 DOI: https://doi.org/10.12349/iser.v6i5.5685

The Application of SM9 Algorithm in Data Security Reporting of Smart Grid

Wenxia Yin

Waitlife (Shanghai) Enterprise Development Co., Ltd., Shanghai, 201601, China

Abstract

The large-scale deployment of smart grids and the deep integration of the energy Internet have put forward higher requirements for the secure data reporting of massive terminal devices. This paper aims at the pain points such as complex key management and high computational overhead of traditional Public Key Infrastructure (PKI) in resource-constrained scenarios such as smart meters and sensors, and proposes a data security reporting scheme based on the SM9 identifier cryptography algorithm. By using the unique device identification (such as the IMEI code) as the public key, combined with the lightweight SM9-Light algorithm and hybrid encryption technology, "certificateless" identity authentication and end-to-end data protection are achieved.

Keywords

sm9 identification password algorithm; Unlicensed documentation; smart grid

SM9 算法在智能电网数据安全上报中的应用

殷文霞

等保（上海）企业发展有限公司，中国 · 上海 201601

摘　要

智能电网的规模化部署与能源互联网的深度融合，对海量终端设备的数据安全上报提出了更高要求。本文针对传统公钥基础设施（PKI）在智能电表、传感器等资源受限场景下的密钥管理复杂、计算开销大等痛点，提出基于SM9标识密码算法的数据安全上报方案。通过将设备唯一标识（如IMEI码）作为公钥，结合轻量化SM9-Light算法与混合加密技术，实现“无证书化”身份认证与端到端数据保护。

关键词

sm9标识密码算法；无证书化；智能电网

1 引言

随着全球能源数字化转型加速，智能电网规模性挑战日益凸显，国际能源署（IEA）2025 年数据显示，全球智能电表数量突破 20 亿台，日均产生数据量超 500TB，亟需高效的数据加密与传输方案；其实时性要求也更加严苛，电网故障检测与负荷调度需毫秒级响应，传统非对称加密算法（如 RSA）因计算延迟高难以适配；在《电力行业密码应用行动计划》明确要求 2025 年前实现国密算法全覆盖的背景下，研究基于 sm9 算法实现智能电网数据安全上报机制具有重要意义。

2 智能电网数据安全上报面临的技术瓶颈

2.1 PKI 体系下成本高效率低

在传统 PKI 体系中，每个智能电表需独立维护数字证书，单省份超 1000 万张证书的生成、更新、吊销流程复杂，导致年运维成本超 3000 万元。证书需定期更新（通常 1~3 年），电表设备分散部署，手动操作不可行，自动化管理需投入高额 CA 服务器与运维人力；单张 X.509 证书大小约 1KB，千万级证书占用 10GB 存储空间，边缘网关需额外处理证书链验证（平均耗时 15ms/ 次）导致证书的存储与传输开销极大；另外，传统 CRL（证书吊销列表）更新周期长（≥ 24 小时），无法实时应对设备私钥泄露风险。

2.2 低功耗设备密码适配困难

在智能电网中，终端设备（如数据采集器、传感器节点）通常采用 超低功耗设计，硬件资源极度受限，导致计算能力低下，如 CPU 频率≤ 50MHz，主流公钥算法（如 RSA-2048）签名耗时高达 420ms，而智能电网的实时性要求通常≤ 10ms；其内存资源匮乏，RAM 容量≤ 64KB，而国密 SM2 算法签名过程涉及椭圆曲线点乘，需多次有限域运算，临时变量占用内存激增，一般签名需占用 32KB 临时内存（包括栈空间和动态分配），极易因内存溢出导致设备崩溃；能

