

新一代商用密码算法征集活动情况

Introduction to Next-generation Commercial Cryptographic Algorithms Program (NGCC)



商用密码标准研究院

INSTITUTE OF COMMERCIAL CRYPTOGRAPHY STANDARDS

2026年3月 March, 2026

商用密码 Commerical Cryptography



根据《中华人民共和国密码法》《商用密码管理条例》等法律法规，**商用密码**是指采用特定变换的方法对不属于国家秘密的信息进行加密保护、安全认证的技术、产品和服务。

According to *Cryptography Law of the People's Republic of China* and *Regulation on the Administration of Commercial Cryptography*, **commercial cryptography** refers to technologies, products, and services utilized for encryption protection and security authentication on information that does not involve anything of State secrets and the like by using specific transformation methods.

现用商用密码算法体系 Current Commercial Cryptographic Algorithm System

密码算法 Cryptographic Algorithm	行标编号 Industry Standard Number	国标编号 National Standard Number	ISO/IEC标准编号 ISO/IEC International Standard Number
ZUC	GM/T 0001-2012	GB/T 33133-2016	ISO/IEC 18033-4/AMD1:2020
SM4	GM/T 0002-2012	GB/T 32907-2016	ISO/IEC 18033-3/AMD1:2021
SM2	GM/T 0003-2012	GB/T 32918-2016	数字签名算法 (Digital Signature) : ISO/IEC 14888-3:2018
SM3	GM/T 0004-2012	GB/T 32905-2016	ISO/IEC 10118-3:2018
SM9	GM/T 0044-2016	GB/T 38635-2020	数字签名算法 (Digital Signature) : ISO/IEC 14888-3:2018 标识加密算法 (Identity-based Encryption) : ISO/IEC 18033-5/AMD1:2021 密钥交换算法 (Key Exchange) : ISO/IEC 11770-3:2021

说明：以上算法按照成为行业标准时间先后进行排序。

Note: The above algorithms are listed in the order of being industry standards.

商用密码标准研究院 Institute of Commercial Cryptography Standards



商用密码标准研究院主要承担商用密码标准战略研究和标准体系实施，商用密码标准制修订，标准试验验证、测试评价、宣贯培训及其科研成果推广应用，标准资源库建设与标准信息服务，以及商用密码国家标准和行业标准秘书处等工作。地址：北京市丰台区南四环西路188号17区10号楼。

Institute of Commercial Cryptography Standards (ICCS) is mainly responsible for conducting research on commercial cryptography standardization strategies, implementing the system of commercial cryptography standards, developing and revising commercial cryptography standards, conducting validation, verification, testing, evaluation, publicity and training of commercial cryptography standards, promoting and applying related scientific achievements, establishing the commercial cryptography standard resource library, offering information services of commercial cryptography standards as well as acting as the Secretariat of national and industry commercial cryptography standards.

Address: Bldg 10, Area 17, No. 188, South 4th Ring Road West, Fengtai District, Beijing



新一代商用密码算法征集活动(NGCC)

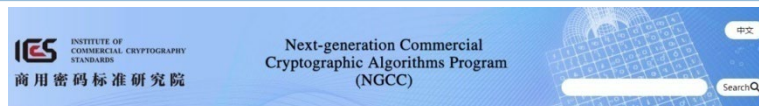
为了抵抗量子计算风险，同时满足大数据、物联网、云计算、人工智能等新技术新应用的发展需求，商用密码标准研究院计划征集**公钥密码算法**、**密码杂凑算法**和**分组密码算法**等3类算法，在前期国际密码研究工作取得的成果基础上做出新探索，希望进一步促进密码算法设计与分析技术发展创新，进一步丰富密码算法特别是抗量子计算密码算法的新颖性、多样性，进一步推动国际密码学术交流、繁荣密码学科发展，以期形成相互适配的新一代商用密码算法体系，推动新一代商用密码算法标准制定。

In response to the threat of quantum computing and to accommodate the evolving demands of emerging technologies such as big data, Internet of Things, cloud computing and artificial intelligence, ICCS 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 of the international 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 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.

