CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 45 卷第 1 期 2023 年 1 月
Vol. 45, No. 1, Jan. 2023

文章编号:1007-130X(2023)01-0077-08

RFID 安全认证协议综述*

寇广岳[1],魏国珩[1],平　源[2],刘　鹏[3]
(1.海军工程大学信息安全系,湖北 武汉 430000;2.许昌学院信息工程学院,河南 许昌 461000;
3.海军参谋部,北京 100000)

摘　要:在物联网发展中,RFID 技术以其轻量化的优势在物联网体系中占据重要地位。同时,RFID 安全认证协议也因物理条件限制受到安全威胁。首先,通过对现行主流 RFID 安全认证协议进行梳理,按加密算法的量级将其划分为超轻量级、轻量级、中量级和重量级安全认证协议;然后,对其中典型的安全认证协议存在的安全问题进行分析,对近年来提出的改进协议安全性能及性能指标按量级进行讨论比较;最后,探讨了 RFID 安全认证协议可能的发展方向。

关键词:物联网;RFID;身份验证;安全认证协议
中图分类号:TP391.41　　**文献标志码**:A
doi:10.3969/j.issn.1007-130X.2023.01.009

Overview of RFID security authentication protocols

KOU Guang-yue[1], WEI Guo-heng[1], PING Yuan[2], LIU Peng[3]
(1.Department of Information Security, Naval University of Engineering, Wuhan 430000;
2.School of Information Engineering, Xuchang University, Xuchang 461000;
3.Naval Staff, Beijing 100000, China)

Abstract: In the development of the Internet of Things, RFID technology with its lightweight advantage plays an important role in the Internet of Things (IoT) system. At the same time, RFID authentication protocols are also subject to security threats due to physical limitations. By sorting out the current mainstream RFID authentication protocols, they are divided into ultra-lightweight, lightweight, middleweight, and heavyweight security authentication protocols according to the magnitude of the encryption algorithm. The security problems of typical security authentication protocols are analyzed, and the security performance and performance indicators of the improved protocols proposed in recent years are discussed and compared according to the magnitude. Finally, the possible development direction of RFID authentication protocols is discussed.

Key words: Internet of Things(IoT); RFID; authentication; security authentication protocol

1　引言

近些年,随着物联网技术的不断成熟,基于物联网技术的各项应用不断深入发展并应用于实际,其中比较典型和成熟的是 RFID(Radio Frequency Identification)技术。RFID 是一种采用射频信号与空间耦合来达成无接触信息传递从而实现目标主体识别的技术。在物流、交通、身份识别、防伪、资产管理、食品、信息统计、查阅应用和安全控制等领域应用广泛。IDTechEx 的数据显示:全球 RFID 市场预计在 2021 年价值 116 亿美元,到 2022 年将达到 122 亿美元[1]。

通常意义的 RFID 系统包含电子标签(Tag)、RFID 标签读写器和后台数据库,如图 1 所示。Tag 主要用于存储用户信息,由天线和射频芯片构

* 收稿日期:2022-09-14;修回日期:2022-10-29
通信地址:430000 湖北省武汉市海军工程大学信息安全系
Address: Department of Information Security, Naval University of Engineering, Wuhan 430000, Hubei, P.R.China

成,由于受制电子标签有限的物理结构,通常认为其运算能力较为有限,且易受到安全威胁。RFID标签读写器用于读写电子标签信息与防止碰撞等方面,理论上RFID标签读写器应在物理层面具有较大的存储空间与较强的计算能力。后台数据库主要存储标签、读写器及其它信息,具有强大的数据处理与存储能力。一般认为在RFID系统中,Tag与Tag读写器之间是不安全信道,Tag读写器与后台数据库之间是安全信道[2]。

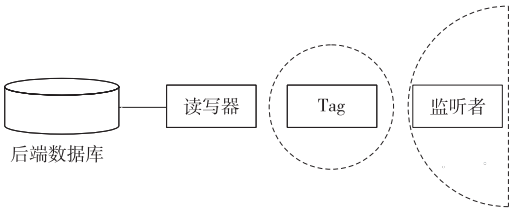

Figure 1 Basic composition of RFID system

图1 RFID系统基本构成

由于电子标签物理结构的局限性,Tag由几百门到几千门电路构成,通常Tag出于经济与轻量化考量不设微处理器,集成签名或加密算法也不方便,因此,在RFID系统中提供安全认证协议十分困难。面对强大且具有针对性的攻击者时,如何在有限的门电路上设计出高效、安全的RFID安全认证协议成为一项具有挑战性的研究,也吸引了众多密码学家的关注。

