设计研究与应用

国密算法应用研究综述

卢秋如
（江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心），江苏无锡 214073）

摘 要：密码是信息安全的核心。推进国密算法的广泛应用，提高国密算法的性能，对保障国家的信息网络安全意义巨大。首先从国密算法产生的背景、常见的国密算法分类及性能等方面进行了综述，然后剖析了我国国密算法的应用研究现状，最后对国密算法未来发展提出建议。旨在为了解国密算法的应用和未来研究提供参考。

关键词：国密算法；信息安全；应用研究；未来发展
中图分类号：TP309.2 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2023.01.033
本文著录格式：卢秋如.国密算法应用研究综述[J].软件,2023,44(01):123-125

National Secret Algorithms Application Research

LU Qiuru
(Jiangsu Electronic Information Product Quality Supervision and Inspection Research Institute (Jiangsu Information Security Evaluation Center), Wuxi Jiangsu 214073)

【Abstract】：Encryption technology is the core of information security. Popularizing the application of national secret algorithm and improving the performance of national secret algorithm is of great significance to maintaining China's information security. Firstly, this paper summarizes the background of state secret algorithms, the classification and performance of common state secret algorithms, then it analyzes the application and research status of national secret algorithm in China, finally, the existing problems and future development suggestions of the state secret algorithm are discussed. The purpose is to provide reference for understanding the application and future research of national secret algorithm.

【Key words】：national secret algorithm;information security;application research;future development

0 背景

当前，国内外网络安全形式严峻，密码算法作为网络安全的“命脉”，是保障我国战略资源与安全的基础。密码应用是信息安全领域的核心技术，目前在全世界大多数核心领域中都采用如 MD5、DES、RSA 等的全球通用密钥算法系统和相关规范。随着互联网技术的发展，部分算法不仅安全性差或者设计不规范，同时也达不到国家网络安全自主可控的目的。近年来，国家有关部门从国家安全的战略高度，提出要避免对国外技术产品过度依赖，增强国产系统的安全可控。基于上述背景，国家密码管理局逐步推出国产加密系列算法 [1]。

1 国密算法应用现状

1.1 国密算法介绍

国产密码算法在商业化应用领域已经具备完整的基础密码体系，如表 1 所示内容描述，包括 SM1、SM2 等多种类型的密码算法。这些算法均符合国家行业标准，其中 SM2、SM3、SM9 和 ZUC 密码算法经过 ISO/IEC 信息安全分技术委员会审核，成为国际标准，SM1、SM4、SM7、祖冲之密码（ZUC）是对称算法，SM2、SM9 是非对称算法，SM3 是哈希算法。SM1 算法是分组密码算法，分组长度为 128 位，密钥长度都为 128 比特，算法安全保密强度及相关软硬件实现性能与 AES 相当，算法不公开，仅以 IP 核的形式存在于芯片中，基于该算法已研发相关芯片、IC 卡、加密机等安全产品，广泛应用于电子政务等领域；验证表明，SM2 与通用的 ECDSA 算法相比，前者的安全性更高；SM3 与 SHA-256 安全性相当，但比 MD5、SHA-1、SHA-224 的安全性高，适用于商用密码中的数字签名和验证；SM4 算法主要用于无线局域网产品，分组长度为 128 比特，密钥长度为 128 比特，加解密算法结构相

作者简介：卢秋如（1990—），女，江苏徐州人，硕士研究生，工程师，从事信息安全测评方面的研究工作。

表 1 国产密码算法及应用

Tab.1 Domestic cryptographic algorithm and application

名称	类型	公开	应用	与国外算法比较
SM1	对称算法	否	电子政务、商务	与 AES 加密程度相当
SM2	公钥算法	是	签名、密码机	基于 ECC，签名和密钥生成速度强于 RSA，比 RSA2048 安全性高，已成为国际标准
SM3	杂凑算法	是	VPN、密码键盘	基于 SHA-256，安全性比 MD5 和 SHA-1 高，已成为国际标准
SM4	对称算法	是	VPN	无线局域网标准的分组数据算法，易于实现，成本低。增加了非线性变换，安全性高于 DES
SM7	对称算法	否	IC 卡	安全性高于 Mifare
SM9	公钥算法	是	云端数据加密	标识密码。同 3072 位密钥的 RSA 算法加密强度相当。已成为国际标准
ZUC	对称算法	是	图像加密	移动通信 4G 加密标准，硬件开销低于 AES

