doi:10.11959/j.issn.1000-436x.2015228

可证明安全的 RFID 标签所有权转移协议

原变青，刘吉强
（北京交通大学 计算机与信息技术学院，北京 100044）

摘 要：随着物品所有权的转移，其上附着的 RFID 标签的所有权也需要转移。安全和隐私问题是标签所有权转移过程中需要研究的重点问题。在通用可组合框架下，形式化定义了 RFID 标签所有权转移的理想函数。提出了一个新的轻量级 RFID 标签所有权转移协议，并证明了该协议安全地实现了所定义的理想函数，即具有双向认证、标签匿名性、抗异步攻击、后向隐私保护和前向隐私保护等安全属性。与已有的 RFID 标签所有权转移协议相比，新协议中 RFID 标签的计算复杂度和存储空间需求都较低，并且与新旧所有者的交互较少，能够更加高效地实现低成本标签的所有权转移。

关键词：通用可组合；无线射频识别；所有权转移；双向认证；隐私保护
中图分类号：TP309 **文献标识码**：A

Provable secure ownership transfer protocol for RFID tag

YUAN Bian-qing, LIU Ji-qiang
(School of Computer and Information Technology，Beijing Jiaotong University，Beijing 100044, China)

Abstract: With the ownership transfer of an object, the ownership of the RFID tag attached to it also needs to be transferred. Security and privacy are the key issues while researchers studying the process of RFID tag ownership transfer. In the UC (universally composable) framework, an ideal functionality of RFID tag ownership transfer is formally defined. Then, a novel lightweight ownership transfer protocol for RFID tag is proposed. Subsequently, it is proved that proposed protocol realizes the previously defined ideal functionality and satisfies the required security properties such as mutual authentication, tag anonymity, resistance to de-synchronization attacks, forward privacy protection and backward privacy protection. Compared with the existing ownership transfer protocols for RFID tags, the computational complexity and the storage requirements of proposed protocol are all lower. Meanwhile, the number of interaction among the entities is small. Therefore, the proposed protocol can efficiently implement ownership transfer for low-cost tags.

Key words: universally composable; RFID; ownership transfer; mutual authentication; privacy protection

1 引言

无线射频识别（RFID）是一种自动识别和数据获取技术。通过将 RFID 标签附着到特定目标，如产品、动物、人等，读写器无需直接接触目标即可实现对特定目标的识别和数据的搜集。RFID 标签具有成本低、读取距离大、耐磨损、数据可加密与修改等优点，其应用已遍布生产制造、交通运输、批发零售以及票证管理等多个领域。在实际的应用中，RFID 标签附着的目标实体的所有权经常发生改变，从而 RFID 标签的所有权在其生命期中也需要发生转移[1]。在 RFID 标签所有权转移过程中，标签的信息安全与隐私问题受到了越来越多学者们的关注。

2005 年，Molnar 等[2]首次提出一个针对 RFID 标签所有权转移的匿名协议，该协议由一个可信中

收稿日期：2015-01-22；**修回日期**：2015-06-18
基金项目：新世纪优秀人才支持计划基金资助项目(NCET-11-0565)；中央高校基本科研业务费专项基金资助项目(2012JBZ010)；教育部高校创新团队基金资助项目(IRT201206)
Foundation Items: Program for New Century Excellent Talents in University (NCET-11-0565); The Fundamental Research Funds for the Central Universities (2012JBZ010); Program for Innovative Research Team in University of Ministry of Education of China (IRT201206)

心（TC）来控制所有的标签信息，要求标签原所有者和新所有者必须相信相同的 TC，这限制了协议的使用范围。同年，Osaka 等[3]基于散列函数和对称密码体制提出了一个高效的所有权转移协议。该方案通过在所有权转移过程中改变对称私钥，实现了对标签原所有者和新所有者的保护。但该方案不能抵抗拒绝服务攻击，也不满足标签的不可追踪性。2007 年，为解决新所有者的隐私保护问题，Fouladgar 和 Afifi[4]提出了一个简单、高效的支持授权和所有权转移的协议。然而，由于标签每次返回的值可能被敌手获取，进而使敌手成功冒充该标签，因此该方案不能抵抗重放攻击。此外，标签还有被追踪的危险。在 2008 年的 RFIDSec 会议上，Song[5]定义了 RFID 标签所有权转移协议的安全和隐私保护需求，并提出了 3 个子协议：所有权转移协议、秘密更新协议以及授权恢复协议。但经多位学者[6,7]分析，该方案存在诸多安全性问题。随后，Song 等对该方案进行了改进，但改进后的方案[8]仍不具备后向隐私保护并且易受到异步攻击。2011 年，金永明等[9]基于 SQUASH 方案，提出了一种新的轻量级所有权转移协议。该协议比基于散列的方案具有更高的效率，还优化了 Song 等[5]的所有权转移协议。但经过分析，在所有权转移时，新所有者可以获得原所有者与标签交互时共享的公私钥(s_i, t_i)，这使新所有者在获得 RFID 标签所有权后还能访问之前 RFID 标签与原所有者交互的数据，因此该协议不具备前向隐私保护。另外，在密钥更新阶段，恶意的原所有者能通过窃取消息 P 以及之前认证阶段获得的随机数 r_T 计算出 t_i'，从而可以继续访问标签，因此该协议也不具备后向隐私保护。在 2011 年 RFIDSec 会议上，针对供应链中标签所有权转移存在的安全和隐私问题，Elkhiyaoui 等[10]提出了 RFID 标签所有权转移协议的安全模型并设计了一个可实现签发者验证的标签所有权转移方案。该方案在标签中存储签发者的签名，且该签名可被供应链中所有参与者进行验证。但 Moriyama[11]指出 Elkhiyaoui 等的安全模型有局限性，如该模型假设所有权转移协议的各参与方均无恶意，这种假设使得其协议在现实中不能提供足够的隐私保护。2012 年，Kapoor 等[12]提出了有可信第三方（TTP）和无 TTP 的 2 个所有权转移方案。然而，有 TTP 的所有权转移方案易受到异步攻击，而无 TTP 的所有权转移方案则存在后向隐私泄漏及易受到拒绝服务攻击等安全性问题。2013 年，Doss 等[13]基于二次剩余理论提出了 2 个标签所有权转移方案：闭环方案和开环方案，但 2 个协议均需要标签与新旧所有者之间执行多次交互且需要在标签上多次执行模平方运算，严重影响了 RFID 标签的转移效率。同年，Chen 等[14]提出了遵循 EPCglobal C1G2 标准的标签所有权转移协议，该协议在标签端仅使用 PRNG 和 CRC 操作。然而，该方案易受到拒绝服务攻击。

