一种改进的Hash 函数 RFID 双向安全认证协议①

谌绍巍 陈 睿 凌 力 (复旦大学 通信科学与工程系 上海 200433)

摘 要： RFID 得到了越来越广泛的关注和应用，但是其存在安全和隐私保护的问题值得重视和关注。在现有的 RFID 认证协议的基础上，提出了一种改进的双向安全认证算法，利用 HASH 函数的单向性，较好地解决了 RFID 的安全隐患问题。该协议具有抗重放、抗分析、防伪造、防跟踪等特性，并且适用于大型分布式系统。

关键词： 射频标识；认证协议；Hash 函数；安全

An Improved Hash-Based RFID Two-Way Security Authentication Algorithm

CHEN Shao-Wei, CHEN Rui, LING Li

(School of Information Science and Engineering, Fudan University, Shanghai 200433, China)

Abstract: Although RFID technology has been increasingly popular and commonly used, there are still a host of defects in security and privacy. This paper proposes a new improved authentication protocol based on the existing protocols and Hash algorithm, and to some extent, it solves the security and privacy problems. This protocal can prevent replay attack, statistical analysis, spoofing attack, privacy track, and is suitable for the distributed system.

Keywords: RFID; authentication protocol; Hash algorithm; security

1 引言

射频标识(Radio Frequency Identification，RFID)技术是 20 世纪 90 年代开始兴起并逐渐走向成熟的一种自动识别技术。RFID 利用射频信号通过空间耦合(交变磁场或电磁场)实现无接触信息传递并通过所传递的信息达到识别目的的技术。

与目前广泛使用的自动识别技术(例如：二维码、条码、磁卡、IC 卡等)相比，射频识别技术具有非接触操作、无机械磨损、寿命长、可识别高速运动物体并可同时识别多个电子标签、安全性更高等突出的优点。然而 RIFD 技术也存在安全隐患，可能会造成信息泄漏、隐私泄漏等问题。因此本文提出了一种基于 HASH 算法和密钥的适于分布式数据库的认证协议。

2 RFID系统组成及安全需求分析

2.1 RFID 系统的组成

RFID 系统主要由标签(Tag)、天线(Antenna)、阅读器(Reader)、后台数据库(Database)几部分组成，图 1 为 RFID 系统及其信道的示意图：

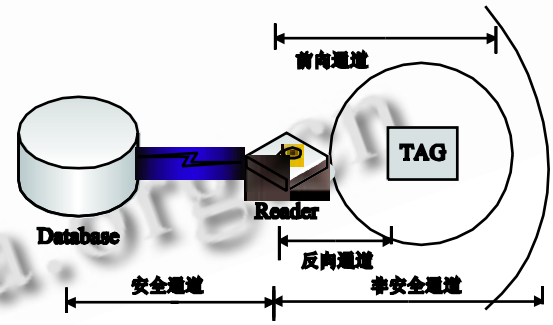

图 1 RFID 系统示意图

2.2 常见攻击分析和安全需求

如上图所见，RFID 系统中，反向通道和前向通道都是占用的无线信道，可以说是暴露在外的，因此很容易收到恶意的攻击和破坏。通常 RFID 系统受到的攻击有如下几种[1]：物理攻击、伪造攻击、重放攻击、使用者跟踪。在此之上，要求一个 RFID 系统应当具有以下的安全特性：

(1) 数据安全性和完整性

首先来说，阅读器和标签之间传输的信息应当是

① 收稿时间:2009-06-26

加密的，收到保护的，对于第三方的监听者无法从截取的信号中分析出信息的原本含义。同时要能保证所传递信息的完整性，一旦被攻击者篡改，通信双方应能分辨。这是系统安全最基本的要求。

(2) 私密性保护

私密性保护主要是为了解决 RFID 系统中可能出现的跟踪使用者而言的。私密性保护的含义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。

(3) 抗重放攻击性和抗通信分析

就是说在信息传递过程中应当保持一定的“随机性”，则攻击者无法通过重放截取的信息进行攻击以及在获得了大量的通信数据样本之后进行分析获得一定的规律性从而达到破解通信协议的可能性。

