RFID安全防碰撞搜索协议的设计与分析

曹 峥[1] 杨 林[2] 谢 辉[1]
(西安电子科技大学计算机学院 西安 710071)[1] (解放军总参第61研究所 北京 100039))[2]

摘 要 针对射频识别(RFID)搜索协议的特殊性,对RFID搜索协议的安全需求进行了扩展,并根据扩展后的安全需求,对原先的SSP协议进行一些必要的安全性增强和改进,提出了一种可防碰撞的RFID安全搜索协议,称之为SSP$^+$协议。对SSP$^+$协议的安全性分析表明,改进后的RFID搜索协议不仅能满足隐私保护、匿名、并发安全、防追踪等一般性的安全需求,还能消除因碰撞问题造成的安全隐患,满足了防碰撞这一搜索协议独特的安全需求。

关键词 射频识别,搜索协议,安全,防碰撞
中图法分类号 TP309 **文献标识码** A

Design and Analysis of Secure Anti-collision Search Protocol for RFID

CAO Zheng[1] YANG Lin[2] XIE Hui[1]
(School of Computer, Xidian University, Xi'an 710071, China)[1]
(61 Institute of General Staff of the Chinese People's Liberation Army, Beijing 100039, China)[2]

Abstract According to the particularity of search protocol for RFID, its security requirements were extended in this paper. Then, on the basis of the extended security requirements, some security enhancements and improvements on the original SSP protocol were achieved, and a secure anti-collision search protocol for RFID called SSP$^+$ protocol was proposed. Subsequently, based on security analysis of SSP$^+$ protocol, it was proved that this improved protocol can not only provide general security requirements, such as privacy protection, anonymity, untraceability, but also eliminate security risk caused by collision, thereby meeting anti-collision that is the unique security requirement on search protocol.

Keywords Radio frequency identification (RFID), Search protocol, Security, Anti-collision

1 引言

射频识别[1](Radio Frequency Identification,简称RFID)是自动识别技术的一种,是由读写器(reader)通过无线射频信号对标签(tag)进行识别。识别过程中,读写器不必与被识别对象直接接触,通过对被识别对象附着的标签非触式及时信息进行感知,就能瞬时完成信息的输入和处理,能快速、及时、准确地采集和处理信息。目前,RFID技术广泛应用于外贸、自动收费、零售、物流、国防等领域,它的安全问题越来越成为关注的焦点。

安全协议[2]是借助于密码算法为有安全需求的各方预先规定一系列步骤,安全、有效地实现密钥分配、身份认证、访问控制等特定目的。而对于RFID安全搜索协议而言,就是要在一组RFID标签中,准确判定某一特定标签是否存在并获取其相关的完整信息,同时协议的攻击者在整个协议过程中无法获得任何有价值的信息或线索。一种传统的办法是通过RFID认证协议逐个认证每一个标签,直至发现目标标签。这样做固然也可以实现搜索的功能,但效率极低且并发性很差,尤其是当组内存在大量标签的情况下,其效率是不能容忍的,因此有必要设计出专门的搜索协议。

当前,除了文献[3-7]涉及到RFID搜索协议,这方面的研究几乎还是空白。文献[3]设计了无需后端数据库的协议,它可以实现搜索功能,但它不是专门的搜索协议。文献[4]设计了专门的搜索协议,但不是轻量级的协议。文献[5]设计出一种轻量级的协议,该协议能满足一般性的安全需求,但需要后端数据库的参与,以牺牲空间的代价实现时间效率的提高。文献[5]对RFID搜索协议在隐私保护、匿名、防追踪、防窃听这几种安全需求方面进行了定义,而这些也都是RFID认证协议[8-11]同样具有的一般性的安全需求。文献[6]则综合上述各文献方案之优点,设计了一种低成本的无需后端数据库参与的RFID搜索协议,但其仍然只能满足同样的安全需求。文献[7]对RFID搜索协议的安全需求做了一些扩展,提出了并发安全的需求,并用通用可组合理论[9,12-14]加以证明。上述文献都没考虑到搜索协议在防碰撞方面的安全需求,所以不够全面。

