计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(11):259−264 [doi: 10.15888/j.cnki.csa.006641]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

一种适用于标签组的所有权转移协议①

于　仕[1], 付萍萍[1], 卓明旺[2], 李　彬[1], 江　虹[1]

[1](国网江西省电力有限公司信息通信分公司, 南昌 330077)
[2](南京南瑞集团公司信息系统集成分公司, 南京 211106)
通讯作者: 于　仕, E-mail: zhuomingwang@126.com

摘　要: 在实际应用中, 经常会遇到一次通话需转移多个标签的所有权问题, 现有的绝大多数所有权转移协议只适用于单标签所有权的转移, 为解决该问题, 设计出一种适用于多标签的所有权转移协议. 所提协议无需依赖可信第三方, 从而可以减少系统中的通信实体数; 协议基于中国剩余定理及交叉位运算对传输消息进行加密, 确保通信消息的安全可靠; 在一次通话过程中, 协议能够同时转移多个标签的所有权. 基于 BAN 逻辑形式化给出数学证明过程, 并对协议进行安全性及性能分析, 表明协议具备所有权转移所需的安全性及较低的计算量.

关键词: 无线射频识别; 所有权转移; 群组标签; 交叉位运算

引用格式: 于仕,付萍萍,卓明旺,李彬,江虹.一种适用于标签组的所有权转移协议.计算机系统应用,2018,27(11):259–264. http://www.c-s-a.org.cn/1003-3254/6641.html

Ownership Transfer Protocol for RFID Tags

YU Shi[1], FU Ping-Ping[1], ZHUO Ming-Wang[2], LI Bin[1], JIANG Hong[1]

[1](Information Communication Branch, State Grid Jiangxi Electric Power Co. Ltd., Nanchang 330077, China)
[2](Information System Integration Company, Nari Group Corporation, Nanjing 211106, China)

Abstract: In practical applications, the ownership problem of multiple tags is often encountered in one call. Most of the existing ownership transfer protocols are applicable only to the transfer of single label ownership. In order to solve the problem, a multi label transfer protocol is designed. The proposed protocol can reduce the number of communication entities in the system without relying on trusted third parties. The protocol encrypts the transmission message based on the Chinese Remainder Theorem and word Cro operation to ensure the safety and reliability of communication messages. In the process of one call, the protocol can transfer the ownership of multiple labels simultaneously. Based on the logic formalization of BAN, the mathematical proof process is given, and the security and performance of the protocol are analyzed. It shows that the protocol has the security and low computation needed for the transfer of ownership.

Key words: RFID; ownership transfer; the group of tags; Cro operation

无线射频识别 (Radio Frequency IDentification, RFID) 是一种自动识别和数据获取技术, 只需要将 RFID 标签附着在目标实体上, 无需直接接触目标实体就可以实现对选定目标的识别[1−3]. 具有体积小、寿命长等优点, 已被广泛应用在商品生产、交通运输等各个领域[4−6]. 在应用中, 通信实体的所有权会不断的发生改变, 比如: 生产者将商品卖给批发商, 商品的所有权就会发生改变, 所有权不再属于生产者, 然而生产者却依旧有可能获取该商品的信息, 而导致批发商的隐私信息遭到泄漏[7−9]. 为了解决上述存在的问题, 需设计出安全的所有权转移协议.

