轻量级RFID双向认证协议设计与分析

张 兵[1,2]，马新新[3]，秦志光[2]

(1. 成都九洲电子信息系统股份有限公司 成都 610041; 2. 电子科技大学计算机科学与工程学院 成都 610054;
3. 中国人民解放军78046部队 成都 610011)

【摘要】针对低成本RFID系统常用的基于Hash运算认证协议的安全性进行研究，分析了该类协议存在的安全缺陷和不足，给出设计低成本RFID认证协议满足安全需求的思路，提出了一种轻量级的RFID双向认证协议，运用BAN逻辑的形式化分析方法，对该协议的安全性进行证明。结果显示，该认证协议能满足RFID应用中面临的机密性、完整性和可追踪性的安全需求，可抵制跟踪、标签假冒、重放等攻击，弥补已有基于Hash运算的认证协议中存在的安全缺陷，更适合低成本RFID系统对应用安全的需求。

关 键 词 认证协议; 形式化方法; 哈希算法; 射频识别; 协议的安全性
中图分类号 TP393.08 **文献标志码** A doi:10.3969/j.issn.1001-0548.2013.03.021

Design and Analysis of a Lightweight Mutual Authentication Protocol for RFID

ZHANG Bing[1,2], MA Xin-xin[3], and QIN Zhi-guang[2]

(1. Chengdu Jiuzhou Electronic Information System Co.Ltd Chengdu 610041;
2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054;
3. 78046 Unit of People's Liberation Army Chengdu 610011)

Abstract The security of Hash-based operation authentication protocol, which is usually used by the low-cost RFID system, is researched. Based on the analysis of security shortcomings and flows of this protocol, a thesis of low-cost RFID authentication protocol to meet the security requirements is formulized and a light-weight RFID bi-directional authentication protocol is proposed. The security of the proposed protocol is proved by using the formal analysis method of BAN logic. The results show that the proposed protocol can meet the security requirements of confidentiality, integrity, and traceability in RFID applications. Besides, the protocol can resist attacks of tracking, label counterfeit, and replay, improve the security flaws existing in the current Hash-based operation authentication protocol, and better meets the security requirements of the low-cost RFID system.

Key words authentication protocol; format method; Hash algorithm; RFID; security of protocol

射频识别(radio frequency identification，RFID)是一种利用射频信号，通过空间耦合(交变磁场或电磁场)实现无传触信息传递，并通过所传递的信息实现对目标物识别的技术。近年来，随着RFID技术在各行业的广泛应用，RFID系统面临的安全威胁和标签安全隐私问题日益显现，亟待解决。

针对RFID系统应用中存在的安全问题，目前有两类安全机制进行防护：一类是通过物理方法阻止标签与读写器之间的通信；另一类是运用软件机制增强RFID系统的安全性能[1-3]。其中，物理防护机制在解决标签中的数据安全与自身定位安全的问题中，采用基于物理的方法保护标签不被追踪，不对未经授权的质询进行应答。在该机制防护方法中，典型有Kill标签机制、法拉第网罩、主动干扰方法与阻塞法等。其中，Kill命令机制旨在保护标签的隐私，阻止标签被恶意追踪，为实现这一目的，每个标签在设计时增加一个Kill命令，当向标签发出该命令后，使标签标识自动失效，自此不再回应任何查询指令，达到阻止扫描和追踪的目的。但在很多情况下，标签的标识要求被多次使用，标签失效的同时，不仅切断了标签功能的后继服务，而且对资源的重复使用需求也是一种违背与浪费。法拉第网罩是采用将标签或带标签的产品放入被称为法拉第罩的容器中，使之不能与外界进行电磁耦合，阻止容器内

收稿日期：2011－03－24；修回日期：2013－01－07
基金项目：国家863项目(2008AA04A107)
作者简介：张兵(1973－)，男，博士生，主要从事信息和网络安全、RFID应用与安全方面的研究.

