第34卷 第12期 计 算 机 工 程 2008年6月
Vol.34 No.12 Computer Engineering June 2008
·安全技术· 文章编号：1000—3428(2008)12—0141—03 文献标识码：A 中图分类号：TP309

基于Hash函数的RFID认证协议

袁署光，戴宏跃，赖声礼
(华南理工大学电子与信息学院，广州 510640)

摘 要：针对射频识别系统存在用户安全、隐私等问题，讨论现有协议的优缺点，提出一种新的基于密码学的安全认证协议。该协议利用Hash函数的单向性特点和对称密钥方法，较好地解决了RFID的安全隐患问题。实验分析表明，该协议具有不可分辨性、前向安全、重传攻击、哄骗攻击等特点，适合于低成本、低计算量、分布式的RFID系统。

关键词：射频识别；隐私；安全协议；Hash函数；密钥

Hash-based RFID Authentication Protocol

YUAN Shu-guang, DAI Hong-yue, LAI Sheng-li
(School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640)

【Abstract】Radio Frequency Identification(RFID) is researched widely and applied to various fields. However, RFID still confronts many problems such as consumers' security and privacy. This paper presents the advantage and deficiency of current solutions to RFID. A new encrypted authentication approach is proposed, which employs the one-way hash function and a symmetric key. Compared with current protocols, it achieves in distinguish ability, forward security, replay attack, and spoofing attack. As a result, the protocol can be used in low-cost, limited computation system, and ubiquitous computing environment.

【Key words】 Radio Frequency Identification(RFID); privacy; security protocol; Hash function; key

射频识别技术(Radio Frequency Identification, RFID)[1]是一种非接触式的自动识别技术，通过无线射频的方式读取和接收信息，达到自动识别的目的。与条形码相比，其使用方便、灵活，在远距离、恶劣环境下，可对移动物体进行数据采集和自动识别，广泛应用于货物销售与分配、物流仓储管理、生产线自动化等方面。然而，RFID技术也存在安全隐患，信息泄漏影响了人们在消费习惯、个人行踪、商业机密等方面的隐私。为此，笔者提出了一种基于Hash函数和密钥的、适合于分布式数据库的认证协议。

1 RFID系统组成及安全需求

1.1 RFID系统的组成

RFID系统组成如图1所示。

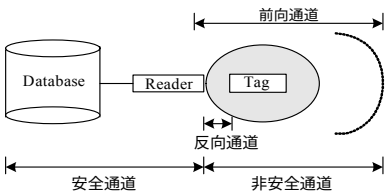

图1 RFID系统组成

(1)标签(Tag)

RFID的标签是由用于无线通信的耦合线圈电路和计算、存储数据的逻辑门电路组成。按照标签能量来源，可以将标签分为主动式和被动式两类。主动式标签是由附带在标签上的电池提供能量，具有较远的数据传送距离。被动式标签由线圈耦合提供能量，数据传送距离较近，具有低成本、永久生命周期等特点。

(2)读卡器(Reader)

读卡器由无线收发模块、天线、控制模块及接口电路等组成，具有读、写标签的能力。当发出询问命令且接收到标签返回的信息后，读卡器就将信息传送给后端数据库。

(3)后端数据库(Database)

后端数据库是可以运行在任何硬件平台的数据库系统。通常它具有巨大的数据分析和存储能力，包含了所有卡片的数据信息。

1.2 RFID系统的安全需求

为确保消费者隐私，RFID系统需满足如下安全需求[2]：

(1)不可分辨性

攻击者无法分辨标签输出的一种安全要求。一方面是指攻击者即使获得了来自于不同标签的输出，也无法区分出是哪一张标签的输出；另一方面是指即使攻击者获得了来自于同一张标签的多次输出，同样无法区分该张标签的输出。

(2)前向安全性

攻击者即使获得了标签发送的数据，也不能够回溯当前数据而获得标签历史事件数据。也就是说攻击者不能够通过联系当前数据和历史数据对标签进行分析，从而获得信息。

(3)重传攻击

在读卡器发出认证请求时，攻击者偷听获取到标签的响应。在下一论的认证过程中，攻击者发送已获得的数据至读卡器，从而通过认证。因此，RFID系统必须具有应对重传攻击的能力。

(4)哄骗攻击

攻击者伪装为合法读卡器，发送认证请求，进而获得标

基金项目：广东珠海科技基金资助项目(PC200320010)
作者简介：袁署光(1981－)，男，硕士，主研方向：RFID系统安全性；戴宏跃，副教授、博士；赖声礼，教授、博士生导师
收稿日期：2007-08-29 **E-mail：**sg_yuan@126.com

