一种轻量级隐私保护的RFID群组证明协议

郭奕旻,李顺东,陈振华,刘 新
(陕西师范大学计算机科学学院,陕西西安 710119)

摘 要: 设计高效安全的群组证明协议有利于RFID(Radio Frequency Identification)系统的广泛应用.本文提出了一种轻量级隐私保护的RFID群组证明协议LPGP(Lightweight Privacy-Preserving Grouping Proof),LPGP协议只使用计算复杂度比较小的伪随机发生器和散列运算来提高协议的运行效率,并且LPGP协议具有认证性、隐私性和可证明安全性,满足了RFID系统群组证明协议的安全性要求.与现有的群组证明协议相比,LPGP协议的标签只需较小的计算复杂度和存储空间,具有较高的效率.

关键词: 群组证明; 射频识别; 可证明安全
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2015)02-0289-04
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.02.013

A Lightweight Privacy-Preserving Grouping Proof Protocol for RFID Systems

GUO Yi-min, LI Shun-dong, CHEN Zhen-hua, LIU Xin
(*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710119, *China*)

Abstract: Efficient and secure grouping proof protocols are necessary for RFID applications. This paper proposes a lightweight privacy-preserving grouping proof (LPGP) protocol for RFID systems, which uses only a pseudo-random generator with relatively lower computational complexity and a hash algorithm to improve the operating efficiency. The LPGP protocol can provide privacy, authentication and provably security, and can meet the security requirements of grouping proofs for RFID systems. Compared with existing grouping proofs protocols, the tags in the LPGP only need a small computational cost and small require storage space, thus LPGP is more effective than other grouping proofs protocols.

Key words: grouping proofs; RFID(radio frequency identification); provable security

1 引言

近些年来,人们发现RFID系统在某些应用中需要证明某些物品必须是"同时"存在,例如药品和其说明书应该是同时存在的,解决的方法是将药品和说明书上都附上RFID标签,再建立一个群组模型表明它们属于同一群组.在这类应用中,只保证单个实体的安全性是不够的,还需要对多个实体是否同时存在于一个群组进行验证,这样才能保证这些实体的完整性和安全性.对群组标签进行识别和同时存在的证明问题称为标签的群组证明.

根据采集数据方式的不同,群组证明协议可以分为两大类:链接式群组证明协议和广播式群组证明协议.链接式群组证明协议[1]在采集群组数据时,由阅读器产生一个查询命令,发送给第一个标签,得到第一个标签的响应后,阅读器对其数据处理后再将查询命令发送给第二个标签,依次处理,阅读器在接收到最后一个标签的响应后才生成群组证明.广播式群证明协议[2,3]是由阅读器广播查询命令,所有标签对命令进行响应,阅读器收集这些响应,并根据这些响应生成群组证明.目前已经提出了一些RFID系统群组证明协议,但这些协议不能很好地均衡协议的安全性和标签计算代价,有的协议存在一些安全性问题,如弱认证[2]、假冒攻击[4]等;有的协议设计过于复杂[5];有的协议存在结构问题[6].一个有效的RFID群组证明协议应该在保证协议安全性的前提下,尽量减少标签的计算负担,从而能扩大协议的应用范围.基于这个目的,本文提出了一种轻量级隐私保护的RFID群组证明(LPGP)协议.

收稿日期:2013-12-23;修回日期:2014-06-16;责任编辑:马兰英
基金项目:国家自然科学基金(No.61070189,No.61272435,No.61373020)

2 RFID 攻击者模型

假设攻击者 A 是一个概率多项式时间算法,它可以对阅读器和标签交换的所有消息进行观察、更改和重放,甚至产生新消息.给定一组标签和阅读器,假设攻击者 A 能够访问以下预言机:

(O_1) $Execute(R, T_i)$:模拟一个阅读器和标签之间运行的协议.

(O_2) $SendTag(T_i, sid, c_{sid})$:模拟向标签 T_i 发送一个挑战 c_{sid},标签响应该挑战,随后该预言机返回标签的响应.

