Computer Science and Application 计算机科学与应用, 2026, 16(6), 75-89
Published Online June 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.166210

Hans汉斯

基于SM2/SM3的智能电表身份认证协议

舒昕沂，高新萌

西京学院计算机学院，陕西 西安

收稿日期：2026年5月6日；录用日期：2026年6月10日；发布日期：2026年6月16日

摘　要

针对智能电网高级计量基础设施中智能电表面临的身份伪造、数据窃听与篡改等安全威胁，以及现有认证方案在计算开销、密钥管理、会话密钥独立与国密算法体系化应用等方面的不足，本文提出了一种基于SM2与SM3的双阶段混合身份认证协议。该协议采用“分层–混合”密码架构，将高开销的SM2椭圆曲线公钥运算限制于设备初始注册阶段，用于实现强安全的双向身份认证与长期主密钥协商；在日常高频通信阶段，则完全基于SM3-HMAC与SM4对称加密实现轻量级重认证与会话密钥动态派生，达到长期密钥仅用于认证、短期密钥专用于加密的密钥分离与纵深防御效果。协议无需实时在线可信第三方，规避了单点故障与性能瓶颈。通过仿真环境下的功能测试、性能测试及安全攻击测试，结果表明：日常会话阶段电表侧计算耗时仅3.39 ms，较第一阶段降低约65%，通信开销仅169 Byte；协议能够有效抵抗假冒、重放及篡改攻击，并满足会话密钥独立性。形式化分析(ProVerif)进一步验证了协议的机密性与双向认证属性。与现有代表性方案相比，本协议在实现国密算法(SM2/SM3/SM4)体系化合规应用的同时，在安全性与计算/通信效率之间取得了更优平衡，为智能电网的自主可控安全建设提供了可行的技术参考。

关键词

智能电表，身份认证，国密算法，SM2，SM3，类前向保密

An Identity Authentication Protocol for Smart Meters Based on SM2/SM3

Xinyi Shu, Xinmeng Gao

School of Computer Science, Xijing University, Xi’an Shanxi

Received: May 6, 2026; accepted: June 10, 2026; published: June 16, 2026

Abstract

In response to the security threats such as identity forgery, data eavesdropping and tampering

文章引用: 舒昕沂, 高新萌. 基于 SM2/SM3 的智能电表身份认证协议[J]. 计算机科学与应用, 2026, 16(6): 75-89.
DOI: 10.12677/csa.2026.166210

faced by smart meters in the advanced metering infrastructure of smart grids, as well as the deficiencies of existing authentication schemes in terms of computational overhead, key management, forward secrecy and systematic application of national cryptographic algorithms, this paper proposes a two-stage hybrid identity authentication protocol based on SM2 and SM3. This protocol adopts a "layered-hybrid" cryptographic architecture, restricting the high-overhead SM2 elliptic curve public key operation to the initial device registration stage to achieve strong two-way identity authentication and long-term master key negotiation; in the daily high-frequency communication stage, it is completely based on SM3-HMAC and SM4 symmetric encryption to achieve lightweight re-authentication and dynamic derivation of session keys, achieving the effect of key separation and depth defense where long-term keys are only used for authentication and short-term keys are exclusively used for encryption. The protocol does not require a real-time online trusted third party, avoiding single point of failure and performance bottlenecks. Through functional tests, performance tests and security attack tests in a simulation environment, the results show that the calculation time on the meter side in the daily communication stage is only 3.39 ms, about 65% lower than the first stage, and the communication overhead is only 169 bytes; the protocol can effectively resist spoofing, replay and tampering attacks, and meet forward secrecy. Formal analysis (ProVerif) further verifies the confidentiality and two-way authentication properties of the protocol. Compared with existing representative schemes, this protocol achieves a better balance between security and computational/communication efficiency while realizing the systematic compliance application of national cryptographic algorithms (SM2/SM3/SM4), providing a feasible technical reference for the autonomous and controllable security construction of smart grids.

Keywords

Smart Electricity Meter, Identity Authentication, National Cryptographic Algorithm, SM2, SM3, Class Forward Secrecy

1. 引言

随着全球能源转型与数字技术深度融合，智能电网成为现代能源体系的核心，而智能电表作为连接用户与电网的关键节点，面临身份伪造、数据窃听与篡改、重放攻击等安全威胁，可能导致电费欺诈、电网误判及隐私泄露。现有安全方案存在计算开销大、密钥管理复杂、会话密钥独立与抗抵赖性不足等问题。国密算法(SM2、SM3、SM4)为此提供了自主可控、高效安全的技术基础。

面向物联网、智能电网等资源受限场景，国密算法的轻量化高效实现成为研究热点，重点优化 SM2 标量乘法。经典方法包括二进制法、NAF、w-NAF、JSF 等，通过降低汉明重量减少点加运算。近期，有学者提出基于多项式分段与并行计算的优化方案[1]，结合 Montgomery 模乘、Co-Z 阶梯与 SIMD 指令集提升效率。硬件层面，集成国密指令集的安全芯片(如华大电子、国民技术等)提供支撑[2] [3]。

在应用方面，研究已深入物联网终端身份认证、数据安全传输及固件升级等场景。在智能电网中，国密算法用于 AMI、分布式能源接入等环节：SM2 用于双向身份认证，SM3 生成 HMAC 做完整性校验[4]，SM4 加密用电数据。

尽管进展显著，仍存挑战与不足：① 算法协同与协议设计优化不足。多数研究侧重单一算法，缺乏体系化协同运用 SM2/SM3/SM4 的分层认证协议，未清晰区分长期认证密钥与会话密钥的生命周期，难以在资源受限下实现会话密钥独立等高级属性。② 与现有工业系统及国际标准的融合兼容性问题，引入

国密可能增加时延。③ 后量子时代安全演进需前瞻布局。本论文正是针对上述不足，设计面向智能电表的体系化、轻量级双向身份认证与动态密钥管理协议。智能电网中海量智能终端与各级控制中心之间的身份认证协议是安全第一道防线。现有研究主要沿三条技术路线演进：

基于传统密码学的方案：分为三类。① 基于双线性配对：如 Tsai 等人方案[5]，Odelu 等人改进[6]，但配对运算复杂，不适用于资源受限的智能电表。② 基于椭圆曲线密码(ECC)的轻量级方案：主流选择，如 Mohammadali 等[7]、Kumar 等(LAKA 协议[8])、Abbasinezhad-Mood 等[9]。虽效率提升，但多数依赖“半诚实”可信第三方，存在单点故障与内部攻击风险；部分方案对会话密钥独立、抗去同步攻击支持不足。③ 基于对称密码与哈希的超轻量级方案：计算快，但难以同时实现双向认证、会话秘钥独立等高级安全属性。

