doi:10.3969/j.issn.1000-436x.2013.04.009

标准模型下可证明安全的 RFID 双向认证协议

肖锋，周亚建，周景贤，钮心忻
(北京邮电大学 信息安全中心，北京 100876)

摘 要：目前，RFID(radio frequency identification)系统安全问题日益突出，为了实现 RFID 系统信息安全与隐私保护，在标准模型提出了一个基于 HB 协议的 RFID 双向安全认证协议。利用规约技术证明协议的安全性，将攻击者的困难规约到伪随机函数与真正随机函数的不可区分性上。协议仅使用轻量级的伪随机发生器以及向量点乘运算，具有较高的安全性和效率。通过从安全性及性能两方面与其他认证协议进行比较，表明协议适用于低成本及存储资源受限的 RFID 标签。
关键词：射频识别；电子标签；认证协议；隐私保护
中图分类号：TN918.5 **文献标识码**：A **文章编号**：1000-436X(2013)04-0082-06

Provable secure mutual authentication protocol for RFID in the standard model

XIAO Feng, ZHOU Ya-jian, ZHOU Jing-xian, NIU Xin-xin
(Information Security Research Center, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: The security issue of RFID is becoming more and more serious, in order to protect the RFID's information security and privacy, a mutual authentication protocol for RFID based on HB protocol was proposed in the standard model. The security proofs for this novel protocol was given by using the reduction method, and the attacker's hardness was reduced to the indistinguishability between pseudo-random function and real random function. The implementation of proposed protocol only required lightweight pseudo-random generator and vector dot product operation and provided higher security and efficiency. The comparisons of security and performance were also given with other authentication protocols, the results show that the proposed protocol is feasible for RFID tags which are low cost and resource-constrained.
Key words: RFID; digital tag; authentication protocol; privacy protection

1 引言

随着物联网技术日新月异的发展，无线射频识别（RFID）作为一种成熟的信息传感技术，已广泛应用于物流、零售、市政交通等领域。RFID 系统由电子标签（tag）、读写器（reader）以及后台数据库(DB，database)组成，在快速传输与读取数据的同时，其安全性及信息的隐私问题受到各界越来越多的关注。

近些年来，密码学技术成为研究 RFID 系统信息安全与隐私保护问题的重要方法。一些基于散列函数及循环冗余码（CRC，cyclic redundancy code）的 RFID 安全认证协议[1~4]相继被提出。但这些协议易遭受仿冒攻击、拒绝服务攻击及重放攻击[5]，并且缺乏形式化证明。Ha[1]等提出的协议中 tag、reader 及 DB 使用 ID 作为共享密钥，tag 另外存储一个 SYNC 标识上次协议是否成功。协议首先由 reader 向 tag 发送随机数 r_R，然后 tag 生成随机数 r_T，并根据上次协议完成后的 SYNC 的值，利用散列函数计算 $P=h(ID)$ 和 $Q=h(ID\|r_R\|r_T)$，将 P、$L(Q)$ 及

收稿日期：2012-08-31；**修回日期**：2013-01-04
基金项目：国家自然科学基金资助项目(60972077, 61121061)；国家重大专项基金资助项目(2010ZX03003-003-01)；北京市自然科学基金项目(9092009)
Foundation Items: The National Natural Science Foundation of China (60972077, 61121061); The National Science and Technology Key Project (2010ZX03003-003-01); The Natural Science of Foundation of Beijing (9092009)

随机数 r_T 发送给 reader 及 DB，其中，h 表示散列函数，$L(Q)$ 表示 Q 的左半部分。DB 收到信息后验证 P 及 Q 的值，并将 Q 的右半部分 $R(Q)$ 发送给 tag。Tag 收到后首先验证 $R(Q)$ 的值，若正确则置 $SYNC=0$，否则 $SYNC=1$。该协议中攻击者可以仿冒 reader 发送零字符串，诱使 DB 认证通过，最终导致 tag 与 DB 之间的密钥更新不同步。故该协议易遭受拒绝服务攻击。