本文将RFID安全认证协议中的代表性工作按所采用密码算法的复杂程度分为超轻量级协议、轻量级协议、中量级协议和重量级协议,并进行了整理、分析与归纳。第2节简要介绍了RFID安全认证协议的构成和分类以及面临的主要威胁;第3节对现有安全协议进行了划分,并简要介绍了每种类别下的经典协议模型,针对近年的论文分类讨论了其在面对安全威胁时的表现;第4节对RFID安全协议的发展进行了预测与展望;第5节对全文进行总结。

2 RFID协议系统构成

2.1 RFID系统协议模型

现有安全认证协议研究中的一个重要指标是要符合现有通行协议标准。ISO/IEC 18000标准[3]决定了RFID标签与RFID读写器之间的通讯规则,模型从上到下依次由物理层、通信层和应用层构成,如图2所示。

此外,常用的RFID协议还包括广泛应用于身

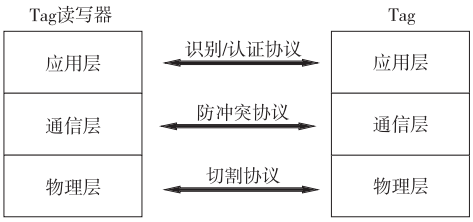

Figure 2 Communication model of RFID system

图2 RFID系统的通信模型

份证银联卡的ISO/IEC 14443[4]、读写距离可达1 m的ISO/IEC 15693[5]和NFC协议ISO 18092[6]。设计安全认证协议时要格外注意必须符合相关协议标准模型。

2.2 RFID安全认证协议面临的威胁

一个成熟且完善的RFID安全认证协议除了需要满足ISO/IEC 18000标准模型外,最重要的是要具备应对现有主流威胁的抵抗能力,即需要满足一定的信息安全需求。本节对RFID安全认证协议面对的安全需求及主要威胁进行讨论。

评估RFID系统及安全认证协议从以下几个安全需求出发:

(1)机密性:完善的RFID安全认证协议应具备保护Tag中所包含的关键敏感信息的基本功能,并只对合法的读写器识别和解密。

(2)完整性:安全认证协议在通信过程中保持准确,应确保在传输过程中不会因误码或攻击导致数据被篡改、添加、删除。

(3)相互认证性:在通信双方传输或交换秘密信息之前,需要在读写器上与Tag进行相互认证,读写器与Tag均需证明各自身份的合法性。

(4)用户隐私性:RFID安全认证协议中的关键信息如标签身份、安全认证协议中关键字段等需要得到保护,以避免暴露其位置或被攻击者跟踪。

(5)前向与后向安全性:面对蓄意的攻击,低成本标签即使采用安全认证协议也很难抵御强力破解。因此RFID系统中的前向与后向安全显得极为重要。

RFID安全认证协议面临的常见攻击类型有以下几种:

(1)拒绝服务攻击:攻击者向服务器发送多个信号,以破坏RFID系统的可用性。

(2)去同步攻击:破坏受害者Tag与后端数据库之间的同步状态,攻击成功后,标签不再被认证为有效。

(3)泄漏风险:攻击者破解RFID系统中的通信密钥。

(4)克隆攻击:攻击者用设备读取标签或读取器信息,并伪造一个能通信的虚拟实体。

(5)可追踪性攻击:攻击者追踪标签信息并找到其位置,对其隐私进行破解。

(6)中间人攻击:攻击者截获 Tag 与阅读器之间的消息,修改并返回。

(7)重放攻击:攻击者捕获 Tag 并将其重新发送给读取器,以与读取器通信并获取秘密信息。

2.3 RFID 系统安全认证协议分类

基于 RFID 系统的用途及工作场合,RFID 具有不同的大小、形状及内部结构,具有多种划分方法。按工作方式可划分为主动式标签、半主动式标签与被动式标签;按标签的工作频率大小可划分为低频(LF)、高频(HF)、超高频(UHF)和微波 4 种;按计算能力可分为超轻量级、轻量级、中量级和重量级[7]。不同量级的划分是按标签结构中存在的等效门电路 GE(Gate Equivalents)的多少来确定的,理论上物理结构越复杂的标签能承载的安全认证协议算法也就越复杂。不同量级的标签采用的加密算法也相对比较固定[8]。超轻量级安全认证协议所采用的认证方法通常只涉及简单的逻辑运算(如与、或、异或);轻量级安全认证协议通常采用 PRNG(PseudoRandom Number Generator)算法及循环冗余码 CRC(Cyclic Redundancy Code);中量级安全认证协议则多用杂凑函数;采用 RSA 或椭圆曲线的算法常出现在重量级安全认证协议中。因此,本文计划按量级分类的方法对 RFID 安全协议进行分类,具体分类如表 1 所示。

