基于 LPN 问题的 RFID 安全协议设计与分析

唐　静　　姬东耀
(中国科学院研究生院信息安全国家重点实验室　北京　100049)

摘　要：该文对现有的基于 LPN 问题的 RFID 安全协议进行了系统分析，总结了这类协议存在的一些设计缺陷。为了克服这类协议中存在的安全漏洞，对其中一个最新版本的协议 HB· 进行改进，设计了一个新的 RFID 安全协议 HB$^{\#}$，并在随机预言模型下给出了新协议的归约性证明。

关键词：射频身份识别；LPN；认证；归约
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)02-0439-05

Design and Analysis of Security Protocols for RFID Based on LPN Problem

Tang Jing　　Ji Dong-yao
(*State Key Laboratory of Information Security*, *Graduate University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract: The existing security protocols for RFID based on LPN problem are systematically analyzed and their secure vulnerabilities are summarized. In order to conquer these security leaks, a new RFID security protocol named HB· is designed, which is an improved version of HB· protocol. Finally, it is proved that HB$^{\#}$ protocol is secure in the random oracle model.

Key words: RFID(Radio Frequency IDentification); LPN(Learning Parity in the Presence of Noise); Authentication; Reduction

1　引言

射频身份识别 (Radio Frequency IDentification，RFID) 是一种非接触式的自动识别技术，将微芯片嵌入产品中，扫描器通过射频信号自动识别目标对象并获取相关数据，具有无线即时读取、大容量和高速数据处理等能力以及高度自动化的特点。这个过程比传统条形码技术具有更好的安全性，可以应用于支付系统、物流和供应管理、访问控制、道路自动收费以及货币和护照的防伪等。目前，RFID 系统已经成为普适计算环境的重要组成部分。

RFID 系统主要由 Tag，Reader 及后台数据库 3 个部分组成。Reader 发射特定频率的无线电波给 Tag，Tag 接收到以后将其内部的数据送出，此时 Reader 便依序接收数据并认证 Tag。

低成本的 Tag 设备具有一些局限性，例如体积小、计算能力低、存储空间少、源供给有限等，从某种意义上来说，这些局限性与人类类似。例如，我们不能记住很长的密码也不能执行大的计算，类似的，Tag 只能存储长度为 32–128 bit 的密钥，用于安全的门电路也不能超过 2000 个。

因为他们的类似性，RFID 协议设计者们考虑将“human -computer”认证协议应用于这样的普适计算环境中，同时积极寻找合适的计算问题来构建安全的认证协议。LPN (Learning Parity in the Presence of Noise)问题是为数不多的“矢量子集求和”困难问题，对计算量和存储量要求不高，适合 Tag 这样的设备，因此受到了设计者们的青睐。2001 年，Hopper 和 Blum 提出了第 1 个基于 LPN 问题的 RFID 认证协议，称为 HB 协议[1,2]。随后又竞相出现了 HB^{+}[2]，HB^{++}[3,4]等协议，这些都是 HB 协议的改进版本。但是这些协议并不完美，分析表明它们都存在安全漏洞，如何克服这些缺陷，设计并证明一个安全的，高效的 RFID 认证协议是本文的主要目的。

本文提出了一个新的基于 LPN 问题的 RFID 认证协议——HB$^{\#}$，并在随机预言模型下证明了其安全性。本文第 2 节主要介绍 LPN 问题和基于 LPN 问题提出的 HB 类协议；第 3 节针对 HB^{+}协议的安全缺陷提出了一个新的协议 HB$^{\#}$；第 4 节给出了具体的安全性证明；最后是结束语。

2　LPN 问题和 HB 类协议

2.1 LPN 问题

假设 User(U)与 Computer(C)之间共享 k 比特密钥 $\boldsymbol{x}$，U 想向 C 证明自己的身份，认证过程如下：C 产生一个随机的 k 比特矢量 $\boldsymbol{a}$ 发送给 U，U 收到后计算 $c=\boldsymbol{a}\bullet\boldsymbol{x}$ 响应给 C(其中 $\bullet$ 表示 GF(2)上的点乘)，C 收到后检查，如果 $c=\boldsymbol{a}\bullet\boldsymbol{x}$ 则认证通过，反之不通过。在一轮认证中，C 接受一个假冒

2007-07-26 收到，2008-12-28 改回
国家自然科学基金(90604010)资助课题

用户的概率是 1/2，重复 r 轮后，理论上 C 接受一个假冒用户的概率是 2^{-r}。很不幸，被动攻击者只要观察 $O(k)$ 次“挑战-响应”对，就可以通过高斯消元法解出共享密钥 $\boldsymbol{x}$，进而伪装成 U。

