链式CRP赋能TEE-PUF的工业5.0轻量级匿名认证协议

宋建华[1,3,4,5],张天羿[1],张 龑[2,3,5*]

(1. 湖北大学网络空间安全学院,湖北武汉 430062;2. 湖北大学计算机学院,湖北武汉 430062;
3. 智能感知系统与安全教育部重点实验室,湖北武汉 430062;
4. 智能网联汽车网络安全湖北省工程研究中心,湖北武汉 430062;
5. 大数据智能分析与行业应用湖北省重点实验室,湖北武汉 430062)

摘 要: 近年来,工业5.0已逐渐成为全球制造业发展的新兴方向,大量资源受限的智能设备广泛应用于开放环境中. 针对现有工业5.0认证协议中计算开销过大、关键安全属性缺失等问题,本文提出了一种基于物理不可克隆函数(Physical Unclonable Functions,PUF)的轻量级匿名认证协议,有效解决了工业5.0环境下计算开销低与高安全性需求之间的矛盾. 所提协议使用了可信执行环境(Trusted Execution Environment,TEE)增强PUF,优化了现有三方认证协议的信息流,提出了链式挑战-响应对(Challenge-Response Pair,CRP)更新机制,实现了用户、网关与工业5.0智能设备的三方认证与密钥协商. 同时,基于形式化与非形式化的安全分析证明了该协议能够有效抵御智能设备窃取攻击及其他常见攻击类型. 与近几年相关协议的对比分析表明,本文协议在平均降低了54%的计算开销的同时满足了更多安全需求.

关键词: 认证协议;身份认证;轻量级;工业5.0;物理不可克隆函数;密钥协商

基金项目: 国家自然科学基金(No.62377009);湖北省重大攻关项目(JD)(No.2023BAA018);湖北省重点研发计划重点项目(No.2021BAA184,No.2021BAA188);湖北省高等学校人文社会科学重点研究基地绩效评价信息管理研究中心课题(No.2020JX01);湖北省科技计划重大科技专项(No.2024BAA008)

中图分类号: TN915.08;TN918.4 **文献标识码:** A **文章编号:** 0372-2112(2025)08-2946-16

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250478

A Lightweight Anonymous Authentication Protocol for Industry 5.0 Based on Chained CRP-Enabled TEE-PUF

SONG Jian-hua[1,3,4,5], ZHANG Tian-yi[1], ZHANG Yan[2,3,5*]

(1. *School of Cyber Science and Technology*, *Hubei University*, *Wuhan*, *Hubei* 430062, *China*;
2. *School of Computer Science*, *Hubei University*, *Wuhan*, *Hubei* 430062, *China*;
3. *Key Laboratory of Intelligent Sensing System and Security*, *Ministry of Education*, *Wuhan*, *Hubei* 430062, *China*;
4. *Hubei Provincial Engineering Research Center of Intelligent Connected Vehicle Network Security*, *Wuhan*, *Hubei* 430062, *China*;
5. *Hubei Key Laboratory of Big Data Intelligent Analysis and Application*, *Hubei University*, *Wuhan*, *Hubei* 430062, *China*)

Abstract: In recent years, Industry 5.0 has gradually emerged as a new direction for the development of global manufacturing, with a large number of resource-constrained smart devices being widely deployed in open environments. To address issues such as excessive computational overhead and the lack of critical security attributes in existing Industry 5.0 authentication protocols, this paper proposes a lightweight anonymous authentication protocol based on physical unclonable functions (PUF), effectively resolving the conflict between low computational overhead and high-security requirements in the Industry 5.0 environment. The proposed protocol utilizes trusted execution environment (TEE) to enhance PUF, optimizes the information flow of existing three-party authentication protocols, and introduces a chained challenge-response pair (CRP) update mechanism, achieving three-party authentication and key agreement among users, gateways, and Industry 5.0 smart devices. Furthermore, formal and informal security analyses demonstrate that the protocol can effectively resist

收稿日期:2025-06-05;录用日期:2025-07-22;责任编辑:覃怀银
*通讯作者:张龑

smart device theft attacks and other common attack types. Comparative analysis with related protocols in recent years shows that the proposed protocol reduces the average computational overhead by 54% while meeting more security requirements.

Key words: authentication protocol; identity authentication; lightweight; industry 5.0; physical unclonable function; key agreement

Foundation Item(s): National Natural Science Foundation of China (No.62377009); Major Project of Hubei Province (JD) (No.2023BAA018); Key Project of Hubei Provincial Key Research and Development Program (No.2021BAA184, No.2021BAA188);Research Center for Performance Evaluation and Information Management of Key Research Bases for Humanities and Social Sciences in Hubei Provincial Colleges and Universities (No.2020JX01); Major Science and Technology Special Project of Hubei Science and Technology Plan (No.2024BAA008)

1 引言

近年来,随着数字化技术、人工智能和物联网等前沿技术的迅猛发展,工业5.0作为工业革命的新阶段,正逐步成为全球制造业转型的核心驱动力. 与工业4.0聚焦于自动化和智能化生产不同,工业5.0更强调人类与智能技术的深度协作,旨在融合人类的创新能力与机器的高效生产能力,推动生产过程向个性化、定制化、绿色化和智能化方向迈进. 这一变革不仅是对传统制造业的升级,更是以人机协作为核心的颠覆性创新,为制造业开启了更加智能、高效的新时代.

然而,工业5.0的普及和实施也面临着一些亟待解决的问题. 其中,通信安全和数据隐私问题尤为突出[1]. 随着物联网、云计算和大数据等技术的普及,工业5.0中的海量的数据交换和认证过程带来了严重的安全隐患. 例如,用户通过移动设备(手机、笔记本等)访问工业机器人时,恶意攻击者可以通过冒充合法实体窃取智能设备的身份信息,或通过物理攻击提取设备内存中的敏感参数. 由于工业5.0中的智能设备和网关通常部署在公共网络环境中,易遭受中间人攻击、重放攻击和窃取攻击等威胁,直接影响工业生产的稳定性和用户隐私的保护.

在这一背景下,认证密钥和协议作为系统安全的第一道防线,其重要性不言而喻. 尤其是在工业5.0环境中,面对大量资源有限的设备和智能终端,设计既高效又安全的认证协议成为确保系统稳定运行的关键[2]. 通过有效的认证协议,可以防止未经授权的访问和数据篡改,而安全的密钥协商则进一步保障后续通信的保密性. 此外,认证协议的匿名性也至关重要,能够有效保护设备和用户的身份隐私,防止恶意攻击者通过身份信息追踪用户行为或进行身份盗用. 然而,工业5.0中的智能设备普遍存在着计算能力和存储能力有限的问题[3],使得传统的认证协议难以直接应用于实际场景. 因此,如何在资源受限的设备上实现安全高效的认证协议,成为工业5.0环境中亟待解决的一个关键问题.

现阶段已有多种工业物联网认证协议被提出,但在计算开销和安全属性等方面仍存在不足,难以满足工业5.0对低能耗和高安全性的要求. 既要实现强大的安全性,又要兼顾轻量级和匿名性,是研究者设计工业5.0认证协议面临的核心挑战. 为此,本文提出了一种基于物理不可克隆函数(Physical Unclonable Function, PUF)的轻量级匿名认证协议BPIT(a authentication protocol Based on PUF for IoT),通过可信执行环境(Trusted Execution Environment, TEE)增强的链式挑战-响应对(Challenge-Response Pair, CRP)动态更新机制,针对工业5.0中工业物联网设备的需求进行了优化.

以下是本协议的具体贡献:

(1)本文提出了适用于工业5.0物联网场景的BPIT认证协议. 该协议不仅实现了用户与工业智能设备之间的匿名身份认证,还确保了会话密钥的安全生成,为通信过程提供了可靠保障,能够有效抵御多种安全威胁. 考虑到工业5.0环境中攻击者的潜在强大能力,本文采用真实或随机(Real-Or-Random, ROR)模型对协议的会话密钥安全性进行了严格证明. 分析结果表明,即便面对具备高级攻击手段的对手,BPIT协议生成的会话密钥依然保持高度安全性,为工业5.0系统的稳定运行奠定了坚实基础.

(2)本文提出了一种链式动态CRP更新流程,有效解决了传统注册阶段因需读取大量CRP而导致的存储开销过大问题. 通过采用不可逆哈希链的设计,协议实现了完美前向保密性——即使攻击者截获当前使用的CRP,也无法逆推出之前的历史CRP,从而显著提高了机器学习建模攻击的难度. 此外,在挑战生成过程中,协议引入种子和基于哈希的消息认证码(Hash-based Message Authentication Code, HMAC),以确保挑战的随机性和不可预测性. 同时,通过将挑战存储于TEE中,进一步增加了攻击者在窃取设备后提取关键信息的难度. 这种硬件与系统层面的双重保护,为工业5.0设备提供了更高的安全保障.

(3)针对工业智能设备计算资源受限的特点,本文设计了一种仅依赖基础加密操作的高效认证方案. 该方案通过优化三实体认证协议的信息流,减少冗余交互,摒弃了计算开销昂贵的非对称加密(如ECC)或混

沌映射等操作，结合哈希函数、PUF等轻量级加密技术，使得协议在保证高安全性的同时显著降低了计算开销，实现了协议的轻量性. 为验证协议的优越性，本文进行了全面的比较分析，即将BPIT协议与现有方案在安全属性、通信代价和计算代价等方面进行了对比. 结果表明，BPIT协议在保持强安全性的前提下，计算代价相较传统方案平均下降54%，更好地满足了工业5.0对低能耗和高效率的需求.

2 相关工作

本节将通过传统认证协议、基于PUF的认证协议和工业5.0现有的认证协议来介绍相关工作.

工业5.0是从工业4.0逐步演进而来. 工业4.0通过自动化、数据交换和制造技术的进步，致力于构建智能工厂，而工业物联网(Industrial Internet of Things，IIoT)作为其核心支柱，通过设备互联和数据分析推动制造业的数字化转型. 随着工业5.0的到来，安全性和隐私保护问题日益突出，尤其是在人机协作和资源受限的场景中. 为应对工业物联网中的安全挑战，学者提出了多种认证协议. 文献[4]针对工业物联网提出了一种轻量级的认证与密钥交换方案. 该方案通过融合认证加密(AEGIS)和哈希函数，在降低计算/通信开销的同时，实现了用户与设备之间的双向认证和动态会话密钥生成. 文献[5]提出了一种基于椭圆曲线密码(Elliptic Curve Cryptography，ECC)的适用于工业物联网的轻量级匿名认证协议ASAP-IIoT，为工业设备的安全通信提供了可行的解决方案. 文献[6]提出了仅使用哈希函数和异或运算的轻量级认证协议，适用于资源受限的IIoT设备. 文献[7]提出了一种双层混合密钥协商协议，结合了椭圆曲线与组密钥机制，支持动态传感器管理.