的标签被扫描，切断标签与读写器之间的任何通信，达到隐私保护。但该防护方法因需要一个额外的物理设备，不但增加了系统的成本，也给操作人员带来极大的不便。主动干扰是通过额外增加了一个被称为主动广播无线信息的设备阻止或破坏邻近RFID读写器的操作，以阻止受保护的标签对外质询进行回复。但该方法在保护的同时，也会干扰附近其他合法RFID系统的质询，实用性不足。阻塞法是通过增加一个特殊的阻止标签干扰，在防冲突算法的同时，阻止读写器对标签的读取，实现标签中的信息安全。但该方法可被恶意攻击者利用，进行拒绝服务攻击，阻止读写器对其他标签的读取，实际运用有待完善。

运用软件机制增强RFID系统的安全性能，是通过以认证协议的方法，确保标签和读写器之间数据传输的安全性，通常在通信前，首先对标签的身份进行认证，防范标签的伪造与阻止标签内容的滥用。同时，通过对读写器读写权限授权进行核实，确保标签只对经过合法授权的读写器的质询进行应答，防范任何未经授权的情况下，不可访问标签中存储的信息，确保标签和读写器之间数据传输的机密性和完整性。

本文针对低成本RFID系统常用的基于Hash运算认证协议的安全性进行研究，分析该类协议存在的安全缺陷和不足，给出设计低成本RFID认证协议满足安全需求的思路，在此基础上，提出了一种轻量级的RFID双向认证协议，和已有的协议进行安全性分析比较，运用BAN逻辑的形式化分析方法，对该协议的安全性进行证明。

1 低成本RFID安全认证协议对比研究

认证协议是系统安全或网络安全的基础，用于确认登录系统或访问网络资源的主体身份，验证其身份的合法性。RFID系统应用中的认证协议主要解决机密性、完整性和可追踪性3个基本问题。

目前，RFID系统的认证协议类型，主要侧重于是对前端标签进行认证，还是对后端读写器认证而划分为前向认证协议或双向认证[4-5]协议两大类。前向认证协议中，主要用于解决前端标签身份合法性问题，典型的有Hash-Lock协议[6]。该类协议引入的目的，是为读写器识别假冒或伪造的标签，提供鉴别手段和方法。双向认证协议在前向认证协议的基础上，实现前端标签对后端读写器读取是否授权进行验证。通过增加对后端读写器身份的验证，使用标签只对经过授权读写器的质询如读取标签内部信息或写入标签信息等，进行应答，该类协议典型的有LCAP(Low Cost Authentication Protocol)协议[7]。上述两类认证协议的具体实际运用中，由于基于Hash-Lock的低成本安全认证协议，在标签安全性和低成本需求两方面进行了折中，而成为低成本RFID安全认证协议运用的代表。目前，采用基于杂凑算法的认证协议典型的有Hash-Lock、随机化Hash-Lock[8]和Hash链协议等[9]。

Hash-Lock协议采用metaID代替真实的标签ID，以防止标签信息的泄漏和被追踪，metaID值是标签的ID经过哈希计算的结果值。该协议的优点是因采用Hash函数，成本很低，仅需计算Hash值和存储一个metaID值，认证过程中使用对真实ID加密后的metaID。但该协议的安全缺陷在于采用替代的方法，尝试保护标签ID不被获取，以保护标签隐私，协议本质上并没有改变其对应且存在的一一映射关系。虽然表面上标签的ID没有暴露，但恶意攻击者仍然可以通过获取的metaID，达到追踪、并定位标签的目的。此外，在该协议的整个过程中，metaID、ID和Key均以明文的形式进行传输，认证过程面临的机密性和完整性也不可能得到保障。

随机Hash-Lock协议针对Hash-Lock协议中标签ID没有刷新机制而产生的安全隐患，而引入随机数与标签ID进行绑定，达到标签ID在任意一次的认证过程中的动态生成，以防范攻击者对标签的恶意追踪。但随机Hash-Lock协议在一次认证过程中，标签ID仍以明文的形式进行传输，导致攻击者一旦截获该信息标识，依然可以实现对标签的有效追踪和标签假冒。

Hash链协议为实现标签ID在每一次认证过程中的动态生成，采用共享秘密的方式，使标签具有自主更新ID的能力。该协议的优点是具有不可分辨性及前向安全性，是一个只对标签身份进行合法性验证的单向认证协议。同时，一次认证过程中，每一个标签都要在后端系统数据库进行j次哈希运算，计算负荷将随标签数量规模的扩大而不断下降，无法满足海量标签认证的性能要求。

