

## 抵抗物理克隆攻击的车载遥控门锁双因子认证协议

刘长庚<sup>1,2,3</sup>, 刘亚丽<sup>1,2,3\*</sup>, 陆琪鹏<sup>1,2,3</sup>, 李涛<sup>1,2,3</sup>, 林昌露<sup>2</sup>, 祝义<sup>1</sup>

(1. 江苏师范大学 计算机科学与技术学院, 江苏 徐州 221116;

2. 福建省网络安全与密码技术重点实验室(福建师范大学), 福州 350117;

3. 广西密码学与信息安全重点实验室(桂林电子科技大学), 广西 桂林 541004)

(\* 通信作者电子邮箱 liuyali@jsnu.edu.cn)

**摘要:**攻击者通过伪造车辆遥控钥匙发送的无线射频识别(RFID)信号可以非法开启车辆;而且当车辆遥控钥匙丢失或被盗窃,攻击者可以获取钥匙内部秘密信息并克隆出可用的车辆遥控钥匙,会对车主的财产与隐私安全造成威胁。针对上述问题,提出一种抵抗物理克隆攻击的车载遥控门锁(RKE)双因子认证(VRTFA)协议。该协议基于物理不可克隆函数(PUF)和生物指纹特征提取与恢复函数,使合法车辆遥控钥匙的特定硬件物理结构无法被伪造。同时,引入生物指纹因子构建双因子身份认证协议,消除车辆遥控钥匙被盗用的安全隐患,进一步保障车载RKE系统的安全双向认证。利用BAN逻辑对协议进行安全性分析的结果表明,VRTFA协议可以抵抗伪造攻击、去同步攻击、重放攻击、中间人攻击、物理克隆攻击以及密钥全泄漏攻击等恶意攻击,并满足前向安全性、双向认证性、数据完整性和不可追踪性等安全属性。性能分析表明,VRTFA协议与现有的RFID认证协议相比具有更强的安全性与隐私性和更好的实用性。

**关键词:**车载遥控门锁;无线射频识别;双向认证;双因子;物理不可克隆函数

**中图分类号:**TP309 **文献标志码:**A

### Vehicle RKE two-factor authentication protocol resistant to physical cloning attack

LIU Changgeng<sup>1,2,3</sup>, LIU Yali<sup>1,2,3\*</sup>, LU Qipeng<sup>1,2,3</sup>, LI Tao<sup>1,2,3</sup>, LIN Changlu<sup>2</sup>, ZHU Yi<sup>1</sup>

(1. College of Computer Science and Technology, Jiangsu Normal University, Xuzhou Jiangsu 221116, China;

2. Fujian Provincial Key Laboratory of Network Security and Cryptology (Fujian Normal University), Fuzhou Fujian 350117, China;

3. Guangxi Key Laboratory of Cryptography and Information Security (Guilin University of Electronic Technology), Guilin Guangxi 541004, China)

**Abstract:** Attackers can illegally open a vehicle by forging the Radio Frequency Identification (RFID) signal sent by the vehicle remote key. Besides, when the vehicle remote key is lost or stolen, the attacker can obtain the secret data inside the vehicle remote key and clone a usable vehicle remote key, which will threaten the property and privacy security of the vehicle owner. Aiming at the above problems, a Vehicle RKE Two-Factor Authentication (VRTFA) protocol for vehicle Remote Keyless Entry (RKE) that resists physical cloning attack was proposed. The protocol is based on Physical Uncloneable Function (PUF) and biological fingerprint feature extraction and recovery functions, so that the specific hardware physical structure of the legal vehicle remote key cannot be forged. At the same time, the biological fingerprint factor was introduced to build a two-factor authentication protocol, thereby solving the security risk of vehicle remote key theft, and further guaranteeing the secure mutual authentication of vehicle RKE system. Security analysis results of the protocol using BAN logic show that VRTFA protocol can resist malicious attacks such as forgery attack, desynchronization attack, replay attack, man-in-the-middle attack, physical cloning attack, and full key leakage attack, and satisfy the security attributes such as forward security, mutual authentication, data integrity, and untraceability. Performance analysis results show that VRTFA protocol has stronger security and privacy and better practicality than the existing RFID authentication protocols.

**Key words:** vehicle Remote Keyless Entry (RKE); Radio Frequency Identification (RFID); mutual authentication; two-factor; Physical Uncloneable Function (PUF)

收稿日期: 2022-11-04; 修回日期: 2023-01-06; 录用日期: 2023-01-10。

**基金项目:**国家自然科学基金资助项目(61702237); 徐州市科技计划项目(KC22052); 福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(NSCL-KF2021-04); 广西密码学与信息安全重点实验室(桂林电子科技大学)研究课题(GCIS202114); 江苏师范大学研究生科研与实践创新计划项目(2021XKT1382, 2022XKT1488); 教育部产学研合作协同育人项目(202101374001)。

**作者简介:**刘长庚(1997—),男,江苏连云港人,硕士研究生,CCF会员,主要研究方向:无线射频识别认证、物联网安全、隐私保护; 刘亚丽(1981—),女,江苏徐州人,博士,教授,CCF高级会员,主要研究方向:信息安全、认证和隐私保护、区块链、车载自组织网络、密码算法和协议; 陆琪鹏(1999—),男,江苏南京人,硕士研究生,主要研究方向:无线射频识别认证、隐私保护、物联网安全、区块链; 李涛(1998—),男,湖北黄冈人,硕士研究生,主要研究方向:无线射频识别认证、隐私保护、物联网安全、区块链; 林昌露(1978—),男,福建大田人,博士,教授,博士生导师,CCF会员,主要研究方向:密码学、网络安全、秘密共享、安全多方计算、公钥密码学; 祝义(1976—),男,江西九江人,博士,教授,CCF高级会员,主要研究方向:形式化分析、软件可靠性、智能化软件和自适应学习。

## 0 引言

智能车辆作为物联网技术的重要研究对象之一,是实现车联网必不可少的载体<sup>[1]</sup>,车辆认证安全对于保障智能车辆通信安全至关重要。随着互联网通信技术的不断发展,攻击者的攻击能力也逐渐变强,但国内现有的智能车辆认证机制还存在诸多不完善之处<sup>[2-3]</sup>,智能车辆在各种通信场景下均存在亟须解决的安全隐患。智能车辆常见通信场景<sup>[4]</sup>包括:车-人通信、车-车通信<sup>[1]</sup>、车-路通信<sup>[5]</sup>、车内通信以及车-云通信,其中车-人通信安全是保障车联网安全的必不可少的前提条件。因此,设计安全高效的车载遥控门锁(Remote Keyless Entry, RKE)认证协议以保障车联网安全具有重要的研究意义。

随着物联网技术飞速发展,车辆被攻击的案例越来越多<sup>[6]</sup>,智能车辆被非法闯入和盗窃的高比率也表明现有 RKE 技术在保障认证安全性方面十分脆弱<sup>[7-8]</sup>,但 RKE 的认证问题仍未受重视。汽车厂商只注重智能车辆功能的开发,仅通过类似车机编码或固定凭证的方式试图保障车辆的认证安全,但由于缺少信息的动态更新而导致车辆的认证安全问题层出不穷。目前主流汽车厂商制造的智能车辆存在射频信号篡改、射频信号窃取重放和遥控钥匙遭到物理克隆等安全隐患<sup>[9-13]</sup>。现有的 RKE 认证方式已经无法满足现阶段车辆认证安全的性能需求,迫切需要设计安全高效的 RKE 认证协议以保障车联网安全。

无线射频识别(Radio Frequency Identification, RFID)双向认证协议<sup>[14]</sup>作为常见的物联网安全认证方式,可以抵抗现有 RKE 认证中由于缺少认证命令码的更新机制而导致的遥控钥匙伪造攻击与重放攻击。针对遥控钥匙存在被物理克隆攻击的风险,物理不可克隆函数(Physical Unclonable Function, PUF)<sup>[15]</sup>的引入可以避免遥控钥匙遭到物理克隆攻击。本文提出的 RKE 双因子认证协议将 RFID 标签嵌入车辆遥控钥匙中,RFID 阅读器放置在车载阅读器中,阅读器和标签通过无线射频信号交互,利用 RFID 双向认证协议保障 RKE 的认证和通信安全。由于 RKE 系统中遥控钥匙体积较小,运算成本和存储成本均受到限制,因此,轻量级 RFID 双向认证协议符合 RKE 低成本的设计要求。综上所述,设计一个适用于 RKE 的安全高效的 RFID 双因子双向认证协议具有重要的研究意义和实用价值。

本文的研究旨在针对当前 RKE 认证存在的安全问题,设计具有密钥更新的 RFID 双因子双向认证协议,并应用于 RKE 场景。本文创新性地提出了一种抵抗标签物理克隆的车载 RKE 双因子认证(Vehicle RKE Two-Factor Authentication, VRTFA)协议以保障 RKE 的认证安全。本文的主要工作如下:

1) RKE 认证:在 RKE 场景下引入 RFID 双因子双向认证替代识别循环认证命令码的认证方式,利用哈希函数、密钥更新机制和随机数机制等技术弥补 RKE 现有加密认证方式的不足,增加了攻击者窃听并破解无线射频信号的难度,为安全性薄弱的 RKE 系统提供高效安全的认证。

2) 抵抗物理克隆攻击:将 PUF 置于 RKE 的遥控钥匙中,使合法车辆遥控钥匙的特定硬件物理结构无法被伪造,防止遥控钥匙电子控制原件中的加密算法和密钥被克隆而导致的物理克隆攻击。

