod \, N$$

$$M' = 2746^{17} \, mod \, 3233$$

- Using modular exponentiation, we get

$$M' = 123$$

- If $M' = M$, the signature is valid. Otherwise, it is invalid.

Thus, the decrypted memorandum is 123, which matches the original memorandum.

RSA Key Generation Coding

```
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import rsa, padding
from cryptography.hazmat.backends import default_backend
import time
```

```
def generate_rsa_keys(key_size):
independent_key = rsa.generate_independent_key(
communal_exponent=65537,
key_size=key_size,
      backend=default_backend()
   )
communal_key = independent_key.communal_key()
   return independent_key, communal_key
```

Explanation

- Cryptography. hazmat. primitives provide various cryptographic utilities.
- hashes are used for hashing the memorandum (SHA-256).
- asymmetric. Sa provides RSA key generation, signing, and verification utilities.
- padding defines how padding is applied when signing.
- The utility accomplishes an RSA key pair (independent and communal keys).
- The key size parameter defines the length of the key (1024, 2048, or 4096 bits).
- The communal exponent is set to 65537, a common choice that balances security and efficiency.
- The independent key is accomplished first, and the communal key is then derived from it.

RSA Signature Generation

To sign a memorandum using RSA, follow these steps:

1.Hash the Memorandum

- Choose a cryptographic hash utility to hash the memorandum m.
- Let H(m) be the hash of the memorandum. The length of the hash depends on the chosen hash algorithm.
- The hash utility produces a fixed-size output, making it easier to sign than the entire memorandum.

2.Sign the Hash

- Gauge the digital signature by raising the hash of the memorandum to the power of d (independent exponent), modulo n
  s = H$(m)^d$ mod n
- The signature s is the result of encrypting the hash using the independent key.

3.Transmit the Memorandum and Signature

- The sender transmits the memorandum m and the signature s to the recipient.

4.Signature of a Memorandum

- The signature s is obtained using modular exponentiation with the hash of the memorandum and the independent key

  s = H$(m)^d$ mod n

RSA Signing Code

```
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes
def rsa_sign(independent_key, memorandum):
```

```
   signature = independent_key.sign(
      memorandum,
padding.PSS(
mgf=padding. MGF1(hashes. SHA256()),
salt_length=padding.PSS.MAX_LENGTH
      ),
hashes. SHA256()
   )
   return signature
```

Explanation

- The utility signs a given memorandum using the independent key.
- It applies the SHA-256 hashing algorithm to ensure memorandum integrity.
- It uses PSS (Probabilistic Signature Scheme) padding, which enhances security by adding randomness.
- The generated signature is returned as the output.

RSA Signature Verification

To authenticate the digital signature, the receiver needs the sender's communal key (n, e). The steps are

1.Hash the Memorandum

- The receiver gauges the hash of the received memorandum m, i.e., H(m).

2.Decrypt the Signature

- The receiver decrypts the signature using the sender's communal key

$$\text{decrypted signature} = signature^{e} \bmod n$$

- The decrypted signature should match the gauged hash of the memorandum if the signature valid.

3.Compare the Hashes

- Compare the decrypted signature with the gauged hash of the memorandum. If they match, the signature is valid, and the memorandum is authenticated.
- If they do not match, the signature is invalid.

To authenticate the signature s for memorandum m, the signature must be decrypted using the communal key (n, e). The hash h is obtained as follows

$$h \equiv s^{e} \bmod n$$

If h matches H(m), then the signature is valid—confirming that the memorandum was signed by the sender and has not been modified.

RSA Signature Verification Code

```
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes
def rsa_authenticate(communal_key, memorandum, signature):
   try:
communal_key.authenticate(
         signature,
         memorandum,
padding.PSS(
mgf=padding. MGF1(hashes. SHA256()),
```

```
salt_length=padding.PSS.MAX_LENGTH
          ),
hashes. SHA256()
       )
       return True
   except:
       return False
```

Explanation

- The utility verifies a digital signature using the communal key.
- If the signature is correct, it returns True.
- If verification fails (e.g., if the memorandum was changed), it returns False.

