doi:10.11835/j.issn.1000-582X.2025.10.010
引用格式:陈萌萌,伦迪,李鸣岩.面向电力物联网的RFID认证方案[J].重庆大学学报,2025,48(10):110-118.

面向电力物联网的RFID认证方案

陈萌萌[1],伦　迪[2],李鸣岩[3]
(1.河南九域腾龙信息工程有限公司,郑州 450000;2.国网河南省电力公司信息通信分公司,郑州 450000;
3.国网河南省电力公司电力科学研究院,郑州 450000)

摘要:随着电力物联网技术的快速发展,建设能源互联网具有重大意义。电力物联终端设备的识别认证是保障能源互联网安全稳定运行的基础。为实现海量电力终端设备信息高效采集与安全认证,研究提出一种面向电力物联网的RFID(radio frequency identification)认证方案,该方案利用RFID技术,基于国密SM3和SM4设计算法,实现了阅读器与电力设备之间的相互认证,保障了电力通信数据的传输安全,降低设备标签的计算复杂度。安全性分析表明,该方案满足不可追踪性、抗重放攻击、抗去同步攻击、抗拒绝服务攻击等安全特性,BAN逻辑分析进一步表明该方案满足相互认证性。性能分析表明,该方案在标签计算量、存储量、通信量及数据库搜索效率方面具有较好的性能优势。

关键词:RFID;电力物联网;认证;国密算法;BAN逻辑
中图分类号:TP309　　**文献标志码:**A　　**文章编号:**1000-582X(2025)10-110-09

RFID authentication scheme for the electric power Internet of Things

CHEN Mengmeng[1], *LUN Di*[2], *LI Mingyan*[3]
(1. Henan Jiuyu Tenglong Information Engineering Co., Ltd., Zhengzhou 450000, P. R. China; 2. State Grid Henan Information & Telecommunication Company, Zhengzhou 450000, P. R. China; 3. State Grid Henan Electric Power Research Institute, Zhengzhou 450000, P. R. China)

Abstract: With the rapid advancement of electric power Internet of Things (EPIoT) technology, the development of a secure and efficient energy Internet has become increasingly important. Identification and authentication of electric power terminal devices are fundamental to ensuring the safe and stable operation of the energy Internet. To realize efficient data collection and secure authentication for a large number of terminal devices, this paper proposes an RFID-based authentication scheme for EPIoT. The scheme integrates RFID (radio frequency identification) technology with the national cryptographic algorithms SM3 and SM4, achieving mutual authentication between readers and terminal devices while ensuring secure transmission of power communication data and reducing computational overhead for device tags. Security analysis shows that the proposed scheme satisfies key security requirements, such as untraceability, resistance to replay attacks, de-synchronization attacks, and denial-of-service attacks. Further verification using BAN logic confirms the mutual authentication capability

收稿日期:2024-02-29　　**网络出版日期:**2025-07-14
基金项目:国家电网公司科技项目(521700250014-153-ZN)。
Supported by Science and Technology Projects of State Grid Corporation of China(521700250014-153-ZN).
作者简介:陈萌萌(1993—),女,硕士研究生,主要从事网络安全方向研究,(E-mail)2423772692@qq.com。

of the scheme, while performance analysis shows advantages in tag computation, storage, communication overhead, and database search efficiency.

Keywords: RFID; electric power Internet of Things; authentication; national cryptographic algorithms; BAN logic

随着互联网与信息技术的高速发展，能源互联网已经成为世界能源研究以及未来能源发展的必然趋势[1]，物联网技术作为智能电网密不可分的支撑技术，是电力行业研究的热点，两者的融合形成了“电力物联网”，对电网发展应用产生里程碑式的意义[2]。电力设备信息的采集是其中的重要环节，由于电力物联网涵盖的设施种类繁多，移动终端、智能采集终端等新型设备的大量接入必将带来终端设备安全认证问题。电力设备使用周期长、使用地点分散，从采购、调试、运行保养、维修到报废的整个寿命周期内会产生海量数据，这些数据需要大量人工进行统计、分析、处理，当设备出现变动时，须及时对设备信息进行更新，这对于设备运作和资产的监督管理都是较大考验[3]。当前，电力设备信息管理普遍依托于集中式存储服务器，对于变电站、输电线路、低压台区等各类设备的信息，其录入、修改及查阅等操作均需要通过后台服务器执行，由于业务量大，且不能实现随时随地查阅，给电力运维人员带来较大麻烦[4]。