签响应输出。当合法读卡器询问标签时，攻击者将获得的标签响应发送给读卡器。这样攻击者屏蔽了真实标签的响应，通过读卡器的认证。

(5)通信量分析

对读卡器和标签的信息截取、分析，提取有用信息的过程。攻击者向标签发送多次的询问请求，接收标签返回数据。从获得的数据中分析标签的响应，达到跟踪标签的目的。

2 RFID 安全协议相关研究

随着RFID技术的广泛应用，研究人员已经认识到其面临的安全问题。研究者试图找到一种更有效、更加经济的方法来解决系统安全问题。已经有许多RFID安全协议[3-5]被提出，下面对其进行简单的介绍。

2.1 Hash 锁协议

Hash 锁协议是文献[4]提出的一种 RFID 安全协议。标签初始处于锁定状态，标签存储 *ID* 值及替代真实 *ID* 的 *metaID*，其中，*metaID*=*Hash*(*key*)；后端数据库存储每一个标签的密钥 *key*, *metaID*, *ID*。认证过程如图 2 所示。

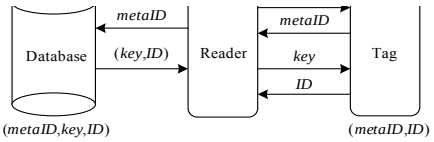

图 2　Hash 锁协议

该协议初步解决了访问控制的隐私保护，但是由于 *metaID* 保持不变，*ID* 也以明文的方式通过不安全信道传送，极易受到重传攻击和哄骗攻击，不具有不可分辨性，攻击者容易对标签进行跟踪。

2.2 随机 Hash 锁协议

随机Hash锁协议[4]是Hash锁协议的一种改进形式。标签中除Hash函数外，还嵌入了伪随机数发生器，后端数据库存储所有标签的*ID*，认证过程如图 3 所示。

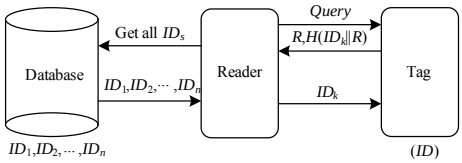

图 3　随机 Hash 锁协议

该协议利用随机数解决了标签的定位隐私问题。但是标签中集成了伪随机数发生器，在低成本和有限运算能力的情况下实现比较困难。同时标签仍然不能够应对重传和哄骗攻击。除此之外，后端数据库与读卡器的通行量较大，读卡器需要从所有的 ID 标识中查找出对应标签的标识，增加了读卡器的运算量。因此，该协议仍然不实用。

2.3 Hash 链协议

Hash链协议[5]中的标签集成了两个不同的Hash函数*H*和*G*。在系统运行前，标签和后端数据库都存储了初始值$s_{i,1}$，同时后端数据库还存储了所有标签的*ID*。认证过程见图 4。

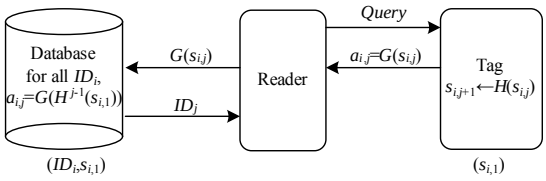

图 4　Hash 链协议

该协议利用标签每次更新标识满足了不可分辨性和前向安全性。然而，Hash 链协议是一个单向认证协议，它只对卡片进行认证，容易受到重传和哄骗攻击。标签中需要两个不同的 Hash 运算，增加了标签的成本。此外，在每次认证过程中，后端数据库都要对每个 *ID* 进行计算和比较。假设存在 *N* 个需要认证的标签，那么后端数据库就必须进行 *N* 次搜索、2*N* 次 Hash 计算、*N* 次比较，这增大了计算的负荷量。因此，该协议并不适合于大量标签系统。

2.4 基于 Hash 的 ID 变化协议

基于Hash的*ID*变化协议[4]与Hash链协议类似，在每一次认证过程中都改变了与读卡器的交换信息。在初始状态，标签中存储*ID*、*TID*(上次发送序号)、*LST*(最后一次发送序号)，且*TID*=*LST*；后端数据库中存储*H*(*ID*), *ID*, *TID*, *LST*, *AE*。认证过程如图 5 所示。