Security

The security of RSA relies on the difficulty of factoring enormous commercial. Given n, it is computationally infeasible to determine p and q, and therefore φ(N), which is required to gauge the independent key d. The RSA key size affects both security and computational performance.

Benchmarking for Different Key Sizes

```
def benchmark_rsa_signing_verification ():
   memorandum = b"Digital Signature with RSA!"
key_sizes = [1024, 2048, 4096]
   for key_size in key_sizes:
       print (f"---RSA_Key_Size: {key_size} bits---")
independent_key, communal_key = generate_rsa_keys(key_size)
start_time = time.time()
       signature = rsa_sign(independent
_key, memorandum)
signing_time = time.time() - start_time
start_time = time.time()
is_valid = rsa_authenticate(communal_key, memorandum, signature)
verification_time = time.time() - start_time
       print (f"RSA_Signing_Time: {signing_time:.6f} seconds")
       print (f"RSA_Verification_Time: {verification_time:.6f}")
       print (f"Signature_Valid: {is_valid}")
print ("-" * 50)
benchmark_rsa_signing_verification ()
```

Explanation

- It tests RSA signing and verification for different key sizes.
- It measures the time taken for signing and verification.
- The code prints RSA signing time.
- The code prints RSA verification time.
- The code prints Whether the signature is valid.

OUTPUT

RSA Key Size: 1024 Bits
RSA Signing Time: 0.001342 sec
RSA Verification Time: 0.000089 sec
Signature Valid: True
RSA Key Size: 2048 Bits
RSA Signing Time: 0.001277 sec
RSA Verification Time: 0.000077 sec
Signature Valid: True
RSA Key Size: 4096 Bits
RSA Signing Time: 0.005791 sec
RSA Verification Time: 0.00143 sec
Signature Valid: True

Analyzing RSA Performance

Signing Time

The signing process in RSA involves exponentiation with a independent key (typically a enormous accumulation like 2048 or 3072 bits). Due to its reliance on modular exponentiation

- Signing time increases significantly with key size.
- Enormousr key sizes result in slower signing times.

Verification Time

Verification in RSA involves exponentiation with the communal key, which is usually a small exponent

- This operation is computationally cheaper than signing.
- Verification is typically faster than signing in RSA.

Signature Validity

RSA digital signatures are well-established and widely used in protocols like TLS, SSH, and PGP

- Due to increasing computational power, RSA key sizes need to grow to maintain security.
- This makes long-term validity a concern.

ELLIPTIC CURVE CRYPTOGRAPHY (ECC) Algorithm

Elliptic Curve Cryptography (ECC) is a communal-key cryptographic path stationed on the algebraic structure of elliptic curves over finite fields. ECC was developed independently by Neal Koblitz and Victor Miller in 1985. An elliptic contour is given by an equation in the pattern of

$$y^2 \equiv x^3 + ax + b \ (mod p)$$

where a and b are constants that assuage certain surroundings to ensure the curve has no singularities. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature algorithm that is part of ECC. ECDSA is a standard for government digital signatures and is described in ANSI X9.62. It was first proposed by Scott Vanstone in 1992.

ECC Key Generation

- Acquisition an elliptic contour E(K), where K is a finite terrain such as F_p or F_2^n. Identify a point Q on E(K) where n is the order of Q.
- Select a pseudo-random number x such that 1≤x ≤(n-1).
- Gauge point $P = xQ$.
- The ECC key pair is (P, x), where P is the communal key and x is the independent key.

Example Calculation of ECC Algorithm

ECC digital signature scheme combines the mathematical complexity of elliptic curves with the practicality of digital signatures, providing a secure and efficient way to authenticate the authenticity and integrity of digital memorandums.