搜索协议与认证协议不同,认证协议中认证双方是明确的一对一关系。但是,搜索协议是从大量的RFID标签中找到"目标"标签,当读写器发出"搜索"的广播信息后,群组内的所有标签都会进行各自的计算,最后由所谓的"目标"标签做出响应。可以看出,RFID搜索协议是典型的一对多的协议,

到稿日期:2013-06-24 返修日期:2013-09-09 本文受国家自然科学基金项目(60573036)资助。
曹 峥(1977—),男,博士生,主要研究方向为信息安全;杨 林 男,研究员,博士生导师,主要研究方向为信息安全;谢 辉 男,博士生,主要研究方向为信息安全。

针对搜索协议的特殊性，搜索协议还应当考虑到防碰撞方面的安全需求，首先必须分析搜索协议的碰撞问题，以及它对协议安全性的影响。

2 碰撞问题

RFID技术被日益广泛地应用到各个领域，尤其在商业、物流等快速流通的领域，对RFID的时效性要求比较高，读写器对标签的搜索与识别必须在瞬间完成。因此，RFID标签的成本与存储空间都必须尽量小，相应地，RFID的密钥算法与密钥长度就受到了很大限制。而另一方面，这些领域的规模在逐渐膨胀，同一个群组内必然存在大量标签，再加上搜索协议又是典型的一对多关系，因而在某一个时间节点，极有可能出现两个或两个以上标签实时密钥或隐私信息相同的情况。如果安全协议在设计时没有考虑防范这种情况，那么密钥的碰撞会引发响应碰撞，结果可能是多个标签同时响应。最为严重的结果是，如果协议设计得不好，一旦发生碰撞，就会造成此协议后的每一轮都发生连环碰撞。从安全性方面考虑，如果几个标签连续每轮都发生碰撞，攻击者就可以将其区别于其它标签，从而实施有效的跟踪。当前RFID的密钥长度通常在32位至48位之间，在某些领域甚至只有16位，随着技术进步与成本的降低，将来RFID的密钥长度可能会有所提高，但破解时的计算速度也在同步提高，所以如果不从协议的设计上加以解决，碰撞问题将会长期伴随于RFID技术。

2.1 响应碰撞与连环响应碰撞

为说明连环响应碰撞发生的过程，以文献[6]中提出的SSP协议为例，该协议的运行过程在文献[6]中有完整描述，由于篇幅有限，这里只说明响应碰撞与连环响应碰撞是如何发生的。不妨以两个标签发生碰撞的情况为例。

比方说，在第 s 轮协议中，标签 α 是 R_i 的搜索目标，该标签当时的密钥值为 $k_{i\alpha}$，在协议的第一步中从 R_i 处接收到一个广播的随机数 r^s，然后计算出 $f(k_{i\alpha},r^s)$的值。在第 $t(s<t)$ 轮协议中，标签 β 是 R_i 的搜索目标，该标签当时的密钥值为 $k_{i\beta}$，在协议的第一步中从 R_i 处接收到一个广播的随机数 r^t，然后计算出 $f(k_{i\beta},r^t)$的值。

然而，巧合的是 $f(k_{i\alpha},r^s)=f(k_{i\beta},r^t)=r^-$，本文2.2节将说明这种巧合发生的概率是很大的。于是，依照SSP协议的过程描述，无论是第 s 轮协议中的标签 α，还是第 t 轮协议的标签 β，都把 r^- 分解成 r_1^-、r_2^-、r_3^-，其中的 r_3^- 用以更新密钥。因此在第 t 轮之后，一旦随后的某一轮是以标签 α 或标签 β 中的任何一个为目标标签，响应碰撞的发生不可避免。

比方说，在随后的第 w 轮($s<t<w$)，标签 β 又一次成为 R_i 的搜索目标。由于在之前的第 s 轮和第 t 轮协议结束时，标签 α 和标签 β 分别把各自的密钥更新为相同的 r_3^- 的值，因此在第 w 轮协议开始时两个标签的实时密钥值 $k_{i\alpha}=k_{i\beta}$。在第 w 轮协议的第一步，R_i 将向群组内的所有标签广播 r 的值和一个随机数 r^w。作为目标标签的 β 计算出 $f(k_{i\beta},r^w)=r$，于是向 R_i 发出响应。但与此同时，不是目标标签的 α 也计算出 $f(k_{i\alpha},r^w)=r$，于是也向 R_i 发出响应。这样，在协议运行到第 w 轮时，标签 α 和标签 β 发生响应碰撞。

