计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20150555
52(10):2323-2331,2015

通用可组合安全的 RFID 标签组所有权转移协议

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)
(yuanbq@bjtu.edu.cn)

A Universally Composable Secure Group Ownership Transfer Protocol for RFID Tags

Yuan Bianqing and Liu Jiqiang
(*School of Computer and Information Technology*, *Beijing Jiaotong University*, *Beijing* 100044)

Abstract　In some applications, it is often needed to simultaneously transfer the ownership of a group of RFID (radio frequency identification) tags in a session. However, most of the existing group ownership transfer schemes for RFID tags generally require the support of a trusted third party, and they often have many security and privacy protection issues. Based on the analysis of security requirements, a secure and efficient group ownership transfer protocol for RFID tags is designed. The new protocol supports simultaneous ownership transfer of a group of RFID tags without a trusted third party. Then, in the UC(universally composable) framework, an ideal functionality capturing the secure group ownership transfer for RFID tags is formally defined, and it is proved that the new protocol realizes the above defined ideal functionality. Compared with the existing group ownership transfer protocols for RFID tags, the new protocol provides the security and privacy properties such as anonymity, untraceability, mutual authentication, authorized access, resistance to de-synchronization attack, forward privacy protection and backward privacy protection. Meanwhile, it satisfies UC security. Furthermore, the new protocol has low computational complexity. In addition, the number of storage on the tag and the number of interaction among the entities are small.

Key words　radio frequency identification (RFID); universally composable (UC); ownership transfer; protocol; Internet of things

摘　要　在某些应用中,往往需要在一次会话中同时完成一组 RFID 标签所有权的转移.然而,现有的标签组所有权转移方案大多需要可信第三方的支持且存在诸多安全和隐私保护问题.在分析安全需求的基础上,设计了一个安全高效的 RFID 标签组所有权转移协议.该协议在无可信第三方支持的情况下实现了一组标签所有权的同时转移.在通用可组合框架下,定义了 RFID 标签组所有权转移的理想函数,并证明新协议实现了所定义的理想函数.与已有同类协议相比,新协议不仅具备匿名性、不可追踪性、授权访问、抗异步攻击、前向隐私保护、后向隐私保护等安全和隐私属性,还具有通用可组合安全性.在性能方面,新方案的计算复杂度相对较低,且交互次数和标签端存储量也较少.

关键词　无线射频识别;通用可组合;所有权转移;协议;物联网

中图法分类号　TP309

收稿日期:2015-06-15;**修回日期**:2015-08-13

基金项目:教育部新世纪优秀人才支持计划基金项目(NCET-11-0565);中央高校基本科研业务费专项资金项目(2012JBZ010);教育部高校创新团队基金项目(IRT201206)

作为物联网感知层的核心技术,无线射频识别(radio frequency identification, RFID)是一种自动识别和数据获取技术.只需将 RFID 标签附着到目标实体,无需直接接触即可实现对特定目标的识别.随着物联网的快速发展, RFID 技术已广泛应用在商品生产、交通运输、物流管理以及票证管理等多个领域.然而,由于 RFID 标签资源有限且运行在开放的无线环境下,使得 RFID 系统通信容易受到窃听攻击、重放攻击与隐私攻击等各种安全威胁,因此保障协议运行的安全性非常重要.

在实际应用中,实体的所有权经常发生改变.例如生产商将商品出售给批发商后,批发商在物理上拥有了商品的所有权.然而,这并不表示批发商完全控制了该商品.如果不改变标签的所有权,生产商依然可以扫描并获取标签的信息,从而导致批发商的隐私遭到泄露.因此,RFID 标签的所有权在其生命期中也需要发生转移[1].自从 2005 年,Molnar 等人[2]首次提出 RFID 标签所有权转移协议以来,研究者们已经设计了多个单标签所有权转移协议[3-5].然而,在某些应用场景,需要在一次会话中同时完成一组标签所有权的转移.例如,某些特殊药品在出售时,要求与说明书同时出售;电子产品和其配件(如电源线等)要同时出售;汽车生产商在向批发商出售汽车时,需要保证汽车的相关零部件(如轮胎、发动机等)同时出厂.为了实现上述应用,需要设计一个安全的标签组所有权转移协议.然而,目前针对标签组所有权转移协议的研究还比较少,且大部分已有协议需要可信第三方的支持,而无可信第三方支持的标签组所有权转移协议大多无法满足组转移的安全性需求.

本文主要有以下贡献:1)设计了一个新的无需可信第三方支持的 RFID 标签组所有权转移协议,该协议可以完成标签组所有权的同时转移;2)新协议有效地解决了已有标签组所有权转移协议未能解决的易受异步攻击和无法实现后向隐私保护的问题;3)定义了标签组所有权转移协议的通用可组合(universally composable, UC)[6]模型,并在该模型下证明了新协议的安全性.

1 相关工作

2005 年,Molnar 等人[2]首次提出一个支持 RFID 标签所有权转移的匿名协议,该协议由标签新旧所有者共同信任的可信中心来控制所有的标签信息,这限制了协议的使用范围.在 2008 年,Song[7]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 个子协议来实现无可信中心的 RFID 标签所有权的转移.但经多位学者[8-9]分析,该协议存在诸多安全性问题.2011 年,Song 等人[10]对上述方案进行了改进,并提出了支持标签所有权转移的可扩展 RFID 认证协议,但改进后的方案仍不具备后向隐私保护且易受到异步攻击.2013 年,Doss 等人[11]提出了 2 个基于二次剩余的标签所有权转移方案,但 2 个方案均需要标签与新旧所有者之间执行多次交互且标签端的运算效率较低.

