Evaluation Criteria for Public-Key Cryptographic Algorithms

Institute of Commercial Cryptography Standards

October, 2025

Contents

This document specifies the considerations of evaluating and selecting public-key cryptographic algorithms in the Next-generation Commercial Cryptographic Algorithm Program (NGCC) held by the Institute of Commercial Cryptography Standards (ICCS).

1 Security

(1) Theoretical Security

Digital signature schemes shall satisfy EUF-CMA or SUF-CMA security. Key encapsulation mechanisms shall satisfy IND-CCA2 security. Key exchange protocols shall satisfy the security under a suitable security model (e.g, CK, CK+, eCK, eCK-PFS models).

(2) Practical Security

All algorithms instances shall achieve the corresponding classical (quantum-resistant) security strength levels with a certain amount of security redundancy. For the purpose of evaluating security strengths, the attacker can be assumed to have access to signatures for no more than 2^{80} chosen messages, or the decapsulations of no more than 2^{80} chosen ciphertexts, etc.

(3) Other Security Properties

The security against side-channel attacks, (perfect) forward secrecy, security against multi-key attacks, and security in the case of (temporary) key reuse, etc., will be taken into consideration during the evaluation.

2 Performance

(1) Efficiency

Digital signature schemes will be evaluated based on the computational efficiency of the key generation, signature and verification operations. Key encapsulation mechanisms will be evaluated based on the computational efficiency of the key generation, encapsulation and decapsulation operations. Key exchange protocols will be evaluated based on the computational efficiency of establishing a shared secret key.

(2) Transmission and Storage Cost

Digital signature schemes will be evaluated based on the sizes of the public keys, private keys and signatures. Key encapsulation mechanisms will be evaluated based on the sizes of the public keys, private keys, and ciphertexts. Key exchange protocols will be evaluated based on the number of rounds, and the sizes of the long-term public keys (if any), long-term private keys (if any) and exchanged messages.

(3) Resource Consumption

Algorithms will be evaluated based on the memory cost for software implementations, and the area, time delay, throughput, throughput-area ratio, power consumption, and energy consumption for hardware implementations.

3 Features

(1) Innovativeness
Algorithms are innovative, reflecting new design rationale and current trends in cryptography.

(2) Simplicity
In order to facilitate comprehensive security evaluation, algorithms are easy to understand and implement.

(3) Flexibility
Algorithms can be implemented securely and efficiently on a wide variety of platforms, supporting various tradeoffs between efficiency and cost.

(4) Compatibility
Algorithms can be based on the same mathematical hard problem and parameter selection strategy, enabling different cryptographic functionalities (digital signature, key encapsulation and key exchange) with the same security strength. Algorithms may be compatible with existing protocols and applications and easy to migrate.

(5) Extensibility
Algorithms can be modified to provide additional functionalities beyond digital signature, key encapsulation mechanism, and key exchange.

(6) Performance Advantages on Variant Platforms
Algorithms can support various implementation advantages, including parallel processing, instruction set acceleration, and secure and efficient implementation in resource-constrained environments.

4 Overall Considerations

All the aspects including security, performance and other features will be taken into account in the evaluation process. Considering the uncertainty of the new quantum algorithms and cryptographic analysis techniques, the evaluation process will also focus on the diversity of the underlying mathematical hard problem.

Furthermore, commitments made in the intellectual property statements by the submitter(s) and the corresponding patent owner(s) will be considered as one of the important factors. The algorithms without factors (e.g., intellectual property) that might hinder standardization and widespread adoption will be preferred.