IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–3. DOI:XXXXXXXX

Implementation and Performance Analysis of XX-DSA Digital Signatures in XXX Protocol Migration

Jiahao Xiang[1] and Lang Li[1]

Hengyang Normal University, College of Computer Science and Technology, Hengyang, China

Abstract. The advent of cryptographically relevant quantum computers poses a significant threat to current public-key cryptography systems. In response, NIST has standardized post-quantum cryptographic algorithms, including XX-DSA (Post-Quantum Digital Signature Algorithm) for secure digital signatures. This paper presents a comprehensive implementation and performance analysis of XX-DSA digital signatures integrated into secure network communication protocols for post-quantum migration.

We implement XX-DSA variants with different security levels in a secure protocol framework and evaluate their performance characteristics, including signature generation/verification times, handshake latency, and network overhead. Our implementation follows the NCCoE SP 1800-38C migration protocol guidelines and incorporates both pure post-quantum and hybrid classical-quantum approaches. Experimental results demonstrate that XX-DSA provides a viable solution for post-quantum authentication with manageable performance trade-offs and certificate size considerations.

Keywords: Post-Quantum Cryptography · XX-DSA · Digital Signatures · Protocol Migration · Secure Communications

1 Introduction

The transition to post-quantum cryptography represents one of the most significant challenges in modern cybersecurity. With NIST's standardization of post-quantum cryptographic algorithms including XX-DSA (Post-Quantum Digital Signature Algorithm) [NIS24], organizations must now prepare for the migration from classical cryptographic systems that will be vulnerable to quantum attacks.

Secure communication protocols, being widely deployed across internet infrastructure, represent critical targets for post-quantum migration. While key exchange migration using post-quantum key encapsulation mechanisms has shown promising results with minimal performance impact [NCC23], the migration of authentication mechanisms using digital signatures presents greater challenges due to significantly larger signature and certificate sizes.

This paper addresses the practical implementation of XX-DSA digital signatures in secure protocol frameworks, focusing on the real-world challenges identified in the NCCoE SP 1800-38C migration protocol testing. We contribute:

- A comprehensive implementation of XX-DSA variants in secure protocols with performance benchmarking
- Analysis of network protocol impacts, particularly certificate size effects on handshake performance

- Practical migration strategies including hybrid approaches and protocol optimization techniques

2 Background and Related Work

2.1 Post-Quantum Cryptography Standardization

NIST's Post-Quantum Cryptography standardization process, initiated in 2016, culminated in the publication of post-quantum cryptographic standards including various digital signature algorithms [NIS24]. XX-DSA represents one approach to post-quantum digital signatures, providing multiple security levels corresponding to different classical security equivalents.

2.2 Secure Protocols and Post-Quantum Migration

Modern secure communication protocols facilitate post-quantum migration through flexible cryptographic negotiation mechanisms and adaptable handshake structures. Previous work has demonstrated successful integration of post-quantum key exchange mechanisms [KSD20, SKD20], but authentication migration presents unique challenges due to the size characteristics of post-quantum signatures.

2.3 NCCoE Migration Protocol Testing

The NCCoE SP 1800-38C testing program provided crucial insights into post-quantum protocol migration, demonstrating high interoperability success rates across vendors while identifying specific performance bottlenecks in authentication scenarios [NCC23]. Our implementation directly addresses the challenges identified in this comprehensive testing effort.

3 XX-DSA Algorithm Overview

3.1 Post-Quantum Digital Signature Foundation

XX-DSA is a post-quantum digital signature algorithm designed to provide security against both classical and quantum adversaries. The algorithm provides digital signatures with strong security guarantees based on mathematical problems believed to be quantum-resistant.

3.2 Parameter Sets and Security Levels

XX-DSA defines multiple parameter sets providing different security levels:

- **XX-DSA Level 1**: Provides security equivalent to AES-128
- **XX-DSA Level 3**: Provides security equivalent to AES-192
- **XX-DSA Level 5**: Provides security equivalent to AES-256

The signature and public key sizes vary with security level, representing increases compared to classical signatures, presenting the primary challenge for protocol integration.

References

[KSD20] Panos Kampanakis, Dimitrios Sikeridis, and Michael Devetsikiotis. Post-quantum authentication in tls 1.3: A performance study. In *Proceedings 2020 Network and Distributed System Security Symposium*. Internet Society, 2020.

[NCC23] NCCoE. Migration to post-quantum cryptography quantum readiness. NIST Special Publication 1800-38, 2023. Available at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

[NIS24] NIST. Post-quantum cryptography standards. NIST Post-Quantum Cryptography Standardization, 2024. Available at: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[SKD20] Dimitrios Sikeridis, Panos Kampanakis, and Michael Devetsikiotis. Assessing the overhead of post-quantum cryptography in tls 1.3 and ssh. In *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies*, pages 149–156. ACM, 2020.