信息与控制　2016 年　第 45 卷　第 6 期：677 ~ 683

DOI：10.13976/j.cnki.xk.2016.0677　　文章编号：1002 - 0411(2016) - 06 - 0677 - 07

一种 RFID 标签所有权完全转移协议

邓春红[1]，左开中[2]，潘　涛[1]

1. 安徽机电职业技术学院，安徽 芜湖　241002；2. 安徽师范大学，安徽 芜湖　241002

基金项目：国家自然科学基金资助项目(61300170)；安徽省自然科学基金资助项目(1308085MF88)；安徽省级物联网实践基地项目(2013sjjd070)；安徽省质量工程通信技术专业改革试点项目(2015zy148)；安徽省高校学科拔尖人才学术资助重点项目(gxbjZD2016098)

通信作者：邓春红，ahjddch@126.com　收稿/录用/修回：2015 - 12 - 28/2016 - 04 - 18/2016 - 06 - 02

摘要

针对射频识别(RFID)标签所有权不能完全转移及系统安全性问题，提出一种 RFID 标签所有权完全转移安全协议. 该协议通过引入原所有者与新所有者间交易关系及身份比对保证标签所有权转移给合法身份的新所有者，利用密钥二次同步更新保证 RFID 标签所有权完全转移. 为了确保标签和阅读器认证不被恶意干扰，采用双向认证保证 RFID 系统通信安全. 形式化证明及分析结果表明，该协议满足标签所有权完全转移要求，可抵御多种攻击，实际应用价值高.

关键词

射频识别
所有权完全转移
安全协议
双向认证
密钥更新

中图分类号：TP309

文献标识码：A

Complete Ownership Transfer Protocol for RFID Tag

DENG Chunhong[1], ZUO Kaizhong[2], PAN Tao[1]

1. *Anhui Technical College of Mechanical and Electrical Engineering*, *Wuhu* 241002, *China*;
2. *Anhui Normal University*, *Wuhu* 241002, *China*

Abstract

As RFID (Radio Frequency IDentification) system tag ownership cannot transfer completely and displays security problems, we propose a novel complete ownership transfer security protocol. Transaction relationship and identity comparison between the current and new owners is introduced to ensure that tag ownership is transferred to the legal new owners, and a key secondary synchronization update is used to ensure a complete ownership transfer of the RFID tag. In order to avoid malicious interference between the reader and the tag during the authenticate process, the new protocol adopts mutual authentication to protect RFID communication security. Formal proof and analysis results show that the proposed protocol not only can satisfy the requirements of complete ownership transfer, but also can defeat possible malicious attacks, which makes it more applicable.

Keywords

RFID (Radio Frequency IDentification);
complete ownership transfer;
security protocol;
mutual authentication;
key updating

1　引言

无线射频识别技术(Radio Frequency IDentification, RFID)是一种非接触式自动识别技术，利用无线广播信号对目标物体识别、追踪和定位，在零售业、智能交通、物流管理等领域有着广泛的应用. 在实际应用中处于生命期内的 RFID 标签所有权会不断转移. 例如，某商品初始被厂商嵌入 RFID 标签，出厂后出售给批发商，接着卖给零售商，最终被消费者购买. 此后，消费者可能还会出售或者赠予其他用户，RFID 标签所有权在各环节不断转移. RFID 标签所有权转移是指原所有者把标签上的信息转交给新所有者，新所有者在接收后能实现对标签所有权控制. 其实质是一旦 RFID 标签所有权发生转移，原所有者则不再拥有标签控制权，不能获取新所有者标签信息；而新所有者不能通过标签获取原所有者信息，保证标签所有权完全转移[1].

RFID 系统一般由标签、阅读器和后台数据库组成，通信模型中，阅读器和标签间的无线广播传输使通信存在安全隐患[2-3]，如何解决电子标签的安全隐私问题是 RFID 研究中的一个热点[4-5]. RFID 标签所有权转移过程中有多个阅读器与同一标签通信，保证无线通信中标签隐私安全前提下还应要求原所有者与新所有者均不能通过标签获取对方信息，安全与隐私问题更为重要[6]. 因此，设计安全的 RFID 标签所有权完全转移协议具有重要的现实意义.

2 相关工作

近年来，RFID 标签所有权转移问题引起研究者广泛重视. 2005 年 Molnar 等基于 RFID 系统框架解决了标签所有权转移问题[7-8]. 方案核心思想是利用密钥树的假名协议保证用户信息安全，通过第三方可信中心为原所有者与新所有者授权标签假名完成所有权转移. 由于其本质是限时授权，因此 RFID 标签所有权未能完全转移. 此外，协议引入第三方可信中心，实际应用有一定限制.

2006 年，Osaka 等分析 RFID 系统安全需求后基于哈希函数与对称密码算法提出一种安全高效的 RFID 所有权转移协议[9]. 该协议分为标签信息写入、认证和所有权转移三个阶段，通过更新密钥保证新所有者与原所有者隐私安全. 由于所有权转移阶段中新所有者未对原所有者发送的信息进行验证，导致密钥更新不同步，所有权不能完全转移，同时易受拒绝服务和主动攻击类型中的中间人攻击.

2008 年，Song 提出一种不需第三方参与的 RFID 所有权转移协议[10]. 该协议包括所有权转移、密钥更新和授权恢复三个子协议，要求新所有者服务器获取所有权后及时更新标签密钥保证隐私安全，同时协议具有授权恢复功能，实际应用价值高. 然而所有者之间通信过程中均为验证对方身份，攻击者易通过重放信息获取标签所有权.

2011 年，Chen 等提出一种基于 EPC C1G2 标准 RFID 标签所有权转移协议[11]. 该协议包括注册、所有权转移询问、相互认证和所有权转移四个阶段，利用数字签名保证转移双方身份不可抵赖性，但未分析重放攻击可能性. 协议相互认证阶段未考虑恶劣环境下标签信息无法发送给阅读器导致密钥更新不同步，标签所有权不能完全转移. 2013 年，Chen 等又提出了一种基于 EPC C1G2 标准的安全所有权转移协议[12]，涉及 PRNG(pseudo-random number generator)和 CRC(cyclic redundancy check)运算，但该协议易受拒绝服务攻击和被动攻击中监听信道攻击. 此外，未考虑原所有者冒充新所有者情况，标签所有权不能很好转移.

