适用于智能电网的三方认证密钥交换协议

王圣宝，周鑫，文康，翁柏森
（杭州师范大学信息科学与技术学院，浙江 杭州 311121）

摘 要：大部分现有智能电网环境下的认证方案都存在需要人工参与或运行性能不高的缺点，不能满足智能电网的实际需求。鉴于此，提出了一种新的三方认证密钥交换协议，用于智能电表、服务提供商和控制中心三方之间的认证和密钥建立。基于物理不可克隆函数，去除了需要人工参与协议运行的缺陷。结合 BAN 逻辑和非形式化分析方法，对协议的安全性进行了证明。与同类代表性协议相比，所提协议具有更好的安全性和更高的效率。

关键词：智能电网；物理不可克隆函数；相互认证；密钥交换；BAN 逻辑
中图分类号：TP309
文献标志码：A
DOI: 10.11959/j.issn.1000–436x.2023039

Tripartite authenticated key exchange protocol for smart grid

WANG Shengbao, ZHOU Xin, WEN Kang, WENG Bosen
School of Information Science and Technology, Hangzhou Normal University, Hangzhou 311121, China

Abstract: Most of the existing authentication schemes in the smart grid environment have the drawbacks of requiring manual participation or low performance, and thus do not meet the practical needs of smart grids. A new tripartite authenticated key exchange protocol was proposed for authentication and key establishment between three parties: smart meters, service providers and control center. The protocol was based on a physical unclonable function, which removed the drawback of requiring manual participation in the operation of the protocol. The security of the protocol was demonstrated by combining BAN logic and non-formal analysis methods. Comparing with similar representative protocols, the proposed protocol has better security and higher efficiency.

Keywords: smart grid, physical unclonable function, mutual authentication, key exchange, BAN logic

0 引言

智能电网是在传统电力系统的基础上，通过集成新能源、新材料、新设备和先进传感技术、信息技术、控制技术、储能技术等新技术，形成的新一代电力系统，具有高度信息化、自动化、互动化等特征，可以更好地实现电网安全、可靠、经济、高效运行[1]。智能电网不仅能满足日益增长的用电需求，还能规避社会用电量爆发式增长、用电需求快速上升、电网规模不断升级以及线路复杂度迅速增加所带来的安全风险，同时也能增加电力需求端和电力供给端的双向互动，降低运营成本，并最大限度地减少资源浪费[2]。因此，全面建立统一“坚强智能电网”是中国电网的发展方向[1]。

随着智能电网基础设施建设的推进，海量电力终端设备投入运营，其种类繁多、部署分散、通信手段多样。这些特点给智能电网的安全防护带来了新的挑战[3-4]。信息和系统安全成已为智能电网广泛部署的一个关键挑战[5]。

此外，隐私保护也是智能电网面临的挑战。智能电表收集的数据（如用电负载、功耗、用电时长等）的泄露可能导致严重的隐私问题。例如，攻击

收稿日期：2022–10–08；**修回日期：**2022–12–26
基金项目：国家自然科学基金资助项目（No.U21A20466）；基于大数据架构的公安信息化应用公安部重点实验室开放课题资助项目（No.2021DSJSYS005）
Foundation Items: The National Natural Science Foundation of China (No.U21A20466), Key Laboratory of Public Security Information Application Based on Big-Data Architecture, Ministry of Public Security (No.2021DSJSYS005)

者可以利用功耗和负载信息推断用户类型，利用用电记录推断用户用电时间段，根据用电习惯推送个性化广告等；攻击者可使用简单的统计工具从高分辨率的消费信息中提取复杂的用户使用模式，继而实现对用户进行画像和监控[6]。

为了保障智能电网环境下信息和隐私安全，需要对通信参与者进行身份认证，并在公开信道上安全有效地建立会话密钥。Wu 等[7]提出了一种容错和可扩展的密钥分发方案，采用基于 Needham-Schroeder 认证协议的对称和基于椭圆曲线密码学（ECC, elliptic curve cryptography）的非对称密钥组合方法。由于该方案使用公钥基础设施，因此存在管理密钥和证书的问题，这会导致通信开销增加。Xia 等[8]进一步的研究证明，上述方案不能保证密钥的安全性，并提出了一种新的密钥分发方案，可抵抗多种攻击。Wazid 等[9]提出了一种智能电网环境下的三因子认证方案。在该方案中，用户和远程仪表之间可以进行双向认证并建立会话密钥。文献[10]提出了一种基于椭圆曲线的智能电网轻量级认证方案，然而 Abbasinezhad-mood 等[11]进一步的研究证明该方案并不安全并提出了一个改进方案。2019 年，Chen 等[12]针对上述方案的不足，提出了一种基于双线性映射的通信认证方案。文献[13]在 V2G（vehicle-to-grid）环境下，为电动汽车充电引入了三方多因素认证。文献[14]在智慧医疗场景下，采用椭圆曲线实现医生和传感器节点的相互认证和密钥建立。

然而，存储在非易失性存储器（NVM, non-volatile memory）中的密钥信息容易遭受侧信道攻击，破坏协议的整体安全。因此，物理不可克隆函数（PUF, physical uncloneable function）被广泛用于认证协议中。作为一种轻量级基本安全模块，PUF 无须使用 NVM，且对侵入式攻击反应灵敏[15]。PUF 提供了数字输入（激励）到数字输出（响应）的不可逆映射。但与加密哈希函数不同的是，其安全性来自物理无序和不可预测性，而非计算复杂性理论。这种“激励–响应”机制的触发不需要存储、易实现且能耗低，多应用于资源受限的物联网设备的安全认证[16]。2018 年，贺章擎等[17]提出了一种基于 PUF 的两方认证与会话密钥交换协议，该协议能抵抗网络和物理攻击。夏艳东等[18]提出了在工业物联网环境下基于 PUF 的轻量级密钥交换协议，适用于资源受限设备的同时能抵抗多种已知攻击。Liyanage 等[19]提出了一种使用 PUF 和公共集群节点在 2 个物联网设备之间进行认证的方案，该方案中的“激励–响应”对（CRP，challenge response pair）不是显式存储的，因此攻击者无法将相关联的存储数据绑定到机器学习算法中。Bian 等[20]则采用不同的方法，将 PUF 和模糊提取器相结合，构造了一种生物认证方案。该方案利用模糊提取器来保护隐私输入，增强生物特征数据的安全性，从而提高了方案的稳健性。

