可证明安全的轻量级 RFID 所有权转移协议

陈秀清[①]　曹天杰*[②]　翟靖轩[②]
[①](徐州医科大学医学信息学院　徐州　221008)
[②](中国矿业大学计算机科学与技术学院　徐州　221008)

摘　要：设计安全的无线射频识别协议有助于实现“智慧城市”的规划和构建完善的智慧网络。安全的 RFID 所有权转移协议要求同时具备安全性和隐私性，标签的前向不可追踪性和后向不可追踪性是 RFID 系统实际应用中需要考量的两个重要的隐私性能。针对现有供应链系统中所有权转移协议存在的各种安全隐私问题，该文改进了原有前向不可追踪性定义的错过密钥更新过程的不合理的假设，提出了强前向不可追踪性的概念。提出了一个基于二次剩余定理的轻量级 RFID 所有权转移协议，并使用改进的模型和定义形式化证明了协议的安全性和隐私性。证明结果表明新方案既可以抵御内部读卡器恶意假冒攻击，追踪攻击，标签假冒攻击和异步攻击，又满足强前向不可追踪性和后向不可追踪性等隐私性能；新协议在实现低成本和高效率认证的基础上，比其他协议安全性和隐私性更好。

关键词：无线射频识别；所有权转移协议；强前向不可追踪性；后向不可追踪性；二次剩余定理
中图分类号：TP391.45　　**文献标识码**：A　　**文章编号**：1009-5896(2016)08-2091-08
DOI: 10.11999/JEIT151049

Provable Secure for the Lightweight RFID Ownership Transfer Protocol

CHEN Xiuqing[①]　CAO Tianjie[②]　ZHAI Jingxuan[②]
[①](*School of Medicine Information*, *Xuzhou Medical University*, *Xuzhou* 221008, *China*)
[②](*College of Computer Science and Technology*, *China University of Mining and Technology*, *Xuzhou* 221008, *China*)

Abstract: In order to implement the “wisdom city” planning and build perfect wisdom network, it is important to design the security Radio Frequency IDentification (RFID) protocol. A secure RFID ownership transfer protocol should be evaluated in terms of the security and privacy properties. In particular, there are two important privacy properties included forward untraceable and backward untraceable in the practical application of RFID system. In order to solve the various security and privacy problems, this paper enhances the unreasonable assumption that the attacker misses the key-update session in the definition of forward untraceable, then proposes the definition of strong forward untraceable. In addition, this paper designs the lightweight RFID ownership transfer protocol based on quadratic residues, and uses the enhanced model and definitions to formal prove the security and privacy properties. Moreover, the proof results not only show that the scheme resists against inner reader malicious im-personation attack, tracing attack, tag impersonation attack and desynchronization attack, but also formally prove that the proposed protocol meets strong forward untraceable and backward untraceable properties. In addition, the analysis results demonstrate that the protocol based on low-cost and high efficiency is superior to other protocols in the security and performance properties.

Key words: Radio Frequency IDentification (RFID); Ownership transfer protocols; Strong forward untraceable; Backward untraceable; Quadratic residues

1　引言

无线射频识别(Radio Frequency IDentification, RFID)技术在带给各行各业的商业应用更多便利和更高效的服务的同时，也将“智慧城市”由想法落实为现实的各种应用，如智能公交系统、智能医疗系统、智能旅游系统等。而智慧城市的全方位处理能力要有很好的现实应用，则需要具备完善的安全和隐私性能的 RFID 安全协议。文献[1–5]都是基于二次剩余定理设计的 RFID 协议。在所有权转移协议中，带有 RFID 标签的物品在其生命周期内的所有权是不断变化的。如果消费者使用物品时出现问

收稿日期：2015-09-17；改回日期：2016-05-13；网络出版：2016-06-24
*通信作者：曹天杰　tjcao@cumt.edu.cn
基金项目：国家自然科学基金(61303263)，江苏省第四期“333高层次人才培养工程”科研项目(BRA2014047)，江苏省“六大人才高峰”科研项目(2014-WLW-023)
Foundation Items: The National Natural Science Foundation of China (61303263), The 333 Project of Jiangsu Province (BRA2014047), The “Six-top-talents” High-level Talent Cultivation Project Research Funds of Jiangsu Province (2014-WLW-023)

题需要将物品交给售后服务部维修人员，此时物品所有权临时转移。所有权转移过程中最重要的就是保证新旧所有者不能利用自己掌握的当前或过往信息对另一方进行跟踪或者获得对方的秘密信息。

列表式和密钥更新式 RFID 协议[6]实现了标签的信息对阅读器的匿名安全性和不可追踪隐私性。最近文献[7]介绍了前向隐私性、后向隐私性和受限后向隐私性的定义。文献[8]给出了不同的前向不可追踪性和后向不可追踪性的定义。在所有权转移协议中，为了保护标签的所有权的隐私性，需要满足所有权转移协议的前向安全隐私和后向安全隐私两种性能。

文献[8]使用Vaudenay模型进行了形式化分析，通过改进模型的预假设，用于形式化证明协议的前向安全隐私和后向安全隐私等性能。文献[9]使用安全证明模型来证明提出的协议满足基本的安全需求，即抵抗内部所有者恶意假冒攻击，随后指出文献[10]中的所有权转移协议存在异步攻击和新旧所有者的密钥泄露的问题。文献[11]也指出文献[10]没有实现新所有者的隐私保护问题。文献[12]给出了所有权转移的模型，证明了所有权者和标签之间的隐私性。文献[5]设计了一种基于二次剩余定理的所有权转移协议，这种协议标签端不需要进行哈希计算，此协议满足 EPC Class-1 Gen-2 标准，并适用于大规模系统应用，但存在内部读卡器恶意假冒攻击。此外，现存的很多所有权转移协议并没有使用文献[8]提出的前向和后向不可追踪性的概念进行形式化分析，导致新所有权转移协议不安全。现有协议[13–18]并没有使用不可追踪模型分析协议的安全性，因此基于不可追踪模型设计了基于二次剩余定理的轻量级所有权转移协议。