通过对上述具有代表性的，基于Hash运算的低成本安全认证协议的对比研究分析，本文设计出实现低成本RFID认证协议的步骤：1) 标签ID需采用动态刷新机制进行隐私保护和防范恶意的追踪；2) 利用Hash运算的单向特性进行消息传递完整性的鉴别与标签ID传输的机密性；3) 通过采用即对标签进行

身份验证，又对读写器身份进行鉴别的双向认证策略，实现一次认证过程中，两方个体身份真实性和授权合法性验证的全过程。根据上述认证协议设计与实现的思路，本文提出一种轻量级的RFID双向认证协议。

2　轻量级RFID双向认证协议设计分析与证明

在进行轻量级RFID双向认证协议设计前，首先对RFID系统应用进行相关假设：前端标签与后端读写器之间的无线信道视为不安全，后端读写器与其对应的系统之间的有线信道视为安全，即前向信道是安全的，后向信道是不安全的；其次，协议中所涉及的伪随机数、哈希与异或等计算函数等均视为安全函数。

2.1　轻量级双向认证协议描述

本文提出的轻量级双向认证协议，由于认证过程中没有传统可信第三方的引入，因此，前端标签和后端读写器之间彼此身份合法性的鉴别，采取预先分配并存储在后端系统数据库中标签标识信息或双方认证过程中共享的信息进行读取、对比验证。同时，以后端系统的本地时间为基准，对每个标签进行预值，以此作为标签一次认证的标识信息，其变化随后端系统的时间变化与更新；再由后端系统数据库，执行一次认证过程中的Hash运算，由标签产生伪随机数，并具有哈希运算与异或运算逻辑。本文提出轻量级双向认证协议中，一次认证过程中所涉及的参数符号定义如表1所示。轻量级双向认证协议执行流程如图2所示[10]。

表1　参数符号定义

符　号	定　义
T	RFID标签
R	RFID读写器
DB	后端系统
$\|\|$	异或运算
ID_i	标签标识
R_t	标签生成的随机数
T_l	标签与后端系统共享的验证时间戳
R_s	后端系统生成的随机数
T_n	后端系统验证过程产生的时间戳
Query	读写器产生的请求消息

R首先向T发送一请求消息，当T收到该请求消息后，产生一随机数R_t，将自身标识信息ID_i、R_t和T_l进行哈希计算，R_t和T_l进行异或运算及T_l构成一三元组回送至R。当R收到该三元组后，直接将其转发到后端系统，由后端系统在本地数据库DB根据T_l值进行对照匹配，若有对应匹配结果，则获取T对应的标识信息ID_i值，将该值与接收到的R_t和T_l哈希计算结果值进行一致性检验，若检验结果为真，则标签身份为合法，认证通过。此时，后端系统提取本地系统时间T_n，并用此时提取的T_n值替代T_l值，作为下一次认证的时间戳，产生一随机数R_s后，将上述T_n与R_t、R_s与R_t二组值进行异或，将标识信息ID_i、T_n与R_t进行哈希计算，将上述三组值构成一三元组，发送到T。当T收到该三元组后，直接向R转发。R收到该三元组后，首先用自身产生的随机数R_t分别与T_n与R_t、R_s与R_t二组值进行异或，提取出T_n与R_s；其次，将上述两个值与自身标识信息ID_i进行哈希计算并与接收到的哈希值进行一致性检验，若验证结果为真，则读写器身份为合法。同时，T对提取的进行T_n与R_s哈希计算，并向T传送该值，由T向后端系统转发。当后端系统DB接收该值后，将该值与本地的T_n与R_s哈希值进行一致性验证，若验证结果为真，则进行T_n对T_l的替换，至此，一次完整的验证过程结束。

