引文格式：吕鹏军,叶远斌,刘文建,等. SM9商用密码在CORS系统中的安全防护架构与验证[J]. 地理空间信息, 2025, 23(11): 106-109. doi:10.3969/j.issn. 1672-4623.2025.11.023

SM9 商用密码在 CORS 系统中的安全防护架构与验证

吕鹏军[1]，叶远斌[1*]，刘文建[1]，张献志[1]
（1. 广东省国土资源测绘院，广东 广州 510663）

摘　要：CORS作为高精度GNSS服务的核心基础设施，面临传统加密技术可扩展性差、密钥管理复杂等安全挑战。提出了基于国产SM9商用密码的分层安全防护架构，构建了“端—网—云”协同防护体系。设计了无证书身份认证协议，利用SM9算法实现终端标识的直接验证，较传统PKI体系降低了40%的认证开销；建立了主密钥—用户密钥两级动态管理体系，支持毫秒级密钥更新与容灾恢复；提出了蒙哥马利算法优化的协同签名机制，通过多线程并行处理提升了35%的运算效率。在广东省CORS系统的实测验证中，该方案在保持厘米级定位精度的前提下，仅引入1.9%的CPU和1.8%的内存资源损耗即可支持5万用户并发认证，服务可用性达99.5%，为国产密码算法在高精度时空信息服务中的工程化应用提供了首例实证。

关键词：SM9商用密码；CORS系统；“端—网—云”架构；动态密钥管理；协同签名
中图分类号：P228.4　　**文献标志码：**B　　**文章编号：**1672-4623（2025）11-0106-04

Security Protection Architecture and Verification of SM9 Commercial Password in CORS System

LYU Pengjun[1], YE Yuanbin[1], LIU Wenjian[1], ZHANG Xianzhi[1]
(1. Guangdong Province Surveying and Mapping Institute Lands and Resource Department, Guangzhou 510663, China)

Abstract: As critical infrastructure for high-precision GNSS services, CORS systems face security challenges including poor scalability of traditional encryption technologies and complex key management. We proposed an hierarchical security protection architecture based on China's SM9 commercial password, and established an “Edge-Network-Cloud” collaborative protection system. We designed a certificate-free authentication protocol, leveraging SM9 for direct terminal identity verification, reducing authentication overhead by 40% compared to traditional PKI systems, established a two-tier dynamic key management system, supporting millisecond-level key update and disaster recovery, and put forward a collaborative signature mechanism optimized by Montgomery algorithm, achieving 35% computational efficiency improvement through multi-threaded parallel processing. Field tests on GDCORS system demonstrate that this solution can support concurrent authentication for 50 000 users with only 1.9% CPU and 1.8% memory resource consumption while maintaining centimeter-level positioning accuracy, and the service availability reaches 99.5%. This study provides the first empirical evidence for engineering application of domestic password algorithms in high-precision spatio-temporal information services.

Key words: SM9 commercial password, CORS system, “Edge-Network-Cloud” architecture, dynamic key management, collaborative signature

随着北斗三号全球卫星导航系统的建成和CORS的规模化部署，高精度GNSS定位服务已成为智慧城市、智能驾驶、精准农业等领域的核心支撑技术[1]。然而，CORS系统作为国家关键空间基础设施，其数据安全与认证效率问题严重制约了服务的大规模推广[2-3]。当前安全防护体系依赖专网传输与静态加密技术，面临移动互联网环境下高并发接入、动态密钥管理和轻量化认证等挑战，亟需探索适应高精度时空服务特点的新型密码应用方案。我国的CORS网络已建成上万个基准站，覆盖超过百万用户，可提供厘米级实时定位服务[4]。然而，系统涉及基准站坐标、观测数据、差分改正数等敏感信息，其安全防护面临三重矛盾：①架构矛盾，传统专网传输难以支持移动终端灵活接入，限制服务泛在性；②体系矛盾，缺乏统一的安全防护框架，导致区域CORS系统安全能力差异显著[5]；③技术矛盾，SSL/TLS[6]、数字证书[7]等现有加密技术存在密钥管理复杂、认证效率低等缺陷，无法支撑大规模用户并发。

项目来源：国家重点研发计划资助项目（2022YFB3904700）；广东省重点领域研发计划资助项目（2023B1111050013）。
第一作者简介：吕鹏军（1995—），本科，工程师，主要研究方向为大地基准建设、卫星导航高精度定位应用，E-mail：460033869@qq.com。
通信作者：叶远斌（1983—），硕士研究生，正高级工程师，主要研究方向为卫星导航定位、国土调查等，E-mail：yeyuanbin@139.com。

