华南师范大学学报(自然科学版)
Journal of South China Normal University(Natural Science Edition)
2016,48(3):64-68
doi:10.6054/j.jscnun.2016.05.005

基于 LPN 抗中间人攻击的两轮认证协议

姜 晓,马昌社*
(华南师范大学计算机学院,广州 510631)

摘要:低成本设备(如 RFID 标签)易受各种攻击,为其提供强安全保证显得尤为重要.基于此,提出了抗中间人攻击安全的两轮对称密钥认证协议 LPNAP.此协议基于 LPN 问题设计,具有较低的计算开销和存储开销.此外,LPNAP 协议的安全性可归约到 subspace LPN 的困难性.为进一步降低存储需求,提出了基于 Toeplitz-LPN 的优化版本.

关键词:强安全;低成本设备;RFID;中间人攻击;LPN;Toeplitz-LPN
中图分类号:TP309 **文献标志码**:A **文章编号**:1000-5463(2016)03-0064-05

MIM Secure Two-Round Authentication Protocols Based on LPN

JIANG Xiao, MA Changshe*
(School of Computer Science, South China Normal University, Guangzhou 510631)

Abstract: It is important to provide strong security guarantees for low cost devices such as Radio Frequency Identification (RFID) tags, since they are more vulnerable to all kinds of attacks. In this vein, this paper presents a two-round symmetric authentication protocol LPNAP which is able to resist man-in-the-middle (MIM) attacks. LPNAP is constructed on the learning parity with noise (LPN) problem. Hence, it has small computation cost and low communication overhead. Moreover, it has been proven to be as secure as the subspace LPN problem. To reduce the storage requirement, an optimized variant of LPNAP is introduced through Toeplitz-LPN.

Key words: strong security; low cost devices; RFID; man-in-the-middle attacks; LPN; Toeplitz-LPN

为轻量级组件设计安全的认证协议是密码学研究中的主要挑战之一.轻量级设备(比如 RFID 标签)在许多领域得到了广泛应用,进而促进了轻量级认证协议的研究[1-4].迄今为止,出现了许多适用于 RFID 系统的认证协议,包括 HB 协议[5]、HB^+协议[6]、$HB^\#$协议[7]和 Auth 协议[8]等,最典型的是 HB 类协议.

一方面,HB 和 HB^+协议均无法抵抗 GILBERT 等[9]提出的攻击(简称 GRS 攻击).尽管 $HB^\#$协议能够抗 GRS 攻击,但是易受一般中间人攻击[10].另一方面,Auth 协议具备紧致安全性规约证明,但是它仅具备主动安全性.最近,RIZOMILIOTIS 和 GRITZALIS[11]给出了 $Auth^\#$抗中间人攻击的证明,但是我们发现其证明存在严重缺陷:证明中对归约成功的概率估算有误.目前尚不清楚 $Auth^\#$协议是否具有抗一般中间人攻击的能力.

上述基于 LPN 的协议[5-8]均具有结构简单、计算量低和抗量子攻击等优点[12],然而都无法抵抗一般中间人攻击[13].此外,大部分基于 LPN 的认证协议只具有非紧致安全归约证明.目前尚不存在基于 LPN 的认证协议能够同时满足低成本和抗一般中间人攻击紧致安全性.

本文提出了具有抗中间人攻击安全的两轮认证协议 LPNAP.根据 EPC Class 1 Generation 2(简称 EPC C1 G2)标准[14]可知两轮协议尤其适用于 RFID 系统,因此在 RFID 应用中设计双向认证协议是可取的.LPNAP 协议的设计在遵循具有主动安全的 $Auth^\#$[8]协议的设计思路的同时,借鉴了基于 LPN 的 MAC(Message Authentication Code)[15]的设计方法.LPNAP 协议仅采用了一个 PI-Hash(Pairwise Independent Hash)函数,比基于 LPN 的 MAC 具有更少的计算和存储开销.此外,相对于 3 轮的 LM13 协

收稿日期:2016-04-20 《华南师范大学学报(自然科学版)》网址:http://journal.scnu.edu.cn/n
基金项目:广东省自然科学基金项目(S2013020011913);广东省教育厅科技创新项目(2013KJCX0055);广州市基础研究重点项目(11C42090777)
*通讯作者:马昌社,教授,Email:chsma@163.com.