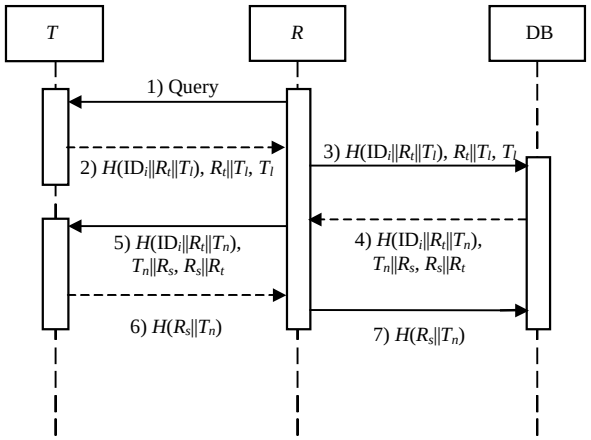

图2　轻量级的RFID双向认证协议

2.2　轻量级双向认证协议安全性分析

本文将分别从协议的机密性、前向安全性、防追踪、双向认证、防伪造与抗重传攻击共6个方面对提出的轻量级双向认证协议进行安全性分析。

1) 机密性。

轻量级双向认证协议中，R、T和后端系统DB三者之间验证的私有信息，均是由Hash函数这一带有单向性的函数进行加密，因此，上述三者之间认证过程中，攻击者即使截获通信的认证信息，也无法从该密文数据中获取原有信息，数据传输的机密性可以得到保证。

2) 前向安全性。

任意一次认证过程中，R与后端系统DB之间协议的相互验证，R与后端系统DB分别产生不同的随

机数R_t与R_s，同时时间戳T_l只与上一次验证结果而变化，带有不可预测性，因此，攻击者无法通过某一次截获的随机数R_t、R_s或时间戳T_l的哈希值推断本次验证的相关值，从而R到T的数据传输安全得到保证。

3) 防追踪。

任意一次认证过程中，R与后端系统DB之间协议的相互验证，R与后端系统DB分别产生不同的随机数R_t与R_s，同时时间戳T_l只与上一次验证结果而变化，并伴随标签标识信息的验证过程，具有随机变化性，保证了前向传输的安全。这一措施，使攻击者无法从截获的协议验证过程中分析出标签标识信息，以及区分两个不同标签的标识特性，从而对标签的恶意跟踪。此外，一次验证过程中，R与后端系统DB二者之间共享的验证时间戳，用于提高查找，同时该值也会随验证过程的变化而发生改变，因此，验证时间戳与T的标识信息产生多对一的映射关系，标签的标识信息不会因时间戳的明文传输而被攻击者获取，并分析出一次验证过程中时间戳对应的标签标识信息。

4) 双向认证。

R向后端系统DB转发协议消息，当后端系统DB收到一次验证过程的哈希值，在本地的DB中与进行R_t和T_l哈希计算结果值的一致性检验，若验证结果为真，则通过对T身份的合法性检验。R对T的身份合法性的验证是通过接收读写器R转发后端系统DB的T_n与R_t、R_s与R_t二组值的异或和与T的标识信息ID_i进行哈希哈希值进行一致性检验，其验证结果为真，则读写器身份为合法。这种既对T身份合法性又对R身份合法性验证的双向认证策略与手段，不仅有效防止T的假冒行为，又能避免非法R对合法T的恶意跟踪，提高了认证的前向性与后向性安全。

5) 防伪造。

T与后端系统DB分别产生不同的随机数R_t与R_s，并以此验证T与R的身份；同时，为确保验证过程消息的机密性，采用Hash函数进行加密，有效防止攻击利用伪造身份进行攻击的可能。

6) 抗重传攻击。

任意一次认证过程中，R与后端系统DB产生不同的随机数以及采用哈希进行加密的方法，使任意一次认证过程中产生的消息内容，没有规律可循，增加攻击者对截获该数据内容后，进行预测与分析的难度。攻击者无法通过对截获的数据，采用试图重放，以获得认证双方中任一方的验证可能。此外，任意一次认证过程中，标签与后端系统共享、使用一致的验证时间戳T_i，并将该值与其自身标识进行哈希加密，上述两种方式叠加的效果，使攻击者无法利用截获上次的信息，去伪造当前验证时间戳，重传攻击行为得到有效防止。

2.3 轻量级双向认证协议性能分析

本文对提出的轻量级双向认证协议分别从标签T的计算复杂度、后端系统DB的计算复杂度、T与R之间通信量及一次验证过程中连续会话次数共4个方面进行分析，并与Hash-Lock协议、随机化Hash-Lock协议及Hash-Lock链协议的性能进行比较，结果如表2所示。

