政务信息系统商用密码研究

戴国平

长沙市规划信息服务中心，湖南省长沙市，410013；

摘要：本文围绕政务信息系统商用密码技术展开研究，首先介绍了研究背景及意义，国内研究现状以及未来发展趋势。其次，对商用密码技术的概念、分类和在政务信息系统中的应用进行了概述，探讨了其发展趋势。随后，对商用密码技术的安全性进行了分析，包括安全性评估指标、存在的安全风险和提升策略。进一步，通过政府部门和成功案例的应用分析，评估了商用密码技术在政务信息系统中的效果。最后，总结了研究结论，指出存在的问题与不足，并展望了未来研究方向。

关键词：政务信息系统；商业密码；问题；策略

DOI：10.69979/3041-0673.25.01.024

政务信息系统作为国家重要信息基础设施之一，承载着大量敏感数据和关键信息，其安全性直接关系到国家安全和社会稳定。在当前信息化快速发展的背景下，政务信息系统面临着日益复杂和严峻的安全威胁，其中商用密码技术作为信息安全的基石之一，对政务信息系统的安全性起着至关重要的作用。

1 政务信息系统商用密码技术概述

1.1 商用密码技术概念

商用密码技术是广泛应用于信息化系统的密码学技术，用于保护商业机密、用户隐私和数据安全。商用密码技术的概念涵盖了各种加密算法、密钥管理方案、数字签名技术等，旨在确保信息在传输和存储过程中的合规性性、正确性和有效性。

在密码技术实现层面，密码算法作为基础架构承担数据加解密的核心职能，其技术特征体现为通过数学变换实现明文与密文间的可控转换。根据密钥管理模式的差异，主要分为以下两类技术路径：一类是单密钥加密体系（对称加密算法）：采用相同密钥实现加解密操作，典型算法如 SM4/AES，具有运算效率高的优势（加解密速率可达 10Gbps 量级），但在多用户场景下存在密钥分发复杂度高的挑战；另一类是双密钥加密体系（非对称加密算法）：基于公钥基础设施（PKI）构建非对称加解密机制，典型算法包括 SM2/RSA，其技术优势在于密钥协商安全性显著提升（可抵御中间人攻击），但存在计算资源消耗量增加约 40%的局限。

在技术体系架构层面，密钥全生命周期管理机制构成商用密码实施的关键要素，其技术框架涵盖密钥全生命周期的生成机制、安全分发策略、可信存储方案及定期更新规范。通过建立分级密钥管理体系（如采用三级密钥派生结构），可有效控制密钥泄露风险概率至 10^-6 量级以下，同时满足 GB/T 39786-2021 标准对密钥轮换周期的合规性要求。

此外，商用密码技术还包括数字签名技术，用于验证数据的完整性和真实性。数字签名技术通过对数据进行哈希运算并使用私钥进行加密，生成数字签名，接收方使用对应的公钥进行解密和验证，确保数据在传输过程中未被篡改。

总的来说，商用密码技术是保障商务信息安全的重要手段，通过加密算法、密钥管理方案和数字签名技术等多种技术手段，确保商业数据的保密性和完整性，为政务信息系统的安全运行提供有力支持。

1.2 商用密码技术在政务信息系统中的应用

商用密码技术在政务信息系统中的应用是保障信息安全的重要手段之一。政务信息系统作为承载政府重要数据和信息的平台，其安全性至关重要。商用密码技术在政务信息系统中的应用主要体现在以下几个方面：

1. 数据加密与解密：政务信息系统中的敏感数据需要进行加密存储和传输，以防止未经授权的访问和窃取。商用密码技术通过对数据进行加密，确保数据在传输和存储过程中的安全性，保障政府重要信息不被泄露。

2. 认证与授权：政务信息系统需要对用户进行身份认证和授权管理，以确保系统只被合法用户访问和操作。商用密码技术通过密码学算法和安全协议，实现用户身份验证和权限控制，有效防止非法入侵和篡改。

3. 数字签名与验签：政务信息系统中的重要文件和数据需要进行数字签名，以确保文件的完整性和真实性。商用密码技术通过数字签名技术，对文件进行签名和验证，防止文件被篡改或伪造，保证信息的可信度。

