国密算法应用研究综述

汪 宇 彭 静

（中铁成都科学技术研究院有限公司，四川 成都 611730）

摘要：随着信息技术的飞速进步，信息安全问题成为全球关注的焦点。国密算法，作为我国自主研发的密码技术体系，其应用研究对于维护国家信息安全具有不可估量的价值。本文全面综述了国密算法的研究现状及其在金融、政府、物联网等领域的应用情况，以期为国密算法的进一步推广和应用提供有力支持。

关键词： 国密算法；信息安全；国密应用

第一章 研究背景与意义

随着互联网技术的飞速发展，信息安全问题更加凸显出其紧迫性和重要性，信息安全已成为国家、企业和个人都必须严肃面对的重要问题。因此，研究和应用高效的安全算法对于保护信息安全至关重要。

国密算法，即国家商用密码算法，是我国自主研发的一套密码算法体系，包括SM2椭圆曲线公钥密码算法[1]、SM3哈希算法、SM4分组密码算法等，经过严格设计和测试，具有较高的安全性和效率。还有众多学者和工程师在算法的优化、实现和应用方面进行了深入研究，推动了国密算法的发展。例如，有研究者基于SM2国密算法对区块链设计进行了优化，提高了区块链的安全性和效率[2]。还有研究将国密算法应用于核安全级DCS中，为保障核设施的安全运行提供了有力支持[3]。在校园信息系统方面，也有研究探索了国密改造的路径，以提升校园信息系统的安全性[4]。同时，随着信息化进程的加速，国密算法在各个领域的应用也越来越广泛。其应用不仅涉及政府、军事等重要领域，还广泛应用于金融、通信、电力等关键行业，对于保障国家信息安全、促进信息化健康发展具有重要意义。

本文旨在综述国密算法的研究进展、应用现状。通过梳理和分析相关文献资料，总结国密算法在各个领域的应用情况。这不仅有助于更好地了解国密算法的研究现状和应用前景，还能为相关领域的研究和应用提供参考和借鉴。

第二章 国密算法概述

2.1 对称密码算法

对称密码算法加解密使用相同的密钥，加密速度较快但密钥管理困难，包括SM1、SM4、SM7、ZUC算法[5]。

SM1算法、SM4算法、SM7算法都是分组密码算法，分组长度和密钥长度均为128位。SM1算法尚未公开，所以其使用依赖于硬件加密卡，用户可通过调用设备提供的加解密接口来使用该算法。SM4算法作为一项标准与无线局域网规范一同公布，主要应用于无线局域网领域。SM7也尚未公开，被广泛应用于非接触式IC卡领域，例如门禁卡、参赛证等。

不同于上述的分组密码算法，ZUC算法是一种序列密码算法，也叫作流密码算法，其核心思想是将一个固定长度的密钥和一个初始向量（IV）通过一个复杂的算法生成一个密钥流，再将其和明文异或，就得到了密文。由于密钥流的生成过程非常复杂，使得密钥流具有很好的随机性和不确定性，从而保证了加密过程的安全性。ZUC算法是面向通信领域特别设计的算法，早已被纳入国际标准，用于移动通信等领域的数据加密和完整性保护。

2.2 非对称密码算法

非对称加密算法即公钥加密算法，使用一对不同但数学上相关的密钥：公钥和私钥来加解密数据，包括SM2[6]、SM9等。SM2算法依据椭圆曲线离散对数问题实现，其密钥长度为256比特[7]。该算法在加解密过程中需要使用到两个密钥，其中被公开的称为公钥，可用于加密数据，用户本人持有的为私钥，可完成对数据的解密处理。

SM9算法是标识密码算法，可使用手机号码或邮件地址等作为公钥，不需要申请数字证书，被广泛用于云存储安全、智能终端保护、物联网安全等各种新兴应用，用于实现身份认证、通道加密等功能。

2.3 哈希算法

哈希算法运用一系列复杂的数学运算，将任意长度的比特序列映射成固定长度的摘要。当输入数据有任何变化时，其输出会有显著变化。哈希算法在身份验证、数据完整性验证等领域得到广泛应用。SM3算法是一种哈希算法[8]，输出长度为256比特的杂凑值。利用这个杂凑值检测数据在传输过程中是否被篡改，从而确保数据的完整性。SM3算法的压缩函数较为复杂，因而其安全性要高于国际上常用的MD5和SHA算法。