通过对比分析，本文发现已有方案主要存在以下 4 个问题。

1) 性能过低。文献[7-8]方案需要使用公钥基础设施，文献[10-12]方案需要多次椭圆曲线乘法运算或双线性配对运算。因此这些方案运行性能低，不适用于资源受限设备（如传感器节点、智能电表）。

2) 需要人工干预。文献[9,20]方案用到了生物识别，因此需要人工输入指纹。这显然不满足智能电表可以自动、周期性地向控制中心（CC）发送数据，而不需要用户实时参与的特点。因此文献[9,20]方案不适用于智能电网环境。

3) 不能抵抗侧信道攻击。大部分工作没有防范侧信道攻击从集成电路中提取秘密信息[21]，如文献[8-14]。然而，智能电表通常安装在远程恶劣环境下，更容易遭受侧信道攻击。

4) 通信效率低。文献[10-12,17,19]所提出的方案都是两方协议，要实现智能电表、服务提供商和控制中心三方安全通信，就需要在两两之间运行两方协议，这就造成了通信轮数的大量增加，大大降低了通信效率。

针对上述问题，本文设计了一个高效的三方认证密钥交换协议。本文协议的运行不需要人工干预，并且使用了 PUF 模块以对抗侧信道攻击。本文分别采用形式化的 BAN 逻辑证明和非形式化方法验证和分析了本文协议的安全性，并通过性能分析和比较证明本文协议更加高效和实用。

1　预备知识

1.1　单向哈希函数

单向哈希函数 $H(\cdot)$ 从任意长度的输入生成固定长度的输出。其安全属性如下[22-23]。

1) 抗原像性。对于给定哈希值 h 和单向哈希函数 $H(\cdot)$，很难找出任何原像 m 使 $h=H(m)$。

2) 抗次原像性。对于给定的原像 a，很难找到另一个原像 b，使 $H(a)=H(b)$。

3) 抗碰撞性。对同一个单向哈希函数 $H(\cdot)$，很难找到 2 个不同的输入，使 $H(a)=H(b)$。

4) 单向性。对于给定哈希值 h 和单向哈希函数 $H(\cdot)$，提取相对应的输入 m 是困难的。

1.2 物理不可克隆函数

物理不可克隆函数[24]是嵌入物理结构（如集成芯片）中的物理实体，通过 $R \leftarrow \mathrm{PUF}(C)$ 的方式，其可以为给定的输入（激励）生成相对应的输出（响应）。物理不可克隆函数提供了一种在不安全环境下认证设备和保护设备免受物理威胁的有效方法。换言之，PUF(·) 可以充当设备的数字指纹。PUF 安全性质如下。

1) 唯一性。对任意 2 个不同的 PUF，即 $\mathrm{PUF}_1(\cdot)$ 和 $\mathrm{PUF}_2(\cdot)$，给定同一输入 C，其输出 $R_1 \leftarrow \mathrm{PUF}_1(C)$ 和 $R_2 \leftarrow \mathrm{PUF}_2(C)$ 是不同的。

2) 可再现性。多次对任一相同 PUF 给定相同的输入，其响应是相同的。

3) 不可克隆性。由于物理结构和技术原因，已嵌入设备的特定 PUF 不可能被克隆。

4) 单向性。PUF 类似于密码学中的单向函数，即给定响应 R 和特定的 PUF(·)，生成相应的激励 C 是困难的。

1.3 系统模型

如图 1 所示，本文提出的基于智能电网环境下的认证密钥交换协议由三方组成，分别为智能电表、控制中心和服务提供商[25-26]。

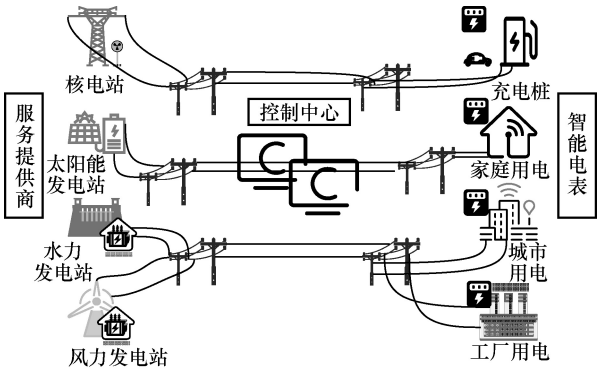


图 1 系统模型

1) 智能电表。智能电表广泛部署于智能电网的需求端（如家庭用电、充电桩等），主要用于收集电力数据，如用电负载、用电量，并将这些数据以及故障信息定期发送给控制中心。这些信息对于控制中心智能调度非常重要。

2) 控制中心。类似于网关和聚合器，控制中心可整合智能电表的数据、估算功耗、智能调控电力服务以及动态定价，从而节省能源、降低电费。

3) 服务提供商。服务提供商部署于智能电网的供给端（如风力发电站、太阳能发电站等），提供能源服务，向控制中心发送发电容量数据以及故障信息等，便于控制中心智能调度。需要注意的是，本文只考虑服务提供商的数据收集、通信元件，不考虑其电力生产元件。

1.4 安全模型

本文采用经典 DY（Dolev-Yao）模型[27]来评估协议的安全性。该模型假设协议中所使用的密码学原语都是安全的，并且攻击者可以截取、篡改、删除、存储和重放来自公开信道的任何消息。除此之外，在智能电网的场景下，本文还额外假设攻击者能够捕获传感器节点，继而发起侧信道攻击以获取节点秘密数据。

2 基于 PUF 的三方认证密钥交换协议

本节详细描述所提三方认证密钥交换协议。协议分为智能电表注册阶段、服务提供商注册阶段以及认证密钥交换阶段 3 个阶段。其中，注册阶段采用安全信道，认证密钥交换阶段基于公开信道。这里，本文给定以下假设。

1) 制造商在制造智能设备的过程中，已经将 PUF 嵌入该设备的集成电路（IC）中，并且每一个设备对应的 PUF 具有唯一性。

2) 控制中心计算能力较强并且是安全可信的，既可以完成复杂计算，又能保证其内部服务器或数据库的安全。

3) 智能电表和服务提供商为资源受限设备。本文协议中所使用的符号说明如表 1 所示。

表 1 符号说明

符号	描述
$\mathrm{ID}_i, \mathrm{ID}_j$	智能电表或服务提供商的身份标识
$\mathrm{TID}_i, \mathrm{TID}_j$	智能电表或服务提供商的伪身份
T_n	第 n 个时间戳
r_n	第 n 个随机数
s	控制中心的主密钥
$h_1(\cdot), h_2(\cdot), h_3(\cdot)$	不同的哈希值
SK	会话密钥
$\langle C_i, R_i \rangle$	PUF 的“激励–响应”对