Molnar 等人在 2005 年首次提出 RFID 标签所有

① 收稿时间: 2018-04-12; 采用时间: 2018-05-14; csa 在线出版时间: 2018-10-24

权转移协议, 但是该协议每次通话只能完成一个标签的所有权转移, 使用范围受到局限[10]; Zuo 等人在 2010 年首次提出 RFID 标签组所有权转移协议, 该协议可以一次通话完成一组标签所有权的转移, 但该协议基于可信第三方, 使其应用也具有一定的局限, 同时该协议无法抵抗异步攻击和假冒攻击[11]; Yang 等人在 2012 年提出了一个适用移动 RFID 系统的 RFID 标签组所有权转移协议, 分析发现, 该协议无法抵抗异步攻击, 同时协议也无法满足后向隐私的安全需求[12]; He 等人在 2014 年提出了一个 RFID 标签组所有权转移协议, 但分析发现, 该协议仍无法抵抗去同步化攻击, 同时不能保证后向隐私的安全性[13]. 原变青等人在 2015 年提出了一个通用可组合安全的 RFID 标签组所有权转移协议, 但分析发现, 该协议无法抵抗暴力破解攻击, 攻击者通过强制手段, 可以暴力破解出标签的相关隐私[14]. 在总结上述协议基础之上, 提出一种适用于的多标签的所有权转移协议. 在所提协议中, 信息通过字合成运算加密后再传输, 使得攻击者只能获取密文; 同时在所提协议中, 保证每个传输的信息中, 都至少有两个以上的量是攻击者事前无法知晓的, 从而使得攻击者无法进行暴力破解攻击; 通过 BAN 逻辑形式证明了协议的正确性.

1 本文协议

1.1 符号说明

对协议中出现的符号进行如下说明:

A: 标签原所有者;

B: 标签新所有者;

T_a: 群组标签 (其中 a 表示群组标签的总个数);

T_i: 群组标签中编号为 i 的标签;

V: 群组标签 T_a 与标签原所有者 A 之间共享的密钥;

U: 群组标签 T_a 与标签新所有者 B 之间共享的密钥;

V_i: 群组标签 T_a 中编号为 i 的标签与标签原所有者 A 之间共享的认证密钥;

U_i: 群组标签 T_a 中编号为 i 的标签与标签新所有者 B 之间共享的认证密钥;

x: 标签原所有者 A 产生的一个随机数;

y: 标签新所有者 B 产生的一个随机数;

z_i、w_i: 群组标签 T_a 中编号为 i 的标签产生的两个随机数;

e、f: 标签新所有者 B 随机选取的两个大素数;

g: e、f 两个大素数的乘积, 即: $g = ef$;

Query: 所有权转移请求命令;

SURE: 所有权转移授权命令;

$Cro(X, Y)$: 交叉位运算;

$\oplus$: 异或运算;

&: 与运算;

$M^2 \bmod d$: 模运算.

其中有关交叉位运算详细实现步骤可参考文献[15], 示例可参考如图 1 所示: 取长度 L=12, 并设定 X= 001100110011, Y= 110101010101, 根据交叉位运算的定义可得: $Cro(X,Y)$ = 101110111011.

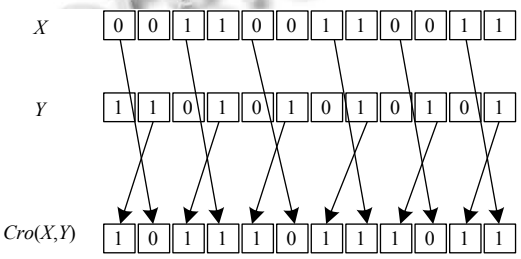

图 1 交叉位运算

1.2 所有权转移协议

所提所有权转移协议分为两个阶段, 第一个阶段是初始化阶段, 完成标签原所有者 A、标签新所有者 B、群组标签 T_a 中各参数的设置; 第二阶段是所有权转移阶段, 完成标签所有权由标签原所有者 A 转移到标签新所有者 B 的过程.

(1) 初始化阶段

在所有权转移协议的初始化阶段, 标签新所有者 B 随机选择两个大素数 e 和 f, 然后计算 $g = ef$ 的值, 并将 g 的值通过安全信道告知标签原所有者 A 和群组标签 T_a. 标签原所有者 A 端存放如下信息: (V_i、V、g); 标签新所有者 B 端存放如下信息: (e、f、g); 群组标签 T_a 中编号为 i 的标签端存放如入信息: (V_i、V、g).

