Feedback on the Comments Received on the Draft Submission Requirements and Evaluation Criteria for Public-Key Cryptographic 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 Public-Key Cryptographic Algorithms* and the *Evaluation Criteria for Public-Key Cryptographic 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 purpose and significance of the NGCC

Some experts inquired about the purpose and significance of NGCC in the context that some countries have completed post-quantum cryptography algorithm solicitation and standardization.

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. This represents a new exploration building upon acquired research achievements in cryptography community, seeking to further stimulate innovation in cryptographic algorithm design and analysis techniques, to enhance the novelty and diversity of cryptographic algorithms (particularly post-quantum public-key cryptographic algorithms), to drive more international academic communications, and to promote the advancement of cryptography. NGCC expects to establish an interoperable cryptographic algorithm suit and facilitate the standardization of the next-generation commercial cryptographic algorithms.

2. On the restrictions on proposals

Some experts asked whether NGCC accepts algorithms that were submitted to other international standardization activities but were not selected for standardization.

According to the *Submission Requirements for Public-Key Cryptographic Algorithms*, the algorithms failed in other international standardization activities will not be excluded, but further innovations are expected.

3. On the requirements for security strength levels

Some experts expressed interest in the requirements for security strength levels, suggesting to add the 192-bit security as an option, and inquiring about the considerations of the 512-bit security level.

For the future technological development, the 256-bit security strength will gradually become the mainstream classical security strength level for the next-generation commercial cryptography applications. To adapt to higher security requirements for

future cryptography applications, the 512-bit security strength level is included in the technical requirements. ICCS sets the security strength requirements for the suit of public-key algorithms, cryptographic hash algorithms and block cipher algorithms to support the integrated deployment in the future. Therefore, NGCC mainly focuses on 256-bit and 512-bit security strength levels, and the 192-bit security strength level is not considered. Meanwhile, given that the next-generation public-key cryptographic algorithms will need to be used in combination with current commercial cryptographic algorithms when transitioning to post-quantum cryptography, a 128-bit security strength level is specifically required for public-key cryptographic algorithm proposals.

4. On the corresponding relationship between quantum-resistant and classical security strength levels of algorithms.

Some experts expressed interest in the corresponding relationship between quantum-resistant and classical security strength levels of public-key cryptographic algorithms, suggesting to specify the target security strength levels according to the quantum-resistant security strength. Some experts suggested that the corresponding quantum-resistant security strength of 128-bit classical security strength shall be 128 bits rather than 80 bits.

Currently, there is significant uncertainty in the evaluation of quantum-resistant security strength. By contrast, the classical security strength, which has been more extensively and thoroughly researched, is more stable. Therefore, ICCS adopted the classical security strength to set the requirements of security strength levels, and proposed the corresponding requirements of quantum-resistant security strength. Algorithms based on different technological routes exhibit significant variations in their security strength. Therefore, NGCC made a set of universal minimum requirements for security strength, and will evaluate the redundancy of algorithm security.

Besides, the requirement of a 128-bit classical security strength level is only set for public-key cryptographic algorithm proposals, which will be mainly used in combination with current 128-bit classical secure block cipher algorithms and cryptographic hash algorithms when transitioning to post-quantum cryptography. The 80-bit quantum-resistant security strength can already meet the needs of interoperability with related symmetric primitives.

5. On the time complexity and space complexity

Some experts suggested to take both time complexity and space complexity of known attacks into consideration when defining the security strength of algorithms.

ICCS adopted this opinion and changed the “time complexity” of known attacks to “complexity” in the *Submission Requirements for Public-Key Cryptographic Algorithms*, in order to cover both.

6. On the requirement for the failure probability of decapsulation

Some experts suggested to clarify the requirement for the failure probability of

decapsulation.

The failure probability of decapsulation has been included in the *Submission Requirements for Public-Key Cryptographic Algorithms*. It will be evaluated based on the specific technical route and related mathematical hard problem, and its impact on algorithm security will be analyzed as well.

7. On the submission requirements of key exchange protocols

Some experts pointed out that "key exchange protocols shall include algorithms for initialization, generating and exchanging messages between two parties" in the *Submission Requirements for Public-Key Cryptographic Algorithms* is not accurate, and suggested to make a revision.

ICCS has adopted their suggestion and revised it as "key exchange protocols shall include algorithms for initialization, message generation and shared secret key derivation of two parties". The programming interfaces are also adjusted.

8. On the design methods and security models of key exchange protocols

Some experts asked whether static-static key exchange protocols would be considered, and whether other security models could be used, such as IND-AA.

In order to enrich the diversity of cryptographic algorithms, there are no constraints on the design methods of key exchange protocols. Key exchange protocols can be constructed based on a KEM with a small size, or designed directly. The security models of key exchange protocols are also not restricted, but the reasonableness of security models and the correctness of proofs will be evaluated. ICCS expects static-static key exchange protocols and other innovative key exchange protocol proposals that are applicable for various application scenarios.

9. On block ciphers used in algorithms

Some experts asked whether self-selected block ciphers could be used to design MPC-in-the-Head signature schemes.

It is acceptable to select or design block ciphers as components of public-key cryptographic algorithms, but the security assumptions and analyses of block cipher algorithms are required in algorithm proposals. NGCC will conduct comprehensive evaluations on proposals.

10. 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 Public-Key Cryptographic 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.

11. 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.

12. On the auxiliary program

Some experts proposed that the auxiliary program provided by ICCS should have good applicability, and suggested that the eXtendable Output Function (XOF) shall support "arbitrary" length output.

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 adopted the opinion, and modified the XOF in the auxiliary program to generate an output of "arbitrary" desired length.

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.