新一代商用密码算法征集活动(NGCC)



新一代商用密码算法征集活动(NGCC)



首页 > 通知公告

关于开展新一代商用密码算法征集活动的公告

2025-02-05

字体: 大 中 小

为应对量子计算威胁,推动新一代商用密码算法标准制定,按照密码行业标准化技术委员会工作安排,我院将面向全球陆续开展新一代公钥密码算法、密码杂凑算法、分组密码算法征集活动,从安全性、性能、特点等方面组织评估,遴选出优胜算法开展标准化工作。欢迎各界积极参与算法提交与公开评议,鼓励在算法设计工作中加强国际合作。

征集活动安排具体事宜后续将在www.niccs.org.cn相继发布,敬请关注。

商用密码标准研究院

2025年2月5日

Home > Notice

Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)

2025-02-05

Font size: Big Middle Small

In response to the threat of quantum computing and to promote the standardization of the next-generation commercial cryptographic algorithms, the Institute of Commercial Cryptography Standards (ICCS) is launching a global program to call for proposals for next-generation public-key cryptographic algorithms (NGCC-PK), cryptographic hash algorithms (NGCC-CH) and block cipher algorithms (NGCC-BC), according to the arrangement of Chinese Cryptography Standardization Technical Committee. The candidate algorithms will be evaluated in terms of security, performance and other features, and the finalists will be considered for standardization. ICCS looks forward to global algorithm submissions and comments, and encourages international cooperations in algorithm design.

Further notifications of the program will be released on www.niccs.org.cn

Institute of Commercial Cryptography Standards, China

February 5, 2025

2025年2月5日, **发布算法征集活动公告**, 正式启动算法征集工作。

On February 5, 2025, ICCS released the announcement of launching NGCC on its official website (<https://www.niccs.org.cn>), marking the beginning of the program.



新一代商用密码算法征集活动(NGCC)

Next-generation Commercial Cryptographic Algorithms Program (NGCC)

中文

Search

Next-generation Commercial Cryptographic Algorithms Program (NGCC)

中文

Search

Home > Notice

Call for Comments on *Submission Requirements for Public-Key Cryptographic Algorithms (Draft)* and *Evaluation Criteria for Public-Key Cryptographic Algorithms (Draft)*

2025-02-05

Font size: Big Middle Small

According to the plan of the Next-generation Commercial Cryptographic Algorithms Program (NGCC), the Institute of Commercial Cryptography Standards (ICCS) calls for comments on *Submission Requirements for Public-Key Cryptographic Algorithms (Draft)* and *Evaluation Criteria for Public-Key Cryptographic Algorithms (Draft)*. ICCS will consider the received comments in the revisions of the two drafts. Comments must be submitted by March 15, 2025 and overdue comments will not be considered.

Comments should be sent via E-mail to plccomment@niccs.org.cn

Attachments:

- Submission Requirements for Public-Key Cryptographic Algorithms (Draft)*
- Evaluation Criteria for Public-Key Cryptographic Algorithms (Draft)*

Institute of Commercial Cryptography Standards, China
February 5, 2025

Home > Notice

Call for Comments on *Submission Requirements for Cryptographic Hash Algorithms (Draft)* and *Evaluation Criteria for Cryptographic Hash Algorithms (Draft)*

2025-02-05

Font size: Big Middle Small

According to the plan of the Next-generation Commercial Cryptographic Algorithms Program (NGCC), the Institute of Commercial Cryptography Standards (ICCS) calls for comments on *Submission Requirements for Cryptographic Hash Algorithms (Draft)* and *Evaluation Criteria for Cryptographic Hash Algorithms (Draft)*. ICCS will consider the received comments in the revisions of the two drafts. Comments must be submitted by March 15, 2025 and overdue comments will not be considered.

Comments should be sent via E-mail to crypthashcomment@niccs.org.cn

Attachments:

- Submission Requirements for Cryptographic Hash Algorithms (Draft)*
- Evaluation Criteria for Cryptographic Hash Algorithms (Draft)*

Institute of Commercial Cryptography Standards, China
February 5, 2025

同步，发布技术文件征求意见通知。

ICCS issued a global call for comments on submission requirements and evaluation criteria (draft) for public-key cryptographic algorithms and cryptographic hash algorithms.

