一种轻量级 RFID 安全协议*

陈瑞鑫，邹传云

（西南科技大学 信息工程学院 移动计算实验室，四川 绵阳 621010）

摘 要：在分析了几种现有的典型 RFID 安全协议的特点和缺陷的基础上，提出了一种轻量级的 RFID 安全协议，该协议将一次性密码本与询问—应答机制相结合，实现了安全高效的读取访问控制，最后建立该协议的理想化模型，利用 BAN 逻辑对该协议进行了形式化分析，在理论上证明其安全性。

关键词：轻量级；安全协议；一次性密码本；BAN 逻辑

中图分类号：TP393.0 **文献标识码**：A

A lightweight RFID security protocol

CHEN Rui Xin，ZOU Chuan Yun

（Mobile Computing Laboratory，School of Information Engineering，Southwest University of Science and Technology，Mianyang 621010，China）

Abstract：The features and issues pertinent to several current typical RFID cryptographic protocols were analyzed. Finally，a lightweight RFID secure protocol was proposed which combines the one time pads with the challenge-response mechanism. After setting up an idealized protocol model，a process of formal analysis of this protocol is presented and the security is proved theoretically by using the BAN logic.

Key words：lightweight；security protocol；one time pads；BAN logic

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，它通过射频信号来自动识别目标对象并获取相关数据[1]。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。但是，关键问题是要确保只有授权用户才能够识别各个标签，而攻击者无法对这些标签进行任何形式的跟踪。针对这一问题，国内外开展了大量关于 RFID 隐私安全保密的研究，已有许多 RFID 安全协议被提出，如 Hash 锁协议、随机化 Hash 锁协议、Hash 链协议等，但这些协议存在着安全隐患高，效率低下等缺陷。针对这些协议的不足，本文提出一种轻量级的 RFID 安全协议，并利用 BAN 逻辑对该协议进行形式化分析，在理论上证明其安全性[2]。

1 RFID 安全协议

基于密码学的发展，到目前为止，已经有许多种 RFID 安全协议被提出来，下面将介绍 3 种典型的 RFID 安全协议，并分析其优缺点[3-4]。

1.1 Hash 锁协议

Hash 锁协议是由 Sarma 等人提出来的，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，读写器向标签发出 ID 访问请求，标签回复根据 metaID 计算 K 值，标签计算 Hash(K)，如果 metaID=Hash(K)，则读写器通过验证，发送 ID 给读写器。如果 ID 值与数据库中的 ID 值相同，则对比标签的验证通过。从上述过程可以看出，Hash 锁协议中没有 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的，因此 Hash 锁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标签进行追踪，也就是说，Hash 锁协议没有达到其安全目标。

1.2 随机化 Hash 锁协议

为了解决 Hash 锁中位置跟踪的问题，将 Hash 锁方法加以改进，采用随机化 Hash 锁协议，此协议由 Weis 等人提出，它采用了基于随机数的询问—应答机制，该方法中数据库存储各个标签的 ID 值，设为 ID1、ID2 … IDk … IDn，标签向读写器发出的 metaID 是变化的，随机

* 基金项目：人事部留学人员科技活动择优资助项目(08ZD0106)；四川教育厅科技项目(2006A096)

化 Hash 锁可以避免跟踪，但是读写器每次识别 1 个标签都需要搜索并计算所有标签的 ID，系统资源消耗过大，容易受到拒绝服务攻击。认证通过后的标签标识 IDk 仍以明文的形式通过不安全信道传送，因此攻击者可以对标签进行有效的追踪。同时，一旦获得了标签的标识 IDk，攻击者就可以对标签进行假冒。而且，该协议也无法抵抗重传攻击。因此，随机化 Hash 锁协议也是不安全的。不仅如此，每 1 次标签验证时，后台数据库都需要将所有标签的标识发送给读写器，二者之间的数据通信量很大，该协议也不实用。

1.3 Hash 链协议[5]

NTT 提出了一种 Hash 链协议。在第 i 次与读写器交换时，射频标签有其初始值 Si，发送 $ai=G(Si)$ 给读写器，再根据以前的 Si 更新密钥 $Si+1=H(Si)$。其中，G 和 H 都是 Hash 函数，该方法满足了不可分辨和前向安全的特性。G 是单向方程，因此攻击者能获得标签输出 ai，但是不能从 ai 获得 Si。G 输出随机值，攻击者能观测到标签的输出，但不能把 ai 和 ai+1 联系起来。H 也是单向方程，攻击者能篡改标签并获得标签的密钥值，但不能从 $Si+1$ 中获得 Si。该算法的优势很明显，但是有太多的计算和比较。为了识别 1 个 ID，后台服务器不得不计算 ID 列表中的每个 ID。假设有 N 个一致的标签 ID 在数据库中，数据库不得不惊醒 N 次 ID 搜索、$2N$ 次 Hash 方程计算以及 N 次比较。计算机处理负载随着 ID 列表长度的增加线性地增加，因此该方法也不适合存在大量射频标签的情况。