(2) 所有权转移阶段

对图 2 中的通信过程中出现的字符进行解释:

$M1 = Cro(V, x)$;

$M2 = Cro(M1, y)$;

$M3 = x \oplus g$;

$M4 = y \oplus g$;

$M5_i = V_i \oplus z_i$;

$M6_i = Cro(z_i, x)$;

$M7_i = (y \& w_i)^2 \bmod g$;

$M8_i = Cro(z_i, V_i)$;

$M9_i = U_i \oplus w_i$;

$M10_i = U \oplus w_i$;

$M11_i = Cro(M8_i \& M9_i, M10_i \& w_i)$.

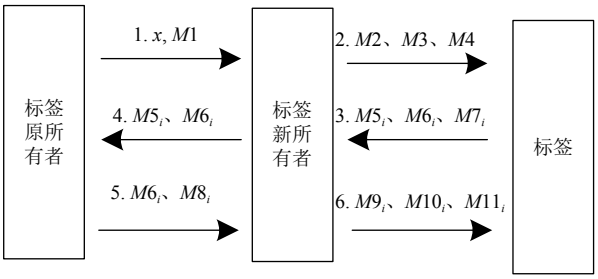

图 2 本文协议

所提所有权转移协议如图 2 所示, 具体的执行步骤如下:

(1) 步骤 1

1) 标签原所有者 A 生成一个随机数, 记作 x.

2) 标签原所有者 A 用自身生成的 x、自身存放的 V 计算得到 $M1$. 标签原所有者 A 用自身生成的 x、接收到的 g 计算得到 $M3$.

3) 标签原所有者 A 将<*Query*、$M1$、$M3$>一并发送给标签新所有者 B.

(2) 步骤 2

标签新所有者 B 在接收到信息之后, 进行如下操作.

1) 标签新所有者 B 生成一个随机数, 记作 y.

2) 标签新所有者 B 用自身生成的 y、接收到的 $M1$ 计算得到 $M2$. 标签新所有者 B 用自身生成的 y、自身存放的 g 计算得到 $M4$.

3) 标签新所有者 B 向标签组 T_a 广播消息<$M2$、$M3$、$M4$>.

(3) 步骤 3

标签 T_i 在接收到信息之后, 进行如下操作.

1) 标签 T_i 用接收到的 $M3$、自身存放的 g 计算得到随机数 x. 标签 T_i 用接收到的 $M4$、自身存放的 g 计算得到随机数 y. 标签 T_i 用计算得到的 x、计算得到的 y、自身存放的 V 计算得到一个 $M2$`的值.

2) 标签 T_i 将计算得到的 $M2$`与接收到的 $M2$ 值进行比对. 若两者值相等, 进行步骤 3); 反之, 协议终止.

3) 标签 T_i 生成两个随机数, 分别记作 z_i、w_i.

4) 标签 T_i 用自身生成的 z_i、自身存放的 V_i 计算得到 $M5_i$. 标签 T_i 用自身生成的 z_i、计算得到的 x 计算得到 $M6_i$. 标签 T_i 用自身生成的 w_i、计算得到的 y、接收到的 g 计算得到 $M7_i$.

5) 标签 T_i 将<$M5_i$、$M6_i$、$M7_i$>一并发送给标签新所有者 B.

(4) 步骤 4

标签新所有者 B 接收到标签 T_i 的响应信息后, 得到集合$\{(M5_i、M6_i、M7_i)|1 \le i \le a\}$. 进行如下操作.

1) 标签新所有者 B 对 $M7_i$ 进行解方程, 即: $M7_i = b^2 \bmod g$. 根据中国剩余定理, 可以计算得出方程的四个解, 依次为: b_1、b_2、b_3、b_4.

2) 若能够找到左边 L 位等于 y 的解 $b_i(1 \le i \le 4)$, 进行步骤 3); 反之, 协议终止.

3) 该解相对应的右边 L 位即为 w_i, 然后存放集合$\{(w_i, M7_i)|1 \le i \le a\}$.