2014 年，Gaith 等基于 RFID 闭环系统提出一种新的标签所有权转移协议[13]. 该协议基于时间戳和共享密钥利用哈希函数保证隐私安全，可以保证前向安全，能抵御重放攻击和拒绝服务攻击. 但要求标签和阅读器集成时间精准同步模块，实现难度大，密钥更新异步导致标签所有权不能完全转移. 此后，Niu 等提出一种超轻量级 RFID 所有权可转移相互认证协议[14]. 该协议所有权转移阶段，协议通过可信第三方(TTP)保证新所有者与标签密钥同步. 由于未考虑可信第三方对新所有者身份验证，原所有者易通过恶意手段再次获取标签所有权.

2015 年，Gan 等提出一种新型 RFID 标签所有权转移协议[15]. 标签接收信息后均对发送方身份进行验证，确保非法用户无法实施欺骗攻击. 但由于新所有者是基于原所有者密钥数据解密获取所有权转移后的新密钥，因此原所有者可监听信道截获标签数据解密得到新密钥，标签所有权不能很好转移.

因此，目前 RFID 所有权转移协议大都存在标签所有权不能完全转移和系统安全性问题，少数协议实现了标签所有权转移，但均假定在理想环境下，实际应用价值低.

3 本文协议

3.1 主要思想

本文针对现有 RFID 所有权转移协议中标签所有权不能完全转移及系统安全性问题，提出一种 RFID 标签所有权完全转移协议. 该协议主要思想是通过引入原所有者与新所有者交易关系及身份比对保证标签所有权转移给合法身份的新所有者，利用密钥二次同步更新确保所有权完全转移，考虑到 RFID 系统无线通信，本文协议采用双向认证确保标签与阅读器通信安全.

协议初始，制造商预处理将 $E_{\boldsymbol{K}_t}(ID)$ 写入标签，CO、NO 和 T 共享哈希函数；CO 和 T 共享标签对称密钥 $\boldsymbol{K}_t$ 及伪随机数生成器 PRNG，同时拥有 NO 公钥 $P_{\text{K-NO}}$；NO 拥有 CO 公钥 $P_{\text{K-CO}}$. 此外，CO 在协议执行前能够确定与 NO 交易关系 s；CO 和 NO 能确定本次交易标签，即明确标签身份 $E_{\boldsymbol{K}_t}(ID)$，这符合实际要求. 表 1 给出了本文有关记号定义.

表 1 记号定义

Fig.1 Notation description

记号	定义
CO	原所有者(current owner)
NO	新所有者(new owner)
T	进行所有权转移的标签
ID	标签唯一身份标识符
ID_{CO}	CO 唯一身份标识符
ID_{NO}	NO 唯一身份标识符
s	CO 与 NO 间交易关系
$\boldsymbol{K}_t$	标签对称密钥
$P_{\text{K-CO}}$，$S_{\text{K-CO}}$	CO 的公钥 $P_{\text{K-CO}}$ 和私钥 $S_{\text{K-CO}}$
$P_{\text{K-CO}}$，$S_{\text{K-CO}}$	NO 的公钥 $P_{\text{K-CO}}$ 和私钥 $S_{\text{K-CO}}$
$h(\,)$	单向哈希函数，$h:\{0,1\}^*\rightarrow\{0,1\}^l$
PRNG()	伪随机数生成器
$\xi_a(b)$	私钥 a 对信息 b 的签名
$E_{k_1}(m)$	公钥 k_1 对信息 m 加密
$D_{k_2}(m)$	私钥 k_2 对信息 m 解密
$\oplus$	异或运算
$\triangleq$	是否等于

3.2 协议描述

本文协议由 3 个阶段构成，分别为认证阶段、所有权转移询问阶段和所有权完全转移阶段，具体执行过程如下.

3.2.1 认证阶段

原所有者在所有权转移前拥有标签控制权，对标签身份合法性进行认证，如图 1 所示. 具体认证过程如下：

步骤 1 CO 生成随机数 R_1，计算并向 T 发送 Query 请求、R_1、$h(R_1)\oplus s$ 和 $ID_{\text{CO}}\oplus\boldsymbol{K}_t$.

步骤 2 T 获取交易关系 s，向 CO 发送响应数据 M_1 和 M_2，同时首次更新密钥.

（a）T 利用接收到 R_1 基于共享哈希函数计算 $u_1 = h(R_1)$，获取并存储 $s = u_1 \oplus h(R_1) \oplus s$，同时利用标签密钥 $\boldsymbol{K}_t$ 获取并存储 $ID_{CO} = ID_{CO} \oplus \boldsymbol{K}_t \oplus \boldsymbol{K}_t$.

（b）计算 $M_1 = h(R_1) \oplus \boldsymbol{K}_t$，$M_2 = R_1 \oplus E_{\boldsymbol{K}_t}(ID)$.

（c）向 CO 发送数据 M_1 和 M_2，更新密钥 $\boldsymbol{K}_t' = \mathrm{PRNG}(\boldsymbol{K}_t)$.

步骤 3　CO 完成对 T 身份合法性认证，更新拥有的标签密钥并保存原密钥.

（a）CO 利用标签共享密钥 $\boldsymbol{K}_t$ 计算 $u_2 = h(R_1') = M_1 \oplus \boldsymbol{K}_t$，比较数据 $u_2 \triangleq h(R_1)$，保证数据的新鲜性.

（b）利用随机数 R_1 计算 $u_3 = E_{\boldsymbol{K}_t}(ID') = M_2 \oplus R_1$，查找数据库匹配标签数据 $u_3 \triangleq E_{\boldsymbol{K}_t}(ID)$，对标签 *ID* 认证.

（c）计算并发送 $h(\mathrm{PRNG}(\boldsymbol{K}_t) \oplus s)$，更新 $\boldsymbol{K}_t' = \mathrm{PRNG}(\boldsymbol{K}_t)$，保存原密钥 $\boldsymbol{K}_t$.

步骤 4　T 利用自己数据 s 及 $\boldsymbol{K}_t'$计算并比较 $h(\boldsymbol{K}_t' \oplus s) \triangleq h(\mathrm{PRNG}(\boldsymbol{K}_t) \oplus s)$，若相同认证成功，否则 T 还原自身 $\boldsymbol{K}_t'$为 $\boldsymbol{K}_t$.