本文简要介绍了证明协议安全性和隐私性的安全模型，提出了新的基于二次剩余定理的所有权转移协议，在安全模型下形式化分析新协议的安全性，同时在安全隐私性能和效率性能两方面与其他协议比较，实验结果证明新协议具有更好的安全性和高效性，满足文中提出的安全和性能需求。

2 安全模型

文献[8,13]分别对RFID协议的隐私性能进行了形式化定义，本文基于 Vaudenay 模型[19]进一步改进安全模型，减弱证明中的安全假设，通过改进敌手建模协议运行环境的能力来证明协议的安全性。本文安全模型可以访问以下预言机：CreateTag(ID), DrawTag(dist), Free(vtag), Launch( ), SendReader (m,π), SendTag(m,T), Corrupt(vtag)。根据攻击者的能力，Vaudenay 首次将攻击者依据能否查询 Corrupt(vtag)预言机划分为弱，前向，破坏，强(Weak, Forward, Destructive, Strong)等 4 个能力等级。强攻击者具有访问任何预言机的能力；弱敌手不能对任何标签执行 Corrupt(vtag)操作。同时依据敌手能否查询 Result(π)预言机将敌手能力分为窄(Narrow)和宽(Wide)两种敌手(窄攻击者不能查询 Result 预言机)。依据以上两种不同的分类可分为 8 种不同能力的敌手。

前向和后向不可追踪性能这两种性能和追踪攻击都属于定位隐私(location privacy)的范畴，与内部读卡器恶意攻击的敌手能力的假设条件并不相同。而在定义前向和后向不可追踪性能的概念时，本文假设敌手的能力是窄-强(Narrow-strong)敌手，分别分析第$(i+1)$次会话和第$(i-1)$次会话。虽然 Vaudenay 模型能够很好地分析当前第i次会话，但并不能进行前向和后向不可追踪性能分析。因此文献[8]进一步使用 Vaudenay 模型进行形式化分析文献[20]提出前向和后向不可追踪性能的两个定义，即使用第$(i+2)$次会话分析前向不可追踪性和使用过去第$(i-1)$次会话分析后向不可追踪性，通过改变预假设条件来改进 Vaudenay 的模型中的缺点。这些定义不仅可以分析所有权转移协议的前向和后向不可追踪性能，还可用于分析密钥更新协议。在原有模型中假设敌手是宽攻击者，且错过了密钥的更新过程，这种假设不符合实际攻击环境。因此假设敌手的攻击能力是窄-强攻击者，没有错过密钥的更新过程，可以持续监听协议的运行，并分析第$(i+1)$次会话中标签密钥的安全性，在改进假设条件后提出了一种强前向不可追踪性的定义。

对安全的 RFID 认证协议定义如下：

定义 1 前向不可追踪性 (forward untraceable)。敌手运行第i次会话，即使得到腐化后的第i次会话的标签密钥和会话内容，但是错过第$(i+1)$次密钥更新过程，即使监听到所有者和标签的将来第$(i+2)$次会话内容，也无法推知出第$(i+2)$次的标签密钥和标签输出信息，无法追踪到第$(i+2)$次会话时的标签状态。

定义 2 后向不可追踪性 (backward untraceable)。敌手运行第i次会话，即使得到腐化后的第次i标签密钥，也无法从协议的过去$(i-1)$次会话内容中推知出第$(i-1)$次的标签密钥和标签输出信息，无法追踪到第$(i-1)$次会话时的标签状态。

定义 3　强前向不可追踪性(strong forward untraceable)。敌手运行第 i 次协议，假设敌手得到腐化后的第 i 次的标签密钥和会话内容，再对第 $(i+1)$ 次会话分析，无法推知第 $(i+1)$ 次的标签密钥和标签输出信息。

3　轻量级 RFID 所有权转移协议

新协议中使用的符号和定义如表 1 所列。

表 1 符号和定义

符号	定义
$R_{\text{old}}(R_{\text{new}})$; $T_i(T_{i+1})$	当前(新)读卡器；当前(新)标签
DB; Adv	数据库，敌手
$h()$; $H()$	两个不同的哈希函数
$r_c(r_n)$; TID	当前(新)读卡器的标识；标签标识
K_{TID}	标签和读卡器共享的密钥 $K_{\text{TID}}=v_1\|\|v_2\|\|v_3\|\|\cdots\|\|v_m$
$v_{p+l}(v_p)$	密钥 K_{TID} 中的 $(p+l)^{\text{th}}(p)^{\text{th}}$ 的随机数 $(l=\|p-m\|)$
n_s; n_t; n_{T2}	同一个标签生成的不同的随机数
n; p; q	大整数 n (使用梅森数 2^t-1 表示)，2 个大素数 p, $q(n=pq)$

新所有权转移协议分为闭环系统和开环系统。闭环 RFID 系统的定义是标签位于新所有者与当前所有者可以识别的范围内的系统。本文仅设计适用于移动读卡器的闭环系统的轻量级所有权转移 RFID 协议(Lightweight RFID Ownership Transfer Protocol, LROTP)。LROTP 协议包括初始化阶段和所有权转移阶段。LROTP 协议步骤如下：