射频识别RFID（radio frequency identification）是物联网中自动识别物体的一项关键技术，它在自动识别、定位和访问控制方面具有强大功能[5]，一个典型的RFID系统由后台数据库、阅读器和标签组成[6]，RFID电子标签使用寿命长，读取范围大，能工作在恶劣环境中。由于RFID系统具有高安全性，被广泛用于各种场景，如无现金支付、公共交通票务系统、住宅门钥匙等[7]。将RFID技术应用于电力物联网中，能有效支撑设备状态检测、用电信息采集、电力巡检、资产全生命周期管理、智能用电等环节，提高电力数据的安全性与可靠性。

由于电力物联网环境下的业务场景类型丰富，涉及大量物联终端设备的采集与认证，且传输数据种类繁杂，包括电量数据、杆塔数据、电力调度检修数据等敏感信息，因此，在设备数据采集时必须确保通信数据的安全可靠[8]。目前已有成熟的REID认证方案被应用于各类场景，如：车联网、智慧交通、医疗系统等，但现有方案无法满足电力环境的高保密性要求，需要设计一种面向电力物联网的RFID认证方案来实现设备高效认证与数据安全传输。

1　相关研究

目前，融合RFID技术与电力物联网方案被相继提出，Washiro[9]提出了在智能电网中将输电线技术与RFID技术相结合，将嵌有IC卡芯片的电器接入装有阅读器的插座，实现对电器的自动识别和检测控制；Chaimae等[10]提出了一种低电压、低配置成本、高可靠性的智能电网自动识别方法，该方法使用了低频和高频的RFID无源标签，有助于智能电网监测和控制电力消耗，也可以应用于智能家居等场景。Vaidya等[11]以智能电网为应用背景，基于RFID技术提出了一个轻量级的高效安全认证协议，该协议使用基本的散列函数、异或等简单的加密操作，在阅读器和后端服务器中使用椭圆曲线加密和零知识协议等技术，减少了网络认证成本；同时，该协议引入了集成认证技术实现基于智能电网的RFID3个实体验证。但该协议的计算复杂度较高，标签需要进行6次哈希和9次异或运算，以及2次随机数的生成，标签密钥一旦泄露，攻击者会利用标签密钥进行安全攻击。宗劲冲等[8]提出了一种基于hash函数的改进方案，涉及哈希及异或运算，验证了标签的合法性，但该协议利用传统的后端数据库，限制了阅读器的移动性。此外，基于RFID技术标准，Yeh[12]提出一种基于EPC（electronic product code）的RFID安全协议，保障了标签信息的安全性，但该协议容易遭受重放攻击（replay attack），存在数据完整性问题。

研究提出了面向电力物联网的射频识别认证方案，采用云数据库代替传统数据库，显著降低系统部署与维护成本，强大的存储容量满足实时认证海量标签的需求；方案利用国密算法实现阅读器与电力设备之间的双向身份认证，确保阅读器与云数据库之间传输数据的机密性与完整性；采用轻量级认证方式，降低了电力

设备标签的存储量、通信量及计算复杂度;通过索引查找方式提高了云数据库的搜索效率。

2 研究方案

综合考虑电力物联网环境下的终端设备安全认证,以及数据存储与传输安全等方面问题,设计了一种面向电力物联网的RFID认证方案,RFID系统组成包括:电力设备(内置电子标签)、阅读器和云数据库服务器,系统结构如图1所示,该架构中电力设备与阅读器、阅读器与云数据库服务器之间的通信信道均为不安全的开放信道。