基于硬件安全原语的方案：主要是物理不可克隆函数(PUF)。利用芯片“数字指纹”实现抗克隆与物理探测。如 Gope 等[10]、Badar 等[11]；王清[12]指出其方案无法抗重放并改进，进而提出基于 PUF 与模糊提取器的轻量级协议。PUF 面临 CRP 数据库管理开销、噪声处理复杂性等挑战。

针对上述不足，本文提出并验证了一套完全基于国密算法体系(SM2/SM3/SM4)的双阶段混合身份认证协议，实现了强安全性与轻量化效率的统一，且无需实时在线可信第三方。与现有仅做“算法替换”的方案不同，本协议的核心贡献在于国密算法的体系化协同应用：SM2 用于初始阶段的强身份认证与长期主密钥协商，SM3 用于 HMAC 完整性校验与密钥派生，SM4 用于日常数据加密。通过“分层–混合”架构，将高开销的公钥运算限制在低频的注册阶段，高频通信阶段完全基于轻量级哈希与对称密码，从而在国密合规的前提下达成安全、效率、去中心化信任三者之间的最佳平衡。

2. 关键技术介绍

为确保网络空间安全自主可控，我国自主设计并颁布了商用密码算法标准体系，统称为“国密算法”。该体系包含对称密码、非对称密码、密码杂凑算法等多种密码原语，旨在为各类信息系统提供完整、安全、高效的密码保护。其中，SM2、SM3、SM4 是三项核心且应用最广泛的算法，已形成相互支撑的算法生态，并在金融、政务、物联网等关键领域逐步替代国际通用算法(如 RSA、SHA-2、AES)，成为保障我国网络安全的重要基石。本研究所提出的认证协议正是基于此三大核心算法构建。

2.1. SM2

SM2 是一种基于椭圆曲线密码学(Elliptic Curve Cryptography, ECC)的非对称密码算法[13]，在同等安全强度下，其 256 位密钥长度远短于 RSA (相当于 RSA 3072 位)，计算更快、存储更小，特别适合资源受限环境。安全性基于椭圆曲线离散对数问题(ECDLP)。算法支持密钥生成(私钥为随机整数，公钥为私钥与基点的点乘)、数字签名(用私钥对消息杂凑值签名，验证身份与完整性)以及密钥交换(双方通过椭圆曲线点乘协商共享秘密值)，可用于加密、签名和密钥协商等场景。

2.2. SM3

SM3 是一种密码杂凑算法[14]，输出长度为 256 位，于 2010 年发布。其结构类似于 SHA-256，但在压缩函数上做了优化，抗碰撞、抗长度扩展攻击能力更强。处理流程包括：① 消息填充(填充至长度模 512 余 448 位)；② 消息扩展(生成 132 个消息字)；③ 迭代压缩(基于压缩函数 CF，结合初始值 IV 进行多轮布尔、模加、循环移位运算)；④ 输出 256 位摘要。

在本协议中，SM3 扮演多重核心角色：

完整性校验与身份认证：通过 HMAC-SM3 构造消息认证码，验证消息来源的真实性与数据完整性。

密钥派生：作为密钥派生函数(KDF)的核心组件，将高熵的共享秘密(如 SM2 协商的 Z)与其它参数混

合，生成指定长度的密码学密钥(如长期主密钥 MS 和会话密钥 SK)。

随机性摘要：对协议中的随机数、时间戳等新鲜性参数进行杂凑，参与认证标签的计算，保障协议抵抗重放攻击。

此外，已有研究(陈锐等)针对工业物联网设计了 HMAC-SM3/SHA256 低开销硬件结构[15]，支持 SM3、SHA256 及 HMAC 模式，逻辑资源缩减 53.3%，证明 SM3-HMAC 在资源受限设备中可行。

2.3. SM4

SM4 是一种分组对称密码算法[16]，分组长度和密钥长度均为 128 位，于 2012 年发布。它采用非平衡 Feistel 结构，共进行 32 轮迭代，每轮使用一个由种子密钥扩展生成的轮密钥。其设计简洁高效，在软件和硬件实现上均具有良好的性能，适用于大数据量的高速加密。

加密与解密过程结构相同，仅轮密钥的使用顺序相反。在本协议中，SM4 的职责明确且单一：数据保密性保护：在协议第二阶段，使用动态派生的、一次一密的会话密钥(SK)，采用 SM4 算法对智能电表与网关间传输的应用数据(如用电信息、控制指令)进行加密和解密，确保数据传输的机密性。

3. 协议设计

3.1. 系统模型

本协议的系统模型面向智能电网高级计量基础设施(AMI)场景，涵盖三类实体：资源受限的智能电表(T)，负责数据采集与加密上传；具备较强计算能力的网关(G)，承担身份认证、会话密钥管理与数据转发；以及离线/半离线的证书颁发机构(CA)，用于设备注册时签发 SM2 数字证书，不参与实时通信。系统采用星型拓扑，通信分为两阶段：初始注册阶段基于 SM2 实现双向认证与长期主密钥(MS)协商；日常通信阶段基于 MS 和 SM3-HMAC 完成轻量级重认证及会话密钥(SK)派生，用于数据加密传输。通信信道为不可信，攻击者可窃听、篡改、重放或伪造报文。

证书吊销机制：尽管本协议不依赖实时在线 TTP，但仍需考虑长期私钥泄露或设备退役场景下的证书吊销问题。建议在实际部署中维护一个轻量级的证书吊销列表(CRL)，由 CA 定期签名并分发至网关。网关在验证设备证书时，可缓存并检查 CRL 中的设备 ID 或证书序列号。若检测到密钥泄露或设备异常，网关应拒绝后续认证请求，并触发重新注册流程。

