# 基于服务器密码机数据加密保护的国密算法升级改造方案研究

杨金贵，赵雄英，赵美箱，杨盼盼，方志辉
（云南滇能智慧能源有限公司 云南 昆明 650228）

【摘要】在数据安全愈发被重视的背景下，国密算法凭借自主可控等优势在数据加密领域的应用日益广泛。本研究针对当前国密算法在服务器密码机应用中存在的性能瓶颈、安全强度不足及与新型计算架构适配性差等问题，提出有针对性的算法优化和系统升级方案。首先阐述国密算法及服务器密码机的工作原理与应用，并分析国密算法在服务器密码机中的应用现状；其次设计国密算法升级改造方案；最后通过应用案例验证方案的有效性，旨在提升服务器密码机的数据加密能力，增强数据安全性，为推动国密算法在数据加密领域的深入应用提供参考。

【关键词】服务器密码机；数据加密保护；国密算法；数据安全
【中图分类号】TP309.7 【文献标识码】A 【文章编号】1009-5624(2025)10-0035-03

## 0 引言

在当今数字化时代，数据安全已成为各领域关注焦点。随着信息技术的快速发展，数据面临着越来越多的安全威胁。服务器密码机作为数据加密保护的关键设备，在保障数据安全方面发挥着重要作用。国密算法作为我国自主研发的加密算法，具有自主可控等诸多优势。随着安全需求的不断提高和技术的持续发展，现有国密算法在服务器密码机中的应用需要进行升级改造，以应对新的安全挑战和应用需求。本文研究国密算法在服务器密码机中的优化升级方案，重点探讨算法性能提升、安全增强，以及与新型计算架构的适配性改进等关键技术问题，为推动国产密码技术的创新发展提供指导。

## 1 国密算法及服务器密码机概述

### 1.1 国密算法概念及特征

国密算法是指国家密码管理局认定的一系列国产密码算法，包括对称加密算法、非对称加密算法和哈希算法等[1]。国密算法具有自主可控性和良好的性能表现，但与国际成熟密码算法相比，其国际认可度相对较低。部分国密算法的实现还存在兼容性问题，需要进一步优化。

### 1.2 服务器密码机的工作原理与应用

服务器密码机是一种专门为服务器提供密码服务的设备，集成了多种密码算法和安全机制，用于保障服务器数据安全，其工作原理是基于密码学基本原理[2-3]。在加密操作中，其首先接收待加密数据和密钥，按照预设算法进行处理。在企业级应用中，服务器密码机用于保护企业内部服务器中的敏感数据；在云计算环境中，服务器密码机可防止云服务提供商的服务器数据被云租户非法获取或篡改；在网络通信中，服务器密码机可对通信数据进行加密。

作者简介：杨金贵(1982—)，男，云南临沧，本科，工程师，研究方向：新能源发电数字化、网络安全及信息化、人工智能。

## 2 国密算法在服务器密码机中的应用现状

### 2.1 服务器密码机对国密算法的支持情况

目前，许多服务器密码机已经能够支持国密算法，但不同厂家的服务器密码机对国密算法的支持程度存在差异。部分高端服务器密码机能全面支持国产商密(ShangMi，SM)，如 SM2、SM3、SM4 等，并能根据应用场景灵活切换算法。部分产品仅支持部分国密算法，或在算法实现上存在限制，例如，对国密算法的某些参数设置存在限制，影响国密算法的性能发挥。

### 2.2 国密算法在服务器密码机中的实现方案

国密算法在服务器密码机中的实现方案通常基于硬件和软件相结合的方式。在硬件方面，服务器密码机内部芯片或电路会优化国密算法以提高算法执行效率。在软件方面，通过编写专门的驱动程序和应用程序接口，使得服务器密码机能够方便地调用国密算法进行数据加密、解密、签名、验签等操作。部分服务器密码机还能通过固件升级方式更新国密算法的实现，以适应不断发展的安全需求[4]。