4) 标签新所有者 B 将集合$\{(M5_i、M6_i)|1 \le i \le a\}$传送给标签原所有者 A.

(5) 步骤 5

标签原所有者 A 在接收到信息之后, 进行如下操作.

1) 标签原所有者 A 检查收到的消息集合中消息对 $(M5_i、M6_i)$ 的数量是否与数据库中存放的待转移的群组标签 T_a 中的标签数一致.

2) 如果数量一致, 进行步骤 6; 反之, 协议终止.

(6) 步骤 6

标签原所有者 A 将对每一个消息对 $(M5_i、M6_i)$ 进行验证, 验证过程如下.

1) 标签原所有者 A 用接收到的 $M5_i$、自身存放的 V_i 计算得到随机数 z_i.

2) 标签原所有者 A 用自身生成的 x、计算得到的 z_i 计算得到一个 $M6_i$`的值.

3) 标签原所有者 A 将计算得到的 $M6_i$`与接收到的 $M6_i$ 值进行比对. 若两者值相等, 进行步骤 4); 反之, 协议终止.

4) 说明群组标签 T_a 中的每个标签 T_i 都存在, 进行步骤 7.

(7) 步骤 7

1) 标签原所有者 A 对群组标签 T_a 中的每个标签 T_i 用自身存放的 V_i、计算得到的 z_i 计算得到 $M8_i$.

2) 标签原所有者 A 向标签新所有者 B 发送授权转移信息<*SURE*, $\{(M6_i, M8_i)|1 \le i \le a\}$>.

(8) 步骤 8

标签新所有者 B 在接收到所有权转移授权命令之后, 进行如下操作.

1) 标签新所有者 B 生成一个标签新所有者 B 与群

组标签 T_a 之间共享的密钥 U. 标签新所有者 B 生成一个标签新所有者 B 与群组标签 T_a 中编号为 i 的标签 T_i 之间共享的认证密钥 U_i.

2) 标签新所有者 B 用自身生成的 U_i、计算得到的 w_i 计算得到 $M9_i$. 标签新所有者 B 用自身生成的 U、计算得到的 w_i 计算得到 $M10_i$. 标签新所有者 B 用计算得到的 $M9_i$、计算得到的 $M10_i$、接收到的 $M8_i$、计算得到的 w_i 计算得到 $M11_i$.

3) 标签新所有者 B 向标签 T_i 发送信息<$M9_i$、$M10_i$、$M11_i$>.

(9) 步骤 9

标签 T_i 在接收到信息之后, 进行如下操作.

1) 标签 T_i 用自身存放的 V_i、自身生成的 z_i 计算得到一个 $M8_i$`的值. 标签 $T_i$ 用接收到的 $M9_i$、接收到的 $M10_i$、计算得到的 $M8_i$`、自身生成的 w_i 计算得到一个 $M11_i$`的值.

2) 标签 T_i 将计算得到的 $M11_i$`与接收到的 $M11_i$ 值进行比对. 若两者值相等, 进行步骤 3); 反之, 协议终止.

3) 标签 T_i 通过计算 $w_i \oplus M9_i$ 得到认证密钥 U_i 的值. 标签 T_i 通过计算 $w_i \oplus M10_i$ 得到共享密钥 U 的值.

4) 标签 T_i 更新标签 T_i 与标签新所有者 B 之间的密钥信息, 到此所有权转移成功.

2 安全性分析

(1) 后向安全

在所有权转移协议中, 当群组标签的所有权转移成功后, 标签组中存放的密钥全部更新, U 取代 V, U_i 取代 V_i, 同时 U 和 U_i 对标签的原所有者 A 是保密的; 密钥更新之后, 标签的原所有者 A 将不能再识别出群组标签中的任何一个标签, 并且无法访问标签与标签的新所有者 B 之间的会话消息. 故所提协议能够保证后向安全性.

