RFID 安全协议的设计与分析

周永彬 冯登国

(中国科学院软件研究所信息安全国家重点实验室 北京 100080)

摘 要 回顾了已有的各种 RFID 安全机制,重点介绍基于密码技术的 RFID 安全协议;分析了这些协议的缺陷;讨论了基于可证明安全性理论来设计和分析 RFID 安全协议的模型和方法.

关键词 RIFD 系统;安全协议;可证明安全性;安全模型

中图法分类号 TP309

Design and Analysis of Cryptographic Protocols for RFID

ZHOU Yong-Bin FENG Deng-Guo

(*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing* 100080)

Abstract Recently, RFID system is being widely considered as a main technology to realize ubiquitous computing environment, but the features of the RFID systems and the constraints of RFID devices may bring about various privacy problems. The biggest challenge for RFID technology is to provide benefits without threatening the privacy of consumers. This paper reviews the existing RFID system security mechanisms, with a focus on cryptographic protocols. Weaknesses or flaws in these protocols are examined. Then a theoretical model and method to design and analyze RFID protocols within the provable security framework is discussed.

Keywords RFID system; cryptographic protocol; provable security; security model

1 引 言

无线射频识别(RFID)系统是使用无线射频技术在开放系统环境中进行对象识别.这种识别的优点之一是无需物理接触或其它任何可见的接触.现在,许多人已将 RFID 系统看作是一项实现普适计算环境的有效技术.RFID 应用十分广泛,例如,它可以用于生产和销售管理场合以简化供应链管理并实现对存货成本的有效控制,可以代替传统的二维条形码用于数字图书馆管理,可用于动物研究和饲养中的动物识别,可用于防伪造的电子护照系统,甚至可以用于构建智能自组网络环境,等等.

部署和使用 RFID 系统时,关键的问题之一是要确保只有授权用户能够识别各个标签(Tag),而攻击者无法对这些标签进行任何形式的跟踪.尽管可追踪性问题(最主要的 RFID 保密性问题)经常被这项技术的支持者所低估,抑或有时被其责难者所夸大,但它确实阻碍了这项技术的推广和应用.使用密码学方法来解决可追踪性问题是一种被研究了多年的方法.迄今为止,已经有许多 RFID 安全协议被提出,如 Hash-Lock 协议[1,2]、随机化 Hash-Lock 协议[3]、Hash 链协议[4]、基于杂凑的 ID 变化协议[5]、David 的数字图书馆 RFID 协议[6]、分布式 RFID 询问-响应认证协议[7]、LCAP 协议[8]、再次加密机制[9,10]等等.但是,到目前为止,还缺乏一个实用的形式化的 RFID 系统攻击者模型,当然更缺乏

收稿日期:2005-12-13;修改稿收到日期:2006-01-13.本课题得到国家自然科学基金(60503014,60273027,60573042)资助.周永彬,男,1973 年生,博士,副研究员,主要研究领域为网络与信息安全理论与技术. E-mail: zhouyongbin@sina.com.冯登国,男,1965 年生,博士,研究员,博士生导师,目前主要从事信息和网络安全的研究.

针对这些协议进行的严格的形式化分析和证明.

尽管用于认证和识别用途的密码技术已相对比较成熟,但是,到目前为止,由于组成 RFID 系统的必备设备 Tag 的特殊性和局限性,设计安全、高效、低成本的 RFID 安全机制仍然是一个具有挑战性的课题. 本文将详细介绍这类协议,并分析这些协议中所存在的安全缺陷. 现有的基于密码技术的 RFID 安全机制大致可以分为两大类:静态 ID 机制以及动态 ID 刷新机制. 所谓"静态 ID 机制"就是 Tag 的标识保持不变,而"动态 ID 刷新机制"则是 Tag 的标识随着每一次 Tag 与 Tag 读写器之间的交互而动态变化. 采用动态 ID 刷新机制时,一个非常重要的问题就是"数据同步问题",也就是说,后端数据库中所保存的 Tag 标识必须和存储在 Tag 中的标识同步进行刷新,否则,在下一次认证识别过程中就可能出现合法 Tag 无法通过认证和识别的系统异常. 此外,与其它系统设备不同,在 RFID 系统中,Tag 面临的一个其它设备通常不会面对的主要威胁就是它很有可能会突然掉电(例如,绝大多数低成本的 Tag 都是依靠外部环境的电磁感应供给能量),这种情况出现时,我们希望 RFID 安全协议或机制应该仍然是健壮的(Sudden-loss-of-Power Robust).

基于可证明安全性理论和方法来进行安全协议的设计和分析,是近来安全协议研究领域的一个重要的研究方向,相关研究也取得了较为丰富的成果. 但是,使用可证明安全性理论和方法来设计和分析 RFID 协议的研究还很少. 针对这个问题,本文进行了尝试性探索,提出了一个 RFID 协议安全模型,并给出了相应的安全性定义.

本文第 2 节简要介绍 RFID 系统的基本构成、通信模型以及基本的安全需求和安全机制;第 3 节介绍已有的 RFID 协议,分析这些协议中存在的安全缺陷和安全漏洞;第 4 节讨论使用可证明安全性理论和方法来分析 RFID 安全协议安全性的方法,提出一个 RFID 系统攻击者模型,并且定义 RFID 协议的安全性;第 5 节总结全文.

2 RFID 系统的基本构成与安全需求

本部分将简要介绍 RFID 系统的基本构成、通信模型以及基本的安全需求等.

2.1 RFID 系统的基本构成

RFID 系统一般由三大部分构成:RFID 标签(Tag)、RFID 标签读写器以及后端数据库,如图 1 所示.