基于可证明安全性理论和方法来进行 RFID 安全协议的设计和分析是近来 RFID 协议重要的研究方向，相关研究也取得了较为丰富的成果[15~17]。通用可组合框架[18]（UC 框架）是用于描述和分析并发环境下协议安全性问题的理论框架。许多学者在通用可组合框架下设计和分析了各种 RFID 协议[19~22]，但是目前还没有学者在该框架下对 RFID 标签所有权转移协议进行研究。本文首先在通用可组合框架下，形式化定义了 RFID 标签所有权转移的理想函数。然后，提出了一个新的轻量级 RFID 标签所有权转移协议，并证明了新协议安全地实现了该理想函数。

2 RFID 标签所有权转移协议模型与安全需求

2.1 交互模型

在 RFID 系统中有 3 类实体：RFID 标签、读写器和后台服务器。其中，RFID 标签具有有限的存储空间和有限的计算能力。而后台服务器则具有较强的处理能力，它通过与其连接的读写器与 RFID 标签进行通信。后台服务器中还有一个数据库，用来存储它所拥有的 RFID 标签的信息。不失一般性，本文假设读写器与标签之间存在不安全的通信信道，而读写器与后台服务器之间有安全的通信信道。同时，后台服务器之间也有安全的通信信道。

标签所有权是指可以识别标签并控制与标签有关的所有信息的能力。标签所有权转移意味着新所有者接管了标签的管理权。由于在分析 RFID 标签所有权转移协议时，通常将后台服务器和读写器看作一个整体，即视二者为一个独立的通信实体[5,8,13]。因此，本文提出的协议涉及到 3 个参与方：当前所有者服务器/读写器（*CS*）、新所有者服务器/读写器（*NS*）和待转移所有权的标签（*T*）。标签所有权转移要经历 3 个阶段：1）认证阶段：*CS* 查询其数据库以确认 *NS* 读取的标签为 *T*；2）授权阶段：*CS* 将 *T* 的信息传送给 *NS*，使 *NS* 能识别和读取 *T*；3）

秘密更新阶段：*NS* 与 *T* 同步更新秘密，安全地实现 *T* 所有权的转移。

2.2 敌手模型

在 RFID 标签所有权转移协议中，敌手 *A* 的攻击可以分为对信道的攻击和对参与方的攻击。对于信道的攻击，假设敌手 *A* 能够完全控制 *NS* 与标签 *T* 之间的通信信道，可以任意地读取、删除、篡改、延迟发送和重放信道中的任何消息, 也可以在任何时候发起与任何参与方的任意会话。此外，本文暂不讨论对标签的物理攻击。因此，对于参与方的攻击，假定敌手 *A* 在协议执行的任何时候都可以攻陷参与方 *CS* 和 *NS*。而对于攻陷后的实体，敌手 *A* 能够成功获取到其内部状态数据。

敌手 *A* 攻击的方法主要有：重放攻击、异步攻击、中间人攻击、假冒攻击、伪造攻击和隐私攻击等。

2.3 安全需求

一个安全的 RFID 标签所有权转移协议需要满足以下安全属性[5]。

1) 双向认证：在所有权转移过程中，只有在 *CS* 成功认证标签 *T* 并且标签 *T* 也成功认证 *CS* 后，才能完成所有权的转移。

2) 标签匿名性：任意的攻击者 *A*，仅通过截获 *CS*（或 *NS*）与标签 *T* 之间的交互信息，无法获得标签 *T* 的任何身份信息，也无法追踪到标签 *T* 的任何活动。

3) 抗异步攻击：在攻击者 *A* 通过任意手段中断所有权转移协议，使 *CS*（或 *NS*）与标签 *T* 的信息同步失败后，协议可以保证标签 *T* 认证的再次成功，并实现信息的同步。

此外，还需要确保以下隐私需求。

1) 后向隐私保护：所有权转移之后，标签 *T* 的原所有者 *CS* 不能再识别该标签，也无法访问该标签和新所有者 *NS* 的会话信息。

2) 前向隐私保护：所有权转移之后，标签的新所有者 *NS* 不能访问所有权转移前标签 *T* 与原所有者 *CS* 之间的会话信息。

3 RFID 标签所有权转移协议的 UC 模型

3.1 通用可组合安全

通用可组合框架（UC 框架）是由 Canetti[18]提出的，该框架下所有的参与方都被抽象为概率多项式时间的交互式图灵机。在该框架下被证明为安全的协议，不论是与其他协议并发运行，还是作为任意系统的组件运行，协议仍然安全。

