# 基于共享秘密的伪随机散列函数 RFID 双向认证协议

石乐义*[①②] 贾 聪[①] 宫 剑[②] 刘 昕[①] 陈鸿龙[①]
[①](中国石油大学(华东)计算机与通信工程学院 青岛 266555)
[②](上海市金融信息技术研究重点实验室 上海 200433)

**摘 要**：针对资源受限的 RFID 标签，结合伪随机数和共享秘密机制，该文提出一种基于散列函数的轻量级双向认证协议，实现了后端数据库、阅读器和标签之间的双向认证。详细分析了双向认证协议的抗攻击性能和效率性能，并基于 BAN 逻辑分析方法对协议模型进行了形式化证明。理论分析表明，该文提出的认证协议能够实现预期安全目标，抗攻击性能好，认证执行效率高且标签开销小，适用于大数量的 RFID 应用。

**关键词**：射频识别；双向认证协议；隐私保护；BAN 逻辑；散列函数
**中图分类号**： TP391.45 **文献标识码**：A **文章编号**：1009-5896(2016)02-0361-06
**DOI**: 10.11999/JEIT150653

# RFID Mutual Authentication Protocol on Pseudo-random Hash Function with Shared Secrets

SHI Leyi[①②] JIA Cong[①] GONG Jian[②] LIU Xin[①] CHEN Honglong[①]
[①](*College of Computer and Communication Engineering*, *China University of Petroleum*, *Qingdao* 266555, *China*)
[②](*Shanghai Key Laboratory of Financial Information Technology*, *Shanghai* 200433, *China*)

**Abstract**: Concerning the resource-limited RFID tags, this paper presents a lightweight mutual authentication scheme based on Hash function, combining with the pseudo-random number and shared secret mechanisms, and implements the mutual authentication among the end database, reader and the tags. The anti-attack performance and the overhead of the scheme are analyzed in detail. Afterwards, the protocol security model is formalized using BAN logical analysis method. Theoretical analysis shows that the proposed authentication scheme could achieve the desired security goals, has good anti-attack performance and high efficiency. It can be applied to big population RFID since its low overhead for RFID tags.

**Key words**: Radio Frequency IDentification (RFID); Mutual authentication protocol; Privacy protection; BAN logic; Hash function

## 1 引言

RFID 射频识别技术是物联网的一项关键技术，它通常由后端数据库、电子标签和阅读器 3 部分组成。阅读器通过天线向标签发送和接收信号，识别读取标签中存储的信息，并将信息数据传送给后端数据库做进一步处理，从而实现对目标的识别。近年来，由于具有非接触、耐磨损、寿命长等优点，RFID 技术受到了广泛关注。然而，阅读器与电子标签之间通过无线信道传输数据，可能会带来非授权访问标签内容、篡改或伪造标签等安全隐患。在此背景下，RFID 隐私安全保护方案如物理机制、认证加密等相继提出。前者使用非密码学方式如 Kill、阻断等机制保护 RFID 标签数据隐私，后者则采用加密方法实现 RFID 安全通信，如 Hash-Lock 协议[1]等。

Hash-Lock 协议是一种基于单向 Hash 散列函数的 RFID 访问控制方法，通过使用 metaID 代替真实标签 ID 来避免信息泄露。而射频通信中的标签一般体积小，内部组成简单，计算存储能力有限，因而使用散列函数进行认证加密是合适的。随机 Hash-Lock[2]和 Hash 链[3]则分别将随机数和共享秘密机制引入 Hash-Lock 协议，能有效防范窃听和跟踪攻击，但仍然存在假冒攻击等问题。

