基于云的轻量级RFID群组标签认证协议

李璐璐 董庆宽 陈萌萌

(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 射频识别技术(Radio Frequency Identification,RFID)作为物联网中标识物品的关键技术,其因低成本、易携带等优势而得到了广泛的应用。基于云存储的RFID技术相较于传统RFID技术更具有应用市场,但其安全隐私问题也更为严重。另外,现有的很多群组标签认证协议不仅不符合轻量级要求,还具有密钥失同步的问题。文中提出一种基于云的轻量级RFID群组标签认证协议。该协议基于Hash函数而设计,它不仅解决了上述安全隐患,还能在群组认证过程中筛除无效标签和假冒标签。最后,利用BAN逻辑对该协议进行了分析。安全目标分析表明,该协议可以抗多重DOS攻击以及其他基本攻击,并满足前向安全性。

关键词 云数据库,RFID,轻量级认证协议,群组认证,BAN逻辑

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.01.028

Cloud-based Lightweight RFID Group Tag Authentication Protocol

LI Lu-lu DONG Qing-kuan CHEN Meng-meng

(State Key Laboratory of Integrated Service Networks,Xidian University,Xi'an 710071,China)

Abstract As a key technology for indentifying objects in the Internet of Things (IoT),radio frequency identification (RFID) technology has been widely used because of its advantages,such as low cost and easy to carry. The RFID system based on cloud storage technology has a more widely application market comparing with the traditional RFID system,but its security and privacy issues are more serious. At the same time,many existing group authentication protocols don't meet the lightweight requirements,and have the lost synchronization problem in key updating process. This paper proposed a cloud-based lightweight RFID tag group authentication protocol. This protocol is based on the Hash function,which not only resolves these issues above,but also filters out the invalid and fake labels. Finally,this paper conducted the formal analysis of the proposed protocol by using BAN logic. The security target analysis shows that the proposed protocol can resist the multi-DOS attack and other common attacks,and possesses the forward security.

Keywords Cloud database,RFID,Lightweight authentication protocol,Group authentication,BAN logic

1 引言

射频识别(Radio Frequency Identification,RFID)技术是物联网中的一项关键技术,它以非接触的方式自动识别物体。RFID技术起源于军事应用,后来投入商业使用。与传统条形码相比,RFID标签具有成本低、体积小、易于携带等一系列优点[1]。现在,RFID技术主要被用于物流管理、访问控制、跟踪、定位、道路桥梁、自动收费和图书分类等[2-3]。

通常,一个RFID系统包括电子标签、阅读器、后台服务器3部分[4-5],阅读器通过无线连接方式[6]进行标签的扫描和数据库的查询,并向后台数据库发出请求。低成本RFID标签也被称为无源标签,它通过阅读器提供的电磁场获得能量,因此它的计算能力和硬件资源非常有限。阅读器可以通过无线信道识别标签,并读取标签上的信息。射频识别技术是物联网感知层的关键技术之一[7]。

传统RFID认证方案假设后台服务器与阅读器之间有线信道连接,我们也认为阅读器和后台数据库之间的有线信道是安全的。然而,这一假设限制了阅读器的移动性以及后台数据库的工作容量。一种无需服务器的认证协议[8]于2012年被提出,该协议可以解决上述问题,但只支持离线认证,而且需要引进可信第三方,并且该协议只支持少量标签的认证;2010年,Huque等[9]提出了一种无后台的Hash函数的认证协议和搜索协议,该方案去掉了传统RFID系统的后台数据库部分,而采用在阅读器中存储具有标签和其身份标识的接入表来进行双向认证,但该方案不能满足大量标签的认证,并且增加了阅读器的计算复杂度和存储复杂度。随着物联网的发展,海量的物品将依靠RFID技术进行管理、识别和认证,这就要求RFID系统需要支持大数据的应用,那么巨大的搜

到稿日期:2017-12-20 返修日期:2018-03-22 本文受国家自然科学基金项目(61373172)资助。

李璐璐(1993-),女,硕士生,主要研究方向为信息安全,E-mail:992946641@qq.com;**董庆宽**(1973-),男,硕士生导师,主要研究方向为信息安全,E-mail:qkdong@mail.xidian.edu.cn(通信作者);**陈萌萌**(1993-),女,硕士生,主要研究方向为信息安全。

索能力、存储能力和计算能力也就成为了传统的后台服务器的瓶颈，而目前快速发展的云存储技术[10]可以解决这个问题。基于云的 RFID 系统引起了学者的广泛关注，在该系统中，用户可以通过购买或租赁云存储服务来部署和维护 RFID 系统，从而降低成本。但与传统的 RFID 系统相比，基于云的 RFID 系统的安全和隐私问题更加严重。在基于云的 RFID 系统中，阅读器和云数据库之间的连接是不安全的，云服务提供商是不可信的。因此，用户必须对其存储在云数据库中的数据进行加密，以防止隐私泄漏。通常，基于云的 RFID 系统的安全隐私问题要比传统的 RFID 系统更加严重。现如今，已有学者提出了一些基于云的 RFID 认证协议（详细内容请见本文第 2 节），但大多数都不安全，且不能支持标签的组认证。

另外，低成本是设计 RFID 认证协议的重要目标，也就是说，需要设计轻量级协议。但是现存的群组认证协议需要标签具有很大的存储和计算能力，不满足低成本无源标签的要求。而到目前为止，轻量级的 RFID 认证协议大都是采用具有一定安全性的 Hash 函数[11]作为基本组件，只需要很小的硬件资源消耗。

本文提出了一个基于云的轻量级 RFID 群组认证协议。该协议基于哈希函数设计，不仅考虑了云和标签组的相互认证，还满足了隐私保护和低成本的要求。更重要的是，其筛选剔除了无效和假冒标签。本文采用的是轻量级哈希函数 Photon-160/36/36，它属于 Photon 函数族[12]，是在 2011 年的 Crypto 上被提出的；本文还分析了它的硬件消耗。

本文第 2 节详细介绍了几个具有代表性的 RFID 认证协议；第 3 节提出了基于云的轻量级 RFID 群组认证协议；第 4 节基于 BAN 逻辑对协议进行安全性分析，并将其与其他方案进行性能对比；第 5 节介绍了本文所用的哈希函数及其硬件逻辑结构，并对其性能进行了分析；最后总结全文。

