Submission Requirements for Public-Key Cryptographic Algorithms (Draft)

Institute of Commercial Cryptography Standards
February, 2025

Contents

This document specifies requirements for public-key cryptographic algorithm submissions in the Next-generation Commercial Cryptographic Algorithms Program.

1 Notes for Algorithm Submitter(s)

Algorithm submitter(s) will be deemed to know and consent to the following:

(1) The Next-generation Commercial Cryptographic Algorithms Program will fully consider various technical features including security, performance, innovation, and factors that might influence widespread adoption of algorithms such as intellectual properties, and then select the finalists through multiple rounds of evaluation, to support the next-generation commercial cryptographic algorithms standardization.

(2) The submitted algorithms and implementations shall be original works of the submitter(s), and the submitter(s) shall fully disclose all patents and patent applications which may cover the algorithms and implementations.

(3) The submitted algorithms and implementations shall be publicly disclosed for a thorough public review. The public review is an important reference for the algorithm evaluation.

(4) The submitted algorithms and implementations shall not contain any data, information or technology which should be confidential according to the laws and regulations of China and other countries, and may infringe upon legitimate rights and interests of any third party.

(5) Considering algorithms innovation, technology diversity and intellectual property issues, the Institute of Commercial Cryptography Standards (ICCS) will not accept the algorithms that are in or have finished the standardization process in international organizations, countries and regions, or related variants with insignificant modifications.

(6) ICCS reserves the right of final interpretation of the Next-generation Commercial Cryptographic Algorithms Program.

2 Technical Requirements

(1) The submitted algorithms shall be capable of supporting three classical security strength levels: 128, 256, and 512 bits. The corresponding quantum-resistant security strength shall be no less than 80, 128, and 256 bits. The algorithms can optionally support 384-bit classical security strength level with no less than 192-bit quantum-resistant security strength. The n-bit classical (quantum-resistant) security strength means that the time complexity of the known classical (quantum-resistant) attacks on the algorithm is at least 2^n. The algorithms shall not incorporate

components that are believed to be insecure against quantum attacks. Moreover, the algorithms shall provide sufficient security redundancy to reduce potential risks from new quantum algorithms and cryptanalysis techniques.

(2) The submitted algorithms shall provide at least one of the following functionalities: digital signature, key encapsulation mechanism, and key exchange.

- Digital signature schemes shall include algorithms for key generation, signature and verification, and be capable of supporting a message size up to 2^{63} bits. Each pair of keys shall support signing and verifying no less than 2^{64} different messages.
- Key encapsulation mechanism schemes shall include algorithms for key generation, encapsulation and decapsulation, and the length of shared secret key shall be no less than the corresponding classical security strength level bits.
- Key exchange protocols shall include algorithms for initialization, generating and exchanging messages between two parties, and the length of shared secret key shall be no less than the corresponding classical security strength level bits.

(3) The submitted algorithms shall be implemented efficiently on a wide range of software and hardware platforms.

(4) It is encouraged that the submitted algorithms supporting different cryptographic functionalities (digital signature, key encapsulation mechanism, and key exchange) be based on the same mathematical hard problem and parameter selection strategy to form a cryptographic suit with the same security strength.

3 Requirements for the Submission Packages

3.1 General Requirements

Submitter(s) may submit one or more algorithms. Each algorithm shall be submitted with an electronic package and a printed package as required. Submission packages are required to be in English and those prepared in Chinese are encouraged as additional materials. Incomplete packages will be considered as not meeting the submission requirements and will not be eligible for the subsequent evaluation.

(1) Electronic Submission Packages

Submitter(s) shall submit an electronic package in a zip file by e-mail. The package shall contain the following:

- Basic information (in a PDF file with signatures).
- Algorithm specifications (in a PDF file).
- Implementation codes (in a file folder labeled “Implementations”).

- Test vectors (in a file folder labeled “Test_Vectors”).
- Intellectual property statements (in a PDF file with signatures).

(2) Printed Submission Packages

Submitter(s) shall submit a printed package by mail. The package shall contain the following:

- Basic information (the original document with handwritten signatures).
- Intellectual property statements (the original documents with handwritten signatures).

3.2 Basic Information

The submission package shall include the following basic information of the algorithm (see Appendix A):

(1) The algorithm name.

(2) Each and every submitter’s name, affiliation, telephone, e-mail address, postal address, and handwritten signature.

(3) The contact’s name, affiliation, telephone, e-mail address, postal address, and handwritten signature.

3.3 Algorithm Specifications

The submission package shall include a complete written specification of the algorithm, which contains algorithm description, design rationale, security statements and analyses, performance evaluation, feature statements, etc.