Tan[2]等的协议中 reader 和 tag 共享密钥 s，当 reader 发起认证请求后，tag 标签生成随机数 r_T 作为回应，reader 将自己的标识 ID_R 及随机数 r_R 发给 tag，tag 计算 $h(ID_R \| s)$ 及 $h(ID_R \| s \| r_R \| r_T) \oplus ID_T$ 发送给 reader。reader 通过对比 $h(ID_R \| s)$ 的值，并从 $h(ID_R \| s \| r_R \| r_T) \oplus ID_T$ 中获取 tag 的标识 ID_T。由于密钥 s 始终不变以及 ID_R 通过明文传输，故攻击者可以重放消息并根据 $h(ID_R \| s)$ 的值追踪 tag。

Chen 和 Deng[3]的协议在初始阶段 tag 和 reader 共享三元组 (s_1, s_2, EPC)，reader 发送随机数 r_R 及 $CRC(r_R \oplus s_1)$ 给 tag 作为挑战，tag 验证 $CRC(r_R \oplus s_1)$ 的值，生成随机数 r_T 并发送 $E = s_2 \oplus EPC \oplus r_T$ 及 $W = CRC(s_1 \oplus x \oplus r_T)$ 作为应答。reader 验证 E 和 W 的正确性，并返回确认信息。由于 CRC 本身的线性性质[6]，导致攻击者可以假冒 tag，截取并篡改 E 与 W 的值，导致非法标签认证成功，因此该协议易遭受仿冒攻击以及重放攻击。

Cai[4]等提出的协议中 reader 和 tag 存储二元组密钥 (s,t)，DB 存储最近 2 次使用密钥 (s,t) 及 (s',t')。reader 生成随机数 r_R 发给 tag，tag 生成随机数 r_T 并计算 $M_1 = r_T \oplus t$ 及 $M_2 = f_t(r_R \oplus r_T)$ 发送给 reader 及 DB，其中，f_t 表示带有密钥 t 的伪随机函数。DB 根据记录逐条比对 M_1 和 M_2 的值对 tag 进行认证，若认证通过，则更新 (s,t) 及 (s',t') 的值并计算 $M_3 = s \oplus h(r_T)$，分别将更新后的 (s,t) 及 M_3 发送给 reader 和 tag。tag 验证收到的 M_3 的值，若正确则更新密钥 (s,t)。该协议下攻击者可以通过阻断 tag 与 reader 间的信息，导致 tag 与 reader 间的密钥无法同步更新，从而导致拒绝服务。

邓淼磊[7]等在可组合安全模型下证明了协议的安全性，但协议中的伪随机函数未实例化。马昌社[8]等提出了具有前向安全性的认证协议，但该协议可能会遭受重放攻击。另外还有利用椭圆曲线加密（ECC, elliptic curve cryptography）算法[9]及 NTRU (num theory research unit)[10]等非对称加密技术设计的认证协议，但协议需要的计算及存储资源对于低成本的 RFID 标签是不适用的。

HB[11]协议是由 Hopper 和 Blum 于 2001 基于 LPN 问题提出的 RFID 认证协议。HB 协议操作简单，且硬件上容易实现。但 HB 协议只能完成单向认证且无法抵抗主动攻击。因此本文在 HB 协议基础上提出一个 RFID 双向安全认证协议，并在标准模型下对协议进行形式化分析，证明对 RFID 系统信息安全与隐私的保护，同时在安全性和性能两方面与其他同类协议进行比较，说明协议对于低成本标签的适用性。

2　RFID 安全认证协议设计需求

在普适计算环境下设计一个安全合理的认证协议，需要考虑多方面因素。首先在安全性方面，协议必须能够对 RFID 系统的信息安全与隐私提供有效保护。另外对于低成本，存储量及计算资源受限的标签，协议所需要的通信量及计算量等性能指标也是重要的因素。

1) 安全性

安全性方面是考虑协议能否抵抗已知的攻击。主要攻击方式包括窃听攻击、重放攻击、拒绝服务攻击、中间人攻击以及自适应攻击。其中，自适应攻击是指攻击者在一定时间内收集正常认证会话信息（有时甚至可以扮演 reader 的角色），在获得充分的信息后，冒充 tag 向 reader 发送信息，并试图通过认证。