Table 1 Level classification of RFID security authentication protocol

表 1 RFID 安全认证协议量级分类

计算量级	搭载加密算法
超轻量级算法	XOR、AND、OR 等
轻量级算法	RNG、CRC
中量级算法	ECC、one-way hash function
重量级算法	Symmetric encryption、elliptic curve algorithm、ECC

3 RFID 安全认证协议及其改进

本节对现有的 RFID 安全认证协议按密码算法所需门电路量级进行划分,并分别介绍了各量级下的经典安全认证协议与近年来改进的安全认证协议。

3.1 超轻量级安全认证协议及其改进

依据超轻量级安全认证协议的安全保障算法,本文将其大致分为 3 类:(1)基于 T 函数的超轻量 RFID 安全认证协议,此类安全认证协议通过 T 函数来保证协议安全,常用的 T 函数包括按位运算的 AND、OR 和 XOR;(2)基于旋转算子的超轻量 RFID 安全认证协议,采用旋转算子与 T 函数进行数据加密;(3)其它类型的超轻量级安全认证协议,通常是由设计者提出新的运算法则,如置换、合并和分离等相结合。前期流行的 RFID 超轻量级安全协议包括 HB 协议簇、UMAP 协议簇和 SASI 协议。HB 协议簇是基于 LPN(Learning Parity with Noise)的安全认证协议[9],LPN 问题是“矢量子集求和”难题,涉及的操作仅包含与或和异或;UMAP 协议簇包括 LMAP(Lightweight Mutual Authentication Protocol)[10]、EMAP(Efficient Mutual Authentication Protocol)[11]及 MMAP(Minimalist Mutual Authentication Protocol)[12],这些安全认证协议为了适应超轻量级受限的门电路环境均使用逐位运算;SASI 协议主要通过左循环移位操作与异或操作实现信息交互。

尽管前期的研究在超轻量级物理环境的限制下,用极小的代价实现了部分保密需求,但已有大量研究表明,上述安全认证协议容易受到重放攻击、去同步攻击和完全泄漏攻击[13-16]。表 2 对比了部分典型超轻量安全认证协议的安全性。Zhuang 等人[17]构造了一个名为 FindIndex 的人工函数来分析以上典型协议保持数据完整性的能力,通过 FindIndex 函数能发现消息中一个元素的某些位发生变化后其它位发生变化的可能性,从而证明了 LMAP、MMAP 、EMAP 和 David-Prasad SLMAP 等超轻量 RFID 安全认证协议都不能抵抗去同步攻击。特别证明了攻击者能够以非常高的成功率破坏基于 T 函数的超轻量 RFID 安全认证协议中标签和阅读器之间的同步。

Table 2 Security comparison of some typical ultra-lightweight security authentication protocols

表 2 部分典型超轻量安全认证协议安全性比较

攻击类型	LMAP	MMAP	EMAP	SASI
标签匿名	×	×	×	×
重放攻击	√	√	√	√
去同步攻击	×	×	×	×
中间人攻击	×	×	×	×
泄漏攻击	×	×	×	×

因此,近些年的研究多集中在改进与提升安全认证协议的安全性方面。Gao 等人[18]设计了URAP(a new Ultra-lightweight RFID Authentication Protocol),通过阅读器生成 PRNG 码开启认证,通过左旋和异或算法对后端服务器和需认证的标签的静态标识(ID)进行认证,能抵抗重放攻击、去同步攻击、中间人攻击和泄漏攻击,并通过 GNY 逻辑证明方法验证了安全认证协议的安全性;Mujahid 等人[19]通过重新定义一种只有左旋和异或构成的递归散列来抵抗去同步、重放和泄漏等攻击。Zhong 等人[20]使用新的密文引理和密文释放引理改进了 LoET (Logic of Events Theory)逻辑系统,分析并证明了 RCIA(Robust Confidentiality, Integrity, and Authentication)协议能够满足强认证特性,可防止重放攻击。Luo 等人[21]通过分析 2 种基于置换的安全认证协议 RRAP (Reconstruction based RFID Authentication Protocol)[22]和 RCIA 存在的安全问题,指出当输出的部分数据或全部数据确定时,攻击者可以复原其他数据,据此在此类安全认证协议基础上提出了新的置换方案 $CON(A,B)$,即根据长度为固定比特的字符串 A 与 B 的汉明权重进行分组并重新排列,此安全认证协议可抵抗重放攻击、去同步攻击、可追溯攻击和泄漏攻击。表 3 比较了以上部分安全认证协议的加密方式及存储成本(其中 L 表示单次通信的消息长度,单位为 bit)。

Table 3 Parameters comparison of some typical ultra-lightweight security authentication protocols

表 3 部分典型超轻量安全认证协议参数比较

	LMAP	SASI	URAP	RCIA	SLAP
加密方式	+⊕OR	+⊕Rot OR	⊕Rot	⊕ Rot AND	⊕ Rot XOR
存储成本	6L	6L	6L	7L	7L