### 2.3 现有方案的优缺点分析

现有方案的优点在于能够快速将国密算法应用到服务器密码机中，为数据加密保护提供有效手段。通过硬件和软件相结合的方式，既能提高算法执行效率，又便于用户使用。然而，现有方案也存在缺点：不同厂家的实现方式差异可能导致国密算法在不同服务器密码机上的性能和安全性表现不一致；现有方案的在面对复杂网络环境和多样化应用需求时，可能缺乏足够的灵活性和适应性。

### 2.4 现有方案的性能评估

从性能评估的角度来看，现有方案能够满足基本的数据加密保护需求。在加密速度方面，对于中小规模的数据加密任务，现有国密算法实现方案能够在可接受时间内完成加密操作。在密钥管理方面，多数服务器密码机能够有效管理国密算法的密钥，降低密钥泄露风险[5]。然而，在大规模数据加密和高并发应用场景下，现有方案性能可能

受到影响，例如，加密速度下降、密钥管理复杂度增加等。

## 3　国密算法升级改造方案设计

### 3.1　改造方案的实施步骤

第一阶段：现状评估。对现有服务器密码机和应用系统进行全面调研和评估，包括服务器密码机的型号、配置、支持的国密算法版本，以及应用系统的架构、业务流程和数据安全需求等。通过评估明确现有系统的优势和不足，为后续改造提供依据。

第二阶段：方案设计与实施。根据现状评估结果，结合改造方案的设计原则，制定详细的改造方案，按照方案要求逐步实施硬件和软件的升级改造。

第三阶段：测试验收。对改造后的系统进行全面测试，包括功能测试、性能测试、安全测试。功能测试验证系统能否正常实现国密算法的加密、解密、签名、验证等功能；性能测试评估系统在加密和解密速度、吞吐量等方面的表现；安全测试检测系统抵御各类攻击的能力。

### 3.2　改造方案的详细设计

本次国密算法升级改造方案主要从硬件架构优化、软件系统升级和密钥管理体系完善 3 个维度进行设计，具体改进措施如下。

#### 3.2.1　硬件架构优化设计

（1）加密芯片升级。采用最新一代国产密码芯片，芯片采用 28 nm 制程工艺，集成专用算法加速引擎，使 SM4 加解密性能提升至 20 Gbit/s，较上一代提升 300%。同时增加抗侧信道攻击设计，通过随机噪声注入和功耗均衡技术有效抵御物理层攻击。

（2）协处理器架构。新增可编程密码协处理器模块，采用现场可编程门阵列（field-programmable gate array，FPGA）+ 专用集成电路（application-specific integrated circuit，ASIC）混合架构。FPGA 部分实现算法动态加载功能，支持通过固件升级方式灵活适配新算法；ASIC 部分固化高频使用的基础算法，确保运算效率。

#### 3.2.2　软件系统升级方案

（1）算法管理模块重构。首先，支持动态算法加载功能，实现不重启服务即可完成算法库热更新，大幅提升系统维护效率；其次，开发智能算法调度机制，根据业务类型自动选择最优算法，例如，针对大文件传输场景优先选用 SM4CTR 模式以提高处理效率；最后，实现混合运算支持功能，允许不同算法协同工作以满足复杂业务场景需求。

（2）软件性能优化。首先，引入单指令流多数据流指令集优化技术，针对 SM3 哈希算法专门实现 AVX-512 指令级并行计算，提升 5 倍吞吐量；其次，采用内存池化管理机制，通过预分配加解密缓冲区有效减少内存碎片产生；最后，实施异步输入/输出（input/output，IO）处理方案，基于 epoll 事件驱动模型重构 IO 处理流程，提升单节点并发处理能力，满足高并发场景下的性能需求。