2　相关工作

本节将简单回顾几个基于云的 RFID 认证协议和群组认证协议。通常，基于云的认证系统包括阅读器、标签和云服务器（云数据库），这里的阅读器是可移动的，并且存储在云数据库中的信息是加密的。对基于云的认证协议的分析和介绍如下。

Wei 等[13]于 2013 年提出了第一个基于云的 RFID 认证方案，该认证方案中的认证系统由标签、阅读器、VPN 代理以及云数据库构成。该方案用一张加密哈希表（EHT）来保护存储在云中的标签的信息。但是此方案的 VPN 部署及维护成本很高，不满足轻量级要求，也不能抵抗跟踪攻击和 DOS 攻击。

Dong 等[14]于 2015 年提出了基于位置隐私云的 RFID 双向认证协议。该协议引入了位置隐私云，阅读器与云的信息交互由位置隐私云转发，且阅读器的 IP 地址在位置隐私云的接入点进行了加密，从而很好地保护了阅读器的位置隐私。但是该方案需要公共基础设施的支持，成本不够低廉。

郑金彬等[15]于 2016 年提出了基于云服务器的 RFID 双向认证协议，其是基于对称密钥实现的标签与阅读器以及标签与云之间的双向认证。虽然该协议的计算复杂度低，但其未进行密钥更新，不具备前/后向安全性，且不能抵抗 DOS 攻击和去同步攻击。

现有的协议大都只能支持单个标签的认证，为了提高 RFID 认证的效率，许多基于群组标签的认证协议被提出。

Kardas 等[16]于 2013 年提出了一种使用云计算实现基于对称密钥的加密认证协议，该协议可以实现多个标签的认证，但只实现了标签与云的单向认证，且当攻击者冒充一个标签进行交互时，其他标签的认证也会被干扰，并且该方案不能抵抗拒绝服务攻击。

Guo 等[17]于 2015 年提出了一种轻量级隐私保护的 RFID 群组认证协议 LPGP，该协议利用复杂度较小的伪随机数发生器及散列运算来提高协议的运行效率，并且可以实现群组的认证，但是该协议不能在群组认证过程中剔除无效标签和假冒标签。

Zhang 等[18]于 2015 年提出了一种安全且高效的 RFID 批量认证协议，该协议是利用群组标签的组密钥和私密钥之间的关系以及融合哈希函数而设计的群组认证协议。该协议要求标签具有较好的计算量和存储量，属于中量级认证协议，不满足轻量级的要求。

这些协议虽然实现了标签的群组认证，但在结合云数据库时缺乏安全有效的方案，不仅不能保证协议的安全性，更不能剔除无效和假冒标签。

本文提出了一个轻量级的基于云的 RFID 组认证协议。该协议基于 Hash 函数设计，既考虑了云和标签组之间的相互认证，又解决了隐私保护和低成本的问题。特别地，该方案可以抵抗多轮 DOS 攻击（即攻击者连续不断地发起 DOS 攻击），还可以用于过滤认证过程中的无效标签和假冒标签。

3　本文提出的协议

3.1　认证系统各构成件技术要求

本文提出的协议包括云服务器、阅读器和群组标签 3 部分。基于云的轻量级 RFID 群组认证系统中各构成件的具体技术要求如下。

（1）标签组所需变量及能力要求：N_i 个组成员标签所属组的共享密钥 K_g、组标签的身份标识 G_{id}、N_i 个组成员标签的身份 id，以及简单的哈希函数计算（本文采用的哈希函数是轻量级哈希函数 photon，详见第 5 节）。

（2）阅读器所需变量及能力要求：阅读器在云端的注册身份信息 id_r、阅读器的密钥 K（只有阅读器知道）、用于加密存储在云中的消息，以及云与阅读器交互的共享密钥 K_{rc}，其还需要支持伪随机数的产生以及哈希函数的计算。

（3）云数据库服务器所需变量及能力要求：阅读器在云端的加密注册身份信息 $\{id_r\}_K$，群组标签的组身份标识的哈希值 $H(G_{id})$，加密的组共享密钥的新、旧密钥对及其哈希值 $H(Kg^{new})$ 和 $H(Kg^{old})$，加密的组标签成员的身份认证信息

$\{id_{Ti}\}_K$，加密的组标签成员对应的商品信息$\{info\}_k$，以及云与阅读器交互的共享密钥 K_{rc} 和加密的变量$\{X\}_K$，变量$\{X\}_K$ 用于在上一轮认证中密钥更新不同步的情况下解密标签组信息。另外，云数据库还要支持伪随机数的产生。

基于云的轻量级 RFID 群组标签认证系统的结构图如图 1 所示。

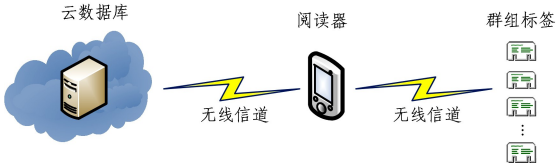

图 1 基于云的轻量级 RFID 群组标签认证系统的结构图

Fig. 1 Structure of cloud-based lightweight RFID group tag authentication system

3.2 基于云的 RFID 双向认证协议

上文介绍了基于云的 RFID 群组标签的系统结构和各构成件的要素，本节将介绍该认证系统的具体协议及认证过程。

3.2.1 协议的符号定义

本协议的符号定义如表 1 所列。

表 1 符号定义

Table 1 Definition of notations

符号	定义
$\|$	消息级联
$H(\cdot)$	单向哈希运算
N_r	阅读器产生的随机数
N_c	云端产生的随机数
N_r^t	阅读器为合法标签生成的随机数
id_{Ti}	标签各自的 id
id_r	阅读器的 id
G_{id}	待认证标签组的身份标识
K_g	待认证标签组的组共享密钥
K_{rc}	云与阅读器之间消息的保密传递
K	加密存储于云中数据的阅读器密钥

3.2.2 协议初始化阶段

协议运行之前，需进行如下初始化：

(1)组标签成员各自存储自己的身份 id_{Ti} 和组共享密钥 K_g；

(2)云数据库服务器存储对应的各标签组的组共享密钥哈希值 $H(Kg)$与组标签身份标识哈希值 $H(G_{id})$。

3.2.3 协议的认证阶段

(1)初始化数据。

(2)阅读器向群组标签广播认证请求。

阅读器扫描一组待认证群组标签，产生一个随机数 N_r，生成认证请求消息并将其广播给待认证群组标签。

(3)标签端做出响应并由阅读器转发给云。

1)标签组接收请求消息，并计算 $H(N_r \| id_{Ti})$，$H(Kg)$，$H(G_{id})$。

2)标签组用该组共享密钥加密，生成$\{H(N_r \| id_{Ti}) \| id_{Ti}\}_{Kg}$，$H(G_{id})$和 $H(Kg)$消息串，并将其发送给阅读器。

