

基于 PUF 的 RFID 系统安全密钥协商协议

郭丽敏¹, 刘 丹¹, 王立辉¹, 单伟君¹, 李 清^{1,2}

(1 上海复旦微电子集团股份有限公司, 上海 200433; 2 复旦大学 微电子学院, 上海 200433)

摘 要: 低成本 RFID 标签与读卡器间的相互认证或安全通信都依赖于通信双方预先共享的密钥, 而攻击者可以通过物理攻击等手段获得该密钥. 利用 PUF 电路的物理不可克隆特性, 提出两个基于 PUF 的密钥协商协议, 从通信双方可以产生相同的随机密钥, 供后续的认证或安全通信使用. 分析结果表明, 该协议可以有效抵抗物理、重放、假冒、中间人、离线猜测及在线猜测攻击, 同时提供前向安全性和后向安全性.

关键词: RFID 系统; 物理不可克隆函数; 密钥协商协议; 安全

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2017)07-0060-05

Secure Key Exchange Protocol for RFID System Based on PUF

GUO Li-min¹, LIU Dan¹, WANG Li-hui¹, SHAN Wei-jun¹, Li Qing^{1,2}

(1 Shanghai Fudan Microelectronics Group Company Limited, Shanghai 200433, China;

2 School of Microelectronics, Fudan University, Shanghai 200433, China)

Abstract: The secure mutual authentication or secure communication between the low-cost RFID tags and the card readers depends on a secret key shared by the two parties, which can be gained directly by a power attacker by means of physical attacks. Taking advantage of the physical unclonable feature of PUF circuits, two secure key exchange protocols are presented in this paper, such that the two parties can generate a same random key which can be used to secure the following authentication or communication. Security analysis shows that these two protocols can resist physical attack, reply attack, counterfeit attack, man-in-the-middle-attack, offline guessing attack and online guessing attack, and also can provide forward security and backward security.

Key words: RFID system; PUF; key exchange protocol; security

1 引言

RFID(无线射频识别)技术是融合了无线射频技术和嵌入式技术为一体的综合技术, 能通过无线电信号识别特定目标并对相关数据信息进行读取.

但是 RFID 技术存在的安全问题也引起了人们越来越多的关注, 这些安全问题制约着 RFID 技术的应用. 通过使用基于传统密码算法的方案在一定程度上可以解决这个问题, 但是由于 RFID 标签通常计算及存储能力有限, 使得许多先进的芯片防护技术无法得到实际应用. 例如, 虽然基于 RSA、ECC 等非对称密码算法的认证和密钥协商协议可以有效解决身份认证及通信数据的保护问题^[1], 但是这些

算法需要很多的计算量及存储开销, 无法在低成本的标签中使用. 所以目前的 RFID 标签的认证协议多基于对称密码算法^[2], 这需要通信双方, 即标签和服务器共享相同的密钥信息, 该密钥需要分别预先存储在标签及服务器中. 此时, 攻击者可以采取物理探针或显微镜扫描等手段获得该密钥^[3]. 一旦攻击者获得该密钥信息, 则该系统的安全就荡然无存了. 一种解决方案是, 每次通信时, 通信双方先协商出当前的会话密钥. 在标签的计算能力、存储能力有限的条件下, 研究安全高效的 RFID 系统的密钥协商协议意义重大.

具有物理不可复制特征的 PUF 技术给高安全性、低成本标签的设计带来了希望. 本文提出基于

PUF 的两个密钥协商协议,使得 RFID 系统中通信双方能共享随机的密钥值。

2 物理不可克隆函数(PUF)

物理不可克隆函数,即 PUF,是一组电路,能提取芯片自身制造过程中的无法预测、复制和控制的细微物理差异,对一个输入,能产生一个不可预测的响应。输入也称为挑战,PUF 的一组输入输出称为挑战响应对,挑战与响应之间的关系仅由设备的某些物理差异决定。由于芯片制造过程中产生的差异具有不可复制的特征,从而 PUF 技术使得芯片具有防伪功能。

PUF 的实现方法有很多,例如基于仲裁器的 PUF^[4]、涂层 PUF^[5]、基于振荡器的 PUF^[6]、基于存储器的 PUF^[7]等。按照挑战响应对的数量,PUF 可以分为强 PUF 及弱 PUF。弱 PUF 只有非常少,并且固定的挑战,例如基于存储器的 PUF、蝴蝶 PUF^[8]等。弱 PUF 通常用来产生存储器加解密所需的密钥。对应地,强 PUF 通常拥有可达到指数量级的挑战,一般用来做身份验证。强 PUF 可基于仲裁器或环形振荡器等结构实现。