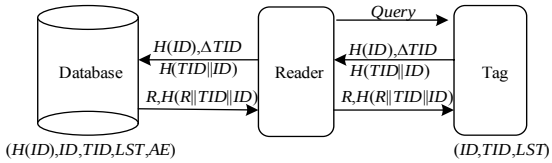

图 5　基于 Hash 的 *ID* 变化协议

该协议使用 *ID* 的变化，能够抵御重传和哄骗攻击，具有不可分辨性和前向安全性。然而，由于读卡器在标签之前已经完成了 *ID* 更新，容易造成数据的严重不同步而使标签丢失。同时由于每次认证 *ID* 都发生变化，因此不适合于分布式数据库环境。

3 基于 Hash 函数和密钥的认证协议

本文提出的协议同样采用了询问–应答机制。与上述相比，本协议同时具备了不可分辨性、前向安全性、重传攻击、哄骗攻击以及通行量分析等特点。由于 *ID* 保持不变，因此该协议能够运用于分布式数据库环境。同时，标签中只嵌入了一个 Hash 函数，适合低存储空间、低成本的应用。

3.1 初始条件及相关说明

在初始状态下，标签中存储标签的标识 *ID* 以及密钥 *key*，且嵌入了一个 Hash 函数运算(如 SHA-1, MD4)。阅读器含有一个随机数发生器。后端数据库存储所有标签的 *ID* 和密钥 *key*，能够进行各种复杂的计算。进行如下设定：

(1)H：$\{0,1\}^*\rightarrow\{0,1\}^l$是单向Hash函数，标签出厂时已经存储$R^0=H(key)$；

(2)S：读卡器产生的随机数；

(3)R^i：标签产生的第i个随机数；

(4)||：连接操作；

(5)?=：比较操作。

3.2 认证步骤

基于 Hash 函数和密钥的认证协议如图 6 所示。

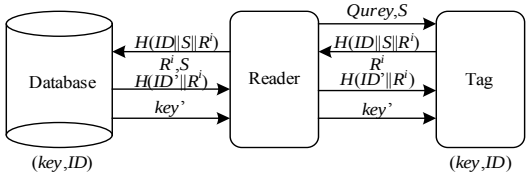

图 6　基于 Hash 函数和密钥的认证协议

对于第 *i* 次认证，步骤如下：

(1)读卡器产生一个随机数 *S*，并发送 *Query*,*S* 至标签作为认证请求；

(2)标签计算$R^i=H(key||R^{i-1}||S)$，并将R^i, $H(ID||S||R^i)$发送给读卡器；

(3)读卡器将R^i, $H(ID||S||R^i)$, S转发给后端数据库；

(4)后端数据库根据接收到的R^i, S，查找是否存在一个ID'，使得$H(ID'||S||R^i)?=H(ID||S||R^i)$。如果存在，则发送$H(ID'||R^i)$至读卡器，否则认证失败；

(5)读卡器转发$H(ID'||R^i)$给标签；

(6)标签验证$H(ID'||R^i)?=H(ID||R^i)$。如果相等，则认证通过，否则认证失败；

(7)为了保护用户隐私，当需要改变密钥时，可以设定新密钥 *new key*，并将 *key'=new key*⊕*old key* 发送给读卡器；

(8)读卡器转发 *key'*给标签；

(9)标签接收到 *key'*，根据旧密钥恢复出新密钥 *new key=old key*⊕*key'*。

这样系统就完成了整个认证过程及密钥更新。

3.3 安全分析

(1)不可分辨性：对于标签响应输出，由于Hash函数的单向性以及使用了随机数，因此攻击者即使获得了多张标签的输出，也无法区分出某一张标签的输出，即$H(ID'||S||R^i)\neq H(ID||S||R^i)$；即使获得了同一张标签的输出，也无法区分出该张标签的某一次输出，即$H(ID||S||R^i)\neq H(ID||S||R^j)$。

(2)前向安全性：假设攻击者获得了某次标签输出$H(ID||S||R^i)$, R^i，但由于Hash函数的单向性，因此攻击者无法根据当前获得的标签输出回溯标签的历史数据，具有前向安全性。

(3)重传攻击：攻击者执行如下操作：读卡器发送*Query*, *S*认证请求，攻击者监听获得标签输出$H(ID||S||R^i)$, R^i；当读卡器再次发送*Query*, *S*认证请求时，标签将上次监听得到的数据发送给读卡器，达到伪装合法标签目的。但是由于$H(ID||S||R^i)$的抗碰撞性以及R^i的随机性，标签输出$H(ID||S||R^i)\neq H(ID||S||R^j)$, $R^i\neq R^j$，其中，$i\neq j$。因此，能够抵御重传攻击。

