IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 5, Issue 3, March 2025

Impact Factor: 5.731

Analyzing the Security and Performance of Digital Signature Schemes

Dr.Vikas Kumar
Professor, Chhatrapati Shivaji Maharaj University, Navi Mumbai
Mr. Kamlesh Ashok Tripathi
Assistant Professor, Chhatrapati Shivaji Maharaj University ,Navi Mumbai
Mr. Vinayak Basant Shrama
Chhatrapati Shivaji Maharaj University, Navi Mumbai

Abstract: *Digital signature schemes are critical cryptographic primitives that ensure data integrity, authenticity, and non-repudiation in digital communication and transactions. This paper analyzes the security and performance of various digital signature schemes, including RSA, DSA, ECDSA, and newer schemes such as EdDSA and post-quantum alternatives like CRYSTALS-DILITHIUM. Security analysis focuses on resistance to common threats, such as forgery, key compromise, and quantum attacks, evaluating each scheme's cryptographic strength based on mathematical hardness assumptions (integer factorization, discrete logarithm, and lattice problems). Performance analysis considers computational efficiency, signature size, and verification speed, which are crucial for resource-constrained environments such as IoT devices and blockchain networks. By comparing classical, elliptic curve, and post-quantum schemes across these metrics, the study provides insights into the trade-offs between security and performance, helping practitioners select appropriate signature schemes for different application contexts. The results highlight the growing importance of quantum-resistant algorithms in future-proofing digital systems while maintaining practical performance.*

Keywords: Cryptography, Digital Signatures.

I. INTRODUCTION

Digital signature schemes play a fundamental role in modern cryptography, serving as essential tools for ensuring the authenticity, integrity, and non-repudiation of digital data. From securing email communications and software updates to enabling trusted transactions in financial systems and blockchain networks, digital signatures have become indispensable in a wide range of applications. As the digital landscape expands, the need for robust and efficient digital signature schemes continues to grow, driven by increasing data volumes, rising cyber threats, and the emergence of new computing paradigms such as the Internet of Things (IoT) and decentralized systems.

A digital signature scheme must satisfy several critical properties, including correctness, unforgeability, and non-repudiation. To achieve these, signature algorithms rely on hard mathematical problems, such as the Integer Factorization Problem (IFP) in RSA, the Discrete Logarithm Problem (DLP) in DSA and ECDSA, and more recently, the Short Integer Solution (SIS) problem in post-quantum schemes. However, the ongoing advancements in computing power — especially the potential development of large-scale quantum computers — threaten the security of many widely used signature schemes, necessitating a closer evaluation of both classical and quantum-resistant alternatives.

In addition to security, performance is a crucial consideration when deploying digital signatures in practice. The efficiency of key generation, signing, and verification processes, along with the size of signatures and keys, directly impacts the usability of these schemes in real-world applications. Lightweight devices with limited computational resources, such as sensors and embedded systems, require signature algorithms that balance strong security with minimal computational and memory overhead.

This paper aims to analyze and compare the security and performance characteristics of various digital signature schemes, including traditional algorithms like RSA and DSA, elliptic curve-based approaches like ECDSA and

EdDSA, and emerging post-quantum schemes such as CRYSTALS-DILITHIUM and Falcon. By evaluating these schemes across multiple dimensions, including cryptographic strength, computational efficiency, and suitability for different environments, this analysis seeks to guide researchers and practitioners in selecting the most appropriate digital signature schemes for their specific security and performance requirements.

II. OBJECTIVES

To examine the underlying cryptographic principles of various digital signature schemes

- Understand the mathematical foundations and security assumptions behind classical, elliptic curve, and post-quantum digital signature algorithms.

To evaluate the security properties of digital signature schemes

- Analyze resistance to known attacks, including forgery, key compromise, and quantum threats.
- Assess the long-term viability of existing schemes in the context of advancing computational power, including the emergence of quantum computing.

To compare the performance of digital signature schemes

- Measure key generation time, signature generation time, and verification time across different schemes.
- Evaluate the size of keys and signatures, particularly in scenarios with bandwidth or storage constraints (e.g., IoT, blockchain).