Step 1: Key Generation

The elliptic curve equation is given by

$$y^2 \equiv x^3 + ax + b\ (mod p)$$

where:

- p = 17 (prime field)
- a = 2, b = 2 (curve parameters)
- Base point Q = (5,1)
- Order of Q: n = 19

Choose a independent key

x = 7, where 1 ≤ x ≤(n-1).

Gauge communal key

$$P = xQ = 7(5,1) = (15,16)$$

We need to gauge 7Q

Further Multiplications of Q

$3Q = 2Q + Q = (13,16)$
$4Q = 2(2Q) = (9,9)$
$5Q = 4Q + Q = (16,13)$
$6Q = 2(3Q) = (10,6)$
$7Q = 6Q + Q = (15,16)$

Communal and Independent Keys

Thus, the communal key is $P = (15,16)$ and the independent key is $x = 7$.

ECC Signature Generation

To create a signature S for a memorandum mmm, using the ECC key pair (p, x) over the elliptic curve E(k):

1. Generate a random accumulation k such that $1 \leq k \leq (n-1)$.
2. Gauge the elliptic curve point $kQ = (xl, yl)$.
3. Gauge $r = xl mod\ n$. If $r = 0$, repeat from step 1.
4. Gauge the modular inverse $k - 1 mod\ n$
5. Convert the memorandum mmm to an accumulation e (typically by hashing).

6. Gauge $s = k - 1(e + xr)\ mod\ n. If\ s = 0$, repeat from step 1.

The signature for memorandum mmm is $S = (r, s)$.

Fuzzy Analysis of ECC (Elliptic Curve Cryptography)

Signing Time (Fuzzy Perspective)

- ECC utilizes elliptic curve point multiplication, a cryptographic operation that belongs to the fuzzy set of "highly efficient" techniques compared to RSA's modular exponentiation, which is "computationally heavier".
- Due to its compact key structure, ECC offers equivalent cryptographic strength using smaller keys—e.g., a 256-bit ECC key provides "approximately strong" security as a 3072-bit RSA key, reflecting a high efficiency-to-security ratio.
- The signing process in ECC exhibits "significantly faster" behavior across most security levels, earning it a high fuzzy membership value in the category of "fast signature algorithms".

Verification Time (Fuzzy Perspective)

- ECC verification involves scalar multiplication and point addition, operations that are "moderately complex" on elliptic curves and less intuitively efficient than RSA's simple exponentiation.
- As a result, ECC verification time is typically "slower than signing" and may fall into the same or a slightly slower fuzzy category than RSA for some configurations.
- In fuzzy terms, ECC verification is "adequate to slightly delayed" depending on the chosen curve and hardware context.

Signature Validity (Fuzzy Perspective)

- ECC ensures "high validity confidence" through its ability to maintain strong security guarantees over time with reduced computational costs, giving it a strong fuzzy grade for "long-term cryptographic validity".
- Standards bodies like NIST and the NSA classify ECC within the "recommended" fuzzy set for secure communication systems, especially when scalability and longevity are considered under uncertain future computing power scenarios.

Results and Discussion

The comparative analysis of RSA and ECC digital signatures, based on fuzzy performance indicators such as signing time, verification time, and key efficiency, reveals distinct trends (see Table 1). These trends can be interpreted through fuzzy linguistic terms like "high," "moderate," or "low" to express performance and resource utilization under varying cryptographic conditions:

- RSA signing time is observed to increase sharply with enormousr key sizes, reflecting a high computational load as the complexity of prime factorization scales.
- ECC signing time remains consistently low even for complex curves (e.g., SECP521R1), due to the inherent computational lightness of elliptic curve arithmetic.

- Verification time shows a fuzzy increase for RSA with enormousr keys, whereas ECC maintains a stable and faster verification trend across curve types.
- Storage and processing demands are significantly lower in ECC due to its smaller key sizes, which makes it more suitable (with a high membership grade) for fuzzy environments like IoT and mobile systems, where resources are variably constrained.
- Key generation in ECC is markedly faster due to the absence of enormous prime generation, a computational bottleneck in RSA.
- Overall, ECC demonstrates strong membership in the fuzzy set of "scalable and efficient algorithms" for modern cryptographic systems.

