Dhaka Univ. J. Sci. 74(1): 179-185, 2026 (January)
Prof. M. Muhibur Rahman Memorial Issue

ISSN 1022 - 2502, E-ISSN 2408- 8528
DOI: https://doi.org/10.3329/dujs.v74i1.84339

Digital Security for Land Registration in Bangladesh: A Framework Based on Elliptic Curve Cryptography

Hasan Mahdi Mahi, Adeeb Shahriar Zaman,* Salma Nasrin, and Sarker Md. Sohel Rana

Department of Mathematics, University of Dhaka, Dhaka-1000, Bangladesh

(Received : 15 September 2025; Accepted : 1 January 2026)

Abstract

Land registration in Bangladesh continues to rely on paper-based processes that are susceptible to forgery, duplication, and inefficiency. These vulnerabilities contribute to widespread disputes over property ownership and create barriers to transparent governance. Recognizing that the root of these issues lies in the absence of a secure mechanism for verification, this study turns to algebraic cryptography as a potential solution. This paper introduces an algebraic cryptographic framework for securing land registration through Elliptic Curve Cryptography (ECC), specifically the Elliptic Curve Digital Signature Algorithm (ECDSA). It is built upon the hardness of the elliptic curve discrete logarithm problem, which ensures signatures that are computationally unforgeable. This study also considers the theoretical advantages of ECC over the Rivest–Shamir–Adleman (RSA) algorithm, particularly its ability to deliver equivalent security with smaller key sizes, faster verification, and lower storage requirements. The mathematical model developed in this paper formalizes these properties and evaluates their implications for a large-scale registry system. It explores how compact signatures, low verification latency, and limited data growth can be aligned with the resource constraints of Bangladeshi land offices. The contribution of this work lies in connecting rigorous mathematical security with a practical national need. By embedding algebraic cryptography into land registration, the framework provides a pathway to prevent fraudulent transfers and enhance institutional trust. This vision points toward a future in which property rights in Bangladesh are secured not by fragile paper, but by the certainty of algebraic cryptography.

Keywords: Digital Land Registry, Forgery Prevention, Information Security in Bangladesh, Algebraic Cryptography, Elliptic Curve Digital Signature Algorithm, Elliptic Curve Cryptography.

I. Introduction

Land administration system of Bangladesh still relies heavily on paper-based records, handwritten deeds, and manual verification, which creates major risks of forgery and manipulation. Fraudulent duplication of documents, forged signatures, and tampering with physical files are common problems reported by both urban and rural citizens[1,2]. Since most records are stored in local offices without tamper-proof digital backups, even small alterations can generate conflicting ownership claims. This has made paper forgery one of the leading causes of land disputes, which today constitute the majority of civil litigation in Bangladesh. For citizens, especially in rural communities, land disputes are not only a legal issue but also a source of economic instability and family conflict[3].

The absence of a robust digital signature system further compounds the problem. At present, property transfers are typically authorized through handwritten signatures and the presence of witnesses, both of which are vulnerable to forgery. Unscrupulous actors can easily impersonate owners or manipulate deeds, especially when landowners are illiterate or living abroad. Moreover, Transparency International reports that over 80% of citizens interacting with land offices face bribery demands. These practices thrive within a bureaucratic maze where one transaction may require multiple approvals and the legal system is overloaded with land disputes that may take 15–20 years to resolve, denying timely justice and perpetuating mistrust in state institutions[4]. As a result, citizens view land offices not as protectors of rights but as obstacles to justice.

These vulnerabilities have wide-ranging consequences. Families lose ancestral land due to falsified papers, small farmers often face eviction from forged sales deeds, and many urban buyers hesitate to invest in property for fear of fraudulent transfers. Lengthy disputes arise not only from corruption but also from the inability of courts to prove authenticity when both parties present seemingly valid, but possibly forged documents. This creates an environment where landowners, particularly vulnerable groups such as women and rural farmers, lack reliable protection for their property rights[3]. Ultimately, the absence of secure digital verification infrastructure has turned land ownership into one of the most fragile legal rights in Bangladesh. The government has launched initiatives such as e-Mutation and cadastral surveys to digitize land services, but these platforms remain limited in scope and do not yet provide cryptographic guarantees of authenticity[5].