本文认证协议的系统模型如图 1 所示。系统主要包括智能电表、网关、主站以及可能控制公共信道的攻击者。

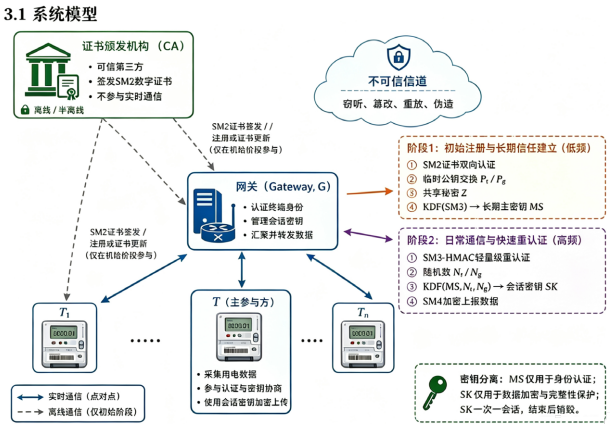

Figure 1. System model diagram
图 1. 系统模型图

3.2. 设计目标

本协议设计以双向身份认证(SM2 证书 ＋SM3-HMAC)、会话密钥独立性(动态派生会话密钥并销毁)、轻量化实现(仅初始阶段使用公钥运算，日常基于 SM3/HMAC)、抗重放与抗篡改(随机数、时间戳、MAC)、密钥分离与生命周期管理(长期密钥仅认证，会话密钥一次一会话)以及国密算法合规(SM2/SM3/SM4)为核心目标，确保方案的有效性、安全性与工程实用性。

3.3. 方案实现

安全方案中涉及的符号表达含义如表 1 所示。

Table 1. Full scheme symbol definitions
表 1. 全方案符号定义

符号	描述
T	智能电表终端(Terminal)
G	数据汇聚网关(Gateway)
CA	证书颁发机构(Certificate Authority)
ID_T	智能电表 T 的唯一身份标识
ID_g	网关 G 的唯一身份标识
$Cert_t$	智能电表 T 的 SM2 数字证书
$Cert_g$	网关 G 的 SM2 数字证书
(d_t, P_t)	T 的 SM2 临时私钥和公钥
(d_g, P_g)	G 的 SM2 临时私钥和公钥
Z	由 SM2 密钥协商生成的共享秘密值
MS	长期主密钥(Master Secret)，用于身份认证
SK	会话密钥(Session Key)，用于数据加密
N_t	终端 T 生成的新鲜随机数
N_g	网关 G 生成的新鲜随机数
Sig_t	终端 T 对协商参数的 SM2 数字签名
Sig_g	网关 G 对协商参数的 SM2 数字签名
$Auth_t$	终端 T 的身份认证标签(SM3-HMAC)
$Auth_g$	网关 G 的响应认证码(SM3-HMAC)
Req	会话请求消息
Data	待传输的应用数据(如用电信息)
KDF( )	基于 SM3 的密钥派生函数
HMAC( )	基于 SM3 的消息认证码生成函数
$Enc_{\{sk\}}( )$	使用会话秘钥 SK 的 SM4 加密函数
|	数据连接操作

本协议实现采用双阶段混合认证架构，第一阶段建立长期信任基础，第二阶段实现日常轻量级安全通信。以下将分步骤详细描述各阶段的实现细节。

3.3.1. 第一阶段：初始化建立与长期主密钥派生

此阶段仅在智能电表首次入网或证书周期性更新时执行，目标是在终端 T 与网关 G 之间建立长期信任关系，并协商生成后续轻量级通信所需的长期主密钥 MS。

1) 系统初始化与证书预置

在协议开始前，证书颁发机构 CA 已为智能电表 T 和网关 G 分别签发 SM2 数字证书 $Cert_t$ 和 $Cert_g$。$Cert_t$ 安全存储于 T 的非易失性存储器中，$Cert_g$ 存储于 G 的密钥库中。双方共享 SM2 椭圆曲线系统参数，包括基点 G、曲线方程系数、以及阶 n 等。

2) 初始协商请求

终端 T 向网关 G 发送入网请求，消息包含 ID_T：终端的唯一身份标识和 $Req_{\{init\}}$：初始化请求标识，网关 G 收到请求后，准备进行密钥协商。

3) SM2 临时密钥对生成

终端 T 生成临时的 SM2 密钥对：随机选择 $d_t \in [1, n-1]$ 作为临时私钥，并且计算临时公钥 $P_t = d_t \cdot G$。

网关 G 同样生成临时 SM2 密钥对：随机选择 $d_g \in [1, n-1]$ 作为临时私钥，并且计算临时公钥 $P_g = d_g \cdot G$。

4) 公钥交换与共享秘密计算

终端 T 将临时公钥 P_t 发送给网关 G，网关 G 将临时公钥 P_g 发送给终端 T，双方根据 SM2 密钥协商协议计算共享秘密值 Z：

T 计算：$Z = d_t \cdot P_g$。

G 计算：$Z = d_g \cdot P_t$。

由椭圆曲线密码性质可知，双方计算的 Z 值相同。

5) 双向认证与密钥确认

终端签名与认证：T 构造签名消息：$M_t = ID_T \| ID_g \| P_t \| P_g$，T 使用其长期私钥(对应 $Cert_t$ 中的公钥)对 M_t 进行 SM2 签名，生成 Sig_t，T 向 G 发送 $\{Cert_t, P_t, Sig_t\}$。

网关验证与响应：G 使用 $Cert_t$ 中的公钥验证 Sig_t 的有效性，验证通过后，G 可以确信自己计算出的共享秘密 $Z = d_g \cdot P_t$ 是与合法 T 协商得到的，随后 G 构造响应消息：$M_g = ID_g \| ID_t \| P_g \| P_t$，G 使用其长期私钥(对应 $Cert_g$ 中的公钥)对 M_g 进行 SM2 签名，生成 Sig_g，G 向 T 发送 $\{Cert_g, P_g, Sig_g\}$。

终端验证：T 使用 $Cert_g$ 中的公钥验证 Sig_g 的有效性，若验证通过，双方完成双向身份认证，双方在不直接传输 Z 的情况下，通过签名验证临时公钥的真实性，间接确认了共享秘密 Z 的一致性。

6) 长期主密钥派生

双方使用基于 SM3 的密钥派生函数 KDF()计算长期主密钥 MS：$MS = KDF(Z \| ID_t \| ID_g \| klen)$，其中 klen 为所需密钥长度(如 256 位)，长期主密钥 MS 安全存储于非易失性存储器中，临时密钥材料 (d_t, d_g, P_t, P_g, Z) 从内存中清除。

第一阶段安全性保障：本阶段基于 SM2 椭圆曲线离散对数难题，实现无第三方参与的强安全双向认证。共享秘密 Z 的协商过程具备前向保密特性，即使长期私钥泄露，也不会影响历史会话密钥的安全性。

3.3.2. 第二阶段：快速重认证与数据会话

此阶段用于智能电表日常数据上报，采用轻量级算法实现高效的身份重认证与数据安全传输。

1) 会话请求

终端 T 需要上报数据时，向网关 G 发送会话请求：$Req\{session\}$：会话请求标识以及 ID_t：终端身份标识。

网关 G 收到请求后，准备发起挑战－响应认证。

第一阶段认证流程如图 2 所示。该阶段包括终端发起认证请求、网关验证终端身份、网关返回认证响应、终端验证网关身份以及双方派生长期主密钥等步骤。图中步骤与上文协议流程描述一一对应。