Application

Digital signatures serve as a fuzzy assurance mechanism in real-world systems, where certainty in identity, integrity, and non-repudiation must be inferred under imperfect conditions. RSA and ECC signatures show context-sensitive performance, applicable across domains with varying degrees of security requirements and system constraints.

Email Security

- Pretty Good Privacy (PGP) and S/MIME leverage RSA or ECC to fuzzily ensure that emails are authentic and unaltered.
- ECC's higher efficiency contributes to stronger applicability in environments where processing power and energy consumption are linguistically low.

Secure Web Transactions (SSL/TLS)

- RSA and ECC contribute to fuzzy authentication of websites and probabilistic data integrity over HTTPS.
- ECC is preferred when security must coexist with fast user experiences and lightweight protocols.

Online Banking and Payment Systems

- ECC provides efficient cryptographic verification for secure logins, fund transfers, and fraud prevention.
- RSA offers robust security, but its heavier computation places it lower in fuzzy desirability for real-time systems.

Blockchain and Cryptocurrencies

- ECC, particularly ECDSA, forms the fuzzy backbone of transaction validation, offering a high security-to-efficiency ratio.
- The use of ECC in smart contracts ensures low-latency validation with strong cryptographic confidence.

Code Signing

- Software distribution uses ECC and RSA to fuzzily authenticate the integrity and origin of executables.
- ECC's low-overhead processing is strongly favored in continuous integration/deployment (CI/CD) environments.

Electronic Health Records (EHRs)

- Digital signatures offer graded confidence in the authenticity and confidentiality of patient data.
- ECC ensures efficient encryption and verification, even on low-resource healthcare systems.

Medical Personnel Authentication

- Doctors and pharmacists use ECC-based signatures to establish secure communication and authenticate identities, where trust levels are not always binary but inferred with varying degrees of certainty.

3. Conclusion

The fuzzy comparative analysis of RSA and ECC digital signatures highlights their performance continuum across key cryptographic dimensions: security strength, computational load, and scalability. RSA, although historically robust, exhibits increasing computational costs and lower fuzzy membership in efficiency-driven applications as key sizes grow. Conversely, ECC achieves equivalent or higher membership in desirable cryptographic properties, compact key structure, lower latency, and better scalability, making it highly suitable for resource-constrained and latency-sensitive environments such as IoT, mobile, and edge devices. Empirical observations confirm ECC's fuzzy dominance in terms of signing and verification speed without compromising security. As security requirements become increasingly uncertain with evolving threats and system variability, ECC is expected to gain broader adoption in future secure communication systems. Future work may explore fuzzy hybrid models combining the strengths of RSA and ECC, or investigate post-quantum cryptographic schemes to address emerging uncertainties in digital authentication.

Acknowledgement. We would like to express our cordial thanks to the honourable referees for their valuable comments, which helped us improve the quality of the paper.

Conflicts of interest. The authors declare no conflict of interest.

Authors' Contributions. This is a single-author paper, and it is entirely the author's contribution.

REFERENCES

1. Y.M. Dalal, S. Supreeth, K. Amuthabala, T.Y. Satheesha, P.N. Asha, and S. Somanath, Optimizing security: A comparative analysis of RSA, ECC, and DH algorithms, 2024 *IEEE North Karnataka Subsection Flagship International Conference* (NKCon), (2024) 1–6.
2. A.K. Yadav, Significance of elliptic curve cryptography in blockchain IoT with comparative analysis of RSA algorithm, 2021 *International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, (2021) 256–262.
3. G. Shankar, L.H. Ai-Farhani, P.A.C. Angelin, P. Singh, A. Alqahtani, A. Singh, et al., Improved multisignature scheme for authenticity of digital document in digital forensics using Edward-curve digital signature algorithm, *Security and Communication Networks*, 2023(1) (2023) Article ID 2093407.