由于SSP协议没有采取防碰撞的设计，在第 w 轮时标签 α 与标签 β 都计算出相同的 r，又把 r 分解成相同的 r_1、r_2、r_3，并都以 r_3 的值来更新 $k_{i\alpha}$ 或 $k_{i\beta}$，得到的 $k_{i\alpha}^+=k_{i\beta}^+=r_3$。同样的道理，在第 w 轮之后的每一轮，只要是该轮中标签 α 或标签 β 中的任何一个成为 R_i 的搜索目标，这两个标签都会根据相同的密钥与从 R_i 处接收的一个相同的随机数计算出一个相同的 r^+，将再次发生响应碰撞，并再以 r^+ 分解出的相同的 r_3^+ 更新成相同的新密钥。于是，从第 w 轮开始，响应碰撞将在标签 α 与标签 β 之间接连发生，从而造成连环响应碰撞。

2.2 响应碰撞发生的概率

设RFID标签与读写器的会话密钥使用的是 m 位的伪随机密钥，该密钥的样本空间为 Q，Q 包含的样本个数为 q，且 $q\lesssim 2^m$。n 为一个组中包含的标签个数，$K_1,K_2,\cdots,K_n$ 分别为这 n 个标签各自对应的当前密钥值，因此它们就是 Q 中的 n 个样本。$x_1,x_2,\cdots,x_q$ 为 Q 中所有可能的样本值。设 $p(x)$ 是 Q 中随样本值 x 变化的概率密度函数，由于密钥是伪随机数，因此 $p(x)$ 是 Q 上的均匀分布，有

$$p(x)=\begin{cases}1/q, & x\in Q\\ 0, & x\notin Q\end{cases}$$

即当密钥初始分配时，对于任意 K_j，$K_j\sim p(x)$。

由于RFID的密钥长度通常在32位至48位之间，且不说系统为每个标签分配初始密钥时存在某两个或多个标签分配相同密钥的情况，即使初始密钥各不相同，协议经过数轮运行之后出现上述情况的概率也是相当大的。

仍然以SSP协议为例，假设第 s 轮协议的搜索目标为标签 j，本轮运行前标签 j 的密钥为一确定值 K_j，r^s 是 R_i 随机产生的一个伪随机数，f 是平均概率分布的伪随机函数，但 f 中变量与函数值的对应关系是确定的。于是，当第 s 轮计算 $r=f(k_j,r^s)$，r 的值将随着 r^s 的值而变化。由于 r^s 是 R_i 随机产生的，产生前有 $p(r^s=x_k)=1/q,k\in[1,q]$，即 r^s 服从平均分布，因此，r 的值也服从平均分布。接下来，把 r 的值分解成 r_1、r_2、r_3，当然 r_1、r_2、r_3 都服从平均分布，又 $|r_1|=|r_2|=|r_3|=m$，所以有

$$r_1\sim p(x),r_2\sim p(x),r_3\sim p(x)$$

依照SSP协议，以 r_3 更新 K_j，则更新后的 $K'_j\sim p(x)$。不失一般性，当协议运行到 s 轮之后的第 t 轮，无论标签 j 是否作为目标标签被更新过，以 K_j' 表示标签 j 的最新密钥，则有 $K_1',K_2',\cdots,K_n'\sim p(x)$。