3.2 轻量级安全认证协议及其改进

不同于超轻量级协议,多数轻量级安全认证协议是为了满足 ISO/IEC 18000(EPC C1Gen2)标准而提出的。EPC C1G2 (Class-1 Gen-2)类型安全认证协议多使用符合相关标准的简单加密手段。2006 年作为低成本轻量级 UHF RFID 标签的 ISO 18000-6 标准修正案出版。新版本的标准于 2013 年获得批准,具有一些可选的加密属性,如随机数生成器(PRNG)与循环冗余校验(CRC)算法。最新的标准标签使用 RNG 生成 16 位伪随机数(RN16)。

部分研究人员关注轻量级协议在满足标准后的安全性。Zavvari 等人[23]分析对比了符合 EPC C1G2 (Class-1 Gen-2)标准的 3 组典型轻量级协议的安全性,得出了在符合轻量级标准下应遵循的安全标准。轻量级安全认证协议的另一个关注重点是 PRNG 的安全性。Vaudenay [24]提出了一种基于 PRF 的弱隐私安全认证协议,通过改进此安全认证协议可以提高协议的隐私性。Arslan 等人[25]在文献[24]的基础上探讨了 RNG 的隐私安全性并提出了改进方案。表 4 比较了部分轻量级安全认证协议的安全性。

Table 4 Security comparison of some lightweight security authentication protocols

表 4 部分轻量安全认证协议安全性比较

协议	重放攻击	完整性	隐私性	去同步攻击	拒绝服务攻击	可追踪性攻击
文献[26]协议	√	√	√	√	√	√
文献[27]协议	√	√	√	×	√	√
文献[28]协议	√	√	√	√	√	√
文献[29]协议	√	√	√	×	×	×
文献[30]协议	√	√	√	√	√	√

针对轻量级安全认证协议的相关问题,众多研究人员在 EPC Class 1 Gen 2 标准下提出了众多轻量级安全认证协议。Cherneva 等人[26]在借鉴《SDZ 议定书》[27]部分构造思想的基础上提出了 SDGPP(Serial-Dependency Grouping-Proof Protocol),通过删除外部可信的时间戳服务器,可防止一个被损害的标签破坏整个系统。使用 EPC 为标签指定固定时间间隔,消除了对特定读取器的依赖,拓展了安全性与隐私性。Eslamnezhad 等人[28]则关注安全认证协议的可追溯性攻击问题,在 Sundaresan 等人[29]研究的基础上引入了 2 个计数参数来解决原安全认证协议易受可追溯性攻击的问题。Xie 等人[30]在 PUF (Physical Unclonable Function)结构的基础上,提出了一种基于双 PUF 的轻量级双向 RFID 身份认证协议,实现了双向认证功能。

3.3 中量级安全认证协议及其改进

中量级安全认证协议相较于前 2 种量级的安全认证协议,由于采用了部分经过轻量化的密码算法且基于单向散列函数,安全性要高于前 2 种协议的,最明显的特征是此类安全认证协议研究的重点是双向认证。虽然部分研究人员将能单向认证的安全认证协议划归到轻量级安全认证协议中,主流观点认为基于散列函数实现单向或双向认证的协

议是典型的中量级安全认证协议。比较经典的安全认证协议包括基于单向散列函数的Hash-Lock协议、改进的随机Hash-Lock协议、Hash链协议和David数字图书馆协议[31-34]等。前期已有大量针对上述经典安全认证协议的安全性分析[35-37]。其面临的主要安全威胁如表5所示。

Table 5 Security threats of typical mid-volume security authentication protocol

表5 典型中量安全认证协议面临的安全威胁

协议	可追踪性攻击	重放攻击	欺骗攻击	去同步攻击	双向认证	密钥更新
文献[31]协议	×	×	×	×	√	×
文献[32]协议	√	×	×	×	√	√
文献[33]协议	√	√	√	√	×	×
文献[34]协议	√	√	√	√	√	×

近年来,此类安全认证协议为基本模型的改进安全认证协议也不胜枚举[28-35],多是对安全性进行加强,或突出其中某项安全属性进行研究。Liu等人[38]在分析了典型中量级安全认证协议的安全问题后提出了改进安全认证协议,通过RFID标签计算散列值,并将散列值分为2部分:左半部分用于验证标签的身份,右半部分用于验证阅读器的身份,这样提高了安全性,减少了标签的计算和存储。Hosseinzadeh等人[39]在分析了Wang等人[40]的安全认证协议脆弱性的基础上,提出了面对强攻击者时分析阅读器与后端服务器之间不安全信道的安全模型,并提出了改进安全认证协议ISMAP(stands for Improved Server-Mounted Authentication Protocol)。Mansoor等人[41]对Gope等人[35]的安全认证协议进行了密码分析,证明了该安全认证协议在防碰撞、窃取验证者和拒绝服务攻击方面存在一些弱点,提出了一种仅使用轻量元素的改进方案来抵抗所有已知的攻击。