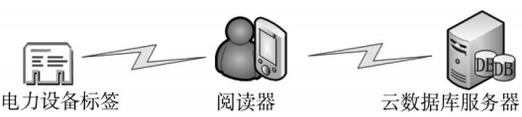

图1 面向电力物联网的RFID系统结构图

Fig.1 The architecture of RFID system for electric power Internet of Things

2.1 符号定义

方案中的符号定义如表1所示。

表1 符号定义

Table 1 Notations definition

符号	说明
T	设备
R	阅读器
C	云数据库服务器
id_T	设备标签身份标识
id_R	阅读器身份标识
secret	标签秘密值
kRC	阅读器与云服务器的共享认证密钥
k	阅读器密钥
r_i	一次性随机数
HMAC	利用HMAC-SM3生成的消息认证码
$h(\ )$	SM3国密算法
$E(\ )$	SM4国密算法
$\|\|$	字符串连接符
EHT	加密哈希表

2.2 协议初始化

1)电力设备标签。设备标签存储自己的身份标识id_T和秘密值secret;支持伪随机数生成,支持SM3国密算法。

2)阅读器。阅读器存储其身份标识id_R、对称加解密密钥k,以及与云服务器之间的共享认证密钥kRC;支持伪随机数生成,支持SM3、SM4国密算法、消息摘要运算操作。

3)云数据库服务器。云数据库服务器存储加密哈希表EHT(encrypt hash table)新旧值对:$\{h(\mathrm{id}_T||\mathrm{secret}),\ E_k(\mathrm{id}_T||\mathrm{secret})\}$,$\{h(\mathrm{id}_T||\mathrm{secert}_{\mathrm{old}}),\ E_k(\mathrm{id}_T||\mathrm{secert}_{\mathrm{old}})\}$,old表示旧秘密值,并令新旧值对相等;按对存储$(h(\mathrm{id}_R),\ \mathrm{kRC})$;支持查询操作及伪随机数生成,支持哈希函数、消息摘要运算操作。其中,共享认证密钥kRC与密钥k定期更新,以防密钥泄露后所产生的安全问题。

2.3　协议认证阶段

1）阅读器→标签：r_R。阅读器生成随机数r_R，向标签发送认证请求消息r_R。

2）标签→阅读器：$r_T \| \text{Auth1} \| \text{index}$

①标签收到消息r_R之后，生成随机数r_T；

②利用SM3算法计算$\text{Auth1} = h(r_R || \text{id}_T)$，$\text{index} = h(\text{id}_T \| \text{secret})$；

③发送$r_T \| \text{Auth1} \| \text{index}$至阅读器作为对其的回应。

3）阅读器→云数据库服务器：$r_T \| h(\text{id}_R) \| \text{index} \| \text{HMAC1}_{\text{kRC}}$

①阅读器存储标签发送的消息Auth1和r_T；

②将消息$r_T \| h(\text{id}_R) \| \text{index} \| \text{HMAC1}_{\text{kRC}}$发送至云服务器，其中，$\text{HMAC1}_{\text{kRC}}$即HMAC_SM3(kRC，$r_T \| h(\text{id}_R) || \text{index}$)，是对本条消息$r_T \| h(\text{id}_R) \| \text{index}$的认证。

4）云数据库服务器→阅读器：$r_T \| E_k(\text{id}_T \| \text{secret}) \| \text{HMAC2}_{\text{kRC}}$

①云数据库根据收到的$h(\text{id}_R)$搜索存储记录，如果能找到与之相符的记录，说明阅读器是合法的，根据$h(\text{id}_R)$找到对应的kRC，利用kRC验证$\text{HMAC1}_{\text{kRC}}$，确定来自阅读器的消息是否被篡改；

②云服务器在数据存储记录中查找是否存在与index相等的哈希值，查找结果有3种可能：

a.未找到匹配的哈希值，结束认证协议；

b.找到$h(\text{id}_T \| \text{secret})$与index相等，表明在上一轮认证会话中云服务器和标签都进行了正常的更新操作。云服务器发送$r_T \| E_k(\text{id}_T \| \text{secret}) \| \text{HMAC2}_{\text{kRC}}$至阅读器，其中，$\text{HMAC2}_{\text{kRC}}$即$\text{HMAC_SM3}(\text{kRC}, r_T \| E_k(\text{id}_T \| \text{secret}))$，是对本条消息$r_T \| E_k(\text{id}_T \| \text{secret})$的认证；