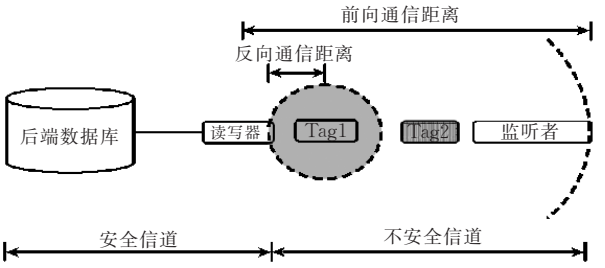


图 1 RFID 系统基本构成

后端数据库可以是运行于任意硬件平台的数据库系统,可由用户根据实际的需要自行选择,通常假设其计算和存储能力强大,同时它包含所有 Tag 的信息. Tag 读写器实际是一个带有天线的无线发射与接收设备,它的处理能力、存储空间都比较大. RFID 标签是配备有天线的微型电路. Tag 通常没有微处理器,仅由数千个逻辑门电路组成,因此要将加密或者签名算法集成到这类设备中确实是一个不小的挑战. Tag 和 Tag 读写器之间的通信距离受到多个参数的影响,特别是通信频率. 目前,主要有两种通信频率的 RFID 系统共存:一种使用 13.56MHz,一种使用 860~960MHz(通信距离更长).

依据其能量来源,可以将 Tag 分为三大类:被动式 Tag、半被动式 Tag 以及主动式 Tag,其特点如表 1 所示.

表 1 Tag 分类及其特点

	能量来源	发送器	最大距离(m)
被动式 Tag	被动式	被动	10
半被动式 Tag	内部电池	被动	100
主动式 Tag	内部电池	主动	1000

依据其功能,可以将 Tag 分为五大类:Class 0,Class 1,Class 2,Class 3 和 Class 4,其功能依次增强,如表 2 所示.

表 2 Tag 分类及其功能

种类	能量来源	别名	存储	特点
Class 0	被动式	防盗窃 Tag	None	EAS 功能
Class 1	任意	EPC	只读	仅用于识别
Class 2	任意	EPC	读写	数据日志记录
Class 3	内部电池	传感器 Tag	读写	环境传感器
Class 4	内部电池	智能颗粒	读写	自组网络

Tag 读写器到 Tag 之间的信道称为"前向信道"(forward channel),而 Tag 到 Tag 读写器之间的信道则称为"反向信道"(backward channel). 由于 Tag 读写器与 Tag 的无线功率差别很大,前向信道的通信范围远远大于反向信道的通信范围. 这种固有的信道"非对称"性自然会对 RFID 系统安全机制的设计和分析产生极大的影响.

一般而言,我们通常做如下基本假设:Tag 与

Tag 读写器之间的通信信道是不安全的，而 Tag 读写器与后端数据库之间的通信信道则是安全的. 这也是出于对 RFID 系统设计、管理和分析方便的考虑.

2.2　RFID 系统的通信模型

ISO/IEC 18000 标准定义了 Tag 读写器与 Tag 之间的双向通信协议[11]，其基本的通信模型如图 2 所示.

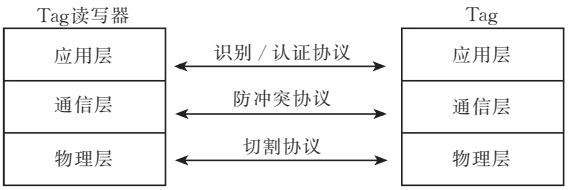


图 2　RFID 系统的通信模型

由图 2 可以看出，RFID 系统的通信模型由三层组成，从下到上依次为：物理层、通信层和应用层. 物理层主要关心的是电气信号问题，例如频道分配、物理载波等，其中最重要的一个问题就是要载波“切割”(singulation)问题. 通信层定义了 Tag 读写器与 Tag 之间双向交换数据和指令的方式，其中最重要的一个问题就是解决多个 Tag 同时访问一个 Tag 读写器时的冲突问题；应用层用于解决和最上层应用直接相关的内容，包括认证、识别以及应用层数据的表示、处理逻辑等. 通常情况下，我们所说的 RFID 安全协议指的就是应用层协议，本文所讨论的所有 RFID 协议都属于这个范畴.

但是，也有学者认为，可追踪性问题必须针对 RFID 通信模型的各层来整体解决，任何一个单层面的解决方案都是不全面的，都有可能导致 RFID 系统出现明显的安全弱点和漏洞[12]. 实际上，这一观点与信息安全中的“深度防御”策略不谋而合. 除此之外，我们还认为，在部署和实施 RFID 系统的安全方案时，同时还应该综合考虑多种其它因素，例如可扩展性、系统开销、可管理性等.

2.3　RFID 系统的安全需求

RFID Tag 设备具有一些局限性，例如有限的计算能力、有限的存储空间(RFID 标签的存储空间极其有限，最便宜的 Tag 只有 64～128bit 的 ROM，仅可容纳唯一标识符)、外形很小、电源供给有限等. 所有这些特点和局限性都对 RFID 系统安全机制的设计带来了特殊的要求，也使得设计者对密码机制的选择受到很多限制. 正因为此，设计安全、高效、低成本的 RFID 协议成为了一个新的具有挑战性的问题，也吸引了许多国际一流密码学家的关注和投入(如 Rivest，Wanger 等)[3,6,13].

RFID 系统很容易受到各种攻击，主要由于它的通信过程中没有任何物理或者可见的接触(通过电磁波的形式进行). 因此，RFID 系统必须能够抵抗各类形式的攻击，如监听、主动攻击、跟踪以及拒绝服务等. 一般说来，一个安全的 RFID 系统都应该解决如下 3 个基本的安全问题：保密性、信息泄漏和可追踪性.

2.4　RFID 安全机制

当前，实现 RFID 安全性机制所采用的方法主要有三大类：物理方法、密码机制以及二者的结合，下面对其进行简要的介绍.

2.4.1　物理安全机制

使用物理方法来保护 RFID Tag 安全性的方法主要有如下几类：Kill 命令机制[3]、静电屏蔽[2]、主动干扰[13]以及 Blocker Tag 方法[13]等. 这些方法主要用于一些低成本的 Tag 中，之所以如此，主要是因为这类 Tag 有严格的成本限制，因此难以采用复杂的密码机制来实现与 Tag 读写器之间的安全通信.