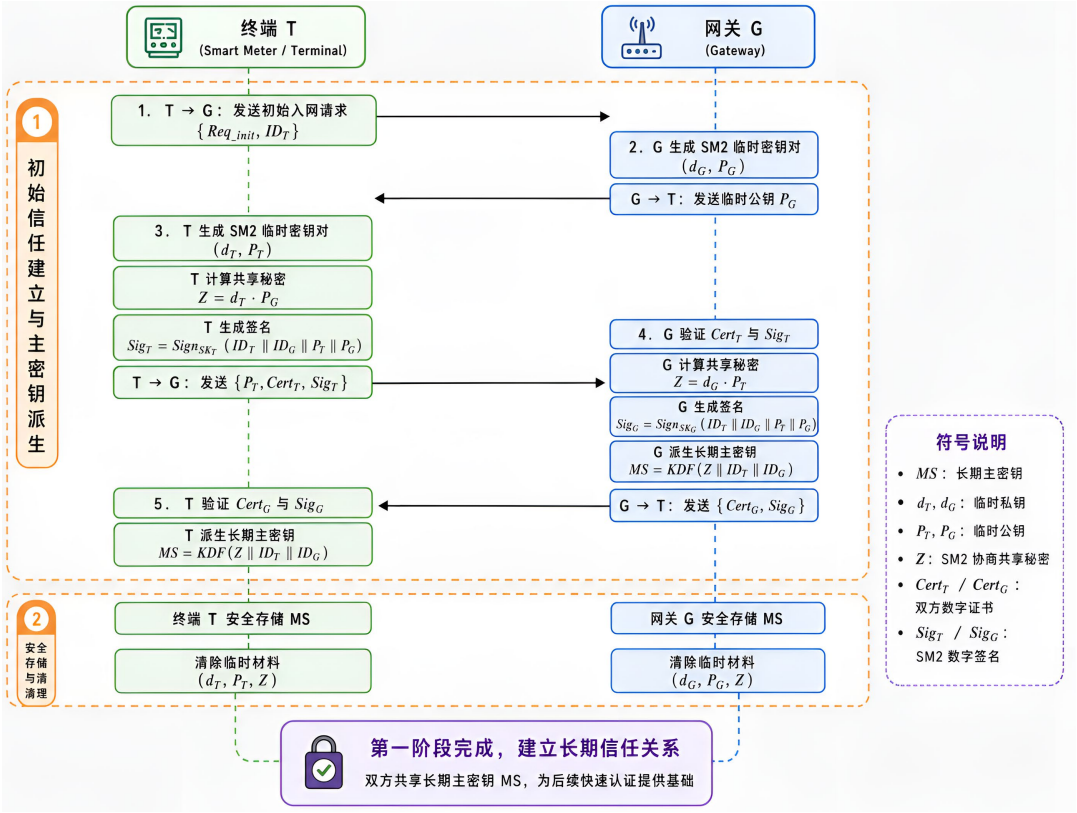

Figure 2. Flowchart of the first stage
图 2. 第一阶段流程图

2) 挑战交换

网关 G 生成高强度随机数 N_g (如 128 位)，G 将挑战 N_g 发送给终端 T，N_g 确保每次会话的新鲜性，防止重放攻击。

3) 终端身份认证响应

随机数生成：终端 T 生成自己的随机数 N_t。

认证标签计算：T 计算身份认证标签 $Auth_t$： $Auth_t = HMAC(MS, ID_t \| N_t \| N_g)$，其中 HMAC( ) 为基于 SM3 的消息认证码函数，MS 作为 HMAC 密钥，证明 T 持有正确的长期主密钥。

响应发送：T 向 G 发送{ N_t， $Auth_t$ }。

4) 网关认证与会话秘钥派生

认证验证：网关G接收到{ N_t， $Auth_t$ }后，使用本地存储的MS计算：$Auth'_t = HMAC(MS, ID_t \| N_t \| N_g)$，验证 $Auth'_t$ 与 $Auth_t$ 是否相等，若相等，则终端 T 身份认证通过。

会话密钥派生：认证通过后，G 计算本次会话的密钥 SK：$SK = KDF(MS \| N_t \| N_g, klen')$，其中 klen′ 为会话密钥所需长度(如 128 位用于 SM4)，SK 结合了长期秘密 MS 和双方的新鲜随机数，确保每次会话密钥的唯一性。

5) 双向认证完成

网关 G 计算响应认证码 Auth_g： $\mathrm{Auth}_g = \mathrm{HMAC}(\mathrm{MS}, \mathrm{N}_t \,|\, \mathrm{Auth}_t)$，G 将 Auth_g 发送给终端 T，终端 T 验证 Auth_g：计算 $\mathrm{Auth}'_g = \mathrm{HMAC}(\mathrm{MS}, \mathrm{N}_t \,|\, \mathrm{Auth}_t)$，验证 Auth_g 与 Auth'_g 是否相等，若相等，则网关 G 身份认证完成。

6) 安全数据通信

终端 T 使用会话密钥 SK 对应用数据 Data 进行加密。每次会话的 SM4 加密初始向量(IV)由 $\mathrm{SK}, \mathrm{N}_t, \mathrm{N}_g$ 通过 KDF 派生：$\mathrm{IV} = \mathrm{KDF}(\mathrm{SK} \,|\, \mathrm{N}_t \,|\, \mathrm{N}_g \,|\, 128)$。加密过程为 $\mathrm{Ciphertext} = \mathrm{Enc}_{\{\mathrm{SK}\}}(\mathrm{Data}, \mathrm{IV})$，同时计算：$\mathrm{MAC} = \mathrm{HMAC}(\mathrm{SK}, \mathrm{Ciphertext})$，T 将 $\{\mathrm{Ciphertext}, \mathrm{MAC}\}$ 发送给网关 G。G 收到数据后，以同样方式派生 IV，验证 MAC 并解密。

7) 会话秘钥销毁

本次数据通信结束后，双方立即从内存中清除会话密钥 SK，所有临时随机数 $(\mathrm{N}_t, \mathrm{N}_g)$ 和中间计算结果均被清除，长期主密钥 MS 继续安全存储，用于下次会话认证。

第二阶段安全性保障：本阶段通过 SM3-HMAC 实现轻量级身份认证，计算开销显著低于公钥运算。会话密钥 SK 的动态派生与即时销毁机制确保了会话密钥独立性。新鲜随机数的使用有效抵抗重放攻击，而消息认证码机制则保障了数据的完整性和来源真实性。

