基于不可追踪模型的轻量级RFID认证协议

陈秀清 曹天杰 郭 玉
(中国矿业大学计算机科学与技术学院 徐州 221116)

摘 要 在Ha等提出的基于Hash函数的低成本RFID认证协议中,敌手捕获标签和读卡器之间传送的信息后,就可以实现跟踪攻击。在分析Ha等提出的低成本RFID认证协议的基础上,设计出了效率更高的追踪攻击算法。Ha等提出的低成本RFID认证协议易于遭受追踪攻击,敌手可以从低位到高位,逐个比特位地猜测出合法的标签密钥的比特位,针对这一缺点提出了可以抵抗追踪攻击的改进协议,并用不可追踪模型形式化证明了该协议不可追踪的鲁棒性。

关键词 RFID认证协议,跟踪攻击,不可追踪模型
中图法分类号 TP311 **文献标识码** A

Lightweight Authentication Protocol for RFID Based on Model of Untraceability

CHEN Xiu-qing CAO Tian-jie GUO Yu
(College of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221116, China)

Abstract We analyzed the security of RFID authentication protocols recently proposed by Ha et al. Our security analysis clearly highlights important security weakness in this article. More precisely, an adversary analyzes the messages between reader and tag and implements traceability attacks. Then, the adversary performs the passive full-disclosure attacks and discloses the tags' secret. In order to evaluate the performance of traceability attacks, we observed the toy experimental results by running several tests on an implementation of the protocol. Finally, we used the formal model of untraceability, which successfully proves the robustness against tracing attacks and the untraceability of the enhanced scheme.

Keywords RFID authentication protocols, Traceability attack, Formal model of untraceability

1 引言

无线射频识别(Radio Frequency Identification, RFID)技术是一种广义上的概念,适用于低成本设备(标签),在RFID系统中如果有一个读卡器就能实现远程查询。RFID可用于多种应用,如供应链管理、访问控制、付款、零售库存控制或产品跟踪。对于一个大规模部署存储标签RFID的系统来说,标签必须保持低成本,也意味着这些标签的存储和计算能力非常受限。在轻量级认证协议中,加密原语和高级加密算法在标签的存储和计算能力上代价很高,不适用于低成本标签的推广使用,因此有必要设计轻量级、低成本、安全的RFID认证协议。

然而在进行协议的设计时,不仅要确保标签和读卡器之间的认证,也要能够保护客户个人信息的RFID隐私不被敌手恶意跟踪[1]。但是目前大部分轻量级协议[2-5]依靠位操作、简单的加法或位旋转操作,都存在着一定的安全追踪问题。事实上,从RFID标签的应答中,攻击者可能捕获一些敏感信息,并用于跟踪标签的持有者。首先分析交互认证原始协议(enhancement of one-way hash based low-cost authentication protocol, EOHLCAP)存在的追踪攻击问题[3],再对与其他轻量级协议不同的追踪攻击算法进行分析(首次全面的分析和比较类似的追踪攻击算法)。通过分析EOHLCAP协议的结构,发现其协议存在追踪攻击,随即提出更高效率的追踪攻击算法。因为这个协议算法实现过程中混合了异或、加法和减法等位操作,敌手通过对这些位操作的分析,可推测出标签的挑战消息的变化规律,从而能够成功追踪标签。最后针对EOHLCAP协议的缺点,提出一个效率更高的追踪攻击算法。

2 RFID协议相关研究

在文献[2]中RFID系统存在的攻击大致划分为4类:拒绝服务、假冒攻击、信息泄露、恶意跟踪。一个安全的轻量级低成本RFID认证协议应该具有以下安全性能:

(1)抵抗拒绝服务攻击

这种类型的拒绝服务攻击是因为在协议设计时仅仅考虑到应用的需要而没有考虑协议的细节,造成的标签和数据库中保存的数据将不再同步。一个安全的协议必须能够抵抗拒绝服务攻击。

到稿日期:2013-08-20 返修日期:2013-09-18 本文受国家自然科学基金(61202478,61303263),中央高校基本科研业务费(2013QNA26)资助。
陈秀清(1981—),女,博士生,主要研究方向为安全协议、RFID认证协议等,E-mail:xiuqingchen@126.com;曹天杰(1967—),男,教授,博士生导师,主要研究方向为安全协议、信息安全等。