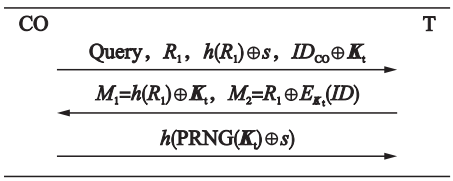

图 1　认证阶段

Fig.1　Authentication process

3.2.2　所有权转移询问阶段

原所有者向新所有者发送信息询问是否接收标签所有权的转移，如图 2 所示. 具体执行过程如下：

步骤 1　CO 利用私钥 $S_{K\text{-}CO}$ 对 ID_{CO} 签名得 $\xi_{S_{K\text{-}CO}}(ID_{CO})$，利用 NO 公钥加密并发送 $E_{P_{K\text{-}NO}}(\boldsymbol{K}_t', s, ID, ID_{CO}, \xi_{S_{K\text{-}CO}}(ID_{CO}))$.

步骤 2　NO 解密数据获取 ID，判断是否为本次希望交易的标签，并向 CO 响应接收或拒绝信号.

（a）NO 利用自己私钥 $S_{K\text{-}NO}$ 解密获取明文 $\boldsymbol{K}_t'$、s、*ID*、ID_{CO} 和 $\xi_{S_{K\text{-}CO}}(ID_{CO})$，利用 CO 公钥结合 $\xi_{S_{K\text{-}CO}}(ID_{CO})$ 对 ID_{CO} 进行验证，确定信息来自合法身份 CO.

（b）判断 $E_{\boldsymbol{K}_t}(ID)$ 是否为本次交易标签 $E_{\boldsymbol{K}_t}(ID)$. 若是，NO 同意接收该标签所有权的转移，存储 $\boldsymbol{K}_t'$和 s，计算并发送 $E_{P_{K\text{-}CO}}(\xi_{S_{K\text{-}NO}}(\boldsymbol{K}_t' \oplus ID_{CO}), \boldsymbol{K}_t' \oplus ID_{CO})$ 及 Accept 响应信号，继续步骤 3；若否，*ID* 非法，NO 判断该标签不是本次交易标签，拒绝接收，发 Refuse 响应信号，协议终止.

步骤 3　CO 利用自己私钥解密获取 $\xi_{S_{K\text{-}NO}}(\boldsymbol{K}_t' \oplus ID_{CO})$ 和 $\boldsymbol{K}_t' \oplus ID_{CO}$，验证 $\boldsymbol{K}_t' \oplus ID_{CO}$ 确定该信息为对自己的回复，利用 NO 公钥结合 $\xi_{S_{K\text{-}NO}}(\boldsymbol{K}_t' \oplus ID_{CO})$ 对 $\boldsymbol{K}_t' \oplus ID_{CO}$ 进行验证，确定信息来自合法身份 NO.

3.2.3　所有权完全转移阶段

原所有者一旦将标签所有权转移给新所有者，不能继续访问标签隐私信息，失去标签控制权，同时标签相关状态与新所有者保持同步，保证所有权完全转移，具体执行过程如图 3 所示.

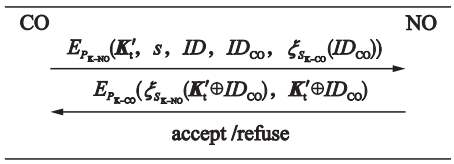

图 2　所有权转移询问阶段

Fig.2　Ownership transfer querying process

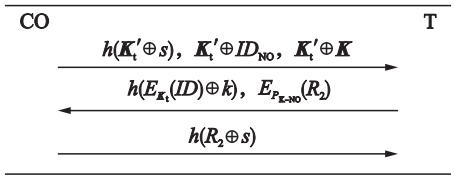

图 3　所有权完全转移阶段

Fig.3　Complete transfer process of the ownership

步骤 1　NO 生成随机数 $\boldsymbol{K}$，计算并向 T 发送 $h(\boldsymbol{K}_t' \oplus s)$、$\boldsymbol{K}_t' \oplus ID_{NO}$ 和 $\boldsymbol{K}_t' \oplus \boldsymbol{K}$.

步骤 2　T 完成对 NO 认证，随后标签密钥二次更新.

（a）T 利用存储数据计算 $u_4 = h(\boldsymbol{K}_t' \oplus s)$，然后与收到数据比较 $u_4 \triangleq h(\boldsymbol{K}_t' \oplus s)$，判断信息是否来自合法身份 NO. 若不同，NO 身份非法或 CO 拥有的共享标签密钥与 T 更新不同步，转认证阶段重新执行.

（b）利用标签密钥计算 $ID_{NO} = \boldsymbol{K}_t' \oplus \boldsymbol{K}_t' \oplus ID_{NO}$，$\boldsymbol{K} = \boldsymbol{K}_t' \oplus \boldsymbol{K}_t' \oplus \boldsymbol{K}$，比较 $ID_{NO} \triangleq ID_{CO}$，防止 CO 以不正当手段再次获取标签所有权.

（c）生成随机数 R_2，计算并发送 $h(E_{\boldsymbol{K}_t}(ID) \oplus K)$ 和 $E_{P_{K\text{-}NO}}(R_2)$，标签密钥二次更新 $\boldsymbol{K}_t'' = \boldsymbol{K} \oplus R_2$.

步骤 3　NO 扫描数据库寻找匹配 $E_{\boldsymbol{K}_t}(ID)$，对标签进行认证，更新自己拥有的标签密钥，同时保存原密钥.

（a）NO 利用自己拥有的数据计算 $u_5 = h(E_{\boldsymbol{K}_t}(ID) \oplus \boldsymbol{K})$，然后与收到数据比较，对标签身份信息 $E_{\boldsymbol{K}_t}(ID)$ 进行验证：若相等，继续（步骤 3（b））；否则认证终止.

（b）基于 NO 私钥利用公钥算法解密获取 $R_2 = D_{S_{K\text{-}CO}}(E_{P_{K\text{-}NO}}(R_2))$，计算并发送 $h(R_2 \oplus s)$，更新标签密钥 $\boldsymbol{K}_t'' = \boldsymbol{K} \oplus R_2$，保存原密钥 $\boldsymbol{K}_t'$.