(4) 防伪造防抵赖

防伪造是值系统对伪造攻击的防范性。应当有一定的措施使攻击者无法进行阅读器和标签任一方的伪造。反过来也就是说，一旦认证成功，要保证对方一定是合法的阅读器或者标签，这也叫做防抵赖。在 RFID 系统中主要是针对防伪造。

2.3 RFID 系统的安全特殊性

RFID 安全的特殊性主要在于 RFID 芯片是低成本芯片，它的存储和计算能力非常有限，典型地，仅能存储几百位，大约有 5,000 至 10,000 个逻辑门，仅有 250 至 3,000 个逻辑门可用于安全功能，所以，很多成熟的密码算法无法直接应用于 RFID 芯片。

目前国内外对低成本标签安全技术进行了一些研究[2]，包括一些物理方法，如 Auto-IDCenter 自动识别中心的 Kill 命令机制方法，主要是对使用过的标签进行 Kill 破坏命令，使标签永久失效，这种方法带来的问题是限制了以后对标签的合法访问,而且标签的一次性使用增加了成本。还有静电屏蔽，也就是所谓的“法拉第罩”，即在标签上罩一个金属外罩，以防止非法防问，但同时屏蔽了授权读写器对标签的合法访问。主动干扰方法也存在同样的问题。而“Block Tag”方法额外增加了一个“附属标签”，增加了成本。

除了物理手段之外，则是基于密码学的加密算法，包括最小限度(minimalist)密码算法、重加密方法和基于 Hash 的方法。基于 Hash 的方法受到了广泛的关注，这是因为此类方法能够为读写器和标签之间提供双向认证，即同时解决用户隐私和标签克隆问题。并且，Hash 函数被认为是轻量级的密码学基本组件，能够在 RFID 芯片内实现。

3 相关技术和协议分析

3.1 Hash 锁协议

Hash 锁协议[3]为了保护标签的真实 ID，以 MetaID 来代替真实的 ID 用以认证操作。后台数据库存储标签的 ID、密钥以及 MetaID。认证过程如图 2：

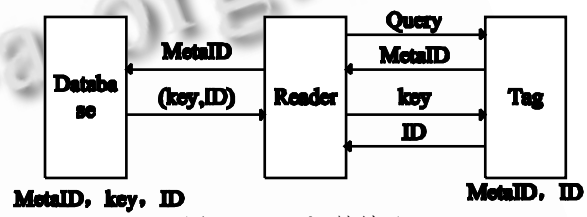

图 2　Hash 锁协议

该协议初步的提出了用 Hash 函数认证的想法，一定程度上解决了隐私保护问题。但是可以看到认证过程中 MetaID 是不变的，并且最后 ID 也以明文形式传输，因此非常容易收到重传攻击和哄骗攻击，并且不具有防跟踪性。

3.2 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。在此协议种提出了添加随机数以保证传输数据的不可测性的想法，认证过程如图 3：

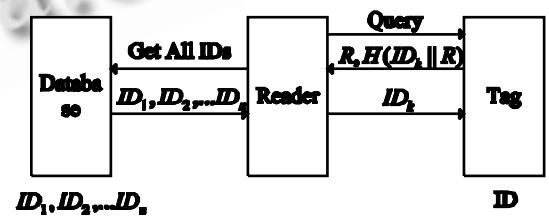

图 3　随机 Hash 锁协议

从图示过程可以看到，随机数的生成操作是由标签完成的，在低成本的标签条件下这个操作是不现实的。接下来这个步骤，数据库将所有的 ID 传输给阅读器，这一步的通行量很大，而且检索的工作交给了阅读器，增加了阅读器的工作量和整个认证的时间消耗；最后一步中 ID 仍然以明文形式传输，极易收到重传攻击和哄骗攻击。

