公钥密码算法提交要求

（征求意见稿）

商用密码标准研究院

2025 年 2 月

目　录

本文档给出新一代商用密码算法征集活动公钥密码算法提交的有关要求。

1 算法提交者须知

算法提交者将被视为知悉并同意以下内容：

（1）新一代商用密码算法征集活动将综合考虑算法安全性、算法性能、算法创新性等技术特点以及知识产权等可能影响算法推广应用的因素，经多轮评估，遴选出优胜算法开展标准化工作。

（2）提交的算法及其实现应为算法提交者的原创性成果，并在算法提交者所知范围内充分披露其可能涉及的专利和专利申请。

（3）提交的算法及其实现将被公开披露，以便于进行充分的社会公开评议。社会公开评议是算法评估工作的重要参考。

（4）提交的算法及其实现不得含有任何依据中国和其他国家法律法规应当保密，或侵犯第三方合法权益的数据、信息或技术。

（5）考虑算法创新、技术多样性发展和知识产权因素，新一代商用密码算法征集活动不接受已在国际相关组织、国家和地区中推进或完成标准化进程的算法及其未涉及核心修改的变种算法。

（6）商用密码标准研究院保留新一代商用密码算法征集活动的解释权。

2 算法技术要求

（1）算法应至少能够同时支持 128 比特、256 比特、512 比特 3 种经典安全强度等级，其量子安全强度分别不低于 80 比特、128 比特、256 比特；可选择支持 384 比特经典安全强度等级，其量子安全

强度不低于 192 比特。n 比特经典（量子）安全强度是指针对算法的已知经典（量子）计算攻击的时间复杂度不低于 2^n。算法应不包含易受量子计算攻击的组件。在上述要求基础上，算法应提供一定的安全冗余，以降低新型量子算法和密码分析技术可能带来的安全风险。

（2）算法应至少提供下列功能中的一种：数字签名、密钥封装、密钥交换。

- 数字签名方案应包含密钥生成算法、签名算法和验证算法，应支持长达 2^{63} 比特消息的数字签名，一组密钥应支持对至少 2^{64} 个不同消息进行签名和验证。
- 密钥封装机制应包含密钥生成算法、封装算法和解封装算法，共享秘密密钥长度应不低于相应经典安全强度等级的比特数。
- 密钥交换协议应包含通信双方的初始化算法、生成和交换消息算法，共享秘密密钥长度应不低于相应经典安全强度等级的比特数。

（3）算法应能够在广泛的软件与硬件平台上高效实现，具备实用性。

（4）鼓励支持数字签名、密钥封装、密钥交换等密码功能的算法，能够基于相同的数学困难问题和参数选择方案，形成安全强度相匹配的算法套件。

3 材料提交要求

3.1 材料总体要求

算法提交者可提交一个或多个算法，每个算法应按要求分别提交电子版和纸质版全套材料。算法提交者应提交英文材料，鼓励同时提交中文材料。材料提交不完整的，将被视为不满足要求，不能进入后续算法评估。

（1）电子版材料

算法提交者应通过电子邮件的方式提交电子版材料（zip 文件），电子版材料包括：

- 算法基本信息（签字扫描 PDF 文件）。
- 算法文本（PDF 文件）。
- 算法实现代码（Implementations 文件夹）。
- 算法测试向量（Test_Vectors 文件夹）。
- 知识产权声明（签字扫描 PDF 文件）。

（2）纸质版材料

算法提交者应通过邮寄的方式提交纸质版材料，纸质版材料包括：

- 算法基本信息（签字原件）。
- 知识产权声明（签字原件）。

3.2 算法基本信息

算法提交者应提供算法基本信息（样例详见附录 A），包括：

（1）算法名称。

（2）算法提交者的姓名、单位、电话、电子邮箱、邮政地址及其

签名。

（3）算法联系人的姓名、单位、电话、电子邮箱、邮政地址及其签名。

3.3 算法文本

算法提交者应提交完整的算法文本，包含算法描述、设计原理、安全性声明与分析、性能评估、特点声明等内容。

3.3.1 算法描述

算法提交者应对算法进行完整描述，包括涉及的运算过程、数学公式、图表、与各安全强度等级对应的算法参数集等。

3.3.2 设计原理

算法提交者应说明算法设计的主要思路和策略，包括：

（1）算法基于的数学困难问题。

（2）参数选择依据。

（3）详细的失败概率分析及其对算法安全性的影响（如果算法存在一定的失败概率）。

（4）其他考虑。

3.3.3 安全性声明与分析

算法提交者应给出算法的安全性声明，并从以下方面进行分析：

（1）理论安全性：应给出算法的安全模型，并证明算法的安全性。鼓励给出量子计算模型下的安全性证明。

（2）具体安全性：针对算法声明的各种安全强度，应分别给出每个参数集抵抗已知经典计算攻击和量子计算攻击的时间复杂度。

（3）其他安全特性：鼓励给出算法满足的其他安全特性分析，例如抗侧信道攻击安全性、（完美）前向安全性、抗多密钥攻击安全性、（临时）密钥重用情况下的安全性。

3.3.4 性能评估

（1）性能分析

算法提交者应从设计原理层面给出算法的性能分析，并给出与已有标准算法的对比分析结果。

（2）性能测试

算法提交者应提供各算法实例的实现代码在主流 64 位 PC 处理器上的性能测试结果（实现代码提交要求详见第 3.4 节），并给出与已有标准算法的对比分析结果。鼓励给出 32 位嵌入式系统等其他软件、硬件实现平台上的性能测试结果。注意，后续评估轮次将要求提供硬件实现性能测试结果。测试结果包括：

