Evaluation Criteria for Cryptographic Hash Algorithms

Institute of Commercial Cryptography Standards

October, 2025

Contents

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

1 Security

(1) Theoretical Security
Cryptographic hash algorithms shall have security proofs or analyses of the overall structures and components under reasonable assumptions.

(2) Practical Security
The classical security strength of cryptographic hash algorithms shall be no less than $h/2$ bits against collision attacks, h bits against preimage attacks and second-preimage attacks, where h is the bit length of message digests. Moreover, the complexity of quantum attacks shall be no less than that of generic ones.

(3) Other Security Properties
Cryptographic hash algorithms shall have good statistical randomness. The security against partial-collision attacks, semi-free-start collision attacks, free-start collision attacks, multi-collision attacks, length-extension attacks, etc., and the resistance against collision attacks, preimage attacks, and second-preimage attacks targeting at any fixed subset of cryptographic hash algorithm outputs, etc., will be taken into consideration during the evaluation.

2 Performance

(1) Efficiency
Algorithms will be evaluated based on the computational efficiency of hash operations.

(2) 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 in theory, structure, or other aspects, reflecting new principles and trends in cryptography.

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

(3) Flexibility
Algorithms can be used to construct secure related cryptographic functionalities easily, such as Message Authentication Code (MAC), Key Derivation Function (KDF), and

eXtendable-Output Function (XOF). Algorithms can be implemented securely and efficiently on a wide variety of platforms, supporting various tradeoffs between efficiency and cost.

(4) 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 features will be taken into account in the evaluation process. 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.