近年来，研究人员基于 Hash 散列函数提出了诸多认证加密方法。文献[4]设计了一种基于距离的

收稿日期：2015-06-01，改回日期：2015-11-08；网络出版：2015-12-18
*通信作者：石乐义 shileyi@upc.edu.cn
基金项目：国家自然科学基金(61309024)，上海市金融信息技术研究重点实验室开放课题(2015)，山东省重点研发计划项目(2015GGX101045)
Foundation Items: The National Natural Science Foundation of China (61309024), The Funding of Shanghai Key Laboratory of Financial Information Technology (2015), Shandong Provincial Key Program of Research and Development (2015GGX191945)

RFID 安全认证协议 Noent，通过距离边界区分阅读器是否合法，适合于大量标签认证的应用，并且由于使用了离线数据库，对于密钥更新和防范去同步攻击有利。文献[5]则基于阅读器和标签之间同步的秘密信息，提出了基于数据库服务器和无数据库服务器两种方式的 RFID 标签双向认证协议。数据库服务器方式下，同步秘密信息由数据库组件监控，因而存在组件失效或被攻击后秘密信息泄漏的风险；而无数据库服务器方式中，标签对阅读器是匿名的，阅读器对标签的认证过程需要可信第三方，因而增加了开销。文献[6,7]通过 RFID 标签发送随机数并使用秘密值替代随机数，设计了基于 Hash 散列函数的 RFID 标签双向认证协议，用于解决假冒攻击、暴力攻击等问题。文献[8,9]则分析认为文献[6,7]的双向认证协议并不能抵御去同步、标签假冒和阅读器假冒等攻击，并随后给出了基于秘密同步的散列函数和标签阅读器双伪随机数改进方案。文献[10]在 Hash 链基础上引入伪随机数以抵抗重放和窃听攻击，标签在向阅读器发送询问响应消息时需要对更新后的密钥值加密，密钥更新代价较大。文献[11]提出了认证识别的单一会话模式和连续会话模式的概念，基于 Hash 函数设计了一个介于 RFID 标签和后端服务器之间的安全认证协议，并基于 GNY 逻辑给出了形式化证明。文献[12]和文献[13]在标签和数据库中共享认证密钥 K，每个标签存储一个自身标识和认证密钥的信息对，让阅读器和标签分别产生伪随机数 Rr 和 Rt，从而实现标签和阅读器间的双向认证，并在每次认证完成都进行密钥更新。显然，标签产生伪随机数和每次都进行密钥更新，增加了计算开销。文献[14]则给出了一种基于密钥值更新的安全认证协议，标签中除存储标识外，还需存储上次认证和本次认证使用的索引值和认证密钥，后端数据库对标签的认证需要多次查询和计算，标签和数据库为了实现同步需要对认证密钥更新，计算量大。文献[15]则给出了一种射频识别空中接口协议，采用异或运算和对称加密的方法进行标签和阅读器之间的加密认证。对称加密计算复杂度和资源开销大，因而对 RFID 标签有较高要求。

本文旨在针对 RFID 系统计算存储能力有限的特点，设计一种具有良好机密性、完整性、可用性的 RFID 认证协议。论文基于单向散列函数方式，引入伪随机数和共享秘密机制，设计了一种计算存储开销较小的 RFID 双向认证协议，分析了认证协议的抗攻击性能和效率性能，并进一步对协议模型安全性进行了形式化证明。

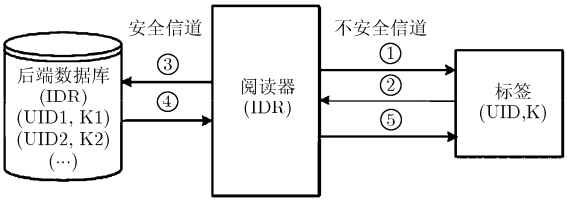
## 2 协议设计与描述

许多 RFID 认证算法假定 RFID 与阅读器之间通信信道是不安全的，而 RFID 系统中数据库与阅读器间通信信道是安全的，认证过程主要关注阅读器与标签之间的通信安全。然而，假冒阅读器在实际应用中会给 RFID 系统带来严重威胁。因此，本文算法假定 RFID 与阅读器之间信道不安全，且阅读器与后端数据库之间的信道也可能不安全。