由于 n 个标签是无差别的，且有过更新的标签彼此不参与其它标签的密钥更新过程，所以 K_1'、K_2'、$\cdots$、K_n' 是相互独立的。

设 P_N 为第 t 轮不会发生响应碰撞的概率，P_C 为第 t 轮会发生响应碰撞的概率，即 $P_C=1-P_N$。

在样本空间 Q 上任选 n 个互不相等的值的全排列数为 P_q^n，所以

$$P_N=P_q^n/q^n$$

其中，$P_q^n=\dfrac{q!}{(q-n)!}$

因此得出

$$P_c=1-\frac{(q-1)!}{q^{n-1}(q-n)!}$$

可以看出，当 q 的值固定，且 $n\ll q$，则 n 的值越大，P_N 越小，P_C 越大。而且，在 n 足够大但仍然 $n\ll q$ 的情况下，$P_C\approx 1$。例如，密钥位数为32位，取 $q=3.6\times10^9<2^{32}$，随着 n 值的变化，P_C 值的变化如表1所列。

表 1　密钥位数为 32 位时 P_C 值随 n 值的变化情况

n	2000	5000	10000	20000
P_C	0.000555	0.003466	0.013792	0.054038
n	50000	100000	200000	400000
P_C	0.293348	0.750648	0.996134	≈1

从表 1 可以看出，若 $q=3.6\times10^9$，则当 n 的值达到 2000 以上时，P_C 的值是不可忽略的。当 n 的值达到 200000 以上时，P_C 的值几乎等于 1，此时 $n:q\approx1:20000$。表 1 中统计的仅仅是某一轮内发生响应碰撞的概率，如果协议多进行几轮，那么对于同一对(n,q)值来说，多轮中至少有一轮发生响应碰撞的概率将更大。

在标签众多的 RFID 系统中，发生响应碰撞的概率是不可忽略的。如果协议设计得不好，正如 2.1 节所述的那样，响应碰撞必然会引起连环响应碰撞。一旦发生连环响应碰撞，攻击者将很容易地统计出规律，对发生碰撞的标签进行跟踪，这样的搜索协议将是不安全的。

3　改进后的 SSP$^+$ 协议

影响搜索协议安全性的是连环响应碰撞，偶尔一次的响应碰撞会使该轮协议运行失败，但不会影响协议的安全性。当然，通过增加秘密参数的个数，可以以 $\sqrt{\ }$ 关系减少发生响应碰撞的概率，进而减少连环响应碰撞的概率，在文献[7]中就是这么做的。然而，不论这个概率如何小，只要发生响应碰撞，就必然会发生连环响应碰撞，从而影响协议的安全性。因此，只靠增加秘密值的个数（增加得太多会影响计算效率）来减少响应碰撞的概率，只能治标不能治本。为了在响应碰撞发生后，杜绝响应碰撞在接下来的一轮中再次发生，使攻击者不能统计出任何有价值的信息，必须对协议进行防碰撞的设计，确切地说是防连环响应碰撞的设计。

本文将对 SSP 协议进行进一步的改进，改进后的协议称为 SSP$^+$ 协议。SSP$^+$ 协议与文献[7]中的协议具有同样的可信设置，但在协议的秘密值参数的更新、非目标标签响应概率值的设定方面做了一些必要的改进，改进后的协议杜绝了多标签连环响应碰撞的隐患，消除了遭受跟踪攻击的危险。

3.1　协议的改进方案

改进后的 SSP$^+$ 搜索协议描述如下：

读写器 R_i 内部存储一个列表，列表的每条记录对应组内的一个标签，每条记录有 3 个字段，分别是 k_{ij}、r_{ij} 及标签不变的 ID 值。每个标签中存储着自己的实时 k_{ij}、r_{ij} 值与不变的 ID 值。

第 1 步　R_i 生成 1 个长度与 r_{ij} 相同的随机数 r_b，计算 $r=f(k_{ij},r_{ij}\oplus r_b)$。随后按照一定的规则，把 r 分解成 4 个随机数 r_1、r_2、r_3、r_4，然后对组中所有标签广播随机数 r_1 和 r_b。

第 2 步　当 T^*（T^* 表示组中任一标签）接收到 r_1 和 r_b 后，利用自己的密钥 k_{i*} 以及随机数 r_{i*} 计算 $r^*=f(k_{i*},r_{i*}\oplus r_b)$，然后按相同规则把 r^* 分解为 4 个随机数 r_1^*、r_2^*、r_3^*、r_4^*，并验证 r_1^* 是否与 r_1 相等。若 $r_1^*=r_1$，则 T^* 正是目标标签 T_j，于是 T_j 用 r_3^* 更新 k_{ij}，用 $r_4\oplus ID_*$ 而不是用 r_4 来更新 r_{ij}，并向 R_i 发送 r_2^*；若 $r_1^*\neq r_1$，则 T^* 不是目标标签 T_j，T^* 仍以 p 的概率向 R_i 发送自己计算出来的 r_2^*，而且 T^* 不做任何更新。