UC 框架定义了 2 种协议运行模型[23]：现实模型和理想模型。其中，现实模型表示现实中协议的执行过程，主要涉及 3 类参与方：环境机 *Z*、执行协议 π 的多个参与方 $\{P_i\}$ 以及现实敌手 *A*。而理想模型则用来描述密码协议的理想运行。理想模型中主要涉及的参与方包括环境机 *Z*、通过虚拟用户 $\{\tilde{P}_i\}$ 与环境机 *Z* 进行交互的理想函数 *F* 以及理想过程敌手 *S*。其中，理想函数 *F* 能够安全地完成协议所执行的特定功能, 它本质上是一个不可攻陷的可信方。目前，已经定义的理想函数有：认证消息传输 F_{AUTH}、密钥交换 F_{KE}、公钥加解密 F_{PKE}、签名 F_{SIG}、零知识证明 F_{ZK}、不经意传输 F_{OT}[24]、基于一次签名（F_{OTS}）的广播认证（F_{BAUTH}）[25]、可信网络连接 F_{TNC}[26]和安全定位 F_{SP}[27]等。

定义 1　如果对于任意敌手 *A*，存在理想过程敌手 *S*，使环境机 *Z* 不能以不可忽略的概率区分它是在与现实过程中的 *A* 和运行协议 π 的参与方$\{P_i\}$交互还是在与理想过程中的 *S* 和 *F* 交互，则称协议 π 安全地实现了理想函数 *F*。即

$$IDEAL_{F,S,Z} \approx REAL_{\pi,A,Z}$$

3.2 RFID 标签所有权转移的理想函数 F_{TRANS}

首先，介绍在定义标签所有权转移理想函数时需要使用的变量和指令：*sid* 为会话标识；Type(*P*) 返回参与方 *P* 的类型；指令(Init, *sid*, *P*, *M*)表示参与方 *P* 接收到了来自环境机 *Z* 的消息并开始发起会话；指令(Authed, *sid*, P_A, P_B, *secret*)表示参与方 P_A 认证了参与方 P_B，且二者共享的秘密为 *secret*；指令(Transfer, *sid*, P_A, P_B, P_C)表示参与方 P_A 将 P_C 的所有权转移给 P_B；指令(Update, *sid*, *P*, *secret*）表示参与方 *P* 更新其秘密为 *secret*；指令(Output, *sid*, *P*, *secret*）表示理想函数的输出。

下面基于第 2 节描述的协议模型和安全需求，形式化定义 RFID 标签所有权转移的理想函数 F_{TRANS}。

由于标签 *T* 和 *CS* 的所属关系是标签所有权转移的前提，因此理想函数 F_{TRANS} 使用记录（*CS*, *T*, *t*, *Info*(*T*))来表示这种所有关系。其中，*t* 为任意随机数，用来标识标签 *T* 的动态身份；*Info*(*T*)表示标签 *T* 的业务数据。

1) 一旦收到 *NS* 发送的消息(Init, *sid*, *NS*, M_{NS})，传送(*sid*, Type(*NS*), M_{NS})给敌手 *S*。一旦收到 *T* 发送

的消息(Init, *sid*, *T*, M_T)，传送（*sid*, Type(*T*) , M_T)给敌手 *S*。

2) 一旦收到来自敌手 *S* 的消息(Authed, *sid*, *CS*, *T*, *k*)，检查记录(*CS*, *T*, *t*, *Info*(*T*))是否存在：

a) 如果记录不存在，记录(Authed, *sid*, *CS*, *T*, *fail*)；

b) 如果记录存在且 $k = t$，则记录(Authed, *sid*, *CS*, *T*, *success*)；

c) 如果记录存在且 $k \neq t$，分 2 种情况：如果 *CS* 已被攻破，由 *S* 决定认证结果；如果 *CS* 没有被攻破，记录(Authed, *sid*, *CS*, *T*, *fail*)。

3) 一旦收到来自敌手 *S* 的消息(Authed, *sid*, *T*, *CS*, *k*′)，检查记录(*CS*, *T*, *t*, *Info*(*T*))是否存在，如果记录存在且 $k' = t$，那么记录(Authed, *sid*, *T*, *CS*, *success*)，否则，记录(Authed, *sid*, *T*, *CS*, *fail*)。

4) 一旦收到 *CS* 发送的消息(Transfer, *sid*, *CS*, *NS*, *T*)，记录(*sid*, *NS*, *CS*, *T*)。

5) 一旦收到 *S* 发送的消息(Update, *sid*, *NS*, γ)，检查记录(Authed, *sid*, *CS*, *T*, *success*)、(Authed, *sid*, *T*, *CS*, *success*)和(*sid*, *NS*, *CS*, *T*)是否全部存在：

a) 如果记录都存在，且 *NS* 没有被攻破，则选择随机数α，并添加记录(*NS*, *T*, α, *Info*(*T*))，然后发送(Output, *sid*, *NS*, α)给 *NS*；

b) 如果记录都存在，且 *NS* 已被攻破，则添加记录(*NS*, *T*, γ, *Info*(*T*))，然后发送(Output, *sid*, *NS*, γ)给 *NS*；

c) 如果有一条记录不存在，则返回失败。

6) 一旦收到 *S* 发送的消息(Update, *sid*, *T*, β)，检查包含(*NS*, *T*)的记录是否存在：如果记录存在，并找到记录(*NS*, *T*, χ, *Info*(*T*))，则发送(Output, *sid*, *T*, χ)给 *T*，然后删除记录(*CS*, *T*, *t*, *Info*(*T*))。如果记录不存在，则返回失败。