议[13],LPNAP 协议仅需要 2 轮通信,而且具有更紧致的安全证明.为进一步减少存储开销,我们将 LPNAP 协议建立在 Toeplitz-LPN 的基础上得到它的改进版本,此版本所需密钥大小与基于 LPN 的其他协议相同,比如 LM13 协议、HB#协议和 Auth 协议等.因此,在计算开销、存储开销、通信开销和安全性证明等方面,该改进版本协议均优于 LM13 协议.

1　预备知识

1.1　符号说明

$a,b\in\mathbb{R}$,$[a,b]=\{x\in\mathbb{R}:a<x<b\}$.$Z_2$表示有限域$\{0,1\}$,其上的运算为模 2 的加法和乘法,$Z_2^k$ 表示 Z_2上的 k 维线性空间;$\boldsymbol{r}\xleftarrow{\$}Z_2^{2l}$ 表示从 Z_2^{2l} 中根据均匀分布抽样出来的 1 个二进制向量 $\boldsymbol{r}$,$\mathrm{wt}(\boldsymbol{r})$代表 $\boldsymbol{r}$ 的汉明重量;假设$\boldsymbol{X}\xleftarrow{\$}Z_2^{2l\times n}$,$\boldsymbol{X}_{\downarrow v}$表示矩阵 $\boldsymbol{X}$ 的子矩阵,其操作为:如果 $v[i]=0$,则删除 $\boldsymbol{X}$ 中的第 i 行.$\mathrm{Ber}(\eta)$表示参数为 η 的贝努利分布($\eta\in[0,1/2]$),即 $P[x\leftarrow\mathrm{Ber}(\eta):x=1]=\eta$;$\boldsymbol{e}\leftarrow\mathrm{Ber}_\eta^n$ 表示从贝努利分布抽样出来的 n 维比特向量;对于$\{0,1\}^k$中的元素有时看成比特串,有时看成 k 维比特的向量(即 Z_2^k 中的元素),具体依上下文而定;符号"‖"可以连接 2 个比特串,也可以连接 2 个向量.

1.2　困难性问题

定义 1(LPN 问题)　假设$\boldsymbol{r}\xleftarrow{\$}Z_2^{2l}$,$\boldsymbol{X}\xleftarrow{\$}Z_2^{2l\times n}$,噪声参数 $\eta\in[0,1/2]$,$\boldsymbol{e}\leftarrow\mathrm{Ber}_\eta^n$.给定 $\boldsymbol{X}$,η 以及 $z=\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}\oplus\boldsymbol{e}$,LPN 问题指的是寻找 $\boldsymbol{X}'\in Z_2^{2l\times n}$ 使其满足 $|z\oplus\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}'|<n\eta$.LPN 假设表明:在给定多项式个噪音序对$(\boldsymbol{r},\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}\oplus\boldsymbol{e})$的情况下,任意攻击者均无法恢复出密钥矩阵 $\boldsymbol{X}$.LPN 问题已被证明是 NP 困难问题[16].

定义 2(Toeplitz 矩阵)　假设 $\boldsymbol{T}\xleftarrow{\$}Z_2^{4l\times n}$ 是 Toeplitz 矩阵,$\boldsymbol{T}$ 中从左上到右下的对角线上的元素相同.由于 Toeplitz 矩阵中对角线上的元素是固定的,因此整个 Toeplitz 矩阵可以用其第 1 行和第 1 列上的元素来表示.如果 $\boldsymbol{T}$ 以均匀概率和 $4l+n-1$ 比特的向量 $\boldsymbol{s}$ 相关联,则此矩阵可用符号 $\boldsymbol{T}_{\boldsymbol{s}}$ 表示,其中向量 $\boldsymbol{s}$ 的元素由 $\boldsymbol{T}$ 中第 1 行和第 1 列的元素所构成.

定义 3(Toeplitz-LPN 问题)　假设 $\boldsymbol{T}\xleftarrow{\$}Z_2^{2l\times n}$ 是 Toeplitz 矩阵,$\boldsymbol{r}\xleftarrow{\$}Z_2^{2l}$,噪声参数 $\eta\in[0,1/2]$,$\boldsymbol{e}\leftarrow\mathrm{Ber}_\eta^n$.给定 $\boldsymbol{T}$,η 以及 $z=\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{T}\oplus\boldsymbol{e}$,Toeplitz-LPN 问题指的是寻找 $\boldsymbol{T}'\in Z_2^{2l\times n}$,使其满足 $|z\oplus\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{T}'|<n\eta$.