第 3 步　当 R_i 接收到数个做出回应的标签发出各自计算的 r_2^* 后，验证每个 r_2^* 是否和 r_2 相等。若 $r_2^*=r_2$，则搜索成功，R_i 判定与该 $r_2{}^*$ 对应的标签就是目标标签 T_j，随即在列表 L_i 中用 r_3 更新 T_j 的密钥 k_{ij}，但不是用 r_4 而是用 $r_4\oplus ID_*$ 更新随机数 r_{ij}。当然，若 $r_2^*\neq r_2$，则搜索失败。

在协议的第 2 步，如果让组内所有的标签都做出回应，则无疑会加大 R_i 的负担，R_i 方不可能象多个标签那样同时做计算，它必须对每个回应的 r_2^* 值逐一进行比较；但如果让组内所有非目标标签都不做回应，则将会暴露目标标签的踪迹，因此 p 必须选择一个恰当的值。在 SSP 协议中，只计算了至少有 1 个非目标标签对 R_i 做出响应的概率为 λ，$\lambda\leqslant1-(1-p)^{q-1}$，于是就得出 p 的取值范围为 $1-(1-\lambda)^{1/q-1}\leqslant p<1$。然而，这样的结论是站不住脚的。比方说，只有一个非目标标签做出响应，这也符合了至少一个非目标标签做出响应的条件，但这意味着攻击者有一半的概率知道哪一个标签是本轮协议的目标标签，这无疑是不安全的。

假设一组标签的个数为 q，正常情况下有 $q-1$ 个非目标标签，每个标签独立地以 p 概率响应，以 $1-p$ 的概率保持沉默。设 Y 为 $q-1$ 个非目标标签中做出响应的个数，$Y\in[0,q-1]$，Y 的概率密度函数为：

$$P(Y=u)=C_{(q-1)}^{u}p^u(1-p)^{q-1-u}$$

很显然，Y 是一个服从于二项分布的离散性随机变量，即 $Y\sim\mathcal{B}(q-1,p)$。

于是，可以得到 Y 的分布函数：

$$F_Y(u)=\sum_{Y=1}^{u}C_{(q-1)}^{Y}p^Y(1-p)^{q-1-Y}$$

为了既不加重 R_i 的负担又不暴露目标标签的踪迹，假定 Y 的合理取值范围为$[a,b]$，并使 $P(Y\in[a,b])>0.99$（0.99 为理想的阈值），即 $F_Y(b)-F_Y(a)>0.99$。根据以上假定求出 p 的取值，只有这样求出的 p 才能最大限度地提高 R_i 效率，并保证目标标签不会暴露。关于 a 与 b 的取值范围，则可以视应用领域的实际需要以及 RFID 技术的发展状况而定。

3.2　改进协议的安全性分析

与文献[6]的 SSP 协议比较，文献[7]只是减少了连环响应碰撞发生的概率，仍然没有采取防碰撞的设计。本文则进行了这方面的设计，根据本文 3.1 节提出的密钥更新方案，当某轮发生响应碰撞后，在下一轮便消除了发生连环响应碰撞的可能性。

比方说，某一轮有两个标签 α 和 β（当然也可以是多个）发生碰撞，也就是说它们计算出的 r 值相同，即 $r^\alpha=r^\beta$。按照相同的分解规则，将 r^α 分解为 r^{α_1}、r^{α_2}、r^{α_3}、r^{α_4}，将 r^β 分解为 r^{β_1}、r^{β_2}、r^{β_3}、r^{β_4}，则必然有：

$$r^{\alpha_3}=r^{\beta_3},r^{\alpha_4}=r^{\beta_4}$$

接下来，以 r^{α_3} 更新 $k_{i\alpha}$ 得到 $k'_{i\alpha}$，并以 r^{β_3} 更新 $k_{i\beta}$ 得到 $k'_{i\beta}$，$k'_{i\alpha}=k'_{i\beta}$。