第二阶段快速重认证流程如图 3 所示。该阶段主要包括终端发起会话请求、网关验证 HMAC、网关返回认证响应、双方派生会话密钥、数据加密传输和会话密钥销毁等步骤。图中步骤与上文流程描述保持一致。

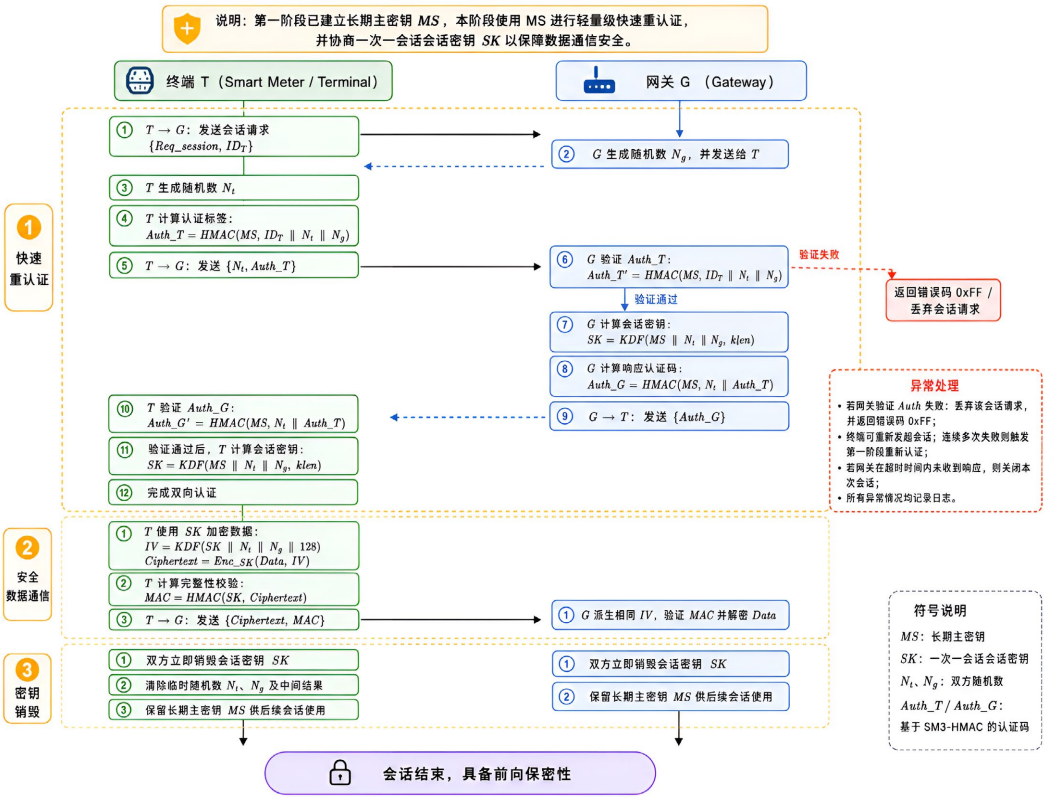

Figure 3. Flowchart of the Second Stage
图 3. 第二阶段流程图

若网关验证 Auth 失败，则丢弃该会话请求，并向终端返回错误码(如 0xFF)，终端可重新发起会话；

若连续多次失败，则触发第一阶段重新认证；若网关未在超时时间内收到响应，则关闭本次会话；所有异常情况均记录日志。

3.4. 方案分析

3.4.1. 非形式化安全分析

本节从抵抗典型攻击的角度，对所提协议进行非形式化安全分析，论证其能够实现预定的安全目标。

抵抗假冒攻击：攻击者若伪装成合法智能电表或网关，需伪造 SM2 签名或 SM3-HMAC。SM2 签名基于椭圆曲线离散对数问题(ECDLP)的难解性，无合法实体私钥无法生成有效签名；SM3-HMAC 依赖于长期主密钥 MS，而 MS 由临时私钥对协商的共享秘密 Z 派生，攻击者无法获得 Z。因此假冒成功的概率等价于破解 SM2 或 SM3 的难度。

抵抗重放攻击：协议在每次会话中引入新鲜性参数：第一阶段使用临时生成的密钥对，第二阶段使用高强度随机数 N_t 、 N_g 作为挑战－响应。攻击者重放旧消息时，由于 N_g 已更新，旧的认证标签 $Auth_t$ 无法通过验证。此外，协议可扩展时间戳机制进一步限制消息的有效窗口。

抵抗中间人攻击：协议要求终端与网关双向认证，且通过 SM2 签名确认双方计算出了相同的共享秘密 Z。若攻击者篡改公钥 P_t 或 P_g ，将导致双方计算的 Z 不一致，签名验证失败。协议中所有关键消息均包含完整性校验，篡改行为可被立即检测。

抵抗密钥泄露攻击：协议采用密钥分离设计：长期主密钥 MS 仅用于身份认证，会话密钥 SK 仅用于数据加密，二者泄露影响隔离。第一阶段基于临时密钥对提供前向保密，即使长期私钥泄露也无法推导历史会话的共享秘密 Z；第二阶段基于 MS 与新鲜随机数提供会话密钥独立，即使 MS 泄露也不影响历史会话数据的机密性。所有密钥均有明确的生命周期和使用限制。

抵抗去同步化攻击：长期主密钥 MS 独立于单次会话存储于非易失性存储器中，单次认证失败不会改变 MS 的一致性。协议定义了明确的失败处理流程：验证失败时双方清除临时状态但保留长期密钥，可随时重新发起认证，不会进入永久去同步状态。

抵抗拒绝服务攻击：在第二阶段，网关 G 首先生成随机数 N_g ，仅当收到合法响应 $Auth_t$ 后才执行 HMAC 计算和密钥派生，避免了无差别消耗计算资源。日常认证使用轻量级的 SM3-HMAC，计算开销小，且可配合基于 IP 或身份的频率限制策略进一步增强防御能力。

状态耗尽型 DoS 攻击分析与缓解：在协议第二阶段，网关需为每个会话生成随机数并维护会话状态。攻击者可大量伪造会话请求，导致网关内存资源耗尽。为缓解此类攻击，建议采取以下策略：源 IP 请求速率限制：网关对每个 IP 地址的会话请求频率进行限制(如每秒不超过 5 次)，超限则临时封锁；无状态随机数生成：网关可采用伪随机函数派生的方式生成，避免为每个会话存储状态，例如 $N_g = \mathrm{PRF}\left(K_g, ID_t, \mathrm{timestamp}\right)$ ，其中 K_g 为网关本地密钥；低开销预过滤：在收到完整认证标签之前，网关仅执行轻量级哈希与速率检查，不分配复杂会话结构。