3.3 Hash 链协议

Hash 链协议[5]中运用两个不同的 Hash 函数。在认证过程中不停的动态刷新标签认证所用的 ID。认证过程见图 4。

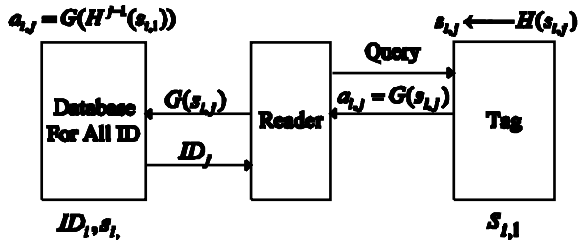

图 4　Hash 链协议

该协议由于添加了标签 ID 的动态更新机制，因此具有强的抗猜测抗分析，然而他的一个很重要的漏洞在于他的强安全性只在于单向的认证。也就是说，如果攻击者伪装成合法的阅读器，标签无法有效辨别对方真伪。同时，后台数据库的运算量非常大：如果有 N 个标签，则后台数据库需要进行 N 次搜索、2N 次 Hash 运算、N 次比较。因此该协议不适用于大量标签的系统。最后，由于动态刷新机制的存在，系统容易同步攻击，影响正常的认证过程。

4　基于Hash函数的改进协议设计

本文提出一个基于Hash函数的改进型RFID认证协议。这个协议在上述几个协议的基础上进行改进，克服了以上几个协议的明显漏洞。

4.1 初始环境和协议初步描述

首先，在发行 RFID 标签的时候，对每个标签入库登记。后台数据库的结构如表 1 所示

表 1　改进协议后台数据库结构

TagID	MetaID	Key
ID_1	m_1	k_1
ID_2	m_2	k_2
…	…	…
ID_n	m_n	k_n

对于每一个标签，不仅有自己的标示 ID，同时有一个 MetaID 和一个对应的“密钥”。

MetaID 的意义和 Hash-lock 协议里的定义一样，可以是标签本身 ID 的一个单向函数结果，比如：MetaID= $G(ID)$。其中 G 是一个 Hash 函数。

Key 的发布则同样保证对于不同的 TagID，key 应当不同。Key 在传输过程中是明文传输的，但是这并不影响系统的安全性。因为验证的时候一定要和另一个参数对应起来才能确认通信对方的可靠性。

另一方面。出场的标签在自己的芯片内同样将 TagID，MetaID 和 key 存储起来。

4.2 协议流程描述

协议的认证过程示意图如图 5 所示：

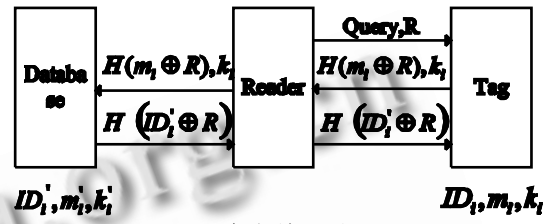

图 5　本文协议认证图

流程描述：

a．阅读器在发送 query 请求的同时，生成一个随机数 R，和 query 请求一同发送。

b．标签计算 $H(m_i\oplus R),k_i$ 并将结果发送回阅读器。

c．阅读器转发结果给数据库，根据 k_i 在数据库中查询，如查询到一个 $k_i'=k_i$，则读取出相应的 m_i' 和 ID_i'，并计算 $H\left(m_i'\oplus R\right)$，如果结果和 $H(m_i\oplus R)$ 相同，则标签通过验证，因为他有正确的 metaID 和 key 对。否则说明标签是非法的。

d．数据库计算 $H\left(ID_i'\oplus R\right)$ 并发送给阅读器，阅读器将之转发给标签。

e．标签从自己的存储空间读取出自己的 ID_i，并同样计算 $H\left(ID_i\oplus R\right)$，如果 $H\left(ID_i\oplus R\right)=H\left(ID_i'\oplus R\right)$，则说明阅读器/后台数据库是合法的，认证完成。否则说明阅读器是非法的。

4.3 协议特点分析

4.3.1 安全性分析

(1) 数据保密性

在此协议中，所有私密消息都通过一个单向的 Hash 函数加密，攻击者和监听者无法从截取的数据中解密得到原有信息。

(2) 抗重放攻击和哄骗攻击，抗数据分析

在改进协议中，对于每次加密操作，都添加了一个随机数，因此最后传输的消息都具有随机性，R 的添加使攻击者无法预测和控制，因此即使攻击者记录下一次通信中的数据，也无法通过重放该数据获得通信双方的任一方的验证。另外，随机性也让通信的数