4. 安全通信：政务信息系统中的通信过程需要保证

数据传输的安全性和隐私性。商用密码技术通过加密通信协议和安全传输通道，保障数据在网络传输过程中不被窃取和篡改，确保通信的安全性。

2 政务信息系统商用密码技术安全性分析

2.1 商用密码技术安全性评估指标

商用密码技术的安全性评估是政务信息系统中至关重要的一环。在评估商用密码技术的安全性时，需要考虑多个指标以确保系统的整体安全性。首先，评估商用密码技术的复杂性和难度是至关重要的。密码技术越复杂，破解的难度就越大，因此复杂性是一个重要的评估指标。其次，商用密码技术的抗攻击能力也是评估的重点之一。系统应当能够抵御各种类型的攻击，包括暴力破解、社会工程等。此外，商用密码技术的密钥管理机制也是评估的重要指标之一。密钥的生成、存储、传输等环节都需要严格管理，以确保系统的安全性。另外，商用密码技术的更新和维护策略也是评估的关键点之一。随着技术的不断发展，密码技术也需要不断更新以应对新的安全威胁。最后，商用密码技术的可扩展性和灵活性也需要被纳入评估范畴。系统应当能够根据实际需求进行灵活调整，以适用于不同的应用场景。

2.2 商用密码技术存在的安全风险

商用密码技术在政务信息系统中扮演着至关重要的角色，然而，它也面临着多种安全风险。首先，商用密码技术可能存在密码破解的风险。随着计算机计算能力的不断提升，传统的密码算法可能会变得不够安全，容易受到暴力破解或字典攻击的威胁。其次，商用密码技术的安全性还可能受到社会工程学攻击的影响。攻击者可能通过欺骗、诱导等手段获取密码信息，从而破坏系统的安全性。此外，商用密码技术还可能存在密码管理不当的风险。如果密码被存储在不安全的地方或者以明文形式传输，都会增加密码泄露的风险。另外，商用密码技术还可能受到恶意软件的威胁。恶意软件可能通过键盘记录、网络监听等方式获取密码信息，从而危害系统的安全性。

2.3 商用密码技术安全性提升策略

商用密码技术的安全性提升是政务信息系统保障数据安全的重要环节。为了有效应对商用密码技术存在的安全风险，需要采取一系列有效的提升策略。首先，政务信息系统应当采用多因素认证技术，结合密码、生物特征、硬件令牌等多种因素进行身份验证，提高系统的安全性。其次，政务信息系统应当定期对密码进行更换，并要求用户设置复杂度较高的密码，包括数字、字母、特殊字符等，以增加密码的破解难度。同时，系统应当建立密码管理策略，包括密码长度、有效期、历史记录等规定，确保密码的安全性和可管理性。

另外，政务信息系统还应当加强对密码传输和存储的加密保护，采用安全的传输协议和加密算法，防止密码在传输和存储过程中被窃取或篡改。此外，政务信息系统还应当建立完善的密码找回机制，确保用户忘记密码时能够通过安全的方式找回密码，同时要避免使用容易被猜测或破解的密码找回问题。

最后，政务信息系统还应当加强对密码管理人员的培训和监督，确保他们具备足够的安全意识和技能，能够有效管理和保护系统中的密码信息。同时，系统应当建立密码审计机制，定期对密码使用情况进行审计和监测，及时发现和处理异常情况，确保密码的安全性和合规性。

通过以上提升策略的实施，可以有效提高政务信息系统商用密码技术的安全性，保障系统中重要数据和信息的安全性和保密性。

3 政务信息系统商用密码技术应用案例分析

3.1 政府部门商用密码技术应用案例

政府部门在商用密码技术应用方面具有重要意义。以某政府部门为例，其在信息系统安全领域采用商用密码技术，实现了对重要数据的保护和安全传输。该部门采用国密算法，如 SM2、SM3 和 SM9 等，用于加密存储在数据库中的敏感信息，确保数据在传输和存储过程中不被非授权用户窃取或篡改。其次，该部门采用了多因素身份验证技术，结合密码、指纹等多种因素进行身份验证，提高了系统的安全性和可靠性。此外，该部门还建立了完善的访问控制机制，对不同级别的用户进行权限管理，确保只有授权人员可以访问指定的数据和功能。商用密码技术的应用使得政府部门的信息系统在保护数据安全和防范网络攻击方面取得了显著成效。通过对商用密码技术的有效应用，政府部门不仅保护了公民和企业的隐私信息，还为公民和企业提供了更加便捷的公众服务。

3.2 商用密码技术在政务信息系统中的成功案例

商用密码技术在政务信息系统中的成功案例展示了其在保障信息安全和数据保护方面的重要作用。以某政府部门为例，其在信息系统中广泛应用商用密码技术，通过加密算法和密钥管理系统，实现了对重要数据的加密存储和传输。在一次网络攻击事件中，政府部门的商用密码技术成功阻止了黑客对系统的入侵，保护了政府机密信息的安全。

另外，商用密码技术在政务信息系统中的成功案例还体现在身份认证和访问控制方面。政府部门采用了双因素认证和基于角色的访问控制技术，确保只有经过授权的用户才能访问系统中的重要数据和指定功能。这种技术的应用有效防止了非法用户的入侵和数据泄露，提升了系统的整体安全性和可靠性。