然而，使用非对称加密原语构建的认证协议在实现关键的安全属性方面具有优势，但执行代价昂贵的非对称加密操作对于资源受限的物联网设备来说效率低下，而使用对称密码原语的认证协议经常因为安全性不足而受到各种攻击[3,8].

为解决上述问题，学者开始探索物理不可克隆函数(PUF)在工业物联网认证中的应用，以提升安全性和降低计算代价. 文献[9]提出了一种结合PUF和动态累加器技术的基于区块链的动态认证协议，旨在实现工业物联网环境下的多因素密钥派生和链上的存储优化，并且设计了零知识证明机制验证设备的身份. 文献[10]提出了WSNEAP协议，结合PUF和布隆过滤器减少了工业物联网设备的存储和查询开销，避免了传统数据库的复杂度，并且在每次认证结束后触发CRP的动态更新，以确保安全性和同步性. 文献[11]提出了一种针对工业物联网中机器对机器(Machine to Machine，M2M)通信的轻量级认证协议，在计算新的挑战时使用了当前会话的挑战，形成了不可逆的哈希链，完成了传感器和路由器的双向认证. 文献[12]利用椭圆曲线密码和PUF设计了一个基于区块链的智能电表和需求响应控制单元双向认证的协议，但是在资源有限的智能设备上执行复杂的椭圆曲线加解密存在计算开销过大的问题，导致整个协议的计算代价提升[13]. 文献[14]提出了一种针对电力物联网智能终端的认证协议，其引入PUF技术并设计了扩展CRP的结构，旨在解决传统方案需要提前存储多个CRP导致存储需求增大的缺陷，但该方案并没有提到如何更新CRP. 实际上，一些现有的基于PUF的认证方案误解了PUF的能力，导致这些方案无法提供物理保护[15].

尽管上述协议在工业4.0中取得一定成效，但工业5.0对高效通信提出了更高要求[16]. 为此，学者针对工业5.0提出了新的认证方案，但部分方案依然存在计算代价高的问题. 文献[17]提出了一种基于混沌映射的可持续认证与密钥协商协议，专为工业5.0设计，旨在解决人机协作场景下的安全通信与资源效率问题. 相较现有的基于混沌映射的协议，解决了前向安全性和认证因子泄露的问题. 然而混沌映射的计算复杂度相较于轻量级哈希函数存在着计算复杂度高的问题，在资源受限的设备中可能存在延迟. 文献[8]首次提出了结合PUF与机器学习的认证框架以实现高安全性与低资源消耗的问题. 但是存在机器学习模型计算开销大，并且难以部署在工业5.0设备上的问题.

综上所述，工业4.0的认证协议难以满足工业5.0的高效通信需求. 目前，工业5.0的部分方案存在缺乏匿名性、不可追踪性的问题[18]，而基于椭圆曲线和混沌映射的改进方案虽然解决了匿名性和不可跟踪性问题，但依然存在着计算和通信代价高的问题[13]. 因此，亟需一种新型认证与密钥协商协议，既能适应工业5.0中资源受限设备的需求，又能保证高安全性.

3 预备知识

3.1 物理不可克隆函数

物理不可克隆函数(PUF)是一种硬件安全原语，由Pappu等人[19]提出，利用物理设备在制造过程中固有且不可控的工艺差异，确保无法生产出完全相同的PUF副本[20]. 其核心特性在于挑战-响应对(CRP)，这一对被视为硬件的“指纹”广泛应用于设备认证、密钥生成及安全通信，提供了一种轻量级且防篡改的解决方案.

PUF的工作机制可描述如下：接收一串m位比特作为输入(称为挑战，C)，并生成一串n位随机比特作为输出(称为响应，R)，即

$$\mathrm{PUF}(C:\{0,1\}^m)=R:\{0,1\}^n.$$

其唯一性和随机性体现在:通常情况下,不同的PUF在面对相同的挑战时会生成不同的响应,即使是相同的PUF,在同一挑战下也会产生不同的响应,即

$$\Pr\left[\mathrm{PUF}_1(C_1)=\mathrm{PUF}_1(C_2\neq C_1)\right]\leqslant\alpha.$$

其中,α是一个可以忽略的小值.

综上所述,PUF的优点如下:

(1)物理安全性. 芯片微结构的天然差异增强了PUF的抗侵入性,使物理攻击成本高昂.

(2)抗克隆性. 由于制造工艺的不可复制性,克隆PUF几乎不可能.

(3)轻量级设计. 相较于传统的哈希算法或公钥加密,PUF无须昂贵的加密硬件,特别适用于资源受限的设备.

3.2 HMAC

基于哈希的消息认证码(HMAC)是一种用于验证消息完整性和真实性的密码学工具[21],它结合加密哈希函数和密钥,确保消息在传输过程中未被篡改,并确认发送者的身份. 它依赖密钥和哈希函数实现,HMAC需要一个信息M和密钥K,并生成一个信息认证码MAC,如果没有获取到密钥K,则无法获得有效信息M. 即

$$\mathrm{MAC}=\mathrm{HMAC}(K,M).$$

本文利用HMAC生成挑战,并使用种子作为密钥,保证了挑战生成的不可逆哈希链. 这一设计较使用简单哈希函数,例如SHA-256,在几乎不增加计算代价的同时大大增加了攻击者通过哈希碰撞等方法获取秘密信息的难度. 此外,种子值的使用使得每次生成的挑战具有高度的随机性和唯一性,进一步提升了系统的抗攻击能力. 通过这种方式,攻击者不仅难以通过反向工程恢复密钥,还有效降低了通过预计算和暴力破解等攻击手段获取挑战信息的风险.

值得注意的是,虽然HMAC比简单哈希函数的计算开销略高,但在本文提出的协议中,HMAC主要用于初始化阶段、注册阶段以及链式动态CRP更新流程中,在认证阶段并没有使用. 相较于现有协议中使用的公钥加密,如椭圆曲线或混沌映射,HMAC增加的微量开销是可以接受的,且远低于这些公钥加密操作. 因此HMAC在不影响认证过程轻量化的情况下提供了高安全性.

3.3 可信执行环境

可信执行环境(TEE)是一种在计算设备中提供安全隔离执行环境的技术. 这种方法允许用户主动选择需要保护的数据,以保证数据不被恶意软件和黑客窃取[22]. 与传统安全技术相比能够更加有效地实现数据的隔离性、完整性、机密性、可信性等安全特性. 可信执行环境体系可抽象成图1所示的结构. 目前,已有学者针对物联网中智能设备提出了高性能、高安全性的可信执行环境系统,实现了对关键数据读取存储的机密性和完整性[23].

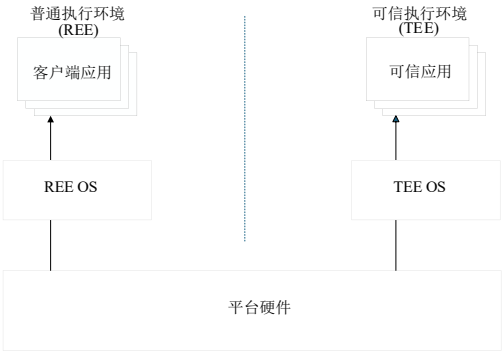


图1　TEE工作模式

本文提出的协议采用了可信执行环境(TEE)来存储协议中使用的挑战-响应对(CRP),从而增强了对挑战的保护. 通过将CRP存储在TEE中,显著增加了攻击者在执行移动设备或智能设备窃取攻击时获取到CRP对的难度. TEE提供的隔离执行环境使得攻击者即使成功物理窃取了设备,也无法直接访问存储在其中的敏感信息. 此外,TEE的安全性进一步降低了攻击者通过侧信道分析、逆向工程或其他手段恢复CRP的可能性.

更重要的是,TEE的使用有效减少了攻击者通过机器学习对CRP进行建模攻击的机会. 由于每次生成的挑战在TEE中进行独立的、加密保护的计算,即便攻击者能够收集到部分挑战-响应数据,也无法轻易通过分析数据之间的关联来推测出其他未公开的挑战或响应. 这种防护机制显著增强了协议的抗攻击性,为系统提供了额外的安全保障,确保了即使在面对高级持久性威胁(Advanced Persistent Threat,APT)时,系统仍能保持高水平的安全性.

BPIT协议部署在TEE内的核心操作主要包括:

(1)秘密存储. 安全存储用户端与智能设备端的挑战. 这是TEE最基本也是最成熟的功能,通过硬件隔离和加密存储实现.

(2)挑战生成. 在注册阶段和链式动态CRP更新流程中执行HMAC生成挑战. 现代TEE(如ARM TrustZone,Intel SGX)普遍集成硬件加密引擎(如ARM CryptoCell,Intel QAT),可高效安全执行HMAC等对称密码操作[24].

(3)PUF响应生成. PUF通常是独立硬件模块,但TEE可通过安全总线或受保护的接口与之交互,确保挑战安全地传递给PUF[25].

因此,BPIT协议在TEE中执行上述操作是可行的.

3.4 系统模型

本文的系统模型如图2所示,其中包括三个主要认证实体:用户(U),网关节点(GW),工业智能设备(SD). 表1中列出了本文中使用的相关符号.

用户(U):用户是指通过各类移动设备(MD)远程控制工业智能设备的个体. 注册过程之后,用户可借助部署在工业环境中的网关节点与工业智能设备建立通话密钥.

网关节点(GW):网关部署在工业环境中,负责连接用户的移动设备和工业智能设备,并提供存储信息、计算和认证等关键服务. 在注册阶段,用户的移动设备与工业智能设备均需向网关节点进行注册以在登录认证阶段进行认证.

工业智能设备(SD):工业智能设备涵盖工业5.0体系下使用的多种智能设备,如协作机器人、传感器、智能电表等. 这些设备需向网关进行注册,以确保用户可以通过网关节点与对应的工业智能设备进行通信.

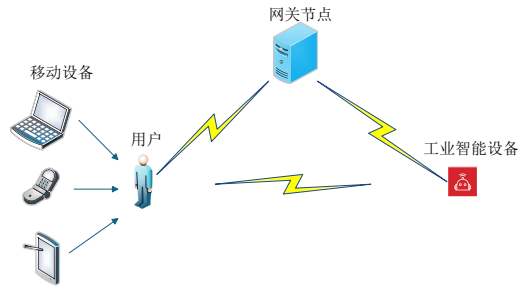


图2 系统模型

表1 BPIT协议符号

符号	相应的含义
U,MD_i	用户以及其移动设备
GW,SD_i	网关节点和工业智能设备
ID_{SD}	工业智能设备的身份标识
TID_i	用户的临时身份标识
K_{GW}	网关节点的长期秘密
ID, PWD, BIO	用户的用户名、密码和生物特征
Gen(·), Rep(·)	两种模糊提取器的算法

3.5 威胁模型

本文使用了Dolev-Yao(DY)威胁模型[26]和CK威胁模型[27]来分析认证协议的安全性. 在认证阶段,协议涉及的实体通过公共频道交换通信信息. 因此,根据该模型对攻击者的能力作出以下假设:

(1)在注册阶段,所有的信息通过安全信道传输. 在登录与认证阶段,通信在开放信道上传输. 攻击者可以完全控制开放信道上的通信,如窃听、删除、重放、伪造信息.