2.1 智能电表注册阶段

在部署之前，每个智能电表都需要向控制中心注册。智能电表 SM_i 提取其唯一身份标识（序列号）ID_i，并向控制中心 CC 发送 ID_i 以及注册请求 Req_i，接收到该请求后，控制中心选择随机数 a_i，并计算 $\mathrm{TID}_i = h_1(\mathrm{ID}_i \| s \| a_i)$ 作为 SM_i 的伪身份。控制中心随机生成激励 C_i，并将 C_i 和 TID_i 通过安全信道发送给智能电表 SM_i。接收到控制中心发送的消息后，智能电表 SM_i 输出响应 $R_i \leftarrow \mathrm{PUF}_i(C_i)$，并将其通过安全信道发送给控制中心。最后，智能电表 SM_i 将 C_i, TID_i 存储在其内存中，控制中心将 $\mathrm{ID}_i, \mathrm{TID}_i, a_i, \langle C_i, R_i \rangle$ 存储在数据库中的列表 $\mathcal{L}_1$ 上。

2.2 服务提供商注册阶段

服务提供商分布于智能电网的另一端，这些设备同样也需要在部署前向控制中心注册。该注册阶段与智能电表的注册阶段相同，这里不再详细描述。最终，服务提供商 SP_j 将 C_j, TID_j 存储在其内存中，控制中心将 $\mathrm{ID}_j, \mathrm{TID}_j, a_j, \langle C_j, R_j \rangle$ 存储在数据库中的列表 $\mathcal{L}_2$ 上。

2.3 认证密钥交换阶段

由于智能电网参与方主要通过不可靠的信道进行通信，因此参与者之间有必要进行相互认证并协商会话密钥。本节详细描述了参与方认证及密钥交换的过程，如图 2 所示。

1) $\mathrm{SM}_i \rightarrow \mathrm{CC}$。智能电表 SM_i 利用其内存中的激励 C_i，输出响应 $R_i \leftarrow \mathrm{PUF}_i(C_i)$。随后，$\mathrm{SM}_i$ 随机选取 2 个随机数 r_1, r_2，生成时间戳 T_1，并计算 $V_1 = h_1(\mathrm{ID}_i \| R_i) \oplus (r_1 \| r_2)$ 以及 $\mathrm{MAC}_1 = h_1(V_1 \| \mathrm{ID}_i \| R_i \| r_1 \| r_2 \| T_1)$，随后 SM_i 将消息 $M_1 \leftarrow \{V_1, \mathrm{MAC}_1, \mathrm{TID}_i, T_1\}$ 通过公开信道发送给控制中心。

2) $\mathrm{CC} \rightarrow \mathrm{SP}_j$。控制中心接收到智能电表的消息后，生成时间戳 T_2 并检查时间戳 T_1，然后通过 M_1 中的 TID_i 检索列表 $\mathcal{L}_1$，获取 SM_i 的 $\mathrm{ID}_i, \mathrm{TID}_i, \langle C_i, R_i \rangle$，计算 $(r_1' \| r_2') = V_1 \oplus h_1(\mathrm{ID}_i \| R_i)$ 以及 $\mathrm{MAC}_1' = h_1(V_1 \| \mathrm{TID}_i \| R_i \| r_1' \| r_2' \| T_1)$，并验证 $\mathrm{MAC}_1' = \mathrm{MAC}_1$ 是否成立。如果不成立，控制中心将中断认证密钥交换过程；反之，控制中心继续执行后续步骤。CC 根据 SM_i 相关信息以及用电需求，自主智能选择提供能源服务的 SP_j，并检索其数据库中的列表 $\mathcal{L}_2$，获取 SP_j 相关信息。随后，CC 随机生成 2 个随机数 r_3, r_4 并计算 $V_2 = h_2(\mathrm{ID}_j \| R_j) \oplus (r_1' \| r_3 \| r_4)$ 以及 $\mathrm{MAC}_2 = h_1(V_2 \| \mathrm{TID}_j \| R_j \| r_1' \| r_3 \| r_4 \| T_2)$。最后，CC 将消息 $M_2 \leftarrow \{V_2, \mathrm{MAC}_2, \mathrm{TID}_j, T_2\}$ 通过公开信道发送给服务提供商 SP_j。

3) $\mathrm{SP}_j \rightarrow \mathrm{CC}$。服务提供商 SP_j 同样先生成时间戳 T_3 并检查时间戳 T_2 的有效性，然后利用其内存中的激励 C_j，输出响应 $R_j \leftarrow \mathrm{PUF}(C_j)$。在此基础上，计算 $(r_1'' \| r_3' \| r_4') = V_2 \oplus h_2(\mathrm{ID}_j \| R_j)$ 以及 $\mathrm{MAC}_2' = h_1(V_2 \| \mathrm{TID}_j \| R_j \| r_1'' \| r_3' \| r_4' \| T_2)$ 并验证 $\mathrm{MAC}_2' = \mathrm{MAC}_2$ 是否成立。如果验证失败，SP_j 将中断认证密钥交换过程；反之，SP_j 继续执行后续步骤。SP_j 生成随机数 r_5，计算会话密钥 $\mathrm{SK} = h_1(r_1'' \| r_3' \| r_5)$。之后，$\mathrm{SP}_j$ 计算 $V_4 = r_5 \oplus h_3(r_4')$ 以及 $\mathrm{MAC}_3 = h_1(\mathrm{SK} \| V_4 \| R_j \| T_3)$。最后，$\mathrm{SP}_j$ 公开发送消息 $M_3 \leftarrow \{V_4, \mathrm{MAC}_3, T_3\}$。