以上分析表明，该协议能够有效抵抗多种典型攻击，满足双向认证、密钥确认、会话密钥独立和消息完整性等安全目标。

3.4.2. 形式化安全分析

为严格验证本文所提出协议的安全性，采用自动化安全协议验证工具 ProVerif 对协议进行形式化建模与分析。ProVerif 基于应用 Pi 演算，能够证明协议的抗攻击性、机密性与认证属性，广泛应用于密码协议的形式化验证领域。

1) 协议建模

密码学原语建模：采用等式理论定义椭圆曲线 Diffie-Hellman 密钥交换(exp(exp(g,x),y) = exp(exp(g,y),x))、签名验证(getmsg(sign(m,sk)) = m)以及对称加密(dec(enc(x,k),k) = x)。HMAC 和 KDF 函数以不可逆哈希函数建模，攻击者无法逆向推导。

攻击者模型：采用 Dolev-Yao 完全控制模型，攻击者可窃听、篡改、重放、伪造任意消息，但无法攻破底层密码学原语的数学困难性。

安全声明(Queries)：设置三类形式化查询：

机密性查询：验证攻击者是否能够获取长期主密钥 MS、会话密钥 SK 或用户上报数据 Data (即 attacker (MasterSecret[])等是否为假)。

认证性查询：验证协议各阶段的事件对应性(Correspondence Assertion)，包括：

event(phase1_complete(T_id,G_id)) ==> event(phase1_started(T_id,G_id))

(第一阶段完成之前必须已开始)

event(end_gateway_verified(T_id)) ==> event(begin_terminal_challenge(T_id))

(网关完成对终端的认证之前，终端必须发起挑战)

event(end_terminal_verified(T_id)) ==> event(begin_gateway_challenge(T_id))

(终端完成对网关的认证之前，网关必须发起挑战)

2) 验证结果

ProVerif 运行后输出所有查询结果为 true，具体数值汇总于表 2。

Table 2. Formal verification results of ProVerif
表 2. ProVerif 形式化验证结果

查询类型	查询内容	结果
机密性	not attacker(MasterSecret[]) (长期主密钥泄露)	True
机密性	not attacker(SessionKey[]) (会话密钥泄露)	True
机密性	not attacker(SecretData[]) (用户数据泄露)	True
认证性	event(phase1_complete(id1,id2)) ==> event(phase1_started(id1,id2))	True
认证性	event(end_gateway_verified(id)) ==> event(begin_terminal_challenge(id))	True
认证性	event(end_terminal_verified(id)) ==> event(begin_gateway_challenge(id))	True

输入结果如图 4 所示：

```
--------------------------------------------------------------
Verification summary:

Query not attacker(MasterSecret[]) is true.

Query not attacker(SessionKey[]) is true.

Query not attacker(SecretData[]) is true.

Query event(end_gateway_verified(id)) ==> event(begin_terminal_challenge(id)) is true.

Query event(end_terminal_verified(id)) ==> event(begin_gateway_challenge(id)) is true.

Query event(phase1_complete(id1,id2)) ==> event(phase1_started(id1,id2)) is true.

--------------------------------------------------------------
```

Figure 4. The output result of ProVerif formal analysis
图 4. ProVerif 形式化分析输出结果

3) 结果分析

机密性保障：攻击者无法获得 MS、SK 及传输的 Data。这表明协议在 Dolev-Yao 攻击模型下能够抵抗被动窃听和主动密钥提取，实现了数据机密性。

双向强认证性：三个对应性查询全部成立。

第一阶段对应性保证：只有双方成功完成 SM2 签名验证并计算出相同的共享秘密 Z 后，phase1_complete 事件才会发生，且该事件一定发生于 phase1_started 之后，严格实现了基于公钥证书的强双向身份认证。

第二阶段对应性保证：end_gateway_verified 事件必然伴随 begin_terminal_challenge，且 end_terminal_verified 必然伴随 begin_gateway_challenge。这说明只有持有正确 MS 的合法实体才能通过挑战－响应认证，证明了第二阶段轻量级 HMAC 认证机制的正确性。

密钥独立性与类前向保密：由于 MS、SK、Data 均被证明不可被攻击者获取，且每次会话独立派生新的 SK，协议满足密钥分离与会话密钥独立的设计目标。

4) 结论

ProVerif 形式化分析证明本文协议在机密性、相互认证、事件对应性等关键安全属性上均达到设计要求，与非形式化安全分析结论完全一致，进一步增强了协议的可信度。

4. 实验测试与分析

为评估本文基于 SM2/SM3 的双阶段混合认证协议的性能与安全性，在笔记本电脑(Windows 11, Python 3.12.6, gmssl 国密库)上模拟智能电表与网关通信，网络延迟设为 10 ms，使用 time.perf_counter()(微秒级)测量各密码操作耗时，通过累加消息长度计算通信字节数。实验环境：13 代 i9-13900HX(2.20 GHz)，32 GB RAM，电表与网关为同机软件实体，通过本地队列交互。本实验仅验证协议逻辑与相对性能，结果不代表真实嵌入式平台表现，后续将进行硬件移植评测。

4.1. 协议功能与正确性验证

首先验证协议的正常工作流程。运行一次第一阶段(初始注册)和 20 次第二阶段(日常会话)。实验结果表明：第二阶段 20 次会话全部成功，成功率为 100%。每次会话均完成双向 HMAC 认证、会话密钥 SK 派生、SM4 数据加密与解密。正确性验证通过，证明协议逻辑无误。

4.2. 性能测试与分析

4.2.1. 计算通信开销

从表 3 可以看出，第二阶段移除了所有公钥运算，电表侧计算耗时降低约 65%。在真实嵌入式平台(无硬件加速)，SM2 点乘耗时可能高达 300 ms，而 HMAC + SM4 仅需约 20 ms，优化效果更显著。在低延迟网络中，第二阶段总耗时仅为第一阶段的 30%；在模拟高延迟(10 ms)网络中，两者总耗时相近，但第二阶段计算负荷已大幅降低，有利于设备能耗与并发处理，在仿真环境下，该耗时远小于典型数据上报周期(秒级至分钟级)，表明本协议在计算开销方面具备满足实时性要求的潜力。