7) 如果在随机数α选择后，敌手 *S* 攻破了 *NS*，则将α发送给敌手 *S*。

3.3 安全性分析

下面证明理想函数 F_{TRANS} 满足 2.3 节中定义的安全需求。

1) 双向认证：在理想环境下，标签所有者 *CS* 对标签 *T* 的认证是通过指令(Authed, *sid*, *CS*, *T*, *k*)来实现的，而指令(Authed, *sid*, *T*, *CS*, *k*′)的实现也确保了标签 *T* 对所有者 *CS* 的认证。只有当 2 个认证都返回成功时，也就是记录(Authed, *sid*, *CS*, *T*, *success*)、(Authed, *sid*, *T*, *CS*, *success*)都存在的条件下，F_{TRANS} 才会添加记录(*NS*, *T*, α, *Info*(*T*))完成秘密更新，实现所有权的转移。

2) 标签匿名性：标签的业务数据 *Info*(*T*)始终存在于可信环境下，而认证过程中使用的标识 *t* 以及更新后的标识α都是随机数，因此敌手通过窃听不安全信道获得的信息 M_{NS} 以及 M_T，都无法识别或追踪标签 *T*。

3) 抗异步攻击：当敌手 *S* 在执行指令(Update, *sid*, *NS*)和(Update, *sid*, *T*)时，可能通过各种手段使 *NS* 和标签 *T* 的信息不同步。此时，如果包含(*NS*, *T*)的记录已经存在，则在执行指令(Update, *sid*, *T*)后会再次同步。如果包含(*NS*, *T*)的记录不存在，那么，由于记录(*CS*, *T*, *t*, *Info*(*T*))还未被删除，重新启动理想过程仍可以保证标签 *T* 再次被成功认证，进而重新同步信息。

4) 后向隐私保护：在理想环境下，当所有权成功转移之后，即指令(Update, *sid*, *T*)执行后，标签的原所有者 *CS* 和标签 *T* 的所属关系记录(*CS*, *T*, *t*, *Info*(*T*))已经被清除，并且更新后的秘密α对 *CS* 是保密的，因此 *CS* 不能再识别标签 *T*，也无法访问标签 *T* 和新所有者 *NS* 的会话信息。

5) 前向隐私保护：在理想环境下，在指令(Update, *sid*, *NS*)执行前，标签的新所有者 *NS* 并没有得到任何信息。而在指令(Update, *sid*, *NS*)执行后，标签的新所有者 *NS* 也只能获得α。即便是所有权成功转移之后，即指令(Update, *sid*, *T*)执行后，*NS* 也无法获得 *t*。因此 *NS* 无法访问所有权转移前标签 *T* 与原所有者 *CS* 之间的会话信息。

4 UC 安全的 RFID 标签所有权转移协议

基于 2.1 节描述的 RFID 所有权转移协议交互模型，本节给出一个轻量级的 RFID 标签所有权转移协议 π_{TRANS}，如图 1 所示。

以下是符号的定义。

l：标签动态身份以及随机数的安全长度；

f：一个轻量级单向函数，f: $\{0,1\}^* \rightarrow \{0,1\}^l$；

Info：存储标签所标识的目标实体的业务信息的变量；

||：字符串连接操作；

$\in_R$：随机数选择操作；

$\oplus$：异或运算；

$\leftarrow$：置换（赋值）运算。

在初始化阶段，每个标签在后台服务器的数据

库中都对应一条记录（$t_{old}, t_{new}, Info(T)$），其中，$t_{new}$ 表示标签的当前身份，t_{old} 表示标签转移前的身份，$Info(T)$记录标签的业务信息。*NS* 选取 2 个大素数 $p \in_R \{0,1\}^l$ 和 $q \in_R \{0,1\}^{l+1}$，满足 $p=q=3 \bmod 4$，然后计算 $n=pq$，并公开 n 给 *CS*。*CS* 中存储的有关 *T* 的记录中，$t_{new}=t$，其中 t 表示 *T* 当前的身份信息。标签 *T* 中存储 l 位的 t 和 $2l+1$ 位的 n。下面描述具体协议过程。

1) *NS* 选取随机数 $r_1 \in_R \{0,1\}^l$，然后通过相应的读写器向 *T* 发送挑战消息 r_1。

2) 收到 *NS* 的挑战消息后，*T* 随机选取 $r_2 \in_R \{0,1\}^l, r_3 \in_R \{0,1\}^l$，然后计算 $M_1 = t \oplus r_2$，$M_2 = f(r_1 \| r_2)$，$M_3 = (r_1 \| r_3)^2 \bmod n$，并向 *NS* 发送响应消息$<M_1, M_2, M_3>$。