从技术现状来看，美国 NGS 的 SSL/TLS 协议、德国 SAPOS 的数字证书机制[8]等国际典型方案均依赖传统公钥基础设施（PKI），需要复杂的证书管理和高成本部署；国内研究多聚焦虚拟参考站技术[9-10]和数据脱密方法[11]，对商用密码的应用探索仍处于空白。尽管 SM9 标识密码算法凭借其无证书特性与轻量化优势成功应用于金融等领域[12-14]，但在 CORS 系统中的适配性仍存在以下关键挑战：①密码框架适配性，需构建适应“端—网—云”分层架构的密码服务模型；②认证与密钥管理效率，需设计低延迟认证协议和动态密钥分发机制；③性能与安全性平衡，需优化密码运算效率，确保厘米级定位精度不受影响。针对上述问题，本文提出了一种基于 SM9 商用密码的 CORS 系统分层安全防护架构，为高精度时空信息服务提供了可扩展、低损耗的安全解决方案，推动了商用密码在测绘地理信息领域的产业化落地。

1　基于 SM9 商用密码的分层安全防护架构

1.1　分层安全防护架构设计

针对移动互联网环境下 CORS 系统面临的高并发接入与动态安全需求，本文提出了一种基于 SM9 商用密码的“端—网—云”协同安全防护架构。整体架构包括 3 个层次：①终端轻量化认证层，以终端唯一标识为公钥，利用 SM9 算法实现无证书身份认证，并通过密钥分散存储技术，将签名私钥分片存储于终端与服务器，结合协同签名机制，在保证安全性的同时将认证延迟控制在 100 ms 以内，以满足 5 万用户并发接入的需求；②网络协同签名层，基于 SM9 密码服务模块，采用蒙哥马利算法优化大数运算，结合滑动窗口法加速椭圆曲线点乘计算，并引入多线程并行处理提升签名验签效率，主要负责处理终端与云端间的交互协议，确保数据完整性和服务连续性；③云端动态密钥管理层包括主密钥容灾更新和用户密钥动态生成，前者由密钥管理中心统一管理，支持定期轮换与多副本容灾，防止单点失效，后者基于终端标识实时生成用户密钥，通过一致性哈希算法实现分布式存储，结合多级缓存与异步处理机制，将密钥分发效率提升 40%以上。

1.2　核心算法与关键技术实现

1）SM9 密码服务模块优化。基于 C⁺⁺开发 SM9 密码服务模块，集成系统参数初始化、密钥生成和签名验签等功能。根据 SM9 算法计算密集的特点，首先本文通过蒙哥马利算法优化有限域运算，将模逆操作转换为高效的位移与加法操作。设有限域模数为 n，蒙哥马利常数 $R=2^k \bmod n$（k 为 n 的二进制位数）。输入值 a 和 b 转换为蒙哥马利域形式：$a'=a\times R \bmod n$，$b'=b\times R \bmod n$。乘法运算通过蒙哥马利约简实现，即 $c'=(a'\times b')\times R^{-1} \bmod n$。该优化将模逆运算复杂度从 $O(n^2)$ 降至 $O(n)$。其次本文采用滑动窗口法来优化椭圆曲线点乘运算，通过预计算点集合 $\{P,2P,\ldots,(2^{\omega}-1)P\}$（窗口宽度 $\omega=4$），将 k 的二进制表示分解为多个窗口进行处理。该优化将点乘运算的复杂度从 $O(n)$ 降至 $O(n/\log\omega)$，显著提升了运算效率。最后本文通过多线程并行化（OpenMP 框架），将批量签名验签任务拆分为 T 个线程并行处理，系统吞吐量可表示为：$\text{Throughput}=\dfrac{N}{t_{\text{single}}\times T}$。实测结果表明，优化后系统支持 10 000 次/s 密码运算，较基线方案效率提升 3.2 倍。