“Kill 命令机制”采用从物理上毁坏 Tag 的办法. 一旦对 Tag 实施了 Kill 毁坏命令，Tag 便不可能再被重用；此外，另外一个重要的问题就是难以验证是否真正对 Tag 实施了 Kill 操作. “静电屏蔽”(也称为“Faraday Cage”)可以对 Tag 进行屏蔽，使之不能接收任何来自 Tag 读写器的信号，但是这自然需要一个额外的物理设备，既造成了不便，也增加了系统的成本. “主动干扰”机制则可能带来法律问题，而“Blocker Tag”方法也需要一个额外的 Tag. 鉴于物理安全机制存在的种种缺点，在最近的 RFID 系统中，提出了许多基于密码技术的安全机制.

2.4.2　基于密码技术的安全机制

与基于物理方法的硬件安全机制相比，基于密码技术的软件安全机制受到人们更多的青睐，其主要研究内容则是利用各种成熟的密码方案和机制来设计和实现符合 RFID 安全需求的密码协议. 这已经成为当前 RFID 安全研究的热点. 目前，已经提出了多种 RFID 安全协议，例如 Hash-Lock 协议[1,2]、随机化 Hash-Lock 协议[3]、Hash 链协议[4]等. 但是，遗憾的是，现有的大多数 RFID 协议都存在着各种各样的缺陷，第 3 节将对此进行详细的分析.

3　RFID 安全协议

到目前为止，已有多种 RFID 安全协议被提出.

分析这类协议时，我们仍然基于关于 RFID 系统信道的基本假设来进行. 此外，我们还假定这些协议所使用的基本密码构造，如伪随机生成函数、加密体制、签名算法、MAC 机制以及杂凑函数等[14]，都是安全的. 本文中，我们用 H 和 G 来表示两个不同的抗碰撞的安全杂凑函数，f 则表示一个安全的伪随机函数.

3.1 Hash-Lock 协议

Hash-Lock 协议[1,2] 是由 Sarma 等人提出的，为了避免信息泄漏和被追踪，它使用 $metaID$ 来代替真实的标签 ID. 其协议流程如图 3 所示.

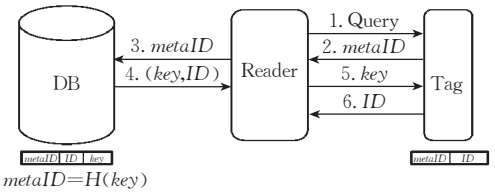


图 3 Hash-Lock 协议

Hash-Lock 协议的执行过程如下：

1. Tag 读写器向 Tag 发送 Query 认证请求；

2. Tag 将 $metaID$ 发送给 Tag 读写器；

3. Tag 读写器将 $metaID$ 转发给后端数据库；

4. 后端数据库查询自己的数据库，如果找到与 $metaID$ 匹配的项，则将该项的 (key, ID) 发送给 Tag 读写器，其中 ID 为待认证 Tag 的标识，$metaID = H(key)$；否则，返回给 Tag 读写器认证失败信息；

5. Tag 读写器将接收自后端数据库的部分信息 key 发送给 Tag；

6. Tag 验证 $metaID = H(key)$ 是否成立，如果成立，则将其 ID 发送给 Tag 读写器；

7. Tag 读写器比较自 Tag 接收到的 ID 是否与后端数据库发送过来的 ID 一致，如一致，则认证通过；否则，认证失败.

由上述过程可以看出，Hash-Lock 协议中没有 ID 动态刷新机制，并且 $metaID$ 也保持不变，ID 是以明文的形式通过不安全的信道传送，因此 Hask-Lock 协议非常容易受到假冒攻击和重传攻击，攻击者也可以很容易地对 Tag 进行追踪. 也就是说，Hask-Lock 协议完全没有达到其安全目标.

3.2 随机化 Hash-Lock 协议

随机化 Hash-Lock 协议[3] 由 Weis 等人提出，它采用了基于随机数的询问-应答机制，其协议流程如图 4 所示.

随机化 Hash-Lock 协议的执行过程如下：

1. Tag 读写器向 Tag 发送 Query 认证请求；

2. Tag 生成一个随机数 R，计算 $H(ID_k \| R)$，其中 ID_k 为 Tag 的标识. Tag 将 $(R, H(ID_k \| R))$ 发送给 Tag 读写器；

3. Tag 读写器向后端数据库提出获得所有 Tag 标识的请求；

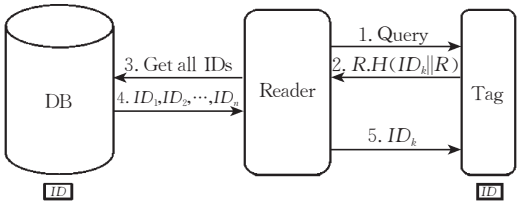


图 4 随机化 Hash-Lock 协议

4. 后端数据库将自己数据库中的所有 Tag 标识 $(ID_1, ID_2, \cdots, ID_n)$ 发送给 Tag 读写器；

5. Tag 读写器检查是否有某个 ID_j $(1 \le j \le n)$，使得 $H(ID_j \| R) = (ID_k \| R)$ 成立；如果有，则认证通过，并将 ID_j 发送给 Tag；

6. Tag 验证 ID_j 与 ID_k 是否相同，如相同，则认证通过.

在随机化 Hash-Lock 协议中，认证通过后的 Tag 标识 ID_k 仍以明文的形式通过不安全信道传送，因此攻击者可以对 Tag 进行有效的追踪. 同时，一旦获得了 Tag 的标识 ID_k，攻击者就可以对 Tag 进行假冒. 当然，该协议也无法抵抗重传攻击. 因此，随机化 Hash-Lock 协议也是不安全的.

不仅如此，每一次 Tag 认证时，后端数据库都需要将所有 Tag 之标识发送给读写器，二者之间的数据通信量很大. 就此而言，该协议也不实用.

