Feedback on the Comments Received on the Draft Submission Requirements and Evaluation Criteria for Cryptographic Hash Algorithms

Institute of Commercial Cryptography Standards

October, 2025

The Institute of Commercial Cryptography Standards (ICCS) is truly grateful for all the attention to the Next-generation Commercial Cryptographic Algorithms Program (NGCC). The *Submission Requirements for Cryptographic Hash Algorithms* and the *Evaluation Criteria for Cryptographic Hash Algorithms* serve as important guidelines for NGCC. Since the solicitation of public comments began, ICCS has received a lot of valuable comments from all over the world. ICCS convened experts to conduct a thorough review and evaluation on each of the comments. The feedback on the comments and document changes is as follows.

1. On the requirements for output length and security strength

Some experts inquired about the rationale for soliciting cryptographic hash algorithms with output lengths of 512 and 1024 bits, and suggested to relax the requirements of the security against preimage attacks and second-preimage attacks.

China's SM algorithms have been developed and applied for over 20 years. It is imperative to develop a new generation of commercial cryptographic algorithms, in response to the threat of quantum computing and to accommodate the evolving demands from emerging technologies, such as big data, Internet of Things, cloud computing and artificial intelligence. NGCC plans to call for proposals for public-key cryptographic algorithms, cryptographic hash algorithms and block cipher algorithms to establish an interoperable cryptographic algorithm suit and facilitate the standardization of the next-generation commercial cryptographic algorithms.

ICCS believes that algorithms with 256-bit classical security strength will gradually become the mainstream in cryptography applications. Therefore, NGCC solicits cryptographic hash algorithms with an output length of 512 bits. At the same time, ICCS also pays close attention to the future trends. By specifying algorithm requirements of 512-bit classical security strength with a 1024-bit output length, it aims to lead technological innovation in cryptography, drive generational advancement in cryptographic algorithm design, and prepare for applications with high security requirements in the future.

ICCS notes that the academic community is actively advancing research on the design and analysis of large-state cryptographic hash algorithms. Given this trend, NGCC considers the requirement is reasonable that the classical security strength of cryptographic hash algorithms against preimage attacks and second-preimage attacks shall not be lower than their output length. ICCS expects proposals featuring innovations in theory, structure and other dimensions.

2. On the functional requirements

Some experts inquired whether the submitted cryptographic hash algorithms must be over binary fields. Some experts pointed out that Key Derivation Function (KDF) and eXtendable-Output Function (XOF) represent significant applications of cryptographic hash algorithms, and suggested that the flexibility of supporting the construction of related functions should be considered in the solicitation and selection of cryptographic hash algorithms.

NGCC targets general-purpose cryptographic hash algorithms. Any proposal meeting the *Submission Requirements for Cryptographic Hash Algorithms* is acceptable. The proposals will be evaluated comprehensively from the aspects including security, performance and features based on the *Evaluation Criteria for Cryptographic Hash Algorithms*.

ICCS adopted the opinion about additional functionalities and added KDF and XOF to the "Features" section of the *Evaluation Criteria for Cryptographic Hash Algorithms* as examples related to algorithm flexibility.

3. On the evaluation of implementation efficiency

Some experts suggested to disclose the performance testing environment and conduct performance tests on a unified environment.

ICCS will conduct performance tests on optimized implementations under the same conditions and perform comprehensive evaluations. ICCS will disclose the unified performance testing environment at an appropriate time.

The performance test results provided by submitters are mainly used to describe the performance advantages of their proposals but will not serve as formal proof in performance evaluations. Given that the performance test results provided by submitters cannot serve as comparable benchmarks, ICCS removed the relevant requirements of providing comparative results with the existing standard algorithms in the *Submission Requirements for Cryptographic Hash Algorithms*.

It should be noted that software and hardware implementation performances are both critical factors in algorithm selection. The first submission shall include the software implementation codes along with self-assessment results, while the hardware implementation code and corresponding test results are recommended to be included in the submission. In subsequent evaluation rounds, both software and hardware implementation codes and test results must be submitted.

4. On intellectual property (IP)

Some experts expressed interest in the NGCC's governing principles regarding intellectual property.

ICCS recognizes the value of cryptography research achievements and places high importance on the IP protection. To foster widespread adoption of standardized algorithms, NGCC adheres to fair, reasonable, and non-discriminatory (FRAND) licensing principles. Therefore, statements and licensing commitments about IP from algorithm submitters and relevant patent holders serve as significant factors in the algorithm selection process. Algorithm submitters are required to fully disclose relevant IP information and submit licensing commitments. When the other factors are equivalent, the algorithms with FRAND-Free IP licensing commitment will be preferred.

5. On the auxiliary program

Some experts proposed that the auxiliary program provided by ICCS should have broad applicability with a wide range of compilers.

To facilitate the algorithm correctness verification, ICCS has developed an auxiliary program that enables algorithm submitters to generate Known Answer Test (KAT) vectors running algorithm implementations. ICCS is always committed to the applicability of the auxiliary program. The auxiliary program supports ISO/IEC 9899:1999 (C99) and is compatible with current mainstream compiler environments.

ICCS extends its gratitude again to all experts who made comments and participated in the discussions! Your professional insights and technical contributions provided helpful references and guidance for the program. ICCS will continue to work with the cryptography and industrial community openly and jointly to promote the development of the next-generation commercial cryptographic technologies.