3) 抵抗密钥全泄露攻击:采用数据库间接存放参与认证的密钥以抵抗由于数据库泄漏而导致的密钥全泄露攻击。

在保障 RKE 系统安全双向认证的同时没有增加认证双方的计算代价,为抵抗密钥全泄露攻击的 RFID 认证协议的设计提供了新思路。

4) 双因子认证:本文 VRTFA 协议采用生物指纹因子和传统密钥因子相结合的方式构建双因子认证,提高了 RKE 认证的安全性和隐私性,消除了现有单因子认证协议无法防止遥控钥匙被盗用非法开启车辆的安全隐患。

5) 强安全性:本文 VRTFA 协议具有良好的安全性和隐私性,满足数据完整性、前向安全性、不可追踪性和双向认证性等多种安全属性,且可以抵抗去同步攻击、伪造攻击、重放攻击、中间人攻击、物理克隆攻击以及密钥全泄漏攻击等恶意攻击。

## 1 相关工作

由于 RFID 标签体积小,设计 RFID 认证协议的加密算法时易受运算成本和存储成本的限制。黄琪等<sup>[16]</sup>提出一种超轻量级 RFID 的双向认证协议,使用比伪随机函数需要的门电路数更少的循环校验函数作为加密算法,用更小的运算代价进行标签以及读写器与后端服务器之间的身份认证;但阅读器明文发送每轮生成的随机数给数据库,存在随机数泄漏的安全隐患。李璐璐等<sup>[17]</sup>设计了基于云的轻量级 RFID 群组标签认证协议,使用哈希函数和对称加密提高云和标签组的认证安全性,但并不满足低成本需求。王悦等<sup>[18]</sup>提出物联网中轻量级 RFID 电子票据安全认证协议,设计了基于字符串混淆移位置换函数  $Per(X, Y)$ ,利用轻量级双向认证协议实现票据防伪;但  $Per(X, Y)$  存在被逆推导出秘密值的安全隐患。王国伟等<sup>[19]</sup>提出了一种基于动态共享密钥的移动 RFID 双向认证协议,在使用轻量级加密运算的同时利用分表存储密钥的方式成功抵抗去同步攻击;但分表存储增加了协议的存储代价。RFID 认证协议<sup>[16, 18-19]</sup>均聚焦于加密运算成本的轻量化,但忽略了轻量级运算更容易被攻击者复制和克隆。攻击者在劫持标签并获取内部密钥与加密算法后可以克隆合法 RFID 标签并通过上述认证协议<sup>[16-19]</sup>的验证。因此,设计可以抵抗物理克隆攻击的 RFID 认证协议具有研究意义。

为防止物理克隆攻击,Gope 等<sup>[20]</sup>提出一种应用 PUF 的 RFID 匿名认证协议,利用 PUF 运算出  $n$  对激励响应对作为标签和数据库认证的共享密钥,保障双向认证的同时唯一标识了合法标签,能成功抵抗物理克隆攻击;但激励响应对明文存放在数据库中仍存在安全隐患。在此之后,Gope 等<sup>[21]</sup>引入 PUF 作为无人机硬件认证和生成安全密钥,提出了一种高效的边缘辅助无人机互联网隐私保护认证协议,同样利用  $n$  对激励响应对作为共享密钥,并利用模糊提取器进一步减小 PUF 输出的误差。文献[21]的方法无须给无人机终端设置认证密钥,在提高可用性的同时保障了无人机与服务提供商之间的认证安全;但数据库存在泄漏激励响应对的安全隐患。经分析,文献[20-21]的方法虽然抵抗了物理克隆攻击,但是数据库明文存储激励响应对存在安全隐患。由于将激励响应对用作标签与数据库的共享密钥,只要数据库遭到攻击就会导致密钥全泄漏。此外,将共享密钥明文存放在数据库的方法如文献[16-21],均有密钥全泄漏的安全隐患。因此,密钥全泄漏攻击是 RFID 认证协议所面临的典型恶意攻击方式。

单因子认证协议是基于单因子(口令或密钥)的认证协议,局限性在于它的安全性仅基于协议当前使用口令的安全



性,现有单因子协议<sup>[16-21]</sup>大多无法抵抗密钥全泄漏攻击。Das等<sup>[22]</sup>引入智能卡因子设计认证协议,开启了无线传感器网络环境下双因子认证的新篇章。Wang等<sup>[23]</sup>提出了匿名双因子认证协议的基本评估指标,为后来的学者更好地设计匿名双因子协议提供了参考和帮助。2019年,李文婷等<sup>[24]</sup>在文献[23]的基本评估指标下总结了抵抗各种恶意攻击的双因子认证协议的设计策略。2020年,Qiu等<sup>[25]</sup>提出了一种基于移动轻型设备扩展混沌映射的可证明安全的多因子认证协议,采用“模糊验证”和“Honeywords”技术保障协议认证的安全性。现有的无线传感器网络场景下通过上述双因子认证协议<sup>[22-25]</sup>可以抵抗数据库泄漏导致的密钥全泄漏攻击,提高了认证的安全性,但智能卡因子不适用于成本受限的RKE应用场景。目前车载RKE认证仍以单因子认证为主,一旦唯一的认证码因子被窃听破解,RKE将受到安全威胁。由于体积较小的遥控钥匙无法引入智能卡作为第二个认证因子,设计基于生物指纹为第二因子的双因子认证协议更适用于成本受限的RKE认证。

综上所述,现有的RFID单因子认证协议不仅存在物理克隆攻击的安全隐患,还无法抵抗密钥全泄漏攻击;同时仅依赖密钥作为唯一认证因子的单因子协议无法满足RKE的需求,无法抵抗由于遥控钥匙盗用导致非法开启车辆的威胁。因此,本文提出一种车载RKE双因子认证(VRTFA)协议,可以抵抗物理克隆攻击和密钥全泄漏攻击,同时引入生物指纹因子作为第二因子使得遥控钥匙被盗用不会对RKE安全造成威胁,可为RKE系统提供高效安全的认证。

## 2 相关知识

### 2.1 双因子认证

双因子认证的安全性不仅依赖于存储在数据库上的口令密码的验证表,而且利用两个因子共同保障认证协议的安全性<sup>[23-24]</sup>。这是双因子认证协议相对于单因子认证的关键优势。因为后者的安全性仅依赖服务器上维护的敏感口令因子,一旦加密传输的口令因子被窃听破解,整个认证协议的安全性会受到威胁,任何获取到泄漏的口令因子的恶意攻击者都可以进行伪造攻击破坏认证协议的安全性。引入智能卡或者生物指纹等作为口令以外的第二个因子,第一因子的口令遭到泄漏时如果没有第二个智能卡因子一起参与认证,攻击者也无法通过认证协议的认证。双因子共同参与认证,两者相对独立又缺一不可,弥补了单因子认证依赖单一因子的局限性,提高了认证安全性。

### 2.2 车载遥控门锁系统结构

RKE系统由遥控钥匙、车载阅读器(即无线信号接收器)、主机数据库端(车身控制模块)构成<sup>[6]</sup>。通常来说,RKE的认证流程如下:

- 1) 合法遥控钥匙内部存有多个认证命令码可以支持RKE系统认证通信时循环使用;
- 2) 车主按下遥控钥匙上的按钮,遥控钥匙发出包含认证命令码的无线射频信号;
- 3) 车载阅读器收到无线射频信号反馈给智能车辆车身控制模块其中的消息认证模块,消息认证模块验证该信号为正确命令后,智能车辆执行打开或关闭门锁的操作。

目前RKE的安全性仅依赖于循环使用的认证命令码的保密性,而认证命令码缺少更新会导致安全隐患。攻击者可利用RKE的安全缺陷非法开启智能车辆,盗窃智能车辆内的物品或智能车辆本身。例如:攻击者通过截获无线信道公

开传输的信息,可伪造遥控钥匙的无线射频信号发送给车载阅读器试图非法开启车辆。

## 3 VRTFA 协议

### 3.1 符号说明

本文提出的VRTFA协议所涉及的相关符号名称及描述如表1所示。

表 1 符号说明

Tab. 1 Description of symbols

符号	含义	符号	含义
$IDS$	遥控钥匙假名	$PUF()$	物理不可克隆函数
$ID$	遥控钥匙身份标识	$h()$	哈希函数
$Bio$	用户生物指纹	$K_T$	遥控钥匙认证密钥
$Gen()$	生物特征提取函数	$K_R$	车载阅读器认证密钥
$Rep()$	生物特征恢复函数		

### 3.2 VRTFA 协议流程

VRTFA协议分为以下四个阶段:1)注册阶段;2)遥控钥匙识别用户阶段;3)双向认证阶段;4)密钥更新阶段。

#### 3.2.1 VRTFA 协议注册阶段

注册阶段不仅支持同一用户可以录入多个生物指纹,还支持录入多个用户的生物指纹。不同指纹注册与认证过程互相独立,遥控钥匙可存储多个生物指纹对应不同的 $IDS$ 、 $K_T$ 和 $K_R$ 。但遥控钥匙内部只存储唯一的 $ID$ 标识。以用户录入单个生物指纹因子为例的注册过程如图2所示。

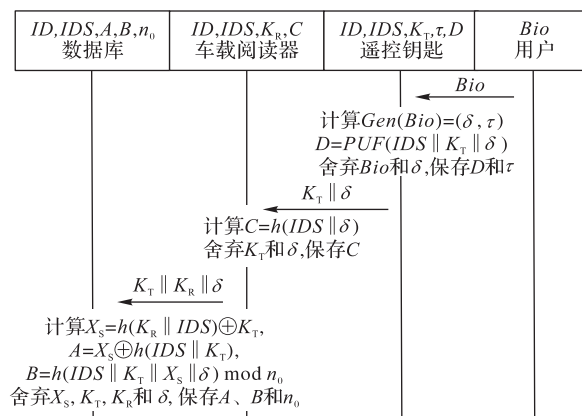


图 1 VRTFA 协议注册阶段

Fig. 1 Registration stage of VRTFA protocol

步骤 1 遥控钥匙录入用户生物指纹信息 $Bio$ ,生成相应的 $IDS$ 与 $K_T$ ,利用生物特征提取函数和物理不可克隆函数计算 $Gen(Bio)=(\delta, \tau)$ , $D=PUF(IDS \parallel K_T \parallel \delta)$ 。遥控钥匙将生物指纹信息 $Bio$ 和参数 $\delta$ 舍弃,保存 $D$ 、 $K_T$ 和 $\tau$ 。