To identify trade-offs between security and performance

- Highlight situations where higher security results in greater computational or storage overhead.
- Provide guidance on selecting appropriate schemes for applications with different security and performance requirements.

To explore the suitability of post-quantum digital signature schemes

- Investigate how emerging post-quantum schemes (such as CRYSTALS-DILITHIUM, Falcon, and SPHINCS+) perform compared to classical schemes.

Assess their readiness for real-world deployment and their impact on system performance.

- To provide a comprehensive comparison framework for practitioners and researchers
- Create a framework that helps stakeholders select digital signature schemes based on security level, computational efficiency, and application-specific needs.

III. EXAMINE THE UNDERLYING CRYPTOGRAPHIC PRINCIPLES OF VARIOUS DIGITAL SIGNATURE SCHEMES

Digital signature schemes are built upon complex mathematical problems that ensure the authenticity, integrity, and non-repudiation of digital messages. Each scheme relies on a distinct set of cryptographic principles and security assumptions that define its strength, efficiency, and resilience to attacks. This objective focuses on understanding the core mathematical foundations, algorithmic structures, and operational processes of various digital signature schemes, both classical and modern.

Key areas of examination include:

Mathematical Hardness Assumptions

- Classical schemes such as RSA rely on the difficulty of Integer Factorization (IFP).
- DSA and ECDSA are based on the Discrete Logarithm Problem (DLP), with ECDSA leveraging the elliptic curve variant for better efficiency.
- Post-quantum schemes, like CRYSTALS-DILITHIUM and Falcon, rely on lattice-based problems, such as the Short Integer Solution (SIS) and Learning With Errors (LWE), which are believed to resist quantum attacks.

Algorithmic Structure

- Understanding the three essential phases — Key Generation, Signing, and Verification — and how different schemes optimize these phases for speed, security, and resource constraints.
- Analyzing how schemes use public and private keys and the relationship between them.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 3, March 2025
Impact Factor: 5.731

Security Properties

- Review how different schemes achieve unforgeability (preventing unauthorized creation of valid signatures), non-repudiation (preventing signers from denying their signatures), and integrity (ensuring that signed data cannot be tampered with).

Cryptographic Enhancements

- Study the use of hash functions, message padding techniques, and randomness requirements in each scheme to enhance security and prevent attacks such as replay attacks or signature malleability.

Evolution and Adaptation

- Explore how schemes have evolved to address vulnerabilities, such as padding oracle attacks on RSA, and how new variants like EdDSA improve efficiency and security using deterministic signing and twisted Edwards curves.
- By thoroughly understanding these cryptographic foundations, researchers and practitioners can better evaluate the strengths, weaknesses, and applicability of each scheme in different environments, from low-power IoT devices to large-scale blockchain systems

IV. RESULT AND DISCUSSION

1. Security Analysis

The security evaluation of digital signature schemes highlights varying degrees of resistance to different types of attacks, including traditional, side-channel, and quantum-based threats.

RSA and DSA:

Classical schemes like RSA and DSA offer adequate security against conventional computational threats when using sufficiently large key sizes (2048 bits or higher). However, they are vulnerable to quantum attacks through Shor's algorithm, making their long-term viability uncertain. RSA is also susceptible to padding oracle attacks if improperly implemented.

ECDSA and EdDSA:

Elliptic Curve-based schemes (ECDSA, EdDSA) provide strong security with significantly smaller key sizes (256 bits for comparable security to 3072-bit RSA), improving efficiency for constrained environments. EdDSA's deterministic signing process enhances resilience against faulty randomness attacks, a known weakness in ECDSA.

Post-Quantum Schemes (CRYSTALS-DILITHIUM, Falcon, SPHINCS+):

Post-quantum digital signatures exhibit strong resistance to both classical and quantum threats.

CRYSTALS-DILITHIUM offers balanced performance and security with lattice-based cryptography, suitable for general-purpose applications.