PUF 实质上是一个函数,即给定一个输入,会得到相应的输出,但是从数学角度来说,又不是一个纯粹意义上的函数,因为,同一个输入可能会得到不同的输出。当响应用二进制序列表示时,响应之间的差异可以用汉明距离来表示。同一个 PUF 电路模块,在两次给定相同的挑战时,产生的两个响应之间的差距,称为片内汉明距离。

SRAM PUF 是一种典型基于存储器的 PUF。由于生产制造过程中的差异,例如掺杂浓度的均匀性、晶体管沟道长宽比等细微差异造成了 SRAM 每个存储单元上电值的唯一性及不可预测性,形成了 SRAM 存储单元特有的芯片指纹。另外,由于上电过程中,例如温度、噪声等环境因素的影响,在不同时刻对相同的 SRAM 单元上电,会得到不同的响应。此时,对给定 SRAM 单元上电即看作 PUF 的挑战。

对使用 PUF 的典型应用而言,通常有两个阶段,即初始化阶段及应用阶段。在初始化阶段,需要读出 PUF 的一系列的挑战响应对,并保存在服务器的数据库中。称此时 PUF 的响应为标准响应数据。在应用阶段,再次给定 PUF 单元某一挑战,获得即时响应数据,将它与注册阶段得到的标准响应数据进行匹配,从而可以完成认证或提取密钥等功能。

3 两个基于 PUF 的密钥协商协议

3.1 基本假设

RFID 系统通常由标签、读卡器及后端服务器三部分组成。一般来说,后端服务器和读卡器具有足够的存储和计算资源,并且他们之间的通信信道是有限通信,因此可以利用传统的密码算法和网络安全协议来保护他们之间的安全通信,即读卡器和数据库之间的通信建立在安全信道上。但 RFID 标签和读卡器之间的通信是通过开放的无线信道传输,因此读卡器和标签之间的通信是不安全的,任何针对无线信道的攻击手段都可能对 RFID 系统标签和读卡器之间的通信造成威胁。

为了阐述方便,对 RFID 系统做出下述假设。首先,假设标签和读卡器上各有一个随机数发生器。其次,假设标签及服务器上可运行一个 Hash 函数 h ,该 Hash 函数可以是轻量级 Hash 函数或定制的简化 Hash 函数等。同时标签和服务服务器上可运行相同的密钥派生函数 KDF,且预先共享了固定密钥 $key1$ 。

3.2 SRAM-PUF-KEP 协议

通常标签内有 SRAM,可用来实现 SRAM PUF。本节提出基于 SRAM PUF 的密钥协商协议 SRAM-PUF-KEP (SRAM PUF based key exchange protocol)。该协议如图 1 所示,包含两个阶段,即初始化阶段与产生共享密钥阶段。

(1) 初始化阶段。读出标签的 ID 及标签内 SRAM PUF 的上电初始值 R ,并将 (ID, R) 保存在服务器的数据库中。称 R 为标准响应数据,将 R 看作二进制序列,每位取值 0 或 1。

(2) 产生共享密钥阶段。详细的产生共享密钥的步骤如下:

① 读卡器产生随机数 I ,将 I 发送给标签,同时发出密钥协商请求。

② 标签接收到读卡器密钥协商的请求后,标签首先读取 SRAM PUF 的上电初始值,记为 R' ,称为即时响应数据。将 R' 也看作二进制序列,每位取值 0 或 1,则 R' 与 R 在若干位上取值不同,且取值不同的这些位是随机发生的。同时,标签产生随机数 r ,即时响应数据 R' 及 r 经过有纠错功能的纠错码进行编码后的值记为 W , W 也称为辅助数据。利用随机数 I 及固定密钥 $key1$,调用密钥派生函数 KDF 产生密钥流,对 W 进行加密,加密后的结果记为 P ,标签将 ID 及 P 发送给读卡器。最后,调用 hash 函数

h , 标签计算得到随机密钥 $key=h(I,R')$.

③读卡器收到 ID 及 P 后, 将 I, ID 及 P 转发给后端服务器.

④服务器从数据库中搜索是否在 ID, 若找到匹配项, 则读出相应的标准响应数据 R; 若不能找到匹配项, 则协议终止. 服务器利用随机数 I 及固定密钥 key_1 , 调用与标签相同的密钥派生函数 KDF 产生密钥流, 对 P 进行解密, 获得 W. 接着, 利用 R 及 W, 经过纠错算法的译码算法 Rep, 计算得到响应数据 R'' . 最后, 通过相同的 hash 算法, 服务器可产生密钥 $key'=h(I,R'')$.