2) 隐私性

隐私性包括标签携带信息的隐私以及标签地理位置的隐私。

信息隐私性：协议必须保护 tag 的私密信息，如密钥及身份标识的隐私安全。

不可追踪性：协议必须保证攻击者无法对 tag 进行追踪。应确保每次会话消息有所变化而不被攻击者追踪。

3) 协议性能

协议的性能方面包括协议认证双方所需的存储量、计算量以及通信量。

信息存储：认证双方在协议运行过程中所需要信息存储量，如共享的密钥及中间变量。

计算量：认证双方在协议运行过程中需要耗费的计算资源。对于计算资源有限的 tag，这点尤为

重要。

通信量：认证协议所需的通信交互次数。在保证安全的前提下，尽可能地减少通信量。

因此如何设计高效、安全的 RFID 双向认证协议将是本文研究的重点。

3 RFID 双向安全认证协议

3.1 数学公式及假设条件

首先给出 RFID 双向安全协议中使用的符号定义。

f：真正的随机函数；

G_k：带有密钥 k 的伪随机函数；

$g(k)$：带种子 k 的伪随机发生器；

$negl(n)$：数量值可忽略的函数；

v：噪声发生器；

η：噪声系数；

D：多项式时间区分器；

pr：事件发生的概率；

ID：标签的唯一标识；

x：标签与读写器之间的共享密钥；

x_{new}：更新后的密钥值；

x_{old}：协议上一次使用的密钥值；

a：读写器发送给标签的挑战向量；

r：标签产生的随机数；

O：预言机；

A：攻击者敌手；

Adv：事件具有优势的概率；

EXP：攻击产生的实验；

$t(n)$：多项式时间；

$\varepsilon(n)$：敌手通过实验的优势；

$q(n)$：多项式时间内攻击者问询次数。

下面给出协议涉及的一些公式及定义。

定义 1 伪随机函数：令 G_k 为带有密钥 k 的函数，$f:\{0,1\}^n \to \{0,1\}^n$ 为能够将 n bit 的字符串均匀地映射到 n bit 字符串的真正的随机函数。如果对于任何多项式时间区分器 D，存在一个可忽略的函数 $negl(n)$，满足

$$\left|\text{pr}\left[D^{G_k}\left(1^n\right)=1\right]-\text{pr}\left[D^{f}\left(1^n\right)=1\right]\right| \leqslant negl(n) \quad (1)$$

则称 G_k 为一个伪随机函数。

定义 2 伪随机函数构造[12]：令 g 是扩展系数 $l(n)=2n$ 伪随机发生器。用 $g_0(k)$ 表示 g 输出的前半部分，用 $g_1(k)$ 表示 g 输出的后半部分。对于每一个 $k\in\{0,1\}^n$，定义伪随机函数函数 $G_k(x):\{0,1\}^n \to \{0,1\}^n$ 为 $G_k(x_1x_2\cdots x_n)=g_{x_n}\left(\cdots\left(g_{x_2}\left(g_{x_1}(k)\right)\right)\cdots\right)$。

RFID 双向安全认证协议的设计基于如下假设。

1) reader 与 tag 之间的通信信道是不安全的。reader 与后台数据库 database 之间通信信道是安全的，为方便说明，省略 database。