步骤 4　T 利用自己数据 s 及 R_2 计算 $h(R_2 \oplus s)$并与接收数据比较：若相同，认证成功；否则认证终止，T 还原自身 $\boldsymbol{K}_t''$为 $\boldsymbol{K}_t'$.

4　基于 SVO 逻辑形式化分析

SVO（syverson-van oorschot）逻辑是在优化和总结 BAN（burrows，abadi-needham）、GNY（gong，needham-yahalom）、AT（abadi tuttle）、VO（van oorschot）四种逻辑的基础上提出的，是目前分析认证协议最常用的形式化方法之一[16-18]. 通信模型中，协议主体每执行一次操作，都可依据 SVO 语法、公理和推理规则更新自身现有状态，通过主体最终拥有的安全目标公式等状态信息验证协议安全.

首先给出本文用到的 SVO 逻辑语法、公理和规则：

（1）$P \overset{K+}{\longleftrightarrow} Q = (P \overset{K}{\longleftrightarrow} Q) \wedge (P \ni \boldsymbol{K}) \wedge (Q \mid \approx (Q \ni \boldsymbol{K}))$.

(2) 信任公理 A_0: $(P\mid\equiv\phi\wedge P\mid\equiv\Psi)\equiv(P\mid\equiv\phi\wedge\Psi)$.

(3) 信任公理 A_1: $P\mid\equiv\varphi\wedge P\mid\equiv(\varphi\supset\Psi)\supset P\mid\equiv\Psi$.

(4) 密钥协商公理 A_5: $PK_\delta(P,\boldsymbol{K}_p)\wedge PK_\delta(Q,\boldsymbol{K}_q)\supset P\overset{\boldsymbol{K}_{pq}}{\longleftrightarrow}Q$.

(5) 消息新鲜性公理 A_{18}: $\#(X_i)\supset\#(F(X_1,\cdots,X_n))$.

(6) 临时值验证公理 A_{19}: $(\#(X)\wedge P\mid\sim X)\supset P\mid\approx X$.

(7) NEC (necessitation) 规则: 由 $\mid-\varphi$ 可以推导出 $\mid-P\mid\equiv\varphi$.

其中, P 和 Q 为通信主体, $\boldsymbol{K}$ 是 P 和 Q 间"好的"共享密钥, X 是消息, ϕ 和 Ψ 是公式. $PK_\delta(P,\boldsymbol{K}_p)$ 说明 $\boldsymbol{K}_p$ 为主体 P 的公开协商密钥, $\boldsymbol{K}_q$ 为主体 Q 的公开协商密钥, $\boldsymbol{K}_{pq}$ 是基于 $\boldsymbol{K}_p$ 和 $\boldsymbol{K}_q$ 形成的、P 和 Q 间"好的"共享密钥, $F(X_i)$ 表示含有参数 X_i 的函数, $\mid-\varphi$ 表示 φ 是定理, $\mid\approx$、$\ni$、$\mid\equiv$、$\supset$、$\equiv$、#、$\mid\sim$、$\lhd$、$\mid-$ 符号分别表示最新发送过、属于、相信、蕴涵、等价于、新鲜、发送过、接收到、元语言.

4.1 协议初始化假设集

给出本文协议关于节点 CO 的初始化假设集, 如下:

(1) $\mathrm{CO}\mid\equiv\mathrm{T}\mid\sim\boldsymbol{K}_t$

(2) $\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim\boldsymbol{K}_t\supset\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t))$

(3) $\mathrm{CO}\mid\equiv\mathrm{CO}\lhd\boldsymbol{K}_t$

(4) $\mathrm{CO}\mid\equiv((\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge\mathrm{CO}\lhd\boldsymbol{K}_t)\supset PK_\delta(\mathrm{T},\boldsymbol{K}_t))$

(5) $\mathrm{CO}\mid\equiv PK_\delta(\mathrm{CO},\boldsymbol{K}_t)$

(6) $\mathrm{CO}\mid\equiv\#(R_1,\boldsymbol{K}_t)$

(7) $\mathrm{CO}\mid\equiv\mathrm{T}\mid\sim(\mathrm{T}\ni\boldsymbol{K}'_t)$

4.2 协议实现目标

协议认证阶段, 要实现节点 CO 对 T 的身份认证, 并相信更新后的密钥是与节点 T 共享的新鲜密钥, 其 SVO 逻辑表示为 G_1 和 G_2:

G_1: $\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}'_t+}{\longleftrightarrow}\mathrm{T}$

G_2: $\mathrm{CO}\mid\equiv\#\boldsymbol{K}'_t$

4.3 验证过程

证明 利用初始化假设集、SVO 公理和规则对协议进行形式化推理分析.

推理 1 $\mathrm{CO}\mid\equiv\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)$.

对假设(1)和假设(2), 应用信任公理 A_1, 得 $\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim\boldsymbol{K}_t\wedge\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim\boldsymbol{K}_t\supset\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t))\supset\mathrm{CO}\mid\equiv\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)$, 可得推理 1.

推理 2 $\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge\mathrm{CO}\lhd\boldsymbol{K}_t)$.

对推理1和假设(3), 应用信任公理 A_0, 得 $(\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge\mathrm{CO}\mid\equiv\mathrm{CO}\lhd\boldsymbol{K}_t)\equiv(\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t))\wedge(\mathrm{CO}\lhd\boldsymbol{K}_t))$, 可得推理 2.

推理 3 $\mathrm{CO}\mid\equiv PK_\delta(\mathrm{T},\boldsymbol{K}_t)$.

对推理2和假设(4), 应用信任公理 A_1, 得 $\mathrm{CO}\mid\equiv(\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge\mathrm{CO}\lhd\boldsymbol{K}_t)\wedge\mathrm{CO}\mid\equiv((\mathrm{T}\mid\sim PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge(\mathrm{CO}\lhd\boldsymbol{K}_t)\supset PK_\delta(\mathrm{T},\boldsymbol{K}_t))\supset\mathrm{CO}\mid\equiv PK_\delta(\mathrm{T},\boldsymbol{K}_t)$, 可得推理 3.

推理 4 $\mathrm{CO}\mid\equiv(PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))$.