(4)哄骗攻击：攻击者伪装为合法读卡器发送*Query*, *S'*至标签，标签响应请求，输出$H(ID||S||R^i)$, R^i。当合法读卡器发出认证请求时，攻击者发送刚才标签的响应以欺骗读卡器。但是由于每次认证读卡器都会产生一个随机数S，$H(ID||S||R^i)\neq H(ID||S'||R^i)$，因此攻击者不可能产生标签的正确响应。

(5)通信量分析：为了获得响应，攻击者伪装成读卡器发送*Query*, *S'*至标签，从而得到标签输出。攻击者试图通过分析$H(ID||S'||R^i)$, R^i来获得具体是哪张标签输出。但是，Hash函数的抗碰撞性和随机数保证了攻击者对标签的通信量分析攻击，从而攻击者无法跟踪标签。

(6)密钥窃取：当通过认证后用户需要更改密钥时，所更新的密钥是通过与旧密钥运算后的值。由于窃听者不知道旧密钥，因此即使用户获得了更新的密钥也不能得到新的密钥，从而防止了密钥丢失。

4 性能比较

表 1 描述了本文提出的协议与第 2 节中已提出协议的安全性能[2]比较，本协议不但具有其他协议的安全性能，而且用户可以根据需要修改密钥。其中，⊙表示具备该项要求；×表示不具备该项要求。

表 1 安全性能比较

功能指标	Hash 锁	随机 Hash 锁	Hash 链	*ID* 变化	本文协议
不可分辨性	×	⊙	⊙	⊙	⊙
前向安全性	⊙	⊙	⊙	⊙	⊙
重传攻击	×	×	×	⊙	⊙
哄骗攻击	×	×	×	×	⊙
通信量分析	×	×	⊙	⊙	⊙
同步	×	×	×	⊙	⊙
密钥修改	×	×	×	×	×
分布式环境	⊙	⊙	⊙	×	⊙

表 2 显示了该协议与其他协议的效率比较，其中，G表示随机数发生器。如果存储key,ID,R^i,S的长度为L，那么本协议中标签只需要 3L存储空间。标签通过一次Hash运算产生随机数R^i，不需要随机数发生器，大大减少了成本；后端数据库对于每次认证只需要作$(\sum ID/2)+1$ 次Hash操作，就能够适合于低计算量应用。

表 2 效率比较

协议名称	存储空间		计算量		
	标签	数据库	标签	读卡器	数据库
Hash 锁	2L	4L	1H	-	-
随机 Hash 锁	1L	1L	1H,1G	$(\sum ID/2)H$	-
Hash 链	1L	2L	2H	-	$(\sum ID/2)i$
ID 变化	3L	8L	3L	-	1G,3H
本文协议	3L	2L	3H	1G	$(\sum ID/2)+1$

5 结束语

本文提出了一种基于 Hash 函数和密钥的 RFID 安全认证协议，有效地解决了 RFID 系统当前面临的隐私问题。本协议具有如下优点：(1)保护全面；(2)密钥更改可以防止丢失；(3)适合于分布式数据库环境；(4)低成本、低存储空间、低计算量；(5)便于扩展，广泛用于物流管理、供应链、仓储管理、生产线自动化等领域，具有较高的实用价值。

参考文献

[1] 游战清, 李苏剑, 张益强. 无线射频识别技术(RFID)理论与应用[M]. 北京: 电子工业出版社, 2004.

[2] Osaka K, Takagi T. An Efficient and Secure RFID Security Method with Ownership Transfer[C]//Proc. of Computational Intelligence and Security. Guangzhou, China: [s. n.], 2006: 1090-1095.

[3] Hun-Wook K, Shu-Yun L, Hoon-Jae L. Symmetric Encryption in RFID Authentication Protocol for Strong Location Privacy and Forward-Security[C]//Proc. of Conference on Hybrid Information Technology. Cheju Island, Korea: [s. n.], 2006: 718-723.

[4] Zhang Lan, Zhou Huaibei, Kong Ruoshan. An Improved Approach to Security and Privacy of RFID Application System[C]//Proc. of Wireless Communications, Networking and Mobile Computing Conference. Wuhan, China: [s. n.], 2005: 1195-1198.

[5] Dimitriou T. A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks[C]//Proc. of Conference on Security and Privacy for Emerging Areas in Communications Networks. Athens, Greece: [s. n.], 2005: 59-66.