本文协议考虑标签、阅读器、后端数据库之间的双向认证，适用于被动标签，阅读器具有伪随机数产生器，可独立生成伪随机数；后端数据库和标签中均设置有两个散列函数模块 H(•)和 f(•)、异或运算和字符连接运算模块，用于对伪随机数和身份标识进行加密和运算。其中，H(•)是 RFID 系统散列函数，而 f(•)则是标签的私有 Hash 映射，不同标签使用不同的 f(•)单向映射。两个单向散列函数的 Hash 映射为：$\{0,1\}^{*}\rightarrow\{0,1\}^{L}$，代表了输入不定长度的二进制数串，可得到定长为 L 的二进制数串输出。

这里，我们使用 Reader, DB, Tag 分别表示阅读器、后端数据库和标签，以 N 表示阅读器产生的伪随机数，K 是标签和数据库之间的共享认证密钥。散列函数运算、按位异或和字符串按比特连接操作分别用 H, f, ⊕和 ‖ 表示。合法标签和阅读器在出厂时被随机分配一个唯一的身份标识和认证密钥，同时这些标识和认证密钥存储在认证系统的数据库中，合法标签的唯一身份标识 UID(长度为 L)、认证密钥 K、私有散列函数 f 以三元组(UID, K, f)的方式存储在后端数据库。后端数据库中同时还存储与其相对应的阅读器标识 IDR，标签除了存储自身三元组标识(UID, K, f)外，还需要存储系统散列函数 H。RFID 双向认证协议流程如图 1 所示。

RFID 双向认证协议的具体步骤执行如下：




① Reader→Tag: (Query, N)

② Tag→Reader: (UID ⊕ H(N ‖ M), M)

③ Reader→DB: (UID ⊕ H(N ‖ M), N, M, IDR)

④ DB→Reader: (H(K ⊕ M), UID)

⑤ Reader→Tag: (H(K ⊕ M))

图 1 RFID 双向认证协议

步骤 1　阅读器用伪随机数发生器生成伪随机数 N，将其和认证询问请求 Query 一起发送至标签；

步骤 2　标签收到认证请求和伪随机数 N 后，先从自身存储器中找出 K，用私有散列函数 f()对认证密钥 K 和伪随机数 N 加密计算后得到 M=f(N||K)，并将其存储在自身存储器中，结合自身标识 UID, M 和伪随机数 N，运用系统散列函数 H()和逻辑运算操作计算 S=UID ⊕ H(N ‖ M)，然后将计算结果和 M 作为询问响应消息发给阅读器；

步骤 3　阅读器将收到的 UID ⊕ H(N ‖ M)和 M，伪随机数 N 和自身身份标识 IDR 一起发送给后端数据库；

步骤 4　后端数据库收到 IDR 后，首先与数据库存储的阅读器标识比较，验证阅读器的合法性。如果不是合法阅读器，则立刻中断认证过程，因为假冒的阅读器与后端数据库进行通信，不仅消耗通信资源，使得其他正常的阅读器无法与数据库完成通信，还可能因通信请求频繁使通信系统崩溃，数据库中存储的大量隐私信息因此泄露。阅读器验证通过后，数据库端将收到的 M、伪随机数 N 进行系统散列函数 H(•)加密得到 H(N ‖ M)，再与收到的 UID ⊕ H(N ‖ M)逻辑运算即可快速获得 UID，然后搜索数据库中是否存在标签标识 UID'与 UID 匹配。如果没有匹配项，说明阅读器对标签认证失败，该标签不合法，阅读器向标签发送认证失败消息；反之若存在匹配项 UID′，则表示标签通过了后台数据库的第 1 次认证。数据库还需进一步读取该标签认证密钥 K 和私有 Hash 函数 f()，加密计算 M′=f(N||K)，并检查是否与 M 一致。若一致，则标签顺利通过第 2 次认证，后台数据库计算 a=H(K ⊕ M)，将计算结果 a 和 UID 一起发给已经通过认证的阅读器；否则若不一致，标签未通过认证，标签不合法；