对推理3和假设(5), 应用信任公理 A_0, 得 $(\mathrm{CO}\mid\equiv PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge\mathrm{CO}\mid\equiv PK_\delta(\mathrm{CO},\boldsymbol{K}_t))\equiv(\mathrm{CO}\mid\equiv PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))$, 可得推理 4.

推理 5 $\mathrm{CO}\mid\equiv((PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))\supset\mathrm{CO}\overset{\boldsymbol{K}_t}{\longleftrightarrow}\mathrm{T})$.

基于推理 4, 将密钥协商公理 A_5 实例化, 得 $(PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))\supset\mathrm{CO}\overset{\boldsymbol{K}_t}{\longleftrightarrow}\mathrm{T}$, 应用 NEC 规则可得推理 5.

推理 6 $\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}_t}{\longleftrightarrow}\mathrm{T}$.

对推理4和推理5, 应用信任公理 A_1, 得 $\mathrm{CO}\mid\equiv(PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))\wedge\mathrm{CO}\mid\equiv((PK_\delta(\mathrm{T},\boldsymbol{K}_t)\wedge PK_\delta(\mathrm{CO},\boldsymbol{K}_t))\supset\mathrm{CO}\overset{\boldsymbol{K}_t}{\longleftrightarrow}\mathrm{T})\supset\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}_t}{\longleftrightarrow}\mathrm{T}$, 可得推理 6.

推理 7 $\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}'_t}{\longleftrightarrow}\mathrm{T}$.

通过推理 6 可知, 通信双方在协议执行后均认定密钥 $\boldsymbol{K}_t$ 为公开协商密钥, 由于 CO 与 T 共享 PRNG, 因此可得推理 7.

推理 8 $\mathrm{CO}\mid\equiv\#\boldsymbol{K}'_t$.

将消息新鲜性公理 A_{18} 实例为 $\#(R_1,\boldsymbol{K}_t)\supset\#(F(R_1,\boldsymbol{K}_t))$, 应用 NEC 规则得 $\mathrm{CO}\mid\equiv(\#(R_1,\boldsymbol{K}_t)\supset\#(F(R_1,\boldsymbol{K}_t)))$. 对假设(6), 应用信任公理 A_1 得 $\mathrm{CO}\mid\equiv\#(R_1,\boldsymbol{K}_t)\wedge\mathrm{CO}\mid\equiv(\#(R_1,\boldsymbol{K}_t)\supset\#(F(R_1,\boldsymbol{K}_t)))\supset\mathrm{CO}\mid\equiv\#(F(R_1,\boldsymbol{K}_t))$, 因为 $\boldsymbol{K}'_t=\mathrm{PRNG}(\boldsymbol{K}_t)$, 可得推理 8.

推理 9 $\mathrm{CO}\mid\equiv(\mathrm{T}\mid\approx(\mathrm{T}\ni\boldsymbol{K}'_t))$.

对推理8和假设(7), 应用信任公理 A_0, 得 $(\mathrm{CO}\mid\equiv\#\boldsymbol{K}'_t\wedge\mathrm{CO}\mid\equiv\mathrm{T}\mid\sim(\mathrm{T}\ni\boldsymbol{K}'_t))\equiv(\mathrm{CO}\mid\equiv(\#\boldsymbol{K}'_t\wedge\mathrm{T}\mid\sim(\mathrm{T}\ni\boldsymbol{K}'_t)))$, 将临时值验证公理 A_{19} 实例化为 $(\#\boldsymbol{K}'_t\wedge\mathrm{T}\mid\sim(\mathrm{T}\ni\boldsymbol{K}'_t))\supset\mathrm{T}\mid\approx(\mathrm{T}\ni\boldsymbol{K}'_t)$, 应用 NEC 规则得 $\mathrm{CO}\mid\equiv((\#\boldsymbol{K}'_t\wedge\mathrm{T}\mid\sim(\mathrm{T}\ni\boldsymbol{K}'_t))\supset\mathrm{T}\mid\approx(\mathrm{T}\ni\boldsymbol{K}'_t))$, 最后根据上述公式, 应用信任公理 A_1, 可得推理 9.

推理 10 $\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}'_t+}{\longleftrightarrow}\mathrm{T}$.

对假设(7)、推理7和推理9, 用信任公理 A_0, 得 $(\mathrm{CO}\mid\equiv\mathrm{CO}\ni\boldsymbol{K}'_t)\wedge(\mathrm{CO}\mid\equiv\mathrm{CO}\overset{\boldsymbol{K}'_t}{\longleftrightarrow}\mathrm{T})\wedge(\mathrm{CO}\mid\equiv\mathrm{T}\mid\approx(\mathrm{T}\ni\boldsymbol{K}'_t))\equiv\mathrm{CO}\mid\equiv(\mathrm{CO}\ni\boldsymbol{K}'_t)\wedge(\mathrm{CO}\overset{\boldsymbol{K}'_t}{\longleftrightarrow}\mathrm{T})\wedge(\mathrm{T}\mid\approx(\mathrm{T}\ni\boldsymbol{K}'_t))$, 根据 $\mathrm{CO}\overset{\boldsymbol{K}+}{\longleftrightarrow}\mathrm{T}$ 符号定义, 可得推理 10.

根据推理 8 和推理 10, 得出协议认证阶段最终实现目标. 同理, 对所有权转移询问阶段和所有权完全转移阶段形式化分析, 得出结果: CO 和 NO 及 NO 和 T 各自相信存在适合双方通信的共享、新鲜密钥.

5 协议分析与性能比较

5.1 安全性分析

本文协议中认证阶段和所有权完全转移阶段为无线通信, 采用双向认证确保信息安全; 所有权转移询问阶段利用数字签名技术保证参与方不可抵赖性. 下面对本文协议安全性进行简要分析.

(1) 拒绝服务攻击: 攻击者截获无线通信信息使得协议双方密钥更新不同步, 导致下一轮通信合法标签无法通过认证. 本文协议可抵御拒绝服务攻击, 过程如下:

认证阶段:

① T 首先更新密钥 $\boldsymbol{K}'_t=\mathrm{PRNG}(\boldsymbol{K}_t)$, 接着 CO 完成对 T

认证，更新密钥为 $\boldsymbol{K}_t'$并保存 $\boldsymbol{K}_t$，计算并发送 $h(\mathrm{PRNG}(\boldsymbol{K}_t)\oplus s)$.

