

密码技术驱动的 污染源监控系统网络安全研究

文 ◆ 宁夏回族自治区生态环境信息与应急中心 马开萍

引言

污染源监控系统是一种利用现代信息技术，对污染源排放和治理设施运行情况进行实时监控的系统^[1]。其核心作用为通过在线监测设备，实时获取污染源排放数据，将监测数据通过无线网络传输至监控中心，进行实时分析和研判，帮助技术人员发现异常排放行为。然而，随着系统逐步向互联网平台转型，网络安全问题逐渐成为其运行和数据保护工作中的重大挑战。密码技术作为保障信息安全的有效手段，已成为污染源监控系统网络安全防护的重要支撑。密码技术是指采用 CA 认证等方式，加强用户身份验证环节的保护，以此缓解暴力破解攻击带来的破坏性影响^[2]。污染源监控系统的核心在于数据采集和实时传输，而这些数据一旦遭到篡改或泄露，会对环境治理工作产生严重影响。传统的网络安全防护方法，虽然能够提供防护，但面对攻击时的有效应对措施不足，而密码技术能够通过加密算法确保数据的机密性和完整性，同时通过数字签名和身份

认证机制验证数据的真实性，提升系统的防护能力。

1 分层加密数据传输

在污染源监控系统中，通过在不同层级采用不同的加密策略，能够应对各层的安全威胁，确保污染源监控数据的保密性、完整性和可用性。在系统终端数据采集层，传感器采集到污染源数据后，会立即使用 AES-GCM 算法（Advanced Encryption Standard—Galois/Counter Mode，高级加密标准—伽罗瓦 / 计数器模式）对数据加密。终端设备先生成随机的初始化向量和加密密钥，再将明文数据分割成 128 位固定大小的块，通过密钥对这些块进行多轮置换和替换操作，将明文转换为密文。加密过程中，GCM 模式会同步生成认证标签，最终加密后的数据和认证标签会封装成数据包，通过网络传输到下一层^[3]。

进入网络传输层前，通信双方（终端设备和云端服务器）需首先完成密钥协商。双方各自生成一对非对称密钥（公钥和私钥），并通过安全方式交换公钥。其次，终端设备生成随机的对称会话密钥，使用云端服务器的公钥对该会话密钥加密并发送。再次，终端设备使用生成的会话密钥，采用对称加密算法（AES）对采集到的污染源数据进行二次加密。最后，将加密后的会话密钥和二次加密的数据包一起发送给云端服务器。云端服务器收到数据后，先通过自己的私钥解密得到会话密钥，再使用会话密钥解密得到原始的污染源数据。

将数据存储至云端层，在不改变数据格式的前提下，对数据格式以及内容保留加密状态。加密前，系统会根据原始数据的格式和特点，设置 FPE 算法相关参数，将存储在云端的污染源数据作为输入，使用预设的 FPE 算法和加密密钥对数据进行加密处理。加密后的数据格式与原始数据完全相同，仅内容被加密，随后存入云端数据库。当需要检索、使用这些数据时，系统会用相同的加密密钥和 FPE 算法对加密数据进行解密，得到原始的污染源数据。

【作者简介】马开萍（1984—），女，回族，宁夏固原人，本科，高级工程师，研究方向：信息化建设及运维、网络安全、数据安全、商用密码应用等。

2 设计认证机制

在污染源监控中，终端设备分布在各个污染源现场，存在地理位置分散、所处环境复杂的特点。为确保仅有合法设备接入系统，需设置 PUF（Physical Unclonable Function，物理不可克隆函数）的身份认证机制^[4]，具体实施流程如下。

第一，设备注册，建立可信身份档案。设备将自身 PUF 响应与唯一设备标识信息绑定，通过安全通道传输至认证服务器；认证服务器接收后，对绑定信息进行校验，确认无误后存储至可信数据库，为后续认证建立基础档案。

第二，设备接入认证，验证身份合法性。当终端设备申请接入系统时，系统通过“挑战—响应”机制完成身份验证。首先，发起挑战。认证服务器向申请接入的设备发送挑战（随机数）。其次，生成响应。终端设备利用自身硬件固有的 PUF 结构，根据接收的挑战生成响应，并为该响应附加数字签名，并回传至认证服务器。最后，双重校验。认证服务器收到响应后，一方面使用数据库中预存的“PUF 激励—响应对”，验证当前响应的正确性，另一方面通过数字签名验证数据来源可信度，只有两项校验均通过，才能确认设备身份合法并允许接入；若为非法设备，因无法生成匹配的 PUF 响应，将被系统直接拒绝接入，避免其对系统发起攻击。