3.3 Hash 链协议

本质上，Hash 链协议[4] 也是基于共享秘密的询问-应答协议. 但是，在 Hash 链协议中，当使用两个不同杂凑函数的 Tag 读写器发起认证时，Tag 总是发送不同的应答，其协议流程如图 5 所示. 值得提出的是，作者声称 Hash 链协议具有完美的前向安全性.

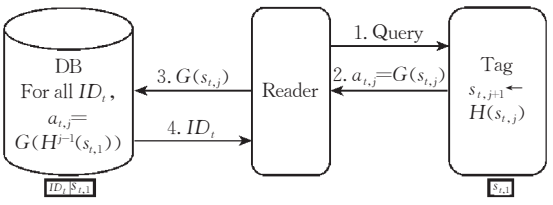


图 5 Hash 链协议

在系统运行之前，Tag 和后端数据库首先要预共享一个初始秘密值 $s_{t,1}$，则 Tag 和 Tag 读写器之间执行第 j 次 Hash 链的过程如下：

1. Tag 读写器向 Tag 发送 Query 认证请求；

2. Tag 使用当前的秘密值 $s_{t,j}$ 计算 $a_{t,j} = H(s_{t,j})$，并更新其秘密值为 $s_{t,j+1} = H(s_{t,j})$. Tag 将 $a_{t,j}$ 发送给 Tag 读写器；

3. Tag 读写器将 $a_{t,j}$ 转发给后端数据库；

4. 后端数据库系统针对所有的 Tag 数据项查找并计算是否存在某个 ID_t $(1 \le t \le n)$ 以及是否存在某个 j $(1 \le t \le m$，其中 m 为系统预设置的最大链长度$)$ 使得 $a_{t,j} =$

$G(H^{j-1}(s_{t,1}))$成立. 如果有，则认证通过，并将ID_i发送给 Tag；否则，认证失败.

实质上，在 Hash 链协议中，Tag 成为了一个具有自主 ID 更新能力的主动式 Tag，如图 6 所示. 同时，由上述流程可以看出，Hash 链协议是一个单向认证协议，即它只能对 Tag 身份进行认证. 不难看出，Hash 链协议非常容易受到重传和假冒攻击，只要攻击者截获某个 $a_{t,j}$，它就可以进行重传攻击，伪装 Tag 通过认证. 此外，每一次 Tag 认证发生时，后端数据库都要对每一个 Tag 进行 j 次杂凑运算，因此其计算载荷也很大. 同时，该协议需要两个不同的杂凑函数，也增加了 Tag 的制造成本.

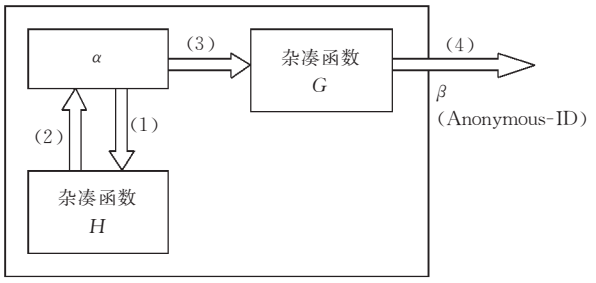


图 6　Hash 链协议中的主动式 Tag 原理

3.4　基于杂凑的 *ID* 变化协议

基于杂凑的 ID 变化协议[5] 与 Hash 链协议相似，每一次回话中的 ID 交换信息都不相同. 该协议可以抗重传攻击，因为系统使用了一个随机数 R 对 Tag 标识不断进行动态刷新，同时还对 TID（最后一次回话号）和 LST（最后一次成功的回话号）信息进行更新，其协议流程如图 7 所示.

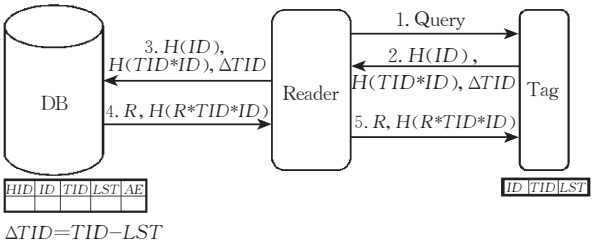


图 7　基于杂凑的 ID 变化协议

基于杂凑的 ID 变化协议的执行过程如下：

1. Tag 读写器向 Tag 发送 Query 认证请求；

2. Tag 将当前回话号加 1，并将 $H(ID)$，$H(TID*ID)$，ΔTID 发送给 Tag 读写器；其中，$H(ID)$可以使得后端数据库恢复出 Tag 的标识，ΔTID 则可以使得后端数据库恢复出 TID，进而计算出 $H(TID*ID)$；

3. Tag 读写器将 $H(ID)$，$H(TID*ID)$，ΔTID 转发给后端数据库；

4. 依据所存储的 Tag 信息，后端数据库检查所接收到数据的有效性. 如果所有的数据全部有效，则它产生一个秘密随机数 R，并将$(R, H(R*TID*ID))$发送给 Tag 读写器. 然后，数据库更新该 Tag 的 ID 为 $ID \oplus R$，并相应地更新 TID 和 LST.

5. Tag 读写器将 R，$H(R*TID*ID)$转发给 Tag；

6. Tag 验证所接收的信息的有效性；如果有效，则认证通过.

由上述可知，Tag 是在接收到消息 5 且验证通过之后才更新其 ID 和 LST 信息的，而在此之前，后端数据库已经成功地完成相关信息的更新. 因此，如果此时攻击者进行攻击（例如，攻击者可以伪造一个假消息，或者干脆实施干扰使 Tag 无法接收到该消息），则就会在后端数据库和 Tag 之间出现严重的数据不同步问题. 这也就意味着合法的 Tag 在以后的回话中将无法通过认证. 也就是说，该协议不适合于使用分布式数据库的普适计算环境，同时存在数据库同步的潜在安全隐患.