(2) 前向安全

在所提所有权转移协议中, 标签的新所有者 B 仅仅只能获得更新后的密钥 U 和 U_i, 根本没有办法获取标签的原所有者 A 与群组标签之间共享的密钥 V 和 V_i, 因此标签的新所有者 B 根本没有权限访问到标签与标签的原所有者 A 之间的会话消息. 故本文协议能够保证前向安全性.

(3) 去同步化攻击

去同步化攻击是要造成群组标签与标签的新所有者 B 之间共享的密钥不相同, 或者是造成群组标签与标签的原所有者 A 之间共享的密钥不相同. 在所提所有权转移协议中, 协议运行的前提是: 群组标签中存放有与标签的原所有者 A 通信所需用到的密钥 V 和 V_i, 因此攻击者无法造成群组标签与标签的原所有者 A 之间的密钥不同. 当标签的新所有者 B 产生新的密钥之后, 群组标签并不是立刻进行更新密钥, 而是通过 $M9_i$、$M10_i$、$M11_i$ 消息来验证标签的新所有者 B 的真伪, 只有标签的新所有者 B 不是伪造的情况下, 群组标签端才会进行密钥的更新, 否则密钥不仅不会更新, 而且协议立刻终止, 因此攻击者无法造成密钥不同步的情况. 故所提协议可以抵抗去同步化攻击.

(4) 暴力破解攻击

在所提所有权转移协议中, 攻击者监听整个通信过程, 可以获得 $M2$、$M3$、$M4$、$M5_i$、$M6_i$、$M7_i$、$M9_i$、$M10_i$、$M11_i$ 这些消息, 但攻击者仍无法从上述消息中获得任何有用的隐私信息. 比如对 $M3$ 进行暴力破解攻击, $M3 = x \oplus g$在该公式中, 随机数 x 攻击者不知晓, 它是由标签原所有者 A 随机产生, 且无法提前预测, 同时又是通过安全通道传送给标签新所有者 B; g 是 e 和 f 的乘积, 对于 e 和 f 的选取, 攻击者更是无法知晓, 且 g 事先已安全存放在群组标签端, 因此在上述公式中, 攻击者仅仅只能截获到 $M3$ 消息, 而 $M3$ 消息中的 x 和 g 都是无法知晓的, 所以攻击者即使对消息 $M3$ 进行强制性破解, 也还是无法获取任何有用的信息; 对其他获取的消息进行强制性攻击同样无法获取信息, 因每个消息中至少有两个量, 攻击者是无法提前知晓的. 故本文协议可以抵抗暴力破解攻击.

(5) 追踪攻击

在所提所有权转移协议中, 攻击者通过监听一个完整的通信过程, 可以获得众多消息中的 $M5_i$、$M6_i$、$M7_i$ 三个消息, 攻击者试图通过分析由群组标签产生的 $M5_i$、$M6_i$、$M7_i$ 三个消息来跟踪群组标签, 但攻击者无法成功. $M5_i$、$M6_i$、$M7_i$ 三个消息中都有用到由群组标签产生的随机数来计算, 而随机数的产生是随机生成且无法提前预测, 并且每次生成的随机数都是不相同的, 因此攻击者截获的 $M5_i$、$M6_i$、$M7_i$ 三个消息每次都是不同的, 从而使得攻击者根本无法跟踪群组标签的具体位置. 故本文协议可以抵抗跟踪攻击.

(6) 重放攻击

在所提所有权转移协议中, 攻击者监听整个通信过程, 可以获得 $M2$、$M3$、$M4$、$M5_i$、$M6_i$、$M7_i$、

$M9_i$、$M10_i$、$M11_i$ 这些消息, 攻击者想通过重放上述信息进行重放攻击, 从而获取标签端的隐私信息, 但攻击者无法成功. 在上述获取的消息中, 每个消息再计算过程中都会用到不同的随机数, 标签原所有者 A 通过随机数 x 来保持每次传输消息的新鲜性; 标签新所有者 B 通过随机数 y 来保持每次传输消息的新鲜性; 标签 T_i 通过随机数 w_i、z_i 来保持每次会话用到的信息的新鲜性. 攻击者不论对谁发送的恶意重放攻击, 都是不可能实现的, 因为随机数 x、y、w_i、z_i 的产生都是随机产生的, 每次都是不同的, 且无法提前预测, 因此重复发送上一次会话的消息无法通过认证. 故本文协议可以抵抗重放攻击.