上述协议均为单标签所有权转移协议.如果将这些协议直接用于含 N 个标签的标签组所有权同时转移的应用场景,那么需要执行 N 次协议才能完成 1 次组转移.这种组转移实现是低效的,且难以保证标签组所有权转移的同时性.针对这种情况,Zuo[12]于 2010 年首次提出了需要可信第三方支持的标签组所有权转移协议,该协议能降低大量标签所有权同时进行转移时的通信与计算负荷,并能防止双重所有权问题.然而,Jannati 等人[13]指出该协议易受到异步攻击和冒充攻击.2011 年,Kapoor 等人[14]分析了供应链环境下存在的多种标签所有权转移的场景,并提出了一个多标签所有权同时转移协议,该协议由可信第三方完全控制多标签所有权的转移.2012 年 Yang[15]提出了适用于移动 RFID 系统的标签组所有权转移协议,该协议使用动态平衡树管理标签和标签组,但该协议不满足后向隐私保护且易遭到异步攻击.2014 年,He 等人[16]提出了一个 RFID 标签组所有权转移协议,但他们的协议同样不能保证后向隐私安全且易受到异步攻击.

2 RFID 标签组所有权转移协议模型

2.1 交互模型

一个典型的 RFID 系统通常由 3 类实体构成:后台服务器、读写器和标签.1)后台服务器一般具有较强的处理能力,它通过数据库管理其所拥有的读写器和标签的信息.2)读写器通过有线或无线的方式和后台服务器相连;通过天线与标签进行无线通信,实现对标签的识别和读写.3)标签由耦合元件及芯片组成,附着在物体上标识目标对象.由于成本因素限制,标签一般具有有限的存储空间和有限的计算能力.一般地,假设后台服务器之间有安全的通信信道,后台服务器同与其相连的读写器之间也有安全

的通信信道,而读写器与标签之间存在不安全的通信信道.

标签所有权是指标签所有者可以识别并管理标签的权力.标签组所有权转移意味着由当前所有者将一组标签的识别和管理权同时转移给新所有者.为了便于描述,在研究标签组所有权转移协议时,通常将后台服务器及与其相连的读写器看作整体,二者统一被视为一个参与方.因此,标签组所有权转移协议涉及到 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)和标签组(G),其中 $G=\{T_i|1\leqslant i\leqslant m\}$,$T_i$ 为 G 内的某个标签,m 表示 G 内标签的数量.一般地,标签组所有权转移要经历 3 个步骤:1)组认证.即 CS 认证标签组 G 中的所有标签同时存在.2)组授权.即 CS 将标签组 G 及组内标签的业务信息同时传送给 NS.3)秘密更新.即 NS 与 T_i 同步更新组秘密及标签秘密,从而安全地实现标签组 G 所有权的同时转移.

2.2 敌手模型

假设敌手 A 能够完全控制 CS(或 NS)与标签组之间的通信信道,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意参与方的会话.敌手 A 的攻击方法主要有: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.本文暂不讨论对标签的物理攻击.对于其他参与方,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.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.

2.3 安全模型

一个安全的标签组所有权转移协议需要满足以下安全和隐私属性:

1) 匿名性.任意的敌手 A,通过截获 CS(或 NS)与标签组 G 内每个标签之间的交互信息,无法获得标签组 G 或组内任意标签 T_i 的身份信息.

2) 不可追踪性.任意的敌手 A,通过截获 CS(或 NS)与标签组 G 之间的交互信息,无法追踪到标签组 G 及组内任意标签 T_i.

3) 授权访问.任意的敌手 A,在未获得 CS 授权的情况下,无法访问标签组 G 内任意标签 T_i.

4) 双向认证.只有在 CS 成功认证 G 中每个标签 T_i 同时存在,而且每个标签 T_i 也成功认证 CS 后,才能进行标签秘密的更新,从而完成标签组 G 的所有权的转移.

5) 抗异步攻击.任意的敌手 A 通过任意手段中断标签组所有权转移过程,使得 CS(或 NS)与标签的信息同步失败后,协议仍可以保证标签认证的再次成功,并实现信息的同步.

6) 前向隐私保护.标签组所有权转移之后,新所有者 NS 不能访问所有权转移前标签组 G 内任意标签 T_i 与原所有者 CS 之间的会话信息.

7) 后向隐私保护.标签组所有权转移之后,原所有者 CS 不能再识别标签组 G 内的任意标签 T_i,也无法访问标签组 G 内任意标签 T_i 和新所有者 NS 的会话信息.

3 RFID 标签组所有权转移协议

本节提出一个符合安全和隐私保护需求的轻量级 RFID 标签组所有权转移协议 π_{GOT},如图 1 所示.

表 1 给出符号的定义:

Table 1 Symbol Notations

表 1 符号定义

Notation	Description
l	Length of a random string or a secret key
$PRNG(\ )$	Pseudo-random number generator
K_G	Shared secret key among a group of tags
K_i	Secret key of T_i
$Info(G)$	The information related to G
$Info(T_i)$	The information related to T_i
$\|$	Concatenation operator
$\in_R$	Random choice operator
$\leftarrow$	Substitution operator
$\oplus$	Bitwise XOR (exclusive OR) operator

初始时,在所有者的后台数据库中,每个标签组对应一条记录$(K_G, Info(G))$,组内每个标签对应一条记录$(K_i, Info(T_i), K_G)$.NS 选取 2 个大素数 $p\in_R\{0,1\}^l$,$q\in_R\{0,1\}^{l+1}$,其中 $p=q=3 \bmod 4$;然后计算 $n=pq$,并公开 n 给 CS.标签 T_i 中存储 K_i,K_G,n.下面给出具体的协议步骤描述.