4. N.J.G. Saho and E.C. Ezin, Securing document by digital signature through RSA and elliptic curve cryptosystems, 2019 International Conference on Smart Applications, *Communications and Networking (SmartNets)*, (2019) 1–6.
5. M. Suárez-Albela, P. Fraga-Lamas, and T.M. Fernández-Caramés, A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices, *Sensors*, 18(11) (2018) 3868.
6. A.A. Talebi, H. Rashmanlou, and N. Mehdipoor, Isomorphism on vague graphs, *Annals of Fuzzy Mathematics and Informatics*, 6(3) (2013) 575–588.
7. Z. Shao, S. Kosari, M. Shoaib, and H. Rashmanlou, Certain concepts of vague graphs with applications to medical diagnosis, *Frontiers in Physics*, 8 (2020) 357.
8. H. Rashmanlou, S. Samanta, M. Pal, and R.A. Borzooei, *A study on vague graphs*, *SpringerPlus*, 5(1) (2016) 1234.
9. S.S. Hussain, I. Rosyida, H. Rashmanlou, and F. Mofidnakhaei, Interval intuitionistic neutrosophic sets with its applications to interval intuitionistic neutrosophic graphs and climatic analysis, *Computational and Applied Mathematics*, 40(4) (2021) 121.
10. M. Shoaib, S. Kosari, H. Rashmanlou, M.A. Malik, Y. Rao, Y. Talebi, et al., Notion of complex Pythagorean fuzzy graph with properties and application, *Journal of Multiple-Valued Logic & Soft Computing*, 34 (2020).
11. S. Kosari, Z. Shao, Y. Rao, X. Liu, R. Cai, and H. Rashmanlou, Some types of domination in vague graphs with application in medicine, *Journal of Multiple-Valued Logic & Soft Computing*, 41 (2023).
12. H. Rashmanlou, M. Pal, R.A. Borzooei, F. Mofidnakhaei, and B. Sarkar, Product of interval-valued fuzzy graphs and degree, *Journal of Intelligent & Fuzzy Systems*, 35(6) (2018) 6443–6451.
13. Y. Talebi and H. Rashmanlou, New concepts of domination set in vague graphs with applications, *International Journal of Computing Science and Mathematics*, 10(4) (2019) 375–389.
14. S. Ali, S. Mathew, J.N. Mordeson, and H. Rashmanlou, Vertex connectivity of fuzzy graphs with applications to human trafficking, *New Mathematics and Natural Computation*, 14(3) (2018) 457–485.
15. S. Kosari, X. Qiang, J. Kacprzyk, Q.T. Ain, and H. Rashmanlou, A study on topological indices in fuzzy graphs with application in decision making problems, *Journal of Multiple-Valued Logic & Soft Computing*, 42 (2024).
16. Y. Rao, S. Kosari, J. Anitha, I. Rajasingh, and H. Rashmanlou, forcing parameters in fully connected cubic networks, *Mathematics*, 10(8) (2022) 1263.
17. Y. Rao, S. Kosari, Z. Shao, A.A. Talebi, A. Mahdavi, and H. Rashmanlou, New concepts of intuitionistic fuzzy trees with applications, *International Journal of Computational Intelligence Systems*, 14 (2021) 1–12.
18. Z. Chen, S. Kosari, S.P. Kaarmukilan, C. Yuvapriya, K.T. Atanassov, et al., A video processing algorithm using temporal intuitionistic fuzzy sets, *Journal of Intelligent & Fuzzy Systems*, 43(6) (2022) 8057–8072.
19. Z. Shao, S. Kosari, H. Rashmanlou, and F. Mofidnakhaei, Fuzzy decision making in medical diagnosis using vague sets, *Journal of Multiple-Valued Logic & Soft Computing*, 40 (2023).

