一种具有阅读器匿名功能的射频识别认证协议

谢 润[①②] 许春香*[①] 陈文杰[①] 李万鹏[①]
[①](电子科技大学计算机科学与工程学院 成都 611731)
[②](宜宾学院数学学院 宜宾 644000)

摘 要：在射频识别(RFID)的应用中，安全问题特别是用户隐私问题正日益凸显。因此，(用户)标签信息的隐私保护的需求越来越迫切。在 RFID 系统中，标签的隐私保护不仅是对外部攻击者，也应该包括阅读器。而现有许多文献提出的认证协议的安全仅针对外部攻击者，甚至在外部攻击者的不同攻击方法下也并不能完全保证安全。该文提出两个标签对阅读器匿名的认证协议：列表式 RFID 认证协议和密钥更新式 RFID 认证协议。这两个协议保证了阅读器对标签认证时，标签的信息不仅对外部攻击者是安全的而且对阅读器也保持匿名和不可追踪。相较于 Armknecht 等人提出的对阅读器匿名和不可追踪的认证协议，该文所提的协议不再需要增加第三方帮助来完成认证。并且密钥更新式 RFID 匿名认证协议还保证了撤销后的标签对阅读器也是匿名性和不可追踪的。

关键词：安全协议；射频识别；匿名认证
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2015)05-1241-07
DOI: 10.11999/JEIT140902

An RFID Authentication Protocol Anonymous against Readers

Xie Run[①②] Xu Chun-xiang[①] Chen Wen-jie[①] Li Wan-peng[①]
[①](*School of Computer Science and Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 611731, *China*)
[②](*School of Mathematical*, *Yibin University*, *Yibin* 644000, *China*)

Abstract: In application of RFID (Radio Frequency IDentification), security threats are on the rise. The demand for the privacy protection of tag is becoming more and more urgent. In RFID system, the privacy protection is against not only the outside attacker, but also the readers. In many exists the representative researches, the tags are only anonymous and untraceable for the outside attackers. In this paper, the list of protocol and the the key updated of protocol are proposed, which allow RFID tags to authenticate to readers without revealing the tag identity or any other information that allows tags to be traced. Compared with the scheme proposed by Armknecht *et al*., two schemes achieves anonymousness and untraceability authentication of RFID tags without the help of anonymizer. Furthermore, the key updated of scheme make sure that the revocatory tags will not be still tracked by updating key .

Key words: Security protocol; Radio Frequency IDentification (RFID); Anonymity authentication

1 引言

RFID(Radio Frequency IDentification)技术，又称电子标签或射频识别技术，使用该技术可通过无线电信号识别特定目标并读写相关数据，无需识别系统与特定目标之间建立机械接触。完整的RFID 系统，由阅读器(reader)与电子标签(tag)及发行者(issuer)3 部分所组成。阅读器根据电子标签提供的信息对电子标签进行认证。该技术被广泛应用于物联网，智能公交系统，车辆位置自我识别[1]，图书管理系统[2]，访问控制等。由于阅读器对电子标签的认证协议过程为无线通信过程，极易泄露电子标签中用户信息的隐私。为此，很多文献研究了电子标签对攻击者匿名和不可追踪的 RFID 认证协议，以保护电子标签 不被入侵[3]或其他形式的攻击。如文献[4,5]分别研究了如何检测克隆攻击和对电子标签的重传攻击。文献[6]和文献[7]中分别提出 RFID 的双向认证协议和基于散列树的认证方案，而文献[8]研究 GPS 认证模式。最近，文献[9]做了 RFID 系统中移动阅读器连续扫描的实验研究，文

2014-07-09 收到，2014-12-08 改回
国家自然科学基金(61370203)和四川省教育厅科研项目基金(12ZB348)资助课题
*通信作者：许春香 chxxu@uestc.edu.cn

献[10]进一步提出了在大规模的 RFID 系统中电子标签的快速搜索协议。

尽管有诸多研究成果，但 RFID 应用中安全问题仍然很突出。这些文献中，大多是基于阅读器是可信的这一假设来讨论认证协议的安全性，因此电子标签对阅读器并不是匿名和不可追踪的。但是，在越来越多的应用中，电子标签的用户希望电子标签对阅读器也保持匿名和不可追踪。例如，在电子票据、访问控制等应用中，用户是不愿自己的消费情况或访问记录被追踪。这些应用场景下，对电子标签的认证不仅要求对外部攻击者是匿名和不可追踪的，而且对阅读器也要求是匿名和不可追踪的。在许多情况下阅读器也仅需要验证电子标签的合法性。显然，实现电子标签对阅读器匿名和不可追踪的认证比仅对外部攻击者实现这种安全性要困难得多。大部分研究 RFID 的认证协议，如文献[11]只是讨论了对外部攻击者保持隐私的的认证方案。近来，文献[12,13]等研究了对阅读器匿名和不可追踪 RFID 认证协议。在文献[13]中，为了实现对阅读器的匿名和不可追踪，引入了第三方匿名器。匿名器的作用是在每次认证前，对电子标签发送给阅读器的消息进行匿名化，从而实现对阅读器匿名。但是该方案需要电子标签在每次认证前与匿名器交互，所以通信代价有很大增加。在对电子标签多次认证的实际环境中，通信次数的增加使得认证安全性下降。通过分析也可以发现：如果匿名器不可信的，那么匿名器能对电子标签进行追踪。另外，文献[14]也利用门限方法讨论了对阅读器匿名和不可追踪的电子标签认证协议，但该文献中的电子标签撤消方案是分别为电子标签和阅读器重新配发私钥和验证公钥。显然，这样做的结果等价于重新生成认证协议的所有密钥，所以系统效率将大大降低。应用文献[15]群签名的思想，本文给出两个 RFID 的匿名认证协议：列表式 RFID 匿名认证协议和密钥更新式 RFID 匿名认证协议。这两个匿名认证协议的特点分别是：