3)阅读器接收消息，并存储$\{H(N_r \| id_{Ti}) \| id_{Ti}\}_{Kg}$，用 K 加密阅读器身份 id_r，再利用密钥 K_{rc} 计算消息认证码 $MAC_{1K_{rc}}=H(H(Kg) \| H(G_{id}) \| \{id_r\}_k \| N_r)$，生成响应消息串并转发给云。

(4)云端验证阅读器身份并验证标签的完整性与合法性，同时检查上一轮认证密钥更新是否同步。

1)云端接收消息，用 K_{rc} 验证消息认证码 $MAC_{1K_{rc}}$，确保消息完整真实；验证阅读器身份$\{id_r\}_K$，在后端数据库查找阅读器的加密注册身份，若查找到对应身份，则继续以下步骤；否则视为阅读器不合法，协议终止。

2)验证阅读器身份后，查找组标签身份标识哈希值 $H(G_{id})$，若查找到对应的标签组，则找出对应存储的加密的组共享密钥$\{Kg\}_K$ 和哈希值 $H(Kg)$；否则，云端返回消息向阅读器报错。

3)找到对应存储的加密组共享密钥$\{Kg\}_K$ 和哈希值 $H(Kg)$后，与接收到的密钥哈希值 $H(Kg)$进行对比，有以下 4 种情况：

①$H(Kg)=H(Kg^{old})$且 $H(Kg)\neq H(Kg^{new})$，云成功更新但标签组未成功更新。则令$\{X\}_K=\{Kg^{old}\}_K$，再返回$\{Kg^{new}\}_K$，$\{Kg^{old}\}_K$。

②$H(Kg)=H(Kg^{old})=H(Kg^{new})$，云和标签组都没有更新成功。则令$\{X\}_K=\{Kg^{old}\}_K$，再返回$\{Kg^{new}\}_K$，$\{Kg^{old}\}_K$。

③$H(Kg)=H(Kg^{new})$，且 $H(Kg)\neq H(Kg^{old})$，标签组和云都更新成功。则令$\{X\}_K=\{Kg^{new}\}_K$，再返回$\{Kg^{new}\}_K$，$\{Kg^{old}\}_K$。

④$H(Kg)\neq H(Kg^{old})$且 $H(Kg)\neq H(Kg^{new})$，则标签组不合法，认证失败，协议终止。

4)认证成功后，云生成随机数 N_c，并返回消息串$\{X\}_K$，N_c，$\{Kg^{new}\}_K$ 和$\{Kg^{old}\}_K$ 给阅读器，并利用 K_{rc} 计算消息认证码 $MAC_{2K_{rc}}=H(\{X\}_K \| N_c \| \{Kg^{new}\}_K \| \{Kg^{old}\}_K)$，一并返回给阅读器。

(5)阅读器接收消息，并利用 K_{rc} 验证消息认证码 $MAC_{2K_{rc}}$，以确认消息的完整性与真实性；阅读器用密钥 K 解密消息，存储 X，并用 X 解密$\{H(N_r \| id_{Ti}) \| id_{Ti}\}_{Kg}$，接收到 α 个消息，其中 β 个消息正常解密，会出现以下 3 种情况：

1)若 $\beta<\alpha<N_i$，则说明这 β 个标签合法且有效，而$(\alpha-\beta)$个标签属于假冒标签，$(N_i-\alpha)$个标签属于无效标签，无法应答。

2)若 $\beta=\alpha<N_i$，则说明这 α 个标签为合法且有效的标签，而$(N_i-\alpha)$个标签为失效标签，无法应答。

3)若 $\beta=\alpha=N_i$，则说明这 N_i 个标签均是合法且有效的标签，阅读器为 β 个合法标签生成随机数 N_r^t，并打包合法标签的身份信息$\{id_{Ti}\}_K^T$。

(6)阅读器解决上一轮密钥更新不同步问题。阅读器对比从云接收到的新、旧密钥对，判断上一轮密钥更新是否同步，并解决以下不同步问题：

1)若 $Kg^{new}=Kg^{old}$，令 $Kg^{new\prime}=H(Kg^{new}\oplus Nr)$。

2）若 $Kg^{new} \neq Kg^{old}$，令 $Kg^{new\prime} = Kg^{new}$；用阅读器密钥加密 $Kg^{new\prime}$，并利用 K_{rc} 生成消息认证码 $MAC_{3K_{rc}} = H(\{Kg^{new\prime}\}_K \| \{id_{Ti}\}_K^T \| N_r^t)$，返回消息给云，同步密钥。

（7）云端接收消息，并验证 $MAC_{3K_{rc}}$，确认消息完整；同步密钥，令 $\{Kg^{new}\}_K = \{Kg^{new\prime}\}_K$；对比合法标签加密 id 信息，人工剔除除 $\{id_{Ti}\}_K^T$ 之外的标签 id 信息以及对应的加密商品信息 $\{info\}_K$。云返回随机数 N_c，确认密钥同步以及筛选剔除假冒无效标签成功。

（8）阅读器接收消息，计算 $H(X \| N_c)$ 和 $H(id_{Ti} \| N_r^t)$，生成消息串 $\{H(X \| N_c) \| H(id_{Ti} \| N_r^t) \| Kg^{new\prime}\}_X, N_c, N_r^t$，并将该消息串发送给标签组。

（9）标签计算 $H(Kg \| N_c)$，并验证 $H(Kg \| N_c)$ 是否等于 $H(X \| N_c)$，若相等，则标签组认证云；否则认证失败，协议终止。认证成功后，人工剔除标签组中未收到消息的标签，并更新密钥 $Kg = Kg^{new\prime}$，使密钥同步；标签组返回消息 $\{Kg \| id_{Ti}\}_{Kg}$ 给阅读器。

（10）阅读器接收消息，用 $Kg^{new\prime}$ 解密得到 id_{Ti}，Kg，对比第（4）步解密得到的 id_{Ti} 与接收到的 id_{Ti}，若相等，则证明剔除的标签无误。阅读器更新密钥，计算 $Kg^{new\prime\prime} = H(Kg | N_r^t)$，再利用 K_{rc} 计算消息认证码 $MAC_{4K_{rc}} = H(\{Kg^{new\prime\prime}\}_K \| H(Kg^{new\prime\prime}) \| N_r^t)$，并发送密钥更新消息给云。