3 性能分析

性能分析主要从标签计算量、标签存储空间大小方面来分析, 分析结果如表 1 所示.

表 1 协议的性能比较

性能因子	计算量	存储空间
文献[12]	3*PE*()	4*L*
文献[13]	9*PH*()	4*L*
文献[14]	6*PR*()+*PM*()+5*XAND*+6*XOR*()	3*L*
本文协议	6*Cro*()+*PM*()+10*XOR*+7*AND*	3*L*

表 1 中, 设定共享密钥值, 共享认证密钥值, 大素数的长度均为 L 位; *PR*() 表示 PRNG 运算, *PH*() 表示哈希函数运算, *PM*() 表示模运算, *PE*() 表示加解密运算, *AND* 表示与运算, *XOR* 表示按位异或运算, *XAND* 表示连接运算, *Cro*() 表示交叉位运算.

由表 1 中可得知, 在存储空间方面, 本文协议相对文献[12]及文献[13]来说, 减少了标签端的存储空间; 相对文献[14]而言, 与其标签端的存储空间相当. 在计算量方面, 本文协议相对文献[12]及文献[13]来说, 标签端的计算量减少较多, 因 *PE*() 加解密运算, *PH*() 哈希函数运算都是轻量级的运算量, 而本文协议中用到的加密方法都是超轻量级的运算量; 相对文献[14]而言, 本文协议在超轻量级方面的运算量稍微多一些, 但超轻量级的计算量本身计算量较少, 因此多几次的超轻量级加密运算量可以忽略不计, 同时文献[14]中采用 *PRNG* 运算进行加密, 而该运算属于轻量级的计算量, 本文协议采用 *Cro*() 字合成运算进行加密, 该加密方法属于超轻量级的算法. 因此综合比较, 本文协议在标签端计算量方面, 要比文献[14]中的计算量少一些, 且文献[14]中的协议存在安全缺陷, 无法抵抗暴力破解攻击, 而本文协议弥补了原协议的安全缺陷问题.

4 基于 BAN 逻辑形式化证明

本文采用 BAN 逻辑形式化分析方法对本文协议进行安全性证明, BAN 逻辑是由 Burrows 等人提出的.

采用 BAN 逻辑对协议进行形式化分析, 证明过程如下所示. 因标签新所有者 B 和标签原所有者 A 中都有读写器部分, 因此可以将两者看成一个整体, 看成一个大的读写器, 用 R 来表示.

(1) 协议的理想化模型

消息① $R\rightarrow T$: $M2$、$M3$、$M4$;

消息② $T\rightarrow R$: $M5_i$、$M6_i$、$M7_i$;

消息③ $R\rightarrow T$: $M9_i$、$M10_i$、$M11_i$.

(2) 协议的预期目标

本协议正确性的证明目标主要有 G1、G2、G3、G4、G5、G6、G7、G8、G9 九个, 即双向认证实体之间对交互信息新鲜性的相信.

G1: $R|\equiv M5_i$, R 相信 $M5_i$.

G2: $R|\equiv M6_i$, R 相信 $M6_i$.

G3: $R|\equiv M7_i$, R 相信 $M7_i$.

G4: $T|\equiv M2$, T 相信 $M2$.

G5: $T|\equiv M3$, T 相信 $M3$.

G6: $T|\equiv M4$, T 相信 $M4$.

G7: $T|\equiv M9_i$, T 相信 $M9_i$.

G8: $T|\equiv M10_i$, T 相信 $M10_i$.

G9: $T|\equiv M11_i$, T 相信 $M11_i$.