步骤 2 遥控钥匙将 $K_T$ 和 $\delta$ 发送给车载阅读器,车载阅读器生成相应的密钥 $K_R$ ,计算 $C=h(IDS \parallel \delta)$ ,并舍弃 $K_T$ 和 $\delta$ ,保存 $C$ 。

步骤 3 车载阅读器将 $K_T \parallel K_R \parallel \delta$ 发送给数据库,数据库计算相应的 $X_s=h(K_R \parallel IDS) \oplus K_T$ , $A=X_s \oplus h(IDS \parallel K_T)$ , $B=h(IDS \parallel K_T \parallel X_s \parallel \delta) \bmod n_0$ 。最后数据库舍弃 $X_s$ 、 $K_T$ 、 $K_R$ 和 $\delta$ ,保存 $A$ 、 $B$ 和 $n_0$ 以备后续认证。

#### 3.2.2 VRTFA 协议遥控钥匙识别用户阶段

遥控钥匙采集用户生物指纹 $Bio$ 后利用指纹恢复函数恢复协议注册阶段舍弃的参数 $\delta'=Rep(Bio, \tau)$ ,计算 $D'=PUF(IDS \parallel K_T \parallel \delta')$ ,验证 $D'$ 是否和 $D$ 相等。验证成功则表

示用户生物指纹合法,遥控钥匙识别用户后进入双向认证阶段,否则遥控钥匙不继续向车载阅读器发送认证请求,如图2所示。

### 3.2.3 VRTFA 协议双向认证阶段

遥控钥匙验证用户成功后进入双向认证阶段,如图2所示。双向认证阶段实现遥控钥匙、车载阅读器和数据库之间两两认证,具体步骤如下:

步骤1 遥控钥匙发送IDS给车载阅读器请求认证,车载阅读器验证IDS合法后产生随机数 $n_1$ ,计算 $M_1=h(ID \parallel IDS) \oplus n_1$ 和 $M_2=h(ID \parallel n_1)$ ,若验证IDS不成功则车载阅读器不作响应。

步骤2 车载阅读器发送 $M_1$ 和 $M_2$ 给遥控钥匙,遥控钥匙计算随机数 $n_1'=h(ID \parallel IDS) \oplus M_1$ 和 $M_2'=h(ID \parallel n_1')$ ,并验证 $M_2'$ 和 $M_2$ 是否相等。若验证成功则说明车载阅读器身份合法,遥控钥匙计算 $M_3=\delta \oplus h(ID \oplus n_1)$ , $M_4=K_T \oplus h(IDS \oplus n_1)$ , $M_5=h(ID \parallel K_T \parallel \delta \parallel n_1)$ 。若验证不成功,遥控钥匙不作响应。

步骤3 遥控钥匙标签发送 $M_3 \parallel M_4 \parallel M_5$ 给车载阅读器,

车载阅读器运算得到 $\delta'$ 、 $K_T'$ 、 $C'$ 和 $M_5'$ ,验证是否满足 $C'=C$ , $M_5'=M_5$ 。验证成功则说明遥控钥匙合法并且发送的消息完整未篡改,车载阅读器将产生随机数 $n_2$ ,计算 $M_6=n_2 \oplus h(ID \oplus IDS)$ , $M_7=\delta \oplus h(IDS \parallel n_2)$ , $M_8=K_T \oplus h(IDS \parallel \delta \parallel n_2)$ ;若验证失败则车载阅读器不作任何回应。

步骤4 车载阅读器发送 $IDS \parallel M_6 \parallel M_7 \parallel M_8$ 给数据库。数据库运算得到 $n_2'$ 、 $\delta'$ 和 $K_T'$ ,数据库计算 $X_s'=A \oplus h(IDS \parallel K_T')$ , $B'=h(IDS \parallel K_T' \parallel X_s' \parallel \delta') \bmod n_0$ ,验证 $B'$ 和 $B$ 是否相等。若验证成功则数据库对车载阅读器和遥控钥匙验证成功,计算 $M_9=h(X_s \oplus n_2)$ ,并进入密钥更新阶段;若验证失败数据库不作任何回应。

步骤5 数据库发送 $M_9$ 给车载阅读器,只有合法车载阅读器拥有 $K_R$ 计算出 $X_s'=h(K_R \parallel IDS) \oplus K_T$ 和 $M_9'=h(X_s' \oplus n_2)$ ,验证 $M_9'$ 和 $M_9$ 是否相等。验证成功则说明车载阅读器验证数据库合法,计算 $M_{10}=h(ID \parallel K_T \parallel \delta) \oplus n_2$ , $M_{11}=h(ID \parallel K_T \parallel \delta \parallel n_2)$ ,车载阅读器进入密钥更新阶段;若验证失败,车载阅读器不作任何回应。

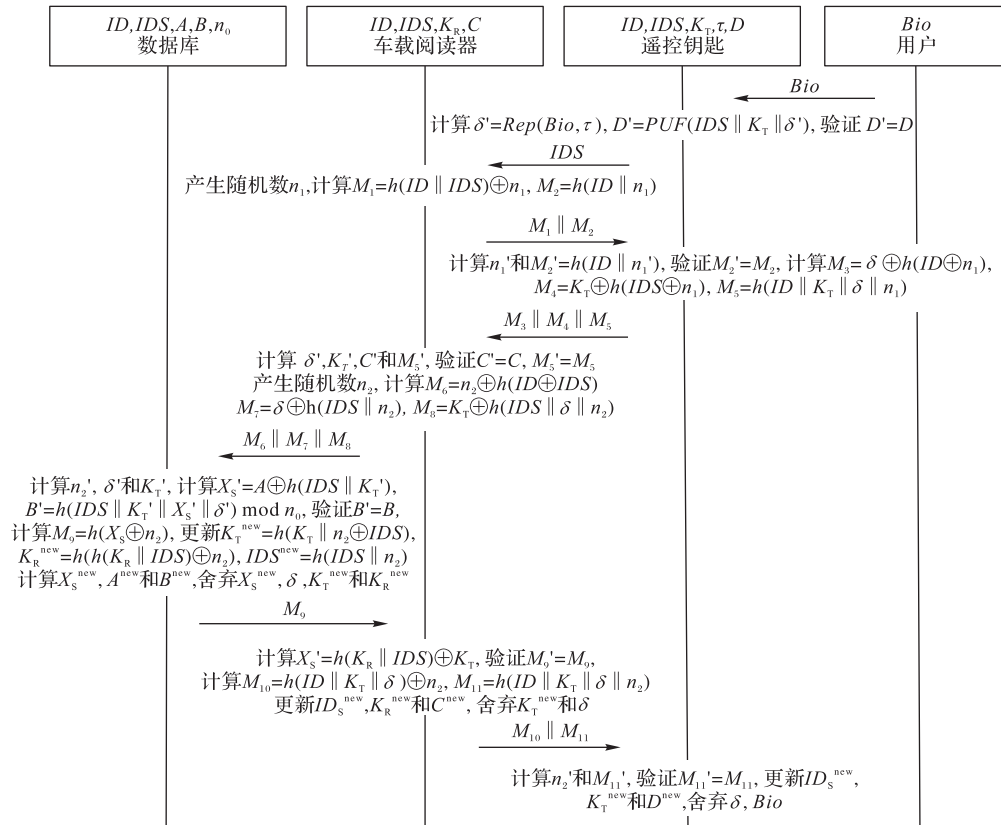


图2 VRTFA 协议认证阶段

Fig. 2 Authentication stage of VRTFA protocol

步骤6 遥控钥匙收到车载阅读器发送的 $M_{10} \parallel M_{11}$ ,计算 $n_2'$ 和 $M_{11}'=h(ID \parallel K_T \parallel \delta \parallel n_2')$ ,验证 $M_{11}'$ 和 $M_{11}$ 是否相等。如果相等则说明遥控钥匙和车载阅读器以及数据库的双向认证成功,遥控钥匙标签进入密钥更新阶段;若验证失败遥控钥匙不作任何回应。

### 3.2.4 VRTFA 协议密钥更新阶段

VRTFA 协议双向认证阶段成功后进入密钥更新阶段,实现遥控钥匙、车载阅读器和数据库之间密钥的同步更新,具体步骤如下:

步骤1 数据库收到车载阅读器发送的消息 $IDS \parallel M_6 \parallel$

$M_7 \parallel M_8$ ,计算 $B'=h(IDS \parallel K_T' \parallel X_s' \parallel \delta') \bmod n_0$ ,验证 $B'$ 和 $B$ 是否相等。若验证成功则数据库对车载阅读器和遥控钥匙验证成功,更新密钥和假名 $K_T^{new}=h(K_T \parallel n_2 \oplus IDS)$ , $K_R^{new}=h(h(K_R \parallel IDS) \oplus n_2)$ , $IDS^{new}=h(IDS \parallel n_2)$ ,计算 $X_s^{new}$ 、 $A^{new}$ 和 $B^{new}$ ,舍弃 $X_s^{new}$ 、 $\delta$ 、 $K_T^{new}$ 和 $K_R^{new}$ ,若验证失败数据库不作任何回应。