2) tag 拥有一个噪声参数 $\eta\in(0,1/2)$ 的噪声发生器，产生噪声 $v=\{0,1|\text{pr}[v=1]=\eta\}$。

3) reader 和 tag 拥有伪随机发生器 g，并且能够计算伪随机函数 G_k。

3.2 RFID 双向安全认证协议步骤

基于 HB 协议的 RFID 双向安全认证协议的步骤如图 1 所示。

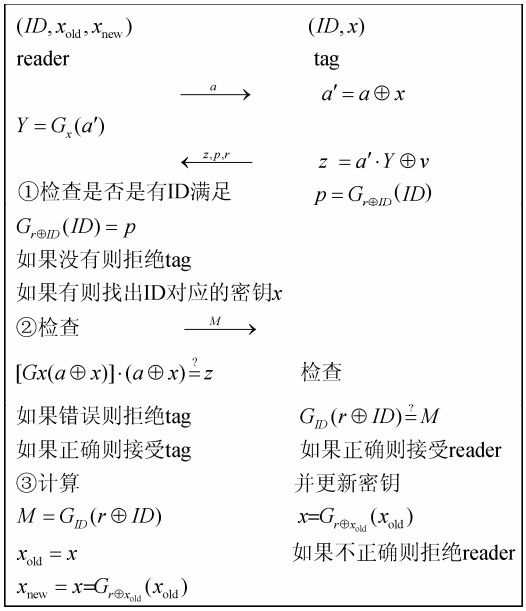

图 1 RFID 双向安全认证协议

在协议开始前，tag 存储一个二元组数据 (ID,x)，其中，ID 为唯一标识其身份的字符串，x 为 tag 与 reader 之间共享的 n 位密钥。reader 在后台数据库存储 tag 的三元组数据 $(ID,x_{\text{new}},x_{\text{old}})$，其中，$ID$ 为 tag 的标识符，x_{old} 为前一次认证成功时 tag 的密钥，x_{new} 为上次认证成功后经过更新而在本次认证使用的密钥。初始阶段置 x_{old} 为空。

协议运行的具体步骤如下。

1) 首先 reader 启动认证，向 tag 发送 n bit 随机挑战向量 a。挑战向量一共发送 s 轮，用矩阵 $(a_1a_2\cdots a_s)$ 表示。

2) tag 收到挑战向量 a 后，首先利用伪随机发生

器，生成 k bit 随机向量 r，进行 s 轮如下计算：

$$a_i' = a_i \oplus x$$

$$Y = G_x(a_i')$$

$$z = a_i' \cdot Y \oplus v$$

$$p = G_{r \oplus ID}(ID)$$

其中，$1 < i < s$，G 为伪随机函数，$\cdot$ 为矢量内积，$\oplus$ 为异或运算。s 轮执行完毕后，tag 将 (z, p, r) 发送给 reader 作为应答响应。

3) reader 收到 tag 的应答响应 (z, p, r) 后，进行如下操作。

① 首先在数据库中搜索是否有 ID 满足 $G_{r \oplus ID}(ID) = p$，如果没有则拒绝该 tag 认证请求。

②查找 ID 对应的 tag 的密钥 $(x_{\text{old}}, x_{\text{new}}) \in x$，进行如下验算：

验证 tag 应答响应中 z 是否满足 $[G_x(a_i \oplus x)] \cdot (a_i \oplus x) = z_i$，（$1 < i < s$），并且错误的轮数小于 ηs，则 tag 认证通过，反之则拒绝 tag。

③若该 tag 通过认证，reader 需要回复认证信息给 tag，以完成 tag 对其的身份认证，并对 tag 的密钥进行更新：

$$M = G_{ID}(r \oplus ID)$$

$$x_{\text{old}} = x$$

$$x_{\text{new}} = G_{r \oplus x_{\text{old}}}(x_{\text{old}})$$

然后 reader 将 M 发送给 tag。

4) tag 收到 reader 的回复后，验证 $G_{ID}(r \oplus ID) = M$ 是否成立：如果错误，则拒绝 reader，保持密钥 x 不变；如果正确，则通过 reader 的认证，并同步更新密钥 $x = G_{r \oplus x_{\text{old}}}(x_{\text{old}})$。

4　攻击模型及假设

在本文中攻击者 A 被设定为概率多项式时间(PPT, probabilistic polynomial time)算法，在多项式时间 $t(n)$ 内，攻击者可以尝试最多 $q(n)$ 次攻击。

1) 攻击者窃听 tag 与 reader 认证会话中的信息。

2) 攻击者阻截甚至篡改 tag 与 reader 认证会话信息。

3) 攻击者冒充 tag，要求 reader 发出挑战信息，并向 reader 返回应答信息。

4) 攻击者冒充 reader，选择挑战信息发送给合法 tag，通过观察 tag 的应答信息获得相关知识。

5) 在获得相关知识后，攻击者冒充 tag，并要求 reader 开启正常认证，选择有利于自己的挑战信息，并返回应答信息，试图通过认证。

攻击分为 2 个阶段：训练阶段和猜测阶段。

在训练阶段中，敌手 A 扮演 reader 的角色，向合法的 tag 发送挑战信息，tag 作为应答预言机 O 回复认证会话信息 $\sigma(z, p, r)$。同时 A 还可以对正常认证会话进行窃听以及阻截，导致合法 tag 和 reader 之间信息不同步，为下一步猜测阶段做准备。