新一代商用密码算法征集活动(NGCC)

The screenshot shows the website interface for the Next-generation Commercial Cryptographic Algorithms Program (NGCC). The header includes the ICS logo and the text 'Next-generation Commercial Cryptographic Algorithms Program (NGCC)'. Below the header, there is a navigation bar with 'Home > Notice'. The main content area features the title 'Call for Proposals for the Next-generation Public-Key Cryptographic Algorithms' and the date '2025-10-09'. The text of the notice is in English and details the call for proposals, submission requirements, and evaluation criteria. It mentions that the deadline for algorithm submission is 24:00 Beijing Time (UTC+8) on June 30, 2026. The footer contains contact information for the Institute of Commercial Cryptography Standards, China, dated October 9, 2025.

The screenshot shows the website interface for the Next-generation Commercial Cryptographic Algorithms Program (NGCC). The header includes the ICS logo and the text 'Next-generation Commercial Cryptographic Algorithms Program (NGCC)'. Below the header, there is a navigation bar with 'Home > Notice'. The main content area features the title 'Call for Proposals for the Next-generation Cryptographic Hash Algorithms' and the date '2025-10-09'. The text of the notice is in English and details the call for proposals, submission requirements, and evaluation criteria. It mentions that the deadline for algorithm submissions is 24:00 Beijing Time (UTC+8) on June 30, 2026. The footer contains contact information for the Institute of Commercial Cryptography Standards, China, dated October 9, 2025.

2025年10月9日，发布公钥和密码杂凑算法征集通知，正式接收算法提案。

On October 9, 2025, ICCS issued a notice soliciting proposals for public-key cryptographic algorithms and cryptographic hash algorithms. ICCS released the official version of the requirements and evaluation criteria for the two algorithms, along with feedback on related issues.



新一代商用密码算法征集活动：

开始提交公钥、杂凑算法提案！

Next-generation Commercial Cryptographic
Algorithms Program (NGCC):

Call for proposals!



新一代商用密码算法征集活动(NGCC)

注 意:

- ◆ 以上两个算法提交时间为**2025年10月9日至2026年6月30日**
其中, 2026年5月1日至6月30日仅可对已提交的算法提案进行更新, 不可提交新的算法提案
- ◆ 算法提案电子文件提交方式:
公钥密码算法提交邮箱: pkcsubmit@niccs.org.cn
密码杂凑算法提交邮箱: crypthashsubmit@niccs.org.cn
- ◆ 算法提案纸质文件递交地址:
商用密码标准研究院 (收件地址: 北京市丰台区南四环西路188号17区10号楼)

Attentions:

- The submission period for these two algorithms is **from October 9, 2025, to June 30, 2026.**
From May 1 to June 30, 2026, submitters could update the previously submitted proposals but **could not submit new proposals.**
- For electronic packages, please send to pkcsubmit@niccs.org.cn and crypthashsubmit@niccs.org.cn
- For printed packages, please mail to Institute of Commercial Cryptography Standards, Building 10, Area 17, No. 188 South 4th Ring Road West, Fengtai District, Beijing, P.R.China .
- Packages should be sent to ICCS in both electronic and printed forms **prior to the deadline.**

新一代商用密码算法征集活动(NGCC)

ICCS will conduct **initial examinations** and then announce the candidate algorithms for the first round of evaluations.

将按照算法提交要求开展**形式审查**，并统一公布进入第一轮评估的候选算法。

ICCS组建**算法征集专家组**，负责相关技术工作；算法遴选从算法**安全性、性能、特点**等方面进行综合评估，鼓励进行理论创新、结构创新。

ICCS established **expert groups** responsible for the technical work of NGCC; the candidate algorithms will be comprehensively evaluated in terms of **security, performance, features** and etc. Innovation in theories and structures is expected.

ICCS promotes active participation of social forces in **public review** of algorithms. ICCS will release mailing lists of public review.

鼓励社会力量积极参与算法**公开评议**，后续将发布公开评议的邮件列表。

鼓励在算法设计工作中加强**国际合作**。

ICCS encourages **international cooperations** in algorithm design.



新一代商用密码算法征集活动(NGCC)



算法征集相关技术问题和意见建议，请通过电子邮箱反馈：

For further inquiries, please contact us via emails:

公钥密码算法咨询邮箱(public-key algorithms): pkccomment@niccs.org.cn

密码杂凑算法咨询邮箱(hashing algorithms): crypthashcomment@niccs.org.cn

欢迎访问官方网站: [https:// www.niccs.org.cn](https://www.niccs.org.cn)



感谢关注！

Thank you for your attention!