(2)由于无法实时监控移动设备与工业智能设备,敌手可能通过物理手段捕获两者,并从其内存中读取秘密信息. 因此,用户的移动设备和工业智能设备被视为不可信实体.

(3)攻击者可以利用侧信道攻击获取工业智能设备和移动设备中存储的敏感信息.

(4)攻击者可以获取用户移动设备、密码、生物特征信息中的任意两种,但是无法同时获取全部三种信息.

4 BPIT协议

4.1 信息流的优化

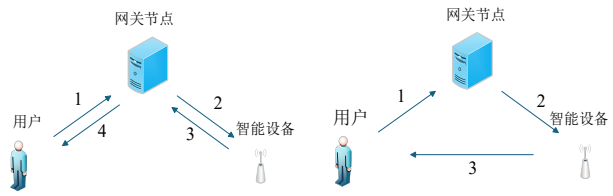
在工业5.0环境中,移动设备和智能设备通常存在着计算能力弱、存储有限、易遭受攻击的问题,因此需要网关承担复杂运算、安全性保障的功能. 该环境下还涉及大量智能设备,协议必须支持动态注册的功能. 在这个背景下,双方认证会导致安全缺陷和密钥管理困难的问题,因此BPIT协议的设计使用了三方认证的模式. 在提出协议之前,应首先分析现阶段三方认证协议的信息流[28~31]. 传统情况下,当用户(U)通过网关(GW)远程访问智能设备(SD)时,典型的信息流为U-GW-SD-GW-U. 协议传输的信息总数(Total Number of Messages,TNM)为4.

具体而言,协议执行了四个步骤:网关节点验证用户,智能设备验证网关,网关验证智能设备,用户验证网关. 然而,许多基于此信息流的协议未能有效抵御去同步攻击[3]. 为了解决这一问题,许多协议通过引入额外的信息来确保同步性,进而使TNM超过了4,增加了通信开销.

如果协议模式发生变化,变为网关验证用户,智能设备验证网关,用户验证智能设备,则协议中需要交换的TNM为3. 显然,在这种模式下,总信息量是最少的. 然而,基于这种模式的许多基于对称加密原语的协议往往未能实现预期的安全目标. 因此,本文的研究目标是设计一个基于PUF的认证协议,该协议能够在该模式下实现最小的认证总信息量,从而减少网络通讯时的不稳定性,提升认证效率. 然而,基于此模式的协议面临一个关键挑战:由于缺少网关向用户传输信息以及智能设备向网关传输信息的环节,无法动态更新CRP以支持后续认证. 为了克服这一挑战,本文提出了链式动态CRP更新流程,旨在确保CRP能够得到及时更新,从而保证认证过程的可持续性. 图3分别展示了TNM为4和3时的信息流.

4.2 协议内容

BPIT协议包括初始化阶段、注册阶段、认证阶段以及链式动态CRP更新流程.



(a) TNM为4的信息流　　(b) TNM为3的信息流

图3　TNM为4或3时的信息流

4.2.1　初始化阶段

初始化阶段是协议的第一步,其目的是为后续的注册和认证过程奠定基础. 该阶段为整个系统提供了加密基础和唯一的种子信息,是后续设备和用户注册的安全保障.

网关GW首先生成一个长期密钥K_{GW},生成初始种子Seed_{init},时间戳$T_{Current}$,计数器t并且赋初值为0,随机数N,并且生成种子

$$\text{Seed}=\text{HMAC}\left(\text{Seed}_{init},K_{GW}\|T_{Current}\|t\|N\right).$$

4.2.2　注册阶段

在认证之前智能设备与用户需要提前在安全信道上进行注册,为防止假冒攻击等攻击方式,网关在这个阶段会为智能设备与用户生成安全标识符、密钥和挑战响应机制,以保证后续安全的通信和认证.

(1)智能设备注册阶段

智能设备在接入物联网之前,需向网关节点进行注册.

步骤1.

智能设备SD在安全信道上向GW发送注册请求,GW为SD生成一个唯一的身份标识ID_{SD},并且生成密钥$K_{SD}=h(K_{GW}\|\text{ID}_{SD})$,之后GW将$\text{ID}_{SD}$存储到内存中,之后GW通过安全信道将$\{\text{Seed},\text{ID}_{SD},K_{SD}\}$发送给SD.

步骤2.

智能设备SD接收到信息之后,生成计数器t并赋值为0,时间戳$T_{Current}$,之后使用Seed生成挑战$C_{SD}=\text{HMAC}\left(\text{Seed},t\|T_{Current}\|\text{ID}_{SD}\right)$,利用挑战$C_{SD}$生成响应$R_{SD}=\text{PUF}\left(C_{SD}\right)$,智能设备将$C_{SD}$保存到可信执行环境中,之后删除Seed,$T_{Current}$,SD将响应$R_{SD}$发送给GW,GW保存$\{C_{SD},R_{SD}\}$.

(2)用户注册阶段

用户远程控制远程智能设备之前,需要向网关节点进行注册,如图4所示. 用户注册阶段由两个步骤组成.

步骤1.

用户U在移动设备MD_i输入用户名ID,密码PWD,MD_i生成一个随机数r_1,之后MD_i计算

$$\text{RID}=h(\text{ID}\|r_1),$$

$$\text{RPWD}=h\left(\text{ID}\|\text{PWD}\|r_1\right).$$

之后MD_i将$\{\text{RID},\text{RPWD}\}$发送给GW,GW接收到信息后,生成用户的临时身份标识TID_i. GW计算$K_U=h\left(K_{GW}\right)\oplus h(\text{RID}\|\text{RPWD})$

之后GW将$\left\{\text{TID}_i^{old}=\text{null},\text{TID}_i^{new}=\text{TID}_i\right\}$保存在内存中,并将$\left\{K_U,\text{TID}_i,\text{Seed}\right\}$发送给$\text{MD}_i$.

步骤2.

MD_i接收到信息后,生成计数器t并赋值为0,时间戳$T_{Current}$,并使用Seed生成挑战C_U:

$$C_U=\text{HMAC}\left(\text{Seed},t\|T_{Current}\|\text{TID}_i\right).$$

之后利用挑战C_U生成响应$R_U=\text{PUF}\left(C_U\right)$. 之后$\text{MD}_i$将$C_U$保存到可信执行环境中,删除Seed,$T_{Current}$. 用户U将其生物特征$\text{BIO}_i$输入到$\text{MD}_i$中. MD_i使用模糊提取器(fuzzy extractor)生成算法$\text{Gen}(\cdot)$计算出BIO_i的公共参数τ_i和秘密参数σ_i,即$\text{Gen}\left(\text{BIO}_i\right)=\left(\sigma_i,\tau_i\right)$. 之后,$\text{MD}_i$计算

$$h\left(K_{GW}\right)=K_U\oplus h(\text{RID}\|\text{RPWD}),$$

$$B_i=r_1\oplus h\left(\text{ID}\|\text{PWD}\|\sigma_i\right),$$

$$C_i=h\left(K_{GW}\right)\oplus h\left(\text{RID}\|\text{RPWD}\|\sigma_i\right),$$

$$\text{Auth}_i=h\left(h\left(\text{RID}\|\text{RPWD}\|\sigma_i\right)\oplus r_1\oplus h\left(K_{GW}\right)\right).$$

之后,MD_i将$\left\{B_i,C_i,\text{Auth}_i,\text{TID}_i^{old}=\text{null},\text{TID}_i^{new}=\text{TID}_i\right\}$保存到内存中,并且将$R_U$发送给GW,GW保存$\left\{C_U,R_U\right\}$.

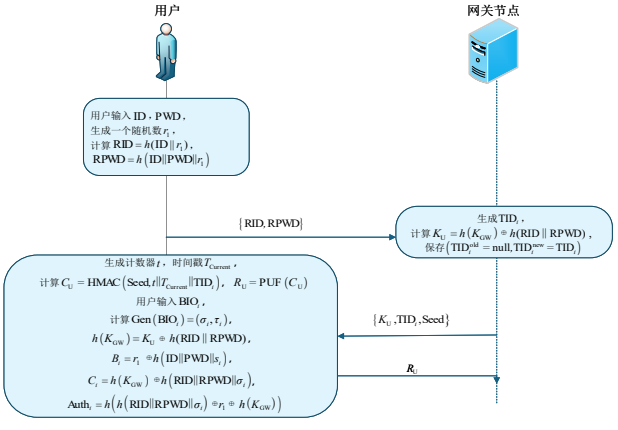


图4　用户注册阶段

4.2.3　认证阶段

本阶段是协议的关键部分,其要达到的目的是在用户与智能设备之间生成一个通话密钥. 在认证阶段,首先网关节点先验证用户的合法性,之后智能设备会验证网关的合法性,最后用户验证智能设备的合法性,在认证的过程中会生成一个会话密钥,在用户验证智能设备之后,即认为会话密钥合法,认证过程如图5所示. 认证过程由四个步骤组成.

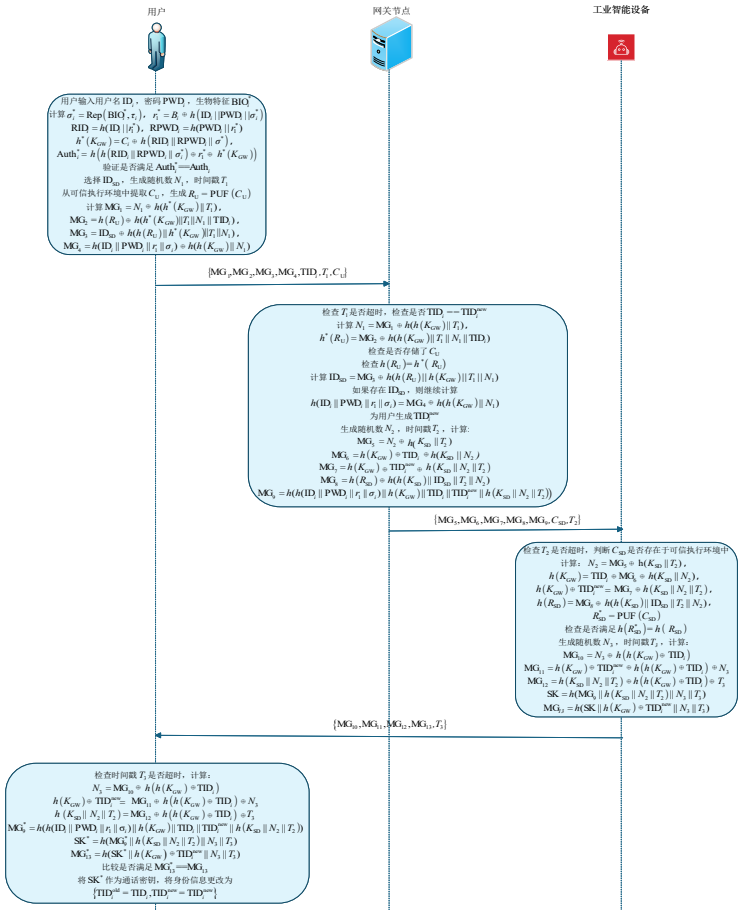


图5 认证阶段

步骤 1.