c.找到$h(\text{id}_T \| \text{secret}_{\text{old}})$与index相等，表明上一轮认证会话中云服务器进行了正常的更新操作，而标签没有正常更新；云服务器发送$r_T \| E_k(\text{id}_T \| \text{secret}_{\text{old}}) \| \text{HMAC2}_{\text{kRC}}$至阅读器，其中，$\text{HMAC2}_{\text{kRC}}$即$\text{HMAC_SM3}(\text{kRC}, r_T \| E_k(\text{id}_T || \text{secret}_{\text{old}}))$，是对本条消息$r_T \| E_k(\text{id}_T \| \text{secret}_{\text{old}})$的认证。

5）阅读器→云服务器：$r_R \| E \| H \| \text{HMAC3}_{\text{kRC}}$

①阅读器验证$\text{HMAC2}_{\text{kRC}}$，若验证通过，利用国密SM4算法对密文$E_k(\text{id}_T \| \text{secret})$进行解密，获得$\text{id}_T$和secret；

②计算$h(r_R || \text{id}_T)$，验证该哈希值与之前存储的Auth1是否相等，若验证通过，则成功认证电力设备标签；

③计算$\text{secret}_{\text{new}} = h(r_T || \text{secret})$，$E = E_k(\text{id}_T \| \text{secret}_{\text{new}})$，$H = h(\text{id}_T \| \text{secret}_{\text{new}})$，new代表新的秘密值；

④发送$r_R \| E \| H \| \text{HMAC3}_{\text{kRC}}$至云服务器，提醒其对存储的EHT进行更新。其中，$\text{HMAC3}_{\text{kRC}}$即$\text{HMAC_SM3}(\text{kRC}, r_R \| E \| H)$。

6）云数据库服务器→阅读器：$r_R \| \text{ACK} \| \text{HMAC4}_{\text{kRC}}$

①云数据库对$\text{HMAC3}_{\text{kRC}}$进行验证，验证通过后，更新存储的EHT新旧值对，令：$h(\text{id}_T \| \text{secret}_{\text{old}}) = h(\text{id}_T \| \text{secret})$，$h(\text{id}_T \| \text{secret}) = H$，$E_k(\text{id}_T \| \text{secret}_{\text{old}}) = E_k(\text{id}_T \| \text{secret})$，$E_k(\text{id}_T \| \text{secret}) = E$；

②发送更新完毕消息$r_R \| \text{ACK} \| \text{HMAC4}_{\text{kRC}}$至阅读器，其中，ACK为确认字符，$\text{HMAC4}_{\text{kRC}}$即$\text{HMAC_SM3}(\text{kRC}, r_R \| \text{ACK})$。

7）阅读器→标签：$r_R \| \text{Auth2}$

①阅读器收到消息$r_R \| \text{ACK} \| \text{HMAC4}_{\text{kRC}}$后，验证$\text{HMAC4}_{\text{kRC}}$，在确认云服务器完成更新后，计算$\text{Auth2} = h(r_R \| \text{secret}_{\text{new}})$，发送$r_R \| \text{Auth2}$至标签；

②标签收到$r_R \| \text{Auth2}$后，计算$\text{temp} = h(r_T \| \text{secret})$，然后计算$h(r_R \| \text{temp})$并验证与Auth2是否相等，若验证通过，则成功认证阅读器；