(1)初始化阶段：　假设当前所有者(读卡器)与标签之间共享一些密钥信息。读卡器生成两个大素数 p 和 q 并计算 $n=pq$。在该系统中每个有效的标签，所有者与标签共享一个私密密钥 $K_{\text{TID}}(K_{\text{TID}}=v_1||v_2||v_3||\cdots||v_m)$，每个 v_i 都代表一个 n bit 字符串。每个标签都被初始化为 $(h(\text{TID}), K_{\text{TID}}, r_c, r_n)$，旧读卡器储存密钥为 $(h(\text{TID}), K_{\text{TID}}, t, r_c)$，新读卡器存储密钥为 $(h(\text{TID}'), K'_{\text{TID}}, t', r_n)$。

(2)所有权转移阶段：

步骤 1　旧读写器 R_i 加密 n 的信息为 $A=n\oplus r_c$。

步骤 1.1　R_i 传递 A 给新读写器 R_{i+1}。

步骤 1.2　R_{i+1} 发送所有权转移信息 (OT, A) 给标签 T_i。

步骤 2　T_i 接收到 OT 后，计算 $R_t=h(\text{TID})\oplus r_c\oplus n_s\oplus v_p$，$R''_t=R_t^4 \bmod n$，$R_p=\arg\ v_p$，$E=r_n\oplus n_T$，$F=r_c\oplus n_s$。

步骤 2.1　T_i 发送 (R''_t, R_p, E, F) 至新读写器 R_{i+1}。

步骤 2.2　R_{i+1} 转发送 (R''_t, R_p, F) 至 R_i。

步骤 3　R_i 收到标签的信息后，当前读卡器 R_i 使用 n 和 R''_t，解出 R_t 的值，即当前读卡器会解出以 n 为模的 R_t^2 的 R_t 的值。利用 p 和 q，获得 R_t^2 的值。同时通过 F 提取 n_s。敌手分别计算 $R_t\oplus n_s\oplus v_p$ 的值和异或值 $h(\text{TID})\oplus r_c$，最后判断这两个计算的值是否相等。如果不相等，传递的信息验证不通过，停止协议；如果相等，则判断传递的消息是合法标签生成的，当前读卡器计算 $\text{ACK}_S=h(\text{TID})\oplus n_s\oplus v_{p+l}$。然后 R_i 通过安全通道发送 ACK_S 至新读卡器。

步骤 4　新读卡器 R_{i+1} 接收到 ACK_S，并生成大素数 $n'=p'q'$。新读卡器使用密钥 r_n 提取 $n_T=r_n\oplus E$，并计算 $n_T=r_n\oplus E$ 和 $H_1=h(\text{ACK}_S||n'||n_T)$。$R_{i+1}$ 利用 H_1 验证传递数据 (G_1, ACK_S) 的完整性。新读卡器向标签发送信息 (G_1, H_1, ACK_S)。

步骤 5　标签 T_i 接收信息后生成 n_{T2}，从接收的消息 G_1 中提取 n' 的值，并进一步验证标签计算的哈希值 $h(h(\text{TID})\oplus\text{ACK}_S||n'||n_T)$ 和接收的值 H_1 是否相等。如果不相等，则终止协议；如果相等，则标签认为提取的数据 n' 是合法的，随后计算 $x=K_{\text{TID}}\oplus n_{T2}$，$x'=x^2 \bmod n'$，$x''=x^4 \bmod n'$ 模运算和 $C_0=h(x||n)$。验证消息 C_0 用于验证传递数据 x'' 的完整性。标签发送消息 (x'', C_0) 给新读写器 R_{i+1}。

步骤 6　R_{i+1} 接收到标签的 (x'', C_0) 后，首先比较 R_{i+1} 计算的哈希值 $h(x\,||\,n)$ 是否和接收到的 C_0 相等。如果不相等则停止协议；如果相等，则新读卡器会解出以 n' 为模的 x^2 的解 R，并利用以 p' 和 q' 为模，识别 x^2 值。新读卡器生成随机数 r' 和新密钥 K'_{TID}，并计算如下信息：$\text{ACK}_n=K'_{\text{TID}}\oplus h(R)$，$G_2=r'\oplus R$，$C=h(r'||\text{ACK}_n)$，最后更新新标签的密钥为 $h(\text{TID}')=h(K'_{\text{TID}}||R)$ 和 $r_n=r'$。R_{i+1} 发送信息 (G_2, ACK_n, C) 到标签 T_i。

步骤 7　标签接收到信息后，核实 $h(G_2\oplus x'||\text{ACK}_n)=C$ 等式是否成立。若标签验证等式不成立，则停止协议；若等式成立，标签进一步更新密钥 $K'_{\text{TID}}=\text{ACK}_n\oplus h(x')$, $r'=G_2\oplus x'$, $h(\text{TID}')=h(K'_{\text{TID}}||x')$。此时标签和新所有者的密钥保存一致，标签的所有权完成转移。

4　形式化安全分析和性能分析

4.1 隐私性和安全性形式化证明

LROTP 协议基于 Vaudenay 模型建模反映运行

环境和不同攻击能力的敌手的安全模型，分别使用定理 1 和定理 2 形式化证明 LROTP 协议的隐私性，使用定理 3，定理 4 和定理 5 证明 LROTP 协议的安全性。

定理 1 在窄-强敌手攻击能力的安全模型下，LROTP 协议满足强前向不可追踪性能。

证明 假设窄-强敌手执行第 i 次协议，腐化得到标签的密钥和输入输出信息，但是可以监听到第 $(i+1)$次的会话内容，敌手无法推断出$(i+1)$次的标签的密钥和输出信息。观察标签的算法结构，标签端的密钥更新都使用了 x' 更新，可以得出计算标签的密钥更新和输出信息都需要知道 x 的值。因此在敌手计算 x 值的方法上，从以下两种情况考虑(证明过程的流程图见图 1)。