同；SM7 算法适用于非接触式 IC 卡，可应用于身份识别类、票务类及支付类产品，如工作证、展会门票、积分卡等；SM9 不需要申请数字证书，适用于互联网新兴应用的安全保障，如智能终端、物联网等方面，实现加密认证，使用方便，易于部署；祖冲之序列密码算法（ZUC）是我国自主研发的密码算法，运用于移动通信 4G 网络中的国际标准密码算法。目前这些算法已应用于国民经济的各个领域。

1.2 应用现状

近年来，我国国产密码从无到有、从弱转强，国产密码已广泛用于通信、金融、教育、社保、能源、国防安全等重要领域，在维护国家安全、保护群众利益中发挥了不可替代的作用。

在工业互联网领域，国产加密算法主要用于身份认证、访问控制等多个方面，其中包含通信协议、认证、电子签名等主要技术。为保障工业互联网数据安全，采用对称密码算法进行数据加密解密，如 SM1、SM4、SM7 和 ZUC 序列等，保证数据的安全；采用非对称加密算法实现电子签名，如 SM2 和 SM9 等算法，保证数据的不可否认性；通过 SM3 杂凑算法保证数据的完整性。工业互联网平台通过边缘终端、MES 系统等实现工业数据采集，实时性、稳定性需求比现场系统设备低，更利于密码技术的应用。国内企业已研发出国产加密芯片、密码机、VPN 和加密硬盘等多种搭载国产密码算法的产品，以及签名验签和电子签章等数据签名类产品，进一步拓展国密算法在工业互联网领域的应用 [2]。

在智能家居领域，国密算法主要用于身份认证和指令数据加密。智能家居采用互联网、线路设备及自动控制等技术与家居终端集成，这种通过网络传输控制指令的数据传输方式存在一定的安全隐患。数据安全才能保障智能家居系统安全，保护用户隐私。身份认证采用 SM3 算法，输出结果 256 比特，32 字节。数据交互使用对称密码算法实现，采用数据包一秘钥的方式进行传输，SM4 算法为公开的国产算法，SM1 算法原理尚不可知，为了确保密钥安全，在实际应用中，密钥均在通过国家检测认证的软硬件密码设备中生成和使用。SM4 为分组加密算法，秘钥长度、数据分组长度为 128 位（16 字节）[3]。智能家居设备多样，设计密码存放、云端指令交互、控制协议等方面，安全性不容忽视，推动国密算法在智能家居的全面应用，是应对智能家居安全威胁的首要措施。

随着国际形式的日益严峻及关键技术自主可控性要求的不断提高，核安全级系统的安全性更加重要，国密算法在设备可信认证、数据加密和通信数据加密等领域发挥的作用与日俱增。其中使用 SM2、SM3 算法进行数字签名，实现可信认证；数据加密使用 SM3 实现数据 HASH 特征值计算及校验；通信数据加密使用 SM4 算法实现安全级数据的密文传输 [4]。

固件是整个存储体系的稳定运行的关键，一旦未经授权用户侵入固件进行更改等非法操作，导致固件内部数据泄露，因此保证数据的存储安全，首要目标就是要确保固件导入、运行等操作的安全。固件导入使用 SM2 算法完成验签，验签公钥存放在主芯片内，验签私钥则由经认证授权的固件厂商保存。固件导入操作，必须先使用私钥签名，签名信息和固件一起导入，带有签名信息的固件下载到高速缓存 RAM 后，通过公共密钥进行 SM2 验签。只有使用有效私钥签名的固件才能通过签名验证，成功完成导入操作，没有签名信息或者固件中签名信息无效都无法通过验签而被丢弃。所以具有合法签名信息的密钥才能拥有固件导入权限，从根源上保证了操作的合法性 [5]。

2 面临的挑战

虽然国产密码算法已应用于多个领域，但是国产密码的应用仍然面临着诸多挑战 [6-9]。

（1）国密算法研究落后于国外，且搭载国密算法产品很少。1996 年开始，我国才逐步开展国密算法的应用研究，除了研究滞后，我国的商用密码检测机构较少，导致产品认证周期长，增加了企业成本，影响了产

品上市时间，产品的竞争力不足，导致大多数企业积极性不高，研发搭载国密算法的产品的意愿不强。

（2）信息系统不支持国内加密认证传输协议。目前系统主流架构多采用 B/S，采用国际 SSL/TLS 协议保证服务端和客户端的数据传输安全。虽然目前国内学者设计了各种基于国密算法的协议，但多数企业前期建设系统无法支持，改造难度大，导致国产加密传输算法推广困难。