4) $\mathrm{CC} \rightarrow \mathrm{SM}_i$。控制中心生成时间戳 T_4，检查 T_3 的有效性，通过 $r_5' = V_4 \| h_3(r_4)$ 恢复出随机数 r_5'，并计算会话密钥 $\mathrm{SK}' = h_1(r_1' \| r_3 \| r_5')$ 以及 $\mathrm{MAC}_3' = h_1(\mathrm{SK}' \| V_4 \| R_j \| T_3)$。控制中心通过验证 $\mathrm{MAC}_3' = \mathrm{MAC}_3$ 是否成立来确定消息的完整性。如果验证失败，则中断协议执行；反之，CC 计算 $V_5 = h_1(r_2') \oplus (r_3 \| r_5')$ 和 $\mathrm{MAC}_4 = h_1(\mathrm{SK}' \| V_5 \| R_i \| T_4)$。最终，CC 将消息 $M_4 \leftarrow \{V_5, \mathrm{MAC}_4, T_4\}$ 发送给智能电表 SM_i。

5) 智能电表 SM_i 首先检查时间戳 T_4，随后使用接收到的 V_5 计算 $(r_3'' \| r_5'') = V_5 \oplus h_1(r_2)$ 以及 $\mathrm{SK}'' = h_1(r_1 \| r_3'' \| r_5'')$。之后，$\mathrm{SM}_i$ 计算并验证 $\mathrm{MAC}_4' = h_1(\mathrm{SK}'' \| V_5 \| R_i \| T_4)$ 是否等于 MAC_4。若验证成功，则认证密钥交换阶段完成；反之，中断执行。

3 安全性分析

3.1 BAN 逻辑证明

BAN 逻辑[28]在认证协议的形式化分析中被广泛应用。本节采用 BAN 逻辑证明协议可以实现相互认证。表 2 给出了 BAN 逻辑符号和含义，表 3 给出了 BAN 逻辑规则。

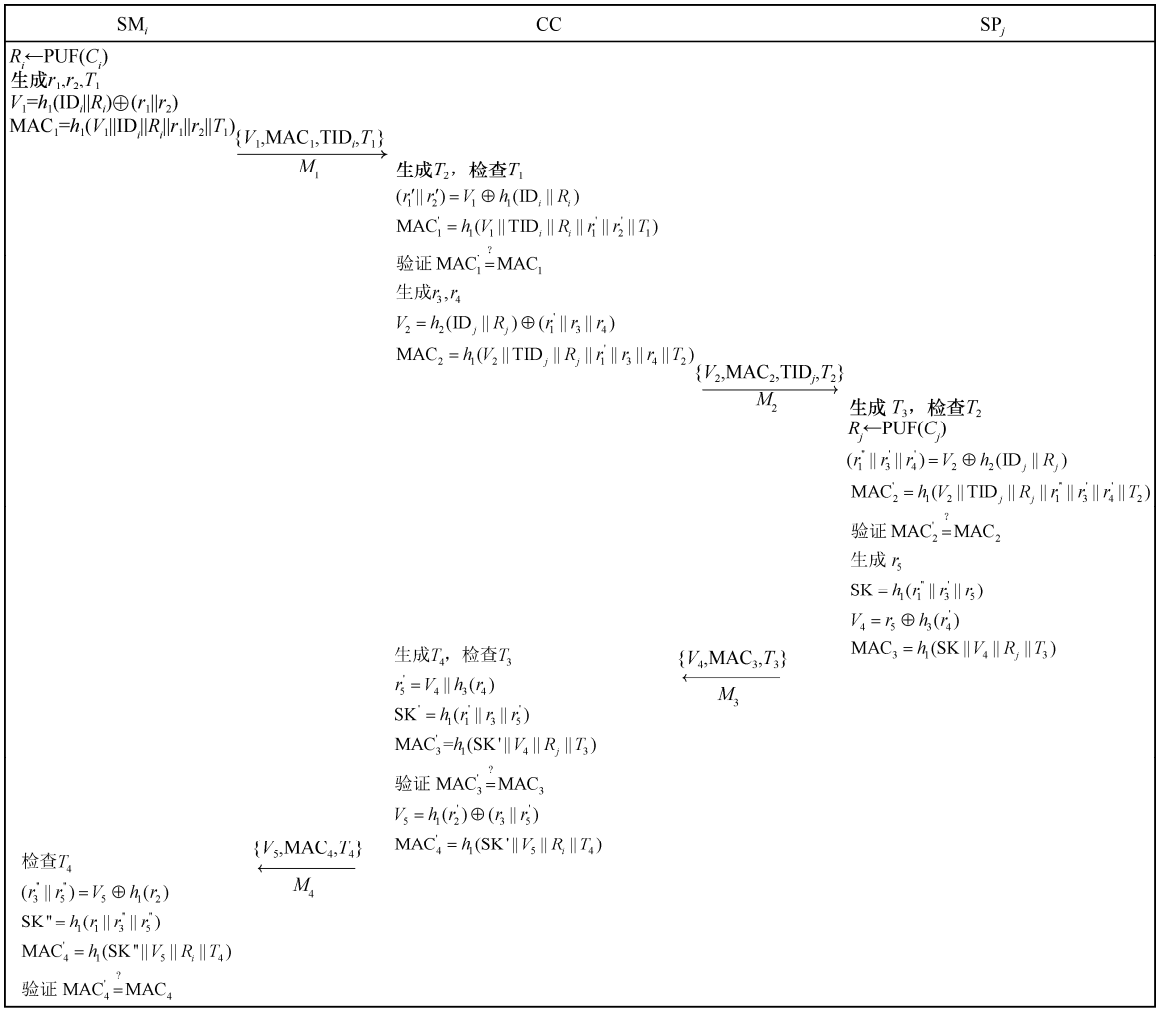


图 2　认证及密钥交换过程

表 2　　BAN 逻辑符号和含义

符号	含义
$P\mid\equiv X$	P 相信 X
$P\lhd X$	P 曾经收到包含 X 的消息
$P\mid\sim X$	P 曾经发送包含 X 的消息
$\#X$	X 是新鲜的
$P\mid\Rightarrow X$	P 对 X 有管辖权
$P\xleftrightarrow{K}Q$	P 和 Q 之间共享密钥 K
$P\overset{X}{\rightleftharpoons}Q$	P 和 Q 之间共享秘密 X
$\langle X\rangle_K$	使用 K 加密 X