第三，数据传输认证，保障数据完整性与真实性。在污染源数据传输过程中，终端设备使用基于自身 PUF 生成的密钥，对采集到的污染源数据进行加密，并在加密数据中添加基于 PUF 响应的认证标签。接收方收到数据后，通过相同的 PUF 机制验证认证标签，确认数据的完整性和真实性。

第四，动态管理，适配系统扩展需求。随着监控系统规模扩大，终端设备数量会不断增加。基于 PUF 的身份认证机制支持新设备的快速注册和统一管理，同时可对已注册设备进行动态身份验证和精细化权限管理，有效提高系统的可扩展性和可管理性。

3 密钥管理

3.1 设计分层密钥派生架构

分层密钥派生架构是指将加密系统中的密钥组织成树状结构，通过

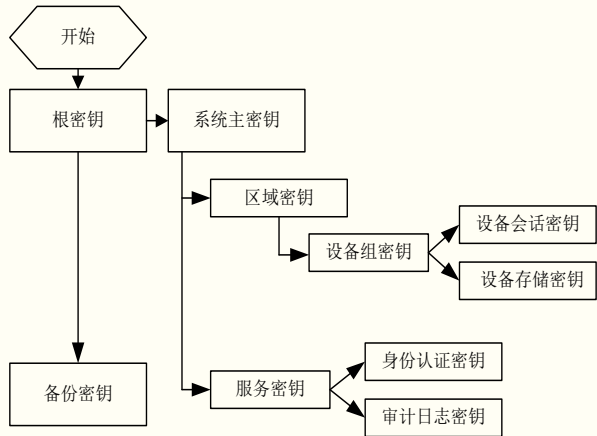


图 1 分层密钥派生架构图

密码学方法从高层级密钥派生出低层级密钥，形成严格的密钥使用边界和可控的密钥生命周期。在污染源监控系统中主要分为系统主密钥层、根密钥层和备份密钥层等三层，分层密钥派生架构图如图 1 所示。

系统主要以物理安全模块保护的根密钥为起始点，通过 SM3-KDF 算法派生出系统主密钥，遵循 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》中规定的密钥派生规范。在区域密钥（Zone Key）层级，采用前向安全的密钥派生方案，通过 HMAC-SM3（主密钥 || 区域标识 || 计数器）函数生成区域专属密钥。设备组密钥派生引入双重认证机制，同时验证设备硬件指纹（PUF 特征）和区域授权证书，完成派生过程。随后，密钥材料通过 SM4-CBC 模式加密后安全分发至终端设备。

在操作层密钥管理中，设备会话密钥采用符合 RFC 5869 的 HKDF-SM3 算法实时派生，结合 EPHEMERAL-DH 密钥交换协议，达到系统规定的网络安全性要求，并将每个会话密钥生存周期控制在 8h 以内。通过基于格式保留加密（FPE）形式包装设备存储密钥，采用 SM4-FF3 算法确保存储密钥与数据格式的兼容性。当传输数据量达到 128MB 阈值或连续使用超过 1h 时，自动触发密钥轮换，轮换过程采用 IETF RFC 8034 定义的密钥更新协议。服务密钥层中的身份认证密钥采用 SM9 标识密码体系，将设备唯一标识符作为公钥输入，通过 KGC（密钥生成中心）签发基于双线性对的私钥。审计日志密钥则采用白盒密码技术，在不可信

环境下安全使用密钥，所有密钥访问操作均记录到符合 ISO/IEC 27001 要求的审计追踪系统。

备份密钥体系采用 Shamir 门限秘密共享方案 (SSSS)，将根密钥拆分为 n 个份额 (默认 $n=5$)，按照 GB/T 36624-2018 标准分散存储在异地容灾中心，恢复过程需要至少 k 个份额 ($k=3$) 才能重构原始密钥。整个密钥派生架构通过 X.509v3 证书链建立完整的信任传递机制，每个派生环节均需验证上级密钥的数字签名，并采用 CRL/OCSP 双机制进行证书状态核查。该设计将密钥使用域的细粒度划分，即使某个子密钥泄露也不会波及到其他安全域，同时支持密钥生命周期的全流程自动化管理，满足《网络安全等级保护基本要求》中对三级系统的密钥管理要求。