我们引入噪声参数 $\eta \in (0,1/2)$，在 U 的响应中参入一些错误的回答，这样被动攻击者就无法简单的利用高斯消元法得到密钥 $\boldsymbol{x}$，这就是 LPN 问题，即噪声存在下的奇偶性问题。LPN 问题在不同的应用环境中有不同的描述，如 MDP 问题[5]，Syndrome 译码问题[6]等都是 LPN 问题的变型。下面，用矩阵运算来定义 LPN 问题。

定义 1(LPN 问题) 假设 $\boldsymbol{D}$ 是一个随机的 $q \times k$ 比特矩阵，$\boldsymbol{x}$ 是一个随机的 k 比特矢量，噪声参数 $\eta \in (0,1/2)$，$\boldsymbol{v}$ 是一个随机的 q 比特矢量，其汉明重量 $|\boldsymbol{v}| \le \eta q$。已知 $\boldsymbol{D}$，η 以及 $\boldsymbol{z} = (\boldsymbol{D}\bullet\boldsymbol{x}) \oplus \boldsymbol{v}$，找一个 k 比特矢量 $\boldsymbol{x}'$ 满足 $|(\boldsymbol{D}\bullet\boldsymbol{x}') \oplus \boldsymbol{v}| \le \eta q$。

LPN 问题已经被证明是 NP-Hard[6,7]，同时要找到一个满足超过一半“挑战-响应”对的 $\boldsymbol{x}'$ 也是 NP-Hard[8]。尽管 Kearns[9]说明了随机的统计询问模型下 LPN 问题是困难的，但是在挑战矩阵完全随机的情况下，LPN 问题的困难性还没有被证明。

Blum 等人[7]的研究结果表明，已知一个随机的 k 比特矢量 $\boldsymbol{a}$，如果敌手可以以 k^{-c} 的优势得到 $\boldsymbol{a}\bullet\boldsymbol{x}$ 的值，那他就能解 LPN 问题。这就是一般的将某个协议规约到 LPN 问题的方法。他们后来又证明了 LPN 问题的伪随机性和 Log 一致性并推测了 LPN 问题的困难性[1,10]。最著名的解 LPN 问题的算法是由 Blum 等提出的 BKW 算法，其计算复杂度为 $2^{O\left(\frac{k}{\log k}\right)}$ [11]。

2.2 HB 协议

HB 协议[1]是 Hopper 和 Blum 基于 LPN 问题提出的。一个完整的 HB 协议包括 r 轮，其中 r 是一个安全参数，Reader 与 Tag 共享 k 比特密钥 $\boldsymbol{x}$。Tag 拥有一个噪声发生器，以 $\eta \in (0,1/2)$ 的概率生成噪声 $v = \{0,1 \mid \text{prob}[v=1] = \eta\}$。一轮协议中，Reader 随机生成 k 比特序列 $\boldsymbol{a}$，发给 Tag，Tag 收到后计算 $z = (\boldsymbol{a}\bullet\boldsymbol{x}) \oplus v$ 发回去，Reader 检验是否 $z = \boldsymbol{a}\bullet\boldsymbol{x}$，其中 $\bullet$ 为矢量内积。这样进行 r 轮后，如果 Tag 响应错误的轮数小于 ηr，认证通过。具体的一轮协议流程如图 1 所示。

HB 协议执行过程简单，r 轮可以并行执行，硬件上也比较容易实现，计算 z 只需要 AND 和 XOR 两个操作，Tag 收到 $\boldsymbol{a}$ 后不用缓存可以直接计算，节省存储空间。噪声 v 也易产生[1]。

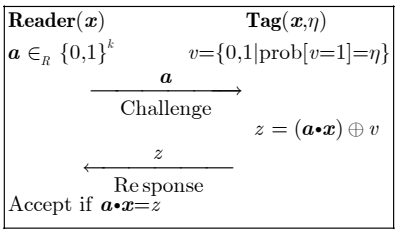

图 1 一轮 HB 认证协议

HB 协议在抗被动攻击方面的安全性可以规约到解 LPN 困难问题[1,2]，因此 HB 协议可以抵抗在线窃听等被动攻击，但是它并不能抵抗主动攻击。攻击者只要重复挑战 $O\left(\frac{1-\eta}{(1-2\eta)^2}\right)$ 次就可以以很大的概率得到 $\boldsymbol{a}\bullet\boldsymbol{x}$。进一步，攻击者选择 k 个特定的挑战向量，用高斯消元法解矩阵方程即可得到密钥 $\boldsymbol{x}$。

2.3 HB$^+$协议

为了解决 HB 协议中不能抵御主动攻击的问题，Juels 和 Weis 设计了 HB$^+$协议[2]。HB$^+$协议也是采用类似于 HB 协议的“挑战-响应”认证模式，与 HB 协议不同的是，HB$^+$协议中 Reader 与 Tag 之间增加了一个共享的 k 比特密钥 $\boldsymbol{y}$，相应地，z 的计算也有所不同；另外 HB$^+$协议中需要 Tag 首先产生 k 比特盲因子 $\boldsymbol{b}$ 发给 Reader。一轮 HB$^+$协议的过程如图 2 所示。