第三章 国密算法应用现状分析

3.1 金融行业

在金融行业，随着信息技术的迅猛发展，数据安全与合规性已成为行业发展的重中之重。近年来，国密算法以其卓越的安全性能和符合国家标准的特点，在金融行业得到了广泛应用。金融领域国密应用推进领先。2014年，在《金融领域密码应用指导意见》中明确指示了各金融机构在接下来的5年内，将国家商用密码技术全面融入并应用于网上银行、移动支付、网络证券等关键金融服务领域。2018年，为了深化密码技术的应用与推动创新发展，中央又印发了《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》，该规划进一步要求了金融、政务等重点行业国密应用。2020年，人行在此基础上颁发《金融领域信息系统国产密码改造基线要求》和《金融领域国产密码改造评价指标体系》，细化金融业国密改造要求。随着《密码法》、信创、密评等产业指引落地，国密改造在各金融机构核心系统中有望持续深化。商密在银行和证券业已经开展广泛应用。

银行业作为金融领域的重要支柱，对交易安全和数据保密有着极高的要求。目前，国内多家银行已积极采用国密算法，涉及数据加密、身份认证及交易签名等多个环节。特别是在网银、手机银行及ATM机等渠道，国密算法的应用日益凸显其重要性。例如，宁夏银行在手机银行支付认证和智能账单系统中成功应用了国密算法，不仅提升了用户体验，还荣获了“数智平台创新案例”和“金融为民创新案例”两项荣誉，这充分展现了国密算法在银行业应用中的创新价值和实际意义。在电子支付方面，随着移动支付的普及和在线交易量的激增，交易数据的安全性成了公众关注的焦点。通过采用国密算法对支付信息进行加密和签名，可以确保支付过程的安全性和可信度，防止支付信息被窃取或篡改]。2016年，资义纯研究了符合中国央行PBOC3.0标准的金融IC芯片硬件加速电路设计。重点探讨了国密算法SM2和SM4在金融IC芯片中的应用，设计了优化的硬件架构和算法实现方案。研究通过硬件加速引擎的设计，显著提高了金融IC芯片的处理速度和安全性，对金融IC行业的发展具有重要意义。国密算法SM2是基于椭圆曲线的密码体制，目前广泛应用于金融、医疗等领域。2024年，沈荣耀等人提出了一种基于国密SM2算法的局部可验证聚合签名方案，利用聚合签名降低存储开销，提高了验证方验证效率。

3.2 政府领域

在当前的政府信息化建设中，国密算法已被广泛应用于密钥交换和身份认证等方面，以确保政务信息的机密性、完整性和真实性。例如，基于国密算法的电子政务系统能够实现安全的数据传输和存储，防止信息泄露和篡改。

基于国密算法的即时通信加密软件系统能够实现端到端的安全通信，确保通信内容的机密性和完整性。这种系统不仅适用于个人用户之间的通信，还可应用于企业、政府机构等组织内部的通信。

在身份认证方面，国密算法可以通过数字证书、智能卡等多种方式，对政府部门工作人员的身份进行有效验证。这种基于国密算法的身份认证机制，不仅可以防止非法用户冒充合法用户进行恶意攻击，还可以确保政府部门信息系统的访问控制权限得到精准管理。

在文件加密传输方面，国密算法同样展现出了其强大的功能。政府部门在日常工作中需要处理大量的敏感文件和机密数据，这些数据一旦泄露或被非法获取，将对国家的安全和利益造成严重损害。因此，利用国密算法对文件进行加密处理，可以确保文件在传输和存储过程中的安全性，即使文件被非法截获，也无法获取其中的明文内容。

3.3 企业领域

在企业领域，国密算法的应用已呈现出深入且广泛的趋势，特别是在大型企业、工业互联网安全以及跨境电商保障方面，其重要性日益凸显。

大型企业在信息安全防护方面，正积极采用国密算法。这些企业在内部网络、数据中心、云计算平台等关键领域，通过引入国密算法，有效加强了信息安全的防护能力。在工业互联网的广阔场景中，国产加密技术占据了身份验证、访问权限管理等关键环节的核心地位，这些技术涵盖了通信协议安全、身份认证机制、电子签名验证等多个技术层面。为筑牢工业互联网数据安全的防线，业界广泛运用了诸如 SM1、SM4、SM7 及 ZUC 等对称加密算法对敏感数据进行加密与解密处理，确保信息传输与存储的安全性。同时，针对数据签名的需求，采用 SM2、SM9 等非对称加密算法，增强了数据的抗抵赖性，确保交易与通信的不可篡改与可追溯。此外，SM3 哈希算法的应用则为数据的完整性验证提供了强有力的保障。工业互联网平台通过集成边缘计算设备、MES（制造执行系统）等先进技术，实现了工业数据的高效采集与处理，相较于现场设备系统，其对实时性与稳定性的要求有所放宽，这为密码技术的深度应用创造了更为有利的环境。国内企业紧跟时代步伐，已成功开发出包含国产加密芯片、密码设备、VPN 解决方案、加密存储硬盘在内的多种硬件产品，以及支持电子签名验证、电子签章等功能的软件服务，这些产品与服务均深度集成了国产加密算法，极大地推动了国密算法在工业互联网领域的广泛应用与普及。2018 年，魏珊珊等人进行了相关研究，该研究聚焦于国密算法和公钥基础设施（PKI）在工控系统中的应用，特别是在以 PLC 为中心的系统中的身份鉴别问题。文中探讨了国家商用密码算法和公钥基础设施（PKI）体系的结合现状，设计了工控系统的证书认证模型及 PKI 的部署方案，为提升身份鉴别的安全性启发了新思考。2021 年，苏彬庭等人聚焦于国密算法在工业互联网领域的实际运用情形及所遭遇的障碍，针对这些问题，他们提出了一种优化设计的轻量级身份验证协议。该协议仅需两次握手即可实现认证，有效契合了工业互联网对快速、安全认证机制的需求，为领域内的安全通信提供了新的解决方案。