3.4 重量级安全认证协议及其改进

重量级安全认证协议也被部分文献命名为完备RFID安全认证协议,主要分为对称加密算法和非对称加密算法。为了实现高安全性,此类安全认证协议需要消耗大量门电路承载加密算法。考虑到RFID系统的物理局限性,其中比较有代表性的是基于对称加密算法DES的"三通互相鉴别"协议和基于RSA算法的认证协议[42]。以上安全认证协议均能达到较高的安全性,但需要1万门以上的逻辑门。为解决成本问题,基于椭圆曲线密码ECC(Ellipse Curve Cryptography)算法的安全认证协议不断被提出[43-55],并成为近几年研究的主流。

不同研究人员利用ECC为RFID认证提供服务,并采用了不同的加密和认证方法。大多数研究表明,只使用一种ECC算法的安全认证协议只能提供单向认证,且整个系统容易受到攻击。随着第2个ECC算法的安全认证协议的加入,双向认证达成,为系统整体提供了更好的安全性。2个ECC安全认证协议耦合的不同导致各个安全认证协议的效率与安全性有差异,表6简单比较了部分重量级安全认证协议的通信成本。表6中显示了每个安全认证协议的读取器与标签的标量乘法次数,并按每次标量乘法64 ms的计算成本计算了总时间。

Table 6 Comparison of communication cost of some heavy-lightweight security authentication protocols

表6 部分重量级协议通信成本比较

协议	标签计算成本/(ms)	服务器计算复杂度	标签通信成本/(bits)	服务器通信成本/(bits)
文献[49]协议	128	$O(n.(\log n))$	960	640
文献[50]协议	320	$O(n.(\log n))$	640	640
文献[51]协议	192	$O(n.(\log n))$	800	640
文献[52]协议	192	$O(n.(\log n))$	960	640
文献[53]协议	192	$O(n.(\log n))$	800	640
文献[54]协议	128	$O(n.(\log n)^2)$	800	160
文献[55]协议	128	$O(n.(\log n)^2)$	1 280	-

4 发展与展望

随着物联网技术的不断发展、RFID技术的不断进步、密码学不断完善,研究重点也在不断发生改变,从早期的几个经典安全认证协议模型基础上不断改进发展到现在根据应用场景的不同,设计适应其应用场景的安全认证协议,RFID安全认证协议正在不断完善与发展。近年已有研究人员将基于ECC算法的安全认证协议门电路控制在轻量级的水平。目前,在现有技术条件下,RFID安全认证协议主要有2个方向,一个是在前人研究基础上针对部分安全性漏洞进行修补并进行安全性的提升,另一个是保障安全性的基础上对现有协议的效率与通信开销进行优化。

同时,有众多研究人员将重心放在RFID安全认证协议的防碰撞性研究上[56-58],通常将防碰撞协议与安全协议作为单独的2部分考虑,也有人提出防碰撞的安全认证协议[59],利用防碰撞协议的模型可以在判断碰撞的同时嵌入认证协议,能同时

实现门电路的优化与认证手段的革新。

引入区块链技术也可能给 RFID 带来的变革和影响[60-64],将区块链的去中心化思想引入到基于散列的中量级安全认证协议中,将验证计算转移至阅读器和区块链节点中,可以有效降低标签的计算成本。

5 结束语

本文梳理了 RFID 系统安全认证协议的结构、标准与分类,并根据其中加密算法所需的门电路的不同将安全认证协议划分为 4 种量级,在列举了每种量级经典协议的基础上,分析了每种量级安全认证协议的典型模型、面临问题和近期研究重点。

(1)超轻量级 RFID 安全认证协议在极其有限的硬件开销下能进行基于一种或几种特别安全需求的认证,不具备较高的安全性,但在实际应用中由于其轻量性,适用的场景多。

(2)轻量级 RFID 安全认证协议多数在标准范畴下进行讨论,主要针对标准中的个别安全需求与计算开销进行优化。

(3)中量级 RFID 安全认证协议的关注重点是如何提高安全认证协议的安全性与减轻开销,以及在此量级下如何实现安全的双向认证功能。

(4)重量级 RFID 安全认证协议是近几年较为热点的 RFID 安全认证协议研究方向。众多研究人员将 ECC 轻量化作为研究重点,在保留较完备的安全性的前提下,本文比较了几个重量级 RFID 安全认证协议的通信成本。