(1)列表式RFID匿名认证协议：该协议中，阅读器存储撤销列表，当有电子标签被撤销时，发行者将撤销电子标签添加到撤销列表，并将新的撤销列表发送给阅读器。对于未撤销的电子标签，认证协议保证了电子标签对阅读器匿名和不可追踪。这一协议不需要引入匿名器，认证过程只在电子标签和阅读器之间进行，简化了认证过程。本文在随机预言机模型下证明了协议的安全性。

对于阅读器能用已撤销电子标签的私钥来追踪这些电子标签的问题，本文提出了下面的改进协议。

(2)密钥更新式RFID匿名认证协议：在此协议中，阅读器不保存撤销列表。当某个电子标签被撤销时，发行者根据被撤销电子标签更新系统的公钥。阅读器用新的系统公钥验证认证消息，已撤销的电子标签不能再生成合法认证消息。而未撤销的电子标签更新其私钥中的一个数据后仍然能生成合法的认证消息。这个协议克服撤销后的电子标签可被追踪的问题。

由于电子标签的计算能力所限，本文采用预计算数据存储在电子标签中的方法，以减轻电子标签的计算荷载。

2 符号和预备知识

首先，给出要用到的符号、预备知识和密码学假设。为简便电子标签简记为 T。用 $\mathbf{QR}_n$ 记 Z_n^* 中的平方剩余集合，即 $\forall a \in \mathbf{QR}_n$ 意味着存在 $b \in Z_n^*$，使得 $b^2 = a \bmod n$。记 $H:\{0,1\}^* \to \{0,1\}^c$ 为理想的抗碰撞哈希函数；也用 l_* 表示元素 * 的比特长度。本文的协议的安全性基于下述困难问题。

定义1[16](强RSA(Riverst, Shamir, Adleman)问题) 设 $n = pq$ 是RSA的模，G 是 Z_n^* 的循环子群，则强RSA问题是：给定模 n 和 $u \in G$，找 $v \in G$ 和 $e > 1$ ($e \in Z$)，满足 $v^e = u \bmod n$。

假设1[16](强RSA假设) 对于给定的RSA的模 n 和 $u \in Z_n^*$，强RSA假是指：找 $e(>1)$ 和 v，使得 $v^e = u \bmod n$ 是计算困难的。

关于离散对数的知识签名方案是指：

定义2[17] 若序对 $(c,s) \in \{0,1\}^k \times Z_n^*$ 满足 $c = H(m \| y \| g \| g^s y^c)$，则称 (c,s) 是 y ($\in G$)在消息 $m \in \{0,1\}^*$ 上关于 g 的离散对数知识签名。

如果知道 $x = \log_g(y)$ 和在 Z_n^* 中随机选择 r，根据 $c = H(m \| y \| g \| g^r)$ 和 $s = r - cx \pmod n$ 可有效计算 (c,s)。

假设2(CDH(Computational Diffie-Hellman)假设) 设 p , q 分别是 l_p 和 l_q 比特的素数，并且 $q \mid p-1$，则 CDH 假设是：对于充分大的 l_p 和 l_q，输入 q 阶元素 $g \in Z_p^*$ 和 $\{g, g^a, g^b\}$，任意概率多项式算法正确计算 $\{g^{ab}\}$ 的概率关于 l_q 是可忽略的。这里 a , b 和 c 是从 $[0, q-1]$ 中随机选取的元素。

3 列表式 RFID 匿名认证协议

3.1 协议过程概述

本文的认证协议涉及三方：标签发行者，电子标签和阅读器。根据安全参数，发行者生成系统公钥 Ipk，撤销列表 RL 和电子标签的私钥 **Tsk**。用文献[17]中的签名方法，发行者对代表电子标签身份的秘密值 x 生成 C-L[17]签名，该签名作为电子标签的

私钥 **Tsk**。然后，发行者将预计算数据集和电子标签的私钥存储在电子标签中。发行者发送撤销列表 RL 和系统公钥 Ipk 至阅读器。发行者对阅读器的区分是通过它们之间的认证协议进行，通过认证发行者能区分一个阅读器是否是自己发行，从而决定是否为其发送撤销列表 RL 和系统公钥。开始认证时，阅读器向电子标签发送随机数 N_d，电子标签用私钥生成应答消息发回阅读器。由撤销列表中的信息，阅读器判断发送认证消息的电子标签是否属于 RL。若电子标签不属于 RL，则阅读器用系统公钥 Ipk 验证其合法性。

3.2 协议的安全假设

在认证过程中，假设敌手能控制电子标签和阅读器之间的通信信道，即他可以窃听、修改、操纵电子标签和阅读器之间通信消息。敌手能获取 Ipk，但不能获得发行者和电子标签的秘密信息。

发行者是可信的，它在安全的环境下初始化电子标签，即发行者和电子标签的秘密信息都不会在初始化时泄露。而阅读器是不可信的，它可能希望获得电子标签的秘密信息。阅读器也拥有系统公钥 Ipk，比电子标签有更强的计算能力，能并行处理多个电子标签的认证信息。电子标签的存储能力和计算能力受限制，它仅能做次数不多的乘法和加法运算，且诚实可信。根据实际情况，我们也假设电子标签会被多次认证。