Step1. $CS\rightarrow NS$:

CS 选取随机数 $r_{CS}\in_R\{0,1\}^l$,计算 $MC=PRNG(K_G\oplus r_{CS})$,并向 NS 发送授权访问消息$\langle r_{CS}, MC\rangle$.

Step2. $NS\rightarrow T_i$:

NS 选取随机数 $r_{NS}\in_R\{0,1\}^l$,计算 $MN=PRNG(r_{NS}\oplus MC)$,并向标签组广播消息$\langle r_{CS}, r_{NS}, MN\rangle$.

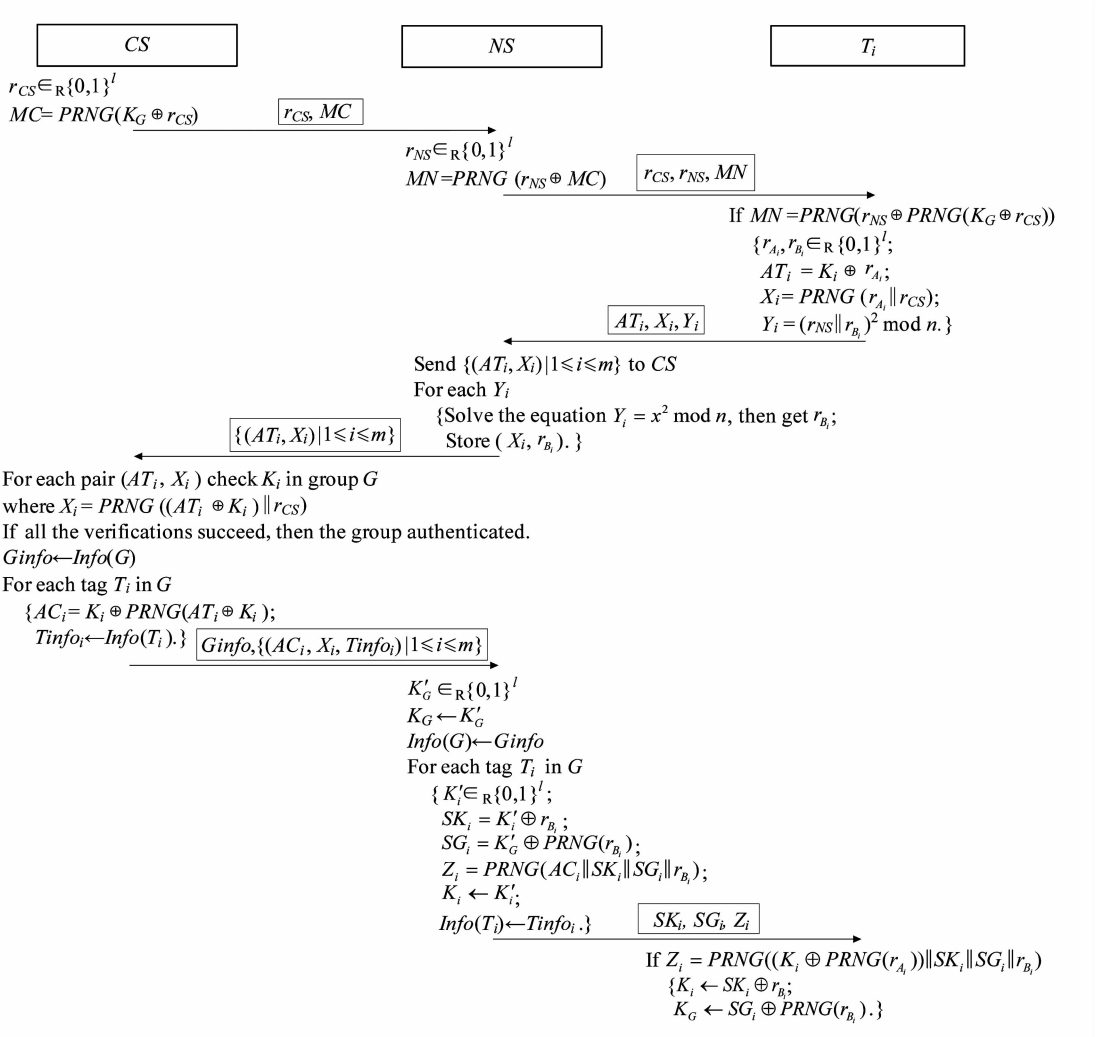


Fig. 1 Group ownership transfer protocol for RFID tags: π_{GOT}.

图 1 RFID 标签组所有权转移协议：π_{GOT}

Step3. $T_i \rightarrow NS$:

收到 NS 的挑战消息后，T_i 验证等式 $PRNG(r_{NS} \oplus PRNG(K_G \oplus r_{CS})) = MN$ 是否成立. 如果等式不成立，则终止执行；否则，T_i 随机选取 $r_{A_i} \in_R \{0,1\}^l$，$r_{B_i} \in_R \{0,1\}^l$，计算 $AT_i = K_i \oplus r_{A_i}$，$X_i = PRNG(r_{A_i} \| r_{CS})$，$Y_i = (r_{NS} \| r_{B_i})^2 \bmod n$，并向 NS 发送响应消息 $\langle AT_i, X_i, Y_i \rangle$.