2 轻量级 RFID 安全协议

为了避免 Hash 锁方法中的人为攻击和恶意跟踪的缺陷，并克服随机数 Hash 锁方法中计算负载过大的不足，本文提出了一种轻量级的 RFID 安全协议，该协议将一次性密码本与询问—应答机制相结合，实现了安全高效的读取访问控制，适用于标签数目较多的情况[6]。

该协议分为两个阶段：初始化阶段和协议执行阶段。假设攻击者可能窃听到无线信道里读写器和标签的所有电文，而读写器和数据库之间是用成熟的网络安全机制加以保证的安全信道。ID 表示电子标签的唯一性代号，$H_K(X)$ 表示用密钥 K 对消息 X 进行加密。

2.1 初始化阶段

(1)密钥的产生：系统按照密钥产生机制生成私钥 S_k 及其对应的公钥 P_k。

(2)标签的初始化：首先系统为每个标签分配 1 个密钥值 K，然后标签生成 1 次性密码本 A，并将 (A,K) 存储在标签中完成初始化过程，进入锁定状态。其中 1 次性密码本 A 由 m 个 1 次性加密值构成，即 $A\leftarrow\{\alpha_1=E_{P_k}(ID\parallel r_1),\cdots\alpha_m=E_{P_k}(ID\parallel r_m)\},r_1,\cdots,r_m$ 表示 m 个随机数，ID 表示该标签的唯一性代，E_{P_k} 表示利用公钥 P_k 对信息进行非对称加密。

(3)数据库的初始化：系统将每个标签的 ID 及其分配的密钥值 K 对应地存储在数据库中。

2.2 协议执行阶段

(1)读写器发出询问指令 Query，并将其产生的 1 个随机数 a 发送给标签。

(2)标签收到询问后，从 1 次性密码本 A 中随机选取 1 个加密值 α_i，计算 $\text{auth}_T=H_K(a\parallel\alpha_i)$ 和 $\text{auth}_R=H_K(\alpha_i\parallel a)$，将 (α_i,auth_T) 发送给读写器。

(3)读写器将产生的随机数 a 和收到的 (α_i,auth_T) 转发给数据库。

(4)数据库利用私钥 S_k 对 α_i 进行解密获得标签的 ID_j，如果 ID_j 无效则数据库放弃操作；否则数据库找到此 ID_j 对应的 K_j 值，计算 $\text{auth}_T'=H_{K_j}(a\parallel\alpha_i)$，若 $\text{auth}_T'=\text{auth}_T$ 则标签通过验证，数据库将 (ID_j,K_j,α_i) 发送给读写器；否则将此标签视为无效。

(5)读写器收到数据后利用随机数 a 计算 $\text{auth}_R'=H_{K_j}(\alpha_i\parallel a)$ 并发送至标签。

(6)标签验证 auth_R' 与 auth_R 是否相等，如果相等则通过验证，证实了读写器的合法性；若不等，则该读写器没有通过认证被屏蔽。如图 1 所示。

图 1 一种轻量级的 RFID 安全协议

3 安全性推导与分析

3.1 BAN 逻辑简介

BAN 逻辑是用于分析安全协议的一种形式化逻辑模型，由于它能够直观地表示出推理的过程，因此得到了广泛的应用。采用 BAN 逻辑已经成功地发现了许多协议的漏洞，也发现在许多协议中存在的冗余。

BAN 逻辑表达式描述如下：A、B 表示具体通信的主体；K 表示一般意义上的加密密钥；K_{ab} 表示具体通信主体的共享密钥；K_a、K_b 表示具体的通信主体的公钥；K_a^{-1}、K_b^{-1} 表示具体的通信主体的私钥；X、Y 表示一般意义上的语句；$P|\equiv X$ 表示 P 相信 X；$P\lhd X$ 表示 P 收到过 X；$P|\Rightarrow X$ 表示 P 对 X 有控制权；$P|\sim X$ 表示 P 说过 X；$\#\{X\}$ 表示 X 是新鲜的；$P\overset{K}{\longleftrightarrow}Q$ 表示 P 和 Q 共享 1 个密钥 K；$|\overset{K}{\longrightarrow}P_M$ 表示 K 是 P 的公钥；$\{X\}_K$ 表示用密钥 K 加密消息 X 的密文。