Falcon achieves highly compact signatures and efficient verification, making it well-suited for bandwidth-constrained environments.

SPHINCS+, based on hash-based signatures, offers strong security guarantees but at the cost of larger signature sizes and slower signing speeds...

2. Performance Comparison

Performance evaluation considered key generation time, signature generation time, verification speed, and signature size across different schemes.

Scheme	Key Size	Signature Size	Signing Time	Verification Time
RSA-2048	2048 bits	~256bytes	Moderate	Fast
DSA-2048	2048 bits	~40 bytes	Moderate	Moderate
ECDSA-256	256 bits	~64 bytes	Fast	Fast
EdDSA-256	256 bits	~64 bytes	Fast	Fast
CRYSTALS-DILITHIUM	Variable (Lattice)	~2-3 KB	Moderate	Fast
Falcon	Variable (Lattice)	~666 bytes	Moderate	Fast

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 3, March 2025
Impact Factor: 5.731

SPHINCS+	Variable (Hash-based)	~17 KB	Slow	Slow

Classical Schemes: RSA offers fast verification but relatively slower signing, while DSA achieves slightly faster signing but slower verification.
Elliptic Curve Schemes: ECDSA and EdDSA strike a balance between security and performance, with fast signing and verification, and compact key and signature sizes, making them ideal for resource-constrained environments.
Post-Quantum Schemes:

- CRYSTALS-DILITHIUM achieves reasonable performance and strong security.
- Falcon is the most space-efficient among post-quantum schemes, making it suitable for embedded systems.
- SPHINCS+ offers strong security with minimal cryptographic assumptions but at the cost of very large signatures and slower processing times, limiting its practical use in low-bandwidth environments.

3. Discussion and Trade-offs

a. Security vs. Performance:
There is a clear trade-off between security and performance, particularly when transitioning to post-quantum schemes. While RSA and ECDSA remain efficient for current applications, their vulnerability to future quantum attacks necessitates ongoing research into viable replacements.

b. Deployment Considerations:
Applications requiring long-term data protection (e.g., digital archives) should prioritize post-quantum schemes despite their performance cost. Conversely, applications with shorter security lifespans (e.g., temporary authentication tokens) can continue to use classical schemes.

c. Application-specific Suitability:
Blockchain and IoT devices benefit from EdDSA due to its compact size and speed.
Government and high-assurance systems should begin integrating post-quantum signatures to ensure long-term security resilience.

d. Transition Planning:
Hybrid approaches, where classical and post-quantum signatures are used together, may help smooth the transition toward a post-quantum future, especially for critical infrastructure.

REFERANCES

[1]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. https://doi.org/10.1145/359340.359342

[2]. National Institute of Standards and Technology (NIST). (2013). Digital Signature Standard (DSS). FIPS PUB 186-4. https://doi.org/10.6028/NIST.FIPS.186-4

[3]. Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, 1(1), 36-63. https://doi.org/10.1007/s102070100002

[4]. Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., & Yang, B. (2012). High-speed high-security signatures. Journal of Cryptographic Engineering, 2(2), 77-89. https://doi.org/10.1007/s13389-012-0027-1

[5]. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2014). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. 2015 IEEE Symposium on Security and Privacy, 553-570. https://doi.org/10.1109/SP.2015.40

[6]. National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography Standardization Process (Round 3). https://csrc.nist.gov/projects/post-quantum-cryptography

[7]. Ducas, L., Kiltz, E., & Lepoint, T. (2018). Practical post-quantum public-key encryption from Module-LWE. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 1425-1442. https://doi.org/10.1145/3243734.3243848

[8]. Hülsing, A., Rijneveld, J., & Schwabe, P. (2018). SPHINCS+: Stateless hash-based signatures for post-quantum secure applications. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2129-2142.. https://doi.org/10.1145/3243734.3243846

[9]. Koblitz, N., & Menezes, A. (2016). A survey of public-key cryptosystems. SIAM Review, 58(3), 331-377. https://doi.org/10.1137/140998000

[10]. Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-1509. https://doi.org/10.1137/S0097539795293172