3.5　David 的数字图书馆 RFID 协议

David 等提出的数字图书馆 RFID 协议[6] 使用基于预共享秘密的伪随机函数来实现认证，其协议流程如图 8 所示.

系统运行之前，后端数据库和每一个 Tag 之间需要预先共享一个秘密值 s. 该协议的执行过程如下：

1. Tag 读写器生成一秘密随机数 R_R，向 Tag 发送 Query 认证请求，将 R_R发送给 Tag；

2. Tag 生成一个随机数 R_T，使用自己的 ID 和秘密值 s 计算$\sigma = ID \oplus f_s(0, R_R, R_T)$. Tag 将$(R_T, \sigma)$发送给 Tag 读写器；

3. Tag 读写器将(R_T, σ)转发给后端数据库；

4. 后端数据库检查是否有某个 ID_j $(1 \le j \le n)$，使得 $ID_j = \sigma \oplus f_s(0, R_R, R_T)$ 成立；如果有，则认证通过，并计算 $\beta = ID_i \oplus f_s(1, R_R, R_T)$，然后将 β 发送给 Tag 读写器；

5. Tag 读写器将 β 转发给 Tag；

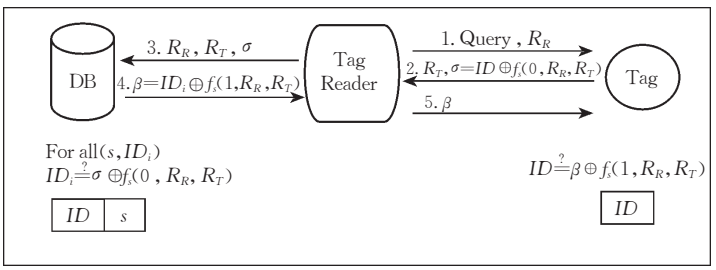


图 8　David 的数字图书馆 RFID 协议

6. Tag 验证 $ID=\beta\oplus f_s(1,R_R,R_T)$ 是否成立，如成立，则认证通过.

到目前为止，还没有发现该协议具有明显的安全漏洞. 但是，为了支持该协议，必需在 Tag 电路中包含实现随机数生成以及安全伪随机函数两大功能模块，故而该协议完全不适用于低成本的 RFID 系统.

3.6 分布式 RFID 询问-应答认证协议

Rhee 等人提了一种适用于分布式数据库环境的 RFID 认证协议，它是典型的询问-应答型双向认证协议[7]，其协议流程如图 9 所示.

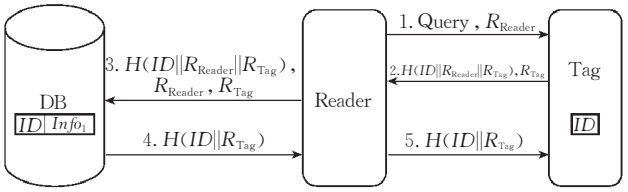


图 9 分布式 RFID 询问-应答认证协议

该分布式 RIFD 询问-应答协议的执行过程如下：

1. Tag 读写器生成一秘密随机数 R_{Reader}，向 Tag 发送 Query 认证请求，将 R_{Reader} 发送给 Tag；

2. Tag 生成一随机数 R_{Tag}，计算 $H(ID\parallel R_{\text{Reader}}\parallel R_{\text{Tag}})$，其中 ID 为 Tag 之标识. Tag 将 $(H(ID\parallel R_{\text{Reader}}\parallel R_{\text{Tag}}),R_{\text{Tag}})$ 发送给 Tag 读写器；

3. Tag 读写器将 $(H(ID\parallel R_{\text{Reader}}\parallel R_{\text{Tag}}),R_{\text{Reader}},R_{\text{Tag}})$ 发送给后端数据库；

4. 后端数据库检查是否有某个 $ID_j\ (1\le j\le n)$，使得 $H(ID_j\parallel R_{\text{Reader}}\parallel R_{\text{Tag}})=H(ID\parallel R_{\text{Reader}}\parallel R_{\text{Tag}})$ 成立；如果有，则认证通过，并将 $H(ID_j\parallel R_{\text{Tag}})$ 发送给 Tag 读写器；

5. Tag 验证 $H(ID_j\parallel R_{\text{Tag}})=H(ID\parallel R_{\text{Tag}})$ 是否相同，如相同，则认证通过.

到目前为止，还没有发现该协议有明显的安全漏洞或缺陷. 但是，在本方案中，执行一次认证协议需要 Tag 进行两次杂凑运算. Tag 电路中自然也需要集成随机数发生器和杂凑函数模块，因此它也不适合于低成本 RFID 系统.

3.7 LCAP 协议

LCAP 协议[8]也是询问-应答协议，但是与前面的同类其它协议不同，它每次执行之后都要动态刷新 Tag 的 ID，其协议流程如图 10 所示.

LCAP 协议的执行过程如下：

1. Tag 读写器生成一秘密随机数 R，向 Tag 发送 Query 认证请求，将 R 发送给 Tag；

2. Tag 计算 $HaID=H(ID)$ 和 $H_L(ID\parallel R)$，其中 ID 为 Tag 之标识，H_L 表示杂凑函数 H 输出的左半部分. Tag 将 $(HaID,H_L(ID\parallel R))$ 发送给 Tag 读写器；

3. Tag 读写器将 $(HaID,R,H_L(ID\parallel R))$ 发送给后端数据库；

4. 后端数据库检查 Prev 数据条目中 $HaID$ 的值是否与所接收到的 $HaID$ 一致. 如果一致，则使用 R 和 Prev 数据条目中的 ID 信息来计算 $H_R(ID\parallel R)$，其中 H_R 表示杂凑函数 H 输出的右半部分. 然后，后端数据库更新 Curr 数据条目中的信息如下：$HaID=H(ID\oplus R)$，$ID=ID\oplus R$. Prev 数据条目中的 TD 数据域设为 $HaID=H(ID\oplus R)$. 最后，将 $H_R(ID\parallel R)$ 发送给 Tag 读写器.