Blockchain technology offers a way to fundamentally redesign land administration by ensuring that once a record is created, it cannot be altered or forged. Every transaction is stored as part of a distributed ledger, where tampering with past entries would require impossible computational resources. For a system plagued by fraudulent duplication and fake signatures, blockchain provides immutability and verifiable timestamps, giving both citizens and authorities confidence that property titles cannot be forged. Several academic studies and prototypes in Bangladesh have

*Author for correspondence. e-mail: adeeb.math@du.ac.bd

already proposed blockchain frameworks for land registry. For example, systems using permissioned blockchains like Hyperledger Fabric allow controlled participation by government offices while ensuring immutability of transactions[6]. Other recent models incorporate smart contracts to automatically validate ownership transfer rules and prevent conflicting deeds[7]. While promising, these models emphasize that blockchain alone is not sufficient: secure cryptographic identity verification is essential to prevent forged authorizations.

This is where Elliptic Curve Cryptography (ECC) becomes critical. ECC enables citizens to authorize land transactions using digital signatures that cannot be forged without their private keys. Unlike handwritten signatures, which can be imitated, ECC-based signatures are mathematically verifiable by anyone with the corresponding public key. This ensures that only the rightful owner can initiate a transaction and that every transfer is provably authentic. Given Bangladesh's mobile-first context, ECC is particularly suitable due to its efficiency, strong security with small key sizes and low computational cost[8].

This paper focuses on the Weierstrass form of ECC, particularly standardized curves such as NIST P-256. These curves are widely used in secure communication systems and offer a balance of efficiency and interoperability. Implementing Weierstrass-form ECC in a blockchain-based land registry would allow Bangladesh to adopt an internationally recognized standard while ensuring that all citizen-to-authority interactions are cryptographically secure. This directly addresses the problem of forged deeds and unauthorized transfers by replacing handwritten signatures with mathematically unforgeable digital ones.

The primary aim of this paper is to introduce a framework for Weierstrass-form ECC as the mathematical foundation of a blockchain-based land registry system for Bangladesh. By grounding ownership verification in algebraic cryptography, the proposed model ensures that property transfers are not only recorded immutably but also authorized securely. In doing so, the paper contributes both a theoretical foundation for ECC in land governance and a practical pathway toward eliminating forgery in one of the country's most sensitive sectors.

II. Background and Literature Review

Land registration systems globally are moving toward digital transformation to ensure security, efficiency, and trust. Developed economies like Sweden, Estonia, and the Netherlands have pioneered electronic property records, while emerging economies such as India and Ghana are experimenting with blockchain for transparency in transactions[9]. These systems demonstrate the role of digital registries in reducing disputes and lowering transaction costs, but their success depends on both technological adoption and institutional readiness.

Beyond land management, blockchain has found applications in voting systems, supply chains, and educational certificate verification. These deployments illustrate blockchain's broader role in ensuring tamper-resistance, auditability, and decentralized verification. For example, Estonia's e-Governance framework integrates blockchain for medical records and voting, while Bangladesh has piloted blockchain in the education and agriculture sectors[10]. Such pilots show the government's growing openness to distributed technologies, but a nationwide property registry remains untested.

The reliability of digital registries relies not only on the database but also on the cryptographic infrastructure that secures transactions. Globally, RSA has long been the foundation for authentication in public services, but the shift toward elliptic curve–based cryptography is accelerating. Countries like India have considered ECC in Aadhaar-related security layers, and the European Union recommends elliptic curves in government PKI standards[11]. These transitions underscore ECC's importance for scalable, mobile-compatible public systems.

Scholarly work increasingly connects blockchain with property rights. A proposal has been presented on blockchain-based smart contracts for property management in developing countries, highlighting efficiency and transparency[12]. Ghana's registry challenges has been analyzed and argued that blockchain could reduce fraudulent transactions[13]. Similar works in Kenya, India, and Latin America study policy, infrastructure, and transparency outcomes, but fewer emphasize the cryptographic backbone enabling secure digital signing[12,13].