（11）云接收消息，验证 $MAC_{4K_{rc}}$，再赋值：$H(Kg^{old}) = H(Kg^{new})$，$H(Kg^{new}) = H(Kg^{new\prime\prime})$，$\{Kg^{old}\}_K = \{Kg^{new}\}_K$，$\{Kg^{new}\}_K = \{Kg^{new\prime\prime}\}_K$。云返回密钥更新成功消息 ACK 给阅读器。

（12）阅读器接收消息后计算 $H(Kg^{new\prime\prime} \| N_c \| N_r^t)$，并将结果发送给标签组。

（13）标签组接收消息后更新密钥。计算 $Kg^{new} = H(Kg \| N_r^t)$，验证 $H(Kg^{new} \| N_c \| N_r^t)$ 是否等于 $H(Kg^{new\prime\prime} \| N_c \| N_r^t)$，若相等，则令 $Kg = Kg^{new}$，标签组密钥更新成功，认证结束；否则标签重新计算 $Kg^{new} = H(Kg \| N_r^t)$。

（14）终止协议。

基于云的轻量级 RFID 群组标签认证协议过程如图 2 所示。

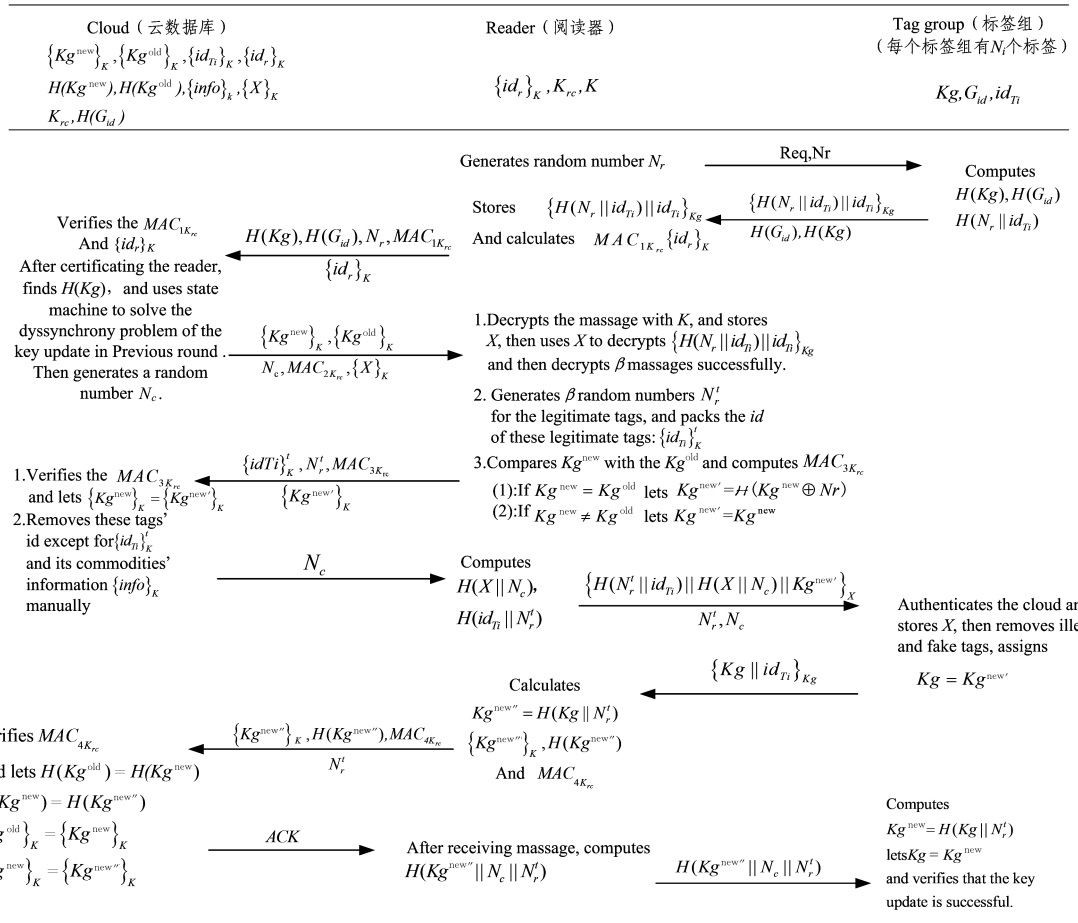

图 2　基于云的轻量级 RFID 群组标签认证协议示意图

Fig. 2　Schematic diagram of cloud-based lightweight RFID group tag authentication protocol

4　安全性及其性能分析

4.1　安全目标实现情况分析

本文提出的基于云的 RFID 群组认证方案不仅实现了云端数据库服务器与标签组的双向认证，还可以抵抗各类攻击，满足各项安全特性。

（1）抗跟踪攻击

标签组的每一次认证都会使用不同的组共享密钥，而该组共享密钥在每一次认证结束之后都会更新，并且其利用阅读器发送的伪随机数计算不同的索引哈希值，因此攻击者不能在下一轮认证中发送同样的信息试图获得同样的回应以跟踪标签组。

(2)抗重放攻击

因为群组标签在每轮认证结束后会更新组共享密钥,并且阅读器在每次认证时也会使用不同的随机数,且随机数无规律可循,所以攻击者不能重放上一轮的消息从而通过认证;就算攻击者使用相同的随机数,也会由于不知道组共享密钥而重放失败。因此,标签组能抵抗重放攻击。

(3)前/后向安全性

因为标签组更新密钥使用一次性单项哈希函数以及随机数,更新规则为 $Kg^{new}=H(Kg \parallel N_r^t)$,所以攻击者无法通过更新规则推测出上一轮或下一轮组共享密钥。因此,标签组具有前/后向安全性。

(4)抗假冒攻击

信息在信道中均以加密的形式传送,且密钥只有合法的3个结构已知,并且云与标签组实现了相互认证,云也在协议运行之前认证了阅读器的合法性,因此攻击者不能假冒任何一个部分解密消息。