表2 基于Hash协议的性能比较

安全因子	Hash-Lock	随机化 Hash-Lock	Hash-Lock 链协议	本文提出协议
T计算复杂度	1h	1h+r	2h	2h+r
DB计算复杂度	0h	0h	nh/2×i	2h+r
通信量	3l	2l	1l	2l
会话次数	$O(m)$	$O(m)$	$O(m\times n)$	$O(m)$

根据表2的性能比较结果可以得出，Hash-Lock协议和随机化的协议虽然在后端数据库不需要进行Hash计算的操作，但安全性得不到保证，Hash-Lock链协议后端数据对每一个电子标签进行i次Hash运算，计算负荷大，同时，会话次数(m)与标签数量(n)成正比，存在明显的数据去同步化问题，实际可行性不高。而本文提出的协议中标签和后端数据库所需计算量均为2h+r(h为Hash计算操作，r为产生的随机数操作)，标签和后端数据库的通信量是2l(l表示标签ID的长度)，会话次数的时间复杂度是常数阶，各方面的性能均衡，且安全性目标达到。

2.4 轻量级双向认证协议形式化证明

认证协议的形式化证明，就是运用某种形式化语言，为安全协议建立模型，并按照规定的假设、分析和验证规则，对协议的正确性和安全性进行推理验证[11-13]。目前，广泛使用的安全协议形式化分析方法是基于知识和信念的形式逻辑分析方法，该方法最有影响的是BAN逻辑[14]，它是一种模态逻辑，其目标是认证参与协议的主体的身份，分析协议能否达到预定的目标。而对协议的证明，是通过形式法的方法精确描述协议的行为，解决认证协议是否正确，认证协议的目标是否达到，应用BAN逻辑首先将协议的消息转换为BAN逻辑中的公式，进行逻辑的理想化步骤，其次根据具体情况进行合理的假设，基于协议理想化和初始化假设，利用逻辑的推理规则进行推理，以推断协议能否达到预期的

目标。本文提出的轻量级的RFID双向认证协议进行BAN逻辑的证明过程描述如下。

1) 协议描述：

① $R\rightarrow T$: Query

② $T\rightarrow R$:$\{H(\mathrm{ID}_i\|R_t\|T_l),\ R_t\|T_l,\ T_l\}$

③ $R\rightarrow$DB:$\{H(\mathrm{ID}_i\|R_t\|T_l),\ R_t\|T_l,\ T_l\}$

④ $DB\rightarrow R$:$\{H(\mathrm{ID}_i\|R_t\|T_n),T_n\|R_s,R_s\|R_t\ \}$

⑤ $R\rightarrow T$:$\{H(\mathrm{ID}_i\|R_t\|T_n),T_n\|R_s,R_s\|R_t\ \}$

⑥ $T\rightarrow R$:$\{H(R_s\|T_n)\}$

⑦ $R\rightarrow$DB:$\{H(R_s\|T_n)\}$

2) 协议理想化：

① $T\rightarrow R\rightarrow$DB:

$$\{R_t,T\xleftrightarrow{T_l}\mathrm{DB},(R_t,T_l),\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}_{\mathrm{H}}\}$$

② DB$\rightarrow R\rightarrow T$:

$$\{R_t,R_s,T\xleftrightarrow{T_n}\mathrm{DB},(R_s,T_n),(R_s,R_t),\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}_{\mathrm{H}}\}$$

③ $T\rightarrow R\rightarrow$DB: $\{\{T_n,R_s\}_{\mathrm{H}}\}$

协议理想化中将协议描述中的第一条消息省略，因为该消息对分析协议没有作用。同时，将转发消息省略，因为对该消息的分析与源消息的分析一致。

3) 初始化假设：

① $T\left|\equiv T\xleftrightarrow{\mathrm{H}}\mathrm{DB}\right.$

② $\mathrm{DB}\left|\equiv T\xleftrightarrow{\mathrm{H}}\mathrm{DB}\right.$

③ $\mathrm{DB}\left|\equiv(T\Rightarrow T\xleftrightarrow{T_l}\mathrm{DB})\right.$