(2)抵抗假冒攻击

假冒攻击可以通过重放攻击来实现假冒标签或读卡器。例如在超市中,如果敌手获取便宜商品的标签密钥,他可以将已知的密钥信息内容覆盖到昂贵的商品上,从而欺骗终端扫描标签的读卡器,以低廉的价格买走昂贵的货物。

(3)抵抗信息泄露

抵抗信息泄漏的措施通常是将真实的标签 ID 保存到数据库中,而传送中使用标签的匿名 ID,只有数据库可以将真实 ID 和匿名 ID 进行匹配。

(4)抵抗恶意跟踪

这是协议中最重要的性能。恶意追踪包括恶意跟踪标签或它的持有者,因此威胁到用户的位置隐私(空间和时间隐私)。例如攻击者能够分析验证会话之间的潜在的关系,从而追踪标签。在设计协议时,为了杜绝出现类似跟踪问题,通过在每次会话中随机改变标签的挑战信息来抵抗恶意追踪,并且不同时期的会话之间不会存在太多关联,敌手即使通过截获的数据来进行分析,也无法分辨它们之间的关系。

最近很多文献分析了不同的轻量级协议,提出了不同的追踪攻击算法。轻量级协议 UMAP family、M2AP、EMAP 存在着各种各样的攻击,例如异步攻击、追踪攻击和全揭露攻击。大部分的攻击算法是利用这些协议中原始设计的算法本身存在的缺陷来发起攻击。然而,现在大部分协议只是改进原始协议,并没有运用模型(不可追踪模型、随机模型、标准模型、串空间模型)进行证明,协议的安全性有待进一步证明。只有部分协议使用模型进行安全证明,例如文献[6]使用扩展的串空间模型形式化分析 RFID 协议中标签的不可追踪性,利用不可追踪性的判定定理对 Feldhofer 协议和 0′-FRAP 协议进行形式化模型证明,前者具有不可追踪性,后者对于主动攻击者不能实现不可追踪性。

文献[7]使用可证明安全模型对作者自己提出的协议进行了形式化分析,定理证明的结论是:如果敌手的识别追踪标签的成功优势是可忽略不计的,则提出的协议是安全的。

通过分析协议[3]已经存在的安全漏洞,提出了改进的协议,并利用文献[8]中的不可追踪模型证明了改进协议是不可追踪的。另外,modulo 加法、和、异或以及或操作等都是 triangular 运算。后三者是字位运算,密钥的每一位字位运算更新机制是从低位(LSB)进行更新,而不是从高位(MSB)更新。如果仅仅只考虑最低一位的运算,那么两个数据的 modulo 加法等同于这两个数据的异或运算。敌手利用这种性质简化协议中的公式,以利于从密钥的最低位依次猜测到最高位,直到获取全部比特位的密钥数据。Peris-Lopez 等人[9]首次指出简单的追踪攻击算法并不适用于所有协议。Phan 等人[10]指出允许被动敌手通过四分之一的概率猜测静态标识符的最低位来实施追踪攻击。Hernandez-Castro 等人[11]提出的基于 SASI 改进的协议中存在被动全揭露攻击,使用的循环算法是基于加法的循环,而在 SASI 原始协议中,使用的循环算法是基于汉明权重的定义。而这种攻击算法只是理论上的,每揭露一定数量的 ID 位数就需要协议运行大数量的轮数。如果揭露 ID 的低 6 位的 LSB 就需要监听大约 2^{18} 次真实协议的运行,但是在现实的攻击中是很难实现如此大量的监听的。文献[2]使用基于汉明权重的循环来揭露 SASI 协议中的全部 ID 也要需要监听大约 2^{17} 次真实协议的运行轮数,而文献[11]使用基于加法循环来揭露全部的 ID 需要监听大约 2^{19} 次真实协议的运行轮数。虽然前者的效率高一些,但是实际协议如果没有运行如此多的轮数,就无法实现全揭露算法。一些超轻量级 RFID 认证协议[12,13]也存在着一些安全问题。

综合分析以上 RFID 安全协议存在的问题,重点研究轻量级 RFID 协议中混合加法操作和字位操作(如异或操作)的本质特性,有助于理解 EOHLCAP 协议中存在的追踪攻击算法。

