可证明安全的射频识别双向认证协议

何　烜，王红军，袁　泉
（国防科技大学电子对抗学院，合肥，230037）

摘要　由于射频识别系统中读写器和标签是在不安全的无线信道中进行通信，而且随着移动读写终端的出现，使得读写器和服务器通信也不安全，容易受到假冒攻击、窃听攻击、中间人攻击等安全威胁，针对此问题提出了基于中国剩余定理的射频识别双向认证协议。该协议利用对称加密、模运算等方式提高信息传输的安全性，引入时间戳来抵抗中间人攻击，并利用中国剩余定理对各方进行认证，最后采用随机更新密钥的方式进行密钥更新，并通过形式化证明的方法和常规攻击分析的方式来验证协议安全性。将该协议与其他协议进行安全性、计算量和存储量的比较，结果表明：文中协议安全性高、计算量小且存储量适中，在射频识别领域安全方面具有一定的应用价值。

关键词　射频识别；中国剩余定理；时间戳；BAN 逻辑；双向认证
DOI　10.3969/j.issn.1009-3516.2018.05.008
中图分类号　TP309　　**文献标志码**　A　　**文章编号**　1009-3516(2018)05-0041-06

Provable Secure Two-Way Authentication Protocol for Radio Frequency Identification

HE Xuan，WANG Hongjun，YUAN Quan
(School of Electronic Countermeasures，National University of Defense Technology，Hefei 230037，China)

Abstract：Aimed at the problems that the reader communication with tags is carried out in insecure wireless channel in the radio frequency identification system，and with the emergence of mobile reader terminals，this makes the communication between the reader and the server unsafe，vulnerable to impersonation attack，eavesdropping attack，middleman attack and other security threats，a two-way authentication protocol for radio frequency identification based on Chinese remainder theorem is proposed. The symmetric encryption and modular operation ways are used to improve the security of information transmission，and the timestamp is adopted to resist the middleman attack in the protocol，and the Chinese remainder theorem is utilized for certificating all sides. Finally，random key update method is used in the key-updating. The protocol security is verified by formal proof method and routine attack analysis. The protocol of this paper is compared with other protocols in terms of security，calculation and storage. The results show that the protocol is high in security，less in calculation and moderate in storage，and has certain application value in the security field of radio frequency identification.

Key words：radio frequency identification；Chinese remainder theorem；timestamp；BAN logic；two-way authentication

收稿日期：2017-08-31
基金项目：国家自然科学基金(61273302)
作者简介：何　烜(1993—)，男，江苏兴化人，硕士生，主要从事物联网安全、轻量级安全协议研究。E-mail：hxdsgyx56@163.com

引用格式：何烜，王红军，袁泉. 可证明安全的射频识别双向认证协议[J]. 空军工程大学学报(自然科学版)，2018，19(5)：41-46. HE Xuan，WANG Hongjun，YUAN Quan. Provable Secure Two-Way Authentication Protocol for Radio Frequency Identification[J]. Journal of Air Force Engineering University (Natural Science Edition)，2018，19(5)：41-46.

作为物联网感知层的核心技术之一,射频识别(Radio Frequency Identification, RFID)技术因其具有自动化程度高、读取速度快、可重复使用等优势,被广泛应用于智能仓库、门禁系统、工业控制以及航空航天等领域[1]211-243。

然而射频识别系统目前仍然存在一定的安全隐患问题。该系统主要由读写器、标签和后端服务器构成[2-3],由于读写器与标签的信息传递是通过无线方式,容易受到第三方的攻击,而且读写器的识别距离远,标签的响应距离近,这种非对称通信方式也增加了系统的安全隐患[4],因此需要设计出可靠的安全认证协议来解决上述问题。文献[5]是基于 Hash 函数来构建安全协议,然而文献[6]指出 Hash 函数的硬件电路需要 8 kB 的存储开销,不适合存储量较小的标签。文献[7]提出利用数字签名协议来解决读写器与标签的安全问题。在数字签名协议中,对于知道公钥的任何一方都可以读取标签的 ID[8],而且无法达到双向认证的要求。文献[9]提出标签所有权转移协议,即新旧所有者不能利用已有信息对另一方进行攻击。该协议存在新所有者的隐私保护问题[10]。文献[11]提出利用 SASI 轻量级协议族来解决读写器与标签的通信安全问题,然而其存在异步攻击和中间人攻击问题。以上文献都是基于"服务器与读写器通信安全、读写器与标签通信不安全"这一模型而设计的安全协议。随着移动智能终端技术的成熟,许多手持无线读写终端出现在实际生活中,那么就需要考虑读写器与服务器传输的安全性。文献[12]提出利用椭圆曲线的方法来解决移动射频识别环境的安全问题,然而该方案不能解决读写器的隐私问题。文献[13]提出利用 Edwards 曲线的方法来设计射频识别认证协议,本质上还是结合 Hash 函数和伪随机数来构建协议,运算量较大、过程复杂,而且不能抵抗中间人转发攻击。