Taken together, global projects and scholarly works illustrate blockchain's potential in property registration but reveal two limitations. First, the Bangladeshi context remains underexplored while pilots exist in other domains, no research provides a blockchain-based land registry model suited to its infrastructure. Second, academic contributions have focused on policy or transparency aspects, while neglecting a mathematical framework that integrates cryptographic primitives into property transactions. This study addresses this gap by introducing Weierstrass-form elliptic curve cryptography (ECC) as a rigorous, efficient solution for digital land registries in Bangladesh.

III. Mathematical Framework

Elliptic Curve Cryptography: Mathematical Foundation

Elliptic Curve Cryptography (ECC) is a class of public-key cryptosystems that derives its security from the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally infeasible to solve within polynomial time [14, 15]. An elliptic curve E over a finite field F_p (where p is prime) is is generally defined in the short Weierstrass form:

$$y^2 = x^3 + ax + b \ (mod\ p), \qquad 4a^3 + 27b^2 \neq 0$$

The non-singularity condition ensures that the curve does not contain any cusps or self-intersections. The set of all solutions $(x, y) \epsilon F_p \times F_p,$ together with a special point at infinity, forms an abelian group under the operation of point addition[16]. This group structure makes elliptic curves suitable for defining secure cryptographic primitives.

Group Law and Operations

The group operation on an elliptic curve is defined through point addition. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on the curve, their sum $R = P + Q$ is obtained by drawing a line through P and Q, finding the third intersection with the curve, and reflecting it across the x-axis. The case $P = Q$ corresponds to the point doubling operation. These rules, when formalized algebraically, endow the set of points on the curve with associativity, identity, and inverse elements, thereby forming a group.

This group structure allows us to generate cyclic subgroups. For a base point P of large order n, the subgroup $\langle P \rangle = \{P,\ 2P,\ 3P, \dots, (n-1)P\}$ is cyclic and forms the basis of key generation in elliptic curve cryptography[16].

Elliptic Curve Discrete Logarithm Problem (ECDLP)

The security of ECC relies on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Specifically, given a base point $Q = dP$ on the curve, it is computationally infeasible to determine the integer d within polynomial time for large parameters. Unlike the integer factorization problem used in RSA, which has sub-exponential algorithms, the best-known algorithms for ECDLP remain exponential in complexity. This hardness ensures that ECC achieves equivalent security with much smaller key sizes, making it highly efficient[17].

Key Generation in ECC

The process of generating keys in ECC is straightforward but mathematically secure. Each user selects a random integer d within the range $[1, n-1]$ as their private key, where n is the order of the base point. The corresponding public key is computed as $Q = dP,$ where P is the base point on the curve. While computing Q from d and P is efficient through repeated point addition (scalar multiplication), recovering d from P and Q is computationally infeasible due to the ECDLP[15,18].

Elliptic Curve Digital Signature Algorithm (ECDSA)

The elliptic curve digital signature algorithm (ECDSA) is one of the most widely used cryptographic protocols based on elliptic curves[19]. It enables secure authentication by binding a digital message to a signer's private key.

- Signature generation: To sign a message digest m, the signer chooses a random ephemeral key k, computes the point $R = kP$, and lets $r = x_R \bmod n$. The second component of the signature is computed as $s = k^{-1}(m + dr) \bmod n,$ where d is the private key. The signature thus the pair (r, s).
- Signature verification: Given (r, s) the verifier computes $w = s^{-1} \bmod n,$ then calculates $u_1 = mw \bmod n$ and $u_2 = rw \bmod n$. The point $X = u_1 P + u_2 Q$ is determined, and the signature is accepted if $r \equiv x_X \bmod n.$

Since the verification process depends on the group structure of the elliptic curve, forging a valid signature without knowledge of the private key is computationally infeasible.

Illustrative Example

To illustrate the mechanics of ECC in a simple manner, consider an elliptic curve over the small finite field F_{17} defined by:

$$E: y^2 = x^3 + 2x + 2 \ (mod\ 17).$$

Let the base point be $P = (5,1)$. Suppose a user selects $d = 7$ as the private key. The corresponding public key is $Q = 7P,$ computed via repeated point addition. If the user wishes to sign a short message, digest t$m = 13$, they follow the ECDSA steps using a chosen random k, producing a signature pair (r, s). The verification process, using only Q and the public parameters, confirms the authenticity of the signature[20].