3 EOHLCAP 协议

EOHLCAP 协议中使用的概念和定义如表 1 所列。

表 1 概念和定义

符号	定义	符号	定义
$\oplus$	异或操作	$+$	加法 modulo 2^l
$\vee$	OR 操作	$\wedge$	AND 操作
$+$	加法 modulo 2^l	$\|\|$	连接操作
$\gg$	右移循环	$\ll$	左移循环
l	标识符的长度(l=96 bit)	n	标签的数量
LSB	最低位字节(标记为 X_0)	MSB	最高位字节(标记为 X_{n-1})
ID	标签的标识符	S	标签的密钥
$B_R(B_L)$	B 的右(左)边的信息	r_1, r_2	l bit 的随机数
h(ID)	标签的标识符的哈希值	Had	标签的标识符的哈希值的索引地址

EOHLCAP 协议中具体的算法公式使用了加法进位的概念(Carry for modular addition),即两个数据在第 k 位做加法运算取决于第 $k-1$ 位上的进位标志 $C(a,b,k-1)$,进位标志的初始值为 $C(a,b,-1)=0$。而进位标志符可以使用如下公式计算得到。

$$C(a,b,k)=([a]_k \wedge [b]_k) \vee ([a]_k \vee [b]_k) \wedge C(a,b,k-1)$$

$$[a+b]_k=[a]_k \oplus [b]_k \oplus C(a,b,k-1)$$

EOHLCAP 协议具体过程如图 1 所示。

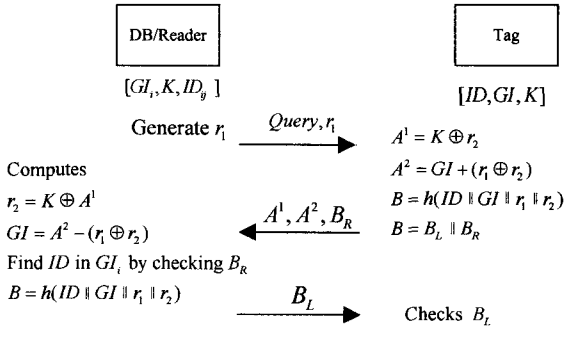

图 1 原始 EOHLCAP 协议

4 EOHLCAP 协议的分析

4.1 跟踪攻击算法

综合分析了其他文献的追踪攻击算法,其存在两个问题。1)需要监听大量真实协议的运行轮数,2)一部分算法只能以很低的概率揭露标签密钥的一个比特位(最低位或最高位)。针对这些问题,提出一种更高效率的追踪攻击算法。EOHLCAP 协议中的计算公式简化介绍如下:

$$A^1=K \oplus r_2 \quad (1)$$

$$A^2=GI+(r_1\oplus r_2) \tag{2}$$

$$r_2=K\oplus A^1 \tag{3}$$

$$A^2=GI+(r_1\oplus A^1\oplus K) \tag{4}$$

$$[A^2]^i=GI+([r_1\oplus A^1]^i\oplus K) \tag{5}$$

$$[A^2]^i|_k=GI|_k+([r_1\oplus A^1]^i|_k\oplus K|_k)=GI|_k\oplus([r_1\oplus A^1]^i|_k\oplus K|_k)\oplus C(GI,[r_1\oplus A^1]^i\oplus K,k-1) \tag{6}$$

$$C(GI,[r_1\oplus A^1]^i\oplus K,k-1)=([GI]_{k-1}\wedge[(r_1\oplus A^1)^i\oplus K]_{k-1}) \tag{7}$$

$$GI|_k\oplus K|_k=[A^2]^j|_k\oplus([r_1\oplus A^1]^j|_k)\oplus C(GI|_k,[r_1\oplus A^1]^j|_k\oplus K|_k,k-1)\vee([GI]_{k-1}\vee[(r_1\oplus A^1)^i\oplus K]_{k-1})\wedge C(GI,[r_1\oplus A^1]^i\oplus K,k-2)] \tag{8}$$

定理 1 敌手锁定目标标签 T^*，通过 Testing 查询来运行 EOHLCAP 协议 t 轮，并把收集的响应信息即测试数据 $\{[A^1]^i,[r_1]^i,[A^2]^i\}$保存到一张数据表中，其中 $1\leqslant i\leqslant t$。对于目标标签 T^* 来说，它的密钥 GI 和 K 是固定的，所以敌手由式(5)可以推理出测试数据 $[r_1\oplus A^1]^i$ 和 $[A^2]^i$ 存在着一定的常量对应关系。

证明：综合式(1)、式(2)和式(3)，得到式(5)，即 $[A^2]^i=GI+([r_1\oplus A^1]^i\oplus K)$。式(5)存在两个变量 $\{[r_1\oplus A^1]^i,[A^2]^i\}$，两个常量 GI 和 K。敌手在测试阶段，保存测试数据到数据表中。可以从数据表中提取 k 位 LSB 的变量 $\{[r_1]^i|_{k\cdots0},[A^1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0}\}(i=1,2,\ldots,t)$，并将计算信息 $\{[r_1\oplus A^1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0}\}$保存到另外一张表中。