3.3 参数选取

取 $n=pq$ 是 RSA 的模，即 $p=2p'+1$ 和 $q=2q'+1$ 是两个安全素数。由文献[17]，$\mathbf{QR}_n$ 是 Z_n^* 的乘法子群，其阶为 $p'q'$。取 l_Q，l_P 比特的素数 Q 和 P，且 $Q|P-1$。记 Z_P^* 为模 P 的乘法群。电子标签的私钥是表征身份的秘密值 x 的签名。为保证对 x 签名的安全，我们选取文献[17]中的抗选择消息攻击的签名方案。因此，以下的参数满足文献[15]和文献[17]中的条件(详细讨论参见文献[15]和文献[17])。

参数 c，e，Q，n，E 的比特长度满足条件：$l_c+l_e+l+1<l_Q$ 和 $l_Q+l_e+l+1<l_E<l_n/2$。这里 l 是比特串的长度。它满足对任意整数 a，选取比特长度为 l_a+l 的随机数 r，则 r 和 $a+r$ 是统计不可区分的。

3.4 认证协议过程

3.4.1 系统初始化　给定满足上述条件的参数的比特长度参数 $(l_n,l_Q,l_P,l_E,l_c,l_e,l)$，则：

(1)随机选择 a，g，$h\in\mathbf{QR}_n$ 和 $r_1,r_2,\cdots,r_k\in Z_n$ (这里 k 是电子标签数)；

(2)随机生成 l_Q 比特和 l_P 比特的素数 Q，P 并且 $Q|P-1$；随机选择 $x_1,x_2,\cdots,x_k\in Z_Q$；

(3)取 f 是 Z_P^* 中的一个 Q 阶元，随机选择 $X_s\in Z_Q$ 并计算 $s=f^{X_s}\bmod P$；

(4)选择 k 个不同的 l_e 比特的数 $e_1,e_2,\cdots,e_k$，使得 $e_1'=2^{l_E}+e_1,\cdots,e_k'=2^{l_E}+e_k$ 是素数；并计算 y_1，$y_2,\cdots,y_k$，使得 $y_1^{e_1'}=ag^{x_1}h^{r_1}\bmod n,\cdots,y_k^{e_k'}=ag^{x_k}h^{r_k}\bmod n$，根据已知 n 的分解，可有效计算[17] y_i；

(5)选取理想抗碰撞的哈希函数 $H:\{0,1\}^*\to\{0,1\}^{l_c}$；

(6)发行者生成公钥 Ipk=(n,a,g,h,Q,P,f,s)，T_i 的私钥 $\mathrm{Tsk}_i=(x_i,e_i,y_i,r_i)$ 和撤销列表 RL。发行者将 Ipk 和 RL 发送阅读器(其中 RL 中包含被撤销的 T_i 的私钥)，保密数据表 (X_s,DB)(其中 DB 为 T 的列表)；

(7)发行者初始化 T_i：在 T_i 中存储它的私钥 $\mathrm{Tsk}_i=(x_i,e_i,y_i,r_i)$ 和预计算的数据集：

$$F=\left\{f_j\mid f_j=f^{2^j}\bmod P;\ 0\le j\le l_Q\right\}$$

$$S=\left\{s_j\mid s_j=s^{2^j}\bmod P,\ 0\le j\le l_Q\right\}$$

$$H'=\left\{h_j\mid h_j=h^{2^j}\bmod n,\ 0\le j\le \frac{l_n}{2}\right\}$$

$$G=\left\{g_j\mid g=g^{2^j}\bmod n,\ 0\le j\le l_Q+l_c+l\right\}$$

$$Y=\left\{y_i\mid y_i=y_i^{2^j}\bmod n,\ 0\le j\le l_e+l_c+l\right\}$$

3.4.2 认证过程

(1)阅读器：随机选择 N_d，发送 N_d 给 T_i；

(2)标签 T_i：取随机数 $r\in\{0,1\}^{l_n/2}$，$z_1\in Z_Q$，$r_x\in\{0,1\}^{l_Q+l_c+l}$，$r_e\in\{0,1\}^{l_e+l_c+l}$，$z_2\in Z_Q$，计算：$M_0=h^r y_i\bmod n$，$M_1=f^{z_1}\bmod P$，$M_2=s^{z_1+x_i}\bmod P$，$V_0=h^{rr_e}y_i^{r_e}g^{r_x}\bmod n$，$V_1=f^{z_2}\bmod P$，$V_2=s^{z_2+r_x}\bmod P$，$c=H(\mathbf{Ipk},M_0,M_1,M_2,V_0,V_1,V_2,N_d)$。根据 T_i 的私钥 $\mathrm{Tsk}_i=(x_i,e_i,y_i,r_i)$，$r$，$r_x$，$r_e$，$z_1$，$z_2$，计算：$m_x=r_x-cx_i$，$m_r=c(-r_i-re_i')$，$m_e=r_e+ce_i$，$m_z=z_2-cz_1\bmod Q$。最后，发送 $\sigma=(c,M_0,M_1,M_2,m_x,m_r,m_e,m_z)$ 给阅读器。为计算 M_0，M_1，M_2，V_0，V_1，V_2，用预计算的数据集 F，S，H'，G，Y，算出 h^r，h^{rr_e}，f^{z_1}，f^{z_2}，$s^{z_1+x_i}$，$s^{z_2+r_x}$，g^{r_x}，$y_i^{r_e}$。因为计算 h^r，h^{rr_e} 等每一个值可用相同的算法实现，所以下面仅以 h^r 计算为例给出算法。