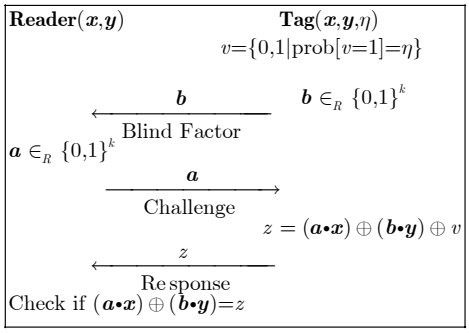

图 2 一轮 HB$^+$认证协议

同 HB 协议一样，r 轮后如果 Tag 回答错误的次数小于 ηr，Reader 就能认证 Tag。相比 HB 协议，HB$^+$协议仅需要多产生一个 k 比特随机向量，增加 k 比特存储空间，多计算 $2r$ 次 AND 和 XOR。

3 对 HB$^+$协议的改进

3.1 中间人攻击

尽管 Juels 和 Weis 证明了 HB$^+$协议在抗主动攻击方面的安全性[2]，但它的安全性还是受到了挑战。

2005 年，Henri Gilbert 等发现了一个简单的中间人攻击[12]，其过程见图 3。攻击者伪装成一个合法的 Tag，截获每一轮 Reader 发送的 $\boldsymbol{a}$，然后异或上同一个 k 比特矢量 $\boldsymbol{\delta}$，伪装成合法的 Reader 将 $\boldsymbol{a}' = \boldsymbol{a} \oplus \boldsymbol{\delta}$ 发送给 Tag。r 轮协议后如果认证通过，可以以很大的概率判断 $\boldsymbol{\delta}\bullet\boldsymbol{x} = 0$；如果认证无法通过，可以以很大的概率判断 $\boldsymbol{\delta}\bullet\boldsymbol{x} = 1$。这样，攻击者可以选择 k 个合适的 $\boldsymbol{\delta}$ 恢复出密钥 $\boldsymbol{x}$ 的每个比特。

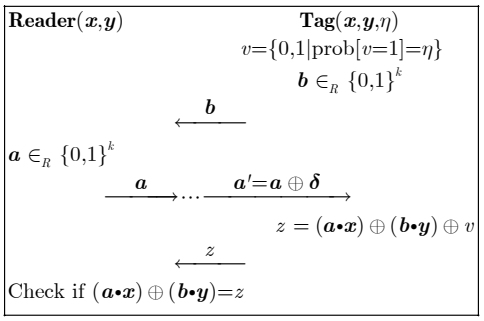

图 3　一轮 HB$^+$协议的中间人攻击

3.2 HB$^\#$协议

为了抵御上面的中间人攻击，本文在 HB$^+$协议的基础上进行改进，提出一个新的协议，暂时把它称为 HB$^\#$。

与 HB$^+$协议不同的是，HB$^\#$引入了一个非线性函数 f，假设 k 比特矢量 $\boldsymbol{a}=a_1,a_2,\cdots,a_{k-1},a_k$，$f(\boldsymbol{a})=f(a_1,a_2,a_3,\cdots,a_{k-1},a_k)=(a_1a_2,a_2a_3,\cdots,a_{k-1}a_k,a_ka_1)$，Tag 计算 $z=(f(\boldsymbol{a})\bullet\boldsymbol{x})\oplus(\boldsymbol{b}\bullet\boldsymbol{y})\oplus v$。这样挑战“$\boldsymbol{a}$”不再直接参与计算，又因为 $f(\boldsymbol{a}\oplus\boldsymbol{\delta})\neq f(\boldsymbol{a})\oplus f(\boldsymbol{\delta})$，所以攻击者就无法将 $\boldsymbol{\delta}$ 与密钥 $\boldsymbol{x}$ 联系起来。具体的一轮 HB$^\#$协议过程见图 4。

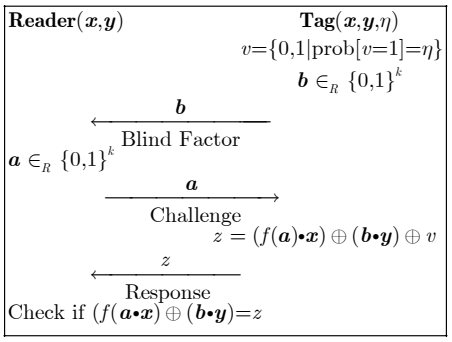

图 4 一轮 HB$^\#$认证协议

4　安全性分析

Blum[1]和 Weis[2]都证明了在随机预言模型下 HB 协议的安全性可以规约到解 LPN 困难问题。我们只要能够将 HB$^\#$协议的安全性规约到 HB 协议的安全性上，那么就可以进一步规约到 LPN 困难问题上，即证明了该协议的安全。