5. Tag 读写器将 $H_R(ID\parallel R)$ 转发给 Tag.

6. Tag 验证 $H_R(ID\parallel R)$ 的有效性. 如果有效，则更新其 ID 为 $ID=ID\oplus R$.

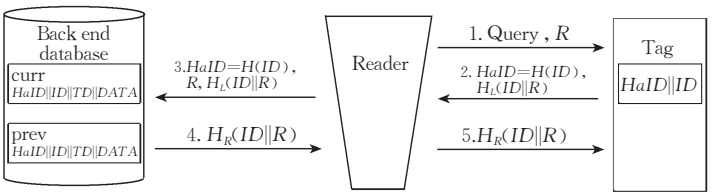


图 10 LCAP 协议

由上述可知，Tag 是在接收到消息 5 且验证通过之后才更新其 ID 的，而在此之前，后端数据库已经成功完成相关 ID 的更新. 因此，与基于杂凑的 ID 变化协议的情况类似，LCAP 协议也不适合于使用分布式数据库的普适计算环境，同时亦存在数据库同步的潜在安全隐患.

3.8 再次加密机制(Re-encryption)

RFID 标签的计算资源和存储资源都十分有限，因此极少有人设计使用公钥密码体制的 RFID 安全机制. 到目前为止，公开发表的基于公钥密码机制的 RFID 安全方案只有两个：(1) Juels 等人提出的用于欧元钞票上 Tag 标识的建议方案[9]；(2) Golle 等人提出的可用于实现 RFID 标签匿名功能的方案[15].

上述两种方案都采用了再次加密机制，但两者还是有显著的不同：Juels 等人的方案基于一般的安全的公钥加密/签名方案，同时给出了一种基于椭圆曲线体制的实现方案(包括安全参数的选择，有关性能分析等)；在这种方案中，完成再次加密的实体知道被加密消息的所有知识(本方案中特指钞票的序列号). 而 Golle 等人的方案则采用了基于 ElGamal 体制的“通用再加密”(Universal Re-ecryption)技

术，这种方案中，完成对消息的再次加密无需知道关于初始加密该消息所使用的公钥的任何知识. 到目前为止，还没有发现 Juels 等人方案的明显安全漏洞和弱点，但是 Golle 等人提出的方案被指出存在安全弱点和漏洞[10,16].

4　RFID 协议的安全模型及安全性

密码协议的安全性分析和证明长期以来一直是信息安全研究的热点和难点问题，从事计算机科学和密码学研究的人员对此进行了不懈的研究，也取得了较为丰硕的研究成果；但是，时至今日，这个问题仍然没有很好地解决. 密码协议和其它协议不同，人们也许永远无法知道攻击者下一步将采取什么样的攻击手段，有时甚至恰恰就是在那些被认为相当安全的细节之处出现了微妙的漏洞，要知道即便这样一个微小的漏洞或缺陷有时对于一个聪明的攻击者来说已经足够. 也许，这也正是密码协议安全设计和分析的魅力所在.

证明密码协议的正确性与安全性的理论和方法通常可以分为两大类：形式化方法和计算复杂性方法[17]. 形式化方法可使协议设计者通过系统分析将注意力专注于接口、系统环境假设、系统在不同条件下的状态、条件不满足时系统出现的(异常)情况以及系统不变量等，并通过系统验证为协议提供必要的安全保证；而计算复杂性方法通常又被称为可证明安全性方法，它基于一些最基础的假设或公理(例如，假设单向函数存在，或某些计算问题的困难性等)，采用规约的方法，将协议的安全目标规约到一个已知或公认的困难问题. 关于这两种方法的详细介绍，请参见文献[17].

计算复杂性方法采用了演绎推理方法(例如，从某个已知的假设推出一个结论的逻辑过程)，其重点则放在攻破协议到某个公认为困难问题的可证明规约. 其中，随机预言机模型(ROM)[18,19]就是这样一种应用最广泛的成功模型，基于 ROM 模型的理论和方法也被称为可证明安全理论. 可证明安全理论和技术始自 20 世纪 80 年代初期[20,21]，最初用于分析加密方案和签名方案的安全性，后来则用于分析密码协议的安全性[18,19]. 使用可证明安全性理论来证明协议的安全性主要包括以下 5 个主要过程：

(1)模型描述；

(2)该模型内安全目标定义；

(3)安全假设说明；

(4)协议描述；

(5)协议在该安全模型内达到其安全目标的证明.

4.1　一种 RFID 协议攻击者模型

目前，使用上述两种方法专门来研究 RFID 协议安全性的公开成果几乎没有. 本文仅讨论使用可证明安全性理论和方法来证明和分析 RFID 协议的一些思考，主要讨论模型描述以及该模型内的安全目标定义(可证明安全性理论中最为关键的部分之一). 首先，我们讨论一下 RFID 系统环境下的攻击者模型. 一个 RFID 系统是由多个主体和通信信道构成. 对 RFID 协议进行安全性分析时，通常将后端数据库和 Tag 读写器当作同一个独立和唯一的通信实体来对待. 这种处理方法符合大多数 RFID 系统通信信道安全假设. 鉴于前向信道与反向信道的不对称性(见图 1)，我们将他们分别进行处理. 这样，攻击者所能获得的信息仅来自于 RFID 系统的信道，如图 11 所示. 在该模型中，所有实体的通信都在攻击者的控制之下，攻击者可以任意地读取、插入、删除、篡改、延迟发送、重放任何的消息，也可以在任何时候发起与任何实体的任意回话.