表 3　　BAN 逻辑规则

标记	含义	计算式
R_1	消息含义规则	$\dfrac{P\mid\equiv Q\xleftrightarrow{K}P,P\lhd\{X\}_K}{P\mid\equiv Q\mid\sim X}$
R_2	管辖权规则	$\dfrac{P\mid\equiv Q\mid\Rightarrow X,P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$
R_3	Nonce 验证规则	$\dfrac{P\mid\equiv\#(X),P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$
R_4	新鲜度规则	$\dfrac{P\mid\equiv\#(X)}{P\mid\equiv\#(X,Y)}$
R_5	信念规则	$\dfrac{P\mid\equiv(X),P\mid\equiv(Y)}{P\mid\equiv(X,Y)},\dfrac{P\mid\equiv Q\mid\equiv(X,Y)}{P\mid\equiv Q\mid\equiv X}$

1) 进行 BAN 逻辑分析的理想化前提如下。

消息 1：

$$\mathrm{SM}_i\rightarrow\mathrm{CC}:\left\langle V_1,\mathrm{MAC}_1\right\rangle_{\mathrm{SM}_i\xleftrightarrow{R_i}\mathrm{CC}},\mathrm{TID}_i,T_1$$

消息 2：

$$\mathrm{CC}\rightarrow\mathrm{SP}_j:\left\langle V_2,\mathrm{MAC}_2\right\rangle_{\mathrm{SP}_j\xleftrightarrow{R_j}\mathrm{CC}},\mathrm{TID}_j,T_2$$

消息 3：

$$\mathrm{SP}_j\rightarrow\mathrm{CC}:\left\langle V_3,\mathrm{MAC}_3\right\rangle_{\mathrm{SP}_j\xleftrightarrow{R_j}\mathrm{CC}},\ T_5$$

消息 4：

$$\mathrm{CC}\rightarrow\mathrm{SM}_i:\left\langle V_4,\mathrm{MAC}_4\right\rangle_{\mathrm{SM}_i\xleftrightarrow{R_i}\mathrm{CC}},\ T_4$$

2) 需要证明的安全目标如下。

GOAL1：$\mathrm{SM}_i \mid\equiv (\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL2：$\mathrm{CC}\left|\equiv \mathrm{SM}_i\right| \equiv (\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL3：$\mathrm{CC} \mid\equiv (\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL4：$\mathrm{SM}_i \left|\equiv \mathrm{CC}\right| \equiv (\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL5：$\mathrm{SP}_j \mid\equiv (\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL6：$\mathrm{CC}\left|\equiv \mathrm{SP}_j\right| \equiv (\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL7：$\mathrm{CC} \mid\equiv (\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

GOAL8：$\mathrm{SP}_j \left|\equiv \mathrm{CC}\right| \equiv (\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$

3) 本文协议的初始假设定义如下。

A1：$\mathrm{SM}_i \mid\equiv \#(r_1, r_2, r_3, r_4, r_5)$

A2：$\mathrm{SP}_j \mid\equiv \#(r_1, r_2, r_3, r_4, r_5)$

A3：$\mathrm{CC} \mid\equiv \#(r_1, r_2, r_3, r_4, r_5)$

A4：$\mathrm{SM}_i \mid\equiv \left(\mathrm{SM}_i \overset{R_1}{\longleftrightarrow} \mathrm{CC}\right)$

A5：$\mathrm{CC} \mid\equiv \left(\mathrm{SM}_i \overset{R_1}{\longleftrightarrow} \mathrm{CC}\right)$

A6：$\mathrm{SM}_i \left|\equiv \mathrm{CC}\right| \Rightarrow \left(\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$

A7：$\mathrm{CC}\left|\equiv \mathrm{SM}_i\right| \Rightarrow \left(\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$

A8：$\mathrm{SP}_j \mid\equiv \left(\mathrm{SP}_j \overset{R_1}{\longleftrightarrow} \mathrm{CC}\right)$

A9：$\mathrm{CC} \mid\equiv \left(\mathrm{SP}_j \overset{R_j}{\longleftrightarrow} \mathrm{CC}\right)$

A10：$\mathrm{SP}_j \left|\equiv \mathrm{CC}\right| \Rightarrow \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$

A11：$\mathrm{CC}\left|\equiv \mathrm{SP}_j\right| \Rightarrow \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$

4) 证明过程如下。

S1：由消息 1 可得到 $\mathrm{CC} \triangleleft \left(V_1, \mathrm{MAC}_{1_{\mathrm{SM}_i \overset{R_1}{\longleftrightarrow} \mathrm{CC}}}, \mathrm{TID}_i, T_1\right)$。

S2：根据 A5 和 R1，得到 $\mathrm{CC}\left|\equiv \mathrm{SM}_i\right| \sim \left(V_1, \mathrm{MAC}_1, \mathrm{TID}_i, T_1\right)$。

S3：根据 A3 和 R4，得到 $\mathrm{CC} \mid\equiv \#\left(V_1, \mathrm{MAC}_1,\right) \mathrm{TID}_i, T_1)$。

S4：根据 S2、S3 和 R3，得到 $\mathrm{CC}\left|\equiv \mathrm{SM}_i\right| \equiv \left(V_1, \mathrm{MAC}_1, \mathrm{TID}_i, T_1\right)$。

S5：根据 S4 和 A5，推导出 $\mathrm{CC}\left|\equiv \mathrm{SM}_i\right| \equiv \left(\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL2。

S6：根据 S4、S5 和 R2，可得 $\mathrm{CC} \mid\equiv \left(\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL3。

S7：根据消息 2 可得到 $\mathrm{SP}_j \triangleleft \left(\left\langle V_2, \mathrm{MAC}_2\right\rangle_{\mathrm{SP}_j \overset{R_j}{\longleftrightarrow} \mathrm{CC}}, \mathrm{TID}_j, T_2\right)$。

S8：根据 A8 和 R1，得到 $\mathrm{SP}_j \left|\equiv \mathrm{CC}\right| \sim \left(V_2, \mathrm{MAC}_2, \mathrm{TID}_j, T_2\right)$。

S9：根据 A2 和 R4，得到 $\mathrm{SP}_j \mid\equiv \#\left(V_2, \mathrm{MAC}_2, \mathrm{TID}_j, T_2\right)$。

S10：根据 S8、S9 和 R3，得到 $\mathrm{SP}_j \left|\equiv \mathrm{CC}\right| \equiv \left(V_2, \mathrm{MAC}_2, \mathrm{TID}_j, T_2\right)$。

S11：根据 S10 和 A8，推导出 $\mathrm{SP}_j \left|\equiv \mathrm{CC}\right| \equiv \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL8。

S12：根据 S10、S11 和 R2，可得 $\mathrm{SP}_j \mid\equiv \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL5。