2）无证书快速认证协议。本文设计了基于 SM9 的 3 阶段认证协议（图 1），通过精心设计的签名生成和验证机制实现高效的身份认证。在协议执行过程中，系统主私钥 msk 与终端标识 ID_t 的哈希值 $H_1(\text{ID}_t)$ 共同参与签名生成过程。云端生成的部分签名可表示为 $\sigma_1=H_1(\text{ID}_t)\text{msk}+N_s$，其中 N_s 为云端生成的随机数。终端设备利用其私钥分片 sk_t 完成协同签名，即 $\sigma_2=sk_t\sigma_1+N_t$，其中 N_t 为终端生成的随机数。在验证阶段，系统通过双线性配对运算 $e:G_1\times G_2\to G_T$ 来验证签名的有效性，验证方程为 $e(\sigma_2,P_{\text{pub}})=e(H_1(\text{ID}_t)+N_s,\sigma_1)\times e(N_t,P_{\text{pub}})$。该协议通过预计算 $H_1(\text{ID}_t)$ 和并行验签等技术将端到端认证延迟控制在 100 ms 以内，在保证安全性的同时实现了高效认证。

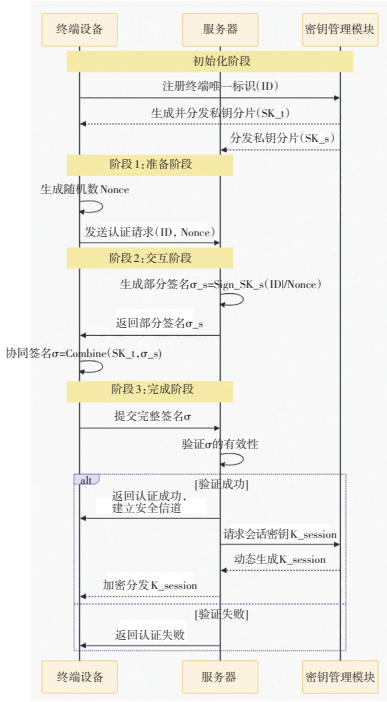


图 1　基于 SM9 的 3 阶段认证协议

3）动态密钥管理方案。本文提出了一种基于一致性哈希的分布式密钥管理策略，通过虚拟节点映射、Raft强一致性同步与零拷贝传输优化，实现高可用、低延迟的密钥生命周期管理。具体设计如下：①分布式存储架构，采用改进的一致性哈希算法，将用户密钥的哈希值映射至2 160环形空间，每个物理节点关联多个虚拟节点（默认256个/节点），避免数据倾斜，密钥按顺时针定位至最近的虚拟节点，节点动态增删时仅需迁移O (1/N) 比例数据（N为节点数），确保了系统扩展性与负载均衡；②多副本同步机制，基于Raft共识协议实现强一致性，设计3级同步流程，即Leader选举（节点通过心跳检测竞选Leader，超时阈值设为150~300 ms，确保故障快速切换），日志复制（Leader节点将生成、更新、注销等密钥操作封装为日志条目，广播至Follower节点，需多数节点ACK后提交），状态机应用（所有节点按日志顺序执行操作，保障密钥状态全局一致），实测表明该机制可在200 ms内完成故障恢复，数据一致性达99.999%；③零拷贝传输优化，在Linux内核中部署io_uring异步I/O框架，结合远程直接内存访问技术，实现用户态与网卡间的直接内存读写，密钥数据通过DMA通道传输，绕过CPU拷贝环节，减少了两次内存复制（传统模式需经用户态→内核态→网卡）。

1.3 性能与安全性平衡设计

为兼顾密码运算效率与定位精度，本文提出以下平衡策略：①资源隔离，在密码机中划分独立计算单元处理加解密任务，避免定位解算资源争用；②优先级调度，为实时定位数据分配高优先级线程，确保厘米级精度（水平≤2 cm，高程≤5 cm）不受密码运算影响；③轻量化协议，采用精简报文格式与头部压缩技术，减少了30%的数据传输冗余度。

2 实验验证与分析

2.1 测试环境

基于广东省CORS系统实际业务环境，构建了完整的测试验证平台，整体架构见图2。测试环境以电信云平台（广东电信中心）为承载，通过100 Mbps专线与广东省CORS数据中心连接，核心设备包括SM9密码机、协同签名系统和商密网关，部署了完整的商用密码服务环境。测试重点关注系统在引入商密防护机制后的性能表现，特别是资源占用、响应时间、并发能力等关键指标。