1 基础知识

1.1 中国剩余定理

设 $b_1,b_2,\cdots,b_m$ 是两两互素的正整数,记 $B=\prod_{i=1}^{m}b_i$,则同余方程组:

$$\begin{cases} k\equiv a_1 (\bmod\ b_1) \\ k\equiv a_2 (\bmod\ b_2) \\ \vdots \\ k\equiv a_m (\bmod\ b_m) \end{cases} \tag{1}$$

在模 B 同余的意义下有唯一解:

$$k\equiv\sum_{i=1}^{m}b^iB_ig_i (\bmod\ B) \tag{2}$$

式中:

$$B_i=\frac{B}{b^i},1\leqslant i\leqslant m \tag{3}$$

$$g_i\equiv b_i^{-1} (\bmod\ b_i),1\leqslant i\leqslant m \tag{4}$$

从中国剩余定理可知:k 具有唯一性[14]。在协议设计中,将 k 作为密钥。为保证协议安全性,并尽可能的减少信息的存储和传输,本文可采用式(1)同余方程组中的 2 对信息,不完全传输其中的部分信息,则可对服务器、读写器和标签三方进行认证。协议安全性在于保留其中的部分信息,保留的信息只有合法的服务器、读写器和标签知道。

1.2 时间戳机制

为了保证信息没有经过第三方处理,服务器、读写器和标签在信息传输时增加时间戳[15]信息。如果有第三方进行截取或者转发两者之间的信息,由于消耗的时间远远超过信息的传输时间,则可以通过时间戳来进行分析和辨别。以读写器和标签通信为例,假设标签传输给读写器信息时的时间戳为 P_1,信息传输的时间 Δt,考虑到有时间偏差 Δs,则读写器记录接收时间,分析时间戳,判断接收时间是否在时间窗口$[P_1+\Delta t-\Delta s,P_1+\Delta t+\Delta s]$内,如果在,则认为标签信息没有经过任何攻击,否则认为标签信息为非法信息。其中时间 Δt 和偏差 Δs 的取值可经过多次实验确定。

2 双向认证协议设计

协议可以分为如下 3 个阶段:①初始化阶段。标签存储 a_1、b_1、ID 和密钥 k、G_1、G_2;读写器存储 a_1、b_1、a_2 和密钥 k、G_1、G_2;服务器存储 a_1、b_1、a_2、b_2、f、ID 和密钥 k、G_1、G_2。其中 a_1 和 b_1、a_2 和 b_2、G_1 和 G_2 对每个标签而言是独有且唯一的。k 是通过中国剩余定理生成的密钥,G_1 和 G_2 为对称密钥体制中的加密密钥,f 表示密钥的更新方式,f 代表的含义是三方约定好的。为防止异步攻击,服务器和读写器在更新密钥后,同时保留未更新的密钥。为抵抗中间人攻击,需要引入时间戳 P。②互认证阶段:因为本文假设的安全模型是服务器和读写器信息传输不安全,读写器与标签信息传输也不安全。则服务器要对读写器和标签进行认证,读写器和标签要对服务器进行认证,读写器和标签也要进行相互认证,才能保证三方信息的安全传输。③密钥更新阶段:服务器、读写器和标签需要进行密钥更新以保证下次信息的传输安全。对协议进行描述之前,先对协议中涉及的符号进行说明,见表 1。