算法： $b\leftarrow r$，$L\leftarrow l_n/2$，　这里 $b=b_{L-1}\cdots b_j\cdots b_0$ (b 的二进制表示)，$h_j\in H'$ (h_j 取自预计算数据集 H')。令：$\tau=1$

```
for j from L−1 to 0 do
    If b_j = 1 then
        τ ← τ · h_j
    end if
end for
τ = h^r
```

类似地，用这一算法可分别计算出 h^{rr_e}, f^{z_1}, f^{z_2}, $s^{z_1+x_i}$, $s^{z_2+r_x}$, g^{r_x}, $y_i^{r_e}$。

(4)阅读器接收： $\sigma=(c,M_0,M_1,M_2,m_x,m_r,m_e,m_z)$

(a)检查是否 $m_e\in\{0,1\}^{l_e+l_c+l}$ 和 $m_x\in\{0,1\}^{l_Q+l_c+l}$；

(b)用撤销列表RL中 T_i 的私钥Tsk$_i$和认证消息中的 m_r，计算 $r=(-m_rc^{-1}(e_i')^{-1}-r_i(e_i')^{-1})$，其中 $e_i'=2^{l_E}+e_i$。若存在某个Tsk$_i$，它计算出的 r 使得 $M_0^{e_i'}h^{-re_i'}=ag^{x_i}h^{r_i} \bmod n$ 成立，则 σ 是由已撤销的 T_i 生成。注：由于 $\mathbf{Tsk}_i=(x_i,y_i,e_i,r_i)$ 保存在阅读器的RL中，所以 $(e_i')^{-1}$, $ag^{x_i}h^{r_i} \bmod n$, $h^{-e_i'}$ 可预计算保存，认证时仅计算 $-m_rc^{-1}(e_i')^{-1}$, $(h^{-e_i'})^r$, $U_0^{e_i'}$。

(c)否则，则用公钥Ipk和 σ 计算： $V_0=a^{-c}g^{m_x}h^{m_r}M_0{}^{c2^{l_E}+m_e} \bmod n$, $V_1=M_1^cf^{m_z} \bmod P$, $V_2=M_2^cs^{m_z+m_x} \bmod P$，并验证：$c=H(\mathbf{Ipk},M_0,M_1,M_2,V_0,V_1,V_2,N_d)$；若验证等式成立，返回成功；否则，返回失败。

3.5 生成新 T_j 和撤销 T_j

3.5.1 生成新 T_j 在协议中，发行者也能灵活地生成新的 T_j。发行者要生成一个新 T_j 时，则选择 $x_j\in Z_Q$, $r_j\in Z_n$ 和 $e_j\in\{0,1\}^{l_e}$，使得 $e_j'=2^{l_E}+e_j$ 为素数，并计算 y_j 满足 $y_j^{e_j'}=ag^{x_j}h^{r_j} \bmod n$。初始化 T_j，即存储 $\mathbf{Tsk}_j=(x_j,y_j,e_j,r_j)$ 和预计算数据到 T_j 中。

3.5.2 撤销 T_j 发行者将 T_j 的私钥 Tsk$_i$=(x_j,y_j,e_j,r_j) 添加到RL，将新RL发给阅读器。阅读器更新它的RL。

根据文中第1节中的分析，在这一认证协议中，撤销后的 T_j 对阅读器不再是匿名和不可追踪的。为此，我们给出下面的改进认证协议。

4 密钥更新式 RFID 匿名认证协议

在这一认证协议中，阅读器不再保存撤销列表。当 T_j 被撤销时，阅读器和未撤销的 T_i 分别从发行者处更新系统公钥和 T_i 的私钥。因此，未撤销的 T_i 仍然能生成合法的认证消息，已撤销标签不能生成合法的认证消息。更重要的是：撤销后的标签对阅读器仍然是匿名和不可追踪的。

密钥更新式匿名认证协议的安全性假设、参数以及参数满足的条件都和列表式匿名认证协议中相同。下面，我们给出密钥更新式匿名认证协议的认证过程。特别地，这里增加选择一随机元素 $t\in QR_n$，它被用于实现密钥的更新。

4.1 认证协议过程

4.1.1 系统初始化 发行者运行第3节中系统初始化时的步骤(1)~步骤(5)步，增加随机选择 $t\in QR_n$。

发行者：(1)生成系统公钥 Ipk=(n,t,a,g,h,Q,P,f,s)；(2)计算 $t_i=(t)^{e_i'^{-1}}$, $i=1,2,\cdots,k$；生成 T_i 的私钥 $\mathbf{Tsk}_i=(t_i,x_i,y_i,e_i,r_i)$ 和撤销列表RL；(3)将Ipk发送阅读器。

发行者初始化 T_i：将 $\mathbf{Tsk}_i=(t_i,x_i,y_i,e_i,r_i)$ 和预计算数据 F, S, H', G, Y 存储到 T_i 中。

4.1.2 认证过程

(1)阅读器随机选择 N_d，发送 N_d 给 T_i。

(2) T_i 取随机数： $r\in\{0,1\}^{l_n/2}$, $z_1\in Z_Q$, $r_x\in\{0,1\}^{l_Q+l_c+l}$, $r_e\in\{0,1\}^{l_e+l_c+l}$, $z_2\in Z_Q$；