在攻击阶段，敌手 A 利用训练阶段收集得到的信息，伪装成 tag，根据 reader 发送过来的挑战 a，回复应答信息 z。

A 需要进行如下猜测实验 EXP_A^G。

1) 在训练阶段 A 首先扮演 reader 的角色，在时间 $t(n)$ 内向合法 tag 发出认证挑战信息 a，tag 使用伪随机函数 G 作为应答预言机 O 返回应答信息，敌手最多可以问询 $q(n)$ 次，然后敌手观察并收集认证会话信息 $I(z, p, r)$。

2) A 可以阻截或篡改某一合法 tag 与 reader 之间的正常认证破坏信息 M，导致 tag 与 reader 之间信息不同步，密钥无法同步更新。

3) 进入猜测阶段后，A 扮演 tag 的角色，此时 tag 随机选择一个比特 $b \leftarrow \{0,1\}$，并且 b 对 reader 是保密的。reader 均匀地随机选择 $a_0, a_1 \in (0,1)^n$。

若 $b = 0$，则发送给 reader 的信息为 z_0；

若 $b = 1$，则发送给 reader 的信息为 z_1。

4) reader 在获得应答信息后，攻击者在现有知识的基础上（包括在训练阶段获得知识 I），要求对 b 进行猜测，输出一个比特 b'。

5) 如果 $b' = b$，则整个实验结果输出为 1，否则输出为 0。

在使用伪随机函数 G 的情况下，设 PPT 敌手 A 在多项式时间 $t(n)$ 内，向应答预言机问询 $q(n)$ 次，定义攻击者 A 通过实验的优势为

$$Adv = \left| \text{pr}\left[EXP_A^G(q,t) = 1 \right] - \frac{1}{2} \right| = \varepsilon(n) \qquad (2)$$

5　协议安全及性能分析

5.1　协议安全性分析

下面首先证明协议在自适应攻击模型下仍然是安全的。

定理 1 在攻击模型下，攻击者 A 通过实验的优势 $Adv=\left|\mathrm{pr}\left[EXP_A^G(q,t)=1\right]-\frac{1}{2}\right|=\varepsilon(n)$ 是可忽略的。

证明 引入一个区分器 D 用来区分伪随机函数 G 和真正随机函数 f，并且 D 可以调用猜测实验 EXP_A^G 中的攻击者 A，使用应答预言机作为其子程序。

在 EXP_A^G 中采用的是伪随机函数 G 作为应答预言机，现在假设其他条件不变，将实验中的伪随机函数 G 替换为真正随机函数 f，此实验记为 EXP_A^f，下面先计算敌手的优势 $\mathrm{pr}\left[EXP_A^f(q,t)=1\right]$ 的大小。

由于攻击者在训练阶段可以扮演 reader 发送挑战向量给 tag，并获得相应的知识。在猜测阶段，敌手扮演 tag 可以自由选择挑战向量 a_c，最后对 b 进行猜测。此时有 2 种情况。

1) 若 a_c 之前在训练阶段被敌手问询过，此时敌手将非常容易猜测出到底是 a_0 还是 a_1 参与认证。因为敌手最多向应答预言机问询 $q(n)$ 次，因此这种情况的可能性最多为 $q(n)/2^n$。

2) 若 a_c 在训练阶段未被敌手问询过，此时敌手在没有掌握随机函数 f 的任何情况下，猜对 b 的可能性为 $1/2$。

综合上面的分析，则在进行实验 EXP_A^f 的情况下，敌手的优势

$$\mathrm{pr}\left[EXP_A^f(q,t)=1\right]\leqslant q(n)/2^n+1/2 \tag{3}$$

接下来通过规约的方法计算出实验 EXP_A^G 下敌手的优势。

1) 假设 D 调用预言机为伪随机函数 G，那么 A 被 D 作为子程序运行时的视图分布与猜测实验 EXP_A^G 中 A 的分布是相同的，因为挑战向量 $\boldsymbol{a}$ 是也是随机选择的。因此