同时，以 $r^{\alpha_4}\oplus ID_\alpha$ 更新 $r_{i\alpha}$ 得到 $r'_{i\alpha}$，并以 $r^{\beta_4}\oplus ID_\beta$ 更新 $r_{i\beta}$ 得到 $r'_{i\beta}$。由于每个标签的 ID 值各不相同，因此 $ID_\alpha\neq ID_\beta$，又有 $r^{\alpha_4}=r^{\beta_4}$，则必然有 $r^{\alpha_4}\oplus ID_\alpha\neq r^{\beta_4}\oplus ID_\beta$，即 $r'_{i\alpha}\neq r'_{i\beta}$。

在下一轮，根据两标签的 k'_{ij} 或 r'_{ij} 的值是否相同，可以分为 3 种情况：

①如果 $k'_{i\alpha}=k'_{i\beta}$ 且 $r'_{i\alpha}=r'_{i\beta}$，而 r_b' 是从 R_i 得到的广播值，则必然有 $f(k'_{i\alpha},r'_{i\alpha}\oplus r_b')=f(k'_{i\beta},r'_{i\beta},\oplus r_b')$，即$(r^\alpha)'=$

$(r^{\beta})'$，于是标签 α 与标签 β 在下一轮(特指以两标签之一作为搜索目标的下一轮)必将再次发生响应碰撞。

②如果 $k'_{i\alpha}\neq k'_{i\beta}$ 且 $r'_{i\alpha}\neq r'_{i\beta}$，则有 $0<P[(r^{\alpha})'=(r^{\beta})']<1$，尽管这个概率很小，但两个标签在下一轮仍然有发生响应碰撞的可能。

③如果 $k'_{i\alpha}=k'_{i\beta}$ 但 $r'_{i\alpha}\neq r'_{i\beta}$，按照协议的设定，二维函数 f 对其中任意一维变量服从平均分布的属性，则必然有 $f(k'_{i\alpha}, r'_{i\alpha}\oplus r_b')\neq f(k'_{i\beta}, r'_{i\beta}\oplus r_b')$，即 $(r^{\alpha})'\neq(r^{\beta})'$，于是这两个标签不会在下一轮再次发生响应碰撞。

很显然，本文的设计正好符合了第 3 种情况，所以从根源上彻底避免了连环响应碰撞的可能性。

其次，由于更新 k_{ij} 与 r_{ij} 这两个秘密值的过程是在标签和 R_i 的硬件内部进行的，ID 值从来没有以明文或加密的方式进入无线环境的通信过程中；因此，标签的 ID 值没有暴露的危险，并且对秘密值更新方案的改进也没有破坏文献[6]中已经证明过的安全性。为了更加保险起见，可以赋予每个标签一个假名，记作 metaID，而 metaID=hash(ID)，更新秘密值时以 $r_4\oplus$ metaID 更新 r_{ij} 的值。

另外，即使攻击者在下一轮幸运地破解了 r'_{ij} 的值，他除非在本轮同样幸运地得到了 r_4 的值，才能在同时掌握 r_4 与 r'_{ij} 两个值的情况下破解 metaID。而要得到 r_4 的值，则必须同时得到本轮的 k_{ij} 与 r_{ij} 的值，即意味着在本轮该标签就已经被攻破，这样就产生了一个悖论，因而 r_4 是安全的。所以，即使下一轮的 r'_{ij} 的值被破解，但由于本轮的 r_4 是安全的，metaID 必然是安全的，而标签的 ID 值更加是安全的。因此，更新后的 SSP$^+$ 协议既具有前向安全性，也具有后向安全性。

综上所述，经过改进后的 SSP$^+$ 协议，除继承了 SSP 协议的安全性能之外，还避免了连环响应碰撞的安全隐患，具有前向与后向安全性。所以，SSP$^+$ 协议是安全的。