【作者简介】殷文霞（1979–），女，中国江苏人，硕士，工程师，从事信息安全研究。

耗限制严格，设备需依靠电池供电运行数年，传统密码算法的高计算复杂度会大幅缩短续航时间。

2.3 多方协同的身份认证缺失

分布式光伏电站使用自建 CA 签发设备（逆变器、传感器）证书，而电网调度中心仅信任国家电网根 CA，无法直接验证电站设备合法性，恶意电站可能伪造证书接入电网，引发虚假数据注入攻击；不同区域运营商（如国网、南网、地方电网）采用独立的 PKI 体系，证书格式、策略互不兼容。跨区数据传输需多次证书转换与链式验证，时延增加 50% 以上；智能电表与配电主站间通常采用单向认证（仅主站验证电表），电表无法确认主站身份。部分老旧设备仍使用默认密码（如 admin/123456），易遭重放攻击（Replay Attack）。

3 基于 sm9 算法的系统架构及流程

3.1 总体架构

基于标识密码算法 sm9，建设的数据安全上报系统设有终端层、边缘层、云平台层、应用层。

终端层考虑老旧设备无法集成 SM9 芯片，可通过外挂支持 GM/T 0044 安全模块 , 预烧录设备唯一标识（如 IMEI/MAC) 作为 SM9 身份公钥，私钥由安全模块保护，以 SPI 接口与原设备通信，终端数据上报采用间歇性签名（如每小时全签 + 分钟级差分签）形式，用 SM9 私钥签名，将数据及签名发送至边缘层。

边缘层集群部署国密安全网关及智能边缘服务器（内置 SM2/SM3/SM4 加速指令集），接收终端层数据后，先验证 SM9 签名以防篡改；采用 SM9-KA 协商会话密钥，对数据包进行 SM4-GCM 加密，附加 16 字节 GMAC 标签，如此聚合多设备数据，生成统一密文批次上传。

云平台层实现集中化密钥管理与策略控制，由国家电网根 KGC 生成主公钥 MPK，其对应的主私钥 MSK 严格离线存储，仅用于派生区域子 KGC 密钥。根 KGC 通过专用光纤或量子密钥分发技术将 MPK 下发至所有区域子 KGC，分发时附加 SM2withSM3 签名防止 MPK 篡改。区域子 KGC 生成用户私钥，并对所有私钥生成记录审计并上链（基于 sm3hash）。

应用层可以包括负荷预测系统、故障诊断平台、电费结算引擎、移动运维 app 等。其中核心业务系统如负荷预测部署在电网私有云，非敏感模块如移动 app 后端使用公有云弹性扩容，通过国密 VPN 与私有云链接，所有内部 API 调研强制使用国密 SSL，移动端与后端采用 SM2 双向认证及 SM4-GCM 加密会话。

3.2 数据上报流程

电网终端设备以智能电表为例，其数据上报流程分为设备注册、数据采集、加密传输、云端处理四个步骤。

设备注册时，电表需要携带设备 ID 如“METER_34010 10001”向区域子 KGC 请求注册，区域子 KGC 向安全策略引擎申请校验设备合法性，安全策略引擎一般以白名单或工单比对形式返回是否允许注册。区域子 KGC 得到允许后，利用 SM9 算法模块，基于主私钥 MKGC 和电表标识生成电表私钥 D_meter=s*H1（ID）[1]，离线或通过国密 SSL 加密方式将私钥 ID 返回给电表，电表通过安全芯片存储私钥。

数据采集时，电表采集电压、电流、功率等数据后，将数据与时间戳串联再通过 SM3 算法生成 H，再用 SM9 算法利用注册时获得的私钥对 H 进行签名。使用的随机数 k 由芯片 TRNG 生成。

数据传输时，首先边缘层安全网关生成 256 位的会话密钥 K_Session，然后使用 SM9 算法使用电网云平台的平台公钥 PKGC 封装 K_Session。对明文包使用 SM4-GCM 算法用网关生成的会话密钥进行加密，并生成 128 位认证标签。传输数据包包括密文数据 +SM9 封装密钥 + 认证标签约计 1.4kb。