调用第4节中算法，计算：

$M_0=h^ry_it_i \bmod n$, $M_1=f^{z_1} \bmod P$, $M_2=s^{z_1+x_i} \bmod P$, $V_0=h^{rr_e}y_i^{re}g^{r_x} \bmod n$, $V_1=f^{z_2} \bmod P$, $V_2=s^{z_2+r_x} \bmod P$; $c=H(\mathbf{Ipk},M_0,M_1,M_2,V_0,V_1,V_2,N_d)$。

根据私钥 $\mathbf{Tsk}_i=(t_i,x_i,y_i,e_i,r_i)$，计算： $m_x=r_x-cx_i$, $m_r=c(-r_i-re_i')$, $m_e=r_e+ce_i$, $m_z=z_2-cz_1 \bmod Q$，发送 $\sigma=(c,M_0,M_1,M_2,m_x,m_r,m_e,m_z)$ 到阅读器。

(3)阅读器检查： $m_e\in\{0,1\}^{l_e+l_c+l}$ 和 $m_x\in\{0,1\}^{l_Q+l_c+l}$，计算： $V_0=(at)^{-c}g^{m_x}h^{m_r}M_0{}^{c2^{l_E}+m_e} \bmod n$, $V_1=M_1^cf^{m_z} \bmod P$, $V_2=M_2^cs^{m_z+m_x} \bmod P$；验证：$c=H(\mathbf{Ipk},M_0,M_1,M_2,V_0,V_1,V_2,N_d)$。

4.2 生成新 T_j 和撤销 T_j

4.2.1 生成新 T_j 发行者用3.5.1中相同的方法生成一个新 T_j，即选择 $x_j\in Z_Q$, $r_j\in Z_n$ 和 $e_j\in\{0,1\}^{l_e}$，使得 $e_j'=2^{l_E}+e_j$ 为素数，并计算 y_j 满足 $y_j^{e_j'}=ag^{x_j}h^{r_j} \bmod n$。根据系统当前公钥中的 t，计算 $t_j=(t)^{e_j'^{-1}}$。生成新 T_j 的私钥 (t_j,x_j,y_j,e_j,r_j)。

发行者初始化 T_j：将 T_j 的私钥 (t_j,x_j,y_j,e_j,r_j) 和预计算数据存储在 T_j 中。

4.2.2 撤销 T_j 发行者将当前系统公钥 Ipk=(n,t,a,g,h,Q,P,f,s) 更新为 $\mathbf{Ipk}=(n,t_j,a,g,h,Q,P,f,s)$，其中 $t_j=(t)^{e_j'^{-1}} \bmod n$。阅读器下载新系统公钥，替换原有公钥。

所有未撤销的 T_i，从发行者处将自己私钥更新为 Tsk$_i$=$((t_i)^{e_j'^{-1}},x_i,y_i,e_i,r_i)$。

5 安全性分析

5.1 认证协议安全性分析

本节给出列表式匿名认证协议和密钥更新式匿名认证协议安全性证明。本文中给出的两个RFID匿名认证协议的区别在于：T_i 的 M_0 和阅读器的 V_0 在两个协议中不同。下面的安全性证明中并不会用到 M_0 和 V_0，所以安全性证明对两个RFID匿名认证协议都是成立的。

标签认证 本文的匿名认证协议阅读器对电子标签实现认证，意味着任何具有概率多项式界的敌

手 A 不能假冒电子标签通过阅读器的认证。将匿名标签认证协议形式化为安全试验 $\mathbf{Exp}_A^{\text{aut}} = \mathbf{out}_R^{\pi}$。对标签认证协议实例 π，若敌手 A 通过阅读器认证，则安全试验 $\mathbf{out}_R^{\pi} = 1$；否则 $\mathbf{out}_R^{\pi} = 0$。

定义 3[13]　在 RFID 匿名认证协议中，对任何具有概率多项式计算能力的敌手 A，如果关于安全参数 $(l_n, l_Q, l_P, l_E, l_c, l_e, l)$，概率 $P[\mathbf{Exp}_A^{\text{aut}} = 1]$ 是可忽略的，则称实现了对电子标签的认证。

根据这一定义，证明协议实现了对电子标签的认证，即要证明下述定理。

定理 1　RFID 匿名认证协议中的认证消息是不可伪造的。

证明　证明过程分 3 部分：(1)敌手通过伪造 T_i 的私钥的方法构造合法的认证消息的概率是可忽略的。(2)认证协议是抗重放攻击的。(3)敌手直接伪造合法认证消息的概率是可忽略的。

(1)敌手通过伪造 T_i 的私钥的方法构造合法的认证消息的概率是可忽略的。

由于匿名认证协议中，T_i 的密钥 Tsk_i 是 x_i 的 C-L 签名。在强 RSA 假设下，由文献[18]定理 3.6,C-L 签名在选择消息攻击下是安全的，即 A 通过伪造有效的 T_i 的密钥生成合法的认证消息 $\sigma = (c, M_0, M_1, M_2, m_x, m_r, m_e, m_z)$ 的概率是可忽略的。

(2)抗重放消息攻击。由于每次进行认证时阅读器都会随机选取 N_d，所以敌手 A 重放旧认证消息 $\sigma = (c, M_0, M_1, M_2, m_x, m_r, m_e, m_z)$ 通过认证，必须满足下面条件之一：

(a) $N_d = N_d'$；(b) $c = H(\mathbf{Ipk}, M_0, M_1, M_2, V_0, V_1, V_2, N_d) = H(\mathbf{Ipk}, M_0, M_1, M_2, V_0, V_1, V_2, N_d')$；其中 N_d, N_d' 分别对应认证消息 σ 初次生成和重放时阅读器所选取的随机数。