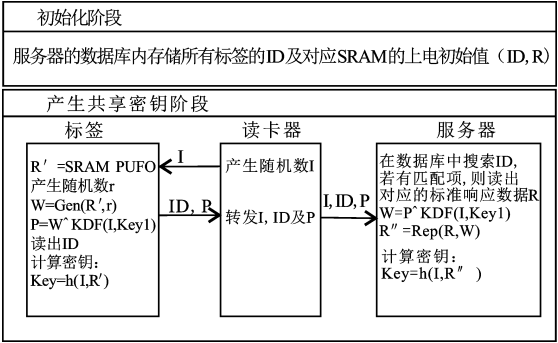


图1 SRAM-PUF-KEP 协议

下面讨论该密钥协商协议的正确性及每次产生的密钥的随机性.

首先, 讨论该密钥协商协议的正确性, 即保证服务器与标签可产生相同的密钥. 密钥协商协议的正确性由纠错算法来保证. 根据 PUF 单元的片内汉明距离, 即 PUF 响应可能出现错误的比特数, 采用具有合适纠错能力的纠错码, 例如重复码、格雷码、BCH 码或它们的组合等, 保证由标准响应数据 R 及辅助数据 W, 经过译码算法, 计算得到的响应数据 R'' , 等于标签内的即时响应数据 R' . 这就保证了经过上述密钥协商协议, 标签及服务器可产生相同的密钥, 即 $key=key'$.

其次, 通过上述密钥协商协议产生的密钥是随机值. 由于每次收到服务器发送的密钥协商请求时, 标签内读出的即时响应数据都是不同的且每次收到的随机数也是不同的, 从而经 hash 函数压缩后产生的密钥也是不同的. 同时, 由于每次读出的即时响应数据是不可预测的, 标签和服务器内部每次产生的密钥也是不可预测的随机值.

另外, 要说明的是, 利用密钥派生函数 KDF 来对辅助数据 W 加密对该密钥协商协议而言并不是必须的. 即对成本受限的标签而言, 可以将该密钥协

商协议修改为发送 W 给读卡器. 这是因为从辅助数据 W 出发, 并不能得到即时响应数据的全部信息, 从而该密钥协商协议仍是安全的.

3.3 S-PUF-KEP 协议

本节假设标签内有利用仲裁器或环形振荡器等结构实现的强 PUF 电路, 提出基于强 PUF 的密钥协商协议 S-PUF-KEP (Strong PUF based key exchange protocol). 该协议如图 2 所示, 包含两个阶段, 即初始化阶段与产生共享密钥阶段. 如图 2 所示, 基于强 PUF 的密钥协商协议包含两个阶段, 即初始化阶段与产生共享密钥阶段.

(1) 在初始化阶段, 读出标签的 ID 及标签内强 PUF 的若干个标准挑战响应对 (C_i, R_i) , 并将 (ID, C_i, R_i) 保存在服务器的数据库中.

(2) 产生共享密钥阶段. 详细的产生共享密钥的步骤如下:

①读卡器产生随机数 I, 将 I 发送给标签, 同时发出密钥协商请求.

②标签接收到随机数 I 后, 将 ID 发送给读卡器.

③读卡器将 ID 转发给后端服务器.

④服务器收到 ID 后, 检索数据库, 若找到标签的 ID, 则从多组挑战响应对中随机挑选一个挑战响应对 (C_i, R_i) , 并将 C_i 发送给读卡器.

⑤读卡器将 C_i 转发给标签.

⑥标签收到 C_i 后, 输入给强 PUF, 得到即时响应数据 R_i' . 标签产生随机数 r , 即时响应数据 R_i' 及 r 经过有纠错功能的纠错码进行编码后的值记为 W, W 也称为辅助数据. 利用随机数 I 及固定密钥 key_1 , 调用密钥派生函数 KDF 产生密钥流, 对 W 进行加密, 加密后的结果记为 P, 标签将 P 发送给读卡器. 最后, 调用 hash 函数 h , 标签计算得到随机密钥 $key=h(I,R_i')$.

⑦读卡器将 I 及 P 转发给服务器.

⑧服务器收到 P 后, 先利用随机数 I 及固定密钥 key_1 , 调用与标签相同的密钥派生函数 KDF 产生密钥流, 对 P 进行解密, 获得 W. 再利用 R_i 及 W, 经过纠错算法的译码算法 Rep, 计算得到响应数据 R_i'' . 再通过相同的 hash 算法, 服务器可产生密钥 $key'=h(I,R_i'')$.

下面讨论该密钥协商协议的正确性及每次产生的密钥的随机性.