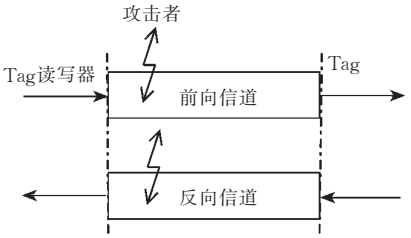


图 11　RFID 系统信道模型

下面我们用 Oracle 查询来模型化攻击者 $\mathcal{A}$ 的能力. 用 T 表示 Tag，用 R 表示 Tag 读写器，两者参与的 RFID 协议为 P. 协议双方都可以发起 P 的多个实例，用 π_T^i 表示第 i 个 Tag 实例，用 π_R^j 表示第 j 个 Tag 读写器实例. 攻击者 $\mathcal{A}$ 可以进行如下 Oracle 查询：

$Query(\pi_T^i, m_1, m_3)$：该查询刻画了攻击者 $\mathcal{A}$ 通过前向信道向 T 发送消息 m_1，并在接收到 T 的应答后再向 T 发送消息 m_3；

$Send(\pi_R^i, m_2)$：该查询刻画了攻击者 $\mathcal{A}$ 通过反向信道向 R 发送消息 m_2，并接收 R 之应答；

$Execute(\pi_T^i, \pi_R^j)$：该查询刻画了攻击者 $\mathcal{A}$ 执行 T 和 R 之间的协议 P 的一个实例，并获得通过前向信道和反向信道交换的所有消息；

$Execute^*(\pi_T^i, \pi_R^j)$：该查询刻画了攻击者 $\mathcal{A}$ 执行 T 和 R 之间的协议 P 的一个实例，但是攻击者 $\mathcal{A}$ 仅能获得通过前向信道交换的所有消息；

$Corrupt(\pi_T^i, sk)$：该查询刻画了攻击者 $\mathcal{A}$ 收买 T 的能力，使 T 泄漏自己私有存储空间内的秘密信

息，并可能会使用攻击者$\mathcal{A}$提供的秘密信息 sk 来代替原 T 存储区中的内容(依据使用的算法和场景的不同，可能是共享秘密或者公钥).

4.2 安全目标定义

令$\mathcal{O}\subseteq\{Q,S,E,E^*,C\}$，其中 Q,S,E,E^*,C 分别表示上述几种 Oracle 查询. 攻击者与目标 T 以及可能的 R 进行一定的交互过程之后，获得一个交互记录 $\Omega_l(T)$. 攻击者的攻击目的是要区分 T_1 和 T_2，以便确认出他所攻击的目标. 此时，攻击者也可以分别与 T_1 和 T_2 再次进行交互过程，并可以获得两个交互记录 $\Omega_{l1}(T)$ 和 $\Omega_{l2}(T)$. 此时，给定协议 P，攻击者的优势定义为

$$Adv_P(\mathcal{A})=2Pr[T_1=T_2]-1.$$

如果攻击者$\mathcal{A}$的优势 $Adv_P(\mathcal{A})$是可忽略的，则说协议 P 是$\mathcal{O}$-安全的.

5 结 论

RFID 已被大多数人认为是实现普适计算环境的一种主要技术，其广泛的应用场景，低廉的成本，部署实施的简单性，已经越来越多地吸引着用户、研究人员和 IT 厂商. 但是，RFID 系统以及设备自身所具有的许多特殊性和局限性也会带来各种各样的安全问题. RFID 技术面临的最大挑战就是让消费者在其隐私安全问题不受到威胁的前提下从中得益. 基于密码技术的 RFID 安全协议是一种实现和保护 RFID 系统安全性的重要方法，也是当前该领域研究的热点问题. 本文详细讨论了已有的 RFID 协议，分析了这些协议中存在的安全缺陷和漏洞. 本文的研究结果表明：目前尚不存在一个安全、高效、实用的低成本 RFID 安全协议.

设计安全、高效、低成本的实用 RFID 安全协议具有很大的挑战性，既有应用环境与 RFID 设备的特殊性和局限性，也有与已有国际相关标准的兼容性问题. 基于可证明安全性理论来设计和分析 RFID 安全协议，提出适用于 RFID 系统环境的协议模型，对于设计和分析安全的 RFID 协议具有重要的现实和理论意义，这是一个值得探索和研究的领域. 使用本文中给出的 RFID 协议攻击者模型与安全目标定义，分析已有 RFID 协议的安全性，将是本文的一个后续工作. 随着可证明安全理论和分析技术的进一步完善，我们有理由相信这个领域的研究会有所突破.

参 考 文 献

1 Sarma S. E., Weis S. A., Engels D. W.. RFID systems and security and privacy implications. In: Kaliski B. S., Koc C. K., Paar C. eds.. Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002). Lectures Notes in Computer Science 2523. Berlin: Springer-Verlag, 2003, 454～469

2 Sarma S. E., Weis S. A., Engels D. W.. Radio-frequency identification: Secure risks and challenges. RSA Laboratories Cryptobytes, 2003, 6(1): 2～9

3 Weis S. A., Sarma S. E., Rivest R. L., Engels D. W.. Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter D., Müller G., Stephan W., Ullmann M. eds.. Proceedings of the 1st International Conference on Security in Pervasive Computing. Lectures Notes in Computer Science 2802. Berlin: Springer-Verlag, 2004, 201～212

4 Ohkubo M., Suzuki K., Kinoshita S.. Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In: Proceedings of the 2004 Symposium on Cryptography and Information Security (SCIS 2004), Sendai, 2004, 719～724

5 Henrici D., Muller P.. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), Washington, DC, USA, 2004, 149～153

6 Molnar D., Wagner D.. Privacy and security in library RFID: Issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security(CCS'04), Washington, DC, USA, 2004, 210～219

7 Rhee K., Kwak J., Kim S., Won D.. Challenge-response based RFID authentication protocol for distributed database environment. In: Hutter D., Ullmann M. eds.. Proceedings of the 2nd International Conference on Security in Pervasive Computing (SPC 2005). Lectures Notes in Computer Science 3450. Berlin: Springer-Verlag, 2005, 70～84

8 Lee S. M., Hwang Y. J., Lee D. H., Lim J. I.. Efficient authentication for low-cost RFID systems. In: Gervasi O., Gavrilova M. L., Kumar V., Laganà A., Lee H. P., Mun Y., Taniar D., Tan C. J. K. eds.. Proceedings of the International Conference on Computational Science and Its Applications (ICCSA 2005). Lectures Notes in Computer Science 3480. Berlin: Springer-Verlag, 2005, 619～627