② 攻击者监听信道，截获 $h(\mathrm{PRNG}(\boldsymbol{K}_t)\oplus s)$，此后发送伪造数据 $h'(\mathrm{PRNG}(\boldsymbol{K}_t)\oplus s)$.

③ T 验证 $h'(\mathrm{PRNG}(\boldsymbol{K}_t)\oplus s)$不正确，还原 $\boldsymbol{K}_t'$为 $\boldsymbol{K}_t$.

所有权转移询问阶段：

CO 向 NO 发送信息询问是否接收标签所有权的转移，NO 获取标签密钥 $\boldsymbol{K}_t'$. 若 NO 拒绝，协议终止，下次认证阶段中 CO 通过扫描数据库仍能对合法标签进行认证.

所有权完全转移阶段：

① NO 生成随机数 $\boldsymbol{K}$，计算并向 T 发送 $h(\boldsymbol{K}_t'\oplus s)$、$\boldsymbol{K}_t'\oplus ID_{\mathrm{NO}}$和 $\boldsymbol{K}_t'\oplus\boldsymbol{K}$.

② 由于认证阶段失败，密钥 $\boldsymbol{K}_t$ 未更新，T 接收信息后验证 $h(\boldsymbol{K}_t'\oplus s)$不正确，判断 NO 身份非法或密钥 $\boldsymbol{K}_t'$有误，为了保证密钥更新同步，T 默认 CO 拥有的标签密钥与 T 更新不同步，继续执行认证阶段操作，拒绝服务攻击无效.

此外，攻击者还可截获所有权完全转移阶段中 NO 发送给 T 的信息，导致 NO 拥有的标签密钥 $\boldsymbol{K}_t''$与 T 自身密钥 $\boldsymbol{K}_t'$不同步，由于 NO 保存原密钥，下次通信仍能对 T 进行认证. 因此，本文协议有效抵御拒绝服务攻击.

（2）重放攻击：攻击者向标签发送请求，通过无线信道截获标签响应信息，继而发送给阅读器以获取合法标签身份. 本文协议认证阶段，CO 收到攻击者信息后利用标签密钥 $\boldsymbol{K}_t$ 计算 $u_2 = h(R_1') = M_1 \oplus \boldsymbol{K}_t$，比较数据 $u_2 \triangleq h(R_1)$，确保数据新鲜性，由于随机数 R_1 每次都不相同，重放攻击失败；所有权完全转移阶段，NO 收到信息后扫描数据库文件计算 $h(E_{\boldsymbol{K}_t}(ID)\oplus\boldsymbol{K})$是否正确，由于随机数 $\boldsymbol{K}$ 临时生成每次都不同，因此本文协议可抵御重放攻击.

（3）被动攻击和主动攻击：攻击者监听信道窃取信息实施被动攻击，本文协议 3 个阶段数据加密涉及公钥加密算法、哈希函数及异或运算，首先攻击者不拥有私钥无法获取明文数据，其次利用哈希函数单向性、强无碰撞性保证数据安全，最后异或运算增加了破译难度，攻击者截获 0/1，均有两种原像可能 1⊕1 或 0⊕0 = 0，0⊕1 或 1⊕0 = 1，当数据位数足够大，穷举法成为不可能，因此本文协议可抵御被动攻击. 攻击者中断信号或篡改信息实施主动攻击，认证阶段与所有权完全转移阶段采用双向认证技术，执行协议双方需要对各自身份进行认证，并且利用随机数变化检验信息是否被篡改以保证新鲜性；所有权转移询问阶段，协议引入签名技术，接收方可迅速判断数据是否被恶意修改，同时也保证交易双方身份不可抵赖性，本文协议可抵御主动攻击.

5.2　所有权完全转移分析

本文协议中，CO 执行协议前与 T 共享标签密钥 $\boldsymbol{K}_t$，拥有标签所有权，经过认证阶段，T 从 CO 获取交易关系 s，双方同时更新密钥 $\boldsymbol{K}_t' = \mathrm{PRNG}(\boldsymbol{K}_t)$；经过所有权转移询问阶段，NO 从 CO 获取交易关系 s 及密钥 $\boldsymbol{K}_t'$，此时 CO 与 NO 均拥有标签控制权；所有权完全转移阶段中，NO 生成随机数 $\boldsymbol{K}$，基于密钥 $\boldsymbol{K}_t'$加密数据并向 T 发送 $h(\boldsymbol{K}_t'\oplus s)$、$\boldsymbol{K}_t'\oplus\boldsymbol{K}$，T 基于密钥 $\boldsymbol{K}_t'$利用 s 完成对 NO 认证，保证所有权转移给具有合法身份 NO，此后双方拥有的标签密钥二次同步更新为 $\boldsymbol{K}_t'' = \boldsymbol{K}\oplus R_2$，其中 R_2 为 T 的随机数. 整个协议执行过程中，CO 拥有标签密钥 $\boldsymbol{K}_t$ 和 $\boldsymbol{K}_t'$，NO 拥有标签密钥 $\boldsymbol{K}_t'$和 $\boldsymbol{K}_t''$. 标签所有权转移完成后，NO 拥有标签控制权，与 T 共享密钥 $\boldsymbol{K}_t''$，由于不拥有密钥 $\boldsymbol{K}_t$，无法获取 CO 与 T 通信信息；而 $\boldsymbol{K}$ 和 R_2 对 CO 未知，CO 不拥有密钥 $\boldsymbol{K}_t''$，无法获取 NO 与 T 通信信息，不再拥有标签控制权，实现标签所有权转移.

此外，现有 RFID 标签所有权转移协议大都不要求标签对发送方身份进行认证，导致原所有者冒充新所有者再次获取标签控制权. 本文协议中，所有权完全转移阶段步骤 2 要求 T 对 NO 身份认证. T 接收信息后首先基于密钥 $\boldsymbol{K}_t'$利用 s 验证 $h(\boldsymbol{K}_t'\oplus s)$，判断信息是否来自合法身份；其次计算 $ID_{\mathrm{NO}} = \boldsymbol{K}_t'\oplus\boldsymbol{K}_t'\oplus ID_{\mathrm{NO}}$，比较 $ID_{\mathrm{NO}} \triangleq ID_{\mathrm{CO}}$，防止 CO 冒充 NO 再次获取标签所有权，因此，本文协议可实现标签所有权完全转移.

