轻工学报® 2018 年 1 月 第 33 卷 第 1 期
JOURNAL OF LIGHT INDUSTRY Vol. 33 No. 1 Jan. 2018

引用格式:甘勇,王凯,贺蕾. 带 TTP 权重的多所有者 RFID 标签所有权动态转换协议[J]. 轻工学报,2018,33(1):72 – 78.
中图分类号:TP393.04 **文献标识码**:A
DOI:10.3969/j.issn.2096 – 1553.2018.01.009
文章编号:2096 – 1553(2018)01 – 0072 – 07

带 TTP 权重的多所有者 RFID 标签所有权动态转换协议

RFID tag dynamic ownership transfer protocol of multi-owner with TTP weight

甘勇,王凯,贺蕾
GAN Yong, WANG Kai, HE Lei

郑州轻工业学院 计算机与通信工程学院,河南 郑州 450002
College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, *China*

关键词:
所有权转换;多所有者;可信第三方;拉格朗日插值多项式算法;秘密共享

Key words:
ownership transfer; multi-owner; trusted third party (TTP); Lagrange polynomial interpolation algorithm; secret sharing

摘要:针对目前 RFID 标签所有权转换协议大多数不具备原所有者无关性和存在安全隐私问题的现状,基于拉格朗日多项式插值算法提出了一种带可信第三方(TTP)权重的多所有者 RFID 标签所有权动态转换协议. 该协议中,新所有者通过购买的方式,从原所有者那里获得原始子密钥和权重,协议分别通过恢复原始密钥和 TTP 来验证原所有者和新所有者的合法性,并且利用秘密共享方案根据新所有者的权重来分发子密钥. 仿真分析结果表明,该协议可明显提高所有权转换的安全性,其计算量和耗时均在可接受的范围之内,适用于低成本标签.

收稿日期:2017 – 10 – 25
基金项目:国家自然科学基金项目 (61572445);河南省高等学校重点科研基金项目(16A520075)

作者简介:甘勇(1965—),男,湖南省株州市人,郑州轻工业学院教授,博士,主要研究方向为分布式计算机系统、计算机网络、信息安全.

Abstract: As most ownership transfer protocols of RFID tags were subject to no independence of the original owner and security privacy issues, the RFID tags ownership dynamic transfer protocol of multi-owner with trusted third party (TTP) weights was proposed based on Lagrange polynomial interpolation algorithm. In the protocol, the new owner would obtain the original subkey and weight from the original owner in the way of purchasing, the legality of the original owner and the new owner were verified by recovering the original key and TTP, and the subkey was distributed according to the weight of the new owner by using the secrete sharing scheme. The simulation result showed that the protocol significantly improved the security of ownership transfer, and the calculation quantity and time-consuming were within the acceptable scope, which was applicable to the low cost tag.

0 引言

随着物联网技术的飞速发展,RFID(radio frequency identification)作为一种通过电子磁场自动识别目标的技术,在供应链管理、零售、安防和交通等物联网领域得到了广泛的应用,但随之也出现了新的安全和隐私问题[1]. 由于 RFID 标签成本低,存储容量和计算能力都非常有限,传统的安全技术不能直接应用在标签上,当所有权转换发生变化时,所有者隐私和 RFID 安全无法得到保证[2]. 当涉及多个 RFID 系统协调工作时,不仅要求原所有者把某些共享信息发送给新所有者,同时还要保证新所有者不能得到其机密信息,且原所有者也不可以再继续访问该标签[3]. RFID 系统本身的安全和隐私问题已经制约了其发展.