敌手在监听阶段，保存监听的变量信息 $\{[r_1\oplus A^1]^j,[A^2]^j\}$到数据表中。通过比较监听的信息值是否在测试的数据表中来判断追踪标签。

然而，敌手很难直接推测出标签密钥的全部 96 位比特位。式(6)只有异或操作，从而可以从低位到高位，逐个比特位地推测已知变量和未知变量之间的关系。所以通过进一步的公式分析就可以推测出两个未知常量$\{GI,K\}$的异或值，从而推测出 GI 和 K 的可能的组合值。

算法 1 针对 EOHLCAP 协议的追踪攻击算法。

Step 1 训练测试(Testing)

敌手发起认证会话，测试 t 轮认证协议后，敌手 A 创建一个包含 2^{k+1}行的表 Table k，分别存储随机数的低 k 位数据，敌手每次测试选择不同比特位数的随机数$(r_1)|_{k\cdots0}$，协议运行时收集所需要的信息$\{r_1|_{k\cdots0},A^1|_{k\cdots0},A^2|_{k\cdots0}\}$，并保存到相应的 Table k 中，测试协议运行如下：

(1)敌手 A 发送$[r_1]^i|_{k\cdots0}$给目标标签 T^*。

(2)一旦目标标签收到$[r_1]^i|_{k\cdots0}$，标签选择不为 0 的随机数$[r_2]^i|_{k\cdots0}$并做如下运算，计算$[A^1]^i|_{k\cdots0}$，$[A^2]^i|_{k\cdots0}$和 B，发送这些信息$\{[A^1]^i|_{k\cdots0},[r_1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0},B_R\}$给读卡器。

(3)敌手 A 使用收集的信息$\{[A^1]^i|_{k\cdots0},[r_1]^i|_{k\cdots0}\}$，计算$[r_1\oplus A^1]^i|_{k\cdots0}$，保存信息$\{[r_1\oplus A^1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0}\}$到 Table k 中。

Step 2 监听(Eavesdropping)

给定标签 T′，敌手 A 监听一轮真实运行的协议，一旦得到所监听到的信息$\{[A^1]^j,[r_1]^j,[A^2]^j\}$，就计算信息$[r_1\oplus A^1]^j$，并保存这些信息$\{[r_1\oplus A^1]^j,[A^2]^j\}$到监听 Table′ j 中。

Step 3 猜测(Guessing)

对于给定的 T′，敌手依据定理 1 来决定 T′是不是原来的目标标签 T^* 发出来的信息。

敌手如果使用监听得到的信息$\{[r_1]^j|_{k\cdots0},[A^1]^j|_{k\cdots0}\}$计算值$[r_1\oplus A^1]^j|_{k\cdots0}$，并判断在表 Table k 中是否存在与这个计算值相等的值，则需要确定监听的值$[A^2]^j|_{k\cdots0}$是否在表 Table k 中存在相等的值，即监听的值$[A^2]^j|_{k\cdots0}$等于测试值$[A^2]^i|_{k\cdots0}$。敌手如果判断$[A^2]^j|_{k\cdots0}\neq[A^2]^i|_{k\cdots0}$，则以概率为 1 的优势确定 $T'\neq T^*$，标签 T'的这些信息不是原来目标标签 T^* 输出的。

If $\exists(((r_1\oplus A^1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0})\in\text{Table }k)\wedge(([r_1\oplus A^1]^j|_{k\cdots0},[A^2]^j|_{k\cdots0})\in\text{Table}'\ j)))|[r_1\oplus A^1]^j|_{k\cdots0}=[r_1\oplus A^1]^i|_{k\cdots0}\wedge([A^2]^j|_{k\cdots0}\neq[A^2]^i|_{k\cdots0})$ then $T'\neq T^*$, for $1\leqslant i\leqslant t$;

Otherwise, if $\exists(((([r_1\oplus A^1]^i|_{k\cdots0},[A^2]^i|_{k\cdots0})\in\text{Table }k)\wedge(([r_1\oplus A^1]^j|_{k\cdots0},[A^2]^j|_{k\cdots0}\in\text{Table}'\ j)))|([r_1\oplus A^1]^j|_{k\cdots0}=[r_1\oplus A^1]^i|_{k\cdots0}\wedge([A^2]^j|_{k\cdots0}=[A^2]^i|_{k\cdots0})$ then $T'=T^*$