对条件(a)，由于阅读器是在足够大的空间中选取 N_d，所以概率是 $P[N_d = N_d']$ 是可忽略的。对条件(b)，若 $c = H(\mathbf{Ipk}, M_0, M_1, M_2, V_0, V_1, V_2, N_d) = H(\mathbf{Ipk}, M_0, M_1, M_2, V_0, V_1, V_2, N_d')$，则将得到哈希函数的一个碰撞。由此可知，协议是抗重放攻击的。

(3)敌手直接伪造合法认证消息的概率是可忽略的。

若敌手 A 能以不可忽略的概率直接伪造认证消息，则我们能得到算法 B，它在多项式时间内以相同概率解离散对数问题。

设 A 能以不可忽略的概率 ε 伪造合法的认证消息 $\sigma = (\sigma_0, c, \sigma_1)$ (其中 $\sigma_0 = (M_0, M_1, M_2)$, $\sigma_1 = (m_x, m_r, m_e, m_z)$)。在随机预言机模型下，根据分叉引理[19]，则 A 能通过对随机预言机询问，以 ε 的概率得到两个有效认证消息：$\sigma = (\sigma_0, c, \sigma_1)$ 和 $\sigma' = (\sigma_0, c', \sigma_1')$，其中 $c \neq c'$, $\sigma_1' = (m_x', m_r', m_e', m_z')$。取 $\sigma = (\sigma_0, c, \sigma_1)$ 和 $\sigma' = (\sigma_0, c', \sigma_1')$ 作为输入，则算法 B 计算：$V_1 = M_1^c f^{m_z} \bmod P$, $V_2 = M_2^c s^{m_z + m_x} \bmod P$ 和 $V_1 = M_1^{c'} f^{m_z'} = M_1^c f^{m_z} \bmod P$, $V_2 = M_2^{c'} f^{m_z' + m_x'} = M_2^c f^{m_z + m_x} \bmod P$。

由这 4 个等式得到 $M_1^{c-c'} = f^{m_z' - m_z}$, $M_2^{c-c'} = f^{(m_z' - m_z) + (m_x' - m_x)}$。又因为 $M_1 = f^{z_1} \bmod P$, $M_2 = f^{z_1 + x_i} \bmod P$，所以 $z_1 = \dfrac{m_z' - m_z}{c - c'}$, $z_1 + x_i = \dfrac{(m_z' - m_z) + (m_x' - m_x)}{c - c'}$。这表明算法 B 以 ε 的概率，正确计算离散对数。

为证明认证消息的不可追踪性，我们给出消息无关联性的安全概念。电子标签认证消息的无关联性是指：敌手区分任意两个认证消息是否来自相同的电子标签的概率优势是可忽略的。这意味着电子标签发送的认证消息，不会向阅读器泄露任何能追踪到它的信息。因此电子标签生成的认证消息如果具有无关联性，则电子标签是不可追踪的。下面给出无关联性的形式化的定义[13]。形式化认证协议为安全试验 $\mathbf{Exp}_{\text{A}}^{\text{prv-}b}, b \in_R \{0,1\}$。具有概率多项式计算能力敌手 A 与随机预言机 O_b 交互。当 $b = 0$ 随机语言机 O_b 表示两个合法标签 T_0 与 T_1 相同，$b = 1$ 时 O_b 表示 T_0 与 T_1 不同。在安全性试验中，敌手 A 能与 RFID 系统和 O_b 交互，得到 b' ($b' = 1$ 或 0)。

定义 4[13]　在 RFID 匿名认证协议中，如果对每个具有概率多项式计算能力的敌手 A，在给定的安全参数下，$\mathbf{Adv}_A^{\text{prv}} = |\mathbf{pr}[\mathbf{Exp}_A^{\text{prv}-0} = 1] - \mathbf{pr}[\mathbf{Exp}_A^{\text{prv}-1} = 1]|$ 是可忽略的，则称认证消息是无关联的。

定理 2　RFID 匿名认证协议中的认证消息是无关联的。

证明　设算法 B 访问 RFID 系统并获取其公钥中的 (f, s)，B 也能访问预言机 O_b；O_b 能生成任意两个标签 T_0 和 T_1 的认证信息(这里也可以直接将标签 T_0 和 T_1 作为语言机)，$b = 0$ 时，O_b 生成其中一个标签的两个认证信息 σ_0 与 σ_0'；$b = 1$ 时，O_b 分别生成 T_0 和 T_1 的认证信息 σ_1 和 σ_1'。

令

$$\sigma_0 = (c, M_{00}, M_{10}, M_{20}, m_{x0}, m_{r0}, m_{e0}, m_{z0})$$

$$\sigma_0' = (c', M_{00}', M_{10}', M_{20}', m_{x0}', m_{r0}', m_{e0}', m_{z0}')$$

$$\sigma_1 = (c, M_0, M_{11}, M_{21}, m_x, m_r, m_e, m_z)$$

$$\sigma_1' = (c', M_0', M_{11}', M_{20}', m_x', m_r', m_e', m_z')$$

算法 B 从 O_b 处获得的认证信息 (σ_0, σ_0') 和 (σ_1, σ_1') 任选一组发送给敌手 A。同时，B 计算 $M_{10}/M_{10}' = f^{z_0 - z_0'}$ 和 $M_{11}/M_{11}' = f^{z_1 - z_1'}$。若 A 能以