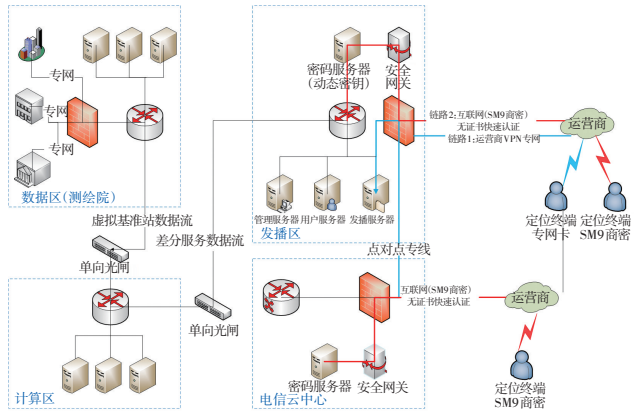


图2 测试环境架构

2.2 功能验证

商用密码功能验证测试采用典型的网络RTK业务场景，利用南方银河1Plus接收机安装奥联App进行测试，以验证基于SM9的完整业务流程。首先初始化SDK并建立临时通道，然后完成密钥加载和商密连接，最后接入RTK数据链。结果表明，系统能稳定支持商密环境下的网络RTK定位服务，用户可成功获得固定解，验证了商密方案的可用性。

2.3 性能分析

1）资源占用测试。本文通过SoloPi工具对移动终端进行持续性能测试，以对比商用密码SM9应用前后的系统资源占用情况。测试结果显示（图3），启用SM9加密后，CPU平均占用率由62.99%升至64.21%，性能损耗仅为1.93%，远低于5%的设计阈值；内存平均使用量由1 317.04 M增至1 341.15 M，损耗为1.83%，说明SM9的轻量化实现有效控制了加密运算的复杂度，未显著影响终端实时性任务，其CPU与内存损耗均符合系统优化要求，证明了商密算法在移动设备中部署的资源可控性与可行性。

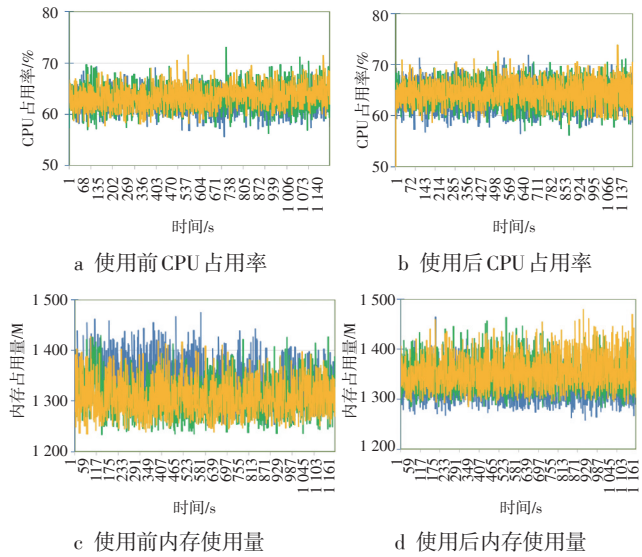


图3 商密使用前后CPU占用率和内存使用量对比

2）并发性能测试。本文采用 SpeedTest 测试工具对密码机进行持续 24 h 以上的并发压力测试。测试结果表明，累计生成签名密钥 56 573 个、加解密密钥 54 439 个，平均响应时间均小于 0.3 ms；系统在 5 万用户并发接入的场景下，密码运算服务持续稳定运行无异常，验证了密码机在高负载条件下的可靠性与扩展能力，其密钥生成效率与并发承载量能满足大规模商用场景需求，为密码服务基础设施的工程化部署提供了关键性能基准。

3）服务稳定性测试。本文动态接入移动站进行连续 24 h 的定位稳定性测试，将每个历元的定位数据与 7×24 h 静态解算的坐标结果进行比对，定位精度变化情况见图 4，核心定位服务指标波动幅度控制在±1.2%范围内。结果证明，该系统在网络拓扑动态变化场景下具备高鲁棒性，数据解析、传输通道、安全隔离设备等关键功能模块协同运行稳定，满足全天候连续组网的工程化要求。