Table 3. Two-stage comprehensive performance comparison chart
表 3. 两阶段综合性能对比图

指标	第一阶段	第二阶段
电表侧计算耗时	9.74 ms	3.39 ms
网关侧计算耗时	9.13 ms	3.85 ms

续表

是否含公钥计算(电表侧)	是	否
通信字节数	315B	169B
端到端耗时	62.80 ms	61.35 ms
端到端耗时(极低延迟)	~23 ms	~7 ms
执行频率	极低	高

4.2.2. 存储开销估算

协议在智能电表端需要存储：长期主密钥 MS (32 字节)、SM2 证书(约 300~500 字节)、SM2 私钥(32 字节)、以及协议代码与密码库。基于 gmssl 库的典型嵌入式移植版本，代码段(含 SM2/SM3/SM4)约占用 60 KB Flash，RAM 峰值(包含栈和临时缓冲区)约 8 KB。根据仿真环境下代码与数据空间的估算，本协议的存储需求(约 60 KB Flash、8 KB RAM)在主流智能电表芯片的标称容量范围内。

4.2.3. 安全性测试

为验证协议抵抗常见主动攻击的能力，我们实施了以下攻击测试：

假冒攻击：攻击者试图使用错误的长期主密钥 MS (全 0)计算 $Auth_T$ 并发送给网关。网关重新计算 $Auth'_T$ 后发现不匹配，拒绝该会话。测试结果：通过。

重放攻击：攻击者记录一次合法会话中的 $N_t \mid Auth_T$，并在下一个会话中(网关已生成新的 Ng)重新发送。由于 $Auth_T$ 的 HMAC 计算包含了 N_g，旧 $Auth_T$ 与新 N_g 不匹配，网关拒绝。测试结果：通过。

篡改攻击：攻击者修改密文 Ciphertext 的一个字节，或修改 MAC 的任意位。网关在验证 MAC 时发现不一致，丢弃数据并记录异常。测试结果：通过(两种篡改方式均被检测)。

Table 4. Attack test result
表 4. 攻击测试结果

攻击类型	结果
假冒攻击(错误 MS)	拒绝
重放攻击(旧 AuthT)	拒绝
篡改攻击(密文/MAC)	拒绝

表 4 表明，本协议能够有效抵抗智能电网环境中的常见主动攻击。假冒攻击因攻击者无法获取合法长期主密钥 MS 而被阻止；重放攻击因认证标签绑定新鲜随机数 N_g 而失效；篡改攻击则因 HMAC 完整性校验机制被立即检测。因此，协议在不可信信道中可保障通信的真实性与完整性。

4.3. 综合讨论

4.3.1. 安全属性对比

特别说明：方案 A 中网关存储扩展 CRP，认证过程无需在线第三方，但注册阶段需安全环境。

表 5 表明，所有对比方案均能实现双向认证、抗重放、抗中间人攻击等基本安全属性，但在高级安全特性上差异明显：方案 B 具备匿名性，但依赖控制中心作为可信第三方，系统复杂度高；方案 C 采用国密 SM9，但仍需密钥生成中心(KGC)，无法去中心化；方案 A 利用 PUF 抵抗物理攻击，但未设计会话密钥独立性与密钥分离；方案 D 实现了前向安全性，却未严格实现长期与短期密钥分离。相比之下，本文协议在满足基础安全的同时，额外具备会话密钥独立性、密钥分离和去中心化信任三项高级安全属性，

并实现了 SM2/SM3/SM4 国密算法的体系化合规应用，在安全全面性与国密自主可控两方面均具优势。

Table 5. Security attribute comparison
表 5. 安全属性对比

安全属性	方案 A [17]	方案 B [18]	方案 C [19]	方案 D [20]	本方案
双向身份认证	是	是	是	是	是
类前向保密	未提及	未提及	未明确	是	是
抗重放攻击	是	是	是	是	是
抗中间人攻击	是	是	是	是	是
密钥分离	未明确	未明确	未明确	未明确	是
匿名性与隐私保护	否	是	是	是	否
无需实时在线 TTP	是	否(依赖 CC)	否(依赖 KGC)	否(依赖 CA)	是
国密合规性	否	否	是(SM9)	否	是

4.3.2. 性能指标对比

在安全属性定性比较的基础上，进一步对本文方案与各对比方案的性能指标进行定量分析。表 6 汇总了各方案在计算开销、通信开销等关键性能指标上的实测或合理推算数据。其中，方案 A、方案 B、方案 D 的数据均来源于各论文原文报告的实验测量值(虽然测试值可能因实验环境等多方面因素存在差异，但是依然有一定参考性)，方案 C 因原文未提供明确的毫秒级耗时数据，采用基于算法复杂度的合理估算，并加注说明。

Table 6. Comprehensive comparison of performance indicators
表 6. 性能指标综合对比

指标	方案 A	方案 B	方案 C	方案 D	本方案二阶段
电表侧计算耗时(ms)	3.85	0.093	约 8	47.72	3.39
通信开销(Byte)	486	400	约 300	432	169
公钥运算(电表侧)	否(PUF 代替)	否(仅哈希)	是(双线性对)	是(ECC 点乘)	否
认证轮次	2	3	3	3	2

计算性能：本文协议电表侧耗时 3.39 ms，低于需公钥运算的方案 D (47.72 ms)，虽高于方案 B (0.093 ms)与方案 A (3.85 ms)，但提供了前向保密性与密钥分离等高级安全属性，效率可接受。

通信性能：本文协议第二阶段仅 169 Byte，优于方案 B (400 Byte)、方案 D (432 Byte)和方案 A (486 Byte)，得益于两阶段设计，日常通信只需随机数与 HMAC 标签。

认证轮次：本文协议第二阶段仅 2 轮交互，少于方案 B、C、D (均需 3 轮)，有利于降低延迟、提升并发能力。

高级安全特性：本文协议同时实现会话密钥独立性与密钥分离；四篇对比方案中仅方案 D 实现了会话密钥独立性但未实现密钥分离且计算开销高，其余均未明确支持这两项特性，印证了本协议“分层–混合”架构与密钥分离机制的显著优势。