步骤 5　阅读器获得标签标识 UID，同时将 a=H(K ⊕ M)转发至标签；

步骤 6　RFID 标签收到 a 后，利用认证密钥 K 和 ROM 中存储的 M 进行一次异或运算和一次散列加密计算可得到 b=H(K ⊕ M)，然后比较 b 和 a 是否一致。如若结果一致，则标签对阅读器认证成功；否则，标签对阅读器认证失败。

至此，阅读器和标签之间已完成双向身份认证，接下来就可以进行正常的数据通信。

## 3　协议性能效率分析

### 3.1 协议抗攻击性能分析

本文协议基于共享秘密机制并引入伪随机数和私有散列函数，认证过程中进行了 2 次阅读器认证和 2 次标签认证，不使用明文直接传输标识数据，因此具有较好的抗攻击性能，分析如下：

(1)假冒攻击：攻击者利用伪造的非法标签、阅读器乃至后端数据库进行假冒攻击。对于标签假冒攻击，后台数据库存储合法标签的(UID, K, f)，并在认证通信过程中进行 2 次标签认证以验证 UID, K 和 f 是否匹配，只有具有正确三元组的标签才可以通过认证，因而可以有效防范标签假冒；对于非法阅读器，后台数据库在认证步骤 4 中对阅读器标识 IDR 进行验证，从而避免非法阅读器攻击。在最坏的假冒攻击情况下，即阅读器和后台数据库均为非法假冒，此时阅读器向合法标签发送查询请求和随机数 N，合法标签根据协议应答 UID ⊕ H(N ‖ M)和 M，非法后台数据库获得消息后，不仅无法获得合法标签的三元组(UID, K, f)，并且即便假冒认证通过，合法标签还要使用自身密钥 K 对 H(K ⊕ M)进行计算以验证是否为正常 RFID 系统，而非法数据库无法得到 K，因而无法通过合法标签的认证。可见，本文协议很好地抵御了假冒攻击。

(2)重放攻击：攻击者收集阅读器和标签认证过程中的查询数据(Query, N)和应答响应 UID ⊕ H(N ‖ M)和 M，随后重放以实现非法访问。本文协议引入伪随机数进行盲化处理，阅读器和标签之间的当前认证数据 UID ⊕ H(N ‖ M)和下次认证通信 UID ⊕ H(N′ ‖ M′)不一致，即便攻击者获得了标签 UID，但由于 N′和 M′失效而不能通过认证，因而可以防范重放攻击。

(3)窃听攻击：攻击者伪装成合法标签或阅读器以窃听分析认证通信数据。本文协议中，标签应答消息 M=f(N||K)和 H(N ‖ M)是单向散列函数与伪随机数 N 加密运算的结果，攻击者无法反向得到标签密钥 K，因而可以有效抵御窃听攻击。

(4)用户跟踪：攻击者根据多次截获的相同的标签认证应答消息确定标签用户并进行跟踪。本文协议中，标签用户每次与阅读器进行认证通信数据 M=f(N||K)和 S=UID ⊕ H(N ‖ M)都在不断变化和不可连接关联，可以解决用户跟踪问题。

(5)拒绝服务攻击：本文协议对标签被访问读取的次数没有限定，标签收到阅读器发送的认证请求和伪随机数后，只进行加密运算而无需密钥更新。因此，相比较密钥动态更新的认证协议而言，当标签收到多个伪造的认证请求时，不会因为计算量过大而停止工作。可见，本文协议具有一定的抗拒绝服务攻击能力。