定义 4(Pairwise-Independent 函数)　给定函数族 $H:D\to F$.如果对任意的 $x_1\in D$,$x_2\in D$,$x_1\neq x_2$,存在 $y_1\in F$,$y_2\in F$,满足 $P[h(x_1)=y_1\cap h(x_2)=y_2]=1/|F|^2$,则称函数族 H 是 Pairwise-Independent.

1.3　认证协议及其安全性

所谓认证协议是指在标签和阅读器之间执行的交互式协议.标签和阅读器共享密钥 $\boldsymbol{x}$,通过无线通信标签向阅读器证明自己的身份(即标签向阅读器证明自己知道密钥 $\boldsymbol{x}$),阅读器以输出'accept'或'reject'的方式向标签反馈认证结果.由于现实环境无线信道的不安全性,认证协议往往面临安全威胁:

(1)被动攻击.在标签与阅读器的通信过程中,敌手 A 可以窃听多项式次通信消息,并试图冒充合法的标签通过阅读器的验证.如果敌手 A 以不可忽略的概率通过阅读器的认证,则称敌手 A 攻击成功.对 1 个认证协议的安全性而言,如果不存在这样的多项式时间敌手以压倒性的概率通过阅读器的认证,则此认证协议具有抗被动攻击安全性.

(2)主动攻击.认证协议更强的安全属性是协议能够抵抗主动攻击.在协议通信过程中,敌手 A 可以与标签进行多项式次交互,然后与阅读器进行 1 次交互企图通过其认证.如果对任意的、具有上述能力的多项式时间敌手 A 而言,其通过阅读器认证的概率均为 $P[(\mathrm{A},\mathrm{Reader}(x))=\mathrm{accept}]\leqslant\varepsilon$($\varepsilon$ 可忽略不计),则称此认证协议抗主动攻击.

(3)中间人攻击.认证协议最强的安全属性是指协议能够抵抗中间人攻击.敌手 A 对任意的两轮认证协议实施中间人攻击的实验如图 1 所示.

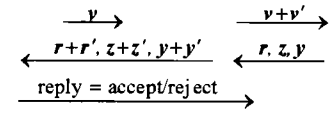

图 1　MIM 攻击实验

Figure 1　MIM attack experiment

具体来讲,两轮认证协议的中间人攻击实验由 3 个阶段构成:

[初始化阶段]标签和阅读器共享密钥.

[第一阶段]敌手 A 对两轮认证协议进行 q 次查询.每次查询中敌手 A 都可以窃听和修改标签与阅读器间的通信消息.此外,敌手 A 还可以获得阅读器每一次的认证结果.具体来讲,敌手 A 将来自阅读器的消息 v 修改为 $v+v'$并将其发送给标签.然后敌手 A 再将标签的回复消息(r,z,y)修改为$(r+r',z+z',y+y')$并发送给阅读器.阅读器根据所收到的消息进行验证:如果消息$(r+r',z+z',y+y')$是有效的,则阅读器回复'accept',否则回复'reject'.

[第二阶段] 敌手 A 与阅读器进行 1 次交互,试图冒充合法的标签通过阅读器认证.

对认证协议而言,如果任意的敌手在多项式时间 t 内对标签和阅读器进行至多 q 次查询后,以 ε 的概率成功冒充标签,则称此协议具有 (t,q,ε)-MIM 安全(ε 可忽略不计).

2 LPNAP 协议

给定安全参数 l、n 是关于 l 的多项式. 标签和阅读器共享 PI-Hash 函数 $h:\{0,1\}^n\to\{0,1\}^{2l}$ 和密钥矩阵 $\boldsymbol{X}\xleftarrow{\$}Z_2^{4l\times n}$,$\eta\in[0,1/2]$ 是贝努利分布 $\mathrm{Ber}(\eta)$ 的参数,$\mu\in[n\eta,\eta/2]$ 是 LPNAP 协议中阅读器验证的阈值.如图 2 所示,LPNAP 协议执行过程如下:

(1)阅读器产生长度为 $2l$ 的比特向量 $\boldsymbol{v}$ 并将其发送给标签,其中 $\mathrm{wt}(\boldsymbol{v})=l$.