步骤2 车载阅读器收到数据库发送的 $M_9$ ,验证 $M_9$ 是否合法,验证成功则说明验证数据库合法,车载阅读器进入密钥更新阶段,车载阅读器更新 $IDS^{new}$ 、 $K_R^{new}$ 和 $C^{new}$ ,舍弃 $K_T^{new}$ 和 $\delta$ ;若验证失败,车载阅读器不作任何回应。

步骤 3 遥控钥匙收到车载阅读器发送的  $M_{10} \parallel M_{11}$ , 计算  $n_2'$  和  $M_{11}' = h(ID \parallel K_r \parallel \delta \parallel n_2')$ , 验证  $M_{11}'$  和  $M_{11}$  是否相等。如果相等则说明遥控钥匙和车载阅读器以及数据库的双向认证成功, 遥控钥匙进入密钥更新阶段, 遥控钥匙更新  $IDS^{new}$ 、 $K_r^{new}$  和  $D^{new}$ , 舍弃  $\delta$  和  $Bio$ ; 若验证失败遥控钥匙不作任何回应。

#### 4 BAN 逻辑分析与证明

本章采用 BAN<sup>[26]</sup> 逻辑分析方法对本文的 VRTFA 协议进行形式化安全性证明。

##### 4.1 BAN 逻辑构件的语法

在 BAN 逻辑模型中,  $P$  和  $Q$  通常用于分别表示两个通信实体<sup>[27]</sup>, 一些符号用于表示实体之间的交互过程。主要使用的表达式如下:

$P \models X$ : 主体  $P$  信任公式  $X$  的真实性;

$P \triangleleft X$ : 主体  $P$  接收到包含公式  $X$  的消息;

$P \vdash X$ : 主体  $P$  曾经发送过包含公式  $X$  的消息;

$\#(X)$ : 消息  $X$  是新鲜的, 即  $X$  没有在当前回合作为某消息的一部分被发送过;

$P \Rightarrow X$ : 主体  $P$  对公式  $X$  有管辖权;

$\{X\}_K$ : 用密钥  $K$  加密  $X$  后得到的密文;

$P \xleftrightarrow{K} Q$ :  $K$  是主体  $P$  和  $Q$  的共享的秘密。

##### 4.2 BAN 逻辑推理规则

BAN 逻辑主要有如下推理法则<sup>[26]</sup> (仅列出本文涉及的主要推理规则):

$R_1$  (message-meaning rule 消息含义法则):

$$\frac{P \models Q \xleftrightarrow{K} P, P \triangleleft \{X\}_K}{P \models Q \models X}$$

上式说明,  $P$  相信  $Q$  与  $P$  之间共享密钥信息  $K$ , 且  $P$  接收到用  $K$  做密钥的加密信息  $X$ , 则可以推出  $P$  相信  $Q$  曾经发送过消息  $X$ 。

$R_2$  (nonce-verification rule 临时验证法则):

$$\frac{P \models \#(X), P \models Q \models X}{P \models Q \models X}$$

上式说明,  $P$  相信  $X$  消息是新鲜的, 且  $P$  相信  $Q$  曾经发送过消息  $X$ , 则可以推出  $P$  相信  $Q$  与  $X$  的真实性。

$R_3$  (freshness rule 消息新鲜性法则):

$$\frac{P \models \#(X)}{P \models \#(X, Y)}$$

上式说明,  $P$  相信  $X$  消息是新鲜的, 则可以推出  $P$  相信  $X$  和  $Y$  级联的整体信息也是新鲜的。

$R_4$  (jurisdiction rule 管辖权法则):

$$\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$$

上式说明,  $P$  相信  $Q$  对  $X$  有管辖权, 且  $P$  相信  $Q$  相信  $X$  的真实性, 则可以推出  $P$  相信  $X$  的真实性。

##### 4.3 VRTFA 协议的形式化描述

为了便于描述, 定义三个角色, 分别为:  $D$ 、 $R$  与  $T$  分别表示参与协议通信方数据库、车载阅读器和遥控钥匙。VRTFA 协议的理想化模型描述如下:

message1:  $T \rightarrow R: \{IDS\}$

message2:  $R \rightarrow T: \{M_1 \parallel M_2\}$

message3:  $T \rightarrow R: \{M_3 \parallel M_4 \parallel M_5\}$

message4:  $R \rightarrow D: \{IDS \parallel M_6 \parallel M_7 \parallel M_8\}$

message5:  $D \rightarrow R: \{M_9\}$

message6:  $R \rightarrow T: \{M_{10} \parallel M_{11}\}$

在 VRTFA 协议中, message1 仅表示发起认证通信协商的简单请求, 以明文传输所以不做安全分析证明。message2~message6 是车载阅读器和数据库间在无线信道上进行的消息通信, 需要进行安全分析证明。因此, 主要利用 BAN 逻辑模型形式化分析 message2~message6 的安全性, 其形式化描述可以转换为如下形式, 其中为了便于描述, 符号  $K$  表示钥匙的  $IDS$ 、 $ID$ 、伪随机数和密钥等秘密信息。

message2:  $T \triangleleft \{M_1 \parallel M_2\}_K$

message3:  $R \triangleleft \{M_3 \parallel M_4 \parallel M_5\}_K$

message4:  $D \triangleleft \{IDS \parallel M_6 \parallel M_7 \parallel M_8\}_K$

message5:  $R \triangleleft \{M_9\}_K$

message6:  $T \triangleleft \{M_{10} \parallel M_{11}\}_K$

##### 4.4 初始化假设

VRTFA 协议满足以下基本假设:

$A_1: R \models R \xleftrightarrow{K} T$ , 车载阅读器信任与遥控钥匙共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_2: R \models R \xleftrightarrow{K} D$ , 车载阅读器信任与数据库共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_3: T \models T \xleftrightarrow{K} R$ , 遥控钥匙信任与车载阅读器共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_4: T \models T \xleftrightarrow{K} D$ , 遥控钥匙信任与数据库共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_5: D \models D \xleftrightarrow{K} R$ , 数据库信任与车载阅读器共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_6: D \models D \xleftrightarrow{K} T$ , 数据库信任与遥控钥匙共享的加密信息  $K$ ,  $K$  包含遥控钥匙的  $ID$  和密钥;

$A_7: R \models \#IDS$ , 车载阅读器信任遥控钥匙假名  $IDS$  的新鲜性;

$A_8: D \models \#IDS$ , 数据库信任遥控钥匙假名  $IDS$  的新鲜性;

$A_9: T \models \#n_1$ , 遥控钥匙信任伪随机数  $n_1$  的新鲜性;

$A_{10}: T \models \#n_2$ , 遥控钥匙信任伪随机数  $n_2$  的新鲜性;

$A_{11}: D \models \#n_2$ , 数据库信任伪随机数  $n_2$  的新鲜性;

$A_{12}: R \models \#K$ , 车载阅读器信任共享的加密信息  $K$  的新鲜性;

$A_{13}: T \models \#K$ , 遥控钥匙信任共享的加密信息  $K$  的新鲜性;

$A_{14}: D \models \#K$ , 数据库信任共享的加密信息  $K$  的新鲜性;

$A_{15}: T \models R \Rightarrow \{M_1 \parallel M_2\}$ , 遥控钥匙信任车载阅读器拥有对消息  $M_1$  和  $M_2$  的管辖权;

$A_{16}: R \models T \Rightarrow \{M_3 \parallel M_4 \parallel M_5\}$ , 车载阅读器信任遥控钥匙拥有对消息  $M_3$ 、 $M_4$  和  $M_5$  的管辖权;

$A_{17}: D \models R \Rightarrow \{IDS \parallel M_6 \parallel M_7 \parallel M_8\}$ , 数据库信任车载阅读器拥有对消息  $IDS$ 、 $M_6$ 、 $M_7$  和  $M_8$  的管辖权;

$A_{18}: R \models D \Rightarrow \{M_9\}$ , 车载阅读器信任数据库拥有对消息  $M_9$  的管辖权;

$A_{19}: T \models R \Rightarrow \{M_{10} \parallel M_{11}\}$ , 遥控钥匙信任车载阅读器拥有对消息  $M_{10}$  和  $M_{11}$  的管辖权;

$A_{20}: T \triangleleft \{M_1 \parallel M_2\}_K$ , 遥控钥匙接收到由密钥信息  $K$  加密的消息  $M_1$  和  $M_2$ ;

$A_{21}: R \triangleleft \{M_3 \parallel M_4 \parallel M_5\}_K$ , 车载阅读器接收到由密钥信息  $K$  加密的消息  $M_3$ 、 $M_4$  和  $M_5$ ;

$A_{22}: D \triangleleft \{IDS \parallel M_6 \parallel M_7 \parallel M_8\}_K$ , 数据库接收到由密钥信息



$K$ 加密的IDS和消息 $M_6$ 、 $M_7$ 和 $M_8$ ;

$A_{23}: R \triangleleft \{M_9\}_K$ , 车载阅读器接收到由密钥信息 $K$ 加密的消息 $M_9$ ;

$A_{24}: T \triangleleft \{M_{10} \| M_{11}\}_K$ , 遥控钥匙接收到由密钥信息 $K$ 加密的消息 $M_{10}$ 和 $M_{11}$ 。

#### 4.5 安全目标

通过4.3节分析可知,VRTFA协议安全性证明的5个目标如下:

- $G_1: T \models \{M_1 \| M_2\}$
- $G_2: R \models \{M_3 \| M_4 \| M_5\}$
- $G_3: D \models \{IDS \| M_6 \| M_7 \| M_8\}$
- $G_4: R \models \{M_9\}$
- $G_5: T \models \{M_{10} \| M_{11}\}$