S13：根据消息 3 可得到 $CC \triangleleft \left(\left\langle V_3, \mathrm{MAC}_3\right\rangle_{\mathrm{SP}_j \overset{R_j}{\longleftrightarrow} \mathrm{CC}}, T_3\right)$。

S14：根据 A9 和 R1，得到 $\mathrm{CC}\left|\equiv \mathrm{SP}_j\right| \sim \left(V_3, \mathrm{MAC}_3, T_3\right)$。

S15：根据 A3 和 R4，得到 $\mathrm{CC} \mid\equiv \#\left(V_3, \mathrm{MAC}_3, T_3\right.$。

S16：根据 S14、S15 和 R3，得到 $\mathrm{CC}\left|\equiv \mathrm{SP}_j\right| \equiv \left(V_3, \mathrm{MAC}_3, T_3\right)$。

S17：根据 S16 和 A9，推导出 $\mathrm{CC}\left|\equiv \mathrm{SP}_j\right| \equiv \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL6。

S18：根据 S16、S17 和 R2，可得 $\mathrm{CC} \mid\equiv \left(\mathrm{SP}_j \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL7。

S19：根据消息 4 可得到 $\mathrm{SM}_i \triangleleft \left(V_4, \mathrm{MAC}_{4_{\mathrm{SM}_i \overset{R_1}{\longleftrightarrow} \mathrm{CC}}}, T_4\right)$。

S20：根据 A4 和 R1，得到 $\mathrm{SM}_i \left|\equiv \mathrm{CC}\right| \sim \left(V_4, \mathrm{MAC}_4, T_4\right)$。

S21：根据 A1 和 R4，得到 $\mathrm{SM}_i \mid\equiv \#\left(V_3, \mathrm{MAC}_4, T_4\right)$。

S22：根据 S20、S21 和 R3，得到 $\mathrm{SM}_i \left|\equiv \mathrm{CC}\right| \equiv \left(V_4, \mathrm{MAC}_4, T_4\right)$。

S23：根据 S22 和 A4，推导出 $\mathrm{SM}_i \left|\equiv \mathrm{CC}\right| \equiv \left(\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC}\right)$，即 GOAL4。

S24：根据 S22，S23 和 R2，可得 $\mathrm{SM}_i \mid\equiv (\mathrm{SM}_i \overset{\mathrm{SK}}{\longleftrightarrow} \mathrm{CC})$，即 GOAL1。

3.2 非形式化证明

3.2.1 相互认证性

协议实现了智能电表 SM_i 和控制中心 CC 之间，

以及控制中心 CC 和服务提供商 SP_j 之间的相互认证。CC 分别通过验证 $MAC'_1 = MAC_1$ 与 $MAC'_3 = MAC_3$ 是否成立来认证 SM_i 和 SP_j 的身份，同样，SM_i 和 SP_j 通过验证 $MAC'_4 = MAC_4$ 与 $MAC'_2 = MAC_2$ 来认证 CC 的身份。因为 MAC'_1 和 MAC'_4 的计算中涉及 SM_i 的秘密值 R_i，MAC'_2 和 MAC'_3 的计算中涉及 SP_j 的秘密值 R_j，而这 2 个值对于敌手 $\mathcal{A}$ 来说都是未知的，因此其不能冒充合法参与者通过身份认证。

3.2.2 匿名性

假设敌手 $\mathcal{A}$ 可能会试图通过捕获智能电表 SM_i 和服务提供商 SP_j 的身份信息 ID_i 和 ID_j 跟踪两者的通信。然而，在本文协议中，身份信息 ID_i 和 ID_j 分别通过随机数 $(r_1 \| r_2)$、$(r_1 \| r_3 \| r_4)$ 以及异或运算加密。因此，敌手 $\mathcal{A}$ 无法捕获智能电表 SM_i 和服务提供商 SP_j 的真实身份信息 ID_i 和 ID_j。

3.2.3 抗克隆和物理攻击

假设敌手 $\mathcal{A}$ 可以尝试篡改 SM_i、SP_j 的内存或者实施侧信道攻击获取内存中存储的数据[29]。然而，这种尝试将改变 PUF 的功能，敌手将获得无法产生任何输出的 PUF。因此，敌手的这种尝试将变得毫无意义。因为物理不可克隆函数具有不可复制的性质，所以本文协议能抵抗克隆和物理攻击。

3.2.4 抗伪装攻击

假设敌手 $\mathcal{A}$ 截取智能电表 SM_i 向控制中心发送的消息 $M_1 \leftarrow \{V_1, MAC_1, TID_i, T_1\}$，然后试图伪装成 SM_i 重新发送篡改后的消息，它必须重新计算 V_1 和 MAC_1。然而，V_1 和 MAC_1 中涉及秘密值 ID_i 与 R_i。通过前述匿名性、抗克隆和物理攻击分析可知，敌手无法获得这些秘密值，因此，所提协议可以抵抗智能电表伪装攻击。类似地，敌手也无法成功冒充控制中心 CC 和服务提供商 SP_j。

3.2.5 抗重放攻击

本文协议引入了时间戳 $T_n (n = 1,2,3,\cdots)$，参与方会检查时间戳的有效性，因此敌手 $\mathcal{A}$ 无法直接转发消息发起重放攻击。并且，在本文协议中，每个时间戳都添加到消息验证码 MAC_n $(n = 1,2,3,\cdots)$ 中，若敌手 $\mathcal{A}$ 通过替换新的时间戳发起重放攻击，则 MAC_n 无法通过验证，导致参与方会中断协议的执行。因此，本文协议可以抵抗重放攻击。

3.2.6 抗 DoS 攻击

拒绝服务（DoS）攻击意味着攻击者可以发送大量的非法消息来消耗实体的计算资源[30]。如前文所述，每个参与方都会检查时间戳 T_n 的有效性并且验证消息验证码 MAC_n。任何一个验证不成功，参与方都会终止协议的执行。因此，本文协议能够抵抗 DoS 攻击。

3.2.7 关于 CRP 泄露攻击

在 CRP 泄露攻击中，敌手首先收集足够多的 CRP 子集，然后试图从这些 CRP 中创建数据模型以预测 PUF 对新“激励”的“响应”。然而在本文协议中，智能电表端和服务提供商端都只保存了激励 C。而认证阶段所需的响应 R 都是在协议运行时临时生成的。因此，本文协议从根本上规避了 CRP 泄露攻击。