5.3　性能比较

综上所述，将本文协议性能分别与现有典型协议进行比较. 表 2 给出了协议间安全性能比较，其中“✓”表示协议具备相应的安全性，“×”表示不具备相应的安全性；表 3 给出了协议间关键性指标比较，包括标签所有权能否完全转移、标签计算量、标签存储需求及协议无线交互次数，其中 T_x 是异或运算代价，T_h 是哈希函数运算代价，T_{CRC}是 CRC 函数的运算代价，T_q 是位移运算代价，m 是第 i 个标签 T_i 的密钥长度.

表 2　安全性能比较

Fig.2　Comparison of safety performance

协议	拒绝服务攻击	重放攻击	主动攻击	被动攻击
文[9]	×	✓	×	✓
文[10]	✓	×	✓	✓
文[11]	✓	×	✓	✓
文[12]	×	✓	✓	×
文[15]	✓	✓	✓	×
本文	✓	✓	✓	✓

表 3　关键性指标比较

Fig.3　Comparison of key indicators

协议	所有权完全转移	标签计算量	标签存储需求	无线交互次数
文[9]	否	$2T_x + T_h$	m	3
文[10]	否	$6T_h + 9T_x + 4T_q$	m	3
文[11]	否	$7T_x + 3T_{\mathrm{PRNG}} + 3T_{\mathrm{CRC}}$	m	3
文[12]	否	$2T_x + 3T_{\mathrm{CRC}} + 3T_{\mathrm{PRNG}}$	$2m$	4
文[15]	否	$5T_h + 2T_x$	$3m$	5
本文	是	$10T_x + 5T_h + T_{\mathrm{PRNG}}$	m	6

从表 2 和表 3 可以看出，相比现有典型标签所有权转移协议，本文协议安全性能好，可抵御多种攻击，满足了标签所有权完全转移需求. 尽管在标签计算量和无线交互次数方面略高于其它协议，但由于用于所有权交换的标签

的商品一般价值比较高，因此标签的成本高一点也是符合实际的[19].

5.4 实验分析

通过实验平台验证本文协议的性能，实验过程中使用具体数据模拟了本文协议的具体流程，限于篇幅本文以协议认证阶段为例. 一般 RFID 系统标签存储能力在 2 048 bit，可划分为 256 B，每个字节对应一个唯一性地址，序号从 0 到 255. 标签内部存储能力分配如图 4 所示.

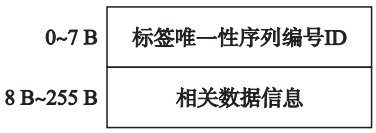

图 4 标签存储能力分配图

Fig.4 Allocation of tag storage capacity

现利用模拟数值实例方式展现本文协议的认证过程. 为了突出认证合理性与简单化. 做如下假设：

（1）标签 CO、NO 与 T 的唯一性序列编号 IDC、IDN 和 IDT 分别是[0x00, 0x00, 0x00, 0x01, 0x01, 0x01, 0x01, 0x32]、[0x00, 0x00, 0x00, 0x01, 0x01, 0x01, 0x01, 0x33]、[0x00, 0x00, 0x00, 0x01, 0x01, 0x01, 0x01, 0x34].

（2）对称密钥 K_t = [0x45, 0xA6, 0xD4, 0x55, 0x11, 0xF2, 0xD3, 0xlE].

（3）CO 生成随机数 R_1，R_1 对应的二进制是[0x5A, 0x31, 0xF0, 0x08].

基于模拟数据，协议认证流程如图 5 所示.

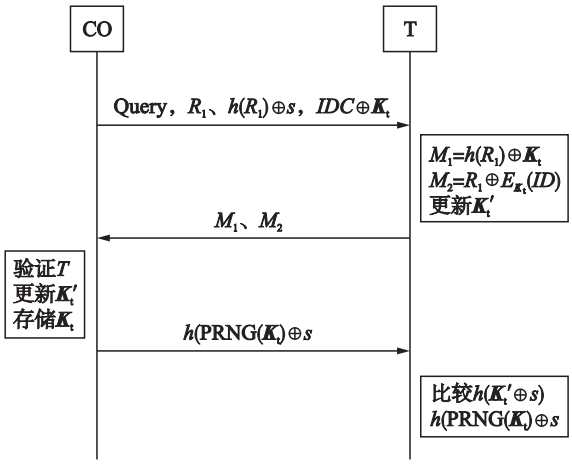

图 5 协议认证流程

Fig.5 Protocol authentication process

运用本文协议的算法流程及数据模拟运算，最终认证成功.

此外，通过实验对比其它类型协议的标签工作场景，建立了采用不同协议之间的标签模拟场景图，如图 6 所示，图中星形标签为正在运行的一个攻击者.

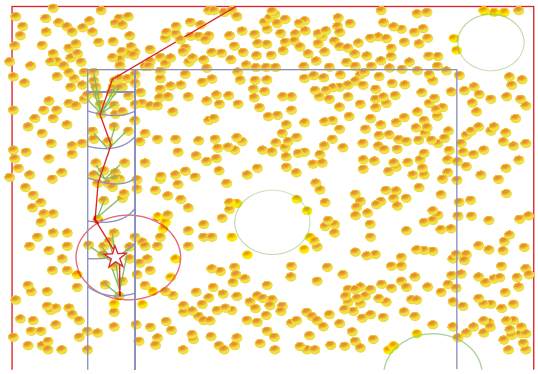

图 6 多协议标签性能比较场景模拟图

Fig.6 Simulation diagram of multi-protocol tags performance comparison

通过多轮的拒绝服务攻击、假冒攻击和重放攻击等方式攻击，针对各类协议的攻击成功率如图 7 所示. 从图 7 可以看出，对于相同的错误接受率，本文协议与之前的协议相比需要更少的轮数就可以达到.