(6)前向安全性：每次认证过程中标签的私有哈希映射 f(•)都对认证密钥 K 与伪随机数 N 逻辑运算

后的结果进行了加密，而且每次都随机产生 N，因此即使认证密钥 K 被攻击者获取，它也无法获取该标签的历史活动信息，从而有效实现了系统的前向安全性。

表 1 给出了本文所提出的基于共享秘密和伪随机机制的双散列函数认证协议与几种经典轻量级 RFID 认证协议，即 Hash-Lock 协议[1]、随机 Hash-Lock 协议[2]、Hash 链协议[3]、数字图书馆协议[16]、LCAP 协议[17]和杂凑 ID 变化协议[18]等认证协议与本文协议安全性能的比较。

**表 1 抗攻击性能对比**

| | 用户跟踪 | 拒绝服务 | 重放攻击 | 窃听攻击 | 假冒攻击 | 明文传输 |
|---|---|---|---|---|---|---|
| Hash-Lock | × | √ | × | × | × | √ |
| 随机Hash | √ | × | × | × | × | √ |
| Hash 链 | √ | × | √ | √ | × | × |
| 数字图书馆 | √ | × | √ | √ | √ | × |
| LCAP | × | × | √ | √ | √ | × |
| 杂凑 ID 变化 | √ | × | √ | √ | √ | × |
| 本文协议 | √ | √ | √ | √ | √ | × |

表中使用“×”表示协议可能会遭受相应的攻击，不具备相应的安全性；用“√”表示协议具备相应的安全性，可以避免相应的攻击。本文协议在用户跟踪、拒绝服务、重放攻击、窃听等方面具备良好的安全防护，并且可以抵御假冒标签、假冒阅读器乃至假冒数据库等攻击。

### 3.2 协议执行效率分析

本文协议认证过程中，阅读器进行 1 次伪随机数生成，标签进行 2 次哈希运算，后端数据库则进行 1 次搜索查询操作和 2 次哈希运算，数据库只需执行 1 次 UID 的搜索查询即可验证标签的合法性，而不是通过对数据库中的标签标识逐个进行散列计算匹配来找到验证，大大降低了计算和搜索匹配的复杂度。本文协议中，标签不需要产生伪随机数，降低了标签的复杂性和制造成本。表 2 给出了与前述几种经典常用协议效率性能的比较结果，其中 n 表示系统中待认证的标签数目，j 表示正在进行第 j 次通信认证，R 表示伪随机数的产生操作次数，H 表示散列运算的次数。为了方便比较，这里将标签标识 UID、共享认证密钥 K 和伪随机数的长度比特统一设定为 L。

从表 2 可以看出，在标签和后端数据库的存储开销上，几种认证协议相差不大，随机 Hash-Lock 协议的存储开销最低，而杂凑 ID 变化协议存储开销

**表 2 效率性能比较**

| | 计算开销 | | | 存储开销 | |
|---|---|---|---|---|---|
| | 标签 | 阅读器 | 后端数据库 | 标签 | 后端数据库 |
| Hash-Lock | 1H | – | – | 2L | 3nL |
| 随机Hash | 1H1R | $\frac{n}{2}$H | – | 1L | nL |
| Hash 链 | 2H | – | $\frac{j*n}{2}$H | 2L | 2nL |
| 数字图书馆 | 2H1R | 1R | $\left(\frac{n}{2}+1\right)$H | 2L | 2nL |
| LCAP | 2H | 1R | $\left(\frac{n+1}{2}+2\right)$H | 2L | 2nL |
| 杂凑 ID 变化 | 3H | – | $\left(\frac{n}{2}+1\right)$H | 3L | 10nL |
| 本文协议 | 2H | 1R | 2H | 2L | 2nL |