(5)部分研究人员在纵向比较各项安全认证协议时忽略了对同级甚至是采用同类型安全认证协议的性能对比,在不考虑开销的情况下,加密机制比较完善的重量级安全认证协议与早期的超轻量级安全认证协议的安全性进行比较显然不严谨。超轻量级 RFID 安全认证协议通常用异或、旋转、移位和迭代次数计算,轻量级 RFID 安全认证协议通常使用随机数和循环冗余次数计算,中量级 RFID 安全认证协议通常用单向哈希及哈希次数计算,重量级 RFID 安全认证协议通常用标量乘法次数计算。

因此,基于 RFID 安全认证协议的量级不同,分析了其采取的典型加密认证手段,阐明了后续研究需要关注的重点,如超轻量安全认证协议关注的重点是如何在有限门条件下尽可能提升安全性;轻量级安全认证协议关注 PRNG 的安全性及是否符合相应行业标准;中量级安全认证协议较多关注隐私性问题与双向互通性;重量级安全认证协议重点在保证安全性的基础上如何降低所需门电路的数量。尽管不同量级的 RFID 安全认证协议安全性存在差异,但根据不同的应用场景,每种安全认证协议都是该应用下的最优协议。

参考文献:

[1] RFID Forecasts, Players and Opportunities 2022-2032 the complete analysis of the global RFID industry[EB/OL]. [2022-09-01]. https://www.idtechex.com/zh/research-report/rfid-forecasts-players-and-opportunities-2022-2032/849.

[2] Zhou Yong-bin, Feng Deng-guo. Design and analysis of cryptographic[J]. Chinese Journal of Computers, 2006, 29(4): 581-589.(in Chinese)

[3] Information technology—Radio frequency identification for item management: ISO/IEC 18000[S]. Switzerland: International Organization for Standardization, 2004.

[4] Cards and security devices for personal identification—Contactless proximity objects: ISO/IEC 14443[S]. Switzerland: International Organization for Standardization, 2018.

[5] Identification cards—Contactless integrated circuit cards—Vicinity cards: ISO/IEC 15693[S]. Switzerland: International Organization for Standardization, 2019.

[6] Information technology—Telecommunications and information exchange between systems—Nearfield communication—Interface and protocol(NFCIP-1): ISO/IEC18092[S]. Switzerland: International Organization for Standardization, 2013.

[7] Wang Ya, Wei Guo-heng, Wei Wei. Research on classification model of lightweight encryption algorithm for RFID applications[J]. Computer & Digital Engineering, 2017, 45(6): 1150-1155.(in Chinese)

[8] Wang Ya, Wei Guo-heng. A research summary on lightweight cryptographic algorithms for RFID[J]. Computer Applications and Software, 2017, 34(1): 9-14.(in Chinese)

[9] Hopper N J, Blum M. A secure human-computer authentication scheme[R]. Pittsburgh : Carnegie Mellon University, 2000.

[10] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags[C]// Proc of the 2nd Workshop on RFID Security, 2006: 6-18.

[11] Peris-Lopez P, Hernandez-Castro J C, Estévez-Tapiador J M, et al. EMAP: An efficient mutual-authentication protocol for low-cost RFID tags[C]// Proc of OTM Confederated International Conference on the Move to Meaningful Internet Systems, 2006: 352-361.

[12] Peris-Lopez P, Hernandez-Castro J C, Estévez-Tapiador J M, et al. M(2)AP: A minimalist mutual-authentication protocol for low-cost RFID tags[C]// Proc of the 3rd International Conference on Ubiquitous and Computing, 2006: 912-923.

[13] Li T, Wang G. Security analysis of two ultra-lightweight RFID authentication protocols[C]// Proc of IFIP International Information Security Conference, 2007:109-120.

[14] Zhuang X, Zhu Y, Chang C C, et al. Security issues in ultralightweight RFID authentication protocols[J]. Wireless Personal Communications, 2018, 98(1):779-814.

[15] Li T, Deng R. Vulnerability analysis of EMAP—An efficient RFID mutual authentication protocol[C]// Proc of the 2nd International Conference on Availability, Reliability and Security, 2007:238-245.

[16] Ain Q U, Mahmood Y, Mujahid U. Cryptanalysis of mutual ultralightweight authentication protocols: SASI & RAPP [C]// Proc of 2014 International Conference on Open Source Systems & Technologies, 2014:136-145.

[17] Zhuang X, Zhu Y, Chang C C, et al. Security issues in ultralightweight RFID authentication protocols[J]. Wireless Personal Communications, 2018, 98:779-814.

[18] Gao M, Lu Y B. URAP: A new ultra-lightweight RFID authentication protocol in passive RFID system[J]. The Journal of Supercomputing, 2022, 78(8):10893-10905.