云端处理时，电网平台调用 HSM 内主私钥 MKGC 解密封装包，还原 K_Session, 再使用 K_Session 解密传输的密文数据包，获取原始明文。之后验证时间戳有效性，将明文和时间戳作为输入采用 SM3 算法重新计算 SM3hash 值，调用 sm9 算法，采用电表公钥验证签名。验证通过后，数据写入数据库，并将操作日志经 SM3 哈希后上链，支持审计追溯。

4 关键技术突破

4.1 轻量级 SM9–Light 算法优化

点压缩技术降低传输开销与存储压力 :SM9 标准椭圆曲线点坐标（x，y）为 128 字节（BN254 曲线），通过仅保留 X 坐标与 1 位标志位（标识 y 坐标奇偶性），压缩后长度降至 65 字节。在电表固件中嵌入点压缩函数库，支持 ASN.1 DER

格式动态切换编码实现。单次签名传输从 128 字节压缩为 65 字节，压缩率为 49%，即节省带宽 49%，能够降低单设备年通信成本，边缘网关缓存签名数据所需存储空间减少 51%，支持更长时间的数据追溯。

预计算加速缩短签名时间与能耗 :SM9 签名需要计算 S=k*P（P 为系统固定几点），将固定几点预计算生成 P,2P,4P,....2^nP 等标量乘法结果，形成查找表（LUT）预存到安全芯片中。签名时直接动态调用预计算结果表，避免实时计算大数乘法，降低 CPU 负载。该方案在 STM32F103 芯片（72MHz Cortex-M3)中预存 512 项 LUT, 占用 Flash 16KB(原算法需实时计算占用 32KB RAM），在环境温度 25^0C 测试数据为 100 万次签名均值的实验中，对比标准 SM9 单次签名时间 15.6ms，SM9-Light 单次签名时间为 6.2ms，耗能从标准 SM9 的 45.2mj 降低到了 18.5mj。满足了电网故障检测的毫秒响应需求。

差分签名机制高效处理高频数据 : 将连续采集的数

据流划分为时间窗口（如每 1 秒），计算窗口内差值 ΔD（如 Δ 功率 = 当前值 - 前次值），采用 SM3 算法仅对增量数据块 ΔD 计算哈希，而非全量数据，哈希链更新公式为 Ht=SM3(Ht−1||ΔDt)，而当 ΔD 超过阈值（如功率波动 ⩾ 5%）或达到时间窗口上限时，对当前哈希值签名。差分签名策略，使得系统稳态场景下签名频率从每秒 1 次降为 10 秒 1 次，计算量减少了 90%；在故障场景触发敏感模式下，签名频率提升 3 倍，确保关键数据实时可信。生成的哈希链依赖前次结果，篡改任一 ΔD 将导致后续所有哈希失效。

4.2 边缘到云动态密钥协商

针对智能电网边缘 - 云协同场景的密钥协商需求，采用基于标识密码的算法 SM9-KA 增强协议，通过临时密钥对（Ephemeral Key）与双线性对（Bilinear Pairing）的创新结合，可实现前向保密即单次会话密钥仅依赖临时私钥，长期主密钥泄露不影响历史会话密钥安全；通过双向身份绑定与双线性对交叉验证，阻断伪造终端或云平台的恶意接入，从而抵抗了中间人攻击。具体流程如下：

首先，协商中临时密钥的生成，边缘网关端主要计算：

①生成临时私钥 dg ∈ [1,n−1]dg ∈ [1,n−1]（n 为 SM9 椭圆曲线阶数，$n\approx2^{256}$）；

②计算临时公钥 Tg=dg • P，其中 P 为系统公开基点；

③将 Tg 发送至云平台，临时私钥 dg 仅存于安全芯片内存，会话结束后销毁。

云平台端主要计算：

①生成临时私钥 dc ∈ [1,n−1]；

②计算临时公钥 Tc=dc*P；

③将 Tc 发送至边缘网关。

其次，双方基于标识密码学原理交叉计算共享密钥：

K=e(dg*H1(IDc),Tc) ⊕ e(dc*H1(IDg),Tg)，其中 H_1(*)：SM9 哈希函数，将标识（如 EDGE_GW_01 或 CLOUD_CENTER）映射为椭圆曲线点；e( ) 为优化的双线性对运算（如 Tate 对或 Ate 对），满足 $e(aP,bQ)=e(P,Q)=e(P,Q)^{ab}$；⊕ 为异或操作，确保共享密钥一致性。