$$\mathrm{pr}[D^G(1^n)=1]=\mathrm{pr}\left[EXP_A^G(q,t)=1\right] \tag{4}$$

2) 同理，假设 D 调用的预言机为真正的随机函数 f，则 A 被 D 作为子程序运行时的试图分布与猜测实验 EXP_A^f 相同。

$$\mathrm{pr}[D^f(1^n)=1]=\mathrm{pr}\left[EXP_A^f(q,t)=1\right] \tag{5}$$

因此根据式(2)~式(5)可以得出

$$\begin{aligned}&\mathrm{pr}[D^f(1^n)=1]-\mathrm{pr}[D^G(1^n)=1]\\&=\mathrm{pr}\left[EXP_A^f(q,t)=1\right]-\mathrm{pr}\left[EXP_A^G(q,t)=1\right]\\&\geqslant\varepsilon(n)-\frac{q(n)}{2^n}\end{aligned}$$

因为根据式(1)，G 作为伪随机函数，区分器 D 能够区分其与真正随机函数 f 的概率小于一个可忽略的函数 $negl(n)$，即 $\varepsilon(n)-\frac{q(n)}{2^n}$ 必须也是可忽略的。故实验 EXP_A^G 中敌手的优势 $Adv=\left|\mathrm{pr}\left[EXP_A^G(q,t)=1\right]-1/2\right|=\varepsilon(n)$ 也是可忽略的。从而得出协议在攻击模型下是安全的，即能够抵抗自适应攻击。

对于拒绝服务攻击，攻击者可能在 reader 完成对 tag 的认证后，截断 reader 返回给 tag 的认证信息，使 tag 无法完成对 reader 的认证，导致认证双方密钥不同步。但协议中 reader 每次在认证后都存储了三元组 $(ID,x_{\mathrm{new}},x_{\mathrm{old}})$，即使 tag 的密钥未更新，由于后台数据库保存有最近一次认证成功的密钥，因此在下次认证时仍可使用旧的密钥认证成功，并在认证完成后进行密钥更新。

对于重放攻击，由于通信双方采用随机向量，并使用伪随机函数进行计算，因此即使攻击者重放已使用的挑战向量或应答信息，也无法通过认证。

定理 2 协议能满足 RFID 系统的信息隐私性与不可追踪性。

证明 1) 信息隐私保护：tag 的隐私信息包括其标识符 ID 以及密钥 x。在认证信息传递的过程中，tag 的标识符 ID 以及密钥 x 均未以明文形式传输，而是通过伪随机函数 G 运算而生成的加密信息 z、p 以及 M。通过上一节的分析得出伪随机函数对于真正随机函数的不可区分性，因此攻击者是无法通过对伪随机函数的猜测而获得 tag 隐私信息 ID 以及密钥 x。

2) 不可追踪性：协议中传递的消息 a、z、p、r 以及 M，其中，a 以及 r 为每次认证会话随机选择向量，而 z、p 以及 M 都是由伪随机函数 G 生成，并且与 a 和 r 相关。这样就能保证每次认证会话中传递的信息是不同的，使得攻击者无法通过会话信息锁定或跟踪 tag。

表 1 列出本文提出的协议与其他几种典型的双向认证协议之间的安全性比较。其中，Y 表示能够抵抗该攻击，N 表示不能抵抗该攻击。

表 1　　安全性比较

安全性比较	文献[1]	文献[2]	文献[3]	文献[4]	本文协议
自适应攻击	N	N	N	Y	Y
重放攻击	Y	N	N	Y	Y
拒绝服务攻击	N	Y	Y	N	Y
隐私保护	Y	N	Y	Y	Y

5.2　协议性能分析

RFID 标签的计算资源以及存储空间都受到一定限制，因此协议必须考虑参与方所需的存储量、计算量以及通信量。

1) 存储量：协议中 tag 需要固定存储的是唯一标识符 ID 以及密钥 x。由于每轮协议可以并行运行，故 tag 不需要存储每轮的中间计算结果。reader 需要存储的是三元组 $(ID, x_{\text{new}}, x_{\text{old}})$。