在跨境电商领域，国密算法的应用同样不可忽视。例如，CFCA 云证通银企版提供的签名验签、加密解密等服务，就能够帮助企业实现业务系统与银行系统的安全对接，保障交易数据的安全性。这不仅有助于提升跨境电商企业的信誉度和市场竞争力，也为消费者打造了更加安全可靠、值得信赖的购物环境。

3.4 物联网行业

随着物联网技术的快速发展，智能家居、智慧城市等应用场景对数据安全提出了更高要求。在物联网的广阔天地中，国密算法以其独特的安全性能和高效性，成了设备间通信的守护者。物联网设备因其分布广泛、数量众多且常常处于无人值守的状态，对通信安全和数据安全提出了极高的要求。

设备认证是物联网安全的第一道防线。通过国密算法，实现网络接入设备的身份验证与授权机制，确保网络访问仅限于预先批准的设备，从而有效防止非法设备的入侵和攻击。这些过程中，国密算法的非对称加密技术发挥了关键作用，它利用公钥和私钥的配对关系，实现了设备身份的安全验证。

物联网设备间的通信数据往往包含大量敏感信息，如用户的个人隐私、设备的运行状态等。若这些数据被窃取或篡改，将带来严重的安全后果。国密算法的对称加密技术能够对通信数据进行高强度的加密处理，确保数据传输的机密性、完整性。

国密算法还为物联网设备的远程升级和维护提供了功能支持。在物联网设备的生命周期中，定期的软件升级和维护是必不可少的环节。然而，这些操作往往涉及设备的安全性和数据的完整性。国密算法通过提供安全的远程验证机制，确保只有经过授权的操作才能对设备进行升级和维护，从而有效防止了恶意攻击和非法操作。

智能家居的多元化特性，涵盖了密码存储、云端指令交互、控制协议等多个安全敏感环节，其安全性问题日益凸显。因此，加速国密算法在智能家居领域的全面部署，成了抵御潜在安全威胁的核心策略。2018 年，徐崇耀介绍了物联网面临的安全挑战，并提出了将国密算法（如 SM2/3/4）集成到安全芯片内部，以实现数据加解密、签名验签等安全功能。2022 年，李敏等人的研究关注于将 SM4 应用于无钥匙进入及启动系统（PEPS）和发动机管理系统（EMS）的安全认证中。该研究旨在缩短加解密时间，提高数传效率，并实现产品的国产化，降低成本。

第四章　展望

随着科技的不断进步和全球化的加速发展，信息安全问题将持续成为国际关注的焦点。国密算法作为我国自主研发的信息安全核心技术，在未来的信息化发展中将起到至关重要的作用。展望未来，国密算法的应用前景广阔。

参考文献

[1] 杨宏志，袁凌云，王舒．基于 SM2 国密算法优化的区块链设计 [J]. 计算机工程与设计 ,2021,42(3):622-627.

[2] 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.DOI:10.16086/j.cnki.issn1000-0380.2021030097.

[3] 唐文军，黄建波．校园信息系统国密改造路径探索 [J]. 中国教育网络，2023(2):78-79.

[4] 沈荣耀，马利民，王佳慧等．基于国密 SM2 算法的局部可验证聚合签名算法研究 [J]. 信息安全研究 ,2024,10(2):156-162.

[5] 于洋，张旭，郑思明，等．基于政务应用场景下的国密算法密码应用方案 [C]//2023 年网络安全优秀创新成果大赛论文集 .2023.

[6] 奚宇航，黄一平，苏检德，等．基于国密算法的即时通信加密软件系统的设计与实现 [J]. 计算机应用与软件，2020, 37(6):7.DOI:CNKI:SUN:JYRJ.0.2020-06-053.

[7] 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):4.

[8] 李敏，陈付龙，庞辉．基于国密算法 SM4 的车载 PEPS 和 EMS 安全认证方法研究 [J]. 南京信息工程大学学报（自然科学版），2022,14(5):543-550.