敌手如果判断$[A^2]^j|_{k\cdots0}=[A^2]^i|_{k\cdots0}$，则可以逐个比特位地猜测密钥值，实施追踪攻击。

(a)使用 $k+1$ 位比特位的 r_1 进行测试；

(b)比较$[A^2]^j|_{k\cdots0}=[A^2]^i|_{k\cdots0}$，$A$ 只能确定 T'的输出有可能是 T^* 输出的，需要对 $k+1$ 位进行进一步测试。在测试前，先推测出标签密钥的 k 个比特位的值。利用定理 1 即可推测出$\{GI|_k,K|_k\}$的值；如果敌手使用监听到的信息$\{r_1,A^1,A^2\}$计算$[r_1\oplus A^1]^j|_{k+1\cdots0}$得到的值与敌手在测试阶段存储的值$[r_1\oplus A^1]^i|_{k+1\cdots0}$相等，并且监听到的$[A^2]^j|_{k+1\cdots0}$值与表 Table $k+1$ 中对应的$[A^2]^i|_{k+1\cdots0}$值相等，则需要推测出标签密钥的第 $k+1$ 位比特位的值。使用式(8)进行计算即可推测出$\{GI|_{k+1},K|_{k+1}\}$的值。

$$GI|_{k+1}\oplus K|_{k+1}=[A^2]^j|_{k+1}\oplus([r_1\oplus A^1]^j|_{k+1})\oplus C(GI|_{k+1},[r_1\oplus A^1]^j|_{k+1}\oplus K|_{k+1},k)$$

$C(GI|_{k+1},[r_1\oplus A^1]^j|_{k+1}\oplus K|_{k+1},k)$的值可以从第 k 位计算推测出来，计算公式如下所示：

$$C(GI,(r_1\oplus A^1)^j\oplus K,k)=([GI]_k\wedge[(r_1\oplus A^1)^j\oplus K]_k)\vee([GI]_k\vee[(r_1\oplus A^1)^j\oplus K]_k)\wedge C(GI|_k,[r_1\oplus A^1]^j|_k\oplus K|_k,k-1)]$$

(c)敌手继续执行以上步骤，可以正确决定监听到的 T'的信息是不是原来的目标标签 T^* 发出来的信息。如果是目标标签发送的信息，则可以全揭露 $T*$ 的密钥值$\{GI,K\}$。虽然不知道$[r_1\oplus A^1]^i$ 的所有 96 位比特值，但它能够逐一分析比特位来比较密钥值，实施追踪攻击。敌手正确猜测所有 k 位标签密钥的值的概率是 $1/2^{k+1}$。

4.2 实例分析

假设以针对低 3 位字节(LSB)的攻击算法为实例。所有的加法操作都是 mod 2^3。假设目标标签 T^* 的真实密钥是 $GI=110,K=010$，监听到的真实协议运行的值是$\{[r_1]^j,[A^1]^j,[A^2]^j\}=\{010,101,011\}$。

敌手执行追踪攻击算法：

(1)敌手仅启动测试一位 LSB 的 r_1

敌手发送 r_1 启动测试阶段的算法，r_1 可能的选择为{0,1}。使用定理 1，可得到所有的测试数据$[r_1]^i|_0$，$[A^1]^i|_0$ 和

$[A^2]^i|_0$。接下来敌手计算$[r_1 \oplus A^1]^i|_0$，在 Table 0 中存储$[r_1 \oplus A^1]^i|_0$和$[A^2]^i|_0$。

表 2　算法中 Table 0 存储的一位测试数据集合

$[r_1 \oplus A^1]^i\|_0$	$[A^2]^i\|_0$
0	0
1	1

当$[r_1 \oplus A^1]^j|_0=[r_1 \oplus A^1]^i|_0=1$且$[A^2]^j|_0=[A^2]^i|_0=1$时，敌手决定监听的 T'信息$\{[r_1]^j,[A^1]^j,[A^2]^j\}$有可能是目标标签 T^* 的输出。

敌手 A 需要揭露标签的密钥$\{GI,K\}$的最低位 LSB，从以下公式中可以推断出其值。已知$[A^2]^j|_0$，$[r_1 \oplus A^1]^j|_0$和$C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,-1)$的值，计算$GI|_0$和$K|_0$。

$$GI|_0 \oplus K|_0 = [A^2]^j|_0 \oplus ([r_1 \oplus A^1]^j|_0) \oplus C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,-1)$$
$$= 1 \oplus 1 \oplus 0 = 0$$