#### 3.2.3　密钥管理体系增强

（1）分级密钥管理：建立严格的三级密钥保护机制。①系统级密钥采用 SM9 标识密码算法进行高强度保护，并存储在服务器密码机的专用硬件安全模块中，确保最高级别的安全性；②业务级密钥经 SM4 分组密码算法加密后采用分布式存储，兼顾安全性与业务访问效率；③会话密钥则基于 SM2 椭圆曲线公钥密码算法动态协商生成，并设置不超过 24 h 的严格生命周期，通过定期自动更新有效防范密钥泄露风险。

（2）密钥全生命周期管理：构建完整的闭环管理体系。第一，密钥生成环节集成符合《随机性检测规范》（GM/T 0005—2012）的真随机数发生器，确保密钥的不可预测性；第二，密钥分发采用基于 SM2 算法的三方安全协议，通过非对称加密保障传输过程的安全性；第三，密钥更新实施智能滚动策略，实现业务无感知的平滑轮换；第四，密钥销毁采用物理级擦除技术，通过多次覆写存储介质确保密钥信息完全不可恢复。

#### 3.2.4　安全增强措施

（1）抗量子计算改造：实施多层次防御策略。首先，预置基于格的 SM2 抗量子扩展算法，为后量子密码迁移奠定基础；其次，对关键业务数据采用“经典国密算法+后量子密码算法”双重加密机制，构建量子计算威胁下的双重保障；最后，部署量子随机数发生器作为系统随机源，确保密钥生成等关键环节的随机性达到量子安全级别。

（2）运行时防护：构建全方位的安全防护机制。首先，实施内存加密技术，确保敏感数据在内存处理过程中始终保持加密状态，有效防范内存转储攻击；其次，采用 SM3 算法对关键代码段进行完整性校验，通过实时验证代码完整性抵御恶意篡改；最后，部署基于机器学习的异常行为监测系统，通过分析加解密操作的行为特征，智能识别潜在的异常攻击行为。

### 3.3　改造方案的安全性与性能评估

#### 3.3.1　测试环境与条件

本次评估采用华为 Fusion Server 2288H V5 服务器作为硬件测试平台，使用江南科友 SJJ1509 服务器密码机作为密码设备进行改造前后对比测试，网络环境搭建了 100 Gbit/s 以太网测试专网，对比方案包括原国密算法实现（SM2-256/SM3/SM4-128）与改造后方案（SM2-384/SM9/SM4-256），分别进行性能与安全性测试，以确保测试环境的一致性及数据可比性。

#### 3.3.2　安全性评估

第一，网络攻击测试使用 Kali Linux 渗透测试工具集模拟分布式拒绝服务、结构化查询语言注入等常见网络攻击。

第二，侧信道分析采用专业差分功耗分析设备对密码机实施物理层攻击测试。

第三，通过量子计算模拟，基于 IBM Qiskit 量子计算

框架构建 Grover 算法攻击模型，模拟量子计算环境下的密码破解场景。

安全性测试评估结果如表 1 所示，改造后的系统在安全性方面明显优于原系统，能够有效抵御常见的网络攻击，并具备一定的抗量子计算攻击能力。这主要得益于新加密芯片、算法管理模块和密钥管理系统的引入。

表 1 安全性测试评估结果

| 项目 | 分布式阻断服务抗性 | 结构化查询语言注入拦截率/% | 侧信道攻击能力 |
|---|---|---|---|
| 原系统 | 50 万 QPS 时崩溃 | 92.5 | 可提取 32%密钥信息 |
| 改造后系统 | 200 万 QPS 稳定运行 | 99.8 | 未提取有效信息 |
| 提升幅度/% | 300 | 7.3 | 100 |

3.3.3 性能评估

第一，使用专业的 crypto-benchmark 工具对 SM2、SM3、SM4 等核心密码算法进行精确的性能测量。

第二，开展系统级功能测试，模拟政务云平台典型业务场景，包括电子证照签发、跨部门数据交换等实际应用场景，评估系统整体性能表现。

第三，采用 Locust 压力测试工具模拟 1 000 个并发用户的极端负载，检验系统在高并发条件下的稳定性和吞吐量。

性能测试评估结果如表 2 所示，改造后的系统性能显著提升，加密和解密速率大幅提高，吞吐量增加，资源占用率降低。在高并发场景下，服务器性能保持稳定，表明国密算法升级改造方案在性能提升方面效果显著。