④ $T\left|\equiv(\mathrm{DB}\Rightarrow T\xleftrightarrow{T_n}\mathrm{DB})\right.$

⑤ $T\left|\equiv(\mathrm{DB}\Rightarrow \mathrm{ID}_i)\right.$

⑥ $\mathrm{DB}\left|\equiv(T\Rightarrow \mathrm{ID}_i)\right.$

⑦ $\mathrm{DB}\left|\equiv\#(R_t)\right.$

⑧ $\mathrm{DB}\left|\equiv\#(T_n)\right.$

协议正确性证明目标：

a. $\mathrm{DB}\left|\equiv T\right|\equiv\{\mathrm{ID}_i\}$　　b. $T\left|\equiv\mathrm{DB}\right|\equiv\{\mathrm{ID}_i\}$

c. $\mathrm{DB}\left|\equiv\{T\xleftrightarrow{T_l}\mathrm{DB}\}\right.$　　d. $T\left|\equiv\{T\xleftrightarrow{T_n}\mathrm{DB}\}\right.$

e. $DB\left|\equiv T\right|\equiv T_n$

4) 证明过程：

将协议理想化的①转换成BAN逻辑公式：

$$\mathrm{DB}\lhd\{R_t,T\xleftrightarrow{T_l}\mathrm{DB},(\mathrm{R}_t,\mathrm{T}_l),\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}_{\mathrm{H}}\}\tag{1}$$

由BAN逻辑的接收消息规则 $\dfrac{P\left|\lhd(X,Y)\right.}{P\left|\lhd X\right.}$，得出：

$$\mathrm{DB}\lhd\{ID_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}_{\mathrm{H}}\tag{2}$$

由初始化假设②和BAN逻辑的消息含义规则中共享秘密：$\dfrac{P\left|\equiv P\xleftrightarrow{Y}Q,P\lhd\{X\}_Y\right.}{P\left|\equiv Q\right|\sim X}$(式中 P 、Q 分别是通信主体，Y 为共享秘密，X 为消息，$\{X\}_Y$ 为经 Y 加密的消息)，得出：

$$\mathrm{DB}\left|\equiv T\sim\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}\right.\tag{3}$$

由初始化假设⑦、式(3)和BAN逻辑的新鲜性规则 $\dfrac{P\left|\equiv\#(X)\right.}{P\left|\equiv(X,Y)\right.}$，得出：

$$\mathrm{DB}\left|\#\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}\right.\tag{4}$$

由式(3)、式(4)和BAN逻辑的临时值校验规则 $\dfrac{P\left|\equiv\#(X),P\right|\equiv Q\left|\sim X\right.}{P\left|\equiv Q\right|\equiv X}$，得出：

$$\mathrm{DB}\left|\equiv T\equiv\{\mathrm{ID}_i,R_t,T\xleftrightarrow{T_l}\mathrm{DB}\}\right.\tag{5}$$

由式(5)和BAN逻辑的信念规则 $\dfrac{P\left|\equiv Q\right|\equiv(X,Y)}{P\left|\equiv Q\right|\equiv X}$，分别得出：

$$\mathrm{DB}\left|\equiv T\right|\equiv\{\mathrm{ID}_i\}\tag{6}$$

$$\mathrm{DB}\left|\equiv T\right|\equiv\{T\xleftrightarrow{T_l}\mathrm{DB}\}\tag{7}$$

由初始化假设③、⑥、式(7)和BAN逻辑的管辖权规则 $\dfrac{P\left|\equiv Q\right|\Rightarrow X,P\left|\equiv Q\right|\equiv X}{P\left|\equiv X\right.}$，得出：

$$\mathrm{DB}\left|\equiv\{T\xleftrightarrow{T_l}\mathrm{DB}\}\right.\tag{8}$$

根据协议理想化②，同理可证：$T\left|\equiv\mathrm{DB}\right|\equiv\{\mathrm{ID}_i\}$，$T\left|\equiv\{T\xleftrightarrow{T_n}\mathrm{DB}\}\right.$；根据协议理想化③，同理可证：$\mathrm{DB}\left|\equiv T\right|\equiv T_n$，完成协议正确性证明目标。