9 Juels A., Pappu R.. Squealing Euros: Privacy protection in RFID-enabled banknotes. In: Wright R. N. ed.. Proceedings of the 7th International Conference on Financial Cryptography (FC'03). Lectures Notes in Computer Science 2742. Berlin: Springer-Verlag, 2003, 103～121

10 Saito J., Ryou J. C., Sakurai K.. Enhancing privacy of universal re-encryption scheme for RFID tags. In: Yang L. T., Guo M., Gao G. R., Jha N. K. eds.. Proceedings of the International Conference on Embedded and Ubiquitous Computing (EUC 2004). Lectures Notes in Computer Science 3207. Berlin: Springer-Verlag, 2004, 879～890

11 International Organization for Standardization. ISO/IEC 18000-3. Information Technology AIDC Techniques-RFID for Item Management, March 2003

12 Avoine G., Oechslin P.. RFID traceability: A multilayer problem. In: Patrick A. S., Yung M. eds.. Proceedings of the

9th International Conference on Financial Cryptography and Data Security(FC 2005). Lectures Notes in Computer Science 3570. Berlin: Springer-Verlag, 2005, 125～140

13 Juels A., Rivest R. L., Szydlo M.. The blocker tag: Selective blocking of RFID tags for consumer Privacy. In: Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS 2003), Washington, DC, USA, 2003, 103～111

14 Menezes A., Oorschot P. V., Vanstone S.. Handbook of Applied Cryptography (1st Edition). New York: CRC Press, 1996

15 Golle P., Jakobsson M., Juels A., Syverson P.. Universal re-encryption for mixnets. In: Okamoto T. ed.. Proceedings of the Cryptographers' Track at the RSA Conference 2004 (CT-RSA 2004). Lectures Notes in Computer Science 2964. Berlin: Springer-Verlag, 2004, 163～178

16 Avoine G.. Adversarial model for radio frequency identification. Available at http://eprint.iacr.org/2005/049.pdf

17 Proceedings of SKLOIS Security Protocol Workshop. State Key Laboratory of Information Security, Beijing, 2004(in Chinese) (**信息安全国家重点实验室安全协议研讨会文集. 北京：信息安全国家重点实验室**, 2004)

18 Bellare M., Rogaway P.. Entity authentication and key distribution. In: Stinson D. R. ed.. Advances in Cryptology-CRYPTO'93. Lecture Notes in Computer Science 773. Berlin: Springer-Verlag, 1993, 232～249

19 Bellare M., Rogaway P.. Provably secure session key distribution: The three party case. In: Proceedings of the 27th ACM Symposium oh the Theory of Computing, 1995, 57～66

20 Goldwasser S., Micali S.. Probabilistic encryption. Special issue of Journal of Computer and Systems Sciences, 1984, 28(2): 270～299

21 Goldwasser S., Micali S., Rivest R. L.. A digital signature scheme secure against adaptive chosen-messege attacks. SIAM Journal of Computing, 1988, 17(2): 281～308

22 Floerkemeier C., Lampe M.. Issues with RFID usage in ubiquitous computing applications. In: Ferscha A., Mattern F. eds.. Proceedings of the 2nd International Conference on Pervasive Computing (PERVASIVE 2004). Lectures Notes in Computer Science 3001. Berlin: Springer-Verlag, 2004, 188～193

23 Avoine G., Oechslin P.. A scalable and provably secure hash-based RFID protocol. In: Proceedings of the 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005), Washington, DC, USA, 2005, 110～114

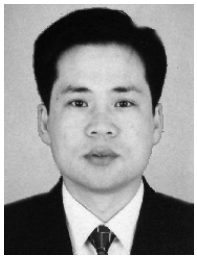
24 Good N., Molnar D., Urban J. M., Mulligan D., Miles E., Quilter L., Wagner D.. Radio frequency ID and privacy with information goods. In: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society(WPES'04), Washington, DC, USA, 2004, 41～42

25 mCloak: Personal/corporate management of wireless devices and technology, 2003. Available at http://www.mobilecloak.com

26 Juels A.. Minimalist cryptography for low-cost RFID tags. In: Blundo C., Cimato S. eds.. Proceedings of the 4th International Conference on Security in Communication Networks (SCN 2004). Lectures Notes in Computer Science 3352. Berlin: Springer-Verlag, 2005, 149～164

27 EPCglobal Inc. EPC Tag Data Standards Version 1.1. Brussels 2004. Available at http://www.epcglobalinc.org/standards_techno_logy/EPCTag-DataSpecification11rev124.pdf

28 Finkenzeller K.. RFID-Handbook, Fundamentals and Applications in Contactless Smart Cards and Identification(2nd Edition). New York: Wiley and Sons, 2003



ZHOU Yong-Bin, born in 1973, Ph. D., associate professor. His research interests include theories and technologies for network and information security.

FENG Deng-Guo, born in 1965, professor and Ph. D. supervisor. He mainly engaged in the research and development of information and network security.

Background

The work of this paper is supported by the National Natural Science Foundation of China under grant No. 60503014, 60273027 and 60573042.

Radio frequency identification (RFID) has been widely believed to be an important and ubiquitous infrastructure technology. However, the features of the RFID systems and the constraints of RFID devices may bring about various privacy problems. The biggest challenge for RFID technology is to provide benefits without threatening the privacy of consumers. Due to the limited computation and storage capabilities of RFID devices, designing a secure, efficient, low-cost and practical protocol for them still remains to be a great challenge.

There have been many papers in the literature that attempt to address the security concerns raised by the use of RFID tags. These solutions are generally divided into three broad categories: physical protection mechanism, cryptographic protocol and the combination of both of them. The authors review the existing RFID system security mechanisms with a main focus on cryptographic protocols, investigate the weakness or flaws of these protocols, and then propose a theoretical model and method within the provable security framework to design and analyze RFID protocols.