3) 对收到的消息 M_3，*NS* 根据保存的 p 和 q，解方程组 $M_3=x^2 \bmod p$ 和 $M_3=x^2 \bmod q$ 可分别得到 2 个解，组合可得 4 个同余方程组，根据中国剩余定理计算得到 4 个解：x_1, x_2, x_3, x_4。如果能找到左 l 位等于 r_1 的解 x_i $(1 \leqslant i \leqslant 4)$，那么该解的右 l 位即为 r_3。然后，*NS* 向 *CS* 发送消息$<r_1, M_1, M_2>$。否则，验证失败，停止协议过程。

4) 一旦收到消息$<r_1, M_1, M_2>$，*CS* 顺序执行以下操作：

a) *CS* 从数据库的 t_{new} 列中查找使下式成立的 t：$M_2 = f(r_1 \| (M_1 \oplus t))$，如找到，则 *T* 通过认证。然后，*CS* 计算 $M_4 = t \oplus f(M_1 \oplus t)$，执行命令 $Info \leftarrow Info(T)$，并更新数据库：$t_{old} \leftarrow t$, $t_{new} \leftarrow$ null，最后，*CS* 向 *NS* 发送授权消息$<M_4, Info>$；

b) 如果上一步查找失败，*CS* 再从数据库的 t_{old} 列中查找，如查找成功，则表明上次所有权转移阶段出现同步异常，此次 *T* 重新通过认证，然后，*CS* 计算 $M_4 = t \oplus f(M_1 \oplus t)$，执行命令 $Info \leftarrow Info(T)$，并向 *NS* 发送授权消息$<M_4, Info>$；

c) 如果前 2 步均查找失败，则停止协议过程。

5) 一旦收到 *CS* 发送的授权消息，*NS* 选取随机数 $t' \in_R \{0,1\}^l$ 作为标签 *T* 的新身份信息，计算 $M_5 = t' \oplus r_3$，$M_6 = f(M_4 \| M_5 \| r_3)$。然后，更新数据库：$t_{new} \leftarrow t'$，$Info(T) \leftarrow Info$，并向 *T* 发送消息$< M_5, M_6 >$。

6) 一旦收到 *NS* 发送的消息$< M_5, M_6 >$，*T* 判断 $M_6 \stackrel{?}{=} f((t \oplus f(r_2)) \| M_5 \| r_3)$，如果成立则 *CS* 和 *NS* 均通过认证，*T* 更新其身份信息：$t \leftarrow M_5 \oplus r_3$。否则，认证失败，停止协议过程。

5　安全性证明及效率分析

5.1　安全性证明

定理 1　协议 π_{TRANS} 在 UC 框架下安全地实现了理想函数 F_{TRANS}。

证明　令 *A* 为现实模型中的任意敌手。下面构建理想过程敌手 *S*，使环境机 *Z* 不能以不可忽略的概率区分它是在与现实过程中的 *A* 和运行协议 π_{TRANS} 的各参与方交互还是在与理想过程中的 *S* 和 F_{TRANS} 交互。

首先，构建理想敌手 *S*，*S* 运行 *A* 的仿真拷贝，它仿真 *A* 与运行 π_{TRANS} 的各方的交互。更具体地，*S* 运行如下。

1) 与环境机 *Z* 的通信：任何来自 *Z* 的输入均被转发给 *A*。任何来自 *A* 的输出被拷贝作为 *S* 的输

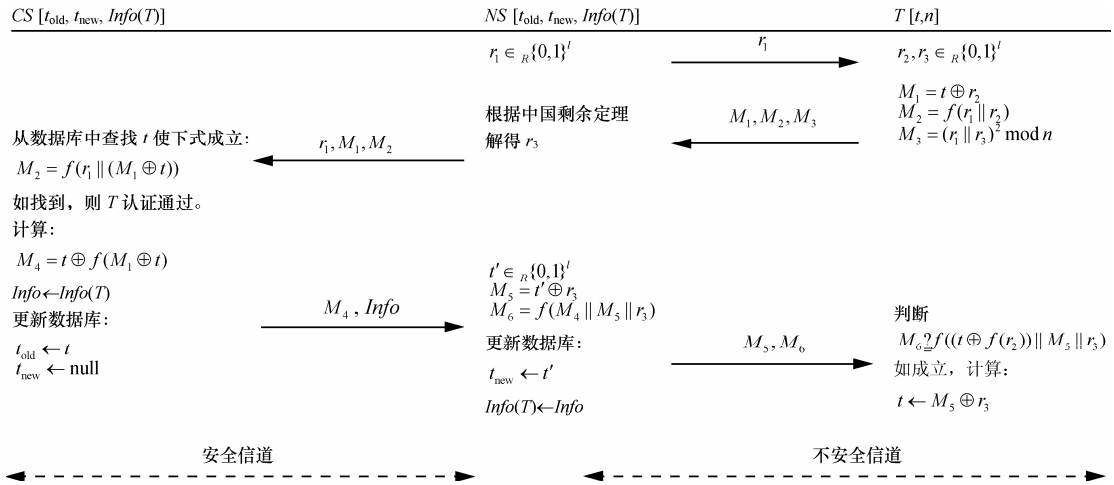

图 1　RFID 标签所有权转移协议 π_{TRANS}

出，并被 Z 读取。

2) 仿真 NS 的初始激活：收到来自 F_{TRANS} 的(*sid*, Type(*NS*), M_{NS})后，S 选择随机数 r_1 并将其传给 A。

3) 仿真 T 收到初始激活消息：当 A 传送初始消息 r_1' 给 T 时，S 首先验证它在理想过程中已经收到来自 F_{TRANS} 的(*sid*, Type(*T*) , M_T)。然后，S 选择随机数 r_2 和 r_3，并将由 T 发送的消息(M_1, M_2, M_3)传给 A，其中，$M_1 = t \oplus r_2$，$M_2 = f(r_1' \| r_2)$，$M_3 = (r_1' \| r_3)^2 \bmod n$。