BAN 逻辑的几条基本逻辑推理规则如下：

(1)消息含义规则 $\dfrac{P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_k}{P|\equiv Q|\sim X}$，

$$\frac{P|\equiv|\xrightarrow{K}Q,P\lhd\{X\}_{k^{-1}}}{P|\equiv Q|\sim X}$$

(2)临时值校验规则 $\dfrac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$

(3)控制权规则 $\dfrac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$

(4)信念规则 $\dfrac{P|\equiv(X,Y)}{P|\equiv X,P|\equiv Y}$，$\dfrac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$

(5)新鲜性规则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$

3.2 形式化分析

共有三方参与协议，即电子标签 A、读写器 B、后台数据库 S。每个 A 与 S 在初始化时共享 1 个密钥 K_{as}，S 具有公钥 K_s 与私钥 K_s^{-1}。此协议可以将读写器和数据库之间的安全信道模型假设为 B 与 S 利用 1 个可靠的良好密钥 K 加密信息。为了简化分析过程，忽略 RFID 安全有线信道良好密钥的新鲜性问题，可以增加 1 条良好密钥规则：

$$\frac{P|\equiv Q\xleftrightarrow{K}P,P\lhd\{X\}_k}{P|\equiv X}$$

增加的这条协议对于讨论 RFID 的无线信道安全性没有影响，因为整个协议目的是验证 A 与 B 的合法性。

首先建立理想化协议模型：

(1)$A\rightarrow B:\{\{ID,r\}_{Ks},\{a,\{ID,r\}_{Ks}\}_{Kas}\}$

(2)$B\rightarrow S:\{\{ID,r\}_{Ks},a,\{a,\{ID,r\}_{Ks}\}_{Kas}\}_K$

(3)$S\rightarrow B:\{ID,K_{as},\{ID,r\}_{Ks}\}_K$

(4)$B\rightarrow A:\{a,B\xleftrightarrow{K}S\}_{Kas}$

然后建立协议的初始假设集合：

$A|\equiv A\xleftrightarrow{Kas}S,B|\equiv B\xleftrightarrow{K}S,B|\equiv K$

$S|\equiv A\xleftrightarrow{Kas}S,S|\equiv B\xleftrightarrow{K}S,S|\equiv K$

$B|\equiv S\Rightarrow ID,A|\equiv\Rightarrow B\xleftrightarrow{K}S,S|\equiv A|\Rightarrow\{ID,r\}_{Ks}$

$B|\equiv\#a,S|\equiv B|\equiv\#a,A|\equiv\#a$

上述协议的目标是 $S|\equiv\{ID,r\}_{Ks},B|\equiv ID,A|\equiv B\xleftrightarrow{K}S$，其实际的意义是经过读写器和标签的双方验证后，两者均能知道对方是合法的。

根据上述模型，运用 BAN 逻辑表达式进行推理：

(1)由模型中的消息(1)，可以得到 $B\lhd\{\{ID,r\}_{Ks},\{a,\{ID,r\}_{Ks}\}_{Kas}\}_K$，B 不能理解加密后的内容，但可以转发给 S。

(2)由模型中消息(2)可知 $S\lhd\{\{ID,r\}_{Ks},a,\{a,\{ID,r\}_{Ks}\}_{Kas}\}$，加上初始的假设条件 $S|\equiv B\xleftrightarrow{K}S,S|\equiv K$，利用规则(7)，得 $S|\equiv\{\{ID,r\}_{Ks},a,\{a,\{ID,r\}_{Ks}\}_{Kas}\}$。由规则(4)可得 $S|\equiv\{ID,r\}_{Ks},S|\equiv\{a,\{ID,r\}_{Ks}\}_{Kas}$ 由假设 $S|\equiv A\xleftrightarrow{Kas}S$，利用规则(1)可得 $S|\equiv A|\sim\{a,\{ID,r\}_{Ks}\}$。由假设 $B|\equiv\#a$，$S|\equiv B|\equiv\#a$ 及规则(5)，得到 $S|\equiv\#\{a,\{ID,r\}_{Ks}\}$，再由规则(2)得 $S|\equiv A|\equiv\{ID,r\}_{Ks}$，又因为假设 $S|\equiv A|\Rightarrow\{ID,r\}_{Ks}$ 得 $S|\equiv\{ID,r\}_{Ks}$。