$\mathbf{Adv}_A^{\mathrm{prv}}=\varepsilon$ 的概率区分 (σ_0,σ_0') 和 (σ_1,σ_1') 中哪一个是同一标签生成的认证信息，即他正确选出 (σ_0,σ_0') 的优势概率为 ε。A 将选出的认证信息 (σ_0,σ_0') 返回给 B，则 B 能对应计算 $M_{20}/M_{20}'=s^{z_0-z_0'}=f^{X_s(z_0-z_0')}$。因此，$B$ 以 ε 的优势概率，$f,s=f^{X_s},f^{z_0-z_0'}$，成功计算了 $f^{X_s(z_0-z_0')}=M_{20}/M_{20}'$。这与 CDH 问题的困难性假设相矛盾，所以定理得证。因为无关联的安全性蕴含了不可追踪性，所以 T_i 对阅读器来说是不可追踪的。

5.2 密钥更新式匿名认证协议中被撤销电子标签的匿名与不可追踪分析

在第 4 节的方案中，由于撤销电子标签的身份不会被发行者公布，所以自然保持了被撤销 T_j 的匿名性和不可联系性。由认证协议，阅读器对认证消息的验证是检验电子标签私钥中 t_i 与公钥中的 t 是否有关系 $t_i=(t)^{e_i^{'-1}}$。当 T_j 被撤销后，公钥中的 t 被替换为 t_j。未撤销的电子标签中 $t_i'=(t_i)^{e_j^{'-1}}=((t)^{e_j^{'-1}})^{e_i^{'-1}}=(t_j)^{e_i^{'-1}}$，所以 t_i' 与新公钥中的 t_j 仍保持 $t_i'=(t_j)^{e_i^{'-1}}$。已撤销 T_j 没有 n 的分解因子信息，由强 RSA 假设，则它不能计算 t_j'，所以无法生成有效认证消息。T_j 下载了其他电子标签的 $(t_i)^{e_j^{'-1}}$，也不能生成正确的证书。

5.3 安全性与计算效率分析

安全性分析 本节列表对比本文与其他文献的各项安全性如表 1。从表中可以看出文献[7]，文献[8]，文献[11]满足的安全项较少。仅有本文的密钥更新式匿名认证协议能保证被撤销后的电子标签对阅读器仍然是匿名和不可追踪的。

计算实现 在 RFID 系统中，电子标签的计算能力和它的成本是成正比的。因此，对安全水平要求较高的 RFID 系统中，对电子标签计算能力的要求也会更高。与文献[13]相比，本文的协议在认证过程中不再需要第三方匿名器，且实现了更高的安全性。

按协议过程，电子标签的计算负载是计算 M_0，M_1,M_2,V_0,V_1,V_2。在平均意义下，利用 F,S,H'，G,Y 计算 M_0 和 V_0 需要计算 $h^r,(h^r y_i)^{r_e}$ 和 g^{r_x}，所以需要运行的乘法次数为 $\left(\frac{l_n}{4}+\frac{1}{2}(l_e+l_Q)+l_c+l\right)$；类似地计算 M_1,M_2 和 V_1,V_2 时，需要计算 f^{z_1},f^{z_2}，s^{z_1},s^{z_2}（f^{x_i},s^{x_i} 可预计算），需进行 $2\times l_Q/2$ 次乘法。但是，从方案的安全性分析可知：在强 RSA 假设下，模 n 和 P 的取值保证了方案的安全，而随机数 r,r_e,r_x 和 z_1,z_2 的是为了保证敌手不能从签名中的 (m_x,m_r,m_e,m_z) 计算出密钥或确定电子标签的身份；因此，只要 r,r_e,r_x 和 z_1,z_2 在足够大的数据集中均匀选取就能保证这一安全目的。

在不影响安全性能的条件下，为了减少计算量和存储，可用预计算方法减少电子标签计算。以计算 h^r 为例，均匀选取 β 个 $r_j\in\{0,1\}^{l_n/2}$，对应计算 h^{r_j} 存储与电子标签中。运行协议时，随机选取长度为 l' 的比特串 $\pm r_j'(\le r_j)$，则计算 $h^r=h^{r_j'}\times h^{r_j}$。显然，$h^r$ 是 0 到 $\beta 2^{l'+1}$ 之间的一个随机数，按此方法计算 h^r 的乘法次数为 $l'/2+1$（平均意义下）。对于 y,g,f,s 的幂，可以用相同的方法计算。因此，可以根据电子标签的计算能力和存储能力，取相应 l' 和 β 的值。

按 1024 bit 的 RSA 的安全水平要求(实际的 RFID 系统远低于这一安全要求)，当 $\beta=2^{10},l'=40$ 时，本协议的执行乘法约 100 次，4 次加法，需要的存储为 512k。根据文献[20]的研究，1024 bit 大数的模乘可以在 38k 门内实现，满足智能卡 40k 门限制的要求。对文献[21]中的电子标签(要求仅含 10k 门左右的芯片)，显然 1024 bit 参数的安全水平无法在这种电子标签上实现。

以上分析表明，该协议能够提供很好的安全性，且实现效率可以根据电子标签性能选取合适的参数，使得实现代价较低。能够提供很强安全性、实现效率高，而代价又很低的 RFID 认证协议是不存在的，较强的安全性意味着其实现代价和性能就会受到影响，所以 RFID 系统要做好安全性与实现代价及性能之间的取舍。随着微电子技术的发展[22]和某些安全要求较高 RFID 系统的应用中，本文的认证协议提供了一种很好的选择。