用户U输入用户名ID_i，密码PWD_i，生物特征BIO_i^*输入到移动设备MD_i. MD_i计算

$$\sigma_i^* = \mathrm{Rep}\left(\mathrm{BIO}_i^*, \tau_i\right),$$

$$r_1^* = B_i \oplus h\left(\mathrm{ID}_i || \mathrm{PWD}_i || \sigma_i^*\right),$$

$$\mathrm{RID}_i = h\left(\mathrm{ID}_i || r_1^*\right),$$

$$\mathrm{RPWD}_i = h\left(\mathrm{PWD}_i || r_1^*\right),$$

$$h^*\left(K_{\mathrm{GW}}\right) = C_i \oplus h\left(\mathrm{RID}_i || \mathrm{RPWD}_i || \sigma_i^*\right),$$

$$\mathrm{Auth}_i^* = h\left(h\left(\mathrm{RID}_i || \mathrm{RPWD}_i || \sigma_i^*\right) \oplus r_1^* \oplus h^*\left(K_{\mathrm{GW}}\right)\right).$$

MD_i验证是否满足$\mathrm{Auth}_i^* = \mathrm{Auth}_i$，如果相同则通过验证. 之后用户通过$\mathrm{ID}_{\mathrm{SD}}$选择想要访问的智能设备，$\mathrm{MD}_i$生成随机数$N_1$和时间戳$T_1$，并且从可信执行环境提取出$C_{\mathrm{U}}$，之后使用PUF函数生成挑战$R_{\mathrm{U}} = \mathrm{PUF}\left(C_{\mathrm{U}}\right)$，计算

$$\mathrm{MG}_1 = N_1 \oplus h\left(h^*\left(K_{\mathrm{GW}}\right) || T_1\right),$$

$$\mathrm{MG}_2 = h\left(R_{\mathrm{U}}\right) \oplus h\left(h^*\left(K_{\mathrm{GW}}\right) || T_1 || N_1 || \mathrm{TID}_i\right),$$

$$\mathrm{MG}_3 = \mathrm{ID}_{\mathrm{SD}} \oplus h\left(h\left(R_{\mathrm{U}}\right) || h^*\left(K_{\mathrm{GW}}\right) || T_1 || N_1\right),$$

$$\mathrm{MG}_4 = h\left(\mathrm{ID}_i || \mathrm{PWD}_i || r_1 || \sigma_i\right) \oplus h\left(h\left(K_{\mathrm{GW}}\right) || N_1\right).$$

MD_i将$\mathrm{MSG}_1 = \left\{\mathrm{MG}_1, \mathrm{MG}_2, \mathrm{MG}_3, \mathrm{MG}_4, \mathrm{TID}_i, T_1, C_{\mathrm{U}}\right\}$发送给GW.

步骤 2.

GW接收到信息后，检查时间戳T_1是否超时，检查是否满足$\mathrm{TID}_i = \mathrm{TID}_i^{\mathrm{new}}$，通过后计算

$$N_1 = \mathrm{MG}_1 \oplus h\left(h\left(K_{\mathrm{GW}}\right) || T_1\right),$$

$$h^*\left(R_{\mathrm{U}}\right) = \mathrm{MG}_2 \oplus h\left(h\left(K_{\mathrm{GW}}\right) || T_1 || N_1 || \mathrm{TID}_i\right).$$

GW检查储存的挑战响应对中是否存在C_{U}，如果不存在，则拒绝认证. 如果存在，则继续检查是否$h\left(R_{\mathrm{U}}\right) = h^*\left(R_{\mathrm{U}}\right)$. 如果相同，则验证通过，继续计算

$$\mathrm{ID}_{\mathrm{SD}} = \mathrm{MG}_3 \oplus h\left(h\left(R_{\mathrm{U}}\right) || h\left(K_{\mathrm{GW}}\right) || T_1 || N_1\right),$$

检查$\mathrm{ID}_{\mathrm{SD}}$是否存在，如果存在，则继续计算

$$h\left(\mathrm{ID}_i || \mathrm{PWD}_i || r_1 || \sigma_i\right) = \mathrm{MG}_4 G_4 \oplus h\left(h\left(K_{\mathrm{GW}}\right) || N_1\right).$$

GW为用户U生成一个新的临时身份$\mathrm{TID}_i^{\mathrm{new}}$，并将$\left\{\mathrm{TID}_i^{\mathrm{old}} = \mathrm{TID}_i, \mathrm{TID}_i^{\mathrm{new}} = \mathrm{TID}_i^{\mathrm{new}}\right\}$存储起来. GW生成随机数$N_2$，时间戳$T_2$，计算

$$\mathrm{MG}_5=N_2\oplus \mathrm{h}(K_{SD}\|T_2),$$

$$\mathrm{MG}_6=h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\oplus h\left(K_{\mathrm{SD}}\|N_2\right),$$

$$\mathrm{MG}_7=h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}\oplus h\left(K_{\mathrm{SD}}\|N_2\|T_2\right),$$

$$\mathrm{MG}_8=h\left(R_{\mathrm{SD}}\right)\oplus h\left(h\left(K_{\mathrm{SD}}\right)\|\mathrm{ID}_{\mathrm{SD}}\|T_2\|N_2\right),$$

$$\mathrm{MG}_9=h\left(h\left(\mathrm{ID}_i\|\mathrm{PWD}_i\|r_1\|\sigma_i\right)\|h\left(K_{\mathrm{GW}}\right)\|\mathrm{TID}_i\|\mathrm{TID}_i^{\mathrm{new}}\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\right).$$

GW将$\mathrm{MSG}_2=\left\{\mathrm{MG}_5,\mathrm{MG}_6,\mathrm{MG}_7,\mathrm{MG}_8,\mathrm{MG}_9,C_{\mathrm{SD}},T_2\right\}$发送给智能设备SD.

步骤3.

SD接收到信息后,检查时间戳T_2是否超时,C_{SD}是否存在于可信执行环境中,计算

$$N_2=\mathrm{MG}_5\oplus h\left(K_{\mathrm{SD}}\|T_2\right),$$

$$h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i=\mathrm{MG}_6\oplus h(K_{\mathrm{SD}}\|N_2),$$

$$h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}=\mathrm{MG}_7\oplus h\left(K_{\mathrm{SD}}\|N_2\|T_2\right),$$

$$h\left(R_{\mathrm{SD}}\right)=\mathrm{MG}_8\oplus h\left(h\left(K_{\mathrm{SD}}\right)\|\mathrm{ID}_{\mathrm{SD}}\|T_2\|N_2\right),$$

$$R_{\mathrm{SD}}^{*}=\mathrm{PUF}\left(C_{\mathrm{SD}}\right).$$

检查是否$h\left(R_{\mathrm{SD}}^{*}\right)=h\left(R_{\mathrm{SD}}\right)$,如果相同,则生成随机数$N_3$,时间戳$T_3$,计算

$$\mathrm{MG}_{10}=N_3\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right),$$

$$\mathrm{MG}_9^{*}=h\left(h\left(\mathrm{ID}_i\|\mathrm{PWD}_i\|r_1\|\sigma_i\right)\|h\left(K_{\mathrm{GW}}\right)\|\mathrm{TID}_i\|\mathrm{TID}_i^{\mathrm{new}}\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\right),$$

$$\mathrm{MG}_{11}=h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right)\oplus N_3,$$

$$\mathrm{MG}_{12}=h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right)\oplus T_3,$$

$$\mathrm{SK}=h\left(\mathrm{MG}_9\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right),$$

$$\mathrm{MG}_{13}=h\left(\mathrm{SK}\|h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}\|N_3\|T_3\right).$$

之后,SD将$\mathrm{MSG}_3=\left\{\mathrm{MG}_{10},\mathrm{MG}_{11},\mathrm{MG}_{12},\mathrm{MG}_{13},T_3\right\}$发送给$\mathrm{MD}_i$.

步骤4.

MD_i接收到信息后,检验时间戳T_3是否超时,然后计算

$$N_3=\mathrm{MG}_{10}\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right),$$

$$h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}=\mathrm{MG}_{11}\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right)\oplus N_3,$$

$$h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)=\mathrm{MG}_{12}\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i\right)\oplus T_3,$$

$$\mathrm{SK}^{*}=h\left(\mathrm{MG}_9^{*}\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right),$$

$$\mathrm{MG}_{13}^{*}=h\left(\mathrm{SK}^{*}\|h\left(K_{\mathrm{GW}}\right)\oplus \mathrm{TID}_i^{\mathrm{new}}\|N_3\|T_3\right).$$

比较是否$\mathrm{MG}_{13}^{*}=\mathrm{MG}_{13}$,如果相同则通过验证,将$\mathrm{SK}^{*}$作为通话密钥.

MD_i将身份信息更改为

$$\left\{\mathrm{TID}_i^{\mathrm{old}}=\mathrm{TID}_i,\mathrm{TID}_i^{\mathrm{new}}=\mathrm{TID}_i^{\mathrm{new}}\right\}.$$

4.2.4　链式动态CRP更新流程

当每次认证结束之后或距离上次更新后达到固定的时间后将会触发链式动态CRP更新流程,由三个步骤组成,以保证每次认证使用的挑战响应对具有唯一性和不可逆性.

步骤1.

网关GW将计数器修改成$t=t+1$,然后生成时间戳T_{Current},随机数N,生成种子:

$$\mathrm{Seed}_{\mathrm{new}}=\mathrm{HMAC}\left(\mathrm{Seed}_{\mathrm{prev}},K_{\mathrm{GW}}\|T_{\mathrm{Current}}\|t\|N\right).$$

其中,$\mathrm{Seed}_{\mathrm{prev}}$是上一次使用的种子.

GW将$\left\{\mathrm{Seed}_{\mathrm{new}},t_{\mathrm{new}},T_{\mathrm{Current}}\right\}$通过安全信道发送给$\mathrm{MD}_i$和SD.