(3) 协议的初始假设

P1: $R|\equiv R\overset{V}{\leftrightarrow}T$, R 相信 R 和 T 共享密钥 V.

P2: $T|\equiv R\overset{V}{\leftrightarrow}T$, T 相信 R 和 T 共享密钥 V.

P3: $R|\equiv R\overset{V_i}{\leftrightarrow}T$, R 相信 R 和 T 共享认证密钥 V_i.

P4: $T|\equiv R\overset{V_i}{\leftrightarrow}T$, T 相信 R 和 T 共享认证密钥 V_i.

P5: $R|\equiv R\overset{g}{\leftrightarrow}T$, R 相信 R 和 T 共享大素数 g.

P6: $T|\equiv R\overset{g}{\leftrightarrow}T$, T 相信 R 和 T 共享大素数 g.

P7: $R|\equiv \#(x)$, R 相信随机数 x 的新鲜性.

P8: $T|\equiv \#(x)$, T 相信随机数 x 的新鲜性.

P9: $R|\equiv \#(y)$, R 相信随机数 y 的新鲜性.

P10: $T|\equiv \#(y)$, T 相信随机数 y 的新鲜性.

P11: $R|\equiv \#(z_i)$, R 相信随机数 z_i 的新鲜性.

P12: $T|\equiv \#(z_i)$, T 相信随机数 z_i 的新鲜性.

P13: $R|\equiv \#(w_i)$, R 相信随机数 w_i 的新鲜性.

P14: $T|\equiv \#(w_i)$, T 相信随机数 w_i 的新鲜性.

P15: $R|\equiv\#(U)$, R 相信随机数 U 的新鲜性.

P16: $T|\equiv\#(U)$, T 相信随机数 U 的新鲜性.

P17: $R|\equiv\#(U_i)$, R 相信随机数 U_i 的新鲜性.

P18: $T|\equiv\#(U_i)$, T 相信随机数 U_i 的新鲜性.

P19: $T|\equiv R|\Rightarrow M3$, T 相信 R 对 $M3$ 的管辖权.

P20: $T|\equiv R|\Rightarrow M4$, T 相信 R 对 $M4$ 的管辖权.

P21: $T|\equiv R|\Rightarrow M2$, T 相信 R 对 $M2$ 的管辖权.

P22: $T|\equiv R|\Rightarrow M9_i$, T 相信 R 对 $M9_i$ 的管辖权.

P23: $T|\equiv R|\Rightarrow M10_i$, T 相信 R 对 $M10_i$ 的管辖权.

P24: $T|\equiv R|\Rightarrow M11_i$, T 相信 R 对 $M11_i$ 的管辖权.

P25: $R|\equiv T|\Rightarrow M5_i$, R 相信 T 对 $M5_i$ 的管辖权.

P26: $R|\equiv T|\Rightarrow M6_i$, R 相信 T 对 $M6_i$ 的管辖权.

P27: $R|\equiv T|\Rightarrow M7_i$, R 相信 T 对 $M7_i$ 的管辖权.

(4) 协议的推导过程

由消息②得$R\triangleleft\{M5_i\}$, 并且由初始假设 P3 及消息含义法则$\frac{P|\equiv P\overset{K}{\leftrightarrow}Q,P\triangleleft\{X\}_K}{P|\equiv Q|\sim X}$, 得到$R|\equiv T|\sim M5_i$.

由假设 P11 及消息新鲜性法则⊕, 得$R|\equiv\#(M5_i)$.

由已经推导出来的$R|\equiv T|\sim M5_i$、$R|\equiv\#(M5_i)$及随机数验证法则⊕, 得到$R|\equiv T|\equiv M5_i$.

由$R|\equiv T|\equiv M5_i$、初始化假设 P25 以及管辖法则$\frac{P|\equiv Q\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$,可得$R|\equiv M5_i$. 因此, 目标 G1 得证.

运用上述条件和法则, 同理可证得 G2、G3、G4、G5、G6、G7、G8、G9. 此处不再赘述.