③标签更新其秘密值secret，令：secret=temp。

上述方案的协议流程如图2所示。

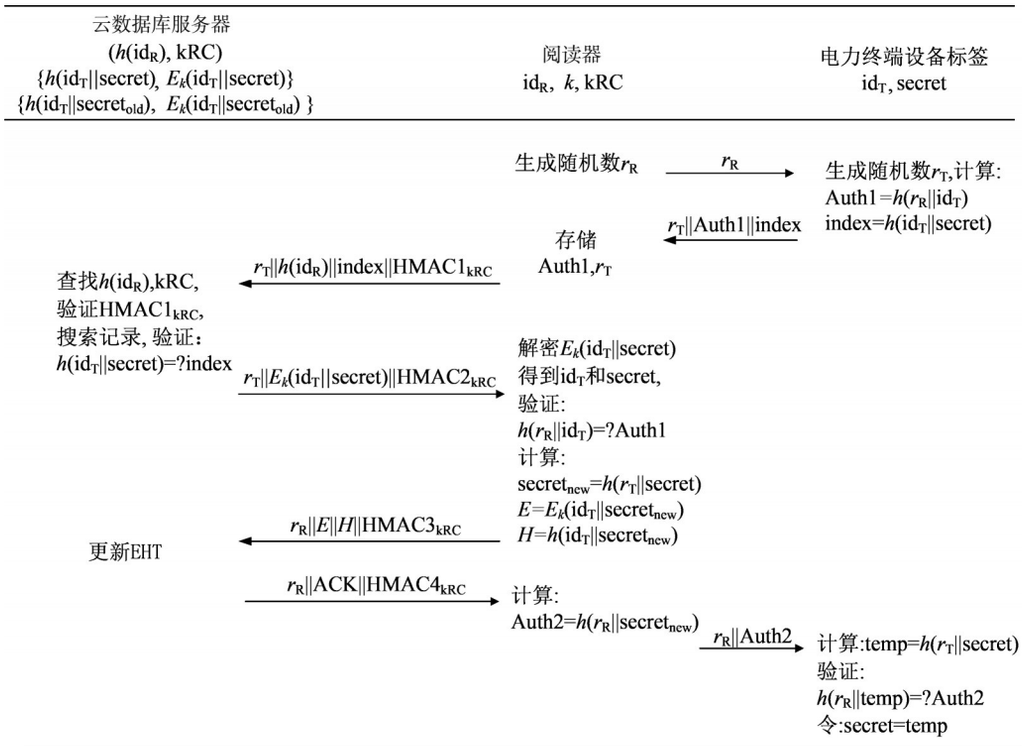

图2 面向电力物联网的RFID认证协议图

Fig.2 RFID authentication scheme for electric power Internet of Things

3 安全性及性能分析

3.1 安全目标分析

研究提出的面向电力物联网的RFID认证方案，不仅实现了阅读器与电力设备之间的双向身份认证，同时具备不可追踪性、抗重放攻击、抗去同步攻击、抗拒绝服务攻击等安全特性，具体分析如下。

3.1.1 不可跟踪性

在阅读器和标签的每次会话请求中，使用新鲜的随机数可以保证标签的不可追踪性[13]。在本方案中，阅读器与电力设备标签均会生成一次性随机数r_R或r_T，且标签秘密值secret在每次认证成功后均会进行更新。标签收到r_R后，计算Auth1=$h(r_R||id_T)$，index=$h(id_T||secret)$，并发送$r_T||Auth1||index$给阅读器。即使攻击者监听了通信信道，其每次截获的会话信息也均不相同，无法将不同会话关联到同一标签，满足了不可追踪性的安全要求。

3.1.2 相互认证性

即阅读器和标签可以在协议的运行过程中进行相互认证[14]。在本方案中，阅读器接收并存储来自电力设备标签的消息Auth1=$h(r_R||id_T)$和r_T，解密云服务器发送过来的密文信息$E_k(id_T||secret)$，得到id_T和secret，计算哈希值$h(r_R||id_T)$，如果与Auth1相等，则成功认证标签；电力设备标签接收来自阅读器的消息Auth2=$h(r_R||secret_{new})$，计算temp=$h(r_T||secret)$和$h(r_R||temp)$并验证与Auth2是否相等，若相等，则成功认证阅读器。

3.1.3 重放攻击

攻击者在截获了之前的通信消息后，可以重放该消息以通过通信实体的验证[15]。在本方案中，阅读器、电力设备标签分别生成会话随机数r_R和r_T，标签秘密值secret在每次认证后均会更新，每轮会话的随机数与秘密值均不相同，每次交互生成的认证消息具有唯一性与时效性，可有效抵御重放攻击。