(3)由消息(3)，即 $B\lhd\{ID,K_{as},\{ID,r\}_{Ks}\}_K$ 且 $B|\equiv B\xleftrightarrow{K}S$，$B|\equiv K$，利用规则(1)可推得 $B|\equiv S|\equiv\{ID,K_{as},\{ID,r\}_{Ks}\}$，由假设 $B|\equiv S\Rightarrow ID$，再利用规则(3)得到 $B|\equiv\{ID,K_{as},\{ID,r\}_{Ks}\}$，最后利用规则(4)得到 $B|\equiv ID$。

(4)由消息(4)，即 $A\lhd\{a,B\xleftrightarrow{K}S\}_{Kas}$，且有假设 $A|\equiv A\xleftrightarrow{Kas}S$，根据规则(1)，有 $A|\equiv S|\sim\{a,B\xleftrightarrow{K}S\}$，由假设 $A|\equiv\#a$ 及规则(5)得到 $A|\equiv\#\{a,B\xleftrightarrow{K}S\}$。再利用规则(2)可得到 $A|\equiv S|\equiv\{a,B\xleftrightarrow{K}S\}$，利用规则(4)可得 $A|\equiv S|\equiv B\xleftrightarrow{K}S$。根据假设 $A|\equiv S|\Rightarrow B\xleftrightarrow{K}S$ 并利用规则(3)，可知 $A|\equiv B\xleftrightarrow{K}S$。

(5)最终可得 $S|\equiv\{ID,r\}_{Ks},B|\equiv ID,A|\equiv B\xleftrightarrow{K}S$ 即证明了该协议实现了其预期目标，安全性得到保证。

4 性能分析及方法特点

(1)简单实用。将随机数产生器等复杂的计算移到了读写器中实现，降低了标签的复杂性，标签只需要实现 1 个 Hash 函数，这在低成本的标签上较易实现。

(2)前向安全。因为读写器每次访问产生 1 个随机数 a，标签每次应答从一次性密码本中随机选取 1 个加密值 α_i，所以攻击者即使窃听到某一次的标签输出也不可能在下一次得到认证，因为每一次认证过程中产生的随机数 a 不同，α_i 值亦不同，标签的输出也不同。

(3)机器运算负载小，效率高。在每次询问过程中，数据库只需对 α_i 进行 1 次解密即可获得标签 ID，这在标签数目较多的情况中，能够极大地提高系统工作效率。

(4)实现了身份的双向验证。通过 auth_T 的计算比较，数据库完成了对标签的验证；通过 auth_R 的计算比较，标签实现了对读写器的验证。

(5)有效实现安全隐私保护。

①防非法读取：只有经过合法认证的读写器才可读取标签的数据信息。

②防位置跟踪：由于随机数 a 和加密值 α_i 是随机选取的，因此，每次标签应答的 auth_T 的数值也是不同的，可以防止外人根据特定输出而进行的跟踪定位。

③防窃听：传输的 ID 值都经过了公钥 S_K 的非对称加密，外人无法解密得出 ID，因此有效地防止了窃听。

④防伪装哄骗：由于外人无法获知一次性密码本，因此无法模拟合法标签发送数据，有效地防止了伪装哄骗攻击。

本文提出了一种轻量级的 RFID 安全协议，具有成本低、负载小、安全性好和效率高等特点，且能保证前向安全性，基本上弥补了目前安全保护方法安全性不够和效率低等缺陷，是一种较为实用的算法，适用于低成本电子标签系统，具有较高的实用价值。理论证明该协议在系统安全需求的前提下，还具有协议执行效率高，双向验证等特点。

参考文献

[1] BURROWS M A,NEEDHAM R. A Logic of authentication [J].ACM Transactions on Computer Systems,1990,8 (1):18-36.

[2] SARMA S E,WEIS S A,ENGELS N W. RFID systems and security and privacy implications [C]. 4th Internationa Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002),Lectures Notes in Computer Science 2523.Berlin:Springer-Verlag,2003:454-469.

[3] OHKUBO M,SUZUKI K, KINOSHITA S. Cryptographic approach to "Privacy-Friendly" tags [C]//Proc of RFID Privacy Workshop, USA MIT, 2003.

[4] SARMA S E, WEIS S A, ENGELS D W. Radio frequency identification:Secure risks and challenges[J]. RSA Laboratories Cryptobytes, 2003,6(1):2-9.

[5] 裴友林,余本功.基于随机Hash-Chain的RFID安全协议研究[J].微计算机信息,2008,10(2):194-196.

[6] 周晓光,王晓华.射频识别(RFID)技术原理与应用实例[M].北京:人民邮电出版社,2006.

(收稿日期:2009-07-01)