4) 仿真 NS 收到要求认证的消息：当 A 传送认证消息(M_1', M_2', M_3')给 NS，S 根据 M_3' 解得 r_3'，并发送消息(r_1, M_1', M_2')给 CS。

5) 仿真 CS 收到要求认证的消息：当收到来自 NS 的消息(r_1, M_1', M_2')，S 首先从数据库中查找使 $M_2' = f(r_1 \| (M_1' \oplus t))$ 成立的 t。

a)如果找到对应的 t，则更新数据库中内容并传送(M_4, *Info*)给 NS，其中 $M_4 = t \oplus f(M_1' \oplus t)$，另外，在理想环境下，传送(Authed, *sid*, *CS*, *T*, *t*)给理想函数 F_{TRANS}；

b)如果没有找到对应的 t，则返回认证失败，协议终止，同时，在理想环境下，传送(Authed, *sid*, *CS*, *T*, *k*)给理想函数 F_{TRANS}，其中 k 为 S 选择的任意随机数。

6) 仿真 NS 发送更新秘密的消息：转发从 NS 收到的(M_5，M_6)给敌手 A，其中 $M_5 = t' \oplus r_3$，$M_6 = f(M_4 \| M_5 \| r_3)$，$t'$ 为 S 选择的任意随机段。

7) 仿真标签 T 收到更新秘密的消息：当 A 传送更新秘密消息(M_5', M_6')给标签 T 时，T 判断等式 $M_6' = f((t \oplus f(r_2)) \| M_5' \| r_3)$ 是否成立。

a)如果等式不成立，返回认证失败，协议终止，同时，在理想环境下，传送(Authed, *sid*, *T*, *CS*, *k'*)给理想函数 F_{TRANS}，其中 k' 为 S 选择的任意随机数；

b)如果等式成立，计算 $\alpha \leftarrow M_5' \oplus r_3$，在理想环境下，先传送(Authed, *sid*, *T*, *CS*, *t*)给理想函数 F_{TRANS}，然后再传送(Update, *sid*, *NS*, α)给理想函数 F_{TRANS}，一旦理想函数传送了 Output 消息给 NS，S 也立即传送该消息。最后，更新 T 的身份信息：$t \leftarrow \alpha$。同时，在理想环境下，传送(Update, *sid*, *T*, α)给理想函数 F_{TRANS}，一旦理想函数传送了 Output 消息给 T，S 也立即传送该消息。

8) 仿真 CS（或 NS）被攻破：如果敌手 A 攻破了 CS 或是 NS，那么在理想环境下，S 也攻破了同样的参与方，并且把被攻破参与方的相应内部数据发送给敌手 A。

其次，对 S 有效性进行分析。令 NSC 表示 NS 被攻破的事件，也就是在 NS 和标签 T 更新秘密之前，敌手 A 攻破了 NS（现实中，一般是指 NS 被腐败后的结果）。在理想环境下，事件 NSC 表示在 S 发送 Update 指令之前，仿真的 A 攻破参与方 NS 的事件。

引理 1 无论事件 NSC 发生与否。对于环境机 Z 而言，真实协议 π_{TRANS} 和理想函数 F_{TRANS} 都是不可区分的，即 $REAL_{\pi_{\text{TRANS}},A,Z} \approx IDEAL_{F_{\text{TRANS}},S,Z}$。

证明 当 NSC 发生时，在现实环境中，对于环境机 Z 而言，敌手 A 和 RFID 标签所有权转移协议 π_{TRANS} 交互后输出的值为 α，其中 $\alpha \leftarrow M_5' \oplus r_3$。而在理想环境中，在 S 中仿真的现实中的 A，在更新秘密阶段，用指令(Update, *sid*, *NS*, α)传送同样的 α 给理想函数 F_{TRANS}，并最后由 F_{TRANS} 输出 α 给 NS；同样，在执行完指令(Update, *sid*, *T*, α)后，标签 T 也得到同样的 α。因此，对于环境机 Z 而言，在 NSC 发生时，真实协议 π_{TRANS} 和理想函数 F_{TRANS} 的输出是完全相同的。

当事件 NSC 没有发生时，在现实环境中，对于环境机 Z 而言，敌手 A 和 RFID 标签所有权转移协议 π_{TRANS} 交互后输出的值为 t'，其中 $t' \in_R \{0,1\}^l$。而在理想环境中，在 S 中仿真的现实中的 A 与理想函数 F_{TRANS} 交互后，由 F_{TRANS} 输出 α 给 NS 和 T，其中 α 为 F_{TRANS} 选择的随机数。由于 2 个随机数是不可区分的，因此，对于环境机 Z 而言，在 NSC 没有发生时，敌手 A 与真实协议 π_{TRANS} 交互后和 S 与理想函数 F_{TRANS} 交互后的输出是不可区分的。

综上，对于任意敌手 A，存在理想过程敌手 S，使环境机 Z 不能以不可忽略的概率区分它是在与现实环境中的 A 和运行协议 π_{TRANS} 的参与方交互还是在与理想环境中的 S 和 F_{TRANS} 交互，即 $REAL_{\pi_{\text{TRANS}},A,Z} \approx IDEAL_{F_{\text{TRANS}},S,Z}$。