(2)标签首先验证 $\mathrm{wt}(\boldsymbol{v})$,若 $\mathrm{wt}(\boldsymbol{v})=l$,则标签产生向量 $\boldsymbol{r}\xleftarrow{\$}Z_2^{2l}$、$\boldsymbol{e}\leftarrow\mathrm{Ber}_\eta^n$ 和 $\boldsymbol{b}\xleftarrow{\$}Z_2^{2l}$,其中要求 $\boldsymbol{b}$ 满足 $\mathrm{wt}(\boldsymbol{b})=l$;然后标签计算 $z=\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(v\|b)}\oplus\boldsymbol{e}$ 和 $y=h(z)\oplus\boldsymbol{b}$,并将 $(\boldsymbol{r},z,y)$ 发送给阅读器.若 $\mathrm{wt}(\boldsymbol{v})\neq l$,则本次执行终止.

(3)阅读器收到标签的消息后先验证 $\boldsymbol{r}$,如果 $\boldsymbol{r}\neq\boldsymbol{0}$,则阅读器计算 $\boldsymbol{b}=h(z)\oplus y$,然后验证 $\mathrm{wt}(z\oplus\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(v\|b)})\leqslant\mu$ 是否成立,若成立则阅读器对标签的认证通过,否则本次认证失败.

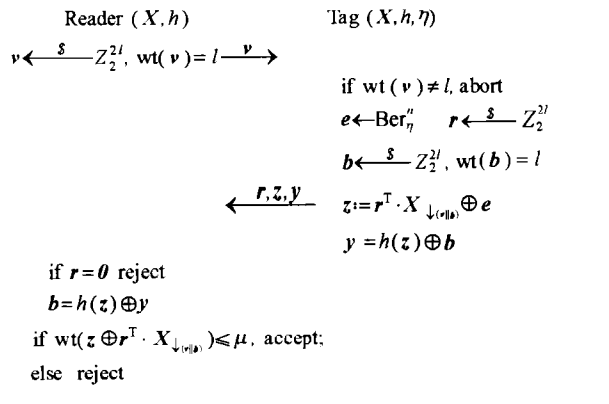

图 2 两轮认证协议 LPNAP

Figure 2 Two-round authentication protocol LPNAP

定理 1 对于参数为 $(2l,2n,\eta,\mu)$ 的 LPNAP 协议,如果存在多项式时间攻击者 $\mathrm{A}^{\#}$ 在对标签和阅读器进行 q 次交互查询后,能够以 $\delta^{\#}$ 的概率成功地对 LPNAP 协议进行 MIM 攻击,则必然存在 1 个多项式时间攻击者 A 对参数为 (l,n,η,μ) 的 $\mathrm{Auth}^{\#}$ 协议进行主动攻击,其攻击成功的概率至少为 δ,其中 $\delta\geqslant\delta^{\#}-q/2^{2l}$.

证明 假设存在攻击者 $\mathrm{A}^{\#}$ 能够对 LPNAP 协议进行一般中间人攻击. 具体来讲,在第一阶段中,攻击者 $\mathrm{A}^{\#}$ 能够将来自阅读器的挑战消息 $\boldsymbol{v}$ 修改为 $\boldsymbol{v}+\boldsymbol{v}'$,然后将来自标签的应答消息 $(\boldsymbol{r},z,y)$ 修改为 $(\boldsymbol{r}+\boldsymbol{r}',z+z',y+y')$,并能够获得阅读器每一次的认证结果.接下来需要构建 1 个能够对 $\mathrm{Auth}^{\#}$ 协议进行主动攻击的攻击者 A.

下面对本节将用到的操作符号进行说明.

$\boldsymbol{r}_{\mathrm{L}}$:向量 $\boldsymbol{r}$ 的左半部分,其中 $\boldsymbol{r}\xleftarrow{\$}Z_2^{2l}$,$\boldsymbol{r}_{\mathrm{L}}\xleftarrow{\$}Z_2^{l}$;

$\boldsymbol{r}_{\mathrm{R}}$:向量 $\boldsymbol{r}$ 的右半部分,其中 $\boldsymbol{r}_{\mathrm{R}}\xleftarrow{\$}Z_2^{l}$;

$\boldsymbol{X}_u$:矩阵 $\boldsymbol{X}$ 的上半部分,其中 $\boldsymbol{X}\xleftarrow{\$}Z_2^{4l\times n}$;

$\boldsymbol{X}_d$:矩阵 $\boldsymbol{X}$ 的下半部分;

r_i:向量 $\boldsymbol{r}_{\mathrm{L}}$ 中的元素,$i\in(1,2,\cdots,l)$;

r_j:向量 $\boldsymbol{r}_{\mathrm{R}}$ 中的元素,$j\in(l+1,\cdots,2l)$;