4.1 符号定义及攻击者模型

首先定义 HB 类协议的认证系统模型，它包括两个函数 (T,R)，分别代表 Tag 和 Reader。

在 HB 协议中 T 包含噪声参数 η，k 比特密钥 $\boldsymbol{x}$，q 个 k 比特矢量 $\boldsymbol{a}^{(i)}(i=1,\cdots,q)$，记为矩阵 $\boldsymbol{A}$，所以 Tag 函数为 $T_{x,A,\eta}$；R 仅包含 k 比特密钥 $\boldsymbol{x}$，所以 Reader 函数为 R_x。

HB 协议中只考虑被动攻击，在第 i 轮交互中：

$T_{x,A,\eta}(\ )\rightarrow(\boldsymbol{a}^{(i)},z)$；

$R_x(\boldsymbol{a},z)\rightarrow$ "accept"\"reject"。

在 HB$^\#$协议中，T 包含噪声参数 η，两个 k 比特密钥 $\boldsymbol{x}$ 和 $\boldsymbol{y}$，故 Tag 函数为 $T_{x,y,\eta}$；Reader 函数为 $R_{x,y}$。

HB$^\#$协议考虑主动攻击，在第 i 轮交互中：

$T_{x,y,\eta}(\boldsymbol{a}^{(i)})\rightarrow(\boldsymbol{b}^{(i)},z)$；

$R_{x,y}(\boldsymbol{a},\boldsymbol{b},z)\rightarrow$ "accept"\"reject"。

下面定义攻击者模型，不管在 HB 协议中还是在 HB$^\#$协议中，攻击者模型都是由 3 个部分组成：一个两阶段的敌手 A (A$^\#$)=($\mathrm{A}_{\mathrm{query}}$，$\mathrm{A}_{\mathrm{clone}}$)，Reader R，Tag T。在 query 阶段，敌手伪装成 Reader，$\mathrm{A}_{\mathrm{query}}$ 将 T 作为一个 oracle 进行询问，得到信息 σ；在 clone 阶段，敌手伪装成 Tag，根据 σ 和 $\boldsymbol{a}$，$\mathrm{A}_{\mathrm{clone}}$ 输出一个响应比特 z。这是 HB 协议中攻击者的模型，HB$^\#$协议中 $\mathrm{A}_{\mathrm{clone}}$ 要先输出盲因子 $\boldsymbol{b}$，继而根据 σ 和 $\boldsymbol{a}$ 输出一个响应比特 z。

HB$^\#$协议中的敌手 A$^\#$ 按如下步骤进行猜测实验：

(1)随机生成 k 比特密钥 $\boldsymbol{x}$，$\boldsymbol{y}$；

(2) $\mathrm{A}_{\mathrm{query}}$ 询问 $T_{x,y,\eta}$，交互多轮后得到信息 σ；

(3) $\mathrm{A}_{\mathrm{clone}}$ 利用 σ 和一些初始信息产生盲因子 $\boldsymbol{b}$；

(4)任意选择新鲜的 $\boldsymbol{a}$；

(5) $\mathrm{A}_{\mathrm{clone}}$ 结合 $\boldsymbol{a}$，$\boldsymbol{b}$，σ 输出对 z 的猜测。

Experiment $\mathrm{Exp}_{\mathrm{A}^\#}^{\mathrm{HB}^\#}[k,\eta,q]$：

$\boldsymbol{x},\boldsymbol{y}\in_R\{0,1\}^k$

$\mathrm{A}_{\mathrm{query}}(T_{x,y,\eta})\rightarrow\sigma$

$\mathrm{A}_{\mathrm{clone}}(\sigma,$"initiate"$)\rightarrow\boldsymbol{b}$

$\boldsymbol{a}\in_R\{0,1\}^k$

$\mathrm{A}_{\mathrm{clone}}(\sigma,\boldsymbol{a},\boldsymbol{b},$"initiate","guess"$)\rightarrow z$

在密钥长度为 k，噪声参数为 η，执行 q 轮的情况下，敌手 A$^\#$ 的优势：

$$\mathrm{Adv}_{\mathrm{A}^\#}^{\mathrm{HB}^\#}(k,\eta,q)=\left|\Pr[\mathrm{Exp}_{\mathrm{A}^\#}^{\mathrm{HB}^\#}[k,\eta,q]=\text{"accept"}]-1/2\right|$$