结束语 随着 RFID 技术日益广泛地应用于人们的生产、生活，需要从大量的 RFID 标签中快速、安全地对目标标签进行搜索，因此设计安全、高效的 RFID 安全搜索协议具有重大的现实意义。本文根据这种现实需要，提出了搜索协议中容易被人们忽视的碰撞问题，并分析了碰撞问题发生的概率及可能引发的安全性问题。然后，在 SSP 协议的基础上，对其进行安全性扩展与改进，改进后的 SSP$^+$ 协议很好地弥补了这一缺陷，消除了遭受追踪攻击的隐患。

参 考 文 献

[1] 孙其博，刘杰，黎彝，等. 物联网：概念、架构与关键技术研究综述[J]. 北京邮电大学学报，2010，33(3)：1-9

[2] 卿斯汉. 安全协议 20 年研究进展[J]. 软件学报，2003，14(10)：1740-1752

[3] Tan C C, Sheng B, Li Q. Serverless search and authentication protocols for RFID[C]// 5th IEEE International Conference on Pervasive Computing and Communications. New York: IEEE Press, 2007: 24-29

[4] Ahamed S, Rahman F, Hoque E, et al. S^{3}PR: secure serverless search protocols for RFID[C]// International Conference on Information Security and Assurance. Hawaii: IEEE Press, 2008: 187-192

[5] Kulseng L, Yu Z, Wei Y. Lightweight secure search protocols for low-cost RFID systems[C]// 29th International Conference on Distributed Computing Systems. Washington: IEEE Press, 2009: 40-48

[6] 邓淼磊，衡晓鹏，鲁志波. 安全的 RFID 搜索协议[J]. 西安通信学院学报，2009，8(5)：78-81

[7] 曹峥，邓淼磊. 通用可组合的 RFID 搜索协议[J]. 华中科技大学学报：自然科学版，2011，39(4)：56-59

[8] van Le T, Burmester M, Medeiros B. Universally composable and forward secure RFID authentication and authenticated key exchange[C]// Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2007: 242-252

[9] Burmester M, van Le T, Medeiros B. Provably secure ubiquitous systems: Universally composable RFID authentication protocols [C]// Proc. of the 2nd International Conference on Security and Privacy in Networks. Maryland: IEEE Press, 2006: 176-186

[10] 邓淼磊，马建峰，周利华，等. RFID 匿名认证协议的设计[J]. 通信学报，2009，30(7)：24-31

[11] Lee S M, Hwang Y J, Lee D H. Efficient authentication for low-cost RFID systems[C]// Proc. of the International Conference on Computational Science and Its Applications (ICCSA2005). Berlin: Springer-Verlag, 2005: 619-627

[12] Canetti R. Universally composable security: a new paradigm for cryptographic protocols[C]// 42th IEEE Annual Symposium on Foundations of Computer Science. Oakland: IEEE Press, 2001: 136-145

[13] Kurosawa K, Furukawa J. Universally composable undeniable signature[C]// Proc. of ICALP'08. Berlin: Springer-Verlag, 2008: 524-535

[14] Canetti R, Herzog J. Universally composable symbolic analysis of mutual authentication and key-exchange protocols[C]// Theory of Cryptography Conference. Berlin: Springer-Verlag, 2006: 380-403

(上接第 115 页)

[13] Panda M, Patra M R. Network Intrusion Det-ection Using Naive Bayes [J]. International Journal of Computer Science and Network Security, 2007, 7(12): 258-263

[14] Farid D M, Harbi N, Rahman M Z. Combining Naive Bayes and Decision Tree for Adaptive Intrusion Detection [J]. International Journal of Network Security & Its Applications, 2010, 2(2): 12-25

[15] 江凯，高阳. 并行化的半监督朴素贝叶斯分类算法[J]. 计算机科学与探索，2012，6(10)：912-918

[16] 欧阳泽华，郭华平，范明. 在逐渐缩小的空间上渐进学习朴素贝叶斯参数[J]. 计算机应用，2012，32(1)：223-227

[17] 周晓庆，肖顺文，肖建琼，等. 一种基于改进的权值调整技术数据源分类算法研究[J]. 计算机应用研究，2012，29(3)：916-918