步骤2.

移动设备MD_i和智能设备SD接收到信息后,更新计数器$t=t_{\mathrm{new}}$. MD_i使用种子$\mathrm{Seed}_{\mathrm{new}}$生成新的挑战$C_{\mathrm{new}}^{\mathrm{U}}=\mathrm{HMAC}\left(\mathrm{Seed}_{\mathrm{new}},t\|T_{\mathrm{Current}}\|\mathrm{TID}_i\right)$,然后使用该挑战生成新的响应$R_{\mathrm{new}}^{\mathrm{U}}=\mathrm{PUF}\left(C_{\mathrm{new}}^{\mathrm{U}}\right)$. SD使用种子$\mathrm{Seed}_{\mathrm{new}}$生成新的挑战$C_{\mathrm{new}}^{\mathrm{SD}}=\mathrm{HMAC}\left(\mathrm{Seed}_{\mathrm{new}},t\|T_{\mathrm{Current}}\|\mathrm{ID}_{\mathrm{SD}}\right)$,然后使用该挑战生成新的响应$R_{\mathrm{new}}^{\mathrm{SD}}=\mathrm{PUF}\left(C_{\mathrm{new}}^{\mathrm{SD}}\right)$. MD_i和SD将$C_{\mathrm{new}}^{\mathrm{U}}$和$C_{\mathrm{new}}^{\mathrm{SD}}$保存在各自的可信执行环境中,然后删除$\mathrm{Seed}_{\mathrm{new}}$和$T_{\mathrm{Current}}$.

步骤3.

MD_i和SD分别将$\left(C_{\mathrm{new}}^{\mathrm{U}},R_{\mathrm{new}}^{\mathrm{U}}\right),\left(C_{\mathrm{new}}^{\mathrm{SD}},R_{\mathrm{new}}^{\mathrm{SD}}\right)$发送给GW. 如果超时或者没有收到$\mathrm{MD}_i$和SD的返回信息,则重新生成种子,并且重新进行更新流程,直到正常更新.

链式动态CRP更新流程通过引入不可逆的哈希链,解决了需要存储多组CRP的问题,并有效抵御了去同步攻击和机器学习建模攻击.

5　安全分析

本节将进行形式化与非形式化安全分析,以证明BPIT的安全性.

5.1　ROR安全模型

为了模拟威胁模型中定义的敌手能力,本文使用真实或随机(ROR)模型来模拟真实环境下敌手的攻击行为. 攻击者的能力通过对预言机(oracle)的不同查询来模拟.

参与者. BPIT协议中的参与者包括用户U、工业智能设备SD和网关GW. 预言机U、SD和GW分别表示为Π_{U}^{t1}、Π_{SD}^{t2}和Π_{GW}^{t3}.

接受状态. 预言机Π_{X}^{t}的接受状态意味着实例Π_{X}^{t}已经接收到了会话中的最后一条预期消息. 实例Π_{X}^{t}的当前会话标识(sid)由它发送和接收的所有信息的有序连接组成.

伙伴关系. 为了使两个预言机成为彼此的伙伴,它们必须满足以下条件:

(1)它们都处于接受状态;

(2)它们互相认证并且有相同的sid;

(3)它们是彼此的伙伴.

新鲜性. 新鲜性意味着预言机及其伙伴创建的会话密钥尚未泄露给A.

敌手模型. 为了模拟敌手的能力,敌手A可以执行以下几种针对协议的查询.

Execute$(\Pi_U^{t1},\Pi_{SD}^{t2},\Pi_{GW}^{t3})$:敌手A可以使用此查询获取协议中所有传输的消息.

Send(Π_X^t,m):执行此查询时,敌手A向预言机Π_X^t发送消息m并从Π_X^t获得回复.

CorruptMD(Π_U^{t1}):此查询模拟了用户的移动设备MD被盗窃的情况,敌手A执行此查询时可以获取MD中存储的秘密信息.

CorruptSD(Π_{SD}^{t2}):此查询模拟了智能设备SD被盗窃的情况,敌手A执行此查询时可以获取SD中存储的秘密信息.

Hash(RO):此查询用于访问一个随机预言机. 加密哈希函数$h(\cdot)$被建模为一个随机预言机,所有协议参与者以及敌手A都可以对其进行查询.

Test(Π_X^t):一旦执行了这个查询,预言机会输出一个会话密钥SK或一个随机数. Test查询的输出由一个随机位b决定. 如果$b=1$,则返回会话密钥SK;如果$b=0$,则返回一个随机数给A.

语义安全性. 敌手A可以多次执行Execute、Send、CorruptMD、CorruptSD和Hash查询预言机,然后使用Test查询来猜测隐藏位b的值. 如果Test查询的结果是b',并且$b'=b$,则敌手A赢得游戏. 让Succ表示A赢得游戏的事件. 敌手A打破协议语义安全性的优势定义为

$$\mathrm{Adv}_{AKA}^{BPIT}(A)=\left|2\cdot\Pr[\mathrm{Succ}]-1\right|.$$

5.2 形式化安全分析

定理1 假设A是一个在ROR模型下运行的多项式时间攻击者. q_f、q_h、q_s、$|\mathrm{Hash}|$、l分别表示PUF查询次数、哈希查询次数、Send操作的查询次数、哈希函数的范围空间、生物特征密钥σ_i的位数. 若A不能以可忽略的优势成功攻击本文协议,则认为本文协议是安全的[29]. 假设敌手A打破BPIT语义安全性的优势为

$$\mathrm{Adv}_{AKA}^{BPIT}(A)\leqslant\frac{q_h^2}{2|\mathrm{Hash}|}+\frac{q_f^2}{2|\mathrm{PUF}|}+\frac{q_s}{2^m}.$$

证明 与现有认证协议的证明方法[32]类似,定理1的证明由一系列游戏$G_i(i=0,1,2,3,4)$组成. 让Succ_i表示敌手正确猜测随机位b的事件,且$\Pr[\mathrm{Succ}_i]$表示敌手在游戏G_i中获胜的概率.

游戏G_0:在G_0中,敌手A仅去猜测随机位b,不执行任何查询操作. 根据BPIT的语义安全性,可以得到

$$\mathrm{Adv}_{AKA}^{BPIT}(A)=\left|2\cdot\Pr[\mathrm{Succ}_0]-1\right| \tag{1}$$

游戏G_1:在G_1中,敌手A被认为执行了Execute查询来进行监听攻击,因而可以拦截所有交换的信息

$$\mathrm{MSG}_1=\{\mathrm{MG}_1,\mathrm{MG}_2,\mathrm{MG}_3,\mathrm{MG}_4,\mathrm{TID}_i,T_1,C_U\},$$

$$\mathrm{MSG}_2=\{\mathrm{MG}_5,\mathrm{MG}_6,\mathrm{MG}_7,\mathrm{MG}_8,\mathrm{MG}_9,C_{SD},T_2\},$$

$$\mathrm{MSG}_3=\{\mathrm{MG}_{10},\mathrm{MG}_{11},\mathrm{MG}_{12},\mathrm{MG}_{13},T_3\}.$$

其中的关键信息均使用了哈希函数进行了隐藏,并且计算会话密钥SK需要K_{GW},K_{SD},N_2,N_3.

敌手A仅使用Execute查询无法得到这些参数,进而无法计算会话密钥. 因此,敌手A在游戏中的优势并没有增加,那么有

$$\Pr[\mathrm{Succ}_0]=\Pr[\mathrm{Succ}_1] \tag{2}$$

游戏G_2:游戏G_2在G_1的基础上增加了Send和Hash查询,以模拟一个真实的攻击. 在这种攻击中,敌手A可以通过Send查询得到伪造的消息,再使用Hash查询进行哈希碰撞. 因为本文使用的Hash函数具有抗碰撞性,并且所有的信息都带有时间戳和随机数,根据生日悖论,得出哈希碰撞的概率为$\frac{q_h^2}{2|\mathrm{Hash}|}$,得到

$$\left|\Pr[\mathrm{Succ}_2]-\Pr[\mathrm{Succ}_1]\right|\leqslant\frac{q_h^2}{2|\mathrm{Hash}|} \tag{3}$$

游戏G_3:游戏G_3在G_2的基础上增加了Send和PUF查询,由于$\mathrm{PUF}(\cdot)$和$h(\cdot)$都是单向函数,并且使用随机预言机模拟,与G_2类似,得到

$$\left|\Pr[\mathrm{Succ}_3]-\Pr[\mathrm{Succ}_2]\right|\leqslant\frac{q_f^2}{2|\mathrm{PUF}|} \tag{4}$$

游戏G_4:游戏G_4在G_3的基础上增加了CorruptMD查询,模拟了用户的移动设备被盗窃的情况. 敌手A可以从移动设备中获得信息:$\{B_i,C_i,\mathrm{Auth}_i,\mathrm{TID}_i^{old}=\mathrm{null},\mathrm{TID}_i^{new}=\mathrm{TID}_i\}$,敌手A依然无法计算出会话密钥SK. 敌手可以根据$h(K_{GW})$来猜测K_{GW}得到长期密钥. 假设K_{GW}的长度是m,那么猜测出K_{GW}的概率为$1/2^m$. 则敌手A在游戏中的优势增加为

$$\left|\Pr[\mathrm{Succ}_4]-\Pr[\mathrm{Succ}_3]\right|\leqslant\frac{q_s}{2^m} \tag{5}$$

游戏G_5:游戏G_5在游戏G_4的基础上增加了CorruptSD查询,模拟了智能设备被盗窃的情况. 敌手A可以从智能设备获取到信息$\{\mathrm{ID}_{SD},K_{SD}\}$,根据这些无法计算出

$$\mathrm{SK}=h\left(\mathrm{MG}_9\|h(K_{SD}\|N_2\|T_2)\|N_3\|T_3\right),$$

$MG_9=$

$h\left(h\left(\mathrm{ID}_i\|\mathrm{PWD}_i\|r_1\|\sigma_i\right)\|h\left(K_{\mathrm{GW}}\right)\|\mathrm{TID}_i\|\mathrm{TID}_i^{\mathrm{new}}\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\right)$.

因此,敌手A的优势并没有增加,得到

$$\Pr\left[\mathrm{Succ}_5\right]=\Pr\left[\mathrm{Succ}_4\right] \tag{6}$$

敌手A已经执行了所有的查询,如果敌手A想要赢得游戏,就必须用Test查询猜测隐藏的随机位b,因此有

$$\Pr\left[\mathrm{Succ}_5\right]=\frac{1}{2} \tag{7}$$

根据式(1)~式(7),可以得到

$$\mathrm{Adv}_{\mathrm{AKA}}^{\mathrm{BPIT}}(\mathrm{A})\leqslant\frac{q_h^2}{2|\mathrm{Hash}|}+\frac{q_f^2}{2|\mathrm{PUF}|}+\frac{q_s}{2^m}.$$

证毕.