4 安全与性能对比

本节从安全性、计算量和通信开销 3 个方面，将本文协议与 Irshad 等[13]和 Chen 等[14]的三方认证方案进行比较。其中，Irshad 等[13]采用生物信息和智能卡来保证密钥的安全性，网关参与认证及密钥协商过程。Chen 等[14]采用椭圆曲线 Diffie-Hellman 密钥交换协议和智能卡来保证密钥的安全性，同时身份信息被加密来保证匿名性。其中，网关只协助认证，不参与密钥的协商。

4.1 安全性对比

表 4 对比了各方案的安全性。其中，“Y”表示方案可以抵抗攻击；“N”表示方案无法抵抗攻击。从表 4 可以看出，本文协议具有更好的安全性。

表 4 安全性对比

安全属性	方案		
	本文协议	Irshad 等方案	Chen 等方案
相互认证性	Y	Y	Y
匿名性	Y	Y	Y
抗克隆和物理攻击	Y	N	N
抗伪装攻击	Y	Y	N
抗重放攻击	Y	Y	N
抗 DoS 攻击	Y	Y	Y
会话密钥安全	Y	Y	Y

4.2 计算开销对比

为统一计算开销的评判标准，本文参考文献[31]

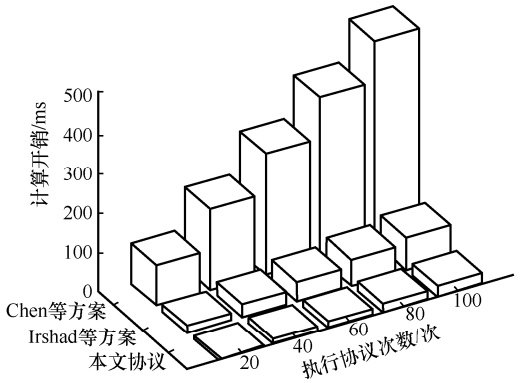
中的统计结果，Gope 等[31]使用基于 ARM Cortex-A9 MPCore 890 MHz CPU、Android 5.1 系统、4 GB RAM 的设备模拟资源受限设备，同时使用基于 Intel Core i5-4300 2.9 GHz CPU、Ubuntu 12.04 系统、16 GB RAM 的设备模拟非资源受限设备，使用 JPBC 库计算上述方案中密码运算的执行时间，如表 5 所示。上述方案计算开销对比如表 6 及图 3(a)所示。

表 5　　密码运算的执行时间

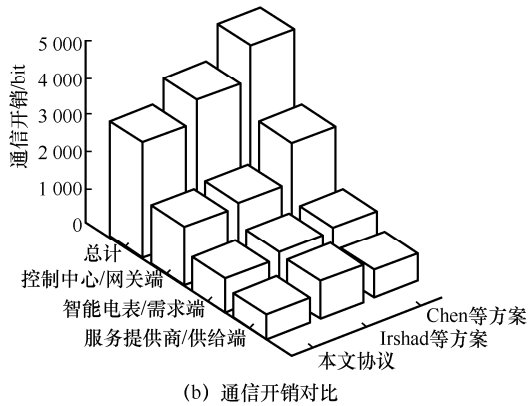
符号	描述	执行时间/ms	
		资源受限设备	非资源受限设备
T_h	Hash 操作所需时间	0.018 6	0.011 0
T_{mul}	椭圆曲线点乘运算所需时间	0.925 5	0.135 2
T_{bio}	生物信息计算所需时间	0.535 0	—

表 6　　计算开销对比

方案	计算开销/ms			
	智能电表/需求端	控制中心/网关端	服务提供商/供给端	总计
本文协议	$5T_h \approx 0.093\ 0$	$9T_h \approx 0.099\ 0$	$5T_h \approx 0.093\ 0$	0.285 0
Irshad 等方案	$7T_h + T_{bio} \approx 0.665\ 2$	$2T_h \approx 0.022\ 0$	$6T_h \approx 0.111\ 6$	0.798 8
Chen 等方案	$5T_h + 3T_{mul} \approx 2.869\ 5$	$7T_h + T_{mul} \approx 0.212\ 2$	$3T_h + 2T_{mul} \approx 1.906\ 8$	4.988 5



(a) 计算开销对比



(b) 通信开销对比

图 3　性能分析

4.3　通信开销对比

通信开销是指参与者在完成认证过程时交换或传输的数据量。这里，本文统一做出如下假设：随机数、身份标识以及时间戳长度为 160 bit，加解密以及哈希函数的输出为 256 bit，椭圆曲线点为 512 bit。各方案中智能电表/需求端、控制中心/网关端和服务提供商/供给端所需的通信开销对比如表 7 及图 3(b)所示。

5　结束语

针对智能电网环境下智能电表、控制中心和服务提供商三方之间的身份认证和会话密钥交换问题，本文提出了一个新的认证密钥交换协议。安全性分析证明，本文协议不仅能抵抗常见的网络攻击，还能抵抗物理攻击。另外，本文协议运行过程中不需要用户实时参与，并且具有较高的运行性能。因此，本文协议在智能电网环境下更加安全、实用和高效。

参考文献：

[1] 发展改革委, 能源局. 关于促进智能电网发展的指导意见[J]. 中华人民共和国国务院公报, 2015(33): 72-76.
National Development and Reform Commission, National Energy Administration. Guiding opinions of energy bureau of development and reform commission on promoting the development of smart grid[J]. Gazette of the State Council of the People's Republic of China, 2015(33): 72-76.