Although the field size is small in this example, making computations feasible by hand, the same principles apply in practice with much larger primes (e.g., 256-bit), where the system becomes secure against brute-force attacks.

IV. Methodology

Rationale for Using ECC

The existing land registration system in Bangladesh relies heavily on handwritten documents and manual seals, which are prone to forgery, loss, and disputes[21]. To overcome these challenges, a digital system with cryptographic safeguards is necessary. Elliptic Curve Cryptography (ECC) is particularly suitable for this purpose because it provides strong security with significantly smaller key sizes compared to traditional RSA systems. This efficiency reduces computational costs and storage requirements, making ECC ideal for deployment in registry offices across Bangladesh where digital infrastructure is often limited.

Application to Land Registry Transactions

In the proposed framework, ECC is employed primarily for digital signatures and authentication between citizens, land officials, and the central registry authority. Each participant is assigned a unique pair of cryptographic keys:

- Private key (d): It is securely stored by the citizen or official.
- Public key (Q): It is stored in the registry database and available for verification.

When a land transaction is initiated (e.g., transfer of ownership), the owner generates a digital signature using the Elliptic Curve Digital Signature Algorithm (ECDSA). The registry authority verifies this signature against the stored public key, ensuring that the transaction was authorized by the rightful owner. Because the verification process is mathematically tied to the elliptic curve group law, fraudulent alterations are computationally infeasible [22].

Workflow Model for Bangladesh

The proposed system follows four essential steps:

a) Registration: Citizens generate ECC key pairs during enrollment, creating a digital identity bound to their property records.

b) Transaction Request: For land transfer, the owner signs the request using ECDSA.

c) Verification: Registry officials verify the digital signature using the stored public key and validate consistency with blockchain records.

d) Ledger Update: Once verified, the transaction is appended to the blockchain, ensuring both immutability and transparency.

This workflow directly addresses issues of forged papers, fake signatures, and unauthorized transfers, which are prevalent in the current manual registry system [21]. Another format of the workflow has been represented in figure 4.1.

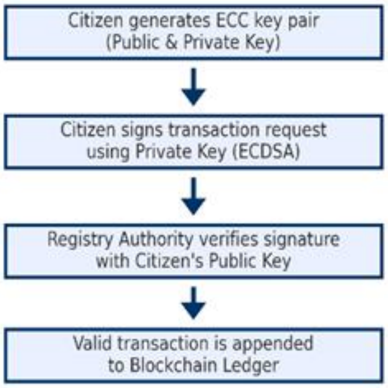
Citizen generates ECC key pair
(Public & Private Key)
Citizen signs transaction request
using Private Key (ECDSA)
Registry Authority verifies signature
with Citizen's Public Key
Valid transaction is appended
to Blockchain Ledger

Fig. 4.1. Flowchart of ECC-based Land Registry.

Table 4.1: Comparison between Manual vs ECC-based land registry system.

Feature	Current Manual System	Proposed ECC-Based System
Verification Method	Handwritten signatures & seals (easily forged)	Digital signatures (ECDSA) with mathematical verification
Forgery Risk	High–fake papers, duplicate seals common	Very low – requires solving ECDLP, practically infeasible
Processing Speed	Slow – manual verification and filing	Fast – automated verification using public keys
Transparency	Limited – records can be hidden or altered	High – verifiable digital records, possible blockchain ledger
Storage & Security	Vulnerable to loss, fire, or tampering	Secure digital database with cryptographic protection
Scalability	Difficult – paper archives are bulky	Easy – supports nationwide digital integration

Integration with Blockchain Framework

The land registry database is maintained on a permissioned blockchain, where each block records verified land transactions. ECC-based digital signatures serve as the access and validation mechanism, ensuring that only legitimate owners and verified officials can authorize updates. This design creates a tamper-resistant ledger of property ownership while preserving accountability at each stage. The blockchain ensures immutability, while ECC ensures transactional authenticity [23].