Step4. $NS \rightarrow CS$:

NS 接收到每个标签 T_i 的响应消息后，得到集合 $\{(AT_i, X_i, Y_i) | 1 \leqslant i \leqslant m\}$，并在预定时间内向 CS 发送响应消息集合 $\{(AT_i, X_i) | 1 \leqslant i \leqslant m\}$；然后，对每个 Y_i，NS 解方程 $Y_i = x^2 \bmod n$. 根据中国剩余定理，计算可得到 4 个解：x_1, x_2, x_3, x_4. 如果能找到左 l 位等于 r_{NS} 的解 x_i，$1 \leqslant i \leqslant 4$，那么该解的右 l 位即为 r_{B_i}；然后 NS 存储集合 $\{(X_i, r_{B_i}) | 1 \leqslant i \leqslant m\}$；否则，停止协议过程.

Step5. $CS \rightarrow NS$:

① CS 检查收到的消息集合中消息对 (AT_i, X_i) 的数量是否与数据库中存储的待转移的标签组 G 中的标签数一致. 如果数量一致则继续验证；否则，停止协议执行.

② 对每一个消息对 (AT_i, X_i)，在标签组 G 中查找使等式 $X_i = PRNG((AT_i \oplus K_i) \| r_{CS})$ 成立的 K_i. 如果每一个消息对均能找到与之对应的 K_i，则说明标签组 G 中的每个标签 T_i 是同时存在的；否则，停止协议执行.

③ CS 执行命令 $Ginfo \leftarrow Info(G)$；然后，对 G 中的每个标签 T_i，计算 $AC_i = K_i \oplus PRNG(AT_i \oplus K_i)$，并执行命令 $Tinfo_i \leftarrow Info(T_i)$；最后，向 NS 发送授权转移消息 $\langle Ginfo, \{(AC_i, X_i, Tinfo_i) | 1 \leqslant i \leqslant m\} \rangle$.

Step6. $NS \rightarrow T_i$:

一旦收到 CS 发送的授权转移消息，NS 查询其数据库中是否存在 $Info(G) = Ginfo$ 的 $(K_G,$

$Info(G)$)对. 如果存在,则令 $K'_G=K_G$;否则,选取随机数 $K'_G\in_R\{0,1\}^l$ 作为标签组 G 的新秘密,并更新数据库:$K_G\leftarrow K'_G$, $Info(G)\leftarrow Ginfo$. 然后,对 G 中的每一个标签 T_i,选取随机数 $K'_i\in_R\{0,1\}^l$,计算 $SK_i=K'_i\oplus r_{B_i}$, $SG_i=K'_G\oplus PRNG(r_{B_i})$, $Z_i=PRNG(AC_i\|SK_i\|SG_i\|r_{B_i})$,并更新数据库:$K_i\leftarrow K'_i$, $Info(T_i)\leftarrow Tinfo_i$. 最后,分别向标签 T_i 发送秘密更新消息$\langle SK_i,SG_i,Z_i\rangle$.

Step7. T_i:

收到 NS 发送的秘密更新消息后,T_i 验证 $PRNG((K_i\oplus PRNG(r_{A_i}))\|SK_i\|SG_i\|r_{B_i})=Z_i$ 是否成立. 如果等式不成立,则终止协议执行;否则,更新 $K_i\leftarrow SK_i\oplus r_{B_i}$, $K_G\leftarrow SG_i\oplus PRNG(r_{B_i})$.

为了保证标签组转移的原子性,协议执行完成后可由 NS 采用安全的标签组认证协议扫描 G. 如果扫描到的标签与 CS 在 Step5 中发送的标签一一对应,则表示标签组所有权转移成功;否则,需要对未成功转移的组内标签重新执行协议 π_{GOT}.

4 协议 π_{GOT} 的安全性证明

本节简要介绍通用可组合安全的定义,给出 RFID 标签组所有权转移的理想函数,证明协议 π_{GOT} 是 UC 安全的.

4.1 通用可组合安全

通用可组合框架(UC 框架)是由 Canetti[6] 提出的描述和分析并发环境下密码协议安全性的理论框架. 如果一个协议在该框架下被证明为安全的,则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,该协议仍然保持安全. 这个特征对于在复杂和不可预测的无线通信环境下保持 RFID 应用协议的安全性是非常重要的[17]. 在 UC 框架下,许多学者分析和设计了各种 RFID 协议[18-20].

UC 框架定义了 2 种协议运行模型: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 类实体:环境机 Z、执行协议 π 的多个参与方$\{P_i\}$以及现实敌手 A;理想模型则用来描述密码协议的理想运行. 理想过程通常被形式化定义为一个特殊的协议,该协议的重要组成部分称为理想函数. 理想函数通过一组指令描述特定任务的功能和安全性需求. 理想模型中主要涉及的实体包括环境机 Z、通过虚拟用户$\{\widetilde{P}_i\}$与环境机 Z 进行交互的理想函数 F 以及理想过程敌手 S. 在 UC 框架下,协议的安全性是通过比较现实模型中的协议执行和该任务的理想过程而定义的.

定义 1. 我们称协议 π 安全地实现了理想函数 F,如果对于任意敌手 A,存在理想过程敌手 S,使得环境机 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. 即:

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

4.2 理想函数 F_{GOT}

基于 RFID 标签组所有权转移的敌手模型和安全模型,本节形式化地定义标签组所有权转移的理想函数 F_{GOT}.

由于标签组 $G=(T_1,T_2,\cdots,T_m)$和 CS 的所属关系是标签组所有权转移的前提,因此理想函数 F_{GOT}使用所有权集合$\{CS,G,K_G,(T_1,t_1),(T_2,t_2),\cdots,(T_i,t_i),\cdots,(T_m,t_m)\}$表示 CS 和标签组 G 的所有关系. 其中 K_G 为任意随机数,表示标签组 G 的组密钥;t_i 为任意随机数,表示标签 T_i 的密钥.