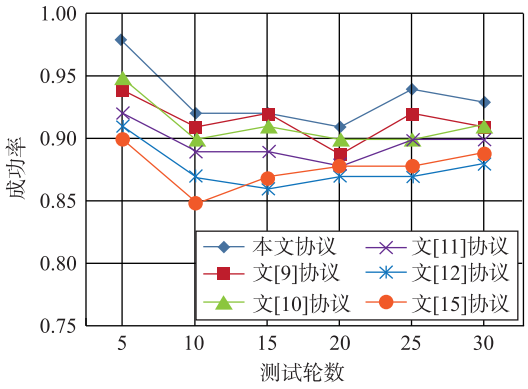

图 7 攻击成功率对比图

Fig.7 Comparison chart of attack success rates

6 结束语

本文协议通过引入原所有者与新所有者间交易关系及身份比对，利用密钥二次同步更新保证了所有权完全转移，采用双向认证保证 RFID 系统通信安全. 最后对该协议的正确性给予了形式化证明，并通过实验数据验证了协议的安全性和有效性. 未来的工作在于研究 RFID 群组标签环境下所有权转移问题，设计出高效、低成本的协议.

参考文献

[1] 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)：1400－1405.
Jin Y M，Sun H P，Guan Z，et al. Ownership transfer protocol for RFID tag[J]. Journal of Computer Research and Development，2011，48(8)：1400－1405.

[2] 刘雅辉，张铁赢，靳小龙，等. 大数据时代的个人隐私保护[J]. 计算机研究与发展，2015，52(1)：221－228.

Liu Y H, Zhang T Y, Jin X L, et al. Personal privacy protection in the era of big data[J]. Journal of Computer Research and Development, 2015, 52(1): 221 – 228.

[3] 潘涛，左开中，郭良敏，等. 基于异或运算的低成本 RFID 双向认证协议[J]. 计算机工程，2012，38(9)：278 – 281.
Pan T, Zuo K Z, Guo L M, et al. Mutual authentication protocol based on XOR operation for low-cost RFID[J]. Computer Engineering, 2012, 38(9): 278 – 281.

[4] 谢润，许春香，陈文杰，等. 一种具有阅读器匿名功能的射频识别认证协议[J]. 电子与信息学报，2015，37(5)：1241 – 1247.
Xie R, Xu C X, Chen W J, et al. An RFID authentication protocol anonymous against readers[J]. Journal of Electronics and Information Technology, 2015, 37(5): 1241 – 1247.

[5] 张辉，侯朝焕，王东辉. 一种基于部分 ID 的新型 RFID 安全隐私相互认证协议[J]. 电子与信息学报，2009，31(4)：853 – 856.
Zhang H, Hou C H, Wang D H. A new security and privacy on RFID mutual authentication protocol based on partial ID[J]. Journal of Electronics and Information Technology, 2009, 31(4): 853 – 856.

[6] 肖锋，周亚建，周景贤，等. 标准模型下可证明安全的 RFID 双向认证协议[J]. 通信学报，2013，34(4)：82 – 87.
Xiao F, Zhou Y J, Zhou J X, et al. Provable secure mutual authen-tication protocol for RFID in the standard model[J]. Journal on Communications, 2013, 34(4): 82 – 87.

[7] David M, Andrea S, David W. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags[M]//Lecture Notes in Computer Science: vol. 3897. Berlin, Germany: Springer-Verlag, 2005: 276 – 290.

[8] Ton V D, Sjouke M, Saša R, et al. Secure ownership and ownership transfer in RFID systems[M]//Lecture Notes in Computer Science: vol. 5789. Berlin, Germany: Springer-Verlag, 2009: 637 – 654.

[9] Kyosuke O, Tsuyoshi T, Kenichi Y, et al. An efficient and secure RFID security method with ownership transfer[C]//Computational Intelligence and Security. Berlin, Germany: Springer-Verlag, 2007: 1090 – 1095.

[10] Boyeon S. RFID tag ownership transfer[C]//Proceedings of the Conference on RFID Security. 2008.

[11] Chin L C, Yeong L L, Chih C C, et al. RFID ownership transfer authorization systems conforming EPCglobal Class-1 Generation-2 standards [J]. International Journal of Network Security, 2011, 13(1): 41 – 48.

[12] Chen C L, Huan Y C, Jiang J R. A secure ownership transfer protocol using EPC global Gen-2 RFID[J]. Telecommunication Systems, 2013, 53(4): 387 – 399.

[13] Ai G K D, Ray B R, Chowdhury M. RFID tag ownership transfer protocol for a closed loop system[C]//IiAi 3rd International Conference on Advanced Applied Informatics. Piscataway, NJ, USA: IEEE, 2014: 575 – 579.

[14] Haifeng N, Jag S, Eyad T. A Gen2v2 compliant RFID authentication and ownership management protocol[C]//39th Annual IEEE Conference on LCN. Piscataway, NJ, USA: IEEE, 2014: 331 – 336.

[15] Yong G, Lei H, Yi F Y. RFID tag ownership transfer protocol with retrospective ability[J]. Cybernetics & Information Technologies, 2015, 14(4): 121 – 130.

[16] Syverson P F, Oorschot P C V. A unified cryptographic protocol logic[R]. Washington: Center for High Assurance Computer System, NRL CHACS Report 5540 – 227, 1996.

[17] 卿斯汉. 安全协议的设计与逻辑分析[J]. 软件学报，2003，14(7)：1301 – 1309.
Qing S H. Design and logical analysis of security protocols[J]. Journal of Software, 2003, 14(7): 1301 – 1309.

[18] 肖茵茵，苏开乐. 电子商务支付协议认证性的 SVO 逻辑验证[J]. 计算机工程与应用，2014，50(8)：6 – 10.
Xiao Y Y, Su K L. Verification of e-commerce payment protocol authentication properties based on SVO logic[J]. Computer Engineering and Applications, 2014, 50(8): 6 – 10.

[19] 陈志德，陈友勤，许力. RFID 标签所有权转换安全协议[J]. 通信学报，2010，31(9A)：202 – 208.
Chen Z D, Chen Y Q, Xu L. RFID tag ownership transfer secure protocol[J]. Journal on Communications, 2010, 31(9A): 202 – 208.

作者简介

邓春红(1970 –)，男，硕士，副教授. 研究领域为网络安全，RFID 技术.

左开中(1974 –)，男，博士，教授，硕士生导师. 研究领域为可信计算，信息安全等.

潘　涛(1986 –)，男，硕士，讲师. 研究领域为无线传感器系统，射频识别技术.