Justification for Weierstrass Form

Although multiple representations of elliptic curves exist (e.g., Edwards, Montgomery), the Weierstrass form remains the most widely standardized and adopted in government and industry cryptographic libraries. Its mathematical properties are well-understood, and it forms the basis of existing standards such as NIST P-256 and secp256k1, widely deployed in financial technologies [24]. By leveraging the Weierstrass form, this framework ensures compatibility with existing security infrastructures, while providing a robust foundation for future upgrades.

V. Results and Discussion

Hardness of Forgery and ECDLP Security

The central mathematical guarantee of the proposed framework comes from the elliptic curve discrete logarithm problem (ECDLP). Formally, given a base point P on a curve $E(F_p)$ of large prime order n, and a public key $Q = dP$, no efficient algorithm is known to recover the private scalar d from (P, Q). The best known generic attacks, such as Pollard's Rho, require $O(\sqrt{n})$ operations. For a 256-bit prime-order subgroup, this corresponds to approximately 2^{128} steps which is far beyond feasible computation[15,25].

This translates directly into the land registry context: forging a digital signature on a property transfer would require solving an instance of the ECDLP. With $|n| \approx 2^{256}$, the expected effort is comparable to 10^{38} operations, rendering forgery mathematically infeasible. This is illustrated in Figure 5.1, which shows the exponential decline in forgery probability as ECC key sizes increase.

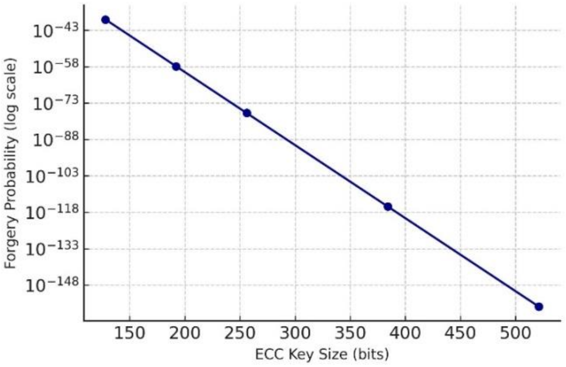

Fig. 5.1. Forgery probability vs ECC key size.

Signature Size and Efficiency of Verification

Another measurable result is the compactness of elliptic curve signatures. An ECDSA signature consists of two integers (r, s), each bounded by the group order n. For a 256-bit curve, both values require 256 bits, giving a total signature size of only 512 bits (64 bytes). By comparison, RSA-3072 requires signatures of at least 384 bytes [19].

Verification also has a mathematical advantage: ECC signature verification involves two scalar multiplications and one addition in the elliptic curve group. With optimized algorithms (e.g., double-and-add, windowed methods), the asymptotic complexity $O(\log n)$. By contrast, RSA verification requires modular exponentiation with a 3072-bit modulus, which is asymptotically more costly.

Here, figure 5.3 compares overall performance metrics such as forgery risk, verification speed, storage efficiency, and transparency.

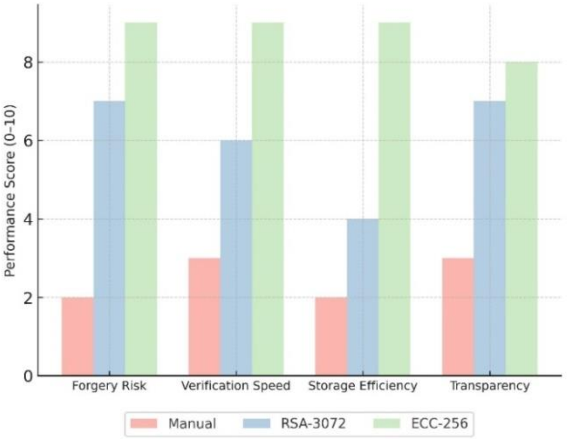

Fig. 5.2. Overall performance matrices for specific systems

Storage and Ledger Growth Analysis

From a mathematical perspective, long-term storage requirements can be modeled as:

$$S(T) = (s + m) \times R \times T,$$

where s is the signature size, m is metadata size, R is the average number of transactions per day, and T is the number of days. Substituting $s = 64$ bytes, $m \approx 256$ bytes, and a conservative R=1000, the growth over five years is approximately:

$$S(5\ years) = (320\ bytes) \times (1000 \times 365 \times 5) \approx 0.58GB$$

This shows that the cryptographic data overhead is negligible for national-scale adoption. Here, figure 5.3 presents projected ledger growth over multiple years under different transaction loads, confirming that even higher activity levels result in manageable storage requirements.