5.3 非形式化安全分析

安全属性,也称为安全特性,即认证方案想要实现的安全目标[2]. 结合形式化与非形式化的安全分析方法,有助于全面评估协议的安全属性. 因此,本节将通过非形式化的安全分析来评估BPIT协议的安全属性.

(1)匿名性和不可跟踪性

在本协议中,所有参与实体均具备匿名性与不可追踪性. 协议中未使用明文传输真实身份,而是采用临时标识符和哈希函数来隐藏真实身份信息. 敌手无法通过窃听通信内容来获取实体的真实身份,从而保障了匿名性. 此外,每次会话后,实体的临时标识符都会更新,并且每条信息都包括时间戳和随机数,从而确保每次会话的内容均不同,这也有效地保障了不可追踪性.

(2)完美前向保密性

协议中的挑战生成基于HMAC和种子,并且依赖上一次使用的种子来生成挑战. 即使敌手获取到当前会话的挑战响应对,也无法推导出先前的挑战响应对. 因此,协议的会话密钥是动态生成的,并不依赖于历史密钥,这保证了完美前向保密性. 具体地,本协议中的会话密钥:

$$\mathrm{SK}=h\left(\mathrm{MG}_9\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right).$$

其中,包含了随机数与时间戳,这确保了每次会话的密钥独立且不可追溯.

(3)用户假冒攻击

为了假冒用户,敌手A需要构造信息$\left\{\mathrm{MG}_1,\mathrm{MG}_2,\mathrm{MG}_3,\mathrm{MG}_4,\mathrm{TID}_i,T_1,C_{\mathrm{U}}\right\}$,而这一过程需要获取用户的密码、生物特征、移动设备的PUF响应以及由随机数保护的秘密参数. 即使敌手A可以伪造随机数和时间戳,也无法同时获得其他秘密信息和移动设备,因此在认证阶段无法成功假冒用户发送信息进行攻击.

(4)重放攻击

协议中的信息包含随机数和时间戳,且每次会话的挑战响应对均基于先前的种子生成. 因此,每次会话的信息都是唯一的,无法与之前会话的信息重复. 且协议中的链式动态CRP动态更新流程保证了挑战生成的不可逆哈希链,每个挑战只在对应的会话生效,敌手A无法通过重放历史会话使用的挑战响应对来达到重放攻击. 以上两点使得协议能够有效防止重放攻击.

(5)智能设备假冒攻击

要假冒智能设备,敌手A需要构造$\mathrm{MSG}_3=\left\{\mathrm{MG}_{10},\mathrm{MG}_{11},\mathrm{MG}_{12},\mathrm{MG}_{13},T_3\right\}$,即使敌手可以伪造随机数和时间戳,但无法获取其他的秘密信息,如不能计算

$$\mathrm{MG}_{10}=N_3\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i\right),$$

$$\mathrm{MG}_{11}=h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i^{\mathrm{new}}\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i\right)\oplus N_3,$$

$$\mathrm{MG}_{12}=h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\oplus h\left(h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i\right)\oplus T_3,$$

$$\mathrm{SK}=h\left(\mathrm{MG}_9\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right),$$

$$\mathrm{MG}_{13}=h\left(\mathrm{SK}\|h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i^{\mathrm{new}}\|N_3\|T_3\right).$$

并且敌手A无法伪造合法设备的$\mathrm{ID}_{\mathrm{SD}}$. 因此,敌手A无法在认证阶段假冒智能设备进行攻击.

(6)移动设备被盗攻击

如果用户的移动设备被盗,敌手A能够获取设备中存储的信息$\left\{B_i,C_i,\mathrm{Auth}_i,\mathrm{TID}_i^{\mathrm{old}}=\mathrm{null},\mathrm{TID}_i^{\mathrm{new}}=\mathrm{TID}_i\right\}$. 然而,由于TEE确保设备中的挑战数据是受保护的,攻击者无法直接访问这些信息以进行挑战响应对的分析. 同时,由于

$$B_i=r_1\oplus h\left(\mathrm{ID}\|\mathrm{PWD}\|\sigma_i\right),$$

$$C_i=h\left(K_{\mathrm{GW}}\right)\oplus h\left(\mathrm{RID}\|\mathrm{RPWD}\|\sigma_i\right),$$

$$\mathrm{Auth}_i=h\left(h\left(\mathrm{RID}\|\mathrm{RPWD}\|\sigma_i\right)\oplus r_1\oplus h\left(K_{\mathrm{GW}}\right)\right).$$

如果敌手A想要计算上面的信息,需要同时知道用户的密码和生物特征,这是不可行的. 因此,本协议有效抵御移动设备被盗攻击.

(7)智能设备被盗攻击

如果工业智能设备被盗,敌手A将能够获取工业智能设备存储的信息$\left\{\mathrm{ID}_{\mathrm{SD}},K_{\mathrm{SD}}\right\}$. 同移动设备被盗攻击,敌手A无法直接获取到智能设备中存储的挑战. 敌手A根据智能设备中存储的信息无法计算出通话密钥. 因此,本协议可以抵抗智能设备被盗攻击.

(8)去同步攻击

假设敌手A可以拦截协议中发出的信息并尝试发起去同步攻击. 本协议通过引入了链式CRP动态更新流程,保证了每次认证之后挑战响应对的更新,以及每次认证都使用了随机生成的随机数和时间戳. 并且,认证的双方还保存了新旧两个临时身份,即使攻击者发

起了去同步攻击，在下一次会话时仍然可以在验证方找到临时身份，并且链式CRP动态更新流程保证了认证实体验证挑战响应对的同步性. 因此，本协议可以抵抗去同步攻击.

(9)中间人攻击

协议的消息均通过哈希函数绑定随机数和时间戳，敌手A更改协议中的信息会导致认证失败. 此外，协议采用PUF进行验证，敌手A无法通过软件手段复制或预测PUF响应. 每次会话后，链式CRP动态更新流程，确保挑战响应对的更新，从而有效防止了中间人攻击.

(10)相互认证

在BPIT中，所有的实体都可以成功进行相互认证. 收到 $\mathrm{MSG}_1=\{\mathrm{MG}_1,\mathrm{MG}_2,\mathrm{MG}_3,\mathrm{MG}_4,\mathrm{TID}_i,T_1,C_{\mathrm{U}}\}$ 后，GW验证CRP与 $\mathrm{ID}_{\mathrm{SD}}$ 是否正确，如果正确则GW验证 MD_i. 收到 $\mathrm{MSG}_2=\{\mathrm{MG}_5,\mathrm{MG}_6,\mathrm{MG}_7,\mathrm{MG}_8,\mathrm{MG}_9,C_{\mathrm{SD}},T_2\}$ 后，SD验证CRP是否正确，如果正确则SD验证GW.

MD_i 收到 $\mathrm{MSG}_3=\{\mathrm{MG}_{10},\mathrm{MG}_{11},\mathrm{MG}_{12},\mathrm{MG}_{13},T_3\}$ 后，验证 $\mathrm{MG}_{13}^*=h\left(\mathrm{SK}^*\|h\left(K_{\mathrm{GW}}\right)\oplus\mathrm{TID}_i^{\mathrm{new}}\|N_3\|T_3\right)$ 是否等于 MG_{13}. 如果正确，则 MD_i 验证SD，并且生成会话密钥 $\mathrm{SK}=h\left(\mathrm{MG}_9\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right)$.

(11)特权内幕攻击

假设一个特权内幕的攻击者知道用户注册时传给网关的信息 $\{\mathrm{RID},\mathrm{RPWD}\}$ 和 $\{R_{\mathrm{U}}\}$，由于 R_{U} 是PUF生成的响应，敌手A无法计算出对应的挑战 C_{U}，也无法根据这些信息计算出会话密钥. 即使敌手A还窃取了移动设备，并且能够提取移动设备中存储的信息

$$\{B_i,C_i,\mathrm{Auth}_i,\mathrm{TID}_i^{\mathrm{old}}=\mathrm{null},\mathrm{TID}_i^{\mathrm{new}}=\mathrm{TID}_i\}.$$

但若不知道用户的用户名、密码和生物特征等信息，敌手A仍不能成功登录移动设备，也不能计算出会话密钥. 因此，本协议能够有效抵御特权内幕攻击.

(12)机器学习建模攻击

敌手A可以通过长期窃听认证过程收集大量CRP，利用机器学习算法(如神经网络、支持向量机)训练模型，预测PUF对任意挑战的响应. 本协议通过链式动态更新CRP机制形成了不可逆不可预测的哈希链，并且使用TEE保护了CRP的泄露，有效解决了传统PUF协议中CRP易被建模的缺陷.

(13)登录失败处理

在认证过程中，如果验证失败，将立即终止会话以防止暴力破解.

(14)会话密钥协商

在确认网关身份之后，智能设备会生成一个会话密钥 $\mathrm{SK}=h\left(\mathrm{MG}_9\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right)$，当移动设备确认智能设备身份之后，移动设备将会生成一个相同的会话密钥 $\mathrm{SK}^*=h\left(\mathrm{MG}_9^*\|h\left(K_{\mathrm{SD}}\|N_2\|T_2\right)\|N_3\|T_3\right)$. 因此在认证结束之后，智能设备与移动设备之间的会话密钥将会被创建.

(15)离线密码猜测攻击

假设敌手A试图通过离线枚举移动设备密码以得到敏感信息. BPIT中移动设备存储的身份信息由用户密码和生物特征组合. 又由

$$\mathrm{Auth}_i^*=h\left(h\left(\mathrm{RID}_i\|\mathrm{RPWD}_i\|\sigma_i^*\right)\oplus r_1^*\oplus h^*\left(K_{\mathrm{GW}}\right)\right),$$

可知，敌手A必须同时获得密码与生物特征才能伪造验证信息，这是不可能做到的. 因此，本协议可以有效抵抗离线密码猜测攻击.

6 性能分析

本节将进行BPIT协议与一些物联网认证协议[33~38]在认证阶段安全属性、通信代价、计算代价的比较分析，以证明BPIT协议在工业5.0环境下的适配性.

6.1 安全属性

本小节以15个核心安全属性为标准，对BPIT协议及相关协议进行安全属性的对比分析.