其中:安全目标 $G_1$ 是指遥控钥匙 $T$ 信任消息 $M_1$ 和 $M_2$ 的真实性;安全目标 $G_2$ 是指车载阅读器 $R$ 信任消息 $M_3$ 、 $M_4$ 和 $M_5$ 的真实性;安全目标 $G_3$ 是指数据库 $D$ 信任消息 $IDS$ 、 $M_6$ 、 $M_7$ 和 $M_8$ 的真实性;安全目标 $G_4$ 是指车载阅读器 $R$ 信任消息 $M_9$ 的真实性;安全目标 $G_5$ 是指遥控钥匙 $T$ 信任消息 $M_{10}$ 、 $M_{11}$ 的真实性。

#### 4.6 安全目标证明

VRTFA协议安全性证明的5个目标分析推理证明过程如下:

1)由message2,根据假设 $A_3$ 、 $A_{20}$ 和规则 $R_1$ ,可以推导出:

$$F_1: T \models R \models \{M_1 \| M_2\}$$

根据假设 $A_9$ 和 $A_{13}$ 和规则 $R_3$ 可以推导出:

$$F_2: T \models \# \{M_1 \| M_2\}$$

根据推导出的 $F_1$ 、 $F_2$ 和规则 $R_2$ 可以推导出:

$$F_3: T \models R \models \{M_1 \| M_2\}$$

根据假设 $A_{15}$ 、推导出的 $F_3$ 和规则 $R_4$ 最终可以推导出:

$$F_4: T \models \{M_1 \| M_2\}$$

综上所述,安全目标 $G_1$ 得证。

2)由message3,根据假设 $A_1$ 、 $A_{21}$ 和规则 $R_1$ ,可以推导出:

$$F_5: R \models T \models \{M_3 \| M_4 \| M_5\}$$

根据假设 $A_7$ 和 $A_{12}$ 和规则 $R_3$ 可以推导出:

$$F_6: R \models \# \{M_3 \| M_4 \| M_5\}$$

根据推导出的 $F_5$ 、 $F_6$ 和规则 $R_2$ 可以推导出:

$$F_7: R \models T \models \{M_3 \| M_4 \| M_5\}$$

根据假设 $A_{16}$ 、推导出的 $F_7$ 和规则 $R_4$ 最终可以推导出:

$$F_8: R \models \{M_3 \| M_4 \| M_5\}$$

综上所述,安全目标 $G_2$ 得证。

3)由message4,根据假设 $A_5$ 、 $A_{22}$ 和规则 $R_1$ ,可以推导出:

$$F_9: D \models R \models \{IDS \| M_6 \| M_7 \| M_8\}$$

根据假设 $A_8$ 、 $A_{11}$ 和 $A_{14}$ 和规则 $R_3$ 可以推导出:

$$F_{10}: D \models \# \{IDS \| M_6 \| M_7 \| M_8\}$$

根据推导出的 $F_9$ 、 $F_{10}$ 和规则 $R_2$ 可以推导出:

$$F_{11}: D \models R \models \{IDS \| M_6 \| M_7 \| M_8\}$$

根据假设 $A_{17}$ 、推导出的 $F_{11}$ 和规则 $R_4$ 最终可以推导出:

$$F_{12}: D \models \{IDS \| M_6 \| M_7 \| M_8\}$$

综上所述,安全目标 $G_3$ 得证。

4)由message5,根据假设 $A_2$ 、 $A_{23}$ 和规则 $R_1$ ,可以推导出:

$$F_{13}: R \models D \models \{M_9\}$$

根据假设 $A_7$ 和 $A_{12}$ 和规则 $R_3$ 可以推导出:

$$F_{14}: R \models \# \{M_9\}$$

根据推导出的 $F_{13}$ 、 $F_{14}$ 和规则 $R_2$ 可以推导出:

$$F_{15}: R \models D \models \{M_9\}$$

根据假设 $A_{18}$ 、推导出的 $F_{15}$ 和规则 $R_4$ 最终可以推导出:

$$F_{16}: R \models \{M_9\}$$

综上所述,安全目标 $G_4$ 得证。

5)由message6,根据假设 $A_3$ 、 $A_{24}$ 和规则 $R_1$ ,可以推导出:

$$F_{17}: T \models R \models \{M_{10} \| M_{11}\}$$

根据假设 $A_{10}$ 和 $A_{13}$ 和规则 $R_3$ 可以推导出:

$$F_{18}: T \models \# \{M_{10} \| M_{11}\}$$

根据推导出的 $F_{17}$ 、 $F_{18}$ 和规则 $R_2$ 可以推导出:

$$F_{19}: T \models R \models \{M_{10} \| M_{11}\}$$

根据假设 $A_{19}$ 、推导出的 $F_{19}$ 和规则 $R_4$ 最终可以推导出:

$$F_{20}: T \models \{M_{10} \| M_{11}\}$$

综上所述,安全目标 $G_5$ 得证。

综上证明结果可知VRTFA协议能够达到期望的安全目标,因此,VRTFA协议是安全的。

### 5 VRTFA协议安全性分析

本章对VRTFA协议的数据完整性、前向安全性、不可追踪性、双向认证性等安全属性以及对去同步攻击、伪造攻击、重放攻击、中间人攻击、物理克隆攻击、密钥全泄漏攻击等多种恶意攻击的抵抗能力进行分析。

#### 5.1 安全属性分析

##### 5.1.1 数据完整性

数据完整性<sup>[28]</sup>指认证双方发送的消息中途未经篡改并完整传输到接收端的能力,VRTFA协议中认证双方利用单向哈希函数对接收到的消息进行完整性校验。例如车载阅读器给遥控钥匙发送消息 $M_1$ 和 $M_2$ ,其中 $M_1=h(ID \| IDS) \oplus n_1$ 和 $M_2=h(ID \| n_1)$ 。为了防止攻击者对消息 $M_1$ 篡改导致遥控钥匙无法验证随机数 $n_1$ 的完整性,车载阅读器对包含随机数 $n_1$ 在内的数据进行哈希运算得到 $M_2$ 一并发送给遥控钥匙,最终遥控钥匙通过验证 $M_2$ 的合法性的同时校验了 $M_1$ 中的 $n_1$ 数据完整性。同理遥控钥匙发送消息 $M_3$ 、 $M_4$ 和 $M_5$ 给车载阅读器,其中 $M_3=\delta \oplus h(ID \oplus n_1)$ , $M_4=K_r \oplus h(IDS \oplus n_1)$ , $M_5=h(ID \| K_r \| \delta \| n_1)$ 。可见 $M_5$ 由 $M_3$ 、 $M_4$ 内包含的 $\delta$ 与 $K_r$ 在内的秘密信息进行哈希运算得到,所以车载阅读器接收消息后可通过从 $M_3$ 、 $M_4$ 提取出 $\delta$ 与 $K_r$ 并对消息 $M_5$ 验证,若验证成功则说明接收的消息 $M_3$ 、 $M_4$ 内 $\delta$ 与 $K_r$ 未被篡改。因此,VRTFA协议可以保障认证过程中交互消息的数据完整性。

##### 5.1.2 前向安全性

前向安全性<sup>[29]</sup>是指攻击者无法通过本轮次认证的加密密钥和加密消息破解历史认证轮次的密钥和加密消息。VRTFA协议在一轮认证结束时使用随机数和单向哈希函数对设备的假名、加密密钥与认证参数进行更新,例如 $K_r^{new}=h(K_r \| n_2 \oplus IDS)$ , $K_r^{new}=h(h(K_r \| IDS) \oplus n_2)$ , $IDS^{new}=h(IDS \| n_2)$ ,在更新阶段引入随机数保证了每轮认证假名、加密密钥和认证参数的新鲜性,攻击者无法通过单向哈希函数的运算结果推导出之前历史轮次的假名、加密密钥与认证参数。因此,VRTFA协议可以保障认证过程的前向安全性。

##### 5.1.3 不可追踪性

不可追踪性<sup>[30]</sup>是指攻击者无法通过持续监听并分析截获的消息,从而确定RFID标签的具体位置。RKE利用遥控钥匙发送的循环认证命令码验证并开启车辆,而认证命令码不更新且数量有限。攻击者可以通过窃听并识别专属于某个车辆的认证命令码并判断车主当前位置在窃听范围内,甚至通过截获认证命令码的发送时间判断车主停车与离开的

时间,所以现有的 RKE 并不满足不可追踪性。而 VRTFA 协议中假名、加密密钥与认证参数每轮认证结束时都进行更新,每轮认证遥控钥匙和车载阅读器发送的随机化消息都具有新鲜性,所以攻击者无法利用窃听的消息追踪到具体车辆。因此,VRTFA 协议可以保障认证过程中交互消息的不可追踪性。

#### 5.1.4 双向认证性

双向认证性<sup>[31]</sup>是在通信双方成功认证彼此身份是否合法,也是通信双方认证成功必不可少的前提。VRTFA 协议中以车载阅读器发送  $IDS \parallel M_6 \parallel M_7 \parallel M_8$  给数据库为例,只有合法数据库才可以从消息中运算得到  $n_2'$ 、 $\delta'$  和  $K_r'$ ,接着计算  $X_s' = A \oplus h(IDS \parallel K_r')$ ,  $B' = h(IDS \parallel K_r' \parallel X_s' \parallel \delta') \bmod n_0$ ,验证  $B'$  和  $B$  成功则数据库对车载阅读器验证成功。然后数据库计算  $M_9 = h(X_s \oplus n_2)$  发送给车载阅读器,而只有拥有  $K_r$  的合法车载阅读器可以计算出  $X_s' = h(K_r \parallel IDS) \oplus K_r$  和  $M_9' = h(X_s' \oplus n_2)$ ,验证  $M_9'$  和  $M_9$  成功则车载阅读器对数据库验证成功,最终车载阅读器与数据库双向认证成功。因此,VRTFA 协议可以保障认证过程的双向认证性。