一是敌手利用标签的算法结构中 ${}^{i}x_x = {}^{i}K_{\mathrm{TID}} \oplus {}^{i}n_{T2}$ 正向计算 x 的值。第 i 次会话时，已知敌手腐化了标签的密钥 ${}^{i}K_{\mathrm{TID}}$ 的值，但是标签每次生成的 ${}^{i}n_{T2}$ 的值都不同，因此敌手是无法依据以上公式计算出 ${}^{i}x_x$ 的值。同理敌手在这种情况下运行第 $(i+1)$次会话时，无法计算 ${}^{i+1}x_x$ 的值。

二是敌手利用公式 $x'' = x^4 \bmod n'$ 和监听的第 i 次信息 n' 和 x''，反向求解 ${}^{i}x_x$ 的值。新协议的安全性取决于基于大整数 n' 的素分解问题的难解性。即使敌手已经腐化 ${}^{i}K_{\mathrm{TID}}$ 的值，并且通过不安全通道获得大整数 n' 和 x'' 的值，但是敌手没有能力无法分解 n'，因此无法得到 x' 和 x 的值。同理在第 2 种情况下利用监听到的第$(i+1)$次信息也无法计算 ${}^{i+1}x_x$ 的值。

由上述两种情况分析可知，敌手不可能计算出 ${}^{i}x_x$ 和 ${}^{i+1}x_x$ 的值。在此基础上，分别从以下两个方面分析敌手在第$(i+1)$次会话时，计算目标标签 T_{i+1} 其他密钥更新值和输出信息。

(1)第$(i+1)$次会话时敌手计算目标标签其他密钥更新值： 敌手计算更新的密钥 ${}^{i+1}K_{\mathrm{TID}} = {}^{i}\mathrm{ACK}_n \oplus {}^{i}h(x_x)$，需要窃听 ${}^{i}\mathrm{ACK}_n$ 和 ${}^{i}h(x_x)$，但是因为敌手无法获取 ${}^{i}x_x$ 就无法计算 ${}^{i}h(x_x)$，所以无法推测 ${}^{i+1}K_{\mathrm{TID}}$。同理敌手无法计算出标签更新后密钥(${}^{i+1}r_x$， ${}^{i+1}h(\mathrm{TID}_x)$)。

(2)第$(i+1)$次会话时敌手计算标签 T_{i+1} 的输出信息：敌手无法获 ${}^{i+1}x_x$ 的值，就无法依据公式 $x'' = x^4 \bmod n'$ 计算 T_{i+1} 的输出信息 ${}^{i+1}x_x''$，同时也无法计算出 ${}^{i+1}C_0$，因此无法追踪和识别$(i+1)$次会话的标签 T_{i+1}。

一方面，如果敌手无法计算出 ${}^{i}x_x$，即无法计算第$(i+1)$次的标签密钥$\{ r_c, r_n, h(\mathrm{TID}), K_{\mathrm{TID}} \}$；另一方面，如果敌手无法计算出 ${}^{i+1}x_x$，就无法计算出标签输出 ${}^{i+1}x_x''$。因此敌手是无法区分出 vtag 和 vtag^x，即敌手的强前向可追踪的优势为 0，LROTP 协议满足强前向不可追踪性能。

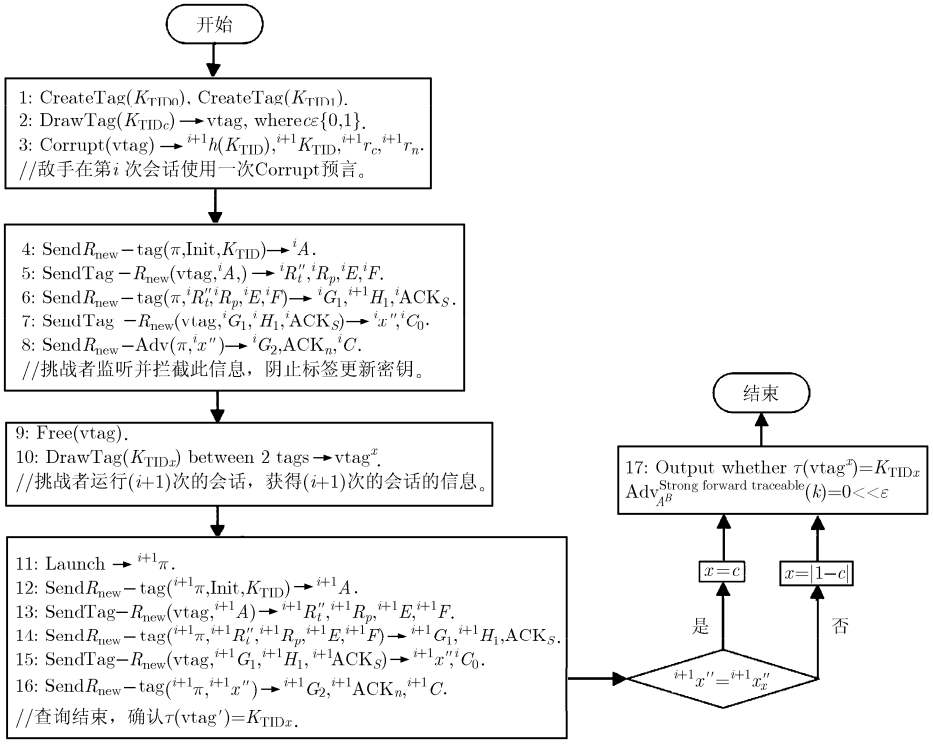

图 1 证明 LROTP 协议满足强前向不可追踪性的算法流程图

大部分协议使用随机数来同步更新密钥，而加密的随机数消息容易被敌手获得，并解出随机数的值。而新的协议使用 x' 更新标签和读卡器密钥。而所有的密钥更新都需要 x' 加密，x' 的安全性决定了更新后密钥的安全性，即协议满足强前向不可追踪性。　　证毕