a. 实现平台的详细配置说明

- 实现方式：编程语言、编译器等信息。
- 软件实现：处理器型号及时钟频率、内存、操作系统、指令集、密码库等信息。
- 硬件实现（可选）：仿真工具、综合工具、工艺库等信息。

b. 性能测试结果

- 软件实现性能：密钥生成、签名、验证、封装、解封装、建立共享秘密密钥等运算效率。
- 硬件实现性能（可选）：密钥生成、签名、验证、封装、解

封装、建立共享秘密密钥等运算效率。

- 传输与存储开销：公钥、私钥、签名、密文、密钥交换消息等数据尺寸，以及密钥交换轮数等。
- 软件实现资源消耗（可选）：内存资源占用等。
- 硬件实现资源消耗（可选）：硬件实现面积、时延、功耗、能耗、吞吐量、吞面比等。

3.3.5 特点声明

算法提交者应对算法特点进行明确声明，可包括：

（1）算法的创新性。

（2）算法的简洁性。

（3）算法的灵活性。

（4）算法的兼容性。

（5）算法的可扩展性。

（6）算法在多平台上的实现性能优势。

3.4 算法实现代码

算法提交者应提供1套参考实现代码（不依赖特定平台指令集）、1套优化实现代码（适用于主流64位PC处理器）。鼓励提供32位嵌入式系统等其他软件、硬件平台上的实现代码。注意，后续评估轮次将要求提供硬件实现代码。实现代码的提交要求如下：

（1）实现代码应涵盖所有算法实例。

（2）参考实现代码、优化实现代码应包含自动化构建脚本，用于对实现代码进行编译并生成可执行文件。

（3）参考实现代码、优化实现代码应使用 ISO C 语言，使用商用密码标准研究院提供的编程接口（详见 API_PKC.zip 文件），并通过适当的注释说明实现代码的每个函数。

（4）实现代码中的密码杂凑算法、可扩展输出函数（XOF）应使用商用密码标准研究院提供的辅助函数（详见 API_PKC.zip 文件）。该辅助函数仅用于正确性验证和初步性能测试，不考虑安全性。在后续评估轮次中，辅助函数将被替换为满足安全性要求的密码杂凑算法、可扩展输出函数。

（5）实现代码文件结构如下：

\Implementations

\Reference_Implementation

\Optimized_Implementation

\Additional_Implementation

\README

其中，“README”给出文件目录及各文件简要描述。

3.5 算法测试向量

算法提交者应提供已知答案测试向量，以验证算法实现正确性。测试向量的提交要求如下：

（1）测试向量应涵盖所有算法实例。

（2）测试向量应使用商用密码标准研究院提供的程序和数据（详见 API_PKC.zip 文件）生成。

（3）测试向量文件结构如下：

\Test_Vectors

\KAT_SIG_AlgorithmInstance.txt

\KAT_KEM_AlgorithmInstance.txt

\KAT_KEX_AlgorithmInstance.txt

3.6 知识产权声明

算法提交者应提交以下经相关人员签署的知识产权声明文件：

（1）算法提交者声明（样文详见附录 B.1）。该文件由算法提交者签署，承诺提交的算法及其实现均符合安全性要求，同意公开算法及其实现并接受算法评估分析与算法公开评议，承诺充分披露算法及其实现可能涉及的知识产权，并承诺如果算法入选标准，将不对算法及其实现的全世界范围公开及免费使用进行任何限制。

（2）专利权人和专利申请人声明（样文详见附录 B.2）。该文件由算法及其实现所涉及的知识产权所有人或其授权代表签署，同意授权算法征集者、公开评议者等相关方以算法评估为目的免费使用专利和专利申请，并承诺如果算法入选标准，将授权标准起草者、标准管理部门以及标准使用者等相关方无附加条件的、公开的、不可撤销的、非排他的、免费的专利和专利申请使用权。在同等条件下，不涉及知识产权事项或涉及的各项知识产权事项均签署了该声明的算法将被优先考虑。

（3）参考实现和优化实现所有人声明（样文详见附录 B.3）。该文件由算法的参考实现和优化实现的所有人或其授权代表签署，同意授权算法征集者、公开评议者等相关方以算法评估为目的免费使用这些实现，并承诺如果算法入选标准，将不对这些实现的全世界范围公开及免费使用进行任何限制。