### 5.2 抵抗恶意攻击的安全分析

#### 5.2.1 去同步攻击

去同步攻击<sup>[32]</sup>是指阻止认证双方同步进行假名、密钥在内的认证信息更新而导致认证某一方密钥等认证信息未成功更新,最终使得合法认证双方由于假名和密钥等信息不一致无法彼此双向认证的安全隐患。在 VRTFA 协议中认证双方在进行密钥更新时不舍弃上一轮次的历史密钥、假名  $IDS$  与认证参数,所以在通信双方利用 VRTFA 协议存放两轮认证信息的方式可以防止去同步攻击。例如上轮认证结束时遥控钥匙更新假名  $IDS^{new}$ 、 $K_r^{new}$  和认证参数  $D^{new}$ ,同时也保留着上轮使用的  $IDS$ 、 $K_r$  和认证参数  $D$ 。若车载阅读器未成功更新  $IDS^{new}$ 、 $K_r^{new}$  和  $C^{new}$  将运算出  $M_1 = h(ID \parallel IDS) \oplus n_1$  和  $M_2 = h(ID \parallel n_1)$  发送给遥控钥匙,遥控钥匙无法利用更新的  $IDS^{new}$  从  $M_1$  和  $M_2$  获取并验证随机数  $n_1$ ,则遥控钥匙可以使用存放上一轮的  $IDS$  获取随机数并验证  $M_2$  合法性,成功在去同步攻击下完成对车载阅读器合法性的认证。因此,VRTFA 协议可以抵抗去同步攻击。

#### 5.2.2 伪造攻击

伪造攻击<sup>[33]</sup>指攻击者伪造发送端的消息发送给接收端并被成功认证为合法发送端。VRTFA 协议中攻击者在没有获取合法密钥和认证参数的条件下无法随意伪造出可被认证双方验证成功的认证消息。例如攻击者试图伪造车载阅读器发送给遥控钥匙的消息  $M_{10}$  和  $M_{11}$ ,其中  $M_{10} = h(ID \parallel K_r \parallel \delta) \oplus n_2$ ,  $M_{11} = h(ID \parallel K_r \parallel \delta \parallel n_2)$ 。而攻击者在未知  $ID$ 、 $K_r$ 、 $\delta$  和  $n_2$  的情况下无法伪造出合法可被遥控钥匙验证通过的  $M_{10}$  和  $M_{11}$ 。因此,VRTFA 协议可以抵抗伪造攻击。

#### 5.2.3 重放攻击

重放攻击<sup>[34]</sup>是攻击者通过窃听认证通信的过程中交互消息,攻击者伪装自己是合法实体将截获的历史轮次消息重放给认证的另一端实体并被验证成功。以往 RKE 的认证命令码认证方式下存在重放攻击的风险,由于数量有限的认证命令码是循环使用且不更新的,所以攻击者可以通过之前窃听截获的认证命令码发送给车载阅读器并且通过验证。而 VRTFA 协议利用轻量级加密运算、单向哈希函数、密钥更新机制以及随机数机制使得每轮发送的认证消息具有随机性和新鲜性。比如攻击者利用上轮截取遥控钥匙的消息  $M_3 =$

$\delta \oplus h(ID \oplus n_1)$ 、 $M_4 = K_r \oplus h(IDS \oplus n_1)$  和  $M_5 = h(ID \parallel K_r \parallel \delta \parallel n_1)$ ,将  $M_3 \parallel M_4 \parallel M_5$  发送给车载阅读器,而车载阅读器假名已经更新为  $IDS^{new}$ ,并且本轮车载阅读器随机产生的  $n_1^{new}$  也与上次使用的  $n_1$  不一样,所以攻击者重放的  $M_3$ 、 $M_4$  和  $M_5$  将无法通过验证。因此,VRTFA 协议可以抵抗重放攻击。

#### 5.2.4 中间人攻击

中间人攻击<sup>[34]</sup>是指攻击者在认证双方中间发挥消息转发的作用的同时,修改窃听交互消息的方式来达到攻击目的。而中间人攻击在 RKE 场景下对认证安全性的威胁不大,用户与车辆的距离近导致无线射频信号送达的时间过短,给攻击者实施中间人攻击提供了较大的难度。此外 VRTFA 协议可以抵抗伪造攻击并且通过单向哈希函数验证消息完整性,所以攻击者实施中间人攻击时篡改的认证消息将无法被验证通过。因此,VRTFA 协议可以抵抗中间人攻击。

#### 5.2.5 物理克隆攻击

物理克隆攻击<sup>[35]</sup>是指攻击者通过复制电子控制元件中的加密算法和密钥从而克隆出车辆的遥控钥匙,最终在未经合法授权的条件下非法开启车辆。VRTFA 协议利用 PUF 对不同硬件物理结构的产生的随机响应不同且不同预测的特性,由于在生产制造过程中自然发生的物理变化具有独特的硬件物理特性导致制造出两个完全相同的芯片的可能性微乎其微,使攻击者仅复制电子控制元件中的加密算法和密钥的条件下无法对遥控钥匙成功克隆。此外具备基于密钥因子与指纹因子的 VRTFA 双因子协议将影响到攻击者克隆的遥控钥匙的可用性。即使攻击者获取合法遥控钥匙,由于没有合法用户的生物指纹因子信息,所以攻击者无法通过遥控钥匙对用户采集生物指纹的认证。例如遥控钥匙向车载阅读器发送消息之前会采集用户生物指纹  $Bio$  后利用指纹恢复函数恢复协议注册阶段舍弃的参数  $\delta' = Rep(Bio, \tau)$ ,计算  $D' = PUF(IDS \parallel K_r \parallel \delta')$ ,验证  $D'$  是否和遥控钥匙内存放的认证参数  $D$  是否相等。验证成功则表示用户生物指纹合法,否则遥控钥匙不向车载阅读器发送认证请求。因此,VRTFA 协议可以抵抗物理克隆攻击。

#### 5.2.6 密钥全泄漏攻击

现有 RFID 认证协议将标签与阅读器等所有认证方密钥信息均明文存放在数据库中,攻击者只需攻击后台数据库就可以获取标签与阅读器等其他认证设备的密钥信息,造成密钥全泄漏攻击<sup>[36]</sup>。VRTFA 协议利用密钥信息提前运算出认证参数并间接验证的认证方式,防止由于数据库泄漏导致对整个认证协议产生密钥全泄漏的安全威胁。具体实现方式是数据库在注册阶段或上一轮认证阶段利用密钥和生物指纹因子等秘密值运算出下次认证阶段使用的认证参数。数据库内只存放假名、 $ID$  以及认证参数,并且遥控钥匙和车载设备均只存储自身设备的密钥并不存储其余认证设备密钥和生物指纹因子在内的秘密信息。在认证阶段数据库利用认证参数提取验证信息从而实现安全双向认证,而攻击者即使攻击数据库获取到认证参数也无法推导出车载阅读器与遥控钥匙的秘密信息。例如注册阶段车载阅读器将  $K_r \parallel K_r \parallel \delta$  发送给数据库,数据库计算相应的认证参数  $X_s = h(K_r \parallel IDS) \oplus K_r$ ,  $A = X_s \oplus h(IDS \parallel K_r)$ ,  $B = h(IDS \parallel K_r \parallel X_s \parallel \delta) \bmod n_0$ 。最后数据库不存储车载阅读器密钥  $K_r$ 、遥控钥匙密钥  $K_r$  和生物指纹因子参数  $\delta$ ,只存储认证参数  $A$ 、 $B$  和  $n_0$  以备后续认证。

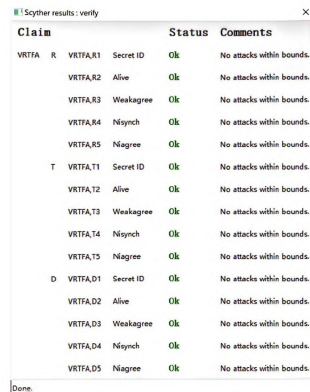


即使攻击者攻击数据库并获取到认证参数 $A$ 、 $B$ 和 $n_0$ 也无法提取出 $K_r$ 、 $K_R$ 和 $\delta$ 等密钥信息。因此,VRTFA 协议可以抵抗密钥全泄漏攻击。

### 5.3 安全属性分析

Scyther<sup>[37]</sup>是一种协议安全性分析验证的工具,以下将利用 Scyther 工具对 VRTFA 协议进行安全性分析验证。

在 VRTFA 协议建模中,定义三个角色 D、R 与 T,分别表示参与协议通信方的主机数据库、车载阅读器和遥控钥匙。本文利用 Scyther 分析验证 VRTFA 协议的安全性,结果如图 4 所示。其中:Secret、Alive、Weakagree、Niagree 和 Nisynch 分别用于检测密钥泄露、重放攻击、中间人攻击等恶意攻击。分析结果表明:Scyther 工具无法找到针对 VRTFA 协议的任何恶意攻击,因此 VRTFA 协议能够保证遥控钥匙与车载阅读器以及主机数据库之间的秘密信息安全。



Claim	Status	Comments
VRTFA R VRTFA.R1 Secret ID	Ok	No attacks within bounds.
VRTFA.R2 Alive	Ok	No attacks within bounds.
VRTFA.R3 Weakagree	Ok	No attacks within bounds.
VRTFA.R4 Nisynch	Ok	No attacks within bounds.
VRTFA.R5 Niagree	Ok	No attacks within bounds.
T VRTFA.T1 Secret ID	Ok	No attacks within bounds.
VRTFA.T2 Alive	Ok	No attacks within bounds.
VRTFA.T3 Weakagree	Ok	No attacks within bounds.
VRTFA.T4 Nisynch	Ok	No attacks within bounds.
VRTFA.T5 Niagree	Ok	No attacks within bounds.
D VRTFA.D1 Secret ID	Ok	No attacks within bounds.
VRTFA.D2 Alive	Ok	No attacks within bounds.
VRTFA.D3 Weakagree	Ok	No attacks within bounds.
VRTFA.D4 Nisynch	Ok	No attacks within bounds.
VRTFA.D5 Niagree	Ok	No attacks within bounds.