(O_3) $SendReader(R, sid, r_{sid})$:模拟给阅读器 R 发送一个响应消息 r_{sid}.

(O_4) $SendVerifier(V, P)$:模拟向验证者 V 发送一个群组证明 P,如果 P 是有效的,输出为 1,否则输出为 0.

(O_5) $Reveal(T_i)$:模拟标签 T_i 将秘密信息暴露给攻击者.

(O_6) $SendReader(R, ticket_v)$:模拟阅读器 R 向验证者请求获得群组证明生成的授权票据 $ticket_v$.

群组证明协议的认证性游戏定义如图 1 所示.

初始化:选择一个阅读器 R 和一个标签 T_i

1.学习阶段

攻击者随意对阅读器 R 和标签 T_i 调用预言机 O_1、O_2、O_3、O_5

2.挑战阶段

攻击者随意调用预言机 O_2、O_3、O_5,假冒阅读器或者标签参与协议中的认证

3.结束阶段

如果一个有效的阅读器或者标签能够认证攻击者假冒的标签或者阅读器是合法的,则攻击者 A 赢得游戏

图 1 认证性游戏

定义 1 认证性 如果一个多项式时间攻击者 A 在认证性游戏中获胜的概率是可以忽略的,则认为一个 RFID 群组证明协议具有认证性.

目前已经存在很多隐私概念[7,8],如通用不可跟踪性、不可辨别性、消息隐私等,群组证明协议的隐私性游戏定义如图 2 所示.

初始化:选择一个阅读器 R 和 n 个标签 $T=\{T_1, T_2, \cdots T_n\}$

1.学习阶段

攻击者随意对阅读器 R 和标签调用预言机 O_1、O_2、O_3、O_5,并在该阶段输出两个没有被预言机 O_5 调用的两个标签 T_0 和 T_1

2.挑战阶段

对于没有被调用 O_5 的两个标签 T_0 和 T_1,挑战者 C 选择一个标签 T_b 作为挑战标签,随机选择的比特 $b\in\{0,1\}$,如果 $b=0$,$T_b=T_0$,否则 $T_b=T_1$

攻击者对 T_b 随意调用预言机 O_1、O_2、O_3 进行查询

3.猜测阶段

攻击者猜测随机数 b,其猜测结果为 b',如果 $b'=b$,则攻击者 A 赢得游戏

图 2 隐私性游戏

定义 2 隐私性 攻击者在隐私游戏中获胜的优势可以表示为 $|Pr[b'=b]-1/2|$,如果一个多项式时间攻击者 A 在隐私游戏中获胜的优势是可以忽略的,则认为一个 RFID 群组证明协议具有隐私性.

群组证明安全性的目标是攻击者不能假冒、插入或者删减任何一个标签,并且验证者可以检验标签的真伪,群组证明的安全性游戏定义如图 3 所示.

初始化:选择验证者 V、阅读器 R 和 n 个标签 $T=\{T_1, T_2, \cdots T_n\}$

1.学习阶段

攻击者随意调用预言机 O_1、O_2、O_3、O_4、O_5、O_6

2.挑战阶段

挑战者用 n 个标签的有效证明 P 作为挑战,攻击者假冒阅读器或者标签,并随意调用预言机 O_1、O_2、O_3、O_4、O_5、O_6,输出一个新的群组证明 P'

3.结束阶段

将群组证明 P' 作为预言机 O_4 的输入,如果预言机 O_4 输出为 1,则攻击者 A 赢得游戏

图 3 群组证明的安全性游戏

定义 3 群组证明的安全性 如果一个多项式时间攻击者 A 在群组证明的安全性游戏中获胜的概率是可以忽略的,则认为一个 RFID 群组证明是安全的.

3 RFID 群组证明协议

LPGP 协议主要分为 5 个部分,系统初始化,阅读器授权、阅读器与标签相互认证、群组证明生成和群组证明验证.