据没有规律可循，有效的防止了数据分析攻击。

(3) 防伪造

在双方的两次认证中，均以配对的两个参数来验证身份，并且用于验证的参数均经过 Hash 单向加密，保证了只有原本就持有正确参数的对方才能通过验证，攻击者无法伪造身份。

(4) 防跟踪/私密性保护

不可跟踪性的非形式化定义具有比较统一的认识，在多种文献中‘5J1J21 都使用了类似定义：如果攻击者不能从一个协议通信报文集中区分出两个具有不同密钥的标签，则称这个 RFID 协议具有不可跟踪性。

容易看出，在本协议中，如果攻击者获取了大量的通信数据，也无法判别出哪些数据属于哪个标签；同样，即使攻击者获取了同一张标签的多次输入也无法进行区分。

4.3.2 算法分析和相关比较

在算法复杂度上，标签在整个验证过程中总共进行 2 次 Hash 运算，2 次异或运算；阅读器需要进行一次随机数的生成计算；后台数据库需要进行 2 次 Hash 运算。

在算法空间度上，标签和数据库都需要存放 ID_i 、m_i 和 k_i 三组数据。

下表标示了本文协议和第三节中的协议的安全性能比较。其中×标示不安全，√表示安全

表 2　协议安全性能比较

安全性能指标	Hash 锁	随机 Hash 锁	Hash 链	本文协议
抗跟踪	×	√	√	√
前向安全性/抗窃听	√	√	√	√
重传攻击	×	×	×	√
哄骗攻击	×	×	×	√
通信量分析	×	×	√	√
分布式环境	√	√	√	√

下表是效率比较，其中 H 表示 Hash 运算，R 表示随机数生成计算

表 3　协议效率比较

协议名称	计算量			存储空间	
	标签	阅读器	数据库	标签	数据库
Hash-lock 协议	1H	-	-	2L	4L
随机 Hash 协议	1H，1R	$(\sum ID/2)$H	-	1L	1L
Hash 链协议	2H	-	$(\sum ID/2)$H	1L	2L
本协议	2H	1R	2H	3L	3L

从上述分析中可以看到，本文的协议在安全性上是最完善的，对于在第二节中分析的各种攻击手段都具有强抵抗性。同时本文协议在计算量上将计算强度相对于随机 Hash 协议和 Hash 链协议减少了很多，标签和数据库在整个验证过程中都只进行 2 次 Hash 运算，可以节省大量的认证时间；虽然相比 Hash-lock 协议增加了一定的运算，但是这些运算总的占用资源量还是很少的，并且增加的运算相对 Hash-lock 协议极大的提高了安全性。存储空间上，和 Hash-lock 协议差不多，只是相对后两种协议有了稍微的提高。可以认为本协议是一种较好的时间空间折衷考虑。

5　结论

本文在现有的基于Hash函数的RFID认证协议上，提出了一种改进的协议方法。该方法在安全性、可靠性、抗攻击性上都相对已有协议有不同程度的提高和完善，同时运算量小、储存需求不大、执行效率高，非常适合低成本的 RFID 系统，且可以运用在大规模的分布式数据库认证系统上，具有较高的实用价值。

参考文献

1 Juels A. RFID Security and Privacy--A Research Survey. IEEE Journal on Selected Areas in Communications, 2006,24(2):382－387.

2 Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A. RFID Systems: A Survey on Security Threats and Proposed Solutions. P. Cuenca and L. Orozco-Barbosa eds. Personal Wireless Communications LNCS 4217. Berlin: Springer-Verlag, 2006:159－170.

3 Sarma S, Weis S, Engels D. RFID Systems and Security and Privacy Implications. Proc. of CHES'02. Springer,2002:454－469.

4 W. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. Security in Pervasive Computing. 2003.201－212.

5 Avoine G, Oechslin P. A Scalable and Provably Secure Hash Based RFID Protocol. The 2nd IEEE International Workshop on Pervasive Computing and Communication Security(PerSec). 2005.125－140.