[2] TUBALLA M L, ABUNDO M L. A review of the development of

表 7　　通信开销对比

方案	通信开销/bit			
	智能电表/需求端	控制中心/网关端	服务提供商/供给端	总计
本文协议	928	1 600	672	3 200
Irshad 等方案	1 184	2 784	768	4 736
Chen 等方案	1 088	1 696	1 024	3 808

smart grid technologies[J]. Renewable and Sustainable Energy Reviews, 2016, 59: 710-725.
[3] 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.
LA Y, ZHAO J G, ZHANG W. Security authentication scheme for power terminals based on the SM9 threshold signature[J]. Journal of Electric Power Science and Technology, 2022, 37(4): 183-188, 226.
[4] 丁志帆, 胡洪波, 杨庆余, 等. 安全增强的智能电网轻量级匿名认证方案[J]. 计算机应用研究, 2022, 39(10): 3124-3129, 3135.
DING Z F, HU H B, YANG Q Y, et al. Security enhanced lightweight anonymous authentication scheme for smart grid[J]. Application Research of Computers, 2022, 39(10): 3124-3129, 3135.
[5] KUMAR N, KAUR K, MISRA S C, et al. An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud[J]. Peer-to-Peer Networking and Applications, 2016, 9(5): 824-840.
[6] ANDERSON R, FULORIA S. Who controls the off switch? [C]// Proceedings of 2010 First IEEE International Conference on Smart Grid Communications. Piscataway: IEEE Press, 2010: 96-101.
[7] WU D P, ZHOU C. Fault-tolerant and scalable key management for smart grid[J]. IEEE Transactions on Smart Grid, 2011, 2(2): 375-381.
[8] XIA J Y, WANG Y G. Secure key distribution for the smart grid[J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1437-1443.
[9] WAZID M, DAS A K, KUMAR N, et al. Secure three-factor user authentication scheme for renewable-energy-based smart grid environment[J]. IEEE Transactions on Industrial Informatics, 2017, 13(6): 3144-3153.
[10] MAHMOOD K, CHAUDHRY S A, NAQVI H, et al. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication[J]. Future Generation Computer Systems, 2018, 81: 557-565.
[11] ABBASINEZHAD-MOOD D, NIKOOGHADAM M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications[J]. Future Generation Computer Systems, 2018, 84: 47-57.
[12] CHEN Y W, MARTÍNEZ J F, CASTILLEJO P, et al. A bilinear map pairing based authentication scheme for smart grid communications: PAuth[J]. IEEE Access, 2019, 7: 22633-22643.
[13] IRSHAD A, USMAN M, CHAUDHRY S A, et al. A provably secure and efficient authenticated key agreement scheme for energy Internet-based vehicle-to-grid technology framework[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4425-4435.
[14] CHEN Y W, MARTÍNEZ J F, CASTILLEJO P, et al. A privacy protection user authentication and key agreement scheme tailored for the Internet of things environment: PriAuth[J]. Wireless Communications and Mobile Computing, 2017, 2017: 1-17.
[15] GAO Y S, AL-SARAWI S F, ABBOTT D. Physical unclonable functions[J]. Nature Electronics, 2020, 3(2): 81-91.
[16] 王振宇, 郭阳, 李少青, 等. 面向轻量级物联网设备的高效匿名身份认证协议设计[J]. 通信学报, 2022, 43(7): 49-61.
WANG Z Y, GUO Y, LI S Q, et al. Design of efficient anonymous identity authentication protocol for lightweight IoT devices[J]. Journal on Communications, 2022, 43(7): 49-61.
[17] 贺章擎, 李红, 万美琳, 等. 一种基于 PUF 的两方认证与会话密钥交换协议[J]. 计算机工程与应用, 2018, 54(18): 17-21.
HE Z Q, LI H, WAN M L, et al. Authentication and session key exchange protocol based on Physical Uncolonable Function[J]. Computer Engineering and Applications, 2018, 54(18): 17-21.
[18] 夏艳东, 戚荣鑫, 季赛. 工业物联网中基于 PUFs 轻量级的密钥交换协议研究[J]. 计算机应用与软件, 2022, 39(3): 316-321.
XIA Y D, QI R X, JI S. Pufs-based lightweight key exchange protocol in iiot[J]. Computer Applications and Software, 2022, 39(3): 316-321.
[19] LIYANAGE M, BRAEKEN A, KUMAR P, et al. IoT security: advances in authentication[M]. New Jersey: John Wiley & Sons, 2020.
[20] BIAN W X, GOPE P, CHENG Y Q, et al. Bio-AKA: an efficient fingerprint based two factor user authentication and key agreement scheme[J]. Future Generation Computer Systems, 2020, 109: 45-55.
[21] 韩丽娟, 钱蕾, 姚恩义, 等. 基于电平转换器的物理不可克隆函数电路设计[J]. 网络与信息安全学报, 2021, 7(2): 86-93.
HAN L J, QIAN L, YAO E Y, et al. Novel level shifter based physical unclonable function circuit design[J]. Chinese Journal of Network and Information Security, 2021, 7(2): 86-93.
[22] BROWN D R L. Generic groups, collision resistance, and ECDSA[J]. Designs, Codes and Cryptography, 2005, 35(1): 119-152.
[23] SAHOO S S, MOHANTY S, MAJHI B. Improved biometric-based mutual authentication and key agreement scheme using ECC[J]. Wireless Personal Communications, 2020, 111(2): 991-1017.
[24] RAWAT G S, SINGH K, ARSHAD N I, et al. A lightweight authentication scheme with privacy preservation for vehicular networks[J]. Computers and Electrical Engineering, 2022, 100: 108016.
[25] ZHU L H, LI M, ZHANG Z J, et al. Privacy-preserving authentication and data aggregation for fog-based smart grid[J]. IEEE Communications Magazine, 2019, 57(6): 80-85.
[26] LU R X, LIANG X H, LI X, et al. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1621-1631.
[27] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.
[28] BURROWS M, ABADI M, NEEDHAM R M. A logic of authentication[J]. Mathematical and Physical Sciences, 1989, 426(1871): 233-271.
[29] KOCHER P C, JAFFE J, JUN B. Differential power analysis[C]//Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. New York: ACM Press, 1999: 388-397.
[30] WU T Y, LEE Y Q, CHEN C M, et al. An enhanced pairing-based authentication scheme for smart grid communications[J]. Journal of Ambient Intelligence and Humanized Computing, 2021: doi.org/10.1007/s12652-020-02740-2.
[31] GOPE P, SIKDAR B. An efficient privacy-preserving authentication scheme for energy Internet-based vehicle-to-grid communication[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 6607-6618.

[作者简介]

王圣宝（1978– ），男，江西鄱阳人，博士，杭州师范大学副教授、硕士生导师，主要研究方向为密码协议、公钥加密、数据安全等。

周鑫（1997– ），男，安徽六安人，杭州师范大学硕士生，主要研究方向为物联网安全、认证密钥交换协议和安全多方计算等。

文康（1999– ），男，湖南衡阳人，杭州师范大学硕士生，主要研究方向为认证密钥交换协议和车联网安全等。

翁柏森（1997– ），男，浙江杭州人，杭州师范大学硕士生，主要研究方向为认证密钥交换协议和智能电网安全等。