系统初始化 根据安全参数 k,为每个标签选择一个秘密数 S_i,一个假名 PID_i,保存在验证者端.为阅读器选择一个主密钥 K_i,该主密钥只有阅读器和验证者知道.选择一个伪随机数发生器 $g:\{0,1\}^n\rightarrow\{0,1\}^l$,它可以把 n 位的输入扩展为 l 位的输出序列,其中 $l>n$.选择一个 hash 函数 $h:\{0,1\}^*\rightarrow\{0,1\}^m$,它可以把任意位的输入压缩为 m 位的输出序列.

阅读器授权 给阅读器授权,允许其生成群组证明.阅读器选择一个临时交互号 $N_1\in_R\{0,1\}^m$,计算 $c_1=h(K_i, ID_R, T_i, N_1)$,其中 ID_R 是阅读器的标识符,T_i 代表第 i 个标签.将 N_1、c_1 和 ID_R 传送给验证者.验证者根据 ID_R 查找阅读器的秘密数 K_i,计算 $h(K_i, ID_R, T_i, N_1)$,判断其值是否等于 c_1,如果相等,生成一个授权票据 $ticket_v\in_R\{0,1\}^l$,将票据和标签的假名 PID_i 用 K_i 加密后传送给阅读器.

$$V_R=E_{K_i}(ticket_v, PID_i)$$

阅读器与标签相互认证阶段 阅读器向标签发起挑战,阅读器随机生成临时交互号 $N_2\in_R\{0,1\}^m$ 广播给标签,作为挑战消息 c_{sid}.标签计算 $r_i=g(PID_i\oplus N_2)$ 作为响应消息 r_{sid},同时生成一个临时交互号 N_3,随机

生成临时交互号 $N_4 \in_R \{0,1\}^m$,并将 r_i和N_3一起作为一个挑战消息,传给阅读器.阅读器计算 $r_i = g(PID_i \oplus N_2)$,如果与标签传送过来的 r_i相等,则认证标签,然后计算 $r_R = g(PID_i \oplus N_3)$,与 N_4一起作为响应消息传送给标签.标签接收后验证阅读器的合法性,同时更新假名 $PID_i' = g(PID_i \oplus S_i)$.

群组证明生成:

标签计算 $r_i' = g(PID_i \oplus N_4)$, $m_i = h(s_i, r_i')$发送给阅读器.阅读器先检验 $g(PID_i \oplus N_4)$是否与标签传送过来的 r_i'相等,如果相等,则接收标签的消息 m_i,并按照下面的公式计算群组证明:

$$P = h(K_i \| ticket_v \| m_1 \oplus m_2 \oplus \cdots \oplus m_n)$$

群组证明验证　阅读器选择临时交互号 $N_5 \in_R \{0,1\}^m$,将 ID_R、N_5、N_4、$E_{K_i}(ticket_v)$、P 一起传送给验证者,验证者首先根据阅读器的标识符 ID_R和主密钥 K_i,验证阅读器的合法性,然后自己计算出群组证明 P,判断与阅读器传来的群组证明值是否相等,如果相等,则完成对群组证明的检验.验证后,验证者更新标签假名 $PID_i' = g(PID_i \oplus S_i)$.

协议流程如图 4 所示.