3.1.4　去同步攻击

攻击者使用一些方法，比如阻断上一条消息，使后端服务器和有效标签分享不同秘密[16]。在本方案中，标签秘密值secret每使用一次将会更新为新的值，云数据库索引值$h(\mathrm{id_T}\|\mathrm{secert})$随之更新。更新规则为：云服务器先进行更新，标签后进行更新。若网络攻击或故障导致标签更新失败，此时，由于云数据库中存储了包含标签旧秘密值信息的EHT新旧值对：$\{h(\mathrm{id_T}\|\mathrm{secert}),E_k(\mathrm{id_T}\|\mathrm{secert})\},\{h(\mathrm{id_T}\|\mathrm{secert_{old}}),E_k(\mathrm{id_T}\|\mathrm{secert_{old}})\}$，在下一轮认证中，系统可基于旧值顺利进行认证，重新恢复同步。

3.1.5　拒绝服务攻击

攻击者可以通过伪造消息和重放消息实施拒绝服务攻击[17]。在本方案中，阅读器与云服务器共享认证密钥kRC，通信消息中包含一次性随机数，方案通过HMAC-SM3算法对传输信息和随机数进行验证，可以抵抗消息重放和消息伪造，抵抗协议层的拒绝服务攻击[18]。

3.2　安全性证明

本节使用BAN逻辑对协议的安全性进行证明，BAN逻辑是由Burrows，Abadi和Needham在1989年提出的一种基于信念的模态逻辑[19]，是分析认证协议的常规方法。

3.2.1　BAN逻辑的基本术语

$P|\equiv X$：P相信X，且在整个协议运行中都相信X；

$P|\sim X$：P发送过包含X的消息；

$P\lhd X$：P收到了包含X的消息；

$P|\Rightarrow X$：P对X拥有仲裁权；

$\#(X)$：X是新鲜的；

$P\overset{K}{\longleftrightarrow}Q$：$K$是$P$和$Q$之间的共享密钥；

$\{X\}_K$：表示用K对X加密后的密文。

3.2.2　BAN逻辑的逻辑推理规则

R1：消息含义规则 $\dfrac{\left(P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_K\right)}{P|\equiv Q|\sim X}$；

R2：新鲜值验证规则 $\dfrac{\left(P|\equiv\#(X),P|\equiv Q|\sim X\right)}{P|\equiv Q|\equiv X}$；

R3：仲裁规则 $\dfrac{\left(P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X\right)}{P|\equiv X}$；

R4：传递规则 $\dfrac{\left(P|\equiv X,P|\equiv Y\right)}{P|\equiv(X,Y)}$；

R5：新鲜性规则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,\ Y)}$。

对于哈希函数$h(X)$，还有以下2条规则

R6：$\dfrac{\left(P|\equiv Q|\sim h(X),P\lhd Q\right)}{P|\equiv Q|\sim X}$；

R7：$\dfrac{\left(P|\equiv Q|\sim h(X_1,X_2,\cdots,X_n),P\lhd X_1,P\lhd X_2,\cdots,P\lhd X_n\right)}{P|\equiv Q|\sim(X_1,X_2,\cdots,X_n)}$。

3.2.3 协议的逻辑分析

利用BAN逻辑对本文协议分析如下：

1)协议描述

$R \rightarrow T: r_R$;

$T \rightarrow R: r_T, h(r_R||id_T), h(id_T||secret)$;

$R \rightarrow C: r_T, h(id_R), h(id_T||secret)$;

$C \rightarrow R: r_T, E_k(id_T||secret)$;

$R \rightarrow C: r_R, E_k(id_T||secret_{new}), h(id_T||secret_{new})$;

$C \rightarrow R: r_R, ACK$;

$R \rightarrow T: r_R, h(r_R||secret_{new})$,

其中：R表示阅读器；T表示电力设备；C表示云数据库服务器。

2)协议理想化

$M1: R \lhd r_T, r_R, h(r_R||id_T), h(id_T||secret), \{id_T||secret\}_k$;

$M2: C \lhd r_T, r_R, h(id_R), h(id_T||secret_{new})$;

$M3: T \lhd r_R, h(r_R||secret_{new})$。

3)初始化假设

$H1: T|\equiv \#(r_T), H2: T|\equiv \#(secret_{new}), H3: T|\equiv R \xleftrightarrow{r_R} T$;