所以敌手正确猜对密钥组合值$GI|_0$和$K|_0$的概率是 1/2，如表 3 所列。

表 3　猜测$GI|_0$和$K|_0$的第 0 位密钥值的概率

$GI\|_0$	$K\|_0$	Probability
0	0	1/2
1	1	1/2

敌手继续执行对两位 LSB 的追踪算法。

(2)敌手启动测试两位 LSB 的 r_1

敌手启动测试阶段，r_1 的数目变为 4 个，即{00,01,10,11}。每接收到测试数据$\{[r_1]^i|_{10},[A^1]^i|_{10},[A^2]^i|_{10}\}$，敌手计算$[r_1 \oplus A^1]^i|_{10}$并在 Table 1 中存储$\{[r_1 \oplus A^1]^i|_{10},[A^2]^i|_{10}\}$的数据值。

表 4　算法中表 1 存储的两位测试数据集合

$[r_1 \oplus A^1]^i\|_{10}$	$[A^2]^i\|_{10}$
00	00
01	01
10	10
11	11

当$[r_1 \oplus A^1]^j|_{10}=[r_1 \oplus A^1]^i|_{10}=11$并且$[A^2]^j|_{10}=[A^2]^i|_{10}=11$时，敌手决定监听到的 T'的输出信息$\{[r_1]^j,[A^1]^j,[A^2]^j\}$有可能是目标标签 T^* 的输出结果。揭露标签两个密钥值 GI 和 K 的第二位 LSB 的计算方法如下所示。

$$[A^2]^j|_1 = GI|_1 \oplus ([r_1 \oplus A^1]^j|_1 \oplus K|_1) \oplus C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,0)$$

假设已经准确猜测密钥值$\{GI|_0=0,K|_0=0\}$。猜对的概率是 1/2。已知$GI|_0=0$，$[r_1 \oplus A^1]^j|_0 \oplus K|_0=1 \oplus 0=1$，敌手计算$C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,0)=(0 \wedge 1) \vee (0 \vee 1) \wedge C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,-1)=(0) \vee (1) \wedge 0=0$。可以推算$GI|_1 \oplus K|_1=[A^2]^j|_1 \oplus ([r_1 \oplus A^1]^j|_1) \oplus C(GI|_0,[r_1 \oplus A^1]^j|_0 \oplus K|_0,0)=1 \oplus 1 \oplus 0=0$。

对于标签密钥的$\{GI|_1,K|_1\}$值只有两种可能的匹配对，所以敌手正确猜对密钥值的概率是 1/4，如表 5 所列。

表 5　猜测$GI|_1$和$K|_1$的第 1 位密钥值的概率

$GI\|_1$	$K\|_1$	Probability
0	0	1/2
1	1	1/2

敌手继续执行对三位 LSB 的追踪算法。

(3)敌手启动测试三位 LSB 的 r_1

敌手启动测试阶段，r_1 的数目变为 8 个，即{000,001,010,011,100,101,110,111}。每接收到测试数据$\{[r_1]^i|_{210},[A^1]^i|_{210},[A^2]^i|_{210}\}$，敌手计算$[r_1 \oplus A^1]^i|_{210}$并在 Table 2 中存储$\{[r_1 \oplus A^1]^i|_{210},[A^2]^i|_{210}\}$的数据值。

表 6　算法中表 2 存储的三位测试数据集合

$[r_1 \oplus A^1]^i\|_{10}$	$[A^2]^i\|_{10}$
*00	*00
*01	*01
*10	*10
011	111
111	011

当$[r_1 \oplus A^1]^j|_{210}=[r_1 \oplus A^1]^i|_{210}=111$并且$[A^2]^j|_{210}=111 \neq [A^2]^i|_{210}=011$时，敌手判断信息$\{[r_1]^j,[A^1]^j,[A^2]^j\}$不是目标标签 T^* 的输出结果，追踪攻击算法成功实施。

5　基于 rotation 操作的 EOHLCAP+协议

通过改进 EOHLCAP 协议，使改进后的协议能够抵抗本文前一部分讨论的追踪攻击算法，随即提出了基于 rotation 操作的 EOHLCAP+协议。敌手即使能够分析测试数据$[r_1 \oplus A^1]^i$和$[A^2]^i$，也无法推断出这两者之间的有规律的对应关系，无法跟踪标签，更不可能全揭露 GI 和 K 的密钥值。EOHLCAP+协议过程如图 2 所示。