20. Z. Shao, S. Kosari, Y. Rao, H. Rashmanlou, and F. Mofidnakhaei, New kind of vague graphs with novel application, *Journal of Multiple-Valued Logic & Soft Computing*, 40 (2023).
21. Z. Shao, Y. Rao, S. Kosari, H. Rashmanlou, and F. Mofidnakhaei, Certain notions of regularity in vague graphs with novel application, *Journal of Multiple-Valued Logic & Soft Computing*, 40(2023).
22. S. Kosari, X. Shi, J. Kacprzyk, Z. Chen, and H. Rashmanlou, A novel description of perfectly regular fuzzy graphs with application in psychological sciences, *Journal of Multiple-Valued Logic & Soft Computing*, 42(2024).
23. Y. Rao, S. Kosari, S. Hameed, and Z. Yousaf, Multi-attribute decision-making using q-rung orthopair fuzzy Zagreb index, *Artificial Intelligence Review*, 58(5) (2025) 1–31.
24. Z. Shao, S. Kosari, S. Raman, and B. Ganesan, A study on strong and geodetic domination integrity sets in graphs, *Communications in Combinatorics and Optimization*, (2025).
25. X. Shi, S. Kosari, M. Ghods, and N. Kheirkhahan, Innovative approaches in QSPR modelling using topological indices for the development of cancer treatments, *PLOS One*, 20(2) (2025) e0317507.
26. H. Rashmanlou, S. Samanta, M. Pal, and R.A. Borzooei, A study on bipolar fuzzy graphs, *Journal of Intelligent & Fuzzy Systems*, 28(2) (2015) 571–580.
27. S. Kosari, On spectral radius and Zagreb Estrada index of graphs, *Asian-European Journal of Mathematics*, 16(10) (2023) 2350176.
28. H. Rashmanlou, S. Samanta, M. Pal, and R.A. Borzooei, Bipolar fuzzy graphs with categorical properties, *International Journal of Computational Intelligence Systems*, 8(5) (2015) 808–818.
29. R.A. Borzooei and H. Rashmanlou, Domination in vague graphs and its applications, *Journal of Intelligent & Fuzzy Systems*, 29(5) (2015) 1933–1940.
30. H. Rashmanlou and Y.B. Jun, Complete interval-valued fuzzy graphs, *Annals of Fuzzy Mathematics and Informatics*, 6(3) (2013) 677–687.
31. R.A. Borzooei, H. Rashmanlou, S. Samanta, and M. Pal, Regularity of vague graphs, *Journal of Intelligent & Fuzzy Systems*, 30(6) (2016) 3681–3689.
32. H. Rashmanlou and M. Pal, Balanced interval-valued fuzzy graphs, *Vidyasagar University, Midnapore, West-Bengal, India*, (2013).
33. N. Ramya and M. Deivanayaki, Numerical simulation of fluid flow over an inclined surface through porous medium, *Journal of Mines Metals & Fuels*, 71(11) (2023) 2143–2149.
34. N. Ramya, M. Deivanayaki, and F. Mofidnakhaei, Influence of Lorentz force on nanofluid flow over a stretching surface in a fuzzy environment, *Annals of Pure and Applied Mathematics*, 29(2) (2023) 133–143.
35. N. Ramya and M. Deivanayaki, Heat radiation on nanofluid flow over an inclined stretching surface with heat and mass diffusions, in *Recent Advancements in Materials Science and Technology, Vol. I, Springer*, (2024) 414.
36. N. Ramya and M. Deivanayaki, Fuzzy logic analysis of the effects of Eckert number on nanofluid flow over an inclined magnetic field with chemical reactions, *International Journal of Fuzzy Mathematical Archive*, 22(1) (2024) 15–32.