$H4: R|\equiv \#(r_R), H5: R|\equiv T \xleftrightarrow{r_R} R$。

4)协议目标

$A1: R|\equiv T|\sim \#(id_T)$ $A2: T|\equiv R|\equiv secret_{new}$;

A1是指阅读器相信电力设备标签发送过包含新鲜id_T的消息；

A2是指电力设备标签相信阅读器相信$secret_{new}$。

5)协议分析

证$A1: R|\equiv T|\sim \#(id_T)$:

①$R \lhd h(r_R||id_T), R|\equiv T \xleftrightarrow{r_R} R$，由消息含义规则R1得：$R|\equiv T|\sim h(r_R||id_T)$。

②$R \lhd \{id_T||secret\}_k$，因为$k$为R自己的密钥，所以$R \lhd (id_T, secret)$，由拆分消息规则可知：$R \lhd id_T, R \lhd secret$。

③$R|\equiv T|\sim h(r_R||id_T), R \lhd r_R, R \lhd id_T$，由哈希函数规则R7得：$R|\equiv T|\sim (r_R, id_T)$；由传递规则R4得：$R|\equiv T|\sim id_T$。

④$R|\equiv \#(r_R)$，由新鲜性规则R5得：$R|\equiv \#(r_R, id_T)$。

⑤由$R|\equiv T|\sim id_T, R|\equiv \#(r_R, id_T)$得：$R|\equiv T|\sim \#(id_T)$。

A1得证。

证$A2: T|\equiv R|\equiv secret_{new}$:

①$T \lhd h(r_R||secret_{new}), T|\equiv R \xleftrightarrow{r_R} T$，由消息含义规则R1得：$T|\equiv R|\sim h(r_R||secret_{new})$；由于T知道secret的更新规则，所以$T \lhd secret_{new}$。

②$T|\equiv R|\sim h(r_R||secret_{new}), T \lhd r_R, T \lhd secret_{new}$，由哈希函数规则R7得：$T|\equiv R|\sim (r_R, secret_{new})$，

由传递规则R4得：$T|\equiv R|\sim secret_{new}$。

③$T|\equiv \#(secret_{new}), T|\equiv R|\sim secret_{new}$，由新鲜值验证规则R2得：$T|\equiv R|\equiv secret_{new}$;

A2得证。

3.3 性能对比分析

从标签计算量、存储量、通信量及数据库搜索效率4个方面，将提出的协议与Vaidya、Zong、Yeh等人的协议进行对比，结果如表2所示。

表 2　性能对比

Table 2　Performance comparisons

性能指标	Vaidya	Zong	Yeh	本文协议
标签计算量	$6h$+9xor	$2h$+4xor	$7r$+8xor	$4h$+$1r$
标签存储量	$2L$	$3L$	$4L$	$2L$
标签通信量	$11l$	$6l$	$6l$	$5l$
数据库搜索效率	Medium	Low	Medium	High

表中：h表示哈希函数运算操作所需的计算量，xor表示异或运算所需的计算量，r表示生成随机数所需的计算量，L表示标签身份、秘密值、时间戳的长度，l表示随机数、时间戳、哈希运算、异或运算的输出长度。

研究提出的协议中，标签共计执行了4次哈希运算和1次随机数生成操作，且存储量与通信量较低。云数据库利用哈希索引进行数据查找，搜索效率较高。综合上述分析，该协议具有良好的性能优势。

4　结束语

研究提出了一种面向电力物联网的RFID认证方案，实现了电力物联网环境下电力设备与阅读器之间的相互认证，保障了云数据库服务器、阅读器与电力设备之间的数据传输安全，同时具备不可追踪性，可以抵抗重放攻击、去同步攻击、拒绝服务攻击等多种安全威胁。通过对比分析，提出的方案具有良好的综合性能。将方案应用于智能电网，能支撑智能用电双向交互、用电信息采集、智能家居控制、分布式电源接入等多种功能的实现，提高供电可靠性与用电效率和智能电网数据的安全性。但是方案尚有改进之处，后续研究将致力于设计一种更为轻量级的认证协议，进一步降低电力设备标签的计算复杂度。