（3）目前国产密码产品基本上代替了国外产品，但是大部分产品仍然采用了国际密码算法，在信息安全领域无法做到自主可控，搭载国产密码算法的产品少，达不到自主安全可控，从根源上保障国家信息安全的机制仍有欠缺。

（4）国产密码算法使用管理审查严格，制约国密算法的发展。我国通过《电子签名法》《商用密码管理条例》《商用密码产品使用管理规定》等法律法规和管理规定规范国产商用密码的使用。总体上国产密码审查相较于国外密码算法而言更加严格，且使用国产密码算法会受到严格监管，企业作为利益体，用脚投票现象明显，极大制约了国产密码的发展。

3 未来发展

伴随云计算技术、物联网、大数据分析与数据挖掘、人工智能等先进信息技术的快速发展，特别是“互联网 +”的推广，信息安全性成为现代信息技术生产和信息安全服务的基础要求，数据加密逐渐成为不可或缺的重要手段，密码应用领域将不断深入和拓展 [10]。

3.1 应用拓展

随着商用密码领域的不断发展，商用密码产业将会形成一条完整的、可控制的产业链和良好的生态系统，整个产业的综合能力将会得到极大地提高，从而形成一批商用密码领域的龙头企业，对中国商用加密产业产生重要的影响和促进作用。

3.2 性能提升

加大技术研发力度，在新型密码算法、量子密钥、生物密钥等方面突破一系列重要的技术难题；在可信计算、区块链等新技术研究，在云计算、大数据、密码管理等方面，生物密码管理技术与生物特征数据结合方面，在核心技术领域，如网络管理与应用技术、网络身份管理技术等方面都达到世界领先水平。

3.3 标准体系完善

加速发展若干基础共性技术、应用技术和技术标准，为我国关键技术应用提供强有力的支持。全面建设科学、先进的密码标准和检测制度，建立完善的密码评价规范与认证体制机制，推动国密算法、产品、服务的高质量发展。

3.4 确保政策落地

政府要加强宣传和监管，确保系列国产密码鼓励政策真正落地。当前，我国已经出台了一系列相关政策法规，通过简化流程、税收优惠等手段规范和推广国产密码应用。但是在实际应用中存在政策执行不力、监管不到位、细则规范不明晰等问题。因此，要积极制定可操作的细则，同时加强政策宣传，使国产密码政策真正落地。

4 结语

当今世界进入了一个新的、万物互联的新世纪，安全问题变得特别重要。目前，安全防范已经势在必然，而加密技术则是最可靠有效的手段。对于密码产品而言，核心技术就是算法和标准。因此要大力研发、推广、使用国产密码算法，使用更多嵌入国产密码算法的设备，推进密码算法和产品自主可控。从目前的密码研究技术来看，现有国密算法的安全性在一段时间内不会遭受任何攻击性危机，但随着密码学技术和量子计算机的发展，未来的国密算法将会面临更大的挑战，现有国密算法的改进、新的密码算法和抗量子密码学的研究将会成为国密算法新的研究热点。

参考文献

[1] 杨宪萍.聚焦聚合聚力 推进商密应用——对金融领域国产密码应用的几点思考[J].中国信息安全,2014(11):105-106.

[2] 苏彬庭,陈明志,许力,等.国密算法在工业互联网安全中的应用研究[J].信息技术与网络安全,2021,40(3):28-31.

[3] 侯宪锋,韩磊,王兴元,等.国密算法在智能家居数据安全应用研究[J].中国新通信,2021,23(20):49-51.

[4] 谌志强,刘明星,韩文兴,等.国密算法在核安全级DCS中的应用研究[J].自动化仪表,2021,42(S1):276-281.

[5] 冷峰,张明凯,延志伟,等.国密算法在资源公钥基础设施(RPKI)中的应用[J].计算机科学,2021,48(S2):678-681.

[6] 刘建兵,马旭艳,杨华,等.国密算法在主动安全网络架构中的应用[J].信息安全研究,2021,7(12):1121-1126.

[7] 刘亚强,李晓宇.利用基于身份的密码算法+短信验证码的移动安全支付方案[J].计算机科学,2020,47(1):293-301.

[8] 赵晗,王燕娜,李建峰.国产密码在城市轨道交通综合监控系统中的应用[J].城市轨道交通研究,2021,24(5):171-174+178.

[9] 黄恺彤,刘晔.国产密码算法在电网信息安全中的应用研究[J].信息安全与通信保密,2015(10):82-83.

[10] 付朋侠.推进国产密码算法应用 实现信息系统自主可控[J].科学家,2015,3(10):104-105.