最多。在计算开销方面，由于 Hash-Lock 协议和随机 Hash-Lock 协议后端数据库没有采用散列运算，因而计算开销最低，但也失去安全保障；Hash 链协议后端数据库计算开销和存储开销都与标签数量 n 成正比，不适合用于大规模标签应用；数字图书馆认证协议在标签中产生伪随机数，增加了标签的成本和复杂性。本文协议标签和后端数据库的存储开销与其他认证协议相当(仅高于随机 Hash-Lock 协议)，计算开销均为 2H，并且实现了双向认证和各安全性目标。这意味着每增加 1 个标签，本文协议将增加 2 次后端数据库 Hash 计算和 1 次随机数生成，因此本文协议可适用于标签数量多的系统。

## 4 协议 BAN 逻辑分析与安全性证明

为了形式化分析和证明本文加密认证协议的安全性，我们采用 BAN 逻辑分析方法[19]进行证明。

### 4.1 协议模型形式化描述

首先对本文协议的认证加密过程进行简化：阅读器和标签分别用 R 和 T 表示，标签向阅读器发送了自身标识 UID，本文协议中阅读器虽然没有将自身标识发送给标签，但形式化分析简化具体认证过程，抽象化之后可以认为阅读器向标签发送了标识 IDR。这样，本文协议模型可以形式化描述为：

$\mathrm{R} \rightarrow \mathrm{T} : \mathrm{Query}, \mathrm{N}$；

$\mathrm{T} \rightarrow \mathrm{R} : \mathrm{M}, \mathrm{S}$；

$\mathrm{R} \rightarrow \mathrm{DB} : \mathrm{M}, \mathrm{N}, \mathrm{S}, \mathrm{ID}_R$；

$\mathrm{DB} \rightarrow \mathrm{R} : \mathrm{a}, \mathrm{UID}$；

$\mathrm{R} \rightarrow \mathrm{T} : \mathrm{a}$。

考虑到通常假定后端数据库和阅读器之间的通信信道是安全的，因而可将阅读器和后端数据库看

作同一认证主体 R，标签则是另一认证主体 T，协议模型可进一步形式化为：

$\mathrm{R} \lhd \{\mathrm{N}, \mathrm{UID}\}_K$；

$\mathrm{T} \lhd \{\mathrm{M}, \mathrm{ID}_R\}_K$。

### 4.2 协议安全目标

(1) $\mathrm{R} \mid\equiv \mathrm{UID}$；

(2) $\mathrm{T} \mid\equiv \mathrm{ID}_R$。

### 4.3 协议初始假设

P1　$\mathrm{R} \mid\equiv \mathrm{R} \leftrightarrow \mathrm{T}$；

P2　$\mathrm{T} \mid\equiv \mathrm{T} \leftrightarrow \mathrm{R}$；

P3　$\mathrm{R} \mid\equiv \#(\mathrm{N})$；

P4　$\mathrm{T} \mid\equiv \#(\mathrm{M})$；

P5　$\mathrm{R} \mid\equiv \mathrm{T} \mid\Rightarrow \mathrm{UID}$；

P6　$\mathrm{T} \mid\equiv \mathrm{R} \mid\Rightarrow \mathrm{ID}_R$。

### 4.4 协议证明分析

首先证明 $\mathrm{R} \mid\equiv \mathrm{UID}$：因为有 $\mathrm{R} \lhd \{\mathrm{N}, \mathrm{UID}\}_K$，由初始假设 P1 和消息规则

$$\mathrm{R1}\ \frac{P \mid\equiv P \leftrightarrow Q, P \lhd \{X\}_K}{(P \mid\equiv Q \mid\sim X)}$$

可形式化推出 $\mathrm{R} \mid\equiv \mathrm{T} \mid\sim \{\mathrm{N}, \mathrm{UID}\}$，即 $\mathrm{R} \mid\equiv \mathrm{T} \mid\sim \mathrm{UID}$。由初始假设 P3 和消息规则 $\mathrm{R11}\ \dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$，可推知 $\mathrm{R} \mid\equiv \#(\mathrm{UID})$。