定义 t_1 为 $\mathrm{A}_{\mathrm{query}}$ 的计算时间，t_2 为 $\mathrm{A}_{\mathrm{clone}}$ 的计算时间，用 $\mathrm{A}^\#\in(t_1,t_2)$ 表示敌手 A$^\#$ 在时间 (t_1,t_2) 内，A$^\#$ 的最大优势：

$$\mathrm{Adv}_{\mathrm{A}^\#}^{\mathrm{HB}^\#}(k,\eta,q,t_1,t_2)=\max_{\mathrm{A}^\#\in(t_1,t_2)}\{\mathrm{Adv}_{\mathrm{A}^\#}^{\mathrm{HB}^\#}(k,\eta,q)\}$$

需要注意的一点是，在上述攻击者模型中，敌手的能力不是最强的，它只能伪造 Tag 参与协议，我们没有考虑 Reader 被伪造的情形，事实上，这种情况也是存在的。

4.2 从 HB#协议到 HB 协议的规约

定理 1　如果 HB$^\#$协议中的敌手 A$^\#$ 拥有优势 ζ，$\mathrm{Adv}^{\mathrm{HB}^\#}(k,\eta,q,t_1,t_2)=\zeta$，(其中 ζ 对于 k 是不可忽略的)，那么 HB 协议中的敌手 A 拥有优势 $\mathrm{Adv}^{\mathrm{HB}}(k,\eta,q',t_1',t_2')\geq\dfrac{(k-2)\zeta^3+2}{2k}$，其中 $q'\leq q(\log_2 q+1)$，$t_1'\leq kt_1q(\log_2 q+1)$，$t_2'\leq 2kt_2$

证明　假设敌手 A$^\#$ 有优势 ζ (ζ 对于 k 是不可忽略的)，如果可以利用 A$^\#$ 去构造 HB 协议中的敌手 A，使得 A 的优势是不可忽略的，那么 HB$^\#$协议的安全性就可以规约到 HB

协议。

让我们回忆一下 HB 协议中敌手的攻击过程[5]，假设敌手 A 在 query 阶段与 T 交互得到至少 rq 个“挑战-响应”对，记为 $(\mathrm{A},z)=(\boldsymbol{a}^{(i)},z^{(i)})\ (i=1,\cdots,rq)$；clone 阶段，A 收到挑战 $\boldsymbol{a}$，试图根据 query 阶段得到的信息输出正确的 $z=\boldsymbol{a}\bullet\boldsymbol{x}$。

猜测 z 的过程中 A 需要调用 $\mathrm{A}^{\#}$ 提供有关于 z 的信息，即 A 模拟 $\mathrm{Exp}_{\mathrm{A}^{\#}}^{\mathrm{HB}^{\#}}$ 的环境。所以整个调用过程就是 $\mathrm{A}^{\#}$ 攻击一个 $\mathrm{HB}^{\#}$协议的过程，所不同的是，此时 A 在扮演 HB协议中的角色。

在 query 阶段 A 充当 T，提供给 $\mathrm{A}^{\#}$ 需要的信息。于此同时，它把自己需要的 z 隐含地嵌入给 $\mathrm{A}^{\#}$ 的信息中，使得 $\mathrm{A}^{\#}$ 在 clone 阶段能够不经意地透漏出来。

A 在充当 T 的时候需要选择一对密钥 $(\boldsymbol{x}^{\#},\boldsymbol{y}^{\#})$ 作为 HB协议中的共享密钥。它生成一个密钥 $\boldsymbol{s}$ 作 $\boldsymbol{x}^{\#}$，将 HB 协议中的密钥 $\boldsymbol{x}$ 作 $\boldsymbol{y}^{\#}$ (当然，它是不知道 $\boldsymbol{x}$ 的)，其中 $\boldsymbol{s}$ 除了第 j 位外的每一位都是 A 随机产生的。如果用 $s[i]$ 表示 $\boldsymbol{s}$ 的第 i 位，即 $s[i]\leftarrow_R\{0,1\}(i\neq j)$，$s[j]$ 未知。

下面分别描述 A 在 query 和 clone 两个阶段是如何调用 $\mathrm{A}^{\#}$ 的。

query 阶段 在前面的敌手模型定义中我们知道，query 阶段，$\mathrm{A}^{\#}_{\mathrm{query}}$ 询问 $\mathrm{HB}^{\#}$协议中的 T (此时由 A 充当)。考虑第 m 轮询问，A 首先向 $\mathrm{A}^{\#}$ 发出 $\boldsymbol{b}^{\#(m)}$，为了后面它能得到有用的信息，A 需要选择合适的 $\boldsymbol{b}^{\#(m)}$。另一方面，A 必须在收到 $\boldsymbol{a}^{\#(m)}$ 之前产生 $\boldsymbol{b}^{\#(m)}$，所以它为了选择合适的 $\boldsymbol{b}^{\#(m)}$，需要对 $f(\boldsymbol{a}^{\#(m)})$ 进行必要的猜测。A 选择一个随机比特 $g(m)$ 作为对 $f(\boldsymbol{a}^{\#(m)})[j]$ 的猜测。如果 $g(m)=0$，取 $\boldsymbol{b}^{\#(m)}=\boldsymbol{a}^{(m)}$；如果 $g(m)=1$，取 $\boldsymbol{b}^{\#(m)}=\boldsymbol{a}^{(m)}\oplus\boldsymbol{a}$。关于 $g(m)$ 的猜测，会出现以下两种情况：