[19] Mujahid U, Najam-Ul-Islam M, Shami M A. RCIA: A new ultralightweight RFID authentication protocol using recursive hash[J]. International Journal of Distributed Sensor Networks, 2015, 11(1):642180.

[20] Zhong X, Xiao M, Zhang T, et al. Proving mutual authentication property of RCIA protocol in RFID based on logic of events[J]. Chinese Journal of Electronics, 2022, 31(1):79-88.

[21] Luo H, Wen G, Su J, et al. SLAP: Succinct and lightweight authentication protocol for low-cost RFID system[J]. Wireless Networks, 2018, 24(1):69-78.

[22] Zhuang X, Zhu Y, Chang C C. A new ultralight-weight RFID protocol for low-cost tags: R2AP[J]. Wireless Personal Communications, 2014, 79(3):1787-1802.

[23] Zavvari A, Islam M T, Shakiba M, et al. Theoretical analysis of RFID security protocols[C]// Proc of 2014 IEEE International Conference on Industrial Engineering and Engineering Management, 2014:302-306.

[24] Vaudenay S. On privacy models for RFID[C]// Proc of International Conference on the Theory and Application of Cryptology and Information Security, 2007:68-87.

[25] Arslan A, Kardas S, Colak S A, et al. Are RNGs achilles' heel of RFID security and privacy protocols? [J]. Wireless Personal Communications, 2018, 100(4):1355-1375.

[26] Cherneva V, Trahan J L. A secure and efficient parallel-dependency RFID grouping-proof protocol[J]. IEEE Journal of Radio Frequency Identification, 2020, 4(1):14-23.

[27] Sundaresan S, Doss R, Zhou W. Zero knowledge grouping proof protocol for RFID EPC C1G2 tags[J]. IEEE Transactions on Computers, 2015, 64(10):2994-3008.

[28] Eslamnezhad N M, Hosseinzadeh M, Bagheri N, et al. A secure search protocol for lightweight and low-cost RFID systems[J]. Telecommunication Systems, 2018, 67(4):539-552.

[29] Sundaresan S, Doss R, Piramuthu S, et al. Secure tag search in RFID systems using mobile readers[J]. IEEE Transactions on Dependable and Secure Computing, 2014, 12(2):230-242.

[30] Xie S, Liang W, Xu J, et al. A novel bidirectional RFID identity authentication protocol[C]// Proc of 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2018:301-307.

[31] Sarma S E, Weis S A, Engels D W. RFID systems and security and privacy implications[C]// Proc of International Workshop on Cryptographic Hardware and Embedded Systems, 2002:454-469.

[32] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost radio frequency identification systems [C]// Proc of the 1st International Conference on Security in Pervasive Computing, 2004:201-212.

[33] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID [C]// Proc of 2004 Symposium on Cryptography and Information Security, 2004:719-724.

[34] Molnar D, Wagner D. Privacy and security in library RFID: Issues, practices, and architectures[C]// Proc of the 11th ACM Conference on Computer and Communications Security, 2004:210-219.

[35] Gope P, Hwang T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system[J]. Computers & Security, 2015, 55:271-280.

[36] Tan X, Dong M, Wu C, et al. An energy-efficient ECC processor of UHF RFID tag for banknote anti-counterfeiting [J]. IEEE Access, 2016, 5:3044-3054.

[37] Sundaresan S, Doss R, Piramuthu S, et al. A secure search protocol for low cost passive RFID tags[J]. Computer Networks, 2017, 122:70-82.

[38] Liu B, Yang B, Su X. An improved two-way security authentication protocol for RFID system[J]. Information, 2018, 9(4):86-99.

[39] Hosseinzadeh M, Lansky J, Rahmani A M, et al. A new strong adversary model for RFID authentication protocols [J]. IEEE Access, 2020, 8:125029-125045.

[40] Wang B, Ma M. A server independent authentication scheme for RFID systems[J]. IEEE Transactions on Industrial Informatics, 2012, 8(3):689-696.

[41] Mansoor K, Ghani A, Chaudhry S A, et al. Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography[J]. Sensors, 2019, 19(21):47-52.

[42] Golle P, Jakobsson M, Juels A, et al. Universal re-encryption for mixnets[C]// Proc of Cryptographers' Track at the RSA Conference, 2004:163-178.

[43] Alamr A A, Kausar F, Kim J, et al. A secure ECC-based RFID mutual authentication protocol for internet of things [J]. The Journal of Supercomputing, 2018, 74(9):4281-

4294.

[44] Qian Y,Zeng P,Shen Z,et al.A lightweight path authentication protocol for RFID-based supply chains[C]// Proc of the 17th IEEE International Conference on Trust,Security and Privacy in Computing and Communications/the 12th IEEE International Conference on Big Data Science and Engineering,2018:1297-1302.