再根据随机数验证规则

$$\mathrm{R4}\ \frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{(P \mid\equiv Q \mid\equiv X)}$$

可推理出 $\mathrm{R} \mid\equiv \mathrm{T} \mid\equiv \mathrm{UID}$。由初始假设 P5 和管辖规则

$$\mathrm{R5}\ \frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{(P \mid\equiv X)}$$

即可证明 $\mathrm{R} \mid\equiv \mathrm{UID}$。

同理证明 $\mathrm{T} \mid\equiv \mathrm{ID}_R$：因为有 $\mathrm{T} \lhd \{\mathrm{M}, \mathrm{ID}_R\}_K$，由初始假设 P2 和消息规则

$$\mathrm{R1}\ \frac{P \mid\equiv P \leftrightarrow Q, P \lhd \{X\}_K}{(P \mid\equiv Q \mid\sim X)}$$

可形式化推出 $\mathrm{T} \mid\equiv \mathrm{R} \mid\sim \{\mathrm{M}, \mathrm{ID}_R\}$，也就是 $\mathrm{T} \mid\equiv \mathrm{R} \mid\sim \mathrm{ID}_R$。由初始假设 P4 和消息规则

$$\mathrm{R11}\ \frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$$

可推知 $\mathrm{T} \mid\equiv \#(\mathrm{ID}_R)$。

再根据随机数验证规则

$$\mathrm{R4}\ \frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{(P \mid\equiv Q \mid\equiv X)}$$

推理得到 $\mathrm{T} \mid\equiv \mathrm{R} \mid\equiv \mathrm{ID}_R$。由初始假设 P6 和管辖规则

$$\mathrm{R5}\ \frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{(P \mid\equiv X)}$$

即可证明 $\mathrm{T} \mid\equiv \mathrm{ID}_R$。

通过以上 BAN 逻辑证明分析可知，本文协议实现了安全目标，标签和阅读器之间实现了安全的双向认证。

## 5　结束语

本文在分析借鉴近年来国内外 RFID 认证加密协议方面的研究工作的基础上，设计了一种基于共享秘密的伪随机散列函数 RFID 双向认证协议。认证协议中引入标签私有 Hash 函数 f 并由后端数据库和标签共享，用于实现标签对阅读器和后端服务器的反向认证，强化标签密钥 K 的保护，提高了抵御窃听和假冒攻击的性能；引入伪随机数并由阅读器而不是标签产生，实现对认证通信数据的盲化处理，有效防范重放攻击，也降低了标签计算存储开销；将标签 UID 与系统单向散列函数的逻辑运算结果作为应答消息，大幅减少了后端数据库的查询开销，也在一定程度上保障了认证通信的机密性。在此基础上，本文分析了认证协议的抗攻击性能和效率性能，并基于经典的 BAN 逻辑分析方法对协议模型进行了分析，证明了本文协议能够实现预期安全目标。

## 参 考 文 献


[1] HUANG H F, YU P K, and LIU K C. A privacy and authentication protocol for mobile RFID system[C]. 2014 IEEE International Symposium on Independent Computing, IEEE, Orlando, USA, 2014: 1–6.

[2] NYALAMADUGU S, LIU J, and DE VELASCO CORTINA F M. Methods and apparatus for preserving privacy in an RFID system[P]. U.S. Patent 8710960. 2014.

[3] LI N, MU Y, SUSILO W, *et al*. Privacy-preserving Authorized RFID Authentication Protocols[M]. Radio Frequency Identification: Security and Privacy Issues. Springer International Publishing, Berlin, Germany, 2014: 108–122.

[4] PERIS-LOPEZ P, ORFILA A, PALOMAR E, *et al*. A secure distance-based RFID identification protocol with an off-line back-end database[J]. *Personal and Ubiquitous Computing*, 2012, 16(3): 351–365.