$(\boldsymbol{x}_1,\cdots,\boldsymbol{x}_l)$:矩阵 $(\boldsymbol{X}_u)_{\downarrow v}$ 中元素的集合;

$(\boldsymbol{x}_{l+1},\cdots,\boldsymbol{x}_{2l})$:矩阵 $(\boldsymbol{X}_d)_{\downarrow b}$ 中元素的集合;

$(\boldsymbol{x}'_{l+1},\cdots,\boldsymbol{x}'_{2l})$:矩阵 $(\boldsymbol{X}_d)_{\downarrow b'}$ 中元素的集合;

$\alpha_1\cdot\hat{\boldsymbol{x}}_1$:如果 $\boldsymbol{x}_{l+1}=\boldsymbol{x}'_{l+1}$,则 $\alpha_1\cdot\hat{\boldsymbol{x}}_1=\boldsymbol{0}$;否则

$$\alpha_1\cdot\hat{\boldsymbol{x}}_1=r_{l+1}\cdot\boldsymbol{x}_{l+1},\alpha_2\cdot\hat{\boldsymbol{x}}_2=r_{l+1}\cdot\boldsymbol{x}'_{l+1}.$$

攻击者 A 需要为攻击者 $\mathrm{A}^{\#}$ 模拟标签和阅读器在 LPNAP 协议中的行为.在初始化阶段,攻击者 A 抽样出 1 个 PI-Hash 函数 $h:\{0,1\}^n\to\{0,1\}^{2l}$,将集合 $\left(\begin{bmatrix}\boldsymbol{X}_u\\ \boldsymbol{X}_d\end{bmatrix},h\right)$ 作为 LPNAP 协议中的密钥,其中 $\boldsymbol{X}_u$ 是 $\mathrm{Auth}^{\#}$ 协议中的密钥.攻击者 A 在第一阶段的操作如下:

(1)攻击者 A 得到来自阅读器的挑战消息 $\boldsymbol{v}$ 并将其发送给攻击者 $\mathrm{A}^{\#}$;

(2)攻击者 $\mathrm{A}^{\#}$ 将消息 $\boldsymbol{v}$ 修改为 $(\boldsymbol{v}+\boldsymbol{v}')$ 后将其发送给攻击者 A;

(3)攻击者 A 用 $(\boldsymbol{v}+\boldsymbol{v}')$ 向 $\mathrm{Auth}^{\#}$ 协议中的标签进行查询,获得标签的回复消息 $(\boldsymbol{r}_{\mathrm{L}},z)$;

(i)攻击者 A 抽样出随机向量 $\boldsymbol{r}_{\mathrm{R}}\xleftarrow{\$}Z_2^{l}$ 和向量 $\boldsymbol{b}\xleftarrow{\$}Z_2^{2l}$,$\mathrm{wt}(\boldsymbol{b})=l$;

(ii)攻击者 A 计算 $z_1=z\oplus(\boldsymbol{r}_{\mathrm{R}})^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow b}$ 和 $y_1=h(z_1)\oplus\boldsymbol{b}$;

(iii)攻击者 A 将应答消息 $((\boldsymbol{r}_{\mathrm{L}}\|\boldsymbol{r}_{\mathrm{R}}),z_1,y_1)$ 发送给攻击者 $\mathrm{A}^{\#}$;

(4)攻击者 $\mathrm{A}^{\#}$ 将收到的应答消息修改成 1 个新的三元组 $((\boldsymbol{r}_{\mathrm{L}}\|\boldsymbol{r}_{\mathrm{R}})+\boldsymbol{r}',z_1+z',y_1+y')$ 后将其发送给攻击者 A;

(5)如果三元组 $(\boldsymbol{r}',z',y')$ 全为 0,则攻击者 A 输出‘accept’,否则攻击者 A 输出‘reject’.