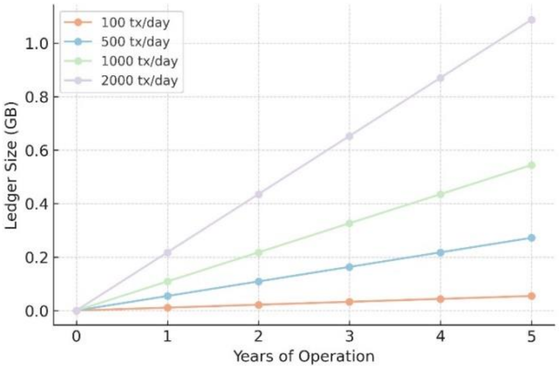

Fig. 5.3. Ledger growth over multiple years for different transactions.

Implications for Bangladesh

The mathematical results have direct relevance for Bangladesh's land registry modernization. Currently, forged deeds and multiple sales of the same property are among the most common sources of dispute, with land-related cases accounting for a large majority of civil litigation[26]. By anchoring every transaction in a mathematically verifiable signature, the possibility of fraudulent duplication is eliminated.

The small size of ECC signatures (64 bytes) also makes them particularly suitable for integration with Bangladesh's existing e-Mutation system, where bandwidth and storage are constrained in rural offices[27]. The computational efficiency ensures that verification can be performed on modest hardware, which is a realistic requirement in local land offices.

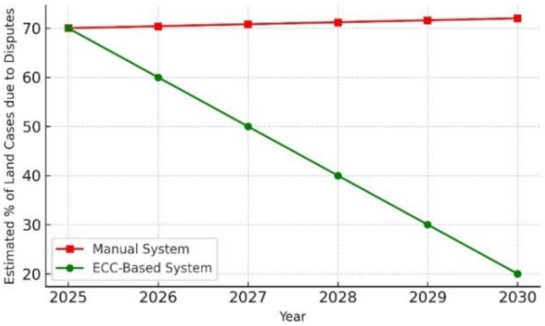

Fig. 5.4. Estimated percent of land cases due to disputes over the next 5 years.

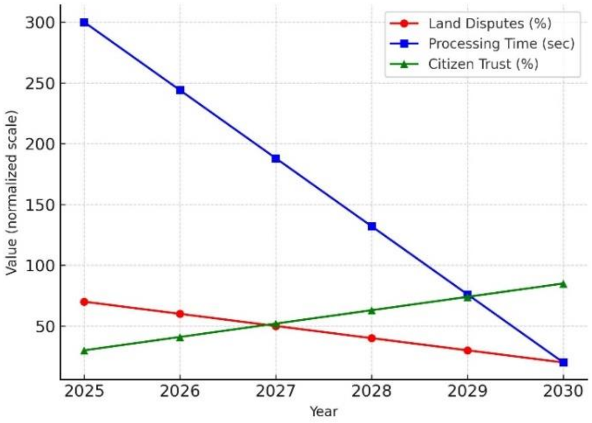

Fig. 5.5. Expected impacts on various factors over time.

Figure 5.4 shows the projected reduction in land-related disputes over time with ECC adoption, while Figure 5.5 summarizes expected impacts on disputes, processing times, and citizen trust. In addition, Figure 5.6 highlights how vulnerabilities such as forgery, data loss, and lack of transparency are significantly reduced under ECC compared with manual or RSA-based systems.