附录 A 算法基本信息样例

算法名称		
算法提交者 1 **（签名）** **年 月 日**	姓名	
	单位	
	电话	
	电子邮箱	
	邮政地址	
算法提交者 2 **（签名）** **年 月 日**	姓名	
	单位	
	电话	
	电子邮箱	
	邮政地址	
……		
算法联系人 **（签名）** **年 月 日**	姓名	
	单位	
	电话	
	电子邮箱	
	邮政地址	

附录 B 知识产权声明样文

B.1 算法提交者声明

本人，（全名），（邮政地址），依据对本人提交的（算法名）算法及其实现（包括参考实现和优化实现）的了解，在此郑重声明：

1. 本人承诺，本人提交的算法及其实现符合安全性要求，包括但不限于算法不包含任何人为设计的后门或缺陷，算法实现不包含任何恶意代码。本人承诺，在本人所知范围内，本人提交的算法及其实现不含有任何侵犯商业秘密，或依据中国和其他国家法律法规应当保密的数据、信息或技术。

2. 本人知悉并同意，本人提交的算法及其实现将被公开，并接受评估分析与公开评议，算法征集者、公开评议者等相关方均可以算法评估为目的免费使用算法及其实现。本人理解，算法征集者将在评估分析和综合考虑下选择若干算法进入下一轮评估或成为优胜算法，本人提交的算法不一定能入选下一轮评估或成为优胜算法。本人理解，提交的算法不会获得算法征集者的经济补偿或其他补偿。

3. 本人知悉并同意，为便于后续新一代商用密码算法标准化工作的开展，如果本人提交的算法被遴选为优胜算法，算法征集者有权出于安全性、可用性或其他考虑，对本人提交的算法及其实现进行修改。本人承诺，如果本人提交的算法被遴选为优胜算法并被标准化，将不对该算法及其实现的全世界范围公开及免费使用进行任何限制。

4. 本人提交的算法及其实现均为本人或本人团队的原创性成果。本人提交的算法实现代码□是/□否应用了需授权使用的第三方代码或代码库。除已明确标注、引用和致谢之外，算法提交材料中的全部观点、文字、图表及数据等均为本人或本人团队的原创性研究成果，不包含任何他人已经发表的研究成果。

5. （请选择以下两项情形中的一项）

□本人未持有且未打算持有与本人提交的算法及其实现相关的专利和专利申请，且在本人所知范围内没有任何专利和专利申请可能会覆盖到本人提交的算法及其实现；

□以下表格中的专利和专利申请可能会覆盖到本人提交的算法及其实现。对于本人持有的专利和专利申请，本人□是/□否提交了全部知识产权声明；对于非本人持有的专利和专利申请，本人□是/□否提交了全部专利权人和专利申请人的知识产权声明。

表　专利和专利申请表

序号	专利号/专利申请号	专利名称	专利权人/专利申请人名单	是否提交了每位专利权人/专利申请人的知识产权声明
				□是　□否
				□是　□否

注：由算法提交者根据实际情况填写。

本人郑重声明，在本人所知范围内，已经公开了与提交的算法及其实现相关的所有专利和专利申请。本人承诺，在本人所知范围内，提交的算法及其实现符合中国和其他国家法律法规，不侵犯任何第三方的合法权益。若存在侵权纠纷或其他违反法律法规的情况，本人承诺由算法提交者负责应对处理、消除影响并承担相应的法律责任。

本人完全意识到本声明的法律后果由本人承担。

签字：

年　月　日

（注意：如果算法提交者为多人，每位算法提交者均应分别签署该文件）

B.2 专利权人和专利申请人声明

（请选择以下两种情形中的一项）

□本人，（全名），（邮政地址），是专利/专利申请（专利号/专利申请号）的所有权人；

□本人，（全名），（邮政地址），是专利/专利申请（专利号/专利申请号）的所有权人（全名）的授权代表，

同意授权算法征集者、公开评议者等相关方以算法评估为目的免费使用上述专利，并承诺如果算法（算法名）入选标准，将授权标准起草者、标准管理部门以及标准使用者等相关方在该算法标准的生命周期中无附加条件的、公开的、不可撤销的、非排他的、免费的专利/专利申请使用权。

签字：

年　月　日

（注意：如果专利权人和专利申请人为多人，每位所有权人或其授权人均应分别签署该文件；授权人需提交授权委托书）

B.3 参考实现和优化实现所有人声明

（请选择以下两种情形中的一项）

□本人，（全名），（邮政地址），是算法（算法名）的参考实现和优化实现的所有人；

□本人，（全名），（邮政地址），是算法（算法名）的参考实现和优化实现的所有人（全名）的授权代表，

同意授权算法征集者、公开评议者等相关方以算法评估为目的免费使用这些实现，并承诺如果算法（算法名）入选标准，将不对这些实现的全世界范围公开及免费使用进行任何限制。

签字：

年 月 日

（注意：如果参考实现和优化实现所有人为多人，每位所有人或其授权人均应分别签署该文件；授权人需提交授权委托书）