(5)抗多轮 DOS 攻击

云端会存储新、旧两个共享密钥的加密形式,若攻击者阻断了阅读器发送给云端的密钥更新消息,导致云端或标签端无法更新密钥,则会暂时使用旧密钥进行认证,不会使协议在当前阶段运行失败,并且在之后的认证过程中使云端和标签组重新更新并同步密钥,以防攻击者多次发起 DOS 攻击后,认证双方始终无法更新和同步密钥,因此标签可以抗多轮 DOS 攻击。

(6)抗去同步攻击

本协议采用状态机机制,在受到 DOS 攻击之后,第二轮认证时会使用旧密钥,但在第二轮认证结束之前会在阅读器端更新旧密钥,然后将加密形式发送给云和标签组,再通过简单的赋值运算,使得云和标签端同步更新为新密钥,以避免在多次受到 DOS 攻击后,反复使用旧密钥而导致跟踪攻击,失去前\后向安全性,因此本协议可以抗去同步攻击。

4.2 协议的形式化证明

BAN 逻辑是一种基于信念的模态逻辑(Modal logic)[19],是目前使用得最为广泛的安全协议分析方法,它是关于主体信仰以及用于从已有信仰推出新的信仰的推理规则的逻辑。这种逻辑通过对认证协议的运行进行形式化分析,来阐述网络系统中认证协议的安全问题。BAN 逻辑是分析安全协议的一个里程碑,现今大多数协议都采用这种逻辑手段进行分析。

4.2.1 BAN 逻辑的基本术语

BAN 逻辑的基本公式的含义如表 2 所列。

表 2 BAN 逻辑的基本公式的含义

Table 2 Interpretation of basic formulas of BAN logic

基本公式	含义
$P\mid\equiv X$	P 相信 X
$P\lhd X$	P 收到过 X
$P\mid\sim X$	P 发送过 X
$P\mid\Rightarrow X$	P 对 X 具有管辖权
$\sharp(X)$	X 是新鲜的
$P\overset{K}{\leftrightarrow}Q$	P 和 Q 共享密钥 K
$\{X\}_K$	用密钥 K 加密 X 后的密文

4.2.2 BAN 逻辑的逻辑推理规则

本节对本协议需要用到的 BAN 逻辑规则进行简单介绍。

R_1:消息含义规则 $\dfrac{(P\mid\equiv Q\overset{K}{\leftrightarrow}P, P\lhd\{X\}_K)}{P\mid\equiv Q\mid\sim X}$

如果 P 相信 K 为 P 与 Q 之间的共享密钥,且 P 接收过用 K 加密的消息,则 P 相信 Q 发送过该消息。

R_2:管辖规则 $\dfrac{P\mid\equiv Q\mid\Rightarrow X, P\mid\equiv Q\mid\equiv X}{P\mid\equiv X}$

若 P 相信 Q 对 X 有管辖权,且 P 相信 Q,Q 相信 X,则 P 相信 X。

R_3:信仰规则 $\dfrac{(P\mid\equiv X, P\mid\equiv Y)}{P\mid\equiv(X,Y)}$

若 P 相信 X,且 P 相信 Y,则 P 相信由 X 和 Y 组成的消息(X,Y)。

R_4:新鲜性规则 $\dfrac{P\mid\equiv\sharp(X)}{P\mid\equiv\sharp(X,Y)}$

若 P 相信 X 是新鲜的,则 P 也相信包含 X 的消息(X,Y)是新鲜的。

R_5:新鲜值验证规则 $\dfrac{P\mid\equiv\sharp(X), P\mid\equiv Q\mid\sim X}{P\mid\equiv Q\mid\equiv X}$

若 P 相信 X 是新鲜的,且 P 相信 Q 发送过 X,则 P 相信 Q 相信 X。

R_6:密钥与秘密共享规则 $\dfrac{P\mid\equiv Q\mid\equiv R\overset{K}{\leftrightarrow}R'}{P\mid\equiv Q\mid\equiv R'\overset{K}{\leftrightarrow}R}$,

$\dfrac{P\mid\equiv Q\mid\equiv R\overset{X}{=\!=\!=}R'}{P\mid\equiv Q\mid\equiv R'\overset{X}{=\!=\!=}R}$

若 R 与 R' 之间存在密钥或者秘密,则 R' 与 R 之间必然存在相同的密钥或者秘密。

R_7:拆分消息规则 $\dfrac{(P\mid\equiv\{X,Y,Z\})}{(P\mid\equiv X, P\mid\equiv Y, P\mid\equiv Z)}$

若 P 曾收到过包含 X,Y,Z 的消息,则认为 P 收到过 X,也收到过 Y,也收到过 Z。

4.2.3 协议分析

利用 BAN 逻辑对本文提出的基于云的 RFID 群组标签认证协议进行形式化分析。

(1)协议描述:

1)$R\rightarrow\{T_i\}_n: N_r$

2)$\{T_i\}_n\rightarrow R:\{H(N_r \parallel id_{Ti}) \parallel id_{Ti}\}_{Kg}, H(Kg), H(G_{id})$

3)$R\rightarrow C: H(Kg), N_r, H(G_{id}), \{id_r\}_K$

4)$C\rightarrow R:\{X\}_K, N_c, \{Kg^{new}\}_K, \{Kg^{old}\}_K$

5)$R\rightarrow C:\{Kg^{new'}\}_K, \{id_{Ti}\}_K^t, N_r^t$

6)$C\rightarrow R: N_c$

7)$R\rightarrow\{T_i\}_n:\{H(X \parallel N_c) \parallel H(id_{Ti} \parallel N_r^t) \parallel Kg^{new'}\}_X, N_r^t, N_c$

8)$\{T_i\}_n\rightarrow R:\{Kg \parallel id_{Ti}\}_{Kg}$

9)$R\rightarrow C:\{Kg^{new''}\}_K, H(Kg^{new''}), N_r^t$

10)$C\rightarrow R: ACK$

11)$R\rightarrow\{T_i\}_n: H(Kg^{new''} \parallel N_c \parallel N_r^t)$

(2)协议理想化

1)$M_1: R\lhd\{H(N_r \parallel id_{Ti}) \parallel id_{Ti}\}_{Kg}, H(Kg), H(G_{id})$

2）$M_2:C\lhd H(Kg),N_r,H(G_{id}),\{id_r\}_K$

3）$M_3:R\lhd \{X\}_K,N_c,\{Kg^{\text{new}}\}_K,\{Kg^{\text{old}}\}_K$

4）$M_4:C\lhd \{Kg^{\text{new}'}\}_K,\{id_{Ti}\}_K^t,N_r^t$

5）$M_5:\{T_i\}_n\lhd \{H(X\parallel N_c)\parallel H(id_{Ti}\parallel N_r^t)\parallel Kg^{\text{new}'}\}_X,N_r^t,N_c$