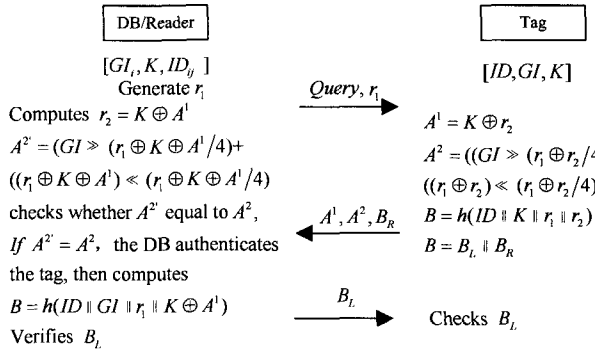

图 2　EOHLCAP+协议

EOHLCAP+协议具体步骤描述如下：

①读卡器随机生成 r_1 并发送给标签。

②标签随机选择 r_2，使用 r_1 和 r_2 进行验证并计算 $A^1=K \oplus r_2$，$B=h(ID \| GI \| r_1 \| r_2)$，$A^2=((GI \gg (r_1 \oplus \frac{r_2}{4}) + ((r_1 \oplus r_2) \ll (r_1 \oplus \frac{r_2}{4}))$，随后发送 A^1，A^2 和 B_R 给读卡器。

③读卡器传送信息 A^1、A^2、B_R 以及 r_1 给数据库 DB。

④数据库 DB 计算 $r_2=K \oplus A^1$ 和 $A^{2'}=(GI \gg (r_1 \oplus K \oplus A^1/4) + ((r_1 \oplus K \oplus A^1) \ll (r_1 \oplus K \oplus A^1/4)$。

如果通过 A^2 的验证即 DB 计算的 $A^{2'}$ 值和接收的 A^2 是相等的，则认证标签为合法标签。然后计算 B 的值，发送 B_L 给标签。

⑤标签接收到 B_L 后，验证自己计算的 B_L 值是否和接收到的值相同。如果相同，一轮完整的协议认证成功。

6 模型证明

针对文献[3]中存在的追踪攻击的问题，使用文献[8]提出的模型证明的数学概念(证明过程中使用到的符号如表7所列)，来证明EOHLCAP+协议可以抵抗标签跟踪攻击。

表7 不可追踪模型的形式化定义符号说明

符号	代表的意义
T,T′	代表2个不同的追踪
L(.)	2个不同的追踪之间的连接关系
~	2个不同的追踪之间的不可分辨性
Trace(P)	针对协议P的一系列追踪步骤
T_i^A	敌手能够针对T_i实施追踪攻击

使用文献[8]中的不可追踪模型的形式化定义来证明该协议能抵抗追踪攻击，其代数表达式见定理2。

定理2 $\forall T\in Trace(P), \forall_{i\neq j} L(T_i^A, T_i'^A)\Rightarrow \exists T'\in Trace(P)$

证明：假设T有两个子跟踪T_i^A和$T_j^A(i\neq j)$。如果存在一个追踪T'符合如下条件：$T\sim T'\wedge\neg L(T_i'^A, T_j'^A)$，则置$agent(T_i^A)=agent(T_j^A)=agent(T_i'^A)=given$和$agent(T_j'^A)=wanted$。

根据协议的具体运行步骤，标记为$wanted$的标签的两个密钥的异或值T_{wanted}需要满足以下要求：

$$A_j^2=(GI_j\gg(r_1\oplus r_2)/4)+((r_1\oplus r_2)\ll(r_1\oplus r_2)/4)$$

$$A_{wanted}^2=(GI_{wanted}\gg(r_1\oplus K\oplus A^1)/4)+((r_1\oplus K\oplus A^1)\ll(r_1\oplus K\oplus A^1)/4)$$

$$A_j^2=A_{wanted}^2$$

通过以上这些假设，敌手就可以重新构建攻击的意图，使用数学语言描述：

$$\pi((GI_{given}\gg(x\oplus K_{given}\oplus A_{given}^1\#\theta)/4)+((x\oplus K_{given}\oplus A_{given}^1\#\theta)\ll(x\oplus K_{given}\oplus A_{given}^1\#\theta)/4))=\pi((GI_{wanted}\gg(x\oplus K_{wanted}\oplus A_{wanted}^1\#\theta)/4)+((x\oplus K_{wanted}\oplus A_{wanted}^1\#\theta)\ll(x\oplus K_{wanted}\oplus A_{wanted}^1\#\theta)/4))$$