情况 1 A 猜测错误，即 $g(m)\neq f(\boldsymbol{a}^{\#(m)})[j]$，那么 A 将丢弃这一对 $(\boldsymbol{a}^{(m)},z^{(m)})$，重新开始第 m 轮询问，直到猜对为止。如果它一直都没有猜对，到所有的 $(\boldsymbol{a}^{(i)},z^{(i)})$ 对全部用完时，A 随机输出一个对 z 的猜测。

情况 2 A 猜测正确，即 $g(m)=f(\boldsymbol{a}^{\#(m)})[j]$，A 计算响应比特

$$z^{\#(m)}=\oplus_{i\neq j}(f(\boldsymbol{a}^{\#(m)})[i]s[j])\oplus z^{(m)} \tag{1}$$

(1)若 $g(m)=f(\boldsymbol{a}^{\#(m)})[j]=0$，此时 $\boldsymbol{b}^{\#(m)}=\boldsymbol{a}^{(m)}$：事实上

$$\begin{aligned}z^{\#(m)}&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{x}^{\#})\oplus(\boldsymbol{b}^{\#(m)}\bullet\boldsymbol{y}^{\#})\oplus v\\&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{s})\oplus(\boldsymbol{a}^{(m)}\bullet\boldsymbol{x})\oplus v\\&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{s})\oplus z^{(m)}\\&=\oplus_i((f(\boldsymbol{a}^{\#(m)})[i])s[i])\oplus z^{(m)}\end{aligned} \tag{2}$$

对比式(1)和式(2)，可以发现，式(1)缺少一项 $u=f(\boldsymbol{a}^{\#(m)})[j])s[j]$，但是因为 $f(\boldsymbol{a}^{\#(m)})[j]=0$，所以响应的 $z^{\#(m)}$ 仍然是正确的；

(2)若 $g(m)=f(\boldsymbol{a}^{\#(m)})[j]=1$，此时 $\boldsymbol{b}^{\#(m)}=\boldsymbol{a}^{(m)}\oplus\boldsymbol{a}$：事实上

$$\begin{aligned}z^{\#(m)}&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{x}^{\#})\oplus(\boldsymbol{b}^{\#(m)}\bullet\boldsymbol{y}^{\#})\oplus v\\&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{x}^{\#})\oplus((\boldsymbol{a}^{(m)}\oplus\boldsymbol{a})\bullet\boldsymbol{x})\oplus v\\&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{s})\oplus(\boldsymbol{a}^{(m)}\bullet\boldsymbol{x})\oplus(\boldsymbol{a}\bullet\boldsymbol{x})\oplus v\\&=(f(\boldsymbol{a}^{\#(m)})\bullet\boldsymbol{s})\oplus z^{(m)}\oplus z\\&=\oplus_i((f(\boldsymbol{a}^{\#(m)})[i])s[i])\oplus z^{(m)}\oplus z\end{aligned} \tag{3}$$

对比式(2)和式(3)，可以发现，式(2)缺少一项 $u=f(\boldsymbol{a}^{\#(m)})[j])s[j]\oplus z$，因为 $f(\boldsymbol{a}^{\#(m)})[j]=1$，$u=s[j]\oplus z$。如果 A 响应的 $z^{\#(m)}$ 仍然是正确的，或者说它对于敌手 $\mathrm{A}^{\#}$ 是有用的，必须满足 $u=0$，即 $z=s[j]$。至此，A 已经成功的把它需要的 z 嵌入 $\mathrm{A}^{\#}$ 的响应消息中。

clone 阶段 在这一阶段，A 的目标是从 $\mathrm{A}^{\#}$ 的响应中抽取 $z=s[j]$。

$\mathrm{A}^{\#}$ 利用上一阶段获得的有效信息开始模拟 T。它首先输出一个盲因子 $\hat{\boldsymbol{b}}$，然后收到挑战 $\hat{\boldsymbol{a}}$，最后输出猜测的响应 $\hat{z}$。如果猜测正确的话，$z=(f(\hat{\boldsymbol{a}})\bullet\boldsymbol{x}^{\#})\oplus(\hat{\boldsymbol{b}}\bullet\boldsymbol{y}^{\#})=(f(\hat{\boldsymbol{a}})\bullet\boldsymbol{s})\oplus(\hat{\boldsymbol{b}}\bullet\boldsymbol{x})$。