参考文献

[1] 李小鹏. 能源互联网电力信息融合风险传递模型与仿真系统研究[D]. 北京: 华北电力大学, 2019.
Li X P. Research on risk transmission model and simulation system of power information fusion on energy Internet[D]. Beijing: North China Electric Power University, 2019. (in Chinese)

[2] 朱从亮. 基于5G电力物联网的低压智能台区管理平台[D]. 杭州: 浙江大学, 2022.
Zhu C L. Low-voltage intelligent station area management platform based on 5G power Internet of Things[D]. Hangzhou: Zhejiang University, 2022. (in Chinese)

[3] Marot A, Kelly A , Naglic M, et al. Perspectives on future power system control centers for energy transition[J]. Journal of Modern Power Systems and Clean Energy, 2022, 10(2): 328-344.

[4] 王继业, 周春雷, 李洋, 等. 数据中心关键技术和发展趋势研究综述[J]. 电力信息与通信技术, 2022, 20(8): 1-21.
Wang J Y, Zhou C L, Li Y, et al. Review of key technologies and development trend of data center construction[J]. Electric Power Information and Communication Technology, 2022, 20(8): 1-21. (in Chinese)

[5] Dass P, Om H. A secure authentication scheme for RFID systems[J]. Procedia Computer Science, 2016, 78: 100-106.

[6] Kardas S, Celik S, Bingol M A, et al. A new security and privacy framework for RFID in cloud computing[C]//2013 IEEE 5th International Conference on Cloud Computing Technology and Science. Bristol, UK: IEEE, 2013: 171-176..

[7] Lacmanovic I, Radulovic B, Lacmanovic D. Contactless payment systems based on RFID technology[C]//33rd International Convention MIPRO. Opatija, Croatia: IEEE, 2010: 1114-1119.

[8] 宗劲冲. RFID技术在智能电网数据采集中的研究[D]. 北京: 华北电力大学, 2013.
Zong J C. Reaserch on data acquisition of smart grid based on RFID technology[D]. Beijing: North China Electric Power University, 2013(in Chinese)

[9] Washiro T. Applications of RFID over power line for Smart Grid[C]//2012 IEEE International Symposium on Power Line Communications and Its Applications.Beijing, China: IEEE, 2012: 83-87.

[10] Chaimae E, Rahal R. New way of passive RFID deployment for smart grid[J]. Journal of Theoretical & Applied Information Technology, 2015. 82(1); 81-84.

[11] Vaidya B, Makrakis D, Mouftah H T. Authentication mechanism for mobile RFID based smart grid network[C]//2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE). Toronto, Canada: IEEE, 2014: 1-6.

[12] Yeh T C, Wang Y J, Kuo T C, et al.Securing RFID systems conforming to EPC class 1 generation 2 standard[J].Expert Systems with Application, 2010, 37(12):7678-7683.

[13] Alqarni A, Alabdulhafith M, Sampalli S. A proposed RFID authentication protocol based on two stages of authentication[J]. Procedia Computer Science, 2014, 37: 503-510.

[14] Xu H, Yin X, Zhu F, et al. An enhanced secure authentication scheme with one more tag for RFID systems[J]. IEEE Sensors Journal, 2021, 21(15):17189-17199.

[15] Patil A T, Acharya R, Patil H A, et al. Improving the potential of enhanced teager energy cepstral coefficients (ETECC) for replay attack detection[J]. Computer Speech & Language, 2022, 72:101281.

[16] Zhou S, Zhang Z, Luo Z, et al. A lightweight anti-desynchronization RFID authentication protocol[J]. Information Systems Frontiers, 2010, 12(5): 521-528.

[17] 朱晓辰 . 物联网感知层轻量级认证技术的研究[D]. 西安: 西安电子科技大学, 2021.
Zhu X C. Research on lightweight authentication technology of perception layer of Internet of Things[D]. Xi'an: Xidian University, 2021. (in Chinese)

[18] Aghili S F, Ashouri-Talouki M, Mala H. DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT[J]. Journal of Supercomputing, 2018, 74(1): 509-525.

[19] Burrows M, Abadi M, Needham R M. A logic of authentication[J]. Acm Transactions on Computer Systems, 1989, 23(5): 1-13.

（编辑　侯　湘）