表 2 性能测试评估结果

| 指标 | SM4 加密吞吐量/(Gbit/s) | SM2 签名速度/(次/s) | 系统延迟(P99)/ms | 最大并发连接数 | 中央处理器利用率(10 Gbit/s)/% |
|---|---|---|---|---|---|
| 原系统性能 | 5 | 1 250 | 68 | 12 000 | 85 |
| 改造后性能 | 18 | 4 800 | 22 | 45 000 | 62 |
| 提升(下降)幅度/% | 260 | 284 | 67.6 | 275 | -27 |

## 4 国密算法升级改造方案的应用案例分析

4.1 应用案例介绍

某大型金融机构拥有庞大的业务系统，包括网上银行、移动支付、理财平台等。随着业务的不断发展和安全需求的日益提高，该机构决定对现有服务器密码机进行国密算法升级改造，采用本研究提出的升级改造方案，对硬件和软件进行全面升级，并引入先进的密钥管理系统。

4.2 改造前后性能对比

改造前，该机构服务器密码机在高峰时段处理交易数据时，加密和解密速率较慢，导致交易响应时间较长，影响用户体验。同时，由于服务器密码机对国密算法的支持有限，在数字签名和密钥交换等业务场景中存在安全隐患。改造后，服务器密码机的加密和解密速率大幅提升，有效保障了业务数据的安全性。改造前后性能对比结果见表 3。

表 3 国密算法升级改造方案效果分析

| 项目 | 改造前 | 改造后 |
|---|---|---|
| 交易响应时间 | 约 2 000 ms | 降至 226 ms，缩短 88.70% |
| 吞吐量 | 100 次/s | 提升至 600 次/s，提升 5 倍 |
| 国密算法支持数量 | 3 种 | 支持全部 8 种国密标准算法 |
| 系统平均无故障运行时间 | 500 h | 提升至 1 200 h，增长 140% |
| 业务数据加密成功率 | 80% | 达到 99.8%，显著降低数据泄露风险 |

4.3 改造方案在实际应用中的效果分析

在实际应用中，改造后的服务器密码机能有效保障金融交易安全、降低安全风险。自改造完成以来，该机构未发生任何数据安全事故，客户对金融服务的满意度显著提升。同时，通过提高业务处理效率有效降低运营成本，为金融机构带来了良好的经济效益和社会效益。

## 5 结语

综上所述，通过对国密算法的概述、服务器密码机的工作原理与应用、国密算法在服务器密码机中的应用现状分析，设计了国密算法升级改造方案。应用案例分析验证了该方案能有效提升服务器密码机的数据加密能力、增强数据安全性。未来，相关行业从业者可探索新型加密技术和安全管理方法，为数据安全提供更可靠的保障。

## 【参考文献】

[1] 裴斐. 国密算法赋能的分布式加密存储系统及应用研究[J]. 网络安全和信息化，2025(3)：109-111.

[2] 张燕平，马晓凯，陈冠祯. 基于国密算法的 5G 移动通信网络远程终端控制系统设计[J]. 计算机测量与控制，2025，33(2)：95-102.

[3] 赵勇波. 政务应用系统密码应用方案探讨[J]. 广东通信技术，2023，43(6)：29-33.

[4] 谢振杰，刘奕明，罗友强，等. 国密算法 SM9 的计算性能改进方法[J]. 信息安全研究，2025，11(1)：5-11.

[5] 王明登，严迎建，郭朋飞，等. 基于 RISC-V 指令扩展方式的国密算法 SM2、SM3 和 SM4 的高效实现[J]. 电子学报，2024，52(8)：2850-2865.