[5] HAN S, DILLON T, POTDAR V, *et al*. RFID mutual authentication protocols for tags and readers with and without a server[J]. *Computer Systems Science and Engineering*, 2013, 28(2): 91–99.

[6] CHO J S, YEO S S, and KIM S K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value[J]. *Computer Communications*, 2011, 34(3): 391–397.

[7] CHO J S, JEONG Y S, and PARK S O. Consideration on the brute-force attack cost and retrieval cost: A hash-based

radio- frequency identification (RFID) tag mutual authentication protocol[J]. *Computers & Mathematics with Applications*, 2012: 1–8.

[8] Kim H. RFID mutual authentication protocol based on synchronized secret[J]. *International Journal of Security & Its Applications*, 2013, 7(4): 37–49.

[9] SAFKHANI M, PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, *et al*. Cryptanalysis of the Cho *et al*. protocol: a hash-based RFID tag mutual authentication protocol[J]. *Journal of Computational and Applied Mathematics*, 2014, 259: 571–577.

[10] 周晔. 基于Hash链的RFID双向认证协议研究[D]. [硕士论文], 西南交通大学, 2012.
ZHOU Y. Research on RFID mutual authentication protocol based on Hash chain[D]. [Master dissertation], South West Jiaotong University, 2012.

[11] 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 Z, LI J, and FENG B. Research on Hash-based RFID security authentication protocol[J]. *Journal of Computer Research and Development*, 2009, 46(4): 583–592.

[12] 孙肖, 赵泽茂. 一种基于哈希函数的 RFID 双向认证协议[J]. 杭州电子科技大学学报, 2012, 32(6): 29–32.
SUN X and ZHAO Z. A Hash-based mutual authentication protocol for the RFID system[J]. *Journal of Hangzhou Dianzi University*, 2012, 32(6): 29–32.

[13] 蔡豪. RFID 安全认证协议的研究与设计[D]. [硕士论文], 华中科技大学, 2010.
CAI H. Studies on RFID security authentication protocol[D]. [Master dissertation], Huazhong University of Science & Technology, 2010.

[14] 李斌. RFID 安全协议的研究[D]. [硕士论文], 复旦大学, 2012.
LI B. Research on RFID security protocol[D]. [Master dissertation], Fudan University, 2012.

[15] 信息技术射频识别 800/900 MHz 空中接口协议[S]. 北京: 中国标准出版社, 2013, GB/T29768-2013.
Information technology-radio frequency identification air interface protocol at 800/900 MHz[S]. Beijing: Standards Press of China, 2013, GB/T 29768–2013.

[16] WANG J, FLOERKEMEIER C, and SARMA S E. Session-based security enhancement of RFID systems for emerging open-loop applications[J]. *Personal and Ubiquitous Computing*, 2014, 18(8): 1881–1891.

[17] MAMUN M S I and MIYAJI A. A privacy–preserving efficient RFID authentication protocol from SLPN assumption[J]. *International Journal of Computational Science and Engineering*, 2015, 10(3): 234–243.

[18] SHOARINEJAD K and SOLTAN M. Systems and methods for RFID security[P]. U.S. Patent Application 14/592,455. 2015-1-8.

[19] BURROWS M, ABADI M, and NEEDHAM R M. A logic of authentication[C]. Proceedings of the Royal Society of London. A: Mathematical and Physical Sciences. The Royal Society, London, 1989, 426(1871): 233–271.

石乐义： 男，1975 年生，博士，教授，硕士生导师，研究方向为网络与信息安全、博弈理论、移动计算.

贾 聪： 男，1989 年生，硕士生，研究方向为网络与信息安全、移动支付安全.

宫 剑： 男，1975 年生，硕士，高级工程师，研究方向为金融信息管理.

刘 昕： 女，1974 年生，博士，讲师，研究方向为网络与信息安全、社会计算.

陈鸿龙： 男，1982 年生，博士，副教授，研究方向为无线传感器网络、网络安全、物联网.