对于任意u都存在$\pi(u)=u$，即存在$\pi(A_{given}^1\#\theta)=A_{wanted}^1\#\theta$，由于$A_j^1=A_{wanted}^1$，因此敌手无法分辨出所有由标签产生并发送的信息$\{A^1,A^2\}$，所以密钥$GI$和$K$也是无法分辨的，即$T\sim T'\wedge\neg L(T_i'^A, T_j'^A)$，证明了改进协议是不可追踪的。

由rotation操作来保证其数据的机密性，敌手无法分析出A^1和A^2之间对应的常量关系，从而保证了标签的不可追踪性。改进的协议抵抗追踪攻击的鲁棒性证明过程如图3所示。

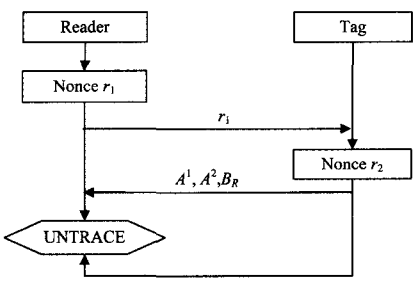

图3 不可追踪模型证明EOHLCAP+协议的核心过程

结束语 对EOHLCAP协议进行安全性分析，指出其存在的追踪攻击，提出了一个新的高效的追踪攻击算法。

随后针对原始协议存在的追踪攻击进行改进，提出一个基于rotation操作的低成本RFID协议，并用不可追踪模型进行了安全证明。改进的协议可以抵抗追踪攻击，与没有进行模型证明的协议相比较，具有更好的不可追踪性和更高的安全性能。

参考文献

[1] 史艳伟，张岩庆，刘克胜. 基于RFID系统的安全性问题研究[J]. 计算机科学，2012，39(6A)：214-216

[2] Avoine G, Carpent X, Martin B. Privacy-friendly synchronized ultralightweight authentication protocols in the storm [J]. Journal of Network and Computer Applications, 2012, 35(2): 826-843

[3] Ha J, Moon S, Nieto J M G, et al. Security analysis and enhancement of one-way hash based low-cost authentication protocol (OHLCAP) [M]. Emerging Technologies in Knowledge Discovery and Data Mining. Springer, 2007: 574-583

[4] Thompson D R, Chaudhry N, Thompson C W. RFID security threat model[C]//Proceedings of the Conf on Applied Research in Information Technology. 2006

[5] 梁昌勇，陆鑫，俞家文，等. 基于云计算的供应链RFID信息服务研究[J]. 计算机应用研究，2011，28(9)：3375-3380

[6] 邓淼磊，朱昭，石金娥，等. RFID标签的不可追踪性[J]. 北京邮电大学学报，2010，33(2)：44-47

[7] 李慧贤. 轻量级RFID双向认证协议设计与分析[J]. 西安电子科技大学学报：自然科学版，2012，39(1)：172-178

[8] Ton V D, Sjouke M, Sa˘sa R. Untraceability of RFID protocols [M]. Information Security Theory and Practices Smart Devices, Convergence and Next Generation Networks. Springer, 2008: 1-15

[9] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J M, et al. M2AP: a minimalist mutual-authentication protocol for low-cost RFID tags[C]//Ma J, Jin H, Tianruo Yang L, Tsai JJP, eds. International conference on ubiquitous intelligence and computing—UIC'06. Lecture notes in computer science, vol. 4259. Wuhan and Three Gorges, China: Springer, 2006: 912-23

[10] Phan R-W. Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI [J]. IEEE Transactions on Dependable and Secure Computing, 2009, 6(4): 316-320

[11] Hernandez-Castro J C, Peris-Lopez P, Phan R C-W, et al. Cryptanalysis of the David-Prasad RFID ultralightweight authentication protocol [M]. Radio Frequency Identification: Security and Privacy Issues. Springer, 2010: 22-34

[12] Peris-Lopez P, Hernandez-Castro J C, Phan R C-W, et al. Quasi-linear cryptanalysis of a secure RFID ultralightweight authentication protocol [C]//Proceedings of the Information Security and Cryptology. 2011

[13] Yeh K-H, Lo N, Winata E. An efficient ultralightweight authentication protocol for RFID systems [J]. Proc of RFIDSec Asia, 2010, 10: 49-60