37. N. Ramya and M. Deivanayaki, Impact of Soret and Dufour effects on Casson nanofluid flow in a magnetic field with heat and mass transfer, *Indian Journal of Science and Technology*, 18(13) (2025) 1059–1070.
38. N. Ramya and M. Deivanayaki, Thermophoresis and Brownian motion effects on the Casson ternary hybrid nanofluids over a horizontal plate containing gyrotactic microorganisms, *Chemical Physics Impact*, 10(2025) 100887.
39. N. Ramya and M. Deivanayaki, Influence of microorganisms on Carreau nanofluid flow through a Darcy–Forchheimer porous medium in magnetohydrodynamic systems, *Journal of Nanofluids*, 14(2025) 251–258.
40. S. Kosari, Z. Shao, R. Khoeilar, H. Karami, S.M. Sheikholeslami, and G. Hao, on a conjecture concerning total domination subdivision number in graphs, *AKCE International Journal of Graphs and Combinatorics*, 18(3) (2021) 154–157.
41. Z. Kou, S. Kosari, G. Hao, J. Amjadi, and N. Khalili, Quadruple Roman domination in trees, *Symmetry*, 13(8) (2021) 1318.
42. Y. Rao, S. Kosari, S.M. Sheikholeslami, M. Chellali, and M. Kheibari, On the outer-independent double Roman domination of graphs, *Frontiers in Applied Mathematics and Statistics*, 2021(2021) Article 70.
43. S. Shaebani, S. Kosari, and L. Asgharsharghi, The restrained-rainbow reinforcement number of graphs, *Discrete Mathematics, Algorithms and Applications*, 13(3) (2021) 2150026.
44. S. Kosari, Y. Rao, Z. Shao, J. Amjadi, and R. Khoeilar, Complexity of signed total-Roman domination problem in graphs, *AIMS Mathematics*, 6(1) (2021) 952–961.
45. A. Lakdashti, H. Rashmanlou, P.K.K. Kumar, G. Ghorai, and M. Pal, Some results on edge irregular product vague graphs, *International Journal of Advanced Intelligence Paradigms*, 27(1) (2024) 18–28.
46. Z. Chen, S. Kosari, S. Omidi, N. Mehdipoor, A.A. Talebi, and H. Rashmanlou, Elementary abelian covers of the Wreath graph W (3,2) and the foster graph F26A, *AKCE International Journal of Graphs and Combinatorics*, 20(1) (2023) 20–28.
47. A.A. Talebi, H. Rashmanlou, and S.H. Sadati, Interval-valued intuitionistic fuzzy soft graph, *TWMS Journal of Applied and Engineering Mathematics*, (2023).
48. A.A. Talebi, H. Rashmanlou, and B. Davvaz, New concepts of regular interval-valued fuzzy graphs, *Journal of Applied Mathematics & Informatics*, 35(1–2) (2017) 95–111.
49. H. Rashmanlou and R.A. Borzooei, Some properties of vague graphs with application, *Journal of Intelligent & Fuzzy Systems*, 30(6) (2016) 3423–3430.
50. S. Kosari, S.M. Sheikholeslami, C. Mustapha, and H. Maryam, Restrained Roman reinforcement number in graphs, *Ural Mathematical Journal*, 8(2) (2022) 81–93.
51. S. Kosari, J. Amjadi, M. Chellali, F. Najafi, and S.M. Sheikholeslami, Independent k-rainbow bondage number of graphs, *AKCE International Journal of Graphs and Combinatorics*, 21(1) (2024) 102–109.
52. S. Kosari, Y. Rao, Z. Shao, J. Amjadi, and R. Khoeilar, Complexity of signed total-Roman domination problem in graphs, *AIMS Mathematics*, 6(1) (2021) 952–961.
53. N. Ramya, M. Deivanayaki, P. Kavya, et al., Influence of homogeneous–heterogeneous reactions on micropolar nanofluid flow over an exponentially stretching surface with the Cattaneo–Christov heat flux model, *Discover Applied Sciences*, 7(2025) Article 554.