3.2 设置动态密钥轮换机制

在密码学驱动的污染源监控系统中，管理密钥生命周期需要严格遵循五阶段状态机模型。在密钥生成阶段采用符合 GB/T 39786-2021 的随机数发生器，通过基于物理熵源的 TRNG (真随机数生成器) 产生符合 SM2/SM4 算法要求的密钥种子，经 SP 800-108 标准的 KDF (密钥派生函数) 扩展后形成主密钥体系。随后，在密钥激活阶段执行 NIST SP 800-135 规定的密钥装载协议，通过安全飞地 (Intel SGX 或 HSM 模块) 注入密钥，同时建立密钥使用策略绑定机制，并在使用阶段实施 FIPS 140-3 Level 3 要求的操作控制，结合 TEE (可信执行环境) 防泄露密钥，所有加密操作均记录到防篡改审计日志。

在进行密钥轮换时，整个轮换过程需要遵循 IETF RFC 8643 自动化策略，基于时间阈值 (30 天) 更新密钥，通过前向安全的密钥派生树实现无缝过渡。轮换过程时序控制逻辑图如图 2 所示。

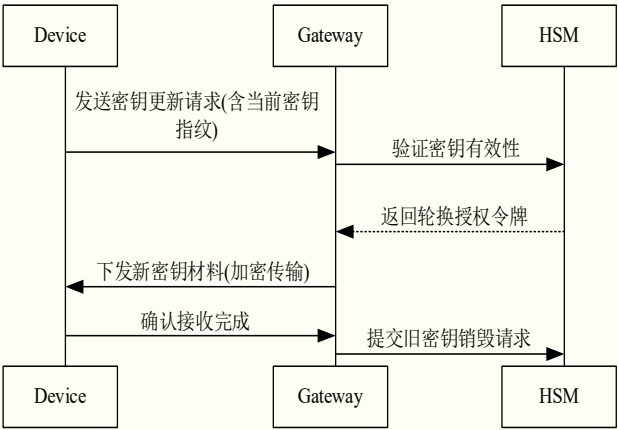


图 2 轮换过程时序控制逻辑图

注：Device 表示设备终端；Gateway 表示安全网关；HSM 表示硬件安全模块。

设备终端先通过 TLS 1.3 安全通道向网关发送密钥更新请求，该请求包含当前活跃密钥的 SM3-256 指纹以及设备 HSM 签名的时序计数器。网关接收到请求后，通过查询密钥管理服务器验证密钥指纹的有效性，并检查密钥状态是否为 ACTIV、密钥使用时长是否超过 GB/T 39786-2021 规定的 30 天阈值、设备证书链是否完整。验证通过后，HSM 基于 SM2 数字签名算法生成轮换授权令牌 (包含新密钥的有效期、使用范围限制以及防重放攻击的 Nonce 值)。设备接收完成后，通过安全启动流程验证新密钥的完整性和真实性，并向网关发送包含 SM3-HMAC 校验值的确认报文。最后，网关向 HSM 提交旧密钥销毁请求，HSM 执行 NIST SP 800-88 标准的清除操作。

结语

本文深入探讨密码技术在污染源监控系统网络安全中的应用，从数据传输加密到身份认证，再到访问控制，密码技术贯穿系统安全各环节，通过分层加密数据传输策略，应对该系统不同层级网络安全威胁。然而，网络安全形势不断演变，仍需未来研究人员持续探索更高效、适应性更强的密码技术，并结合人工智能技术优化系统安全架构，以适应不断变化的网络安全环境。

引用

[1] 王广硕,侯昊,李永杰,等.网络安全中的密码学技术应用[J].数字技术与应用, 2023,41(5):230-232.

[2] 周建金.论密码技术在网络安全中的应用[J].移动信息,2023,45(6):192-194.

[3] 王新可.互联网环境下计算机网络数据安全加密技术[J].信息记录材料,2023, 24(6):76-78+82.

[4] 黄柳莹.信息安全和密码技术的要点分析[J].产业科技创新,2023,5(2):75-77.