定理 2　在窄-强敌手攻击能力的安全模型下，LROTP 协议满足后向不可追踪性能。

证明　敌手利用第$(i+1)$次的标签密钥和监听到的信息，也无法计算出第 i 次会话的标签的密钥 $\{r_c, r_n, h(\mathrm{TID}), K_{\mathrm{TID}}\}$，同时也无法推测出第 i 次的标签输出信息 ${}^{i}x_x''$，因此敌手无法比较自身的计算值 ${}^{i}x_x''$ 和监听到的 ${}^{i}x_x''$ 是否相同，从而无法区分出 vtag 和 vtag^x。因此敌手分析标签的后向可追踪性能的优势为 0, LROTP 协议满足后向不可追踪性能，证明过程的流程图见图 2。　　证毕

定理 3　在弱敌手攻击能力的安全模型下，LROTP 协议是抵抗内部读卡器恶意攻击的。

证明　从以下两种情况分析内部读卡器恶意攻击(证明过程的流程图见图 3)。

(1)抵抗新读卡器恶意假冒旧读卡器攻击：　假设旧读卡器没有参与生成消息 ACK_S，新读卡器利用监听攻击的结果，窃听了新读卡器和标签之间的信息，无法利用自己的密钥和已知的信息来计算出旧读卡器的输出的信息 ${}^{i}\mathrm{ACK}_S$，或者是推断出旧读卡器的任何密钥$(h(\mathrm{TID}), K_{\mathrm{TID}}, r_c, t)$，所以新读卡器无法恶意假冒旧读卡器。从以下两方面分析这种情况。一方面，新读卡器计算 ${}^{i}\mathrm{ACK}_S$ 需要知道$(h(\mathrm{TID}), v_{P+l}, n_s)$的值，但是新读卡器不知旧标签的密钥值 $h(\mathrm{TID})$ 和 r_c，并且无法从 ${}^{i}F$ 中得到 n_s 的值，而且 v_{P+l} 的值也是随机的。另一方面，新读卡器无法利用自己的密钥和监听的信息计算出旧读卡器的密钥。例如新读卡器仅分析监听的消息 R_p 和 F 是无法推断出标签的密钥 K_{TID} 和 r_c 的值，因为 R_p 是随机选取的，而 F 中含有随机数 n_s。

(2)抵抗旧读卡器恶意假冒新读卡器攻击：　假设新读卡器没有参与系统并生成任何消息(G_1, H_1)，而旧读卡器利用自己的密钥和已知的信息$({}^{i}R_p, {}^{i}F, {}^{i}\mathrm{ACK}_S)$，可以计算出和新读卡器相同的输出的信息$(G_1, H_1)$和$(G_2, \mathrm{ACK}_n, C)$，或者是推断出新读卡器的密钥。分析以下两种情况：一方面，旧读卡器利用监听攻击获取新读卡器和标签之间的信息，无法推算出新读卡器或是标签的的密钥，经过验证可知标签的信息都是加密并且不能获取任何实体的密钥。另一方面，因为旧读卡器计算 G_1 和 H_1 的值都需要知道 n' 和 n_T 值，但是旧读卡器不能从 E 中提取出标签的生成的随机值 n_T，因此也不能从 G_1 中提取读卡器的密钥 n'。同理旧读卡器也无法计算出只有新读卡器才能产生的信息(G_2, ACK_n, C)，因此旧读卡器无法恶意假冒新读卡器。当且仅当读卡器恶意假冒旧读卡器和假冒新读卡器的优势都为 0 时，LROTP 协议抵抗内部读卡器恶意攻击。　　证毕