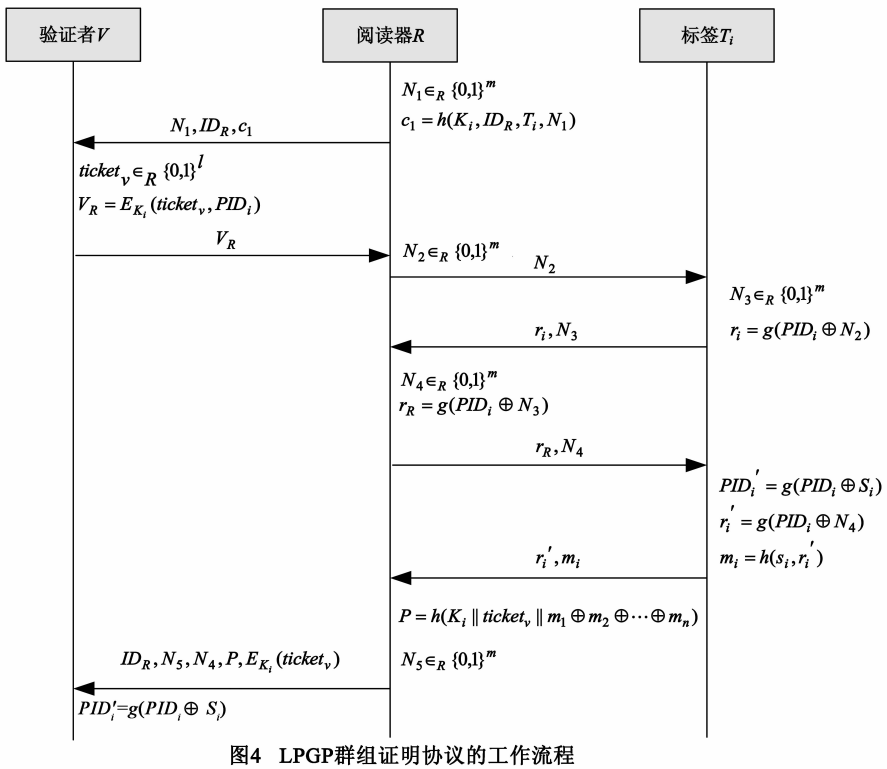

图4　LPGP群组证明协议的工作流程

4　安全性证明和性能分析

4.1　安全性证明

定理 1　对于一个多项式时间攻击者 A 而言,LPGP 协议具有认证性.

证明　在学习阶段,攻击者 A 可以随意调用预言机 O_1、O_2、O_3、O_5,在第二阶段,挑战者选取一个标签 T_i,当攻击者调用预言机 O_2 即 $SendTag(T_i, sid, c_{sid})$时,挑战者将会返回 $g(PID_i \oplus N_2)$,这样就存在三种情况:

(1)当所有的 $g(PID_i \oplus N_2)$都被预言机 O_2查询过时,这相当于攻击者 A 构造了一个伪随机数发生器.此时攻击者 A 赢得游戏的优势与攻击者分辨伪随机数发生器输出序列和真随机数序列的优势一致,根据伪随机数发生器的定义,攻击者 A 获得胜利的优势 ε 是可以忽略的.

(2)当标签 T_i被预言机 O_5即 $Reveal(T_i)$查询过时,这相当于攻击者 A 知道了标签 T_i的内部状态,即攻击者知道标签 T_i的当前假名 PID_i.假设攻击者利用该标签运行协议 q 次,系统总共有 N 个假名,那么攻击者需要区分一个假名,需要收集的假名数为[8]:

$$N(1 - (\frac{N-1}{N})^q)$$

攻击者 A 获得胜利的优势等于区分两个标签假名的概率:

$$1 - (\frac{N-1}{N})^{2q}$$

如果假名长度为 n, N 值为 2^n,当 n 取值为 32 位时, N 值为 2^{32},即为 4.3×10^9.因此当假名取到合适长度时,攻击者 A 获得胜利的优势 ε 是可以忽略不计的.

(3)如果 $g(PID_i \oplus N_2)$被预言机 O_1、O_2、O_3 共调用了 n 次,攻击者 A 成功的概率为 $n/2^M$, M 为 PID_i 和 N_2 位长之和.

综合上面三种情况,攻击者 A 赢得游戏概率小于

$$2\varepsilon + 1 - (\frac{N-1}{N})^{2q} + n/2^M$$

因此攻击者 A 赢得认证性游戏的概率是可以忽略的,定理得证.

用同样的方法可以证明以下两个定理.

定理 2 对于一个多项式时间攻击者 A 而言,LPGP 协议具有隐私性.

定理 3 对于一个多项式时间攻击者 A 而言,LPGP 协议的群组证明是安全的.