A 选择一对挑战 $(\hat{\boldsymbol{a}}_1,\hat{\boldsymbol{a}}_2)$，使得 $f(\hat{\boldsymbol{a}}_1)$，$f(\hat{\boldsymbol{a}}_2)$ 只有第 j 位不同，不妨假设 $f(\hat{\boldsymbol{a}}_1)[j]=0$，$f(\hat{\boldsymbol{a}}_2)[j]=1$。A 在收到 $\hat{\boldsymbol{b}}$ 后，重绕 $\mathrm{A}^{\#}$ 关于 $\hat{\boldsymbol{b}}$ 进行两个不同的挑战 $\hat{\boldsymbol{a}}_1$，$\hat{\boldsymbol{a}}_2$，分别得到响应 $\hat{z}_1$，$\hat{z}_2$。如果 $\hat{z}_1$ 和 $\hat{z}_2$ 都正确，那么

$$\begin{aligned}\hat{z}_1\oplus\hat{z}_2&=(f(\hat{\boldsymbol{a}}_1)\bullet\boldsymbol{s})\oplus(\hat{\boldsymbol{b}}\bullet\boldsymbol{x})\oplus(f(\hat{\boldsymbol{a}}_2)\bullet\boldsymbol{s})\oplus(\hat{\boldsymbol{b}}\bullet\boldsymbol{x})\\&=(f(\hat{\boldsymbol{a}}_1)\bullet\boldsymbol{s})\oplus(f(\hat{\boldsymbol{a}}_2)\bullet\boldsymbol{s})\\&=\left(\sum_{i\neq j}(f(\hat{\boldsymbol{a}}_1[i])\bullet\boldsymbol{s}[i])\oplus(f(\hat{\boldsymbol{a}}_2[i])\bullet\boldsymbol{s}[i])\right)\oplus s[j]\end{aligned} \tag{4}$$

因为 A 知道 $\boldsymbol{s}$ 的所有位除了 $s[j]$，它可以计算式(4)的前半部分，继而得到 $z=s[j]$。如果 $\hat{z}_1$ 和 $\hat{z}_2$ 都错误，异或运算错误抵消，仍然可以得到 z。

下面计算 A 能成功得到 z 的概率，即 $\hat{z}_1$，$\hat{z}_2$ 同时正确或者错误的概率。令 Z_d 为随机变量，如果用 $Z_d=1$ 表示 $\hat{z}_d$ 正确，$Z_d=0$ 表示 $\hat{z}_d$ 错误，$d\in\{0,1\}$，那么 $\Pr[\mathrm{A\ succeed}]=\Pr[Z_1=Z_2]$。

Weis 在文献[2]中证明了下面的引理：

引理 1 一个黑盒，输入矩阵 $\boldsymbol{A}_{r\times k}$ 和一个 k 比特矢量 $\boldsymbol{u}$，输出 0 或者 1。$p_{\boldsymbol{A}}$ 表示对于随机选择的矩阵 $\boldsymbol{A}$ 输出 1 的概率，假设一对随机的 k 比特矢量 $(\boldsymbol{u}_1,\boldsymbol{u}_2)$，对于随机选择的 $j\in\{1,2,\cdots,k\}$，$u_1[j]=0$，$u_2[j]=1$。$q_{\boldsymbol{A}}$ 表示对于随机选择的矢量，都输出 1 或者都输出 0 的概率。如果 $p=\Sigma_A p_A\geq 1/2+\delta$，那么 $q=\Sigma_A p_A\geq 1/2+\delta'$ 其中 $\delta'=\delta^3/2-(\delta^3+1)/k$。

回忆定理 1 的前提，假设新协议中的敌手拥有优势 ζ，即此处的 $p=1/2+\zeta$，那么根据引理 1，$\Pr[Z_1=Z_2]\geq\dfrac{1}{2}+\dfrac{\zeta^3}{2}-\dfrac{\zeta^3+1}{k}$，即敌手 A 攻击 HB 协议成功的概率，故敌

手 A 的优势 $\mathrm{Adv}^{\mathrm{HB}}(k,\eta,q',t_1',t_2')=\dfrac{(k-2)\zeta^3+2}{2k}$。其中 q' 是 A 对 HB 协议中 Tag oracle 的询问次数，因为 A 猜测 $f(\boldsymbol{a}^{\#(m)})[j]$ 的时候需要丢弃没有用的 $(\boldsymbol{a}^{(m)},z^{(m)})$，所以它最多询问 qr 次，即 $q'\le qr$，取 $r=\log_2 q+1$，$q'\le q(\log_2 q+1)$；同理 $\mathrm{A}_{\mathrm{query}}$ 的计算时间 $t_1'=kt_1q'\le kt_1q(\log_2 q+1)$；$\mathrm{A}_{\mathrm{clone}}$ 的计算时间等于 $\mathrm{A}^{\#}_{\mathrm{clone}}$ 计算时间的 2 倍，因为在 query 阶段，A 提供了两个挑战给 $\mathrm{A}^{\#}$，因此 $t_2'\le 2kt_2$，这里的 k 是要对密钥的 k 比特分别计算。