图3 Scyther 工具验证 VRTFA 协议安全性的结果

Fig. 3 Result of verifying VRTFA protocol security with Scyther tool

## 6 VRTFA 协议性能分析

### 6.1 安全性对比分析

VRTFA 协议和现有典型 RFID 双向认证协议<sup>[16-17,20-21]</sup>的安全性对比分析如表 2 所示,其中 Yes 表示该协议满足该安全性,No 表示不满足该安全性。通过表 2 可以得出与现有 RFID 双向认证协议<sup>[16-17,20-21]</sup>相比,VRTFA 协议具有更高的安全性,可以抵抗文献[16-17]中协议无法抵抗的物理克隆攻击和文献[16-17,20-21]中协议无法抵抗的密钥全泄漏攻击。

### 6.2 性能对比分析

#### 6.2.1 存储开销对比分析

在存储开销方面,VRTFA 协议中遥控钥匙需要存储的信息包括标签 ID、标签假名 IDS、认证参数 $D$ 、 $\tau$ 、密钥 $K_r$ 和 $IDS^{old}$ 、 $D^{old}$ 、 $K_r^{old}$ 共 8 个单位长度 $L$ 的数据,所以标签存储开销为 $8L$ 。文献[16]协议的标签存储开销为 $3L$ ,文献[17]协议的标签存储开销为 $3L$ ,文献[20]协议的标签存储 $TID$ 和 $n$ 个 $PID_i$ 开销为 $(n+1)*L$ ,文献[21]协议的标签存储 $FID$ 和 $n$ 个 $PID_i$ 开销为 $(n+1)*L$ 。VRTFA 协议虽然存储开销大于文献[16-17]协议,但是安全性更高。此外,VRTFA 协议不仅存储开销小于文献[20-21]协议,而且可以解决文献[20-21]协议存在的密钥全泄漏安全隐患。

表2 VRTFA 协议与其他 RFID 认证协议的安全性对比分析

Tab. 2 Security comparison and analysis of VRTFA protocol and other RFID authentication protocols

安全属性	文献[16]协议	文献[17]协议	文献[20]协议	文献[21]协议	VRTFA 协议
数据完整性	Yes	Yes	Yes	Yes	Yes
前向安全性	Yes	Yes	Yes	Yes	Yes
不可追踪性	Yes	Yes	Yes	Yes	Yes
双向认证性	Yes	Yes	Yes	Yes	Yes
去同步攻击	Yes	Yes	Yes	Yes	Yes
抗伪造攻击	Yes	Yes	Yes	Yes	Yes
抗重放攻击	Yes	Yes	Yes	Yes	Yes
抗中间人攻击	Yes	Yes	Yes	Yes	Yes
抗物理克隆攻击	No	No	Yes	Yes	Yes
抗密钥全泄露攻击	No	No	No	No	Yes

#### 6.2.2 计算代价对比分析

在计算代价方面,利用运算函数的执行次数对比 VRTFA 协议与其他 RFID 认证协议的计算代价,其中 $T_h$ 表示计算一次哈希函数的计算量, $T_r$ 表示产生一个随机数的计算量, $T_x$ 表示一次异或运算的计算量, $T_e$ 表示一次对称加解密的计算量, $T_p$ 表示计算一次 PUF 的计算量, $T_c$ 表示计算一次循环校验函数的计算量。

文献[16]协议:标签端执行了 2 次循环校验函数和 3 次异或运算;阅读器与数据库(以下简称服务端)一共执行了 5 次循环校验函数和 4 次异或运算。

文献[17]协议:标签端执行了 2 次对称加密运算和 7 次哈希函数;服务端一共执行了 10 次对称加密运算、14 次哈希函数和 2 次随机数运算。

文献[20]协议:标签端执行了 1 次随机数运算、3 次 PUF、6 次哈希函数和 3 次异或运算;服务端一共执行了 1 次随机数运算、1 次 PUF、6 次哈希函数和 2 次异或运算;标签端执行了 1 次随机数运算、4 次 PUF、7 次哈希函数和 4 次异或运算;服务端一共执行了 2 次随机数运算、7 次哈希函数和 4 次异或运算。

VRTFA 协议的标签端执行了 2 次 PUF、9 次哈希函数和 7 次异或运算;服务端一共执行了 2 次随机数运算、28 次哈希函数和 17 次异或运算。

文献[16]协议仅使用轻量级运算所以计算代价最低,而物理克隆攻击的难度也最低。文献[17]协议使用对称加密运算导致计算代价比 VRTFA 协议高。文献[20-21]协议标签会产生随机数的开销,VRTFA 协议为减少遥控钥匙的计算代价,由服务器端负担随机数运算的开销,所以文献[20-21]协议标签端的计算代价比 VRTFA 协议高。文献[20-21]协议中阅读器仅用作转发消息,阅读器本身不参与运算也不存储密钥,这样虽然降低了文献[20-21]协议服务器端计算代价,但也存在缺少阅读器与数据库之间的双向认证的安全隐患;而 VRTFA 协议实现双向认证的同时,可以抵抗文献[20-21]协议无法抵抗的密钥全泄漏攻击,具有更高的安全性。

#### 6.2.3 通信开销对比分析

在通信开销方面,VRTFA 协议在认证流程中发送 13 个单位长度 $L$ 的数据,所以总通信开销为 $13L$ 。文献[16]协议通信开销为 $8L$ ,文献[17]协议通信开销为 $32L$ ,文献[20]协



议通信开销为  $7L$ , 文献[21]协议通信开销为  $13L$ 。VRTFA 协议与文献[17]协议相比具备通信成本更低的优势, 同时 VRTFA 协议在牺牲少量通信开销的情况下可以抵抗文献

[16-17]协议无法抵抗的物理克隆攻击和密钥全泄漏攻击。

VRTFA 协议和现有 RFID 双向认证协议<sup>[16-17, 20-21]</sup>的详细性能对比分析如表 3 所示。

表 3 VRTFA 协议与其他 RFID 认证协议性能对比分析

Tab. 3 Performance comparison and analysis of VRTFA protocol and other RFID authentication protocols

协议	标签计算代价	服务端计算代价	通信开销	标签存储开销	服务端存储开销
文献[16]协议	$2T_C + 3T_X$	$5T_C + 4T_X$	$8L$	$3L$	$7L$
文献[17]协议	$2T_E + 7T_H$	$10T_E + 14T_H + 2T_R$	$32L$	$3L$	$10L$
文献[20]协议	$1T_R + 3T_P + 6T_H + 3T_X$	$1T_R + 1T_P + 6T_H + 2T_X$	$7L$	$(n+1)*L$	$9n*L$
文献[21]协议	$1T_R + 4T_P + 7T_H + 4T_X$	$2T_R + 7T_H + 4T_X$	$13L$	$(n+1)*L$	$6n*L$
VRTFA 协议	$2T_P + 9T_H + 7T_X$	$2T_R + 28T_H + 17T_X$	$13L$	$8L$	$8L$

通过表 3 可以看出, 与文献[16-17]的认证协议相比, 虽然 VRTFA 协议的标签端存储成本较高, 但它牺牲了部分计算代价与存储开销, 抵抗了物理克隆攻击和密钥全泄漏攻击。VRTFA 协议存储开销和标签计算代价比文献[21-21]的认证协议更低, 成功实现了阅读器与数据库之间的安全双向认证。综上所述, VRTFA 协议避免了现有协议<sup>[16-17, 20-21]</sup>存在的安全隐患, 在能够实现更好安全性的同时也满足 RKE 成本受限的需求。

## 7 结语

本文针对现有 RKE 存在重放攻击与物理克隆攻击的风险, 提出一种抵抗物理克隆攻击的 RFID 双因子认证 (VRTFA) 协议。通过 PUF 和双因子认证防止遥控钥匙被物理克隆或者非法盗用。VRTFA 协议通过提前存放认证参数的方式, 在保障双向认证性的前提下解决了数据库被攻击而导致密钥信息全泄漏的安全问题。VRTFA 协议安全高效地保障了 RKE 的双向认证, 更加适用于 RKE 等资源受限的实际应用场景, 为解决现有 RKE 认证机制存在的安全隐患提出了一种新思路。