1) 一旦收到 CS 发送的消息(Init,sid,CS,NS,K_G),记录(sid,CS,NS,K_G),其中 sid 为本次的会话标识.

2) 一旦收到 NS 发送的消息(Init,sid,NS,K_G),传送(sid,$Type(NS)$,$|K_G|$)给敌手 S,其中 $Type(NS)$指参与方 NS 的类型;然后检查包含(NS,K_G)的记录是否存在. 如果记录存在,则继续执行;否则,终止执行.

3) 一旦收到 T_i 发送的消息(Init,sid,T_i,K_G),传送(sid,$Type(T_i)$,$|K_G|$)给敌手 S.

4) 一旦收到来自敌手 S 的认证消息(Authed,sid,CS,T_i,t'_i),检查包含(CS,(T_i,t_i))的记录是否存在. 如果记录存在,修改(T_i,t_i)为(T_i,t_i,v_i),其中 v_i 的值由下列情况决定:

① 如果存在 $t'_i=t_i$,则令 $v_i=$success.

② 如果存在 $t'_i\neq t_i$,则分 2 种情况:Ⅰ 如果 CS 已被攻破,由 S 决定 v_i 的值;Ⅱ 如果 CS 没有被攻破,则令 $v_i=$fail.

如果修改后的所有权集合$\{CS,G,K_G,(T_1,t_1,v_1),(T_2,t_2,v_2),\cdots,(T_i,t_i,v_i),\cdots,(T_m,t_m,v_m)\}$中每个 v_i 的值均为 success,则记录(Authed,sid,CS,G,success);否则,记录(Authed,sid,CS,G,fail).

5) 一旦收到来自敌手 S 的认证消息(Authed,sid,T_i,CS,t''_i),检查包含(CS,(T_i,t_i))的记录是否存在. 如果记录存在且 $t''_i=t_i$,那么记录(Authed,sid,T_i,CS,success);否则,记录(Authed,sid,T_i,CS,fail).

6) 一旦收到 CS 发送的消息(Transfer,sid,CS,NS,G),选择随机数 k,并记录(sid,CS,NS,G,k).

7) 一旦收到 S 发送的消息(Update, sid, NS, G, k', T_i, γ_i),检查记录(Authed, sid, CS, G, success),(Authed, sid, T_i, CS, success),(sid, CS, NS, G)是否全部存在:

① 如果记录都存在且 NS 没有被攻破,则为该标签选择随机数 α_i,并添加记录(sid, NS, G, T_i, α_i). 如果对于 G 中每一个 T_i,都有一条记录(sid, NS, G, T_i, α_i)存在,则产生新所有权集合(NS, G, k, (T_1, α_1), (T_2, α_2), …, (T_i, α_i), …, (T_m, α_m));然后,对于 G 中每一个 T_i,发送(Output, sid, NS, k, α_i)给 NS,并删除所有的(sid, NS, G, T_i, α_i)记录.

② 如果记录都存在且 NS 已被攻破,更新记录(sid, CS, NS, G, k)中的 k 为 k',并添加记录(sid, NS, G, T_i, γ_i). 如果对于 G 中每一个 T_i,都有一条记录(sid, NS, G, T_i, γ_i)存在,则产生新所有权集合(NS, G, k', (T_1, γ_1), (T_2, γ_2), …, (T_i, γ_i), …, (T_m, γ_m));然后,对于 G 中每一个 T_i,发送(Output, sid, NS, k', γ_i)给 NS,并删除所有的(sid, NS, G, T_i, γ_i)记录.

③ 如果有一条记录不存在,则返回失败.

8) 一旦收到 S 发送的消息(Update, sid, T_i, k'', β_i),检查新所有权集合中是否存在 T_i 项:如果不存在,则返回失败;否则,得到形如(NS, G, k_G, (T_i, χ_i))的记录,发送(Output, sid, T_i, k_G, χ_i)给 T_i. 然后,删除旧所有权集合中的 T_i 项. 如果此时旧所有权集合中的标签项已不存在,则删除整个集合.

9) 如果在选择随机数 k 或 α_i 后,敌手 S 攻破了 NS,则将 k 或 α_i 发送给敌手 S.

下面证明理想函数 F_{GOT} 满足 2.3 节定义的安全和隐私需求.

1) 匿名性. 敌手在不安全信道中仅能获得标签组身份信息的长度 $|K_G|$ 和标签类型 $Type(T_i)$,而无法获得标签组或组内任意标签 T_i 的身份信息,这保证了标签组及标签的匿名性.

2) 不可追踪性. 敌手在不安全信道中仅能获得标签组身份信息的长度 $|K_G|$ 和标签类型 $Type(T_i)$,而无法根据这些信息追踪到标签组 G 及组内任意标签 T_i.

3) 授权访问. 收到 NS 发送的消息(Init, sid, NS, K_G)后,F_{GOT} 首先检查记录(sid, CS, NS, K_G)是否存在. 只有记录存在(即 NS 获得 CS 授权)的情况下,F_{GOT} 才继续执行.

4) 双向认证. 只有在记录(Authed, sid, CS, G, success),(Authed, sid, T_i, CS, success)全部存在时,即 CS 成功认证 G 中每个标签 T_i 同时存在且标签 T_i 也成功认证 CS 后,F_{GOT} 才执行秘密更新操作,进而实现标签组所有权的转移.