表 1　符号说明

Tab. 1　Symbol description

符号	含义
a_1，b_1，a_2，b_2	中国剩余定理运算的信息
k	由中国剩余定理唯一产生
G_1，G_2	加密密钥
P	时间戳
ID	标签的唯一序列号
$\vee$	按位或运算
$\wedge$	按位与运算
$\|\|$	连接运算
$\oplus$	异或运算
$+$	模 2^m 加

协议流程图见图 1。

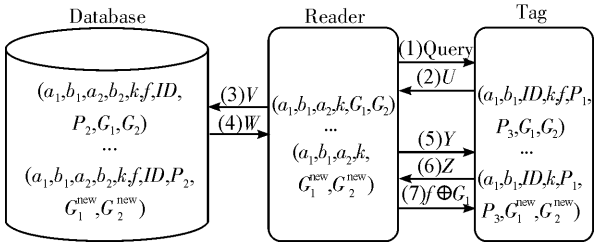

图 1　协议流程图

Fig. 1　Flow chart of the protocol

具体过程如下：

1）读写器认证标签。读写器向标签发送 Query 请求，标签接收到 Query 请求后，通过计算 $U=(a_1 \| P_1)\oplus G_1$，并将 U 发送给读写器。读写器用 G_1 进行解密，验证时间戳 P_1，如果合法则得出 a_1，然后比较是否和自己存储的某对信息中的 a_1 相同，如果相同，则读写器通过对标签的认证，读写器将此对信息中的 a_2 取出，计算 V：

$$V=((a_1\oplus a_2)+a_1)\oplus G_2 \tag{5}$$

将 V 发送给服务器；如果不相同，读写器则认为标签非法，不再对该标签认证。

2）服务器认证读写器和标签。服务器接收到 V，利用 G_2 解密得到 a_1 和 a_2。查询自身数据库，比较是否与自己存储的某对信息中的 a_1 和 a_2 相同。如果相同，则服务器通过对读写器和标签的认证，并计算 W：

$$W=(ID \| b_2 \| P_2 \| f)\oplus G \tag{6}$$

然后将 W 发送给读写器；如果不相同，则服务器认为读写器和标签非法。

3）读写器认证服务器。读写器接收到 W，用 G_1 进行解密，得到 ID、b_2、时间戳 P_2 和 f。首先判断时间戳 P_2 是否合法，如果合法，再将 b_2 和自身对应的信息进行计算，判断计算出的 k_1 是否等于存储的 k，如果相等，则读写器通过对服务器的认证，并且认为 ID 为真实 ID；然后读写器计算 Y：

$$Y=(G_1\wedge(a_2 \| b_2))\oplus G_2 \tag{7}$$

并将 Y 发送给标签。如果有一步没有通过，则读写器认为服务器非法。

4）标签认证服务器和读写器。标签接收到 Y 后，用 G_2 进行解密，计算得出 G_1、a_1 和 b_2。首先判断 G_1 是否和自身存储的 G_1 相同，如果相同，则标签通过对读写器的认证；如果不相同，则标签认定读写器非法。然后将 a_2 和 b_2 与自身 a_1 和 b_1 进行运算，得到密钥 k_2，判断密钥 k_2 是否与自身存储的密钥 k 相等，如果相等，则标签通过对服务器的认证，同时计算 Z：

$$A=(ID\oplus a_1)\oplus G_1 \| P_3 \tag{8}$$

并将 Z 发送给读写器；如果不相等，则标签认为服务器非法。

5）读写器识别标签 ID。读写器接收到 Z，首先判断时间戳 P_3 是否合法，如果合法，则用 G_1 进行解密，计算出标签的 ID，判断其和服务器发送过来的 ID 是否一致，如果一致，则对标签成功识别。

6）密钥更新。读写器对标签认证通过后，进行密钥更新，并发送 $f\oplus G_1$ 指令给标签。标签接收到 $f\oplus G_1$ 指令后，按照信息 f 进行更新。在密钥更新阶段，服务器、读写器和标签均按照信息 f 进行密钥更新。信息 f 代表的意义是三方约定好的，例如 $f=0$ 表示不更新，还按照原来的密钥来进行信息传输。$f=1$ 表示密钥 G_1 和 G_2 互换；$f=2$ 表示密钥 G_1 是 G_1 和 G_2 的异或，G_2 保持不变等。以 $f=2$ 为例，密钥更新公式为：

$$\begin{cases} G_1^{\text{new}}=G_1\oplus G_2 \\ G_2^{\text{new}}=g_2 \end{cases} \tag{9}$$