6）$M_6:R\lhd \{Kg\parallel id_{Ti}\}_{Kg}$

7）$M_7:C\lhd :\{Kg^{\text{new}''}\}_K,H(Kg^{\text{new}''}),N_r^t$

8）$M_8:\{T_i\}_n\lhd H(Kg^{\text{new}''}\parallel N_c\parallel N_r^t)$

（3）初始化假设

$H_1:R|\equiv \#(N_r)$

$H_2:R|\equiv \#(N_r^t)$

$H_3:C|\equiv \#(N_c)$

$H_4:R|\equiv R\overset{N_r}{\longleftrightarrow}\{T_i\}_n$

$H_5:R|\equiv R\overset{N_r}{\longrightarrow}C$

$H_6:R|\equiv C\overset{N_c}{\longrightarrow}R$

$H_7:\{T_i\}_n|\equiv C\overset{H(Kg)}{\longleftrightarrow}\{T_i\}_n$

$H_8:R|\equiv C\overset{\{id_r\}_K}{\longleftrightarrow}R$

$H_9:C|\equiv C\overset{H(Kg)}{\longleftrightarrow}\{T_i\}_n$

$H_{10}:C|\equiv C\overset{\{id_r\}_K}{\longleftrightarrow}R$

（4）协议目标

$A_1:C|\equiv\{T_i\}_n|\equiv C\overset{H(K_g)}{\longleftrightarrow}\{T_i\}_n$

$A_2:C|\equiv R|\sim \#(\{id_r\}_K)$

$A_3:C|\equiv R|\equiv\{id_r\}_K$

$A_4:\{T_i\}_n|\equiv C|\sim \#(N_c)$

$A_5:\{T_i\}_n|\equiv C|\equiv N_c$

（5）安全性证明

1）证：$A_1:C|\equiv\{T_i\}_n|\equiv C\overset{H(K_g)}{\longleftrightarrow}\{T_i\}_n$

①由消息 M_1，M_2 及假设 H_9，根据消息含义规则 $\dfrac{(P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_K)}{P|\equiv Q|\sim X}$ 得 $C|\equiv\{T_i\}_n|\sim\{H(Kg),H(G_{id}),N_r\}$。

②由假设 H_1 和新鲜性规则 $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$，有 $C|\equiv\#\{H(Kg),H(G_{id}),N_r\}$。

③由新鲜值验证规则 $\dfrac{P|\equiv\#(X),P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$，有 $C|\equiv\{T_i\}_n|\equiv\{H(Kg),H(G_{id}),N_r\}$。

④由信念规则 $\dfrac{P|\equiv Q|\equiv(X,Y)}{P|\equiv Q|\equiv X}$ 得 $C|\equiv\{T_i\}_n|\equiv C\overset{H(K_g)}{\longleftrightarrow}\{T_i\}_n$。

得证。

2）证 $A_2:C|\equiv R|\sim\#(\{id_r\}_K)$

①由消息 M_2 及消息含义规则得 $C|\equiv R|\sim\{\{id_r\}_K,N_r\}$。

②由于假设 H_1 及新鲜性规则得 $R|\equiv\#\{\{id_r\}_K,N_r\}$。

③由①，②得 $C|\equiv R|\sim\#(\{id_r\}_K)$。

得证。

3）证 $A_3:C|\equiv R|\equiv\{id_r\}_K$

①由 M_2 知 $C\lhd\{H(Kg),N_r,H(G_{id}),\{id_r\}_K\}$，由消息拆分规则可知 $C\lhd\{id_r\}_K$。

②由假设 H_{10} 及消息含义规则得 $C|\equiv R|\sim\{id_r\}_k$。

③由证明 A_2 及新鲜值验证规则可得 $C|\equiv R|\equiv\{id_r\}_K$。

得证。

4）证 $A_4:\{T_i\}_n|\equiv C|\sim\#(N_c)$

①由消息 M_5 及假设 H_2，根据新鲜性规则得 $\{T_i\}_n|\equiv R|\sim\#\{\{H(X\parallel N_c)\}_{X=K_g},N_r^t\}$，再由消息含义规则得 $\{T_i\}_n|\equiv R|\sim\#\{H(X\parallel N_c)\}_{X=K_g}$。

②由假设 H_3，H_6 得 $R|\equiv C|\sim\#\{N_c\}$。

③由①，②及消息管辖规则得 $\{T_i\}_n|\equiv C|\sim\#(N_c)$。

得证。

5）证 $A_5:\{T_i\}_n|\equiv C|\equiv N_c$

①由消息 M_5 及证明 A_4 得 $\{T_i\}_n|\equiv C|\sim\#(N_c)$。

②由于假设 H_3 及 $\{T_i\}_n|\equiv\#(N_c)$，由新鲜值验证规则得 $\{T_i\}_n|\equiv C|\equiv N_c$。

得证。

4.3　协议的安全性及性能对比分析

本文协议与其他协议的安全性对比如表 3 所列。

表 3　安全性对比

Table 3　Comparison of security

性能指标	跟踪攻击	假冒攻击	前/后向安全	重放攻击	去同步攻击	DOS 攻击	双向认证
Wei[13]	No	Yes	Yes	Yes	Yes	No	Yes
Tong[14]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Zheng[15]	Yes	Yes	No	Yes	No	No	Yes
Kardas[16]	Yes	No	Yes	Yes	Yes	No	No
本文协议	Yes	Yes	Yes	Yes	Yes	Yes	Yes

注：Yes 表示具备此属性或可以抵抗此攻击，No 表示不具备此属性或不能抵抗此攻击

表 3 将本文提出的协议与其他几个具有代表性的基于云的协议进行了性能对比，进一步说明了本文提出的协议相较于其他协议具有更高的安全性。

本文协议与其他协议的计算量和实现复杂度的对比如表 4 所列。

表 4　计算量与实现复杂度对比

Table 4　Comparison of calculation and implement complexity

性能指标	标签计算量	标签通信量	标签存储量	云搜索效率	硬件实现成本
Wei[13]	$4h+1r+1xor$	$3l$	$3S$	L	H
Tong[14]	$3h+1r+1xor$	$3l$	$2S$	H	M
Zheng[15]	$1h+1r$	$4l$	$3S$	M	L
Kardas[16]	$3h+1r+2E$	$3l$	$5S$	H	M
本文协议	$5h$	$3l$	$3S$	H	L