5) 抗异步攻击. 敌手 S 在执行指令(Update, sid, NS)和(Update, sid, T_i)时,可能通过各种手段使得 CS(或 NS)和标签 T_i 的信息不同步. 此时,如果新所有权集合中已包含 T_i 项,则在执行指令(Update, sid, T_i)后信息会再次同步;否则,由于旧所有权集合中的 T_i 项还未被删除,所以重启理想过程仍可以保证标签 T_i 再次被成功认证.

6) 前向隐私保护. 在标签组所有权转移过程中,NS 只能获得更新后的组秘密和组内标签的秘密,而无法获得原有的组秘密和组内标签的秘密. 因此 NS 无法访问所有权转移前标签 T_i 与原所有者 CS 之间的会话信息.

7) 后向隐私保护. 当标签组所有权成功转移之后,即指令(Update, sid, T_i)执行后,标签的原所有权集合中的 T_i 项将被清除,并且更新后的秘密对 CS 是保密的. 因此,CS 不能再识别标签 T_i,也无法访问标签 T_i 和新所有者 NS 的会话信息.

4.3 安全性证明

定理 1. 协议 π_{GOT} 安全地实现了理想函数 F_{GOT}.

证明. 1)构建理想敌手 S. 令 A 为与真实协议 π_{GOT} 交互的任意敌手,S 仿真 A 与运行 π_{GOT} 的各参与方的交互,具体操作如下:

(1) 任何来自环境机 Z 的输入均被转发给 A. 任何来自 A 的输出被拷贝作为 S 的输出,并被 Z 读取.

(2) 仿真 CS 的激活. S 选择随机数 r_{CS},并计算 $MC = PRNG(K_G \oplus r_{CS})$.

(3) 仿真 NS 的激活. 收到来自 F_{GOT} 的消息(sid, $Type(NS)$, $|K_G|$)后,S 选择随机数 r_{NS},并计算 $MN = PRNG(r_{NS} \oplus MC)$;然后,将($r_{CS}$, r_{NS}, MN)传给 A.

(4) 仿真 T_i 的激活. 当 A 传送(r'_{CS}, r'_{NS}, MN')给 T_i 时,S 首先验证它在理想过程中已经收到来自 F_{GOT} 的(sid, $Type(T_i)$, $|K_G|$). 然后,S 验证等式 $PRNG(r'_{NS} \oplus PRNG(K_G \oplus r'_{CS})) = MN'$ 是否成立:如果成立,S 选择随机数 r_{A_i} 和 r_{B_i},并将由 T_i 发送的消息(AT_i, X_i, Y_i)传给 A,其中 $AT_i = K_i \oplus r_{A_i}$, $X_i = PRNG(r_{A_i} \| r'_{CS})$, $Y_i = (r'_{NS} \| r_{B_i})^2 \bmod n$;否则,返回失败,协议终止.

(5) 仿真 NS 收到 T_i 的响应消息. 待 NS 收到 A 传送的所有响应消息$\{(AT'_i, X'_i, Y'_i) \mid 1 \leqslant i \leqslant m\}$后,

S 发送消息集合$\{(AT'_i, X'_i) \mid 1 \leqslant i \leqslant m\}$给 CS;然后,S 根据 Y'_i 解得 r'_{B_i} 并存储$\{(X'_i, r'_{B_i}) \mid 1 \leqslant i \leqslant m\}$.

(6) 仿真 CS 收到要求认证的消息. 当收到来自 NS 的消息集合$\{(AT'_i, X'_i) \mid 1 \leqslant i \leqslant m\}$,$S$ 检查消息集合中消息对的数量是否与标签组 G 中标签的数量一致. 如果不一致,则停止协议执行;否则,对每一个消息对$\{(AT'_i, X'_i) \mid 1 \leqslant i \leqslant m\}$,在标签组 G 中查找使等式 $X'_i = PRNG((K_i \oplus AT'_i) \| r_{CS})$成立的 K_i:

① 如果每一个消息对均能找到与之对应的 K_i,则传送$\langle Ginfo, \{(AC_i, X'_i, Tinfo_i) \mid 1 \leqslant i \leqslant m\}\rangle$给 NS,其中 $Ginfo = Info(G)$,$AC_i = K_i \oplus PRNG(AT'_i \oplus K_i)$,$Tinfo_i = Info(T_i)$. 同时,在理想环境下,对应每个标签分别传送(Authed, sid, CS, T_i, K_i)给 F_{GOT}.

② 如果存在消息对没有找到对应的 K_i,则返回认证失败,协议终止. 同时,在理想环境下,对应每个标签分别传送(Authed, sid, CS, T_i, t'_i)给 F_{GOT},其中 t'_i 为 S 选择的任意随机数.

(7) 仿真 NS 发送更新秘密的消息. S 转发从 NS 收到的(SK_i, SG_i, Z_i)给敌手 A,其中,$SK_i = k_i \oplus r'_{B_i}$,$SG_i = k_G \oplus PRNG(r'_{B_i})$,$Z_i = PRNG(AC_i \| SK_i \| SG_i \| r'_{B_i})$,且 k_i 和 k_G 为 S 选择的任意随机数.

(8) 仿真标签 T_i 收到更新秘密的消息. 当 A 传送消息(SK'_i, SG'_i, Z'_i)给标签 T_i 时,T_i 判断等式 $PRNG((K_i \oplus PRNG(r_{A_i})) \| SK'_i \| SG'_i \| r_{B_i}) = Z'_i$ 是否成立:

① 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_i, CS, t''_i)给 F_{GOT},其中 t''_i 为 S 选择的任意随机数.