此种密钥更新方式可以有多种变化，且服务器发送的信息 f 具有随机性，没有规律可循，则可以有效抵抗攻击者的攻击。

协议采用先进行双向认证、再识别 ID 的方式，最终达到读写器识别标签 ID 的目的。在服务器对读写器和标签的认证过程中，利用了标签 a_1 和读写器 a_2 的唯一性，其中 a_2 与标签 a_1 对应。协议通过对称加密、模运算、时间戳等方式来保证 a_2 和 a_1 难以被破解。在标签对读写器和服务器的认证过程中，利用了密钥 k 的唯一性。由于三方没有传输 b_1 信息，所以攻击者无法获取密钥 k，从而达到了双向认证的目的。最终读写器验证 ID 的一致性，从而可以对标签进行识别。

3　协议安全性证明与分析

3.1　协议安全性证明

本文主要利用 BAN 逻辑对所提出的协议进行

形式化证明[16]。协议证明分为 3 个步骤：

步骤 1 协议描述：

A1：$R\rightarrow T$：Query

A2：$T\rightarrow R$：$\{U\}_{G_1}$

A3：$R\rightarrow DB$：$\{V\}_{G_2}$

A4：$DB\rightarrow R$：$\{W\}_{G_1}$

A5：$R\rightarrow T$：$\{Y\}_{G_2}$

A6：$T\rightarrow R$：$\{Z\}_{G_1}$

A7：$R\rightarrow T$：$f\oplus a_1$

A1～A7 分别对应图(1)中的(1)～(7)步，以 A1 为例，读写器向标签发送 Query 请求，表明标签接收到 Query 请求，则可以写成：

$$T\lhd\text{Query} \tag{10}$$

A2～A7 都可以写成上述格式。

步骤 2 协议初始化假设：

B1：$R|\equiv R\overset{G_1,G_2}{\longleftrightarrow}T,R|\equiv R\overset{G_1,G_2}{\longleftrightarrow}DB$

B2：$T|\equiv T\overset{G_1,G_2}{\longleftrightarrow}R,T|\equiv T\overset{G_1,G_2}{\longleftrightarrow}DB$

B3：$DB|\equiv DB\overset{G_1,G_2}{\longleftrightarrow}R,DB|\equiv DB\overset{G_1,G_2}{\longleftrightarrow}T$

B4：$R|\equiv\sharp W$

B5：$R|\equiv\sharp Z$

B6：$R|\equiv DB|\Rightarrow W$

B7：$R|\equiv T|\Rightarrow Z$

G_1、G_2 都是 3 方约定好的共同密钥，所以 B1、B2、B3 成立。W 和 Z 信息中包含时间戳，所以当读写器接收 W 和 Z 时，则先验证 W 和 Z 的时间戳，则读写器相信 W 和 Z 是新鲜的，所以 B4 和 B5 成立。W 和 Z 分别由服务器和标签发送给读写器，所以读写器相信服务器对 W 有仲裁权，标签对 Z 有仲裁权，所以 B6 和 B7 成立。

步骤 3 协议证明的目标：

C1：$R|\equiv ID$

因为读写器既接收从服务器发送过来的 ID，同时接收从标签发送过来的 ID，所以要分别证明。

证明读写器相信服务器发送过来的 ID 是真实的：由消息规则 $\dfrac{P|\equiv Q\overset{K}{\longleftrightarrow}P,P\lhd\{X\}_K}{P|\equiv Q|\sim X}$，结合 B1 和 A4 可知：

$$\frac{R|\equiv R\overset{G_1}{\longleftrightarrow}DB,R\lhd\{W\}_G}{R|\equiv DB|\sim W} \tag{11}$$