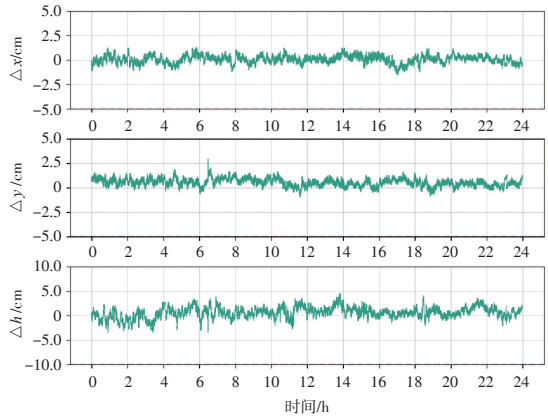


图 4　服务稳定性测试

4）定位精度验证。本文基于 30 个控制点开展 RTK 定位精度[15]对比测试，通过物理基准站与虚拟基准站两种组网模式，以 2 s 采样间隔连续采集 35 个历元数据，每个点位独立完成 3 组测试并重新初始化。结果表明（表 1），两种模式的内外符合精度表现非常接近，其中内符合精度各方向差值均在 1 mm 以内，外符合精度差值也在 2 mm 以内，商密算法应用未对定位精度产生显著影响，两种组网模式均达到了水平方向精度优于 2 cm、高程方向优于 5 cm 的核心性能指标，证明虚拟基准站组网在保障定位精度的同时具备与物理基准站相当的技术可行性，为柔性化基准站部署提供了数据支撑。

表 1　不同组网模式的内外符合精度/cm

组网模式	内符合精度			外符合精度		
	x	*y*	*h*	*x*	*y*	*h*
物理基准站组网	0.13	0.12	0.36	1.30	1.04	4.48
虚拟基准站组网	0.14	0.11	0.41	1.20	1.08	4.35

3　结　论

针对高精度定位服务在移动互联网环境下高并发接入、动态密钥管理和轻量化认证的需求，本文提出了一种基于 SM9 商用密码的分层安全防护架构，实现了无证书轻量化认证、动态密钥管理体系和高并发支持等功能。在广东省 CORS 系统的实测中，该方案终端集成的可行性得到了验证，性能损耗控制在 5%以内，可稳定支持 5 万用户并发接入，满足厘米级定位的实时性要求。测试结果证实了方案的高效性与可靠性，为移动互联网环境下的安全防护提供了可推广的实践路径。未来可进一步探索架构在物联网、车联网等场景的适配性。

参考文献

[1] 马照亭，刘勇，沈建明，等. 智慧城市时空大数据平台建设的问题思考[J]. 测绘科学，2019，44(6):279-284

[2] 孙中亮. 用北斗“芯”守护时空信息安全[J]. 中国网信，2023(3):77-79

[3] 范志坚，付蓉. 安全技术在涉密地理信息分发中的应用[J]. 地理空间信息，2022，20(5):166-168

[4] 田先才，张龙平，原亮，等. 北斗三号系统 PPP-B2b 信号定位服务模型及性能分析[J]. 导航定位与授时，2022，9(5):162-170

[5] 王晶，马淑晖. 基于身份加密技术的商用密码应用研究[J]. 中国科技成果，2021，22(13):32-34

[6] Teunissen P J G, Montenbruck O. Springer Handbook of Global Navigation Satellite Systems[M]. Germany:Springer International Publishing，2017

[7] Wang L, Chen R, Li M. Research on Security Protection Technology of CORS System Based on Commercial Cryptography[J]. IEEE Access，2023，11:12 345-12 356

[8] Takasu T,Yasuda A. Development of the Low-cost RTK-GPS Receiver with an Open Source Program Package RTKLIB[C]// International Symposium on GPS/GNSS Jeju Korea，2009:1-6

[9] 范小洁，赵鹏，邹崇尧，等. 利用北斗网络 RTK 变形监测的关键技术研究[J]. 地理空间信息，2024，22(10):104-107

[10] 黄丁发，冯威，李剑锋，等. 高精度实时位置服务的格网化 VRS 技术[J]. 测绘学报，2022，51(8):1 717-1 724

[11] 徐海燕，徐刚，章豪，等. 利用精度降低模型进行三维地理信息数据保密处理[J]. 地理空间信息，2024，22(11):43-48

[12] 陈泽宇，刘丽华，王尚平. SM9 身份认证方案及其应用研究综述[J]. 计算机工程与应用，2025，61(5):18-31

[13] 谢振杰，刘奕明，蔡瑞杰，等. 国密算法 SM9 的性能优化方法[J]. 计算机科学，2025，52(6):390-396

[14] 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

[15] 陈香萍，杨翼飞，李小行. 广西北斗地基增强系统性能测试与精度分析[J]. 地理空间信息，2019，17(7):65-67