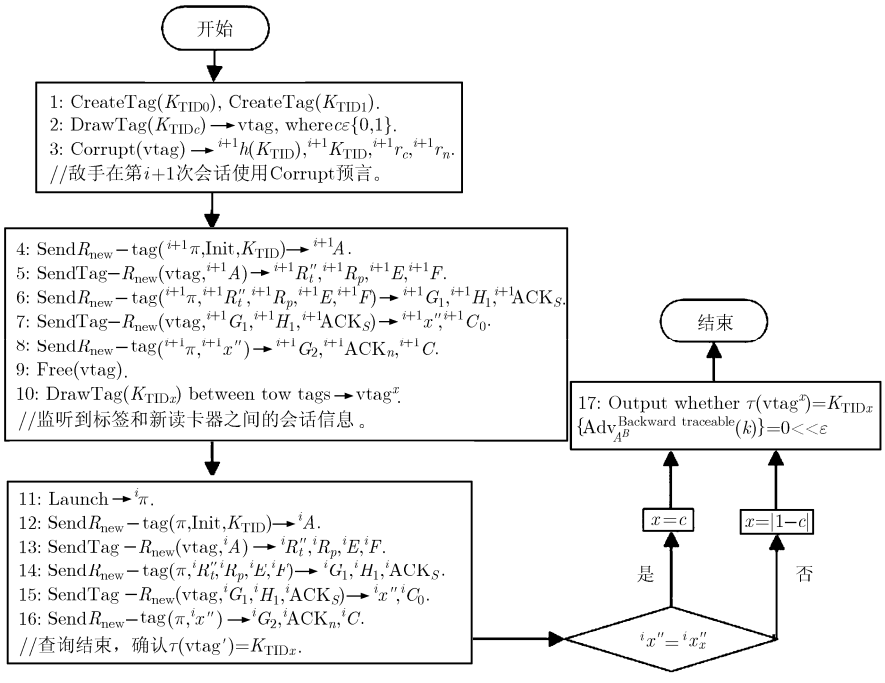

图 2 证明 LROTP 协议满足后向不可追踪性的算法流程图

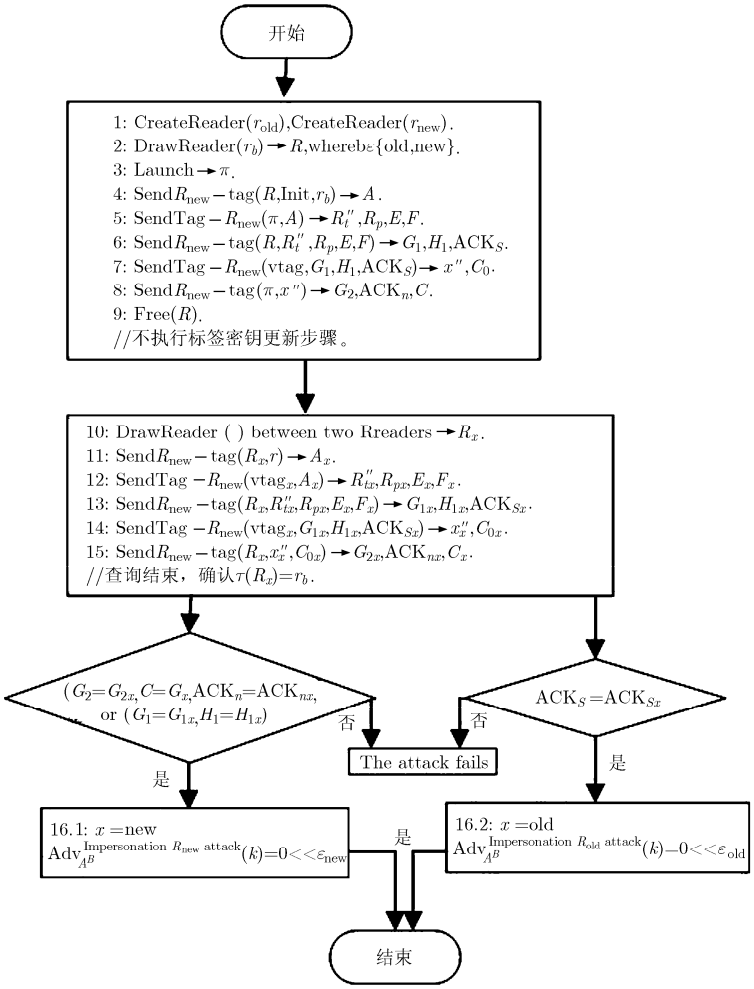

图 3 证明 LROTP 协议是抵抗内部读卡器恶意攻击的算法流程图

定理 4 在弱敌手攻击能力的安全模型下，LROTP 协议可以抵抗标签假冒攻击和异步攻击。

证明 敌手实现异步攻击的方式有以下 3 种情况：

(1)敌手阻止读卡器更新，而更新标签的密钥。

新协议采用先更新读卡器的密钥，再更新标签的密钥，因此敌手无法实现这种情况下的异步攻击。

(2)敌手在实施假冒标签攻击后，促使读卡器两次更新标签密钥，而标签不更新密钥。

第 1 步，敌手监听协议的第 i 次正常会话，拦截 LROTP 协议的所有权转移阶段中的步骤 6 的信息(G_2,ACK$_n$,C)，阻止标签接收正确的消息和更新密钥。第 2 步，敌手启动第$(i+1)$次会话，并修改标签的输出消息(x'',C_0)，使得修改后的假冒的标签信息通过读卡器的验证，读卡器计算错误的消息，随后使用错误的参数更新密钥；标签接收读卡器发送的消息并验证消息的正确性，标签拒绝并阻止密钥更新。

但是敌手修改 x'' 为 ${}^{A}x''$ 的值，C_0 的哈希计算中包含敌手无法计算的，在读卡器验证传递的信息($^{A}x''$,C_0)的完整性，并不能通过包含 $^{A}x''$ 的 C_0 的验证。因此新协议不存在标签假冒攻击导致的异步攻击。

(3)敌手修改读卡器发送的消息，即在外部非法读卡器假冒攻击的前提下，读卡器正常更新密钥，而标签使用错误的参数错误更新的密钥。

敌手启动 LROTP 协议，在所有权转移阶段中执行步骤 1 到步骤 6，修改步骤 6 传递的信息(G_2,ACK$_n$,C)，使得修改后的信息通过标签的验证，并使得标签更新密钥。但是验证消息 C 中含有 G_2 和 ACK$_n$，所以敌手不能通过修改 G_2 和 ACK$_n$ 而通过标签验证。

因此敌手在任何一种情况下都无法实现异步攻击，LROTP 协议抵抗标签假冒攻击和异步攻击。

证毕

定理 5 在弱敌手攻击能力的安全模型下，LROTP 协议可以抵抗追踪攻击。

证明　标签每次响应时都会产生随机数，并将生成的随机数用于加密标签和读卡器传输的数据。即使在标签密钥没有更新的情况下，标签在不同的会话中，每个阶段标签输出的信息仍然不同；并且输出的信息之间经过简单的运算操作(异或，加减运算)不存在任何恒等的关系。例如，敌手想利用监听到的信息(OT , A)重放给密钥未更新的标签 T_i, T_i 反馈(${}^{A}R_t''$, ${}^{A}R_p$, ${}^{A}E$, ${}^{A}F$)给敌手，但是这 4 个信息中都含有标签生成的随机数。其中消息 $R_t = h(\mathrm{TID}) \oplus r_c \oplus n_s \oplus v_p$ ，在不同的会话中标签选择的随机数 n_s 和 v_p 不相同，因此生成的信息 R_t 都不相同，因此 LROTP 协议可以抵抗追踪攻击。