目前,国内外学者对 RFID 标签所有权转换协议进行了大量研究. 文献[4]最早针对标签的所有权转换问题,设计了基于密钥树的假名协议,通过给 RFID 标签提供一个假名来保护用户隐私信息,并基于该协议提出了两种方法来实现标签的所有权转换,但是新所有者无法安全获得标签的控制权,并没有实现所有权的完全转换. 文献[5]基于是否带有可信第三方(TTP)提出了两种不同的协议,但这两种协议也仅仅涉及密钥交换,需要结合其他的安全认证协议来实现所有权的转换. 文献[6]通过对已经提出的协议和 RFID 系统安全性的分析,设计了一个可以实现所有权完全转换的双向认证协议,但该方案要求标签具有较高的计算能力. 文献[7]中协议通信过程采用轻量级运算,密钥由通信双方协商并动态更新,但该协议不能抵抗去同步化攻击,不具备原所有者无关性. 文献[8]提出了一种基于 SQUASH 方案的轻量级所有权转移协议,但该协议中存在不安全的因素,例如不能很好地抵御去同步化攻击. 文献[9]论述了文献[8]协议存在的安全漏洞,并提出了改进的轻量级所有权转换协议,弥补了文献[8]协议的安全漏洞缺陷,但仍然存在新的安全漏洞和成本花销问题. 文献[10]针对文献[9]中存在的安全漏洞和成本问题,提出了一种基于密钥共享的超轻量级 RFID 标签所有权转换协议,但是该协议并不能有效保护标签信息的后向安全.

以上分析表明,现已存在的所有权转换协议主要存在两个问题:一是不具备原所有者无关性,即原所有者没有完全地将标签的所有权转移给新所有者;二是拥有标签不同份额即权重不同的多个所有者进行 RFID 标签所有权转换时的安全隐私问题,并没有得到完美的解决. 鉴于此,本文拟基于拉格朗日多项式插值算法设计一个带 TTP 的多所有者标签所有权动态转换协议,在不同权重的多个所有者之间转换标签的所有权,以期提高所有权转换的安全性.

1　协议描述

1.1　主要思想

不同权重状态下带 TTP 的多所有者标签所有权动态转换协议的核心思想是使用秘密共享门限方案管理密钥,即在 (t,n) 门限秘密共享方案中,密钥分发者首先把密钥分为 n 份,分配给 n 个参与者. 当其他新的实体通过购买方式成为标签新的所有者,并且从原所有者处获得权重和原始子密钥时,必须恢复初始密钥,验证标签和所有者的合法性. 但是,只有当参与恢复密钥的所有者权重之和等于或大于 t 时,才可根据拉格朗日公式获取共享密钥:

$$f(0) = \sum_{i=1}^{t} y_i \left\{ \prod_{1 \leqslant j \leqslant i, i \neq j} \frac{(0 - x_i)}{(x_i - x_j)} \right\}$$

同理,新所有者和标签也必须通过验证. 最后,新密钥将通过秘密共享方案,分成数个子密钥,新所有者将根据其权重,获得相应的子密钥.

1.2　协议初始化

设 $P = \{P_1, P_2, \cdots\cdots, P_n\}$ 为标签的 n 个原所有者,W_i 是原所有者 P_i 所对应的权重,$Q = \{Q_1, Q_2, \cdots\cdots, Q_m\}$ 为标签的 m 个新所有者,W_{mi} 表示新所有者 Q_i 的相应权重值(在 m 的边界上),W_{ii} 是新所有者 Q_i 从原所有者 P_i 处购买的权重,TID 是标签的唯一标识,S 表示标签与原所有者通信的原密钥,$S_{ij}(1 \leqslant j \leqslant W_i)$ 表示具有不同权重的原所有者的子密钥,S_{new} 表示标签与新所有者通信的新密钥,$S_{mij}(1 \leqslant j \leqslant W_{mi})$ 表示具有不同权重的新所有者根据权重得到的不同数量的子密钥,PID 表示原所有者的唯一身份标识,QID 表示新所有者的唯一身份标识,ID_{TTP} 为可信第三方的唯一身份标识,K 代表标签和可信第三方共享的密钥,而 a,b 为变量 a 和 b 的串联,$a \oplus b$ 为变量 a 和 b 的异或,$H(x)$ 为对变量 x 求其 Hash 值.