由随机数验证规则 $\dfrac{P|\equiv\sharp(X),P|\equiv Q|\sim X}{R|\equiv DB|\sim W}$，结合 B4 和式(11)可知：

$$\frac{R|\equiv\sharp(W),R|\equiv DB|\sim W}{R|\equiv DB|\equiv W} \tag{12}$$

由仲裁规则 $\dfrac{P|\equiv Q|\Rightarrow X,P|\equiv Q|\equiv X}{P|\equiv X}$，结合 B6 和式(12)可知：

$$\frac{R|\equiv DB|\Rightarrow W,R|\equiv DB|\equiv W}{R|\equiv W} \tag{13}$$

因为 W 是由 ID、a_2、b_2、P_2 和 f 组成，所以由信息规则 $\dfrac{P|\equiv(X,Y)}{P|\equiv X}$ 可知：

$$\frac{P|\equiv(ID,a_2,b_2,P_2,f)}{R|\equiv ID} \tag{14}$$

所以得证。按照上述方法，同样可以证明读写器相信标签发送的 ID 为真实的。因此可以达到协议目标。

3.2 协议安全性分析

以下就常规攻击技术对本文所设计的协议进行安全性分析。

1) 假冒攻击。本文协议要求信息传输的唯一性。攻击者在无法获取信息的情况下，假冒和伪造的信息无法通过射频识别系统的双向认证，因此本文协议可以抵抗假冒攻击。

2) 窃听攻击。在本文所设计的协议中，信息是通过对称加密、异或、连接等方式处理后传输的，并且 b_1、k 并没有在空间中传输，故攻击者无法通过窃听获取信息，所以本文协议可以抵抗窃听攻击。

3) 重放攻击。在本文协议中，读写器、标签和服务器具有时间戳，只有在时间窗口内的信息才认为是合法信息。而且三方都有密钥更新机制，并且本文协议中的密钥更新方式是随机的，加强了协议的安全性。所以本文协议可以抵抗重放攻击。

4) 异步攻击。本文协议可以抵抗异步攻击，以读写器和标签之间的通信为例分析如下：①假设攻击者攻击协议中的第 5)步，成功篡改了标签的 ID，当读写器收到的信息发现与服务器发送过来的 ID 不符，则读写器不会发送 $f\oplus G_1$，标签没有接收到此信息，则标签不进行密钥更新。然而读写器在初始化过程中保留了未更新前的密钥信息，则当标签以未更新的信息发送时，依然可以获得认证。②假设攻击者攻击协议中的第 6)步，当攻击者篡改 $f\oplus G_1$ 这一指令时，则标签没有接收到正确的信息，无法按照读写器的指令进行密钥更新，只能发送当前密钥加密的信息，然而读写器保留了未更新的密钥，依然可以认证。所以本文协议可以发现攻击者并抵抗异步攻击。

5) 中间人攻击。服务器和读写器、读写器和标签之间在传输标签 ID 信息时，会加上时间戳，只有时间戳合法，才进行下一步的验证。所以本文协议可以抵抗中间人攻击。

4 协议性能比较

在协议性能比较分析中，将本文协议与其它轻

量级安全协议进行安全性、计算量和存储量的比较与分析。主要将本文协议与 Hash-Lock 改进协议、数字签名协议、标签所有权转移协议、PUF-LMAP＋协议和基于 Edwards 曲线协议进行比较，比较结果如表 2 所示。表 3 为本文协议与其它协议在计算量和存储量方面的比较与分析。在分析计算量时，对各个协议的运算量进行统计和计算，其中用 H 表示 Hash 运算，Q 表示签名运算，R 表示伪随机数运算，X 表示异或运算，A 表示位与运算，O 表示或运算，M_1 表示模加运算，M_2 表示模乘运算，C 表示连接运算，S 表示平方运算，T_C 表示时间戳运算。在分析存储量时，由文献[17]知，为方便比较，可将标签索引假名、伪随机数、共享密钥和 ID 长度都设置成 L。

表 2　各协议安全性比较

Tab. 2　Security comparison of different protocol

协议类型	假冒攻击	窃听攻击	重放攻击	异步攻击	中间人攻击	移动 RFID 环境
Hash-Lock[5]	√	×	×	√	×	×
数字签名[7]	√	×	√	√	√	×
所有权转移[9]	√	√	√	√	×	×
PUF-LMAP＋[11]	√	√	√	×	×	×
Edwards 曲线[13]	√	√	√	√	×	√
本文协议	√	√	√	√	√	√