文献[33]所提出的协议不具有匿名性和不可跟踪性，并且不能抵抗移动设备被盗攻击、智能设备被盗攻击和去同步攻击. 文献[34]所提出的协议存在用户假冒、智能设备假冒和去同步攻击的安全隐患. 文献[35]所提出的协议在智能设备被盗和去同步攻击下存在安全问题. 文献[36]无法抵抗智能设备被盗攻击. 文献[37]使用了PUF并且声称可以抵御设备被窃攻击和机器学习建模攻击，但在提出的协议中并没有更新和保护CRP的机制，攻击者可以通过窃取智能设备和移动设备进行侧信道攻击获取到CRP或者通过机器学习建模攻击的方法预测响应值. 因此，该协议不能防御设备被窃攻击、机器学习建模攻击且不满足完美前向保密性. 文献[38]所提出的协议声称具有前向完美保密性，但如果长期密钥泄露，攻击者可利用历史信息推导出过往会话密钥，因此不具备完美前向保密性. 本文所提出的BPIT协议较相关协议实现了更多的安全属性，可以抵抗更多的攻击，更加适合工业5.0环境下使用.

表2展示了相关协议的安全属性，其中 S_1 指移动设备被盗攻击，S_2 指智能设备被盗攻击，S_3 指重放攻击，S_4 指用户假冒攻击，S_5 指智能设备假冒攻击，S_6 指匿名性，S_7 指不可跟踪性，S_8 指去同步攻击，S_9 指中间人攻击，S_{10} 指特权内幕攻击，S_{11} 指完美前向安全保密性，S_{12} 指机器学习建模攻击，S_{13} 指登录尝试失败，S_{14} 指相互认证，S_{15} 指离线密码猜测攻击.

表2　相关协议的安全属性

安全属性	文献[33]	文献[34]	文献[35]	文献[36]	文献[37]	文献[38]	BPIT
S_1	×	√	√	√	×	√	√
S_2	×	√	√	×	×	√	√
S_3	√	√	√	√	√	√	√
S_4	√	×	√	√	√	√	√
S_5	√	×	√	√	√	√	√
S_6	×	√	√	√	√	√	√
S_7	×	√	√	√	√	√	√
S_8	×	√	×	√	√	√	√
S_9	√	√	√	√	√	√	√
S_{10}	√	√	√	√	√	√	√
S_{11}	√	√	√	√	×	×	√
S_{12}	√	√	√	√	×	√	√
S_{13}	√	√	√	√	√	√	√
S_{14}	√	√	√	√	√	√	√
S_{15}	√	√	√	√	√	√	√

6.2　通信代价

通信代价主要取决于协议中定义的消息结构及其大小,可以通过静态分析方式进行精确估算. 由于其不依赖于具体实现平台或运行环境,理论计算具有较强的通用性与可比性. 因此本文使用通信中认证过程的交换信息的总位数来表示通信代价. 假设身份、伪身份、临时身份、临时交互号、会话钥、PUF的挑战和响应的长度都是128 bits,时间戳是32 bits,哈希摘要和MAC长度是256 bits,对称加密/解密块大小是128 bits. 表3展示了相关协议的通信代价.

表3　通信代价比较

协议	通信代价/bits
文献[33]	2 656
文献[34]	2 688
文献[35]	3 840
文献[36]	4 672
文献[37]	2 880
文献[38]	3 840
BPIT	3 808

文献[33]~文献[36]的总通信代分别为(1 824+288+544)=2 656 bits,(1 536+384+384+384)=2 688 bits,(672+1 056+768+1 344)=3 840 bits,(1 568+1 056+672+1 376)=4 672 bits,文献[37]的通信代价为(928+704+288+960)=2 880 bits,文献[38]的通信代价为(672+1 056+800+1 312)=3 840 bits. 而在本协议认证过程中需要交换的信息分别是

$$\{\mathrm{MG}_1,\mathrm{MG}_2,\mathrm{MG}_3,\mathrm{MG}_4,\mathrm{TID}_i,T_1,C_{\mathrm{U}}\},$$

$$\{\mathrm{MG}_{10},\mathrm{MG}_{11},\mathrm{MG}_{12},\mathrm{MG}_{13},T_3\},$$

$$\{\mathrm{MG}_5,\mathrm{MG}_6,\mathrm{MG}_7,\mathrm{MG}_8,\mathrm{MG}_9,C_{\mathrm{SD}},T_2\}.$$

它们的位长分别是(256+256+256+256+128+32+128)=1 312 bits,(256+256+256+256+32)=1 056 bits,(256+256+256+256+256+128+32)=1 440 bits,因此BPIT协议认证过程总的通信代价为(1 312+1 056+1 440)=3 808 bits.

由表3可知,文献[33]、文献[34]和文献[37]的通信代价最低. 但由表2可知,三者不满足一些关键的安全属性,并且由6.3节可知,计算代价也高于本文协议,同时文献[35]在通信代价与计算代价上略高于本文协议,并且本文协议相较于文献[35]实现了更多的安全属性. 综上所述,本文协议在确保满足关键安全属性的同时实现了更低的通信代价.

6.3　计算代价

本小节首先使用协议中所有参与方执行密码原语的总操作时间来评估计算代价. 令T_h、T_e、T_{epm}、T_{mac}、T_{hmac}、T_{puf}分别表示哈希函数、对称密码加密或者解密、ECC点乘、MAC、哈希MAC和PUF的运算时间. 为保证计算方法的统一性,本文使用已有论文的实验结果[28,37,39]以在同一标准下对对比协议的计算代价进行估算,现有实验在以下设备上进行了模拟实验:用户设备MD_i使用HTC One X(搭载890 MHz ARM Cortex-A9 MPCore处理器),工业智能设备SD使用MSB-430模块化传感器板(采用T1 MSP430微控制器和TMP36温度传感器),网关GW使用Intel Core i5-2500处理器笔记本电脑(主频3.3 GHz),实验使用JPBC库Pbc-05.14和JCE库来评估密码原语的执行时间,并且$T_h \approx T_{\mathrm{mac}} \approx T_{\mathrm{hmac}}$,密码源语近似操作时间如表4所示.

在文献[33]的协议中,移动设备的执行时间是

表4 密码原语近似运行时间 单位:ms

设备	T_h	T_e	T_{epm}	T_{puf}
移动设备	0.067	0.085	13.56	0.023
智能设备	1.420	2.180	21.82	0.023
网关	0.037	0.055	8.77	—

$10T_h+3T_e+2T_{hmac}+2T_{epm}\approx28.179$ ms,智能设备的执行时间 $1T_h+1T_e\approx3.6$ ms,网关的执行时间是 $11T_h+4T_e+2T_{hmac}+22T_{epm}\approx18.241$ ms,总计算代价为50.020 ms. 在文献[34]的协议中,移动设备、智能设备、网关的执行时间分别是 $2T_{epm}+3T_h\approx27.321$ ms,$3T_h\approx4.26$ ms,$1T_{epm}+7T_h\approx9.029$ ms,总计算代价为40.610 ms. 文献[35]的协议中,移动设备、智能设备、网关的执行时间分别是 $4T_h+1T_e\approx0.353$ ms,$10T_h+1T_e\approx16.38$ ms,$9T_h+2T_e\approx0.443$ ms,总计算代价为17.176 ms. 文献[36]的协议中,移动设备、智能设备、网关的执行时间是 $T_{puf}+13T_h+2T_{epm}+T_e\approx28.099$ ms,$T_{puf}+12T_h+T_{epm}\approx38.883$ ms,$T_{epm}+19T_h\approx9.473$ ms,总计算代价为76.455 ms. 文献[37]的协议中,移动设备、智能设备、网关的执行时间分别是 $9T_h\approx0.603$ ms,$10T_h+2T_e\approx18.56$ ms,$5T_h+2T_e\approx0.295$ ms,总计算代价为19.458 ms. 文献[38]的协议中,移动设备、智能设备、网关的执行时间分别是 $10T_h\approx0.67$ ms,$7T_h+1T_{epm}\approx31.76$ ms,$14T_h\approx0.518$ ms,总计算代价为32.948 ms.

由表5计算代价对比结果可知,本文提出的协议计算代价最低,本文提出的协议采用Hash、PUF轻量化密码操作,平均减少了约54%的计算开销.

本文进一步补充了在实际运行环境下的计算成本差异分析. 具体而言,我们在一台配备Intel i5-12400F 2.50 GHz CPU和16 GB内存的台式机上,基于Python 3.11.9环境,对各项密码学原语分别执行了1 000次迭代,并计算其平均耗时. 同时,本文基于Python的socket、hashlib、numpy等库,对所提出的协议及对比方案进行了端到端仿真,得出了不同协议在实际运行中的认证总开销,从而为计算成本比较提供了更具可操作性和参考价值的实验依据. 各密码学原语的平均耗时结果如表6所示.

表5 相关协议计算代价 单位:ms

协议	MD	SD	GW	总代价
文献[33]	$10T_h+3T_e+2T_{hmac}+2T_{epm}\approx28.179$	$1T_h+1T_e\approx3.6$	$11T_h+4T_e+2T_{hmac}+22T_{epm}\approx18.241$	50.020
文献[34]	$2T_{epm}+3T_h\approx27.321$	$3T_h\approx4.26$	$1T_{epm}+7T_h\approx9.029$	40.610
文献[35]	$4T_h+1T_e\approx0.353$	$10T_h+1T_e\approx16.38$	$9T_h+2T_e\approx0.443$	17.176
文献[36]	$T_{puf}+13T_h+2T_{epm}+T_e\approx28.099$	$T_{puf}+12T_h+T_{epm}\approx38.883$	$T_{epm}+19T_h\approx9.473$	76.455
文献[37]	$9T_h\approx0.603$	$10T_h+2T_e\approx18.56$	$5T_h+2T_e\approx0.295$	19.458
文献[38]	$10T_h\approx0.67$	$7T_h+T_{epm}\approx31.76$	$14T_h\approx0.518$	32.948
BPIT	$17T_h+1T_{puf}\approx1.162$	$11T_h+T_{puf}\approx15.643$	$9T_h\approx0.356$	17.161

表6 实际环境中密码原语的平均耗时

密码原语	描述	平均耗时/ms
T_h	哈希函数(采用SHA-3)	0.002 0
T_e	对称加密或解密	0.004 5
T_{epm}	ECC点乘	1.561 5
T_{puf}	PUF生成	0.002 0

而表7则给出了协议仿真的理论计算开销与实际测得总耗时的对比情况. 由表7可见,在本次仿真测试中,本文所提出的BPIT协议在理论计算开销与实际测得耗时方面均表现出最优,充分体现了所设计方案的轻量化特性. 需要指出的是,理论估算值与仿真得到的实际值之间存在一定差异,主要原因在于:尽管各密码学操作在理想条件下单独测得了平均执行时间,实际系统运行时仍需考虑函数调用、上下文切换、内存读写、I/O等待以及可能的任务抢占等不可忽略的系统开销,这些因素共同导致协议的端到端实际耗时往往大于单一操作耗时的简单累加. 值得注意的是,通信代价本应体现为通信双方交换数据的总位数(包括消息长度、协议轮数等),而在本研究的端到端实验中,所测得的运行时间实际上已隐含了通信延迟的影响,例如数据传输过程中所需的等待时间以及多轮交互带来的累积开销. 因此,本文基于实际仿真的端到端耗时更能真实反映方案在工业物联网(IIoT)场景下的计算性能开销.