1.3　协议执行过程

1.3.1　所有权出售过程　假设标签具有 P_1,P_2,P_3 3 个原所有者,其对应的权重比例分别是 1,2,3,并且新所有者与原所有者之间的通信信道是安全的. 原所有者出售全部权重份额,RFID 标签的所有者将完全改变,具体的出售过程如图 1 所示.

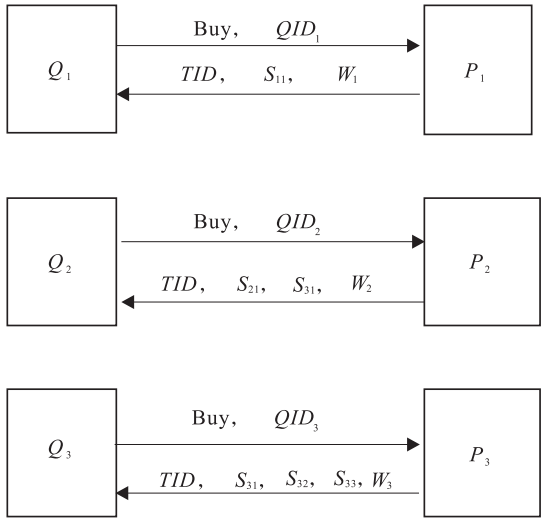

图 1　原所有者所有权出售过程

Fig. 1　The process of purchasing shares from original owners

由图 1 可见,当一个新所有者想从原所有者那里购买权重份额时,新所有者会发送一个购买请求和它自己的身份标识;当原所有者同意出售自己的权重份额时,它将发送标签的唯一身份标识 TID 和自己的子密钥及所占有的权重给新所有者.

1.3.2　原所有者认证过程　当 RFID 标签的原所有者完全改变时,需要及时更新密钥. 因此,原所有者首先需要通过恢复原密钥 S 来完成与标签的相互认证,以防止来自攻击者的假冒攻击,使原所有者与标签之间的正常通信被破坏. 具体的认证过程如图 2 所示,其主要步骤如下.

步骤 1　原所有者 P_1 向标签 Tag 发送所有

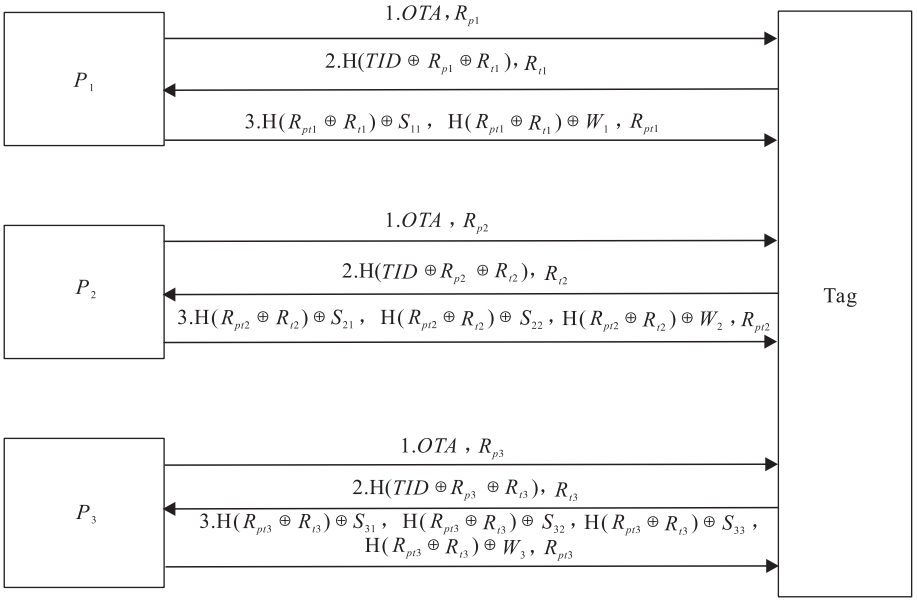

图 2　原所有者和标签认证过程

Fig. 2　The process of mutual authentication between the old owner and the tag

权转换许可 OTA,并生成随机数 R_{p1},将 R_{p1} 和 OTA 同时发送给标签.