证毕

4.2 协议比较

(1)协议安全性比较：　对 LROTP 协议进行安全性分析，将 LROTP 方案与其他协议的安全性对比，相关比较结果如表 2 所列。文献[3]详细分析了文献[1]存在标签追踪攻击和异步攻击，但是并没有指出协议[1,2]存在的其他问题。本文指出文献[3]提出的协议存在追踪攻击。在文献[2]的协议中，标签输出信息(X , T)的数据结构和文献[3]协议标签输出(x'' , t'')是相同的，因此文献[2]协议也存在追踪攻击。文献[1]存在的标签假冒攻击，因为标签的输出数据结构相同，因此文献[2,3]也存在标签假冒攻击。

表 2 相关协议安全性比较

协议	S1	S2	S3	S4	S5
文献[1]	否	–	否	是	否
文献[2]	否	–	否	是	否
文献[3]	否	–	否	是	否
文献[4]	否	否	是	是	否
文献[5]	否	否	是	是	否
本文协议	是	是	是	是	是

注：S1：抵抗标签假冒攻击和异步攻击；S2：抵抗内部读卡器恶意攻击；S3：抵抗追踪攻击；S4：后向不可追踪性；S5：强前向不可追踪性

文献[1–3]协议中没有区分新旧读卡器，所以不需要分析读卡器恶意攻击。在文献[5]协议存在内部读卡器假冒攻击。文献[4]协议和文献[5]协议结构类似，因此存在着相同的安全性问题。本文 LROTP 协议中新属主只是传递加密的 n' 的值给标签，基于 NP 难解问题，而敌手或是其他恶意读卡器很难计算大素数 p 和 q 的值。另外旧属主无法获取更新后标签的任何密钥和新属主的密钥。同理新属主也无法获取更新前标签的旧属主的密钥，防止恶意所有者攻击。

文献[1–3]协议中只需要更新标签密钥 $r_{i+1} = \mathrm{PRNG}(r_i)$，因此只分析密钥 r 的状态即可分析标签的后向和强前向不可追踪性等性能。因为密钥更新采用 PRNG 函数，此函数无法反向计算出种子值，即使敌手已经腐化了当前密钥 r_i，但是无法推知过去密钥 r_{i-1}，因此文献[1–3]协议满足后向不可追踪性；如果敌手利用腐化的当前密钥 r_i 和 PRNG 函数就可以计算出 r_{i+1} 值，因此这种密钥更新机制导致文献[1–3]协议不满足强前向不可追踪性。文献[21]协议提出了认证和所有权管理协议，但是由于没有采用二次剩余定理，所以不满足强前向不可追踪性。

为了解决更新标签密钥机制中的使用的随机数容易泄露的问题，当前所有者与目标标签认证 LROTP 协议和文献[4,5]协议时，使用 x' 同步更新标签和新所有者的密钥，使得这类协议满足强前向不可追踪性和后向不可追踪性，可以抵抗追踪攻击，但是仅有 LROTP 协议能抵抗异步攻击和内部读卡器恶意攻击。

(2)协议性能比较：　从存储量和计算量，通信代价等 3 个方面对提出的协议进行性能分析，评估比较的结果如表 3 所列。

表 3 相关协议性能比较

协议	N1	N2	N3	N4	N5
文献[1]	4	4	1	2M+3H	3
文献[2]	4	4	2	3M+4H	3
文献[3]	8/3	4	3	3M	3
文献[4]	5	4	2	2M+2C	7
文献[5]	5	4	4	3M	7
本文协议	4	4	3	3M+3H	5

注：N1：数据库/读卡器存储密钥的数目；N2：标签存储密钥的数目；N3：标签生成的伪随机数的数目；N4：标签端加密函数和数目；N5：标签与读卡器交换的信息的数目；H: Hash function; C: Cyclic Redundancy Code; M: Modulo squaring

(a)计算代价：为了实现较低的计算代价，协议[1–3]虽然没有使用哈希函数，但是存在着很大的安全问题。LROTP 协议使用哈希函数保证了协议的安全性，并且标签使用的伪随机数比文献[5]少。

(b)通信代价：通过减少通信循环次数或者通信通道传输的数据量来降低通信代价。在表 3 中，本文的 LROTP 协议标签和读卡器之间的通信次数是 5 轮，与文献[4,5] 7 轮的通信代价相比减少了 2 轮。

(c)存储代价：减少读卡器端的存储量会减少协议整体的计算量。由表 3 可知，LROTP 协议与文献[4,5]相比，在降低读卡器和标签存储空间的基础

上实现了更高的安全性能和隐私特性。因为读卡器不再保存长比特密钥 n，而用梅森数 2^t-1 来表示 n，只存储 t 降低了读卡器存储空间，提高读卡器的计算性能。

5 结束语

本文的轻量级所有权转移 LROTP 协议解决现有所有权转移协议存在的内部读卡器恶意攻击等安全问题，并满足强前向不可追踪性和后向不可追踪性。与其他所有权转移协议比较，LROTP 协议具有较好的安全性和较高的效率。在未来的研究工作中，将使用 Vaudenay 模型中的基于强敌手攻击能力的安全模型分析新设计的协议，并同时分析在强敌手攻击能力的安全模型下其他协议的安全性。

参 考 文 献

[1] CHEN Yalin, CHOU Juesam, and SUN Hungmin. A novel mutual authentication scheme based on quadratic residues for RFID systems[J]. *Computer Networks*, 2008, 52(12): 2373–2380. doi: 10.1016/j.comnet.2008.04.016.