4 结论与展望

针对 RFID 系统中标签所有权转移的实际问题, 提出了一种轻量级的群组 RFID 标签所有权转移协议. 该协议弥补了一次会话只能转移单个标签所有权的缺陷, 本文协议可以在一次会话中转移多个标签的所有权; 所提协议弥补了原协议存在的安全缺陷, 本文协议可以抵抗暴力破解攻击; 所提协议在传输过程中所有的信息都是经过简单的加密后再传输, 从而增加了攻击者破解的难度; 通过安全性分析以及 BAN 逻辑形式化, 证明了协议的安全性; 通过性能分析, 表明了该协议适用于低成本的 RFID 系统.

参考文献

1 王少辉, 刘素娟, 陈丹伟. 满足后向隐私的可扩展 RFID 双向认证方案. 计算机研究与发展, 2013, 50(6): 1276–1284. [doi: 10.7544/issn1000-1239.2013.20121268]

2 Xie R, Jian BY, Liu DW. An improved ownership transfer for RFID protocol. International Journal of Network Security, 2018, 20(1): 149–156.

3 金永明, 吴棋滢, 石志强, 等. 基于 PRF 的 RFID 轻量级认证协议研究. 计算机研究与发展, 2014, 51(7): 1506–1514. [doi: 10.7544/issn1000-1239.2014.20131663]

4 张朝晖, 刘悦, 刘道微. 基于标签 ID 的 RFID 系统密钥无线生成算法. 计算机应用研究, 2017, 34(1): 261–263, 269. [doi: 10.3969/j.issn.1001-3695.2017.01.059]

5 鲁力. RFID 系统密钥无线生成. 计算机学报, 2015, 38(4): 822–832.

6 胡炜, 李永忠, 李正洁. 一种能抵抗拒绝服务攻击的 RFID 安全认证协议. 计算机应用研究, 2012, 29(2): 676–678, 682. [doi: 10.3969/j.issn.1001-3695.2012.02.073]

7 刘道微, 凌捷, 杨昕. 一种改进的满足后向隐私的 RFID 认证协议. 计算机科学, 2016, 43(8): 128–130, 158. [doi: 10.11896/j.issn.1002-137X.2016.08.027]

8 陶源, 周喜, 马玉鹏, 等. 基于 Hash 函数的移动双向认证协议. 计算机应用, 2016, 36(3): 657–660. [doi: 10.11772/j.issn.1001-9081.2016.03.657]

9 梁樱, 姚孝明. 群组 RFID 标签所有权转移协议的分析与设计. 计算机工程与设计, 2014, 35(8): 2645–2649, 2659. [doi: 10.3969/j.issn.1000-7024.2014.08.005]

10 Molnar D, Soppera A, Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. Proceedings of the 12th International Conference on Selected Areas in Cryptography. Kingston, ON, Canada. 2005. 276–290.

11 Zuo YJ. Changing hands together: A secure group ownership transfer protocol for RFID tags. Proceedings of the 2010 43rd Hawaii International Conference on System Sciences. Honolulu, HI, USA. 2010. 1–10.

12 Yang MH. Secure multiple group ownership transfer protocol for mobile RFID. Electronic Commerce Research and Applications, 2012, 11(4): 361–373. [doi: 10.1016/j.elerap.2012.01.004]

13 He L, Gan Y, Yin YF. Secure group ownership transfer protocol for tags in RFID system. International Journal of Security and Its Applications, 2014, 8(3): 21–30. [doi: 10.14257/ijsia]

14 原变青, 刘吉强. 通用可组合安全的 RFID 标签组所有权转移协议. 计算机研究与发展, 2015, 52(10): 2323–2331. [doi: 10.7544/issn1000-1239.2015.20150555]

15 Chiou SY, Ko WT, Lu EH. A secure ECC-based mobile RFID mutual authentication protocol and its application. International Journal of Network Security, 2018, 20(2): 396–402.