② 如果等式成立,计算 $k_i = SK'_i \oplus r_{B_i}$,$k_G = SG'_i \oplus PRNG(r_{B_i})$. 在理想环境下,$S$ 先传送(Authed, sid, T_i, CS, K_i)给 F_{GOT},然后再传送(Update, sid, NS, G, k_G, T_i, k_i)给 F_{GOT}. 一旦 F_{GOT} 传送了 Output 消息给 NS,S 也立即传送该消息. 最后,更新 T_i 的身份信息和组秘密:$K_i \leftarrow k_i$,$K_G \leftarrow k_G$. 同时,在理想环境下,传送(Update, sid, T_i, k_G, k_i)给 F_{GOT}. 一旦 F_{GOT} 传送了 Output 消息给 T_i,S 也立即传送该消息.

(9) 仿真 CS(或是 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.

2) 分析仿真器 S 的合法性,即对于环境机 Z 而言,理想函数 F_{GOT} 和真实协议 π_{GOT} 是不可区分的.

下面定义事件 NSC 和 CSC. ①事件 NSC 表示 NS 被攻破的事件,也就是在 NS 和标签 T_i 更新秘密之前,敌手 A 攻破了 NS. 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. ②事件 CSC 表示 CS 被攻破的事件,也就是在 CS 认证标签组 G 之前,敌手 A 攻破了 CS. 在理想环境下,事件 CSC 表示在 S 发送(Authed, sid, CS, T_i, t'_i)指令之前,仿真的 A 攻破参与方 CS 的事件. 根据 UC 框架[6] 的设定,事件 NSC 和 CSC 不会同时发生.

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

当 NSC 发生时,事件 CSC 不会发生. 那么,在现实环境中,对于环境机 Z 而言,敌手 A 和真实协议 π_{GOT} 交互后,输出的值为 k_i 和 k_G,其中 $k_i = SK'_i \oplus r_{B_i}$,$k_G = SG'_i \oplus PRNG(r_{B_i})$. 而在理想环境中,在更新秘密阶段,在 S 中仿真的现实敌手 A 用指令(Update, sid, NS, G, k_G, T_i, k_i)传送同样的 k_i 和 k_G 给 F_{GOT},并最后由 F_{GOT} 输出 k_i 和 k_G 给 NS. 同样,在执行指令(Update, sid, T_i, k_G, k_i)后,标签 T_i 也得到同样的 k_i 和 k_G. 因此,对于环境机 Z 而言,在 NSC 发生时,真实协议 π_{GOT} 和理想函数 F_{GOT} 的输出是完全相同的.

当事件 NSC 没有发生时,无论事件 CSC 是否发生,在现实环境中,对于环境机 Z 而言,敌手 A 和真实协议 π_{GOT} 交互后,输出的值为 K'_i 和 K'_G,其中 $K'_i \in_{\mathrm{R}} \{0,1\}^l$,$K'_G \in_{\mathrm{R}} \{0,1\}^l$. 而在理想环境中,在 S 中仿真的现实中的 A 与理想函数 F_{GOT} 交互后,由 F_{GOT} 输出 k_i 和 k_G 给 NS 和 T,其中 k_i 和 k_G 均为随机数. 由于随机数 K'_i,K'_G,k_i 和 k_G 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_{GOT} 交互后的输出和 S 与理想函数 F_{GOT} 交互后的输出也是不可区分的.

引理 2. 无论事件 CSC 发生与否,对于环境机 Z 而言,理想函数 F_{GOT} 和真实协议 π_{GOT} 都是不可区分的,即 $IDEAL_{F_{\mathrm{GOT}}, S, Z} \approx REAL_{\pi_{\mathrm{GOT}}, A, Z}$.

根据引理 1,无论事件 CSC 发生与否,对于环境机 Z 而言,理想函数 F_{GOT} 和真实协议 π_{GOT} 都是不可区分的.

综上,对于任意现实敌手 A,存在理想过程敌手 S,使得环境机 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_{GOT} 的参与方

交互还是在与理想环境中的 S 和理想函数 F_{GOT} 交互,即 $IDEAL_{F_{GOT},S,Z} \approx REAL_{\pi_{GOT},A,Z}$. 根据定义 1,定理 1 得证. 证毕.

5 安全性与性能比较

本节对本文提出的协议与已有的典型协议进行比较. 表 2 给出了协议间安全和隐私属性的比较,其中"√"表示满足该安全属性,"×"表示不满足该安全属性. 表 3 给出了协议间性能的比较,其中 Pr 表示 PRNG 运算,Pc 表示 CRC 运算,Ph 表示单向 Hash 函数运算,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. 运算量统计是基于每个标签组内标签个数为 M 的情况.