表 3　各协议计算量和存储量比较

Tab. 3　Computation and storage comparison of different protocol

协议类型	计算量			存储量		
	标签	读写器	服务器	标签	读写器	服务器
Hash-Lock[5]	H	—	—	$2L$	—	$3nL$
数字签名[7]	$3X+2M_1+Q+R+C$	$3X+4M_1+R$	—	$5L$	$7nL$	—
所有权转移[9]	$H+3X+4C+S$	$H+X+2C+S$	$2H+X+2C$	$3L$	$3nL$	$4nL$
PUF-LMAP＋[11]	$9X+18M_1+3C+2P$	$5X+10M_1+C$	$4X+8M_1$	$5L$	$4nL$	$5nL$
Edwards 曲线[13]	$H+2M_1+3M_2+C$	$2H+X+3M_1+4M_2$	$3H+X+7M_1+3M_2+C$	$7L$	$9nL$	$12nL$
本文协议	$5X+2C+2T_C$	$7X+M_1+C+A$	$3X+M_1+3C+T_C$	$6L$	$8nL$	$11nL$

由表 2 可知，本文协议由于结合对称加密体制和时间戳等方式，再利用中国剩余定理进行认证，安全性较高，可以抵抗常规攻击，同样也适合移动 RFID 环境。而其它协议对某些攻击并不能抵抗，文献[5]提出的协议没有密钥更新机制，而且密钥和 ID 是以明文形式传送，不能抵抗窃听、重放等攻击，所以安全性差；文献[7]、[9]、[11]提出的协议也没有综合考虑各种安全隐患问题，在协议设计过程中存在一定的缺陷，而且不适用于移动 RFID 环境，所以安全性较差；文献[13]提出的 Edwards 曲线，是对椭圆曲线协议的改进，增强了安全性，然而该协议运算量、存储量较大，不能抵抗中间人攻击。综上分析，本文协议的安全性高于其他协议。

由表 3 可知，从计算量上分析，本文协议只是进行异或、模加、连接等基本运算，运行速度快，没有进行运算量较大的 Hash 运算，Hash 运算至少需要消耗 1 700 个逻辑门电路[18]，而文献[5]、[9]、[13]提出的协议都利用了 Hash 运算，计算量较大。文献[7]中进行了第三方公证签名操作，操作难度高。所以本文协议计算量小，处理实效性强，可在实际情况中实现。从存储量上分析，因为出于安全性考虑，服务器需要存储中国剩余定理中的所有信息，所以服务器的存储量比其它协议高，然而依然比 Edwards 曲线协议低。读写器和标签的存储量和其它协议相当，可在实际读写器电路和标签电路中实现，综上分析，本文协议存储量适合于标签、读写器和服务器的存储空间。

5　结语

本文利用中国剩余定理来构建射频识别双向认证协议，通过对称加密、时间戳和保留部分信息等方式来确保认证的安全性。这样不仅可以保证读写器和标签的安全传输，而且可以保证服务器和读写器的安全传输，即适合移动射频识别认证环境。本文协议得到了 BAN 逻辑的证明，并可以抵抗常规攻击。最后将本文协议与其它协议进行安全性、计算量和存储量的比较，结果表明本文协议安全性高、计算量小、存储量适中。在实际工程应用中，具有参考价值。

参考文献(References):

[1] 宁焕生,王睿. RFID 重大工程与国家物联网[M]. 北京:机械工业出版社,2015.
NING H S, WANG R. RFID Major Projects and the National Internet of Things[M]. Beijing: China Machine Press,2015. (in Chinese)

[2] ARKAN I, VANDEGHEM H V. Evaluating the Performance of a Discrete Manufacturing Process Using RIFD: A Case Study[J]. Robotics and Computer-Integrated Manufacturing, 2013,29(6):502-512.

[3] NGAI E W T, CHAU D C K, POON J K I, et al. Implementing an RFID-Based Manufacturing Process Management System: Lessons Learned and Success Factors[J]. Journal of Engineering and Technology Management, 2012,29(1):112-130.

[4] 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):4581-4589.
ZHOU Y B, FENG D G. Design and Analysis of Cryptographic Protocols for RFID[J]. Chinese Journal of Computers, 2006,29(4):4581-4589. (in Chinese)

[5] YU Y H, ZHANG L. Research on a Provable Security RFID Authentication Protocol Based on Hash Function [J]. The Journal of China Universities of Posts and Telecommunications, 2016, 23(2):31-37.