4.2 性能分析

在 RFID 系统中通常用标签的计算复杂度和存储开销来度量 RFID 协议的性能.表 1 中 H 表示密码学中的 hash 运算,M 表示消息认证码运算,P 表示伪随机数发生器运算,C 表示循环冗余校验运算,B 表示移位运算.由于各种参数以及标识符的长度差别很小,所以本文将它们的长度都用 l 表示.为了能够用统一标准进行比较,表中的数据表示的是两个标签计算量和存储量的总和.通过表 1 可以看到,LPGP 协议中标签的计算复杂度和存储开销都相对较小.采用文献[7]的时钟周期计算方式,也可以看到 LPGP 协议中操作的时钟周期数相对较小.

表 1 相关协议的标签所需代价比较

性能	文献[1]	文献[2]	文献[3]	文献[4]	LPGP
标签的计算代价	4M + 8P + 8B	4M + 2P	2M	23P + 20B	4P + 2H
标签的存储开销	3l	3l	2l	4l	3l
时钟周期数	9976	8816	4224	4462	2936

5 结束语

制约 RFID 系统广泛应用的两个主要因素是标签的成本和系统的安全性,低成本标签的计算能力有限,不能进行复杂的密码运算,但复杂的密码运算能够更好地保证 RFID 系统的安全,如何权衡两者之间的关系具有非常重要的意义.LPGP 协议的设计思路是在满足群组证明协议安全需求的前提下,尽可能降低计算复杂度.为了达到这个目标,LPGP 协议只使用密码学中的 hash 函数运算和伪随机数发生器运算,在任何阶段都对 RFID 系统中的阅读器和标签进行认证,从而保证了群组证明的安全性.LPGP 协议既满足了安全需要,又减少了标签的计算量,对 RFID 的广泛应用具有非常重要的实际意义.

参考文献

[1] Lo N W, Yeh K H. Anonymous coexistence proofs for RFID tags[J]. Journal of Information Science and Engineering, 2010, 26(4): 1213 – 1230.

[2] 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 Zhong, et al. Universal composable grouping-proof protocol for RFID tags in the Internet of Things[J]. Chinese Journal of Computers, 2011, 34(7): 1188 – 1194. (in Chinese)

[3] Duc D N, et al. A survey on RFID security and provably secure grouping-proof protocols[J]. International Journal of Internet Technology and Secured Transactions, 2010, 2(3): 222 – 249.

[4] Peris-Lopez P, et al. Flaws on RFID grouping-proofs. Guidelines for future sound protocols[J]. Journal of Network and Computer Applications, 2011, 34(3): 833 – 845.

[5] Liu H, et al. Grouping-proofs-based authentication protocol for distributed RFID systems[J]. IEEE Transactions on parallel and distributed systems, 2013, 24(7): 1321 – 1330.

[6] Ko W T, Chiou S Y, Lu E H, et al. A privacy-preserving grouping proof protocol based on ECC with untraceability for RFID[J]. Applied Mathematics, 2012, 3(4): 336 – 341.

[7] 马昌社.前向隐私安全的低成本 RFID 认证协议[J].计算机学报,2011,34(8):1387 – 1398.
Ma Changshe. Low cost RFID authentication protocol with forward privacy[J]. Chinese Journal of Computers, 2011, 34(8): 1387 – 1398. (in Chinese)

[8] Alomair B, Clark A, Cuellar J, et al. Scalable RFID systems: a privacy-preserving protocol with constant-time identification [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1536 – 1550.

作者简介

郭奕旻(通信作者) 女,1992 年生,湖北黄梅人,陕西师范大学计算机科学学院硕士研究生,研究方向为信息安全与密码学.
E-mail: yiminguo@snnu.edu.cn

李顺东 男,1963 年 12 月生,河南平顶山人.1984、1987 年在西安工程大学获工学学士、硕士学位;2003 年在西安交通大学获计算机科学与技术工学博士学位.现为陕西师范大学计算机科学学院教授、博士生导师.主要从事密码学与信息安全研究.
E-mail: shundong@snnu.edu.cn