注：h 表示计算一次哈希函数的计算量，r 表示产生一个随机数的计算量，xor 表示一次异或运算的计算量，S 表示标签端存储的数据长度，l 表示标签端哈希值的输出长度，E 表示椭圆曲线计算量，L 表示指标程度低，M 表示指标程度中等，H 表示指标程度高

5　协议中哈希函数的分析与硬件实现结构

标签所要承担的主要算法是哈希函数、随机数的产生以

及其他的一些基本运算(如异或),而随机数的产生可以基于哈希函数设计,因此哈希函数决定了本方案的硬件消耗。本方案使用的轻量级哈希函数是在 2011 年的 CRYPTO 上,由南洋理工大学 Guo 等提出的 Photon 哈希函数[12]。本文根据安全性、输出比特长度以及标签能承受的轻量级要求,选用 Photon-160/36/36 函数,下面主要介绍 Photon-160/36/36 函数的算法及硬件实现。

5.1 主拓展算法

主拓展算法是一个扩展的 Sponge 结构,其内部状态 S 为 196-bits,包括了 160-bits 的存储量和 36-bits 的比特率(即 $t=c+r$)。在初始化内部状态 $S_0=IV=\{0\}^{136}\parallel 40\parallel 36\parallel 36$ 之后,将待哈希运算的消息适当地分裂为 12 个 36-bits 的消息块。在消息的分裂过程中,可以根据需要给最后一个消息块填充一个'1'和若干个'0'来完成 12 个消息块的分裂。然后进行简单的吸收和压缩,最后连续输出 5 个 z(每一个 z 都为 36-bits),并将这些 z 串联起来就得到了最终的输出哈希值,其中最后一个输出消息块的大小为 16 bits。

Photon-160/36/36 函数的主拓展结构如图 3 所示。

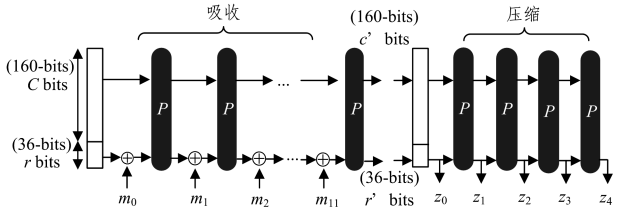

图 3 Photon-160/36/36 函数的主拓展结构

Fig. 3 Main extension structure of Photon-160/36/36 function

5.2 内部置换算法

该函数的内部置换算法主要是由一个类似 AES 的置换矩阵 P_t 组成。对 Photon-160/36/36 函数来说,P_t 是一个 7 维的矩阵 P_{196},矩阵的每个元素的大小为 4 bits,需要注意的是,内部状态 S 的每个元素也是 4 bits。内部置换算法主要包括 4 个模块:AC,SC,ShR,MCS。Photon-160/36/36 函数 12 轮压缩的轮常数为 $RC(v)=[1,3,7,14,13,11,6,12,9,2,5,10]$。

AC:在第 v 次压缩(v 的取值范围为 1～12)时,采用该轮的轮常数异或内部状态 S 的第一列 $S[i,0]$,然后再用内部常数 $IC_d(\cdot)=[0,1,2,5,3,6,4]$分别异或该列的每个元素,即 $S'[i,0]=S[i,0]\oplus RC(v)\oplus IC_d(i)$,$0\leqslant i\leqslant d\leqslant 6$,$1\leqslant v\leqslant 7$。

SC:将 4 bits 的 S 盒 $\mathrm{SBOX_{PRE}}$ 应用于内部状态的每一个单元格 $S'[i,0]=SBOX(S[i,j])$,$0\leqslant i<d$,$0\leqslant j<d$。4 bits 的 S 盒 $\mathrm{SBOX_{PRE}}$ 为[0xc,0x5,0x6,0xb,0x9,0x0,0xa,0xd,0x3,0xe,0xf,0x8,0x4,0x7,0x1,0x2]。

ShR:这一层主要实现的功能是行的循环左移,即将内部状态 S 的第 i 行的每一个单元格向左循环移动 i 个位置,i 从第 0 行开始,直到所有行都左移完毕。$S'[i,j]=S[i,(i+j)\bmod d]$,$0\leqslant i<d$,$0\leqslant j<d$。

MCS:这一个混合层实现的功能是内部状态 S 的列混合,对于第 j 列的输入向量,计算$(S'[0,j],\cdots,S'[6,j])^{\mathrm{T}}=A_{196}^{7}*(S[0,j],\cdots,S[6,j])^{\mathrm{T}}$,$0\leqslant j\leqslant 6$。矩阵 A_{196}^{7} 为:

$$(A_{196})^7=\begin{bmatrix}0&1&0&0&0&0&0\\0&0&1&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&1&0&0\\0&0&0&0&0&1&0\\0&0&0&0&0&0&1\\1&4&6&1&1&6&4\end{bmatrix}^7$$

$$=\begin{bmatrix}1&4&6&1&1&6&4\\4&2&15&2&5&10&5\\5&3&15&10&7&8&13\\13&4&11&2&7&15&9\\9&15&7&2&11&4&13\\13&8&7&10&15&3&5\\5&10&5&2&15&2&4\end{bmatrix}$$

5.3 硬件实现结构及性能分析

Photon-160/36/36 的串行硬件结构如图 4 所示。其中 IO 模块负责初始化内部状态以及吸收消息块,然后将状态模块的输出转发给 AC 模块;AC 模块负责用内部状态 S 的第一列异或轮常数和内部常数;Controller 模块用 FSM(有限状态机)产生所需的控制信号,包括轮常数 RC 以及内部常数 IC;SC 模块由一个 4 bits 的 S 盒组成,它用来实现 5.2 节所示的 SC 模块的运算功能;State 模块包含一个 7 * 7 的触发器,每一行构成一个移位寄存器,并且构成一个反馈(例如,列 0 作为相同行或者下一行的输入),从而节约硬件成本;MCS 模块实现列混合,即在一个时钟周期中计算 A_{196}^{7} 的最后一行,将结果反馈给 State 模块,并同时向上移动,在整个列都运算过后,整个状态数组向左旋转一定的位置,继续执行 MCS 模块运算,在 7 * 8 个时钟周期过后,完成列混合。