首先, 该密钥协商协议的正确性, 即服务器与标签可产生相同的密钥, 由纠错算法来保证. 根据强

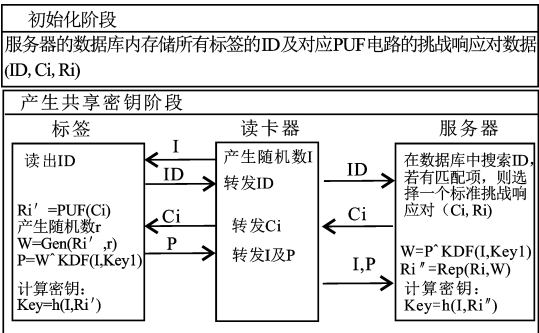


图 2 S-PUF-KEP 协议

PUF 的片内汉明距离,选用具有适当纠错能力的纠错码,例如重复码、格雷码、BCH 码等,保证由标准响应数据及辅助数据,经过译码算法,可以得到标签内的即时响应数据.即服务器经过译码算法,计算得到的响应数据 Ri'' ,等于标签内的即时响应数据 Ri' .这就保证经过上述密钥协商协议,标签及服务器可产生相同的密钥,即 $key = key'$.

即使对相同的挑战,标签内每次产生的即时响应数据也是不同的,经 hash 函数压缩后产生的密钥也是不同的.所以标签和服务器内部每次产生的密钥是一个不可预测的随机值.

另外,同样的,利用密钥派生函数 KDF 来对辅助数据 W 加密对该密钥协商协议而言并不是必须的.

4 安全性分析

本协议的主要特点是安全、方法新颖且易于实现.该协议能有效抵抗物理攻击、重放攻击、假冒攻击、中间人攻击、离线猜测攻击和在线猜测攻击,同时提供前向安全性和后向安全性,满足射频识别系统的安全认证及安全通信需求.

4.1 物理攻击

由于生产制造过程中的细微差异,造成了每个存储单元的唯一性及不可预测性,因此很难从物理上复制出两个不同的 SRAM,满足上电时具有相同的初值.若使用探针等直接读取 SRAM 单元的值,则相较数据库中存储的标准响应值,此时读出 SRAM 的值也会发生较大改变,从而不能建立与服务器一方相同的随机密钥.而利用基于 SRAM PUF 的密钥协商协议 1,标签及服务器产生的密钥是基于 SRAM 每次上电的初始值的,从而该协议是抗物理攻击的.

而强 PUF 的响应依赖于制造过程中不可避免产生的差异,要从物理上复制两个相同的 PUF 电

路,使得他们对相同的挑战,响应是相同的,这是很难实现的.同时,辅助数据是经过加密后再传输给读卡器的,攻击者不能通过未加密的辅助数据,进一步分析得到 PUF 的响应,也不能通过对挑战响应对建模来从功能上复制 PUF 电路.因此基于强 PUF 的密钥协商协议 2 也是抗物理攻击的.

4.2 重放攻击

无论对于基于 SRAM PUF 的密钥协商协议 1,还是基于强 PUF 的密钥协商协议 2 来说,服务器和标签内产生的密钥都依赖于标签内 PUF 单元的即时响应数据.即使对于相同的挑战,同一个 PUF 的响应数据每次也都是不同且无法预测的,攻击者记录前次密钥协商时使用的随机数 I、挑战 Ci 及加密后的辅助数据 P,SRAM PUF 或强 PUF 单元产生的即时响应数据也会与前次有所不同,且攻击者不能预测或控制这些不同值出现的位置,再经过 hash 算法,标签内必然产生完全不同与前次的共享密钥.从而,标签和服务器会产生两个完全不同的随机密钥.因此,重放攻击不能对上述两个密钥协商协议产生安全威胁.

4.3 假冒攻击

首先,由于标签内部的 PUF 电路具有物理不可复制的特征,攻击者无法直接伪造标签进行攻击.同时,由于标签发送的辅助数据是经过加密的,攻击者也不能利用它来对 PUF 电路进行建模,达到对标签内部 PUF 电路进行功能伪造的目的.其次,由于服务器需要组合内部存储的标准 PUF 挑战响应数据及标签发送的数据 P,得到标签内部的即时响应数据,进一步产生随机密钥,在不知道内部存储的标准挑战响应数据时,攻击者也无法假冒服务器进行攻击.

4.4 中间人攻击

即使攻击者通过监听等手段能获得密钥协商期间在无线信道上传输的所有数据,由于他既没有与标签内部相同的 PUF 单元,也得不到服务器内部存储的标准挑战响应对数据,不能获得标签及服务器内部生成的密钥.