[6] 贾庆轩,陈鹏,高欣,等. 抗去同步化的轻量级 RFID 双向认证协议[J]. 中南大学学报(自然科学版),2015,46(6):2149-2156.
JIA Q X, CHEN P, GAO X, et al. Lightweight Anti-Desynchronization RFID mutual Authentication Protocol[J]. Journal of Central South University (Science and Technology), 2015,46 (6):2149-2156. (in Chinese)

[7] 刘亚丽,秦小麟,赵向军,等. 基于数字签名的轻量级 RFID 认证协议[J]. 计算机科学,2015,42(2):95-99,107.
LIU Y L, QIN X L, ZHAO X J, et al. Lightweight RFID Authentication Protocol Based on Digital Signature[J]. Computer Science, 2015,42(2):95-99,107. (in Chinese)

[8] 王贵林,卿斯汉. 一个证实数字签名方案的安全缺陷[J]. 软件学报,2004,15(5):752-756.
WANG G L, QING S H. Security Flaws in a Confirmer Signature Scheme[J]. Journal of Software, 2004, 15(5):752-756. (in Chinese)

[9] 陈秀清,曹天杰,翟靖轩. 可证明安全的轻量级 RFID 所有权转移协议[J]. 电子与信息学报,2016,38(8):2091-2098.
CHEN X Q, CAO T J, ZHAI J X. Provable Secure for the Lightweight RFID Ownership Transfer Protocol[J]. Journal of Electronics & Information Technology, 2016,38(8):2091-2098. (in Chinese)

[10] MUNILLA J, BURMESTER M, PEINADO A. Attacks on Ownership Transfer Scheme for Multi-Tag Multi-Owner Passive RFID Environments[J]. Computer Communications, 2016, 88(5):84-88.

[11] 朱峰,白恩健. 新的轻量级 RFID 双向认证协议:PUF-LMAP+[J]. 微型机与应用,2016,35(1):1-4,8.
ZHU F, BAI E J. A New Lightweight Mutual Authentication Protocol for RFID: PUF-LMAP + [J]. Microcomputer & Its Applications, 2016, 35(1): 1-4, 8. (in Chinese)

[12] ZHOU J, ZHOU Y, XIAO F, et al. Mutual Authentication Protocol for Mobile RFID Systems[J]. Journal of Computational Information Systems, 2012, 8(8): 3261-3268.

[13] 杨玉龙,彭长根,周洲,等. 基于 Edwards 曲线的移动 RFID 安全认证协议[J]. 通信学报,2014,35(11):132-138,145.
YANG Y L, PENG C G, ZHOU Z, et al. Edwards Curves Based Security Authentication Protocol for Mobile RFID Systems[J]. Journal on Communications, 2014,35(11):132-138,145. (in Chinese)

[14] 胡向东,魏琴芳,胡蓉. 应用密码学[M]. 3 版. 北京:清华大学出版社,2014.
HU X D, WEI Q F, HU R. Applied Cryptography [M]. 3rd Edition. Beijing: Tsinghua University Press, 2014. (in Chinese)

[15] AIASH M, LOO J. An Integrated Authentication and Authorization Approach for the Network of Information Arthitecture[J]. Journal of Network and Computer Applications, 2015,50(4):73-79.

[16] 张玉清,吴建平,李星. BAN 类逻辑的由来与发展[J]. 清华大学学报(自然科学版),2002,42(1):96-99.
ZHANG Y Q, WU J P, LI X. The Origin and Development of BAN-Like Logic[J]. Journal of Tsinghua University (Science and Technology),2002,42(1):96-99. (in Chinese)

[17] 石乐义,贾聪,宫剑,等. 基于共享秘密的伪随机散列函数 RFID 双向认证协议[J]. 电子与信息学报,2016,38(2):361-366.
SHI L Y, JIA C, GONG J, et al. RFID Mutual Authentication Protocol on Pseudo-Random Hash Function with Shared Secrets[J]. Journal of Electronics & Information Technology, 2016, 38(2): 361-366. (in Chinese)

[18] YAUKSEL K. Universal Hashing for Ultra-Low-Power Cryptographic Hardware Applications[D]. Worcester, MA: Worcester Polytechnic Institute, 2004.

(编辑:徐楠楠)