3.3.1 Algorithm Description

The algorithm specifications shall provide a complete algorithm description, including algorithm operation processes, mathematical formulas, tables, diagrams, and parameters required for each algorithm instance.

3.3.2 Design Rationale

The algorithm specifications shall illustrate the main ideas and rationales of the design, including:

(1) The mathematical hard problem.

(2) The criterion for parameter selection.

(3) Detailed analysis of failure probability and its impact on security, if a certain

probability of failure exists in the algorithm.

(4) Other considerations.

3.3.3 Security Statements and Analyses

The algorithm specifications shall include security statements of the algorithm, and security analyses based on the following aspects:

(1) Theoretical security: Provide the security model along with the security proof. It is encouraged to provide security proof under the quantum computing model.

(2) Practical security: Provide the time complexity against the known classical and quantum attacks for each algorithm instance parameter.

(3) Other security properties: It is encouraged to provide other security analyses, such as security against side-channel attacks, (perfect) forward secrecy, security against multi-key attacks, security in the case of (temporary) key reuse, etc.

3.3.4 Performance Evaluation

(1) Performance Analyses

The algorithm specifications shall provide the performance analyses of the algorithm according to its design rationale, and give comparative results with the existing standard algorithms.

(2) Performance Test

The algorithm specifications shall provide performance test results of implementations (see Section 3.4 for requirements) for all algorithm instances on popular 64-bit PC processors, and comparative results with the existing standard algorithms. It is encouraged to provide test results on other software and hardware implementation platforms, such as 32-bit embedded systems. It should be noted that test results on hardware implementation platforms would be required in the subsequent evaluation rounds. The test results shall include:

a. Detailed Configuration of Implementation Platforms

- Implementation method: programming language, compiler, etc.
- Software implementation: processor model and clock rate, memory, operating system, instruction sets, crypto libraries, etc.
- (Optional) Hardware implementation: simulation tools, synthesis tools, technology libraries, etc.

b. Performance Test Results

- Software implementation efficiency: the computational efficiency of the key generation, signature, verification, encapsulation, decapsulation, establishing

a shared secret key, etc.

- (Optional) Hardware implementation efficiency: the computational efficiency of key generation, signature, verification, encapsulation, decapsulation, establishing a shared secret key, etc.
- Transmission and storage cost: the sizes of public keys, private keys, signatures, ciphertexts, exchanging messages, and the rounds of key exchange, etc.
- (Optional) Software resource consumption: memory cost, etc.
- (Optional) Hardware resource consumption: hardware implementation area, time delay, power consumption, energy consumption, throughput and throughput-area ratio, etc.

3.3.5 Feature Statements

The algorithm specifications shall clearly state the algorithm features, such as:

(1) Innovativeness.

(2) Simplicity.

(3) Flexibility.

(4) Compatibility.

(5) Extensibility.

(6) Performance advantages on multiple platforms.

3.4 Implementation Codes

The submission package shall include a reference implementation (with no platform-specific instruction), and an optimized implementation (on popular 64-bit PC processors). Implementations on other software and hardware platforms, such as 32-bit embedded systems, are encouraged. It should be noted that hardware implementation would be required in the subsequent evaluation rounds. Submission requirements for implementations are as follows:

(1) Implementations shall cover all instances of the algorithm.

(2) The reference and optimized implementations shall include automated build scripts for compiling source codes and generating executable files.

(3) The source codes of reference and optimized implementations shall be written in ISO C, and the programming interfaces provided by ICCS (see API_PKC.zip) shall be used. Appropriate comments shall be included to explain each function of the implementations.

(4) The cryptographic hash algorithm and eXtendable-Output Function (XOF) in the

implementations shall use the auxiliary functions provided by ICCS (see API_PKC.zip). These auxiliary functions are only used to verify the correctness of implementations and preliminarily evaluate performance, without considering security. In the subsequent evaluation rounds, these will be replaced with new auxiliary functions based on new cryptographic hash algorithms.

(5) The file folder of implementations shall have the following structure:

\Implementations
\Reference_Implementation
\Optimized_Implementation
\Additional_Implementation
\README

The "README" file shall list all files in the folder with a brief description of each file.

3.5 Test Vectors

The submission package shall include a set of Known Answer Test (KAT) vectors to verify the correctness of implementations. Submission requirements for test vectors are as follows:

(1) Test vectors shall cover all instances of the algorithm.

(2) Test vectors shall be generated using the program and input data provided by ICCS (see API_PKC.zip).