4.5 猜测攻击

攻击者可以收集标签和服务器之间的交互消息,即可以得到加密后的辅助数据 P,但是仅从 P 并出发,通过离线计算或在线计算并不能得到关于 PUF 的即时响应数据的信息,因此攻击者不能恢复出标签及服务器的共享密钥值.

4.6 前向安全性和后向安全性

每一次密钥协商协议后,标签及服务器产生的密钥都是不同于前一次的随机值.由于 PUF 每次的响应是不可预测的,即使是合法的通信双方,即标签及服务器也不能预测下一次密钥协商时将要产生的密钥值.因此,该协议提供密钥的前向安全性和后向安全性.

5 结束语

本文提出两种基于 PUF 的密钥协商协议,通过该协议,通信双方,即标签和服务器能得到相同的随机密钥.只有合法的服务器才拥有标签的 ID 及标准的挑战响应对数据,从而结合 P 才能计算得到密钥 key' .由于标签内的 PUF 单元具有不可复制的特征,从而只有合法的标签才能产生与 key' 相等的密钥 key .该密钥可以用于后续的身份认证或安全通信.这两种协议能够有效防止物理攻击、重放攻击、假冒攻击、中间人攻击、离线猜测攻击及在线猜测攻击,同时提供前向安全性及后向安全性.

参考文献:

- [1] Godor G, Giczi N, Lmre S. Elliptic curve cryptography based mutual authentication protocol for low computational capacity RFID systems-performance analysis by simulations[C]// 2010 IEEE International Conference on. IEEE, 2010:650-657.
- [2] 张兴, 韩冬, 曹光辉, 等. 基于 PRESENT 算法的 RFID 安全认证协议[J]. 通信学报, 2015, 36(增刊 1):65-74.
- [3] Samyde D, Skorobogatov S, Anderson R, et al. On a new way to read data from memory[C]// International

IEEE Security in Storage Workshop. IEEE, 2002: 65-69.

- [4] Lim D, Lee J W. Extracting secret keys from integrated circuits[J]. IEEE Transactions on VLSI Systems, 2005, 13(10), 1200-1205.
- [5] Tuyls P, Schrijen G, Skoric B. Read-proof hardware from protective coatings [M]. Springer, 2006, 369-383.
- [6] Gassend B, Clarke D, Van Dijk M, et al. Silicon physical random functions [C]// Acm Conference on Computer and Communications Security. ACM, 2002: 148-160.
- [7] Holcomb D E, Burleson W P, Fu K. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags [C]// Proceedings of the Conference on RFID Security. IEEE, 2007: 11-13.
- [8] Kumar S, Guajardo J, Maes R, et al. The butterfly PUF protecting IP over every FPGA [C]// IEEE International Workshop on Hardware oriented Security and Trust. IEEE, 2008: 67-70.

作者简介:

郭丽敏 女, (1986-), 硕士, 工程师. 研究方向为集成电路设计开发. E-mail: guolimin@fms.h. com. cn.

刘 丹 男, (1981-), 硕士, 工程师. 研究方向为集成电路设计开发.

王立辉 男, (1982-), 硕士, 工程师. 研究方向为集成电路设计开发.

单伟君 男, (1988-), 硕士, 工程师. 研究方向为集成电路设计开发.

李 清 女, (1968-), 硕士, 高级工程师. 研究方向为集成电路设计开发.

(上接第 59 页)

- [4] Huss S A. Advances in design and specification languages for embedded systems[M]. Dordrecht: Springer, 2007.
- [5] Khaligh R, Radetzki M. Efficient and extensible transaction level modeling based on an object oriented Model of Bus Transactions[J]. Embedded System Design: Topics, Techniques and Trends, 2007, 231: 313-324.
- [6] IEEE. Carrier sense multiple access with collision detection(CSMA/CD) access method and physical layer specifications[Z]. New York: IEEE, 2005.
- [7] Glasser M, Bergeron J. TLM-2. 0 in SystemVerilog

[EB/OL]. [2016-03-08]. http://events.dvcon.org/2011/proceedings/papers/04_2.pdf.

作者简介:

彭智聪 女, (1988-), 助理研究员. 研究方向为虚拟原型验证. E-mail: brenda123456@yeah. net.

陈 岚 女, (1968-), 研究员, 博士生导师. 研究方向为超深亚微米芯片设计方法学及计算机体系结构.

冯 燕 女, (1980-), 博士研究生, 助理研究员. 研究方向为 SoC 设计与验证、IP 核标准与共性技术.

马 娟 女, (1988-), 工程师. 研究方向为虚拟原型验证.