2) 计算量：tag 和 reader 需要计算的信息为 z、p、M 以及密钥的更新 x_{new}，涉及到运算为伪随机函数 G，异或运算以及向量的点乘。

3) 通信量：协议一共分为 4 步，其中，tag 需要传递的信息为 (z, p, r)，reader 需要传递的信息为 a 与 M。

表 2 列出本文提出的协议与其他几个双向安全认证协议的性能比较。存储量的统计是基于 1 个读写器对应 n 个标签时需存储的参数个数，计算量是协议参与方需要进行的密码学运算。通信交互数为参与方在 1 次协议完成时所需要的交互次数。在保证安全的前提下，新协议采用基于伪随机发生器生成的伪随机函数，伪随机发生器只需要不超过 1 500 个门电路即可实现[13]，相对于占用资源较大的散列函数，不管是从硬件资源还是计算量上，都更适用于 RFID 标签。另外向量的点乘和异或运算也无需占用过多计算资源。

表 2　　协议性能比较

性能比较	Tag 存储量	Reader 存储量	通信交互数	计算量
文献[1]	2	n	5	散列函数+连接运算
文献[2]	1	n	4	散列函数+异或运算+连接运算
文献[3]	3	$3n$	3	循环冗余校验+异或运算
文献[4]	2	$2n$	5	散列函数+异或运算+连接运算+移位运算
本文协议	2	$3n$	4	伪随机发生器+异或运算+向量点乘

6　结束语

本文设计了一个基于 HB 协议的 RFID 双向安全认证协议，并在标准模型下通过形式化分析方式证明协议能够实现对 RFID 系统的信息安全与隐私的保护。通过与其他同类型 RFID 双向安全认证协议进行比较，表明协议具有较高的效率及安全性。

随着 RFID 标签的广泛使用，数量众多的标签密钥的管理与分配将成为新的研究热点，另外标签的寻址也是一个亟待解决的问题。因此设计一个适用于 RFID 标签密钥管理及分配机制以及标签寻址方案将是笔者今后工作的目标。

参考文献：

[1] HA J, MOON S, *et al*. Lightweight and resynchronous mutual authentication protocol for RFID system[A]. LNCS[C]. 2007. 4412:80-89.

[2] TAN C C, SHENG B, LI Q. Secure and serverless RFID authentication and search protocols[J].IEEE Transactions on Wireless Communications, 2008, 7 (4):1400-1407.

[3] CHEN C L, DENG Y Y. Conformation of EPC class 1 and generation 2 standards RFID system with mutual authentication and privacy protection[J]. Engineering Applications of Artificial Intelligence, 2009, 22(8):1284-1291.

[4] CAI S, LI Y, LI T, *et al*. Attacks and improvements to an RFID mutual authentication protocol[A]. WiSec '09[C]. 2009. 51-58.

[5] PIRAMUTHU S. RFID mutual authentication protocols[J]. Decision Support Systems, 2011, 50(2):387-393.

[6] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J E, *et al*. Cryptanalysis of an EPC class-1generation-2 standard compliant authentication protocol[J]. Engineering Applications of Artificial Intelligence, 2011, 24(6):1061-1069.

[7] 邓淼磊,王玉磊,邱罡等.无需后端数据库的 RFID 认证协议[J].北京邮电大学学报, 2009, 32(4):59-62.
DENG M L, WANG Y L, QIU G, *et al*. Authentication protocol for RFID without back-end database[J].Journal of Beijing University of Posts and Telecommunications, 2009, 32(4):59-62.

[8] 马昌社.前向隐私安全的低成本 RFID 认证协议[J].计算机学报, 2011, 34(8):1387-1398.
MA C S. Low cost RFID authentication protocol with forward privacy[J]. Chinese Journal of Computer, 2011, 34(8):1387-1398.

[9] GODOR G, GICZI N, SANDOR I. Elliptic curve cryptography based mutual authentication protocol for low computational complexity environment[A]. ISWPC'2010[C]. 2010. 331-336

[10] 蔡庆玲, 詹宜巨, 余松森等. 基于 NTRU 公钥密码系统的 RFID 通信安全协议的研究[J].中山大学学报(自然科学版), 2009, 48(5):6-11.
CAI Q L, ZHAN Y J, YU S S, *et al*. RFID communication security protocol based on NTRU public key cryptosystem[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2009, 48(5):6-11.

[11] HOPPER N J, BLUM M. Security human identification protocol[A]. ASIACRYPT'01[C]. 2001. 52-66.

（下转第 98 页）