5.2 效率分析

下面对本文提出的协议与已有的典型协议进行比较。表 1 给出了协议间安全属性的比较，其中“√”表示满足该安全属性，“×”表示不满足该安全属性。表 2 给出了协议间计算与存储代价的比较，

其中，Pr 表示 PRNG 运算，Po 表示按位运算，Pf 表示单向函数运算，Pc 表示冗余校验运算，Pm 表示模平方运算，Ps 表示求解二次剩余根运算，Pe 表示加解密运算，m 指 Song 等方案[8]中服务器端预定义的标签 ID 的个数。

从表 1 和表 2 可以看出，文献[3]和文献[5]提出的方案性能相对较高，但其安全性较差。相比文献[5]，文献[8] 提出的方案虽然其 *CS* 端的运算效率有所提高，但 *CS* 及 *T* 的存储需求有所增加，而且协议仍然无法抵抗异步攻击和无法满足后向隐私保护。文献[9]提出的方案减少了协议执行的交互次数，但该方案不能满足前向隐私保护和后向隐私保护。文献[13]提出的方案安全性有所提高。但该协议所需交互次数最多，而且标签端的运算量和存储量也最高，因此其性能最差。此外，上述协议均未能证明其具备通用可组合安全性。

相比已有的标签所有权转移协议，本文提出的方案只有在 *CS* 成功认证标签 *T* 后才将 *T* 的相关信息授权给 *NS*，并且只有在标签 *T* 成功认证 *CS* 后，才更新其秘密，进而完成所有权的转移；此外，仅拥有 *CS*（或 *NS*）与标签 *T* 之间的交互信息，无法获得标签 *T* 的任何身份信息，也无法追踪到标签 *T* 的任何活动；如果该协议因被任意敌手中断而导致标签 *T* 的信息同步失败，那么利用 *CS*（或 *NS*）中保存的新/旧秘密，协议仍可以保证标签 *T* 的成功认证；由于标签的原所有者 *CS* 无法获得 *NS* 和 *T* 之间的秘密消息 r_3，所以所有权转移后 *CS* 不能再识别和访问 *T*；而标签的新所有者 *NS* 无法获得所有权转移前标签 *T* 与原所有者 *CS* 之间的秘密 t，所以 *NS* 也不能访问所有权转移前标签 *T* 与原所有者 *CS* 之间的会话信息。因此，新方案不仅满足了双向认证、标签匿名性、抗异步攻击、前向隐私保护等安全需求，更有效地解决了已有所有权转移协议未能解决的后向隐私保护问题。此外，本文在 UC 框架下证明了新协议的安全性，使协议具备通用可组合安全性。在性能方面，新方案的计算复杂度和存储需求也相对较小，而且交互次数做到了最少。

6　结束语

随着物联网技术的快速发展，RFID 技术应用越来越广泛。然而，由于 RFID 标签的资源限制，如何设计一个安全、高效的轻量级 RFID 标签所有权转移协议是当前需要重点研究的一个问题。首先，本文对 RFID 标签所有权转移协议的交互模型和攻击模型做了分析和描述。然后，在通用可组合安全框架下，形式化定义了理想函数 F_{TRANS}。最后，设计了轻量级 RFID 标签所有权转移协议 π_{TRANS}，并证明了协议 π_{TRANS} 安全地实现了理想函数 F_{TRANS}。

表 1　　**类似协议安全属性比较**

方案	双向认证	标签匿名性	抗异步攻击	后向隐私保护	前向隐私保护	通用可组合安全
文献[3]方案	×	×	×	×	×	×
文献[5]方案	√	√	×	×	×	×
文献[8]方案	√	√	×	×	√	×
文献[9]方案	√	√	√	×	×	×
文献[13]方案（开环）	√	√	√	×	√	×
本文方案	√	√	√	√	√	√

表 2　　**类似协议性能比较**

方案	*T* 的存储需求[1]	*T* 的运算量	*CS* 的运算量[2]	*NS* 的运算量	交互次数[3]
文献[3]方案	1	3Po+Pf	(*O*(*N*)+1) Po+2Pe+ *O*(*N*) Pf	Po+Pe	5
文献[5]方案	1	13Po+6Pf	(2*O*(*N*)+8) Po+(*O*(*N*)+1) Pf	4Po+3Pf	7
文献[8]方案	3	2Po+7Pf	Po+(*O*(1)+*m*+2)Pf	Po+(3+*m*) Pf	6
文献[9]方案	3	6Po+Pm	(*O*(*N*)+1)Po+*O*(*N*)Pm	5Po+Pm	5
文献[13]方案（开环）	4	21Po+4Pm+5Pr+Pc	(2*O*(*N*)+5)Po+2Ps+Pr+Pc	7Po+2Ps+3Pr	10
本文方案	2	3Po+3Pf+Pm	(*O*(*N*)+2)Po+(*O*(*N*)+1)Pf	Po+Ps+Pf	5

[1] 统计是需要存储的参数数量；[2] 统计是基于 *CS* 数据库中有 *N* 个标签的情况；[3] 统计是协议执行过程中总的信息传输次数。

参考文献：

[1] LIM C H, KWON T. Strong and robust RFID authentication enabling perfect ownership transfer[A]. 8th International Conference on Information and Communications Security[C]. Raleigh, NC, USA, 2006. 1-20.