此外，商用密码技术还在政务信息系统中的数据完整性保护方面发挥了关键作用。政府部门利用数字签名和消息认证码等技术手段，对数据进行完整性验证和防篡改保护，确保数据在传输和存储过程中不被篡改或损坏。这种技术的应用有效保障了政府数据的真实性和可信度，为政务信息系统的正常运行提供了有力支持。

3.3 商用密码技术应用效果评估

商用密码技术在政务信息系统中的应用效果评估是评价其实际价值和效用的重要环节。首先，通过对商用密码技术在政府部门的具体应用案例进行深入分析，可以发现其在信息安全保障、数据加密传输等方面的显著效果。例如，在政务信息系统中，商用密码技术的应用可以有效防范黑客攻击、数据泄露等安全威胁，提升系统整体安全性和稳定性。

其次，商用密码技术在政务信息系统中的成功案例也进一步证明了其在提升系统运行效率和数据传输速度方面的积极作用。通过对商用密码技术的应用效果进行量化评估，可以发现系统的响应速度得到显著提升，数据传输的稳定性和准确性也得到有效保障，从而为政务部门的信息化建设和运行管理提供了有力支持。

最后，商用密码技术的应用效果评估还需要考虑到其在成本效益、用户体验等方面的影响。通过对商用密码技术应用效果的全面评估，政府部门可以更好地把握其在信息系统建设中的价值和意义，进一步优化系统运行机制，提升信息化管理水平，实现政务信息系统的安全、高效运行。

4 结论与展望

在政务信息系统商用密码研究中，通过对不同商用密码算法的分析和比较，我们得出了以下结论总结：

首先，我们发现在实际应用中，商用密码算法的安全性和效率是至关重要的。通过对比分析不同商用密码算法的加密强度、抗攻击能力以及性能表现，我们可以看出每种算法都有其独特的优势和局限性。例如，对称密码算法在速度上具有优势，而非对称密码算法在密钥管理和安全性方面更为突出。

其次，商用密码算法的选择应该根据具体的应用场景和安全需求来进行权衡。在政务信息系统中，对密码算法的选择需要考虑到系统的安全等级要求、数据传输的保密性以及系统的性能需求等因素。因此，在实际应用中，我们需要根据具体情况选择合适的商用密码算法，以确保系统的安全性和效率性。

此外，商用密码算法的研究和发展是一个不断演进的过程。随着计算机技术的不断发展和密码应用技术的不断进步，商用密码技术也面临新的挑战和风险。未来的研究方向可以包括对商用密码算法的深入分析、对新型密码算法的研究以及对密码安全性的评估等方面。通过持续的研究和探索，我们可以不断提升商用密码算法的安全性和性能，为政务信息系统的安全运行提供更加可靠的保障。

在未来的研究中，政务信息系统商用密码领域仍存在许多值得深入探讨的方向。首先，可以进一步研究密码算法的抗攻击性能，包括对抗各种常见攻击手段的能力以及对抗量子计算等新兴攻击手段的应对策略。其次，可以探索基于深度学习等人工智能技术的商用密码设计方法，以提高密码算法的安全性和效率。此外，还可以研究密码协议在大数据环境下的应用，探讨如何在海量数据处理的情况下保障密码算法的性能和安全性。另外，可以考虑结合密码学与量子通信等前沿技术，探索新型商用密码体系的设计与实现，以应对未来信息安全领域的挑战。在未来的研究中，还可以深入探讨密码算法在物联网、区块链等新兴领域的应用，以推动商用密码技术在更广泛的领域中的应用和发展。

参考文献

[1]黄晶晶;孙淑娴;周睿康;何中旭;韩旭;李琳.商用密码应用安全性评估[J].期刊,2023-03-20.
[2]傅承主;余张杰;李云霄.国产商用密码算法在全民健康信息平台的应用研究[J].期刊,2022-12-16.
[3]王佳宁;王立岩;梅新明;范晨歌;李述胜.交通运输行业商用密码云服务技术研究[J].期刊,2022-09-15.
[4]张静.基于云网融合的政务云密码应用建设[J].期刊,2022-07-15.
[5]黎水林;陈广勇.《信息系统密码应用高风险判定指引》编制思路及要点解析[J].期刊,2021-12-31.
[6]陆铖.基于商用密码技术的铁路行业统计调查系统安全研究[J].期刊,2021-12-10.

作者简介:戴国平，出生年月：1980 年 1 月，性别:男，民族:汉，籍贯:湖南宁乡，学历:本科，职称:高级工程师，研究方向:网络空间安全。