最后，密钥派生与验证对共享密钥 K 进行使用密钥派生函数 SM3-KDF 处理，生成会话密钥 $K_{session}$ 及认证标签，双方交换 SM3 哈希摘要，验证密钥一致性，失败则触发密钥重置流程。

4.3 混合加密架构实现分层安全增强

对智能电网数据的异构特性（高频统计结果、海量终端数据、敏感控制指令）与资源差异性（边缘设备低算力、云端高并发、控制信道高安全）采用“分类 - 分级 - 分速”加密策略，实现安全性与效率的最优平衡。

针对电表原始数据的高吞吐、端到端保密需求，可采用 SM9 签名 +SM4-GCM 防护策略。边缘侧智能电表采集原始数据后，生成结构化数据包，对数据包及时间戳进行 SM3 哈希计算生成 256 位摘要，SM9 算法使用电表私钥对摘要值进行签名，签名结果为 65 字节（压缩点格式）；边缘网关动态生成 256 位会话密钥，用云平台公钥封装，支持一次封装多次解密，使用会话密钥加密原始数据并生成认证标签。云端侧 HSM 使用主私钥解封会话密钥，使用 SM4-GCM 算法还原数据与签名，进行完整性校验，校验失败则丢弃数据包，通过电表标识 ID 提取 SM9 公钥，验签签名有效性，最后将明文数据写入序列数据库，进行字段级 SM4 加密，表单级 SM3-HMAC 完整性保护。

SM9 直接以电表 ID 为公钥，规避了 PKI 证书同步延迟，实现了无证书化管理。SM4-GCM 的认证标签使用（128 位）绑定时间戳，实现了抗重放攻击。

针对聚合统计数据的低延迟、完整性优先的需求，可采用 SM2 签名 +SM3 哈希防护策略。因其侧重防篡改而非全加密，可采用签名 - 哈希链对聚合结果分块（如每 1000 条为一组），然后利用 SM3 生成全局哈希 H_total，最后使用 SM2 算法对全局哈希进行签名。哈希链的设计：H_n=SM3(H_{n-1}|| 数据块 $_n$)，篡改任意数据块导致链断裂。

针对运维指令类数据的抗量子、抗篡改需求，采用 SM9 标识加密 + 时间戳绑定方式防护。对常规指令内容采用 SM9 加密（公钥为接收方 ID），而高危指令（如全网参数升级指令），则采用 SM9+Kyber 双加密，形成复合密文，密钥分离存储形式。其中 Kyber 为 NIST 后量子候选算法 CRYSTALS-Kyber（LAC-256 参数）。

5 结论与展望

本文针对智能电网海量终端设备数据安全上报的三大技术瓶颈——PKI 体系的高成本低效率、低功耗设备的密码适配困难、多方协同的身份认证缺失，提出轻量化 SM9-Light 算法优化、动态密钥协商协议及分层混合加密策略，形成无证书化身份认证、低功耗加密突破，动态安全增强方案。未来为应对量子技术发展，需加速 SM9 与后量子算法的融合研究，探索基于格密码的混合密钥封装机制，研究轻量化协同签名技术（如门限 SM9），在保障隐私的前提下支持多终端联合生成签名，解决老旧设备（无安全芯片）的合规化改造难题。

参考文献：

[1] GM/T 0044-2023. 标识密码算法SM9规范[S]. 北京: 国家密码管理局, 2023.

[2] 国家电网公司. 电力监控系统安全防护规定[Z]. 2023.

[3] Boneh D, et al. Identity-Based Encryption from the Weil Pairing[J]. CRYPTO 2001: 213-229.