[2] MOLNAR D, SOPPERA A, WAGNER D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags[A]. 12th International Workshop on Selected Areas in Cryptography[C]. Kingston, Ont, Canada, 2006. 276-290.

[3] OSAKA K, TAKAGI T, YAMAZAKI K, *et al.* An efficient and secure RFID security method with ownership transfer[A]. Proceedings of IEEE 2006 International Conference on Computational Intelligence and Security[C]. Guangzhou, China, 2006. 1090-1095.

[4] FOULADGAR S, AFIFI H. An efficient delegation and transfer of ownership protocol for RFID tags[A]. Proceedings of the 1st International EURASIP Workshop on RFID Technology[C]. Vienna, Austria, 2007. 68-93.

[5] SONG B. RFID tag ownership transfer[EB/OL]. http://rfidsec2013.iaik.tugraz.at/RFIDSec08/Papers/, 2008.

[6] RIZOMILIOTIS P, REKLEITIS E. Security analysis of the Song－Mitchell authentication protocol for low-cost RFID tags[J]. IEEE Communications Letters, 2009, 13(4):274-276.

[7] PERIS-LOPEZ P, HEMANDEZ-CASTRO J C, TAPIADOR J M E, *et al.* Vulnerability analysis of RFID protocols for tag ownership transfer[J]. Computer Networks, 2010, 54(9): 1502-1508.

[8] SONG B, MITCHELL C J. Scalable RFID security protocols supporting tag ownership transfer[J]. Computer Communications, 2011, 34(4): 556-566.

[9] 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.

[10] ELKHIYAOUI K, BLASS E O, MOLVA R. ROTIV: RFID ownership transfer with issuer verification[A]. LNCS7055:7th International Workshop on RFID Security and Privacy[C]. Berlin: Springer, 2012. 163-182.

[11] MORIYAMA D. Cryptanalysis and improvement of a provably secure RFID ownership transfer protocol[A]. LNCS8162: 2nd International Workshop on Lightweight Cryptography for Security and Privacy[C]. Berlin: Springer, 2013.114-129.

[12] 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):164–173.

[13] DOSS R, ZHOU W, YU S. Secure RFID tag ownership transfer based on quadratic residues[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(2):390-401.

[14] 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.

[15] 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): 581-589.
ZHOU Y B, FENG D G. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computers, 2006, 29(4): 581-589.

[16] 邓淼磊, 马建峰, 周利华. RFID 匿名认证协议的设计[J].通信学报,2009,30(7):20-26.
DENG M L, MA J F, ZHOU L H. Design of anonymous authentication protocol for RFID[J]. Journal on Communications, 2009, 30(7):20-26.

[17] 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 authentication protocol for RFID in the standard model[J]. Journal on Communications, 2013, 34(4): 82-87.

[18] CANETTI R. Universally composable security: a new paradigm for cryptographic protocols[A]. Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science[C]. Las Vegas, Nevada, USA, 2001. 136-145.

[19] 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): 1754-1767.
ZHANG F, SUN X, MA J F,*et al.* A universally compoable secure RFID communication protocol in supply chains[J].Chinese Journal of Computers,2008, 31(10): 1754-1767.

[20] BURMESTER M, TRI V L, DE MEDEIROS B, *et al.* Universally composable RFID identification and authentication protocols [J]. ACM Transactions on Information and System Security, 2009, 12(4): 1-33.

[21] BURMESTER M, MUNILLA J. Lightweight RFID authentication with forward and backward security[J]. ACM Transactions on Information and System Security, 2011, 14(1): 11.

[22] 张忠, 徐秋亮. 物联网环境下UC安全的组证明RFID协议[J]. 计算机学报, 2011, 34(7): 1188-1194.
ZHANG Z, XU Q L. Universally compoable grouping-proof protocol for RFID tags in the Internet of things[J]. Chinese Journal of Computers, 2011, 34(7): 1188-1194.

[23] CANETTI R. Obtaining universally compoable security: towards the bare bones of trust[A]. Proceedings of 13th International Conference on the Theory and Application of Cryptology and Information security[C]. 2007. 88-112.

[24] 李凤华, 冯涛, 马建峰. 基于 VSPH 的 UC 不经意传输协议[J]. 通信学报, 2007, 28(7):28-34.
LI F H, FENG T, MA J F. Universally composable oblivious transfer protocol based on VSPH[J]. Journal on Communications, 2007, 28(7):28-34.

[25] 张俊伟,马建峰,杨力. UC 安全的基于一次签名的广播认证[J]. 通信学报, 2010, 31(5):31-36.
ZHANG J W, MA J F, YANG L. UC secure one-time signature based broadcast authentication[J]. Journal on Communications, 2010, 31(5): 31-36.

[26] ZHANG J W, MA J F, MOON S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T[J]. Science China Information Sciences, 2010, 53(3): 465-482.

[27] 张俊伟, 马建峰, 杨超. 安全定位协议的 UC 模型[J]. 通信学报,2013, 34(2) : 117-122.
ZHANG J W, MA J F, YANG C. UC model of secure positioning protocols[J]. Journal on Communications, 2013, 34(2): 117-122.

作者简介：

原变青（1980-），女，山西祁县人，北京交通大学博士生，主要研究方向为安全协议、物联网安全等。

刘吉强（1973-），男，山东海阳人，北京交通大学教授、博士生导师，主要研究方向为可信计算、应用密码学、安全协议等。