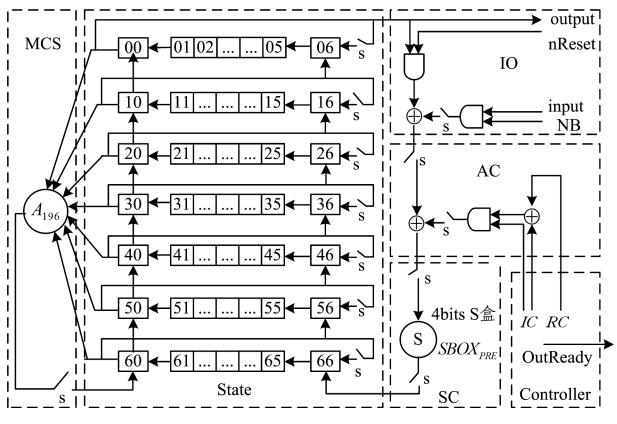

图 4 Photon-160/36/36 的串行硬件结构

Fig. 4 Serial hardware structure of Photon-160/36/36

Photon-160/36/36 函数可以输出长度为 160 bits 的哈希值,它不仅具有 80 bits 的安全性,而且所需要的逻辑门总数也不足 1400 GE,其运算速率达到了 2.7 kbps。相比于其他同等安全性的 Hash 函数,Photon 满足了我们所需要的轻量级需求。

结束语　本文提出了一种基于云的轻量级 RFID 群组认证协议，该协议不仅实现了云数据库和群组标签的双向认证，而且提高了存储的数据和用户的安全隐私保护能力，降低了协议的运行成本，保障了安全性和可行性。文中还将该协议与已有的几个具有代表性的协议进行了性能对比，结果表明本文提出的协议具有更高的安全性和实用性，更重要的是，本文提出的协议还具有在双向认证过程中剔除无效标签和假冒标签，以及抵抗多轮 DOS 攻击的优势。文中还介绍了本协议所用的 Hash 函数 Photon，并且给出了其硬件实现结构。但本文提出的协议仍然还有一些地方需要改进，如降低协议复杂度、硬件仿真等，我们将在后续的研究工作中继续优化。

参 考 文 献

[1] ZHANG D Q, QIAN Y M, WAN J F, et al. An Efficient RFID Search Protocol Based on Clouds[J]. Mobile Networks & Applications, 2015, 20(3): 356-362.

[2] WEIS S. Security and Privacy in Radio-frequency Identification Devices[D]. Boston: Massachusetts Institute of Technology, 2003.

[3] TSUDIK G. YA-TRAP: yet another trivial RFID authentication protocol[C]// IEEE International Conference on Pervasive Computing and Communications Workshops. Italy, IEEE Computer Society, 2006: 640-643.

[4] RHEE K, JIN K, KIM S, et al. Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment [J]. Kips Transactions Partc, 2005, 3450(3): 309-316.

[5] YAN F, LIU B W, HUO L Y, et al. Research and Design of a Security Framework for RFID System[C]// International Forum on Information Technology and Applications. Beijing, IEEE Computer Society, 2010: 443-445.

[6] XIAO H, ALSHEHRI A, CHRISTIANSON B. A Cloud-Based RFID Authentication Protocol with Insecure Communication Channels[C]// IEEE Trustcom/BigDatase/ISPA. IEEE, 2017: 332-339.

[7] DA L M. Research on Information Security Technology of the Internet of Things at the Perceived Layers of RFID and WSN [J]. Journal of Nanjing Institute of Industry Technology, 2014 (1): 8-11. (in Chinese)
笪林梅. 物联网感知层 RFID 和 WSN 信息安全技术研究[J]. 南京：工业技术学院学报，2014(1)：8-11.

[8] LEE C F, CHIEN H Y, LAIH C S. Server-less RFID authentication and searching protocol with enhanced security[J]. International Journal of Communication Systems, 2012, 25(3): 376-385.

[9] HOQUE M E, RAHMAN F, AHAMED S I, et al. Enhancing Privacy and Security of RFID System with Serverless Authentication and Search Protocols in Pervasive Environments[J]. Wireless Personal Communications, 2010, 55(1): 65-79.

[10] ZHAN Y, SUN Y. Cloud Storage Management Technology [C]// International Conference on Information and Computing Science. 2009: 309-311.

[11] BELLARE M, RAN C, KRAWCZYK H. H·: Keying Hash Functions for Message Authentication[M]// Advances in Cryptology——CRYPTO'96. Springer Berlin Heidelberg, 1991.

[12] GUO J, PEYRIN T, POSCHMANN A. The PHOTON Family of Lightweight Hash Functions[OL]. http://www.reshaem.net/tasks/task_152522.pdf.

[13] WEI X, LEI X, CHEN Z. Cloud-based RFID Authentication [C]// IEEE International Conference on RFID. 2013: 168-175.

[14] DONG Q K, TONG J Q, CHEN Y. Cloud-Based RFID Mutual Authentication Protocol without Leaking Location Privacy to the Cloud[C]// International Journal of Distributed Sensor Networks. 2015: 1-9.

[15] ZHENG J B. RFID mutual authentication protocol based on Cloud Server [J]. Journal of Mudanjiang University, 2016, 25(7): 152-154. (in China)
郑金彬. 基于云服务器的 RFID 双向认证协议[J]. 牡丹江大学学报，2016，25(7)：152-154.

[16] KARDAS S, CELIK S, BINGOL M A, et al. A New Security and Privacy Framework for RFID in Cloud Computing[C]// IEEE International Conference on Cloud Computing Technology and Science. Bristol, UK, IEEE, 2013: 171-176.

[17] GUO Y M, LI S D, CHEN Z H, et al. A lightweight privacy-preserving grouping proof protocol for RFID systems[J]. Tien Tzu Hsueh Pao/acta Electronica Sinica, 2015, 43(2): 289-292.

[18] ZHANG R, ZHU L, XU C, et al. An Efficient and Secure RFID Batch Authentication Protocol with Group Tags Ownership Transfer[C]// Conference on Collaboration and Internet Computing. Hangzhou, China, IEEE, 2015: 168-175.

[19] BURROWS M, ABADI M, NEEDHAM R M. A logic of authentication[J]. Proceedings of the Royal Society A Mathematical Physical & Engineering Sciences, 1989, 426(1871): 1-13.