步骤 2　标签从 P_1 接收到 OTA 之后,它将生成随机数 R_{t1} 并且计算 $M = \mathrm{H}(TID \oplus R_{p1} \oplus R_{t1})$,将 M 和 R_{t1} 同时发送给原所有者 P_1.

步骤 3　当所有者 P_1 接收到来自标签的消息时,使用存储在后端数据库中的 TID'',R_{t1} 和 R_{p1} 来计算结果. 如果有 $\mathrm{H}(TID'' \oplus R_{p1} \oplus R_{t1}) = M$,则标签通过认证,然后后端数据库生成随机数 R_{pt1},所有者 P_1 将向标签发送 $\mathrm{H}(R_{pt1} \oplus R_{t1}) \oplus S_{11}$,$\mathrm{H}(R_{pt1} \oplus R_{t1}) \oplus W_1$ 和 R_{pt1} 给标签 Tag.

步骤 4　标签 Tag 收到原所有者发送的消息后,判断参与恢复密钥的原所有者权重之和是否大于或等于要求的阈值,若满足,标签根据拉格朗日算法恢复密钥 S',此时用标签的原密钥 S 与拉格朗日算法恢复的密钥 S' 进行比较,若存在 $S = S'$,则说明原所有者合法,此时标签与原所有者之间完成了双向验证,且恢复了标签的原密钥 S.

原所有者标签的认证过程类似,仅以 P_1 为例进行阐述.

1.3.3　所有权转换过程　当标签的多个原所有者出售其权重给其他多个新实体时,该新实体就成为 RFID 标签新的所有者. 不仅原所有者需要与标签完成双向认证,新所有者也需要与标签完成双向认证以防攻击者攻击. 此时需要在 TTP 的参与下进行双向认证过程,以防止有攻击者伪装成合法的新所有者向标签发送信息,并确保实现原所有者无关性. 当多个新所有者认证合法时,标签将更新密钥,并把该密钥分割成多份,根据新所有者的权重分发新的子密钥. 具体所有权转换流程如图 3 所示,以 Q_1 为例进行阐述,其主要步骤如下.

步骤 1　新所有者 Q_1 向标签发送所有权转换申请 OTR,并生成随机数 R_{q1} 同时发送给标签.

步骤 2　当标签接收到来自 Q_1 的请求消息后,它将产生一个随机数 R_{nt1},并计算 $M = \mathrm{H}(TID \oplus R_{q1} \oplus R_{nt1})$,将 M 和 R_{nt1} 同时发送给新所有者 Q_1.

步骤 3　新所有者 Q_1 接收到标签发来的消息后,计算 $M' = \mathrm{H}(TID \oplus R_{q1} \oplus R_{nt1})$. 如果