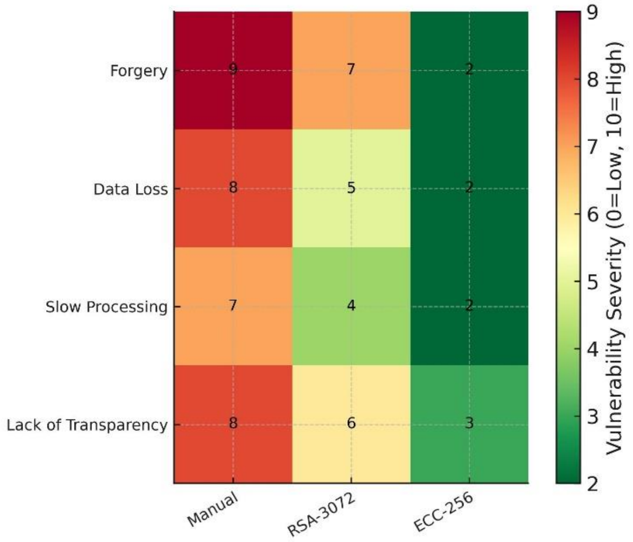

Fig. 5.6. Vulnerability comparison between various systems

Limitations and Path Forward

Although the mathematical foundations are sound, practical limitations remain. Key management poses a challenge: if private keys are lost or misused, rightful owners could face new types of disputes. Institutional readiness, including the legal recognition of digital signatures under land law, is also essential [28]. Furthermore, while blockchain integration could provide stronger immutability guarantees, it introduces higher storage and synchronization costs, making ECC-only solutions an immediate option.

VI. Conclusion and Future Work

This paper has proposed an algebraic cryptographic framework, based on elliptic curve digital signatures, for strengthening Bangladesh's land registration system. By implementing the design in the hardness of the elliptic curve discrete logarithm problem, the framework ensures mathematical resistance against forgery. The analysis showed that ECC signatures are compact, efficient to verify, and impose negligible storage growth even at nationwide transaction volumes. These properties make ECC particularly well suited for Bangladesh, where land disputes are pervasive, legal processes are slow, and rural offices face resource constraints. Integrating such a system would significantly reduce fraudulent transfers, increase transparency, and enhance trust in property ownership records.

At the same time, the study has recognized key challenges. Legal recognition of digital signatures under land law, institutional preparedness, and citizen-level awareness remain essential for successful implementation. Furthermore, key management and recovery policies must be developed to address potential risks arising from the loss or misuse of private keys.

Looking forward, several research and implementation pathways remain open. First, pilot deployments could empirically measure transaction throughput, latency, and storage behavior in local land offices, validating the mathematical projections. Second, integration with national digital identity infrastructure could create a seamless link between individuals and their cryptographic property records. Finally, blockchain-based extensions such as smart contracts for automated ownership transfer could be explored once foundational ECC adoption is in place, providing stronger immutability at the cost of higher system overhead.

In conclusion, this work demonstrates that algebraic cryptography offers a mathematically rigorous, practically efficient, and contextually relevant solution for digitizing Bangladesh's land registry. By combining strong security guarantees with realistic implementation strategies, it establishes a foundation for transparent, corruption-resistant, and future-ready land governance.

References

1. Raihan S, Jalal MdJE, E, Sharmin MA. Eusuf Institutional Challenges in Land Administration and Management in Bangladesh. In: Raihan S, Bourguignon F, Salam U, eds. Is the Bangladesh Paradox Sustainable?: The Institutional Diagnostic Project. Cambridge University Press; 2024:262-294.

2. Sakib NH, M, Islam Shishir MFJ. National integrity strategy implementation in land administration to prevent corruption in Bangladesh. SN Soc Sci. 2022;2(4):43. doi: 10.1007/s43545-022-00352-5. Epub 2022 Apr 14. PMID: 35437518; PMCID: PMC9008375.

3. Report on the corruption in the land sector of Bangladesh, https://www.dhakatribune.com/bangladesh/bangladesh-others/107841/tib-land-sector-heavily-corrupt

4. Land registry issues in Bangladesh, https://www.observerbd.com/news/526778

5. Challenges of scaling e-Mutation in Bangladesh, https://bigd.bracu.ac.bd/study/effectiveness-and-challenges-of-scaling-up-e-mutation-in-bangladesh/?

