

**Evaluation Criteria for  
Cryptographic Hash Algorithms  
(Draft)**

Institute of Commercial Cryptography Standards  
February, 2025

# Contents

1 Security .....	1
2 Performance .....	1
3 Features .....	1
4 Overall Considerations .....	2

This document specifies the considerations of evaluating and selecting cryptographic hash algorithms in the Next-generation Commercial Cryptographic Algorithm Program.

## **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 software implementation memory cost, and the area, time delay, power consumption, energy consumption, throughput, and throughput-area ratio 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 support related cryptographic functionalities, such as Message Authentication Code (MAC). Algorithms can be implemented securely and efficiently on a wide variety of platforms, supporting various tradeoffs between efficiency and cost.

#### **(4) Other Advantages**

Algorithms can support various implementation advantages including parallel processing, extended 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.