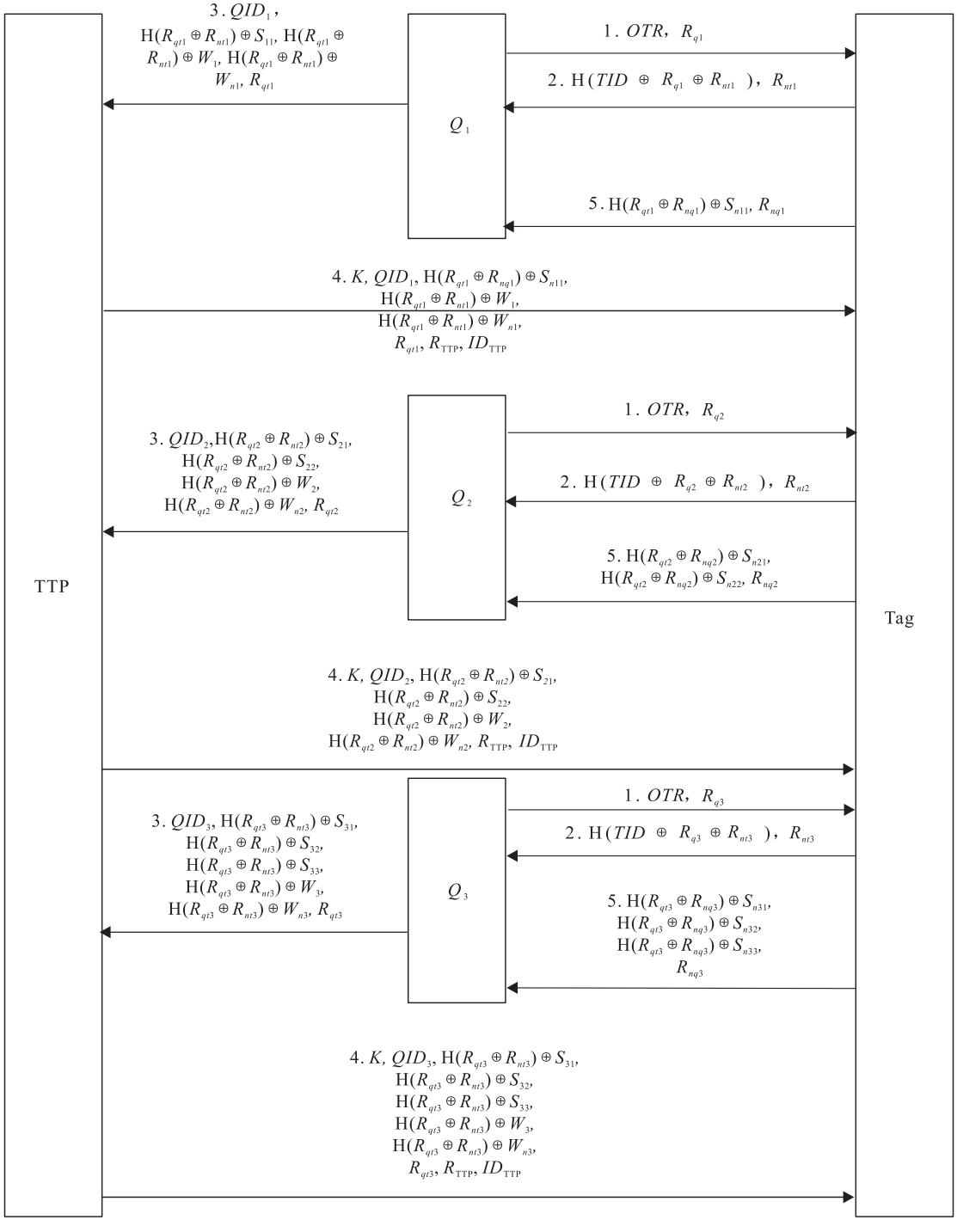

图 3　所有权转换过程

Fig. 3　The process of RFID tag ownership transfer

存在 $M' = M$,则说明标签是合法的,并通过该认证;然后后端数据库生成随机数 R_{qt1},新所有者 Q_1 将把 QID_1,$H(R_{qt1} \oplus R_{nt1}) \oplus S_{11}$,$H(R_{qt1} \oplus R_{nt1}) \oplus W_1$,$H(R_{qt1} \oplus R_{nt1}) \oplus W_{n1}$ 和 R_{qt1} 发送给 TTP.