Table 2 Comparison of Security and Privacy Properties

表 2 安全和隐私属性比较

Schemes	Anonymity	Untraceability	Mutual Authentication	Authorized Access	Resistance to Desynchronization Attack	Forward Privacy Protection	Backward Privacy Protection	UC Security
Ref[11] (Open Loop Scheme)	√	√	√	×	√	√	×	×
Ref[15]	√	√	√	√	×	√	×	×
Ref[16]	√	√	√	√	×	√	×	×
Our Scheme	√	√	√	√	√	√	√	√

Table 3 Comparison of Performance Properties

表 3 性能比较

Schemes	Number of Storage on T_i	Computation Cost of T_i	Computation Cost of CS	Computation Cost of NS	Number of Messages
Ref[11] (Open Loop Scheme)	4	4Pm+5Pr+Pc	$2M$Ps+MPr+MPc	$2M$Ps+$3M$Pr	$10M$
Ref[15]	4	3Pe	$9M$Pe	$4M$Pe	$5M+1$
Ref[16]	4	9Ph	$(4M+1)$ Ph	$(3M+1)$ Ph	$3M+5$
Our Scheme	3	6Pr+Pm	$M[1+O(M)/2]$ Pr+Pr	$(2M+1)$Pr+MPs	$2M+4$

从表 2 和表 3 可以看出,Yang[15]和 He 等人[16]提出的方案性能相对较高,但 2 个方案均无法抵抗异步攻击,也无法满足后向隐私保护. 作为单标签所有权转移协议,Doss 等人[11]的方案用于标签组所有权转移时,协议的交互次数明显增多且运算量相对较大,因此该方案效率最低. 此外,上述协议均不具备通用可组合安全性. 新协议不仅满足了匿名性、不可追踪性、授权访问、前向隐私保护等安全需求,更有效地解决了已有标签组所有权转移协议存在的易受异步攻击和无法实现后向隐私保护的问题. 此外,本文还证明了新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相对较低,且标签端存储量和实体间交互次数也较少.

6 结 论

近年来,RFID 技术已被广泛应用在各种场景. 然而,由于标签资源有限且运行在开放的无线通信环境下,因此保证系统的安全和隐私性是设计 RFID 应用协议时需要考虑的重点问题. 针对 RFID 标签组所有权经常需要转移的实际问题,本文详细地分析和描述了标签组转移方案的交互模型、敌手模型和安全模型. 在此基础上,设计了一个安全、高效的轻量级 RFID 标签组所有权转移协议. 随后在 UC 框架下,形式化证明了新协议的安全性.

参 考 文 献

[1] Lim C H, Kwon T. Strong and robust RFID authentication enabling perfect ownership transfer [G] //LNCS 4307: Proc of the 8th Int Conf on Information and Communications Security. Berlin: Springer, 2006: 1-20

[2] Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags [G] //LNCS 3897: Proc of the 12th Int Workshop on Selected Areas in Cryptography. Berlin: Springer, 2006: 276-290

[3] Kulseng L, Yu Z, Wei Y, et al. Lightweight mutual authentication and ownership transfer for RFID systems [C] //Proc of IEEE INFOCOM 2010. Piscataway, NJ: IEEE, 2010: 1-5

[4] 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 (in Chinese)
(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)

[5] Kapoor G, Piramuthu S. Single RFID tag ownership transfer protocols [J]. IEEE Trans on Systems, Man, and Cybernetics—Part C: Applications and Reviews, 2012, 42(2):164-173

[6] Canetti R. Universally composable security: A new paradigm for cryptographic protocols [C] //Proc of the 42nd IEEE Symp on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society, 2001: 136-145

[7] Song B. RFID tag ownership transfer [C/OL] //Proc of the Workshop on RFID Security. 2008 [2015-07-21]. http://rfidsec2013. iaik. tugraz. at/RFIDSec08/Papers

[8] 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

[9] 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

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

[11] Doss R, Zhou W, Yu S. Secure RFID tag ownership transfer based on quadratic residues [J]. IEEE Trans on Information Forensics and Security, 2013, 8(2): 390-401

[12] Zuo Y. Changing hands together: A secure group ownership transfer protocol for RFID tags [C] //Proc of the 43rd Hawaii Int Conf on System Sciences. Piscataway, NJ: IEEE, 2010: 1-10

[13] Jannati H, Falahati A. Cryptanalysis and enhancement of a secure group ownership transfer protocol for RFID tags [C] //Proc of the 7th Int Global Security, Safety and Sustainability and the 4th e-Democracy Joint Conf. Berlin: Springer, 2012: 186-193

[14] Kapoor G, Zhou W, Piramuthu S. Multi-tag and multi-owner RFID ownership transfer in supply chains [J]. Decision Support Systems, 2011, 52(1): 258-270

[15] Yang M H. Secure multiple group ownership transfer protocol for mobile RFID [J]. Electronic Commerce Research and Applications, 2012, 11(4): 361-373

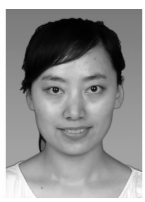
[16] He L, Gan Y, Yin Y. Secure group ownership transfer protocol for tags in RFID system [J]. International Journal of Security and Its Applications, 2014, 8(3): 21-30

[17] Zhang Fan, Sun Xuan, Ma Jianfeng, et al. A universally composable secure RFID communication protocol in supply chains [J]. Chinese Journal of Computers, 2008, 31(10): 1754-1767 (in Chinese)
(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)

[18] Burmester M, Van Le T, De Medeiros B, et al. Universally composable RFID identification and authentication protocols [J]. ACM Trans on Information and System Security, 2009, 12(4): 1-33

[19] Zhang Zhong, Xu Qiuliang. Universally composable grouping-proof protocol for RFID tags in the Internet of Things [J]. Chinese Journal of Computers, 2011, 34(7): 1188-1194 (in Chinese)
(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)

[20] Burmester M, Munilla J. Lightweight RFID authentication with forward and backward security [J]. ACM Trans on Information and System Security, 2011, 14(1): 1165-1182



Yuan Bianqing, born in 1980. PhD candidate at Beijing Jiaotong University. Her current research interests include protocol design and RFID security.

Liu Jiqiang, born in 1973. Professor and PhD supervisor at Beijing Jiaotong University. His main research interests include trusted computing, privacy preserving, security protocol.