[2] YEH Tzuchang, WU Chienhung, and TSENG Yuhmin. Improvement of the RFID authentication scheme based on quadratic residues[J]. *Computer Communications*, 2011, 34(3): 337–341. doi: 10.1016/j.comcom.2010.05.011.

[3] DOSS Robin, SUNDARESAN Saravanan, and ZHOU Wanlei. A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems[J]. *Ad Hoc Networks*, 2013, 11(1): 383–396. doi: 10.1016/j.adhoc.2012.06.015.

[4] DOSS Robin and ZHOU Wanlei. A secure tag ownership transfer scheme in a closed loop RFID system[C]. Proceedings of the Wireless Communications and Networking Conference Workshops (WCNCW), Paris, 2012: 164–169.

[5] DOSS Robin, ZHOU Wanlei, and YU Shui. Secure RFID tag ownership transfer based on quadratic residues[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(2): 390–401. doi: 10.1109/TIFS.2012.2235834.

[6] 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. doi: 10.11999/JEIT140902.
XIE Run, XU Chunxiang, CHEN Wenjie, *et al*. An RFID authentication protocol anonymous against readers[J]. *Journal of Electronics & Information Technology*, 2015, 37(5): 1241–1247. doi: 10.11999/JEIT140902.

[7] 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 Yongming, SUN Huiping, GUAN Zhi, *et al*. Ownership transfer protocol for RFID tag[J]. *Journal of Computer Research and Development*, 2011, 48(8): 1400–1405.

[8] ALAGHEBAND Mahdi R and AREF Mohammad R. Simulation-based traceability analysis of RFID authentication protocols[J]. *Wireless Personal Communications*, 2014, 77(2): 1019–1038. doi: 10.1007/s11277-013-1552-7.

[9] MORIYAMA Daisuke. Cryptanalysis and Improvement of A Provably Secure RFID Ownership Transfer Protocol[M]. Lightweight Cryptography for Security and Privacy, Springer Berlin Heidelberg, 2013: 114–129. doi: 10.1007/978-3-642-40392-7_9.

[10] ELKHIYAOUI Kaoutar, BLASS Erik-Oliver, and MOLVA Refik. ROTIV: RFID Ownership Transfer with Issuer Verification[M]. RFID Security and Privacy, Springer Berlin Heidelberg, 2012: 163–182. doi: 10.1007/978-3-642-25286-0_11.

[11] CHIEN Hungyu. Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices[J]. *Computer Networks*, 2013, 57(14): 2705–2717. doi: 10.1016/j.comnet.2013.06.005.

[12] VAN Deursen T. Security of RFID protocols[D]. [Ph.D. dissertation], University of Luxembourg, Luxembourg, 2011.

[13] 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 Hui, HOU Chaohuan, and WANG Donghui. A new security and privacy on RFID mutual authentication protocol based on partial ID[J]. *Journal of Electronics & Information Technology*, 2009, 31(4): 853–856.

[14] LI Nan, MU Yi, SUSILOA Willy, *et al*. Shared RFID ownership transfer protocols[J]. *Computer Standards & Interfaces*, 2015, 42: 95–104. doi: 10.1016/j.csi.2015.05.003.

[15] ZHANG Shigeng, LIU Xuan, WANG Jianxin, *et al*. Energy-efficient active tag searching in large scale RFID systems shigeng[J]. *Information Sciences*, 2015, 317: 143–156. doi: 10.1016/j.ins.2015.04.048.

[16] HSI Chengter, LIEN Yuanhung, CHIU Junghui, *et al*. Solving scalability problems on secure RFID grouping-proof protocol [J]. *Wireless Personal Communications*, 2015, 84(2): 1069–1088. doi: 10.1007/s11277-015-2676-8.

[17] AKGUN Mete and ÇAGLAYAN M Ufuk. Providing destructive privacy and scalability in RFID systems using PUFs[J]. *Ad Hoc Networks*, 2015, 32: 32–42. doi: 10.1016/j.adhoc.2015.02.001.

[18] ZHANG Daqiang, QIAN Yuming, WAN Jiafu, *et al*. An efficient RFID search protocol based on clouds[J]. *Mobile Network Application*, 2015, 20: 356–362. doi: 10.1007/s11036-015-0597-0.

[19] VAUDENAY Serge. On Privacy Models for RFID[M]. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2007, 4833: 68–87. doi: 10.1007/978-3-540-76900-2_5.

[20] PHAN Raphael C W, WU Jiang, OUAFI Khaled, *et al*. Privacy analysis of forward and backward untraceable RFID authentication schemes[J]. *Wireless Personal Communications*, 2011, 61(1): 69–81. doi: 10.1007/s11277-010-0001-0.

[21] NIU Haifeng, TAQIEDDIN Eyad, and JAGANNATHAN S. EPC gen2v2 RFID standard authentication and ownership management protocol[J]. *IEEE Transactions on Mobile Computing*, 2016, 15(1): 137–149. doi: 10.1109/TMC.2015.2412933.

陈秀清： 女，1981 年生，讲师，研究方向为信息安全和安全协议.
曹天杰： 男，1965 年生，教授，研究方向为信息安全和安全协议.
翟靖轩： 男，1982 年生，博士，研究方向为信息安全和安全协议.