步骤 4　TTP 接收到新所有者 Q_1 的通信消息后,核查该消息的正确性:若不正确,则认为新所有者没有获得对标签的控制所有权,协议停止;若正确,则认为新所有者获得了对标签的控制所有权,原所有者同意将控制所有权转

交给新所有者. TTP 生成随机数 R_{TTP},并发送 $K, QID_1, \mathrm{H}(R_{qt1} \oplus R_{nt1}) \oplus S_{11}, \mathrm{H}(R_{qt1} \oplus R_{nt1}) \oplus W_1, \mathrm{H}(R_{qt1} \oplus R_{nt1}) \oplus W_{n1}, R_{qt1}, R_{\mathrm{TTP}}$ 和 ID_{TTP} 给标签.

步骤 5 当标签收到 TTP 发来的通讯信息后,检查这个信息是否新鲜且正确:如果不正确,则停止协议;如果正确,则认为新所有者获得了原所有者对标签的所有权,标签将先更新密钥 S_{new},再将该密钥根据权重值分割成新的子密钥 $S_{n11}, S_{n21}, S_{n22}, S_{n31}, S_{n32}$ 和 S_{n33},然后生成随机数 R_{nq1}, R_{nq2} 和 R_{nq3},再分别通过 Hash 函数加密的子密钥发送给多个新的所有者.

2 协议安全性分析

RFID 标签存在的安全和隐私问题,是其尚未被广泛应用的主要原因之一. 在所有权转换过程中,需要满足以下要求: 1)原所有者不可以继续操作标签,以保护标签所有权转换后新所有者的安全隐私,即具备原所有者无关性; 2)当新所有者获得标签的所有权后,不能查看以前的数据,以保护原所有者的安全隐私,即保护标签信息的前向安全; 3)确保在所有权转换过程中能够抵抗假冒攻击、重放攻击、跟踪攻击等. 笔者将从上述几个方面分析和验证本文协议.

2.1 前后向安全

当有新实体成为新所有者时,该协议能及时地更新标签密钥,以确保原所有者不能对标签进行任何操作,即具备了原所有者无关性,新所有者获得标签的所有信息以实现 RFID 标签所有权的完全转换;确保新所有者知道标签的部分子密钥,而不知道原所有者与标签的通信密钥,不能获得标签之前的所有信息. 总之,该方案同时保证了前向和后向安全性.

2.2 假冒攻击

如果有攻击者伪装成合法的新所有者向标签发送消息时,标签需验证发送者的身份,由于新所有者的身份标识 QID 是唯一的,所以攻击者的攻击无效. 这表明该协议对于假冒攻击是安全可靠的.

2.3 重放攻击

当标签收到原所有者发送的 OTA 和 R_{p1} 认证消息后,就会对该消息进行响应. 攻击者也能获得该消息,然后重复地将消息发送给合法的原所有者以进行重放攻击. 但是由于原所有者发送的通信消息和标签每次的响应消息都会生成不同的随机数,因此重复发送相同的消息不能通过认证. 这表明该协议可以抵抗重放攻击.

2.4 跟踪攻击

当伪装成合法的新所有者的攻击者向标签发送 OTR 和 R_{q1} 时,它将从标签处获得响应信息,然后通过分析该信息以跟踪标签. 但是标签与所有者之间的每次认证会话通信中,都将生成新的随机数 R_{nt1},并且 Hash 函数是单向的,因此攻击者无法区分该响应信息来自于哪个标签区域. 这表明该协议可以抵抗跟踪攻击,具有不可跟踪性.

3 协议计算性能分析

在 CPU 为 3.60 GHz,存储器为 4 GB 的 Linux 系统环境中,获取标签在执行本文协议和现有的其他同类协议时所消耗的时间并进行比较,结果如图 4 所示. 从图 4 可以看出,与其他同类协议相比,本文所提出的所有权转移协议中标签的计算耗时较短,适用于低成本标签.