6. Kazi Masudul Alam, J.M. Ashfiqur Rahman, Anisha Tasnim, Aysha Akther, A Blockchain-based Land Title Management System for Bangladesh, Journal of King Saud University - Computer and Information Sciences, 34(6A), 2022, 3096-3110, 1319-1578, https://doi.org/10.1016/j.jksuci.2020.10.011.

7. Mohammad Rifat Ahmmad Rashid, Abdullah Al Rafi, Md. Ashraful Islam, Sifat Ullah Sharkar, Ziaul Haque Rafi, Mahamudul Hasan, Md Sawkat Ali, M. Saddam Hossain Khan, Enhancing land management policy in Bangladesh: A blockchain-based framework for transparent and efficient land management, Land Use Policy, 150, 2025, 107436, 0264-8377, https://doi.org/10.1016/j.landusepol.2024.107436.

8. A Secure Land Record Management System using Blockchain Technology, https://arxiv.org/abs/2304.13512

9. Land Registry using Blcokchain in India, https://www.undp.org/blog/using-blockchain-make-land-registry-more-reliable-india

10. Initiative taken in Bangladesh using Blockchain in the education and agriculture sectors, https://a2i.gov.bd/site/page/74e7e5ae-2f91-47a9-b339-00c5c76a92aa/-

11. Introducing DSS Publishing Guidelines, https://www.nist.gov/news-events/news/2023/02/nist-revises-digital-signature-standard-dss-and-publishes-guideline

12. [12] N. Kuze, A. Sakakibara and T. Ushio, "WiP Abstract: Detection of False Injection Attacks Based on LTL for Fallback Control," 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), Sydney, NSW, Australia, 2020, pp. 194-195, doi: 10.1109/ICCPS48487.2020.00030.

13. K. Sato et al., "Development of Augmented Reality-Based Application to Search for Electric Appliances and Furniture," 2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech), Nara, Japan, 2021, pp. 214-216, doi: 10.1109/LifeTech52111.2021.9391825.

14. Silverman, J.H. (2009). The Arithmetic of Elliptic Curves. Springer.

15. Koblitz, N. (1987). “Elliptic curve cryptosystems.” Mathematics of Computation, 48(177), 203–209.

16. Washington, L.C. (2008). Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC.

17. Miller, V.S. (1985). “Use of elliptic curves in cryptography.” Advances in Cryptology—CRYPTO’85 Proceedings. Springer, 417–426.

18. Hankerson, D., A., Menezes, & S. Vanstone, (2004). Guide to Elliptic Curve Cryptography. Springer.

19. Johnson, D., A., Menezes, & S. Vanstone, (2001). “The Elliptic Curve Digital Signature Algorithm (ECDSA).” International Journal of Information Security, 1(1), 36–63.

20. Blake, I., G., Seroussi, & N. Smart, (1999). Elliptic Curves in Cryptography. Cambridge University Press.

21. Alam, S., & Rabby, M.F. (2019). “Challenges in digitizing land records in Bangladesh.” Journal of Land Use Policy, 85, 59–67.

22. Paar, C., & J. Pelzl, (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

23. Hossain, M., & M. Rahman, (2021). “Blockchain-based land registry system: A study for Bangladesh.” International Journal of Computer Applications, **174(12),** 1–6.

24. NIST. (2013). Digital Signature Standard (DSS), FIPS PUB 186-4. U.S. Department of Commerce.

25. Miller, V.S. (1986). Use of Elliptic Curves in Cryptography. In: Williams, H.C. (eds) Advances in Cryptology — CRYPTO ’85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

26. Mattsson, M and A. M. Mobarak, (2025), Formalizing Dispute Resolution: Effects of Village Courts in Bangladesh, http://dx.doi.org/10.2139/ssrn.4740074

27. Ministry of Land (2023). Towards Star Quality Land Services by 2026. Dhaka: Government of Bangladesh.

28. VDB-LoI (2022). Electronic Signatures and Certification Authorities in Bangladesh, https://www.vdb-loi.com/bd_publications/rules-on-electronic-signatures-in-bangladesh/