## 参考文献 (References)

- [1] CHENG J J, CHENG J L, ZHOU M C, et al. Routing in Internet of Vehicles: a review [J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(5): 2339-2352.
- [2] 侯琬钰, 孙钰, 李大伟, 等. 基于 PUF 的 5G 车联网 V2V 匿名认证与密钥协商协议[J]. 计算机研究与发展, 2021, 58(10): 2265-2277. (HOU W Y, SUN Y, LI D W, et al. Anonymous authentication and key agreement protocol for 5G-V2V based on PUF [J]. Journal of Computer Research and Development, 2021, 58(10): 2265-2277.)
- [3] 宋涛, 李秀华, 李辉, 等. 大数据时代下车联网安全加密认证技术研究综述[J]. 计算机科学, 2022, 49(4): 340-353. (SONG T, LI X H, LI H, et al. Overview of research on security encryption authentication technology of IoV in big data era [J]. Computer Science, 2022, 49(4): 340-353.)
- [4] 王春东, 罗婉薇, 莫秀良, 等. 车联网互信认证与安全通信综述[J]. 计算机科学, 2020, 47(11): 1-9. (WANG C D, LUO W W, MO X L, et al. Survey on mutual trust authentication and secure communication of Internet of Vehicles [J]. Computer Science, 2020, 47(11): 1-9.)
- [5] FENG X, SHI Q, XIE Q, et al. P2BA: a privacy-preserving protocol with batch authentication against semi-trusted RSUs in Vehicular Ad hoc Networks [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3888-3899.
- [6] PASCALE F, ADINOLFI E A, COPPOLA S, et al. Cybersecurity in automotive: an intrusion detection system in connected vehicles [J]. Electronics, 2021, 10(15): No. 1765.
- [7] LANG D, HAAR D van der. Recommendations for biometric access control system deployment in a vehicle context in South Africa [M]// KIM K J, KIM H Y. Information Science and Applications: ICISA 2019, LNEE 621. Singapore: Springer, 2020: 305-317.
- [8] ALLADI T, KOHLI V, CHAMOLA V, et al. Artificial Intelligence (AI)-empowered intrusion detection architecture for the Internet of Vehicles [J]. IEEE Wireless Communications, 2021, 28(3): 144-149.
- [9] KAFAN. 360 Network Attack and Defense Lab announces that Tesla's vulnerability can be removed without a key [EB/OL]. [2022-01-21]. <https://bbs.kafan.cn/thread-1804633-1-1.html>.
- [10] 刘晓龙. 车联网 OBU 多级安全架构及通信方案研究 [D]. 镇江: 江苏大学, 2018. (LIU X L. Research on OBU-based multilevel security architecture and communication scheme for Internet of Vehicles [D]. Zhenjiang: Jiangsu University, 2018.)
- [11] ELECFANS. 百度成功破解 T-BOX 系统 车联网安全迈上新高度 [EB/OL]. (2016-11-30) [2022-01-21]. <http://www.elecfans.com/qichedianzi/20161130453520.html>. (ELECFANS. Baidu successfully cracked the T-BOX system and brought Internet of Vehicles security to a new level [EB/OL]. (2016-11-30) [2022-01-21]. <http://www.elecfans.com/qichedianzi/20161130453520.html>.)
- [12] TENCENT. Tencent Cohen Lab successfully invaded Tesla remotely for the first time [EB/OL]. (2016-09-20) [2022-01-21]. <https://tech.qq.com/a/20160920/048201.html>.
- [13] OK 特斯拉. 喜闻乐见! 特斯拉 Model S 被盗: 1 分钟内打开车门, 3 分钟盗走车辆 [EB/OL]. (2019-12-02) [2022-01-21]. <https://www.oktesla.cn/2019/12/33280.html>. (OK TESLA. Love to see and hear! Tesla Model S was stolen: open the door within 1 minute and steal the vehicle within 3 minutes [EB/OL]. (2019-12-02) [2022-01-21]. <https://www.oktesla.cn/2019/12/33280.html>.)
- [14] LIU Y, YIN X, DONG Y, et al. Lightweight authentication scheme with inverse operation on passive RFID tags [J]. Journal of the Chinese Institute of Engineers, 2019, 42(1): 74-79.
- [15] 李涛, 刘亚丽. 一种基于双 PUF 的 RFID 认证协议 [J]. 计算机研究与发展, 2021, 58(8): 1801-1810. (LI T, LIU Y L. A double PUF-based RFID authentication protocol [J]. Journal of Computer Research and Development, 2021, 58(8): 1801-1810.)
- [16] 黄琪, 凌捷. 一种超轻量级移动射频识别的双向认证协议 [J]. 计算机科学, 2017, 44(7): 111-115. (HUANG Q, LING J. Ultra-lightweight mutual authentication protocol for mobile radio frequency identification [J]. Computer Science, 2017, 44(7): 111-115.)
- [17] 李璐璐, 董庆宽, 陈萌萌. 基于云的轻量级 RFID 群组标签认证

- 协议[J]. 计算机科学, 2019, 46(1): 182-189. (LI L L, DONG Q K, CHEN M M. Cloud-based lightweight RFID group tag authentication protocol [J]. Computer Science, 2019, 46(1): 182-189.)
- [18] 王悦, 樊凯. 物联网中超轻量级 RFID 电子票据安全认证方案[J]. 计算机研究与发展, 2018, 55(7): 1432-1439. (WANG Y, FAN K. Ultra-lightweight RFID electronic ticket authentication scheme in IoT [J]. Journal of Computer Research and Development, 2018, 55(7): 1432-1439.)
- [19] 王国伟, 贾宗璞, 彭维平. 基于动态共享密钥的移动 RFID 双向认证协议[J]. 电子学报, 2017, 45(3): 612-618. (WANG G W, JIA Z P, PENG W P. A mutual authentication protocol of mobile RFID based on dynamic shared-key [J]. Acta Electronica Sinica, 2017, 45(3): 612-618.)
- [20] GOPE P, LEE J, QUEK T Q S. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(11): 2831-2843.
- [21] GOPE P, SIKDAR B. An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones[J]. IEEE Transactions on Vehicular Technology, 2020, 69(11): 13621-13630.
- [22] DAS M L. Two-factor user authentication in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086-1090.
- [23] WANG D, HE D, WANG P, et al. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment [J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(4): 428-442.
- [24] 李文婷, 汪定, 王平. 无线传感器网络下多因素身份认证协议的内部人员攻击[J]. 软件学报, 2019, 30(8): 2375-2391. (LI W T, WANG D, WANG P. Insider attacks against multi-factor authentication protocols for wireless sensor networks [J]. Journal of Software, 2019, 30(8): 2375-2391.)
- [25] QIU S, WANG D, XU G. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 1338-1351.
- [26] CAI Q, ZHAN Y, WANG Y. A minimalist mutual authentication protocol for RFID system & BAN logic analysis [C]// Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management — Volume 2. Piscataway: IEEE, 2008: 449-453.
- [27] LIU K, YE J, WANG Y. The security analysis on Otway-Rees protocol based on BAN logic [C]// Proceedings of the 4th International Conference on Computational and Information Sciences. Piscataway: IEEE, 2012: 341-344.
- [28] XU H, DING J, LI P, et al. A lightweight RFID mutual authentication protocol based on physical unclonable function [J]. Sensors, 2018, 18(3): No. 760.
- [29] 马昌社. 前向隐私安全的低成本 RFID 认证协议[J]. 计算机学报, 2011, 34(8): 1387-1398. (MA C S. Low cost RFID authentication protocol with forward privacy [J]. Chinese Journal of Computers, 2011, 34(8): 1387-1398.)
- [30] YE H K. A lightweight authentication scheme with user untraceability [J]. Frontiers of Information Technology and Electronic Engineering, 2015, 16(4): 259-271.
- [31] JAN M A, KHAN F, ALAM M, et al. A payload-based mutual authentication scheme for Internet of Things [J]. Future Generation Computer Systems, 2019, 92: 1028-1039.
- [32] LIU Y, EZERMAN M F, WANG H. Double verification protocol via secret sharing for low-cost RFID tags [J]. Future Generation Computer Systems, 2019, 90: 118-128.
- [33] WANG W, CHEN Q, YIN Z, et al. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks [J]. IEEE Internet of Things Journal, 2022, 9(11): 8883-8891.
- [34] SYAFRILAH Z, PERMANA A A, HANDAYANI A D. Modified RAP-WOTA for preventing man in the middle and replay attacks [C]// Proceedings of the 2019 International Workshop on Big Data and Information Security. Piscataway: IEEE, 2019: 73-78.
- [35] BENDAVID Y, BAGHERI N, SAFKHANI M, et al. IoT device security: challenging “a lightweight RFID mutual authentication protocol based on physical unclonable function” [J]. Sensors, 2018, 18(12): No. 4444.
- [36] MENG L, XU H, XIONG H, et al. An efficient certificateless authenticated key exchange protocol resistant to ephemeral key leakage attack for V2V communication in IoV [J]. IEEE Transactions on Vehicular Technology, 2021, 70(11): 11736-11747.
- [37] CREMERS C J F. The Scyther tool: verification, falsification and analysis of security protocols [C]// Proceedings of the 2008 International Conference on Computer Aided Verification, LNCS 5123. Berlin: Springer, 2008: 414-418.
- This work is partially supported by National Natural Science Foundation of China (61702237), Science and Technology Planning Foundation of Xuzhou City (KC22052), Opening Foundation of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund, Fujian Normal University (NSCL-KF2021-04), Opening Foundation of Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology (GCIS202114), Postgraduate Research and Practice Innovation Program of Jiangsu Normal University (2021XKT1382, 2022XKT1488), Ministry of Education University-Industry Collaborative Education Program of China (202101374001).
- LIU Changgeng**, born in 1997, M. S. candidate. His research interests include Radio Frequency Identification (RFID) authentication, Internet of Things security, privacy-preserving.
- LIU Yali**, born in 1981, Ph. D., professor. Her research interests include information security, authentication and privacy-preserving, blockchain, vehicular ad-hoc network, cryptographic algorithms and protocols.
- LU Qipeng**, born in 1999, M. S. candidate. His research interests include Radio Frequency Identification (RFID) authentication, privacy-preserving, Internet of Things security, blockchain.
- LI Tao**, born in 1998, M. S. candidate. His research interests include Radio Frequency Identification (RFID) authentication, privacy-preserving, Internet of Things security, blockchain.
- LIN Changlu**, born in 1978, Ph. D., professor. His research interests include cryptography, network security, secret sharing, secure multi-party computation, public-key cryptography.
- ZHU Yi**, born in 1976, Ph. D., professor. His research interests include formal analysis, software reliability, intelligent software, adaptive learning.