表7 相关协议的理论计算代价与模拟计算代价 单位:ms

协议	理论计算代价	模拟计算代价
文献[33]	37.524	39.258
文献[34]	4.783	10.032
文献[35]	0.064	5.234
文献[36]	6.330	8.398
文献[37]	0.066	5.567
文献[38]	1.622	7.782
BPIT	0.062	4.608

7 结论

本研究针对工业5.0中智能设备的动态认证与密钥协商问题,提出基于物理不可克隆函数(PUF)与可信执行环境(TEE)的轻量级匿名协议BPIT. 该协议通过

链式CRP动态更新机制与TEE硬件安全防护,实现三方认证与密钥协商. 采用轻量级哈希优化消息流,降低通信开销,适配资源受限设备. 协议通过链式CRP防御物理攻击、随机数-时间戳策略抵御中间人攻击、双向同步消除去同步风险,构建针对设备假冒等威胁的多维度防御. 经ROR模型证明安全且可抵抗多种已知攻击. 与现有方案相比,BPIT在可接受通信代价和更低计算代价下支持更多安全属性,适用于工业5.0物联网环境.

参考文献

[1] 彭磊. 新基建时代如何保障工业互联网数据安全[J]. 中国工业和信息化, 2021, 8: 38-44.
PENG L. How to ensure the security of industrial Internet data in the new infrastructure era[J]. China Industry & Information Technology, 2021, 8: 38-44. (in Chinese)

[2] GUO Y M, GUO Y J, XIONG P, et al. Deeper insight into why authentication schemes in IoT environments fail to achieve the desired security[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4615-4627.

[3] GUO Y M, GUO Y J. CS-LAKA: A lightweight authenticated key agreement protocol with critical security properties for IoT environments[J]. IEEE Transactions on Services Computing, 2023, 16(6): 4102-4114.

[4] TANVEER M, ALKHAYYAT A, KHAN A U, et al. REAP-IIoT: Resource-efficient authentication protocol for the industrial Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(23): 24453-24465.

[5] LI N, MA M D, WANG H. ASAP-IIOT: An anonymous secure authentication protocol for industrial Internet of Things[J]. Sensors, 2024, 24(4): 1243.

[6] JAIN U, TRIPATHI A, KUMAR S, et al. Simple, secure and lightweight authentication protocol with session-key generation for IIoT device in IIoT networks[J]. Microsystem Technologies, 2025, 31(2): 299-311.

[7] VINOTH R, DEBORAH L J. An efficient key agreement and authentication protocol for secure communication in industrial IoT applications[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(3): 1431-1443.

[8] SADHU P K, ABDELGAWAD A. PMVU Auth. Physical unclonable function and machine learning based zero knowledge internet of vehicle unlock and authentication framework[EB/OL]. (2023-08-18) [2025-05-05]. https://www.techrxiv.org/doi/full/10.36227/techrxiv.23891277.

[9] ZHANG Y, LI B, WU J X, et al. Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT[J]. IEEE Internet of Things Journal, 2022, 9(22): 22501-22515.

[10] YI F M, ZHANG L, XU L J, et al. WSNEAP: An efficient authentication protocol for IIoT-oriented wireless sensor networks[J]. Sensors, 2022, 22(19): 7413.

[11] KHARGHANI E, ALIAKBARI S, BIDAD J, et al. A lightweight authentication protocol for M2M communication in IIoT using physical unclonable functions[C]// 2023 31st International Conference on Electrical Engineering (ICEE). Piscataway: IEEE, 2023: 676-683.

[12] AYUB M F, LI X, MAHMOOD K, et al. Secure consumer-centric demand response management in resilient smart grid as industry 5.0 application with blockchain-based authentication[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 1370-1379.

[13] GAO Y M, ZHOU T Q, ZHENG W Y, et al. High-availability authentication and key agreement for Internet of Things-based devices in industry 5.0[J]. IEEE Transactions on Industrial Informatics, 2024, 20(12): 13571-13579.

[14] 袁征, 张跃飞, 冯笑, 等. 基于PUF的电力物联网智能终端认证协议[J]. 信息网络安全, 2025, 25(1): 13-26.
YUAN Z, ZHANG Y F, FENG X, et al. PUF-based smart terminal authentication protocol for power Internet of Things[J]. Netinfo Security, 2025, 25(1): 13-26. (in Chinese)

[15] TIAN C, MA J F, LI T, et al. Provably and physically secure UAV-assisted authentication protocol for IoT devices in unattended settings[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4448-4463.

[16] MAJERNÍK M, DANESHJO N, MALEGA P, et al. Sustainable development of the intelligent industry from industry 4.0 to industry 5.0[J]. Advances in Science and Technology Research Journal, 2022, 16(2): 12-18.

[17] ZHANG T, SHEN J, YANG H J, et al. Sustainable authentication and key agreement protocol using chaotic maps for industry 5.0[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 1580-1589.

[18] XU Z S, LIANG W, LI K C, et al. A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(10): 7118-7127.

[19] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[20] GAO Y S, AL-SARAWI S F, ABBOTT D. Physical un-

clonable functions[J]. Nature Electronics, 2020, 3(2): 81-91.

[21] KRAWCZYK H, BELLARE M, CANETTI R. HMAC: Keyed-Hashing for Message Authentication, RFC 2104[S/OL]. [2025-06-30]. https://datatracker. ietf. org/doc/html/rfc2104.

[22] 范冠男, 董攀. 基于TrustZone的可信执行环境构建技术研究[J]. 信息网络安全, 2016, 16(3): 21-27.
FAN G N, DONG P. Research on trusted execution environment building technology based on TrustZone[J]. Netinfo Security, 2016, 16(3): 21-27. (in Chinese)

[23] 杜冬冬, 杨璧丞, 余炀, 等. SegTEE: 面向小型端侧设备的可信执行环境系统[J]. 计算机学报, 2025, 48(1): 188-209.
DU D D, YANG B C, YU Y, et al. SegTEE: Trusted execution environment for lightweight edge devices[J]. Chinese Journal of Computers, 2025, 48(1): 188-209. (in Chinese)

[24] 付裕, 林璟锵, 冯登国. 虚拟化与密码技术应用: 现状与未来[J]. 密码学报(中英文), 2024, 11(1): 3-21.
FU Y, LIN J Q, FENG D G. When virtualization meets applied cryptography: Current status and future trend[J]. Journal of Cryptologic Research, 2024, 11(1): 3-21. (in Chinese)

[25] AITCHISON C, BUCKLE R, CH'NG A, et al. On the integration of physically unclonable functions into ARM TrustZone security technology[C]//2020 European Conference on Circuit Theory and Design. Piscataway: IEEE, 2020: 1-4.

[26] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[27] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[M]// Advances in Cryptology — EUROCRYPT 2001. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 453-474.

[28] 郭奕旻, 张振峰, 熊平, 等. 基于PUF的轻量级雾辅助物联网认证协议[J]. 计算机学报, 2022, 45(7): 1412-1430.
GUO Y M, ZHANG Z F, XIONG P, et al. PUF-based lightweight authentication protocols for fog assisted IoT[J]. Chinese Journal of Computers, 2022, 45(7): 1412-1430. (in Chinese)

[29] 范馨月, 刘洁, 何嘉辉. V2G中基于PUF的轻量级匿名认证协议[J]. 通信学报, 2024, 45(10): 129-141.
FAN X Y, LIU J, HE J H. Lightweight PUF-based anonymous authentication protocol in V2G[J]. Journal on Communications, 2024, 45(10): 129-141. (in Chinese)

[30] 夏卓群, 苏潮, 徐梓桑, 等. 基于物理不可克隆函数的轻量级可证明安全车联网认证协议[J]. 电子与信息学报, 2024, 46(9): 3788-3796.
XIA Z Q, SU C, XU Z S, et al. A lightweight and provably secure authentication protocol for internet of vehicles using physical unclonable function[J]. Journal of Electronics & Information Technology, 2024, 46(9): 3788-3796. (in Chinese)

[31] 邹光南, 尤启迪, 金星虎, 等. 面向车联网车辆的轻量级持续身份认证协议[J]. 电子学报, 2024, 52(6): 1903-1910.
ZOU G N, YOU Q D, JIN X H, et al. Lightweight continuous authentication protocol for vehicles in vehicular networks[J]. Acta Electronica Sinica, 2024, 52(6): 1903-1910. (in Chinese)

[32] GUO Y M, ZHANG Z F, GUO Y J. Anonymous authenticated key agreement and group proof protocol for wearable computing[J]. IEEE Transactions on Mobile Computing, 2022, 21(8): 2718-2731.

[33] NAOUI S, ELHDHILI M E, SAIDANE L A. Lightweight and secure password based smart home authentication protocol: LSP-SHAP[J]. Journal of Network and Systems Management, 2019, 27(4): 1020-1042.

[34] GUPTA A, TRIPATHI M, SHAIKH T J, et al. A lightweight anonymous user authentication and key establishment scheme for wearable devices[J]. Computer Networks, 2019, 149: 29-42.

[35] WAZID M, DAS A K, ODELU V, et al. Secure remote user authenticated key establishment protocol for smart home environment[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(2): 391-406.

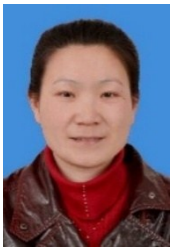
[36] JIANG Q, ZHANG X, ZHANG N, et al. Three-factor authentication protocol using physical unclonable function for IoV[J]. Computer Communications, 2021, 173: 45-55.

[37] YU S, PARK K. PUF-based robust and anonymous authentication and key establishment scheme for V2G networks[J]. IEEE Internet of Things Journal, 2024, 11(9): 15450-15464.

[38] CHEN C M, CHEN Z T, KUMARI S, et al. LAP-IoHT: A lightweight authentication protocol for the Internet of health things[J]. Sensors, 2022, 22(14): 5401.

[39] POH G S, GOPE P, NING J T. PrivHome: Privacy-preserving authenticated communication in smart home environment[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1095-1107.

作者简介



宋建华　女,1973年出生于湖北省襄阳市.现为湖北大学网络空间安全学院教授、研究生导师.主要研究方向为网络与信息安全.
E-mail: sjhhubu@126.com

张天羿　男,2001年出生于湖北省武汉市.现为湖北大学网络空间安全学院硕士研究生.主要研究方向为协议认证、密钥协商.
E-mail: 984503219@qq.com

张　龑　男,1974年出生于湖北省宜昌市.现为湖北大学计算机学院教授、博士生导师.主要研究方向为代码安全.中国电子学会会员编号:E190197582M.
E-mail: zhangyan@hubu.edu.cn