(3) The file folder of test vectors shall have the following structure:

\Test_Vectors
\KAT_SIG_AlgorithmInstance.txt
\KAT_KEM_AlgorithmInstance.txt
\KAT_KEX_AlgorithmInstance.txt

3.6 Intellectual Property Statements

The algorithm submitter(s) shall submit signed intellectual property statements as follows:

(1) Statement by each algorithm submitter (see Appendix B.1). This document shall be signed by each and every algorithm submitter, committing that the submitted algorithm and its implementations meet the security requirements, agreeing to provide the algorithm and its implementations to the public for evaluation, analyses and review, committing that all patents and patent applications which may cover the algorithm and its implementations are disclosed sufficiently and place no restriction on worldwide disclosure and free adoption if the submitted algorithm is selected for standardization.

(2) Statement by patent (and patent application) owner(s) (see Appendix B.2). This document shall be signed by each and every owner, or the owner's authorized representative, of each patent (and patent application) which may cover the algorithm and its implementations, agreeing to grant to any interested party, including the program organizer, public reviewers, etc., the right to freely use the patent (and patent application) for evaluation purpose, and committing to grant to any interested party, including standard drafter, standard organization department, standard users, etc., a public, irrevocable, nonexclusive, royalty-free license for using the patent (and patent application) without any conditions, if the algorithm is selected for standardization. Under equal conditions, the algorithms that are not covered by any patent (or patent application) or whose statements are signed by each and every owner of related patents (and patent application) will be preferred.

(3) Statement by reference and optimized implementations' owner(s) (see Appendix B.3). This document shall be signed by each and every owner or the owner's authorized representative, of the algorithm's reference and optimized implementations, agreeing that any interested party, including the program organizer, public reviewers, etc., can freely use such implementations for evaluation purpose, and committing to place no restriction on worldwide disclosure and free adoption if the submitted algorithm is selected for standardization.

Appendix A: Basic Algorithm Information (Sample)

Algorithm Name		
Submitter 1 *(Signature)* YYYY-MM-DD	Name	
	Affiliation	
	Telephone	
	E-mail	
	Postal Address	
Submitter 2 *(Signature)* YYYY-MM-DD	Name	
	Affiliation	
	Telephone	
	E-mail	
	Postal Address	
……		
Contact *(Signature)* YYYY-MM-DD	Name	
	Affiliation	
	Telephone	
	E-mail	
	Postal Address	

Appendix B: Intellectual Property Statements (Samples)

B.1 Statement by Each Algorithm Submitter

I, *(full name)*, *(full postal address)*, to the best of my knowledge of my submitted algorithm *(name of algorithm)* and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.

2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.

3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.

4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐*do*/☐*do not* adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.

5. *(Please check one of the following two options.)*

- ☐ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

☐ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☐*have submitted*/☐*have not submitted* all statements; as for patent(s) and patent application(s) held by others, I ☐*have submitted*/☐*have not submitted* all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
				☐*Yes* ☐*No*
				☐*Yes* ☐*No*

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed:

Date:

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.2 Statement by Patent (and Patent Application) Owner(s)

(Please check one of the following two options.)

☐ I, *(full name)*, *(full postal address)*, am the owner of the patent/patent application *(patent number/patent application number)*;

☐ I, *(full name)*, *(full postal address)*, am the authorized representative of the owner *(full name)* of the patent/patent application *(patent number/patent application number)*,

and do hereby agree to grant to any interested party, including the program organizer, public reviewers, etc., the right to freely use the above patent (and patent application) for evaluation purpose, and commit to grant to any interested party, including standard drafter, standard organization department, standard users, etc., a public, irrevocable, nonexclusive, royalty-free license for using the patent (and patent application) without any conditions, if the algorithm *(name of algorithm)* is selected for standardization.

Signed:

Date:

(Note: If there are multiple owners of the patent (and patent application), the statements shall be signed by each and every one of them or their authorized representatives. The authorized representative shall submit the letter of authorization.)

B.3 Statement by Reference and Optimized Implementations' Owner(s)

(Please check one of the following two options)

☐ I, *(full name)*, *(full postal address)*, am the owner of the submitted reference implementation and optimized implementations of the algorithm *(name of algorithm)*;

☐ I, *(full name)*, *(full postal address)*, am the authorized representative of the owner *(full name)* of the submitted reference implementation and optimized implementations of the algorithm *(name of algorithm)*,

and do hereby agree that any interested party, including the program organizer, public reviewers, etc., can freely use such implementations for evaluation purpose, and commit to place no restriction on worldwide disclosure and free adoption if the algorithm is selected for standardization.

Signed:

Date:

(Note: If there are multiple owners of the reference and optimized implementations, the statements shall be signed by each and every one of them or their authorized representatives. The authorized representative shall submit the letter of authorization.)