4.4. 实验结论

通过仿真实验全面评估了基于 SM2/SM3 的双阶段身份认证协议。实验结果表明：

功能正确：两阶段协议均可成功执行，双向认证、密钥派生、数据加密解密均正确。

计算轻量：日常会话电表侧计算耗时为 3.39 ms，无公钥运算，在仿真测试中可支持高频次会话模拟。

通信高效：第一阶段 315 B，第二阶段 169 B (64 B 数据)，适合窄带通信。

安全强健：能有效抵抗假冒、重放、篡改等主动攻击。

综上，本协议在保证高安全性的前提下，实现了资源受限环境下的轻量化认证，为智能电网高级计量基础设施提供了一种符合国密标准、切实可行的安全解决方案。

5. 总结与展望

针对智能电网高级计量中身份认证与数据安全传输难以兼顾安全强度、计算效率与国产化合规的问题，本文提出基于 SM2/SM3 的双阶段混合认证协议。采用“分层–混合”密码架构：高开销的 SM2 公钥运算仅限初始注册阶段，日常高频会话基于 SM3-HMAC 与 SM4 对称加密。仿真实验表明，日常会话电表侧计算耗时仅 3.39 ms，较第一阶段降低约 65%。协议通过每次会话动态派生一次性会话密钥并即时销毁，实现会话密钥独立性；长期密钥仅用于认证、短期密钥专用于加密，形成密钥分离与纵深防御。全程采用 SM2/SM3/SM4 国密标准，符合国产化要求，且无需实时在线可信第三方。性能测试显示：第二阶段单次会话总耗时 61.35 ms (含 10 ms 网络延迟)，通信开销仅 169 Byte；协议能有效抵抗假冒、重放及篡改攻击。

本文协议在仿真中表现良好，但仍存在以下局限性及未来改进方向：① 当前基于 x86 模拟，尚未在真实电表 MCU (如 ARM Cortex-M)上验证，后续计划移植至 STM32 等平台评估闪存、RAM 及能耗；② 证书管理假设 CA 预签发，未处理吊销列表与有效期检查，实际部署需集成完整证书管理及安全更新协议；③ SM4 采用全零初始向量，存在相同明文块产生相同密文块的风险，后续可由随机数派生增强安全性；⑤ 量子计算对椭圆曲线构成长期威胁，未来可研究基于格的后量子国密算法替代 SM2。综上，本协议为智能电网自主可控安全提供了有益参考，期望推动国密算法在电力物联网中的深度应用。

本文提出并验证了一套完全基于国密算法体系(SM2/SM3/SM4)的双阶段身份认证协议，其核心创新在于：① 体系化协同应用国密三算法，而非单一算法替换，形成完整的自主可控密码闭环；② 长期密钥仅认证、短期密钥专加密的分层密钥架构，实现类前向保密；③ 无需实时在线可信第三方，避免单点故障，适用于分布式智能电网环境。实验与形式化分析表明，该协议在日常高频通信阶段电表侧计算耗时仅 3.39 ms，通信开销仅 169 Byte，能有效抵抗假冒、重放及篡改攻击。本文为智能电网高级计量基础设施提供了一种符合国密标准、兼顾安全与效率的可行技术方案，有望推动国密算法在电力物联网中的深度工程化应用。

参考文献

[1] Zhu, H., Li, D., Sun, Y., Chen, Q., Tian, Z. and Song, Y. (2024) Optimization of SM2 Algorithm Based on Polynomial Segmentation and Parallel Computing. *Electronics*, **13**, Article No. 4661. https://doi.org/10.3390/electronics13234661

[2] 付元元, 高献伟, 董秀则. 基于 FPGA 的 SM2 加解密算法的优化设计[J]. 北京电子科技学院学报, 2022, 30(3): 71-80.

[3] 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.

[4] 区永通, 陈重辰, 谭浩彬, 等. 基于 SM3 算法的智能配电网报文安全认证方法[J]. 机电工程技术, 2024, 53(2): 263-266.

[5] Tsai, J.L. and Lo, N.W. (2016) Secure Anonymous Key Distribution Scheme for Smart Grid. *IEEE Transactions on Smart Grid*, **7**, 906-914.

[6] Odelu, V., Das, A.K., Wazid, M., *et al*. (2018) Provably Secure Authenticated Key Agreement Scheme for Smart Grid.

IEEE Transactions on Smart Grid, **9**, 1900-1910.

[7] Mohammadali, A., Sayad Haghighi, M., Tadayon, M.H. and Mohammadi-Nodooshan, A. (2018) A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid. *IEEE Transactions on Smart Grid*, **9**, 2834-2842. https://doi.org/10.1109/tsg.2016.2620939

[8] Kumar, P., Gurtov, A., Sain, M., Martin, A. and Ha, P.H. (2019) Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks. *IEEE Transactions on Smart Grid*, **10**, 4349-4359. https://doi.org/10.1109/tsg.2018.2857558

[9] Abbasinezhad-Mood, D. and Nikooghadam, M. (2018) An Anonymous ECC-Based Self-Certified Key Distribution Scheme for the Smart Grid. *IEEE Transactions on Industrial Electronics*, **65**, 7996-8004. https://doi.org/10.1109/tie.2018.2807383

[10] Gope, P. and Sikdar, B. (2021) A Privacy-Aware Reconfigurable Authenticated Key Exchange Scheme for Secure Communication in Smart Grids. *IEEE Transactions on Smart Grid*, **12**, 5335-5348. https://doi.org/10.1109/tsg.2021.3106105

[11] Badar, H.M.S., Mahmood, K., Akram, W., Ghaffar, Z., Umar, M. and Das, A.K. (2023) Secure Authentication Protocol for Home Area Network in Smart Grid-Based Smart Cities. *Computers and Electrical Engineering*, **108**, Article ID: 108721. https://doi.org/10.1016/j.compeleceng.2023.108721

[12] 王清. 智能电网的认证与密钥协商协议研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2023.

[13] 国家密码管理局. GM/T 0002-2012. SM2 椭圆曲线公钥密码算法[S]. 北京: 中国标准出版社, 2012.

[14] 国家密码管理局. GM/T 0003-2012. SM3 密码杂凑算法[S]. 北京: 中国标准出版社, 2012.

[15] 陈锐, 李冰, 朱家乐, 等. HMAC-SM3/SHA256 算法的低开销硬件结构设计[J]. 电子器件, 2023, 46(4): 888-894.

[16] 国家密码管理局. GM/T 0004-2012. SM4 分组密码算法[S]. 北京: 中国标准出版社, 2012.

[17] 张跃飞, 袁征, 冯笑, 等. 面向电力物联网设备的基于 PUF 的轻量级认证协议[J]. 计算机应用研究, 2025, 42(5): 1541-1548.

[18] 王圣宝, 周鑫, 文康, 等. 适用于智能电网的三方认证密钥交换协议[J]. 通信学报, 2023(2): 210-218.

[19] 喇元, 赵继光, 张伟. 基于 SM9 门限签名的电力终端安全认证方案[J]. 电力科学与技术学报, 2022, 37(4): 183-188, 226.

[20] 王胜, 张凌浩, 滕予非, 等. 基于隐式证书的电力工业互联网轻量级身份认证方案[J]. 电子与信息学报, 2026, 48(2): 597-606.