3 结 束 语

本文在对基于Hash运算的RFID认证协议进行安全分析的基础上，提出低成本RFID认证协议的设计思路，在此基础上，设计了一种轻量级的RFID双向认证协议，并从理论证明和安全性分析的角度对该协议的安全性进行了描述，分析和证明结果显示，本文提出的认证协议能满足RFID应用中面临的机密性、完整性和可追踪性3个基本问题的安全需求，可抵制跟踪、标签假冒、重放等攻击，弥补已有基于Hash运算的认证协议中存在的安全缺陷，更适合低成本RFID系统对应用安全的需求。

参 考 文 献

[1] 周永彬, 冯登国. RFID安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581-589.

ZHOU Yong-bin, FENG Deng-guo. Design and analysis of cryptographic protocols for RFID[J]. Chinese Journal of Computer, 2006, 29(4): 581-589.

[2] JUELS A, RIVEST R, SZYDLO M. The blocker tag: Selective blocking of RFID tags for consumer privacy[C]// Proceeding of the 8th ACM Conference on Computer and Communication Security. New York: ACM, 2003: 103-111.

[3] PEDRO P L, JULIO C H C, JUAN M, et al. RFID system: a survey on security threats and proposed solutions[J]. Lecture Notes in Computer Science, 2006, 42(17): 159-170.

[4] 丁振华, 李锦涛, 冯波. 基于Hash函数的RFID安全认证协议研究[J]. 计算机研究与发展, 2009, 46(4): 583-592.
DING Zhen-hua, LI Jin-tao, FENG Bo. Research on hash-based RFID security authentication protocol[J]. Journal of Computer Research and Development, 2009, 46(4): 583-592.

[5] 谌绍巍, 陈睿, 凌力. 一种改进的Hash函数RFID双向安全认证协议[J]. 计算机系统应用, 2010, 19(3): 67-70.
CHEN Shao-wei, CHEN Rui, LING Li. An improved hash-based RFID two-way security authentication algorithm[J]. Computer Systems and Applications, 2010, 19(3): 67-70.

[6] SARMA S E, WEI S A, ENGLES D W. Radio-frequency identification: Security risks and challenges[J]. CryptoBytes Technical Newsletter from RSA Laboratories, 2003, 6(1): 2-9.

[7] LEE S M, HWANG Y J, LEED H, et al. Efficient authentication for low cost RFID System[C]//International Conference on Computational science and its Applications. Singapore: World Scientific Publish Company, 2005: 619-627.

[8] HENRICI D, MAULLER P. Hash-based enhancement of location privacy for radio frequency identification devices using varying identifiers[C]//International Workshop on Pervasive Computing and Communication. Orlando, USA: [s.n.], 2004: 149-153.

[9] SEIS A, SAIMA S E, RIVEST R L. Security and privacy aspects of low-cost radio frequency identification System[C]//Proceeding of the 1st International Conference on Security in Pervasive Computing. [S.l.]: Springer, 2004: 201-212.

[10] 张兵, 马新新, 秦志光. Hash运算的RFID认证协议分析和改进[J]. 计算机应用研究, 2011, 28(11): 4311-4314.
ZHANG Bing, MA Xin-xin, QIN Zhi-guang. Analysis and improvement of hash-based RFID authentication protocol[J]. Application Research of Computer, 2011, 28(11): 4311-4314.

[11] MOINAR D, WAGNER D. Privacy and Security in Library RFID: Issues, practices, and architectures[C]//Proceeding of the 11th ACM Conference on Computer and Communication Security. [S.l.]: Springer, 2004: 210-219.

[12] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743-1756.
FENG Deng-guo. Research on theory and approach of provable security[J]. Journal of Software, 2005, 16(10): 1743-1756.

[13] 卿斯汉. 安全协议的设计与逻辑分析[J]. 软件学报, 2003, 14(7): 1300-1309.
QING Si-han. Design and logical analysis of security protocols[J]. Journal of Software, 2003, 14(7): 1300-1309.

[14] BURROWS M, ABADI M, NEEDHAM R M. A logic of authentication[J]. ACM Transactions on Computer Systems, 1989, 8(1): 233-271.

编 辑 税 红