4 结语

本文基于拉格朗日多项式插值算法,提出了带有 TTP 权重的多所有者 RFID 标签所有权转换协议. 该协议通过原所有者与标签之间的双向认证、在可信第三方参与下的新所有者与标签之间的双向认证,保证原所有者与新所有

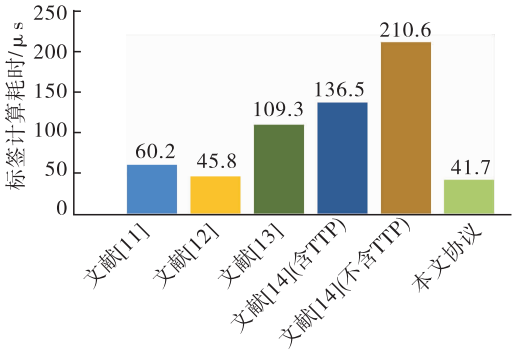

图 4　本文协议与同类协议的标签计算耗时对比

Fig. 4　Comparison of computation time cost by tag among the proposed protocol and the similar protocols

者的合法性;之后标签更新密钥,再将新密钥分割成多份子密钥,新所有者根据获得的权重值得到相应数量的子密钥份数. 对该协议进行安全性分析和仿真实验性能分析,结果表明该协议能抵抗转换过程中的多种攻击,同时标签耗时较短,适用于低成本标签.

参考文献:

[1] 张帆,孙璇,马建峰,等. 供应链环境下通用可组合安全的 RFID 通信协议[J]. 计算机学报,2008,31(10):1754.

[2] 周永彬,冯登国. RFID 安全协议的设计和分析[J]. 计算机学报,2006,29(4):581.

[3] 邵婧,陈越,常振华. RFID 标签所有权转换模式及协议设计[J]. 计算机工程,2009,15:143.

[4] MOLNAR D, SOPPERA A, WAGNER D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags[J]. Lecture Notes in Computer Science, 2005, 3897(2):276.

[5] SAITO J, IMAMOTO K, SAKURAI K. Reassignment scheme of an RFID tag's key for owner transfer[C]// Embedded and Ubiquitous Computing—EUC 2005 Workshops. Heidelberg: Springer, 2005:1303.

[6] LIM C H, KWON T. Strong and robust RFID authentication enabling perfect ownership transfer [C] // Information and Communications Security. Heidelberg: Springer, 2006:1.

[7] 甘勇,李天豹,许允倩. 轻量级 RFID 标签所有权匿名安全转换协议的研究[J]. 郑州轻工业学院学报(自然科学版),2015,30(2):52.

[8] 金永明,孙惠平,关志,等. RFID 标签所有权转移协议研究[J]. 计算机研究与发展,2011,48(8):1400.

[9] 沈金伟,凌捷. 一种改进的超轻量级 RFID 所有权转移协议[J]. 计算机科学,2014,41(12):125.

[10] 苏庆,李倩,张俊源,等. 基于共享密钥的超轻量 RFID 标签所有权转移协议[J/OL]. 计算机工程与应用:1 - 6. [2017 - 02 - 27]. http://kns.cnki.net/kcms/detail/11.2127.TP.20170227.1544.042.html.

[11] YOON E J, YOO K Y. Two security problems of RFID security method with ownership transfer [C] // 2008 IFIP International Conference on Network and Parallel Computing. Piscataway: IEEE, 2008:68.

[12] JAPPINEN P, HAMALAINEN H. Enhanced RFID security method with ownership transfer [C] // 2008 International Conference on Computational Intelligence and Security. Piscataway: IEEE, 2008, 2:382.

[13] ZHOU W, YOON E J, PIRAMUTHU S. Varying levels of RFID tag ownership in supply chains [C] // On the Move to Meaningful Internet Systems: OTM 2011 Workshops. Heidelberg: Springer, 2011:228.

[14] KAPOOR G, PIRAMUTHU S. Single RFID tag ownership transfer protocols[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2012, 42(2):164.