4.3 从 HB$^{\#}$协议到 LPN 问题的规约

Blum[1]和 Weis[2]在随机预言模型下证明了 HB 协议的安全性可以规约到解 LPN 困难问题，即引理 2。

引理 2　如果 HB 协议的敌手 A 拥有优势 ε，$\mathrm{Adv}^{\mathrm{HB}}(k,\eta,q,t_1,t_2)=\varepsilon$，存在算法 D 可以在 $t_1'\le kt_1$，$t_2'\le kt_2$，$q'\le kq+1$ 的条件下以 $\varepsilon'\ge 1/k$ 的概率得到密钥 $\boldsymbol{x}$。

在 4.2 节中我们把 HB$^{\#}$协议的安全性规约到了 HB 协议的安全性上，得到了定理 1。结合定理 1 和引理 2，我们可以将 HB$^{\#}$协议的安全性规约到 LPN 困难问题，继而得到下面的结论。

定理 2　如果 HB$^{\#}$协议的敌手 $\mathrm{A}^{\#}$ 具有对于 k 不可忽略的优势 ζ，$\mathrm{Adv}(k,\eta,q,t_1,t_2)=\zeta$，存在算法 D 可以在时间 (t_1',t_2') 内以 $1/k$ 的概率解一个随机的 $q'\times k$ 的 LPN 问题，其中 $t_1'\le k^2t_1q(\log_2 q+1)$，$t_2'\le 2k^2t_2$，$q'\le kq(\log_2 q+1)+1$。

5　结束语

作为普适计算应用环境的重要组成部分，RFID 系统的研究受到广泛关注，也是目前学术界研究的一个热点。本文对一类基于 LPN 困难问题的 RFID 认证协议进行了分析并加以改进，提出了一个 HB$^{\#}$协议，该协议可以抵抗被动攻击、主动攻击和中间人攻击并且能够达到 Reader 对 Tag 的单向认证。

本文证明 HB$^{\#}$协议的安全性是将其规约到 LPN 困难问题上的，但是在挑战矩阵完全随机的情况下，LPN 问题的困难性还没有被证明，这是一个亟待解决的问题。另外 HB 类协议都是“human-computer”协议，只有合法的 Tag 才能参与协议，没有考虑 Reader 的伪造假冒，设计并证明一个安全的双向 RFID 认证协议是我们今后工作的目标。

参 考 文 献

[1] Hopper N J and Blum M. Secure human identification protocols. In Advances in Cryptology ASIA CRYPT'01, vol. 2248 of Lecture Notes in Computer Science, 2001: 52–66.

[2] Juels A and Weis S. Authenticating pervasive devices with human protocols. In Advances in Cryptology –CRYPTO'05, vol.3621 of Lecture Notes in Computer Science, 2005: 293–308.

[3] Bringer J, Chabanne H, and Dottax E. HB^{++}: a lightweight authentication protocol secure against some attacks. IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in pervasive and Ubiquitous Computing ——SecPerU, 2006: 28–33.

[4] Selwyn P. HB and related lightweight authentication protocols for secure RFID Tag/Reader authentication. CollECTeR Europe Conference, Basel, Switzerland, June 2006.

[5] Crawford J M, Kearns M J, and Shapire R E. The minimal disagreement parity problem as a hard satisfiability problem. Tech. rep., Computational Intelligence Research Laboratory and AT&T Bell Labs, February 1994.

[6] Berlekamp E R, McEliece R J, and Tilborg V. On the inherent intractability of certain coding problems. *IEEE Trans. on Information Theory*, 1978, 24(3): 384–386.

[7] Blum A, Furst M, Kearns M, and Lipton R J. Cryptographic primitives based on hard learning problems. In Advances in Cryptology——CRYPTO'93, Vol.773 of Lecture Notes in Computer Science, 1993: 278–291.

[8] HÅstad J. Some optimal inapproximability results. In Symposium on Theory of Computing, El paso, Texas, Unitied States, 1997, Vol 48: 1–10.

[9] Kearns M. Efficient noise-tolerant learning from statistical queries. *Journal of the ACM*, 1998, 45(6): 983–1006.

[10] Hopper N J and Blum M A. Secure human-computer authentication scheme. Tech. Rep. CMU-CS-00-139, Carnegie Mellon University, 2000.

[11] Blum A, Kalai A, and Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*, 2003, 50(4): 506–519.

[12] Bringer J, Chabanne H, and Dottax E. HB++: a lightweight authentication protocol secure against some attacks. Proceeding of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Lyon, France, June 2006: 28–33.

唐　静：　女，1984 年生，硕士，研究方向为安全协议.

姬东耀：　男，1965 年生，副研究员，研究方向为安全协议理论与技术.