表 1 本文与其他文献安全性对比表

方法	认证	抗重放攻击	抗选择消息攻击	对攻击者匿名、不可追踪	对阅读器匿名、不可追踪	撤销标签的匿名与不可追踪性(对阅读器)	第三方辅助
文献[7]方法	实现	实现	无	实现	不能实现	不能实现	无
文献[8]方法	实现	实现	无	实现	不能实现	不能实现	无
文献[11]方法	实现	实现	无	实现	不能实现	不能实现	无
文献[13]方法	实现	实现	实现	实现	实现	不能实现	需要
本文方法	实现	实现	实现	实现	实现	实现	无

6　结束语

RFID 认证协议的安全性问题正变得越来越重要。本文给出了两个 RFID 匿名认证协议。列表式匿名认证协议使阅读器对电子标签的匿名认证不需要第三方的辅助，克服了文献[13]中引入第三方实现匿名认证产生的问题。密钥更新式匿名认证协议，使得撤销后的电子标签对阅读器仍然保持了匿名和不可追踪性，提高了 RFID 系统的安全性。

参 考 文 献

[1] Park S and Lee H. Self-recognition of vehicle position using UHF passive RFID tags[J]. *IEEE Transactions on Industrial Electronics*, 2013, 60(1): 226–234.

[2] Sing J, Brar N, and Fong C. The state of RFID applications in libraries[J]. *Information Technology and Libraries*, 2013, 25(1): 24–32.

[3] Sakai K, Ku W S, Zimmermann R, *et al.*. Dynamic bit encoding for privacy protection against correlation attacks in RFID backward channel[J]. *IEEE Transactions on Computers*, 2013, 62(1): 112–123.

[4] Zanetti D, Capkun S, and Juels A. Tailing RFID tags for clone detection[C]. NDSS 2013: 20th Network & Distributed System Security Symposium, San Diego, CA, USA, 2013.

[5] 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 and Feng Deng-guo. Design and analysis of cryptographic protocols for RFID[J]. *Chinese Journal of Computers*, 2006, 29(4): 581–589.

[6] Yang L, Yu P, Bailing W, *et al.*. A bi-direction authentication protocol for RFID based on the variable update in IOT[C]. Proceedings of the 2nd International Conference on Computer and Applications ASTL 2013, Vol. 17: 23–26.

[7] Molnar D, Soppera A, and Wagner D. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID Tags[C]. Selected Areas in Cryptography, Springer Berlin Heidelberg, 2006: 276–290.

[8] McLoone M and Robshaw M J B. Public Key Cryptography and RFID Tags[M]. Topics in Cryptology–CT-RSA 2007, Berlin Heidelberg Springer, 2006: 372–384.

[9] Xie L, Li Q, Chen X, *et al.*. Continuous scanning with mobile reader in RFID systems: an experimental study[C]. Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM, Bangalore, India, 2013: 11–20.

[10] Zheng Y and Li M. Fast tag searching protocol for large-scale RFID systems[J]. *IEEE/ACM Transactions on Networking*, 2013, 21(3): 924–934.

[11] Ryu E K and Takagi T. A hybrid approach for privacy-preserving RFID tags[J]. *Computer Standards & Interfaces*, 2009, 31(4): 812–815.

[12] Blass E O, Kurmus A, Molva R, *et al.*. PSP: private and secure payment with RFID[C]. Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, ACM, Chicago, IL, USA, 2009: 51–60.

[13] Armknecht F, Chen L, Sadeghi A R, *et al.*. Anonymous Authentication for RFID Systems[M]. Radio Frequency Identification: Security and Privacy Issues. Springer Berlin Heidelberg, 2010: 158–175.

[14] Kiraz M S, Bingöl M A, Karda S, *et al.*. Anonymous RFID authentication for cloud Services[J]. *International Journal of Information Security Science*, 2012, 1(2): 32–42.

[15] Camenisch J and Groth J. Group Signatures: Better Efficiency and New Theoretical Aspects[M]. Security in Communication Networks, Berlin Heidelberg Springer, 2005: 120–133.

[16] Camenisch J and Lysyanskaya A. A Signature Scheme with Efficient Protocols[M]. Security in Communication Networks, Berlin Heidelberg Springer, 2003: 268–289.

[17] Camenisch J and Stadler M. Efficient group signature schemes for large groups[C]. Advances in Cryptology-CRYPTO'97, Berlin Heidelberg Springer, 1997: 410–424.

[18] Goldreich O and Rosen V. On the security of modular exponentiation with application to the construction of pseudorandom generators[J]. *Journal of Cryptology*, 2003, 16(2): 71–93.

[19] Pointcheval D and Stern J. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396.

[20] 李树国, 周润德, 冯建华, 等. RSA 密码协处理器的实现[J]. 电子学报, 2001, 29(11): 1441–1444.
Li Shu-guo, Zhou Run-de, Feng Jian-hua, *et al.*. Implementation for RSA cryptography coprocessor[J]. *Acta Electronica Sinica*, 2001, 29(11): 1441–1444.

[21] Li Hui-yun. Development and Implementation of RFID Technology[M]. Vienna, Austria, I-Tech Education and Publishing KG, 2009: 1–12.

[22] Chae H J, Salajegheh M, Yeager D J, *et al.*. Maximalist Cryptography and Computation on the WISP UHF RFID Tag [M]. Wirelessly Powered Sensor Networks and Computational RFID, Springer New York, 2013: 175–187.

谢　润：　男，1976 年生，博士，副教授，主要研究领域为密码学、信息安全.

许春香：　女，1965 年生，博士生导师，教授，主要研究领域为密码学、信息安全、安全电子商务.

陈文杰：　女，1989 年生，研究方向为 RFID 认证协议.