[45] Singh A K,Patro B D K.Elliptic curve signcryption based security protocol for RFID[J].KSII Transactions on Internet and Information Systems,2020,14(1):344-365.

[46] Sun H,Su C,Chen S.A high security RFID system authentication protocol design base on cloud computer[J].Wireless Personal Communications,2018,102(2):1255-1267.

[47] Tu Y J,Kapoor G,Piramuthu S.On group owner-ship delegate protocol for RFID systems[J].Information Systems Frontiers,2021,24(5):1577-1584.

[48] Xie S,Zhang F,Cheng R.Security enhanced RFID authentication protocols for healthcare environment[J].Wireless Personal Communications,2021,117(1):71-86.

[49] Zhao Z.A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem[J].Journal of Medical Systems,2014,38(5):1-7.

[50] Zhang X,Li L,Wu Y,et al.An ECDLP-based randomized key RFID authentication protocol[C]// Proc of 2011 International Conference on Network Computing and Information Security,2011:146-149.

[51] Liao Y P,Hsiao C M.A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol[J].Ad Hoc Networks,2014,18:133-146.

[52] Dinarvand N,Barati H.An efficient and secure RFID authentication protocol using elliptic curve cryptography[J].Wireless Networks,2019,25(1):415-428.

[53] Chien H Y.Elliptic curve cryptography-based RFID authentication resisting active tracking[J].Wireless Personal Communications,2017,94(4):2925-2936.

[54] Pakniat N,Eslami Z.Cryptanalysis and improvement of a group RFID authentication protocol[J].Wireless Networks,2020,26(5):3363-3372.

[55] Liu Y,Sun Q,Wang Y,et al.Efficient group authentication in RFID using secret sharing scheme[J].Cluster Computing,2019,22(4):8605-8611.

[56] Su J,Sheng Z,Leung V C M,et al.Energy efficient tag identification algorithms for RFID:Survey,motivation and new design[J].IEEE Wireless Communications,2019,26(3):118-124.

[57] Su J,Sheng Z,Liu A X,et al.A group-based binary splitting algorithm for UHF RFID anti-collision systems[J].IEEE Transactions on Communications,2019,68(2):998-1012.

[58] Su J,Sheng Z,Xie L,et al.Fast splitting-based tag identification algorithm for anti-collision in UHF RFID system[J].IEEE Transactions on Communications,2018,67(3):2527-2538.

[59] Mbacke A A,Mitton N,Rivano H.A survey of RFID readers anticollision protocols[J].IEEE Journal of Radio Frequency Identification,2018,2(1):38-48.

[60] Rahman F, Ahamed S I.Efficient detection of counterfeit products in large-scale RFID systems using batch authentication protocols[J].Personal and Ubiquitous Computing,2014,18(1):177-188.

[61] Yue K Q,Sun L L,Qin Y,et al.Design of anti-collision integrated security mechanism based on chaotic sequence in UHF RFID system[J].China Communication,2014,11:137-147.

[62] Li Peng,Zheng Tian-tian,Xu He,et al.RFID security authentication protocol based on blockchain technology[J].Netinfo Security,2021,21(5):1-11.(in Chinese)

[63] Sidorov M,Ong M,Sridharan R,et al.Ultralight-weight mutual authentication RFID protocol for blockchain enabled supply chains[J].IEEE Access,2019,19(7):7273-7285.

[64] Jangirala S, Das A, Vasilakos A.Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment[J].IEEE Transactions on Industrial Informatics,2019,16(11):7081-7093.

附中文参考文献:

[2] 周永彬,冯登国.RFID安全协议的设计与分析[J].计算机学报,2006,29(4):4581-4589.

[7] 汪亚,魏国珩,魏巍.面向RFID应用的轻量级加密算法分类模型研究[J].计算机与数字工程,2017,45(6):1150-1155.

[8] 汪亚,魏国珩.适用于RFID的轻量级密码算法研究综述[J].计算机应用与软件,2017,34(1):9-14.

[62] 李鹏,郑田甜,徐鹤,等.基于区块链技术的RFID安全认证协议[J].信息网络安全,2021,21(5):1-11.

作者简介:

寇广岳(1992-),男,河南许昌人,硕士生,助理工程师,研究方向为物联网安全。**E-mail**:632126332@qq.com

KOU Guang-yue, born in 1992, MS candidate, assistant engineer, his research interest includes Internet of Things security.

魏国珩(1977-),男,湖北武穴人,硕士,副教授,研究方向为物联网安全、通信安全和密码工程。**E-mail**:1784269050@qq.com

WEI Guo-heng, born in 1977, MS, associate professor, his research interests include Internet of Things security, communication security, and cryptography engineering.