在攻击者 A 的第二阶段中,攻击者 $A^{\#}$ 不再与标签进行任何交互,只能与阅读器进行一次交互,试图冒充标签通过阅读器的认证.攻击者 A 的第二阶段执行过程如下:首先将挑战消息 $\boldsymbol{v}$ 发送给攻击者 $A^{\#}$ 并得到攻击者 $A^{\#}$ 的应答消息 $(\bar{\boldsymbol{r}},\bar{z},\bar{y})$;然后从向量 $\bar{\boldsymbol{r}}$ 中分离出子向量 $\bar{\boldsymbol{r}}_L$、$\bar{\boldsymbol{r}}_R$,并从矩阵 $\boldsymbol{X}$ 中分离出子矩阵 $\boldsymbol{X}_d$,计算得到 $\boldsymbol{b}'=h(\bar{z})\oplus\bar{y}$ 和 $z=\bar{z}\oplus(\bar{\boldsymbol{r}}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}$;最后输出 $(\bar{\boldsymbol{r}}_L,z)$ 作为对 $\mathrm{Auth}^{\#}$ 协议中标签的模拟.

接下来计算攻击者 A 成功地为攻击者 $A^{\#}$ 提供模拟攻击环境的概率.在此之前先介绍下文将用到的引理.

引理 1[17]　假设 $\hat{x}_1,\cdots,\hat{x}_m$ 表示均匀随机比特,对任意一个非空子集 $S\subseteq[n]$,定义 $X_S=\oplus_{i\in S}\hat{x}_i$,则集合 $\{X_S\}_{\varphi\neq S\subseteq[n]}$ 中的元素是两两独立的.

模拟的攻击环境和真实的攻击环境唯一的区别在于对协议中交互消息的回答.假设用 $(\boldsymbol{r},z,y)$ 表示合法标签的应答消息,$(\bar{\boldsymbol{r}},\bar{z},\bar{y})$ 表示阅读器实际收到的消息.由于在协议的执行过程中,攻击者 A 能够修改来自标签的消息,因此消息 $(\boldsymbol{r},z,y)$ 和消息 $(\bar{\boldsymbol{r}},\bar{z},\bar{y})$ 极有可能不相等.为了说明攻击者 $A^{\#}$ 给出的消息 $(\bar{\boldsymbol{r}},\bar{z},\bar{y})$ 的有效性,需要考虑 2 种情况:

(1)$\bar{\boldsymbol{r}}=\boldsymbol{r}$,即攻击者 $A^{\#}$ 未对消息 $\boldsymbol{r}$ 做任何修改的情况.在模拟的攻击环境中,攻击者 A 首先验证 $\boldsymbol{r}$,如果 $\boldsymbol{r}\neq\boldsymbol{0}$,则计算 $\boldsymbol{b}'=h(\bar{z})\oplus\bar{y}$ 并验证 $\mathrm{wt}(\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')})\leqslant\mu$ 是否成立.$\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}$ 展开为:

$$\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b})}\oplus\boldsymbol{e}\oplus\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}=$$

$$(\boldsymbol{r}_L\|\boldsymbol{r}_R)^{\mathrm{T}}\cdot\begin{bmatrix}\boldsymbol{X}_u\\ \boldsymbol{X}_d\end{bmatrix}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b})}\oplus\boldsymbol{e}\oplus(\boldsymbol{r}_L\|\boldsymbol{r}_R)^{\mathrm{T}}\cdot\begin{bmatrix}\boldsymbol{X}_u\\ \boldsymbol{X}_d\end{bmatrix}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}=$$

$$(\boldsymbol{r}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}}\oplus(\boldsymbol{r}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}\oplus\boldsymbol{e}=$$

$$\{r_{l+1}\cdot\boldsymbol{x}_{l+1}+\cdots+r_{2l}\cdot\boldsymbol{x}_{2l}\}\oplus\{r_{l+1}\cdot\boldsymbol{x}'_{l+1}+\cdots+r_{2l}\cdot\boldsymbol{x}'_{2l}\}\oplus\boldsymbol{e}=$$

$$\{\alpha_1\cdot\hat{\boldsymbol{x}}_1+\cdots+\alpha_m\cdot\hat{\boldsymbol{x}}_m\}\oplus\boldsymbol{e},$$

其中 $m>l+1$. 如果 $\boldsymbol{b}\neq\boldsymbol{b}'$,则 $\hat{\boldsymbol{x}}_1,\cdots,\hat{\boldsymbol{x}}_m$ 是均匀随机的比特向量,根据引理 1 可知 $\{\alpha_1\cdot\hat{\boldsymbol{x}}_1,\cdots,\alpha_m\cdot\hat{\boldsymbol{x}}_m\}$ 是均匀随机的分布.攻击者 $A^{\#}$ 成功通过认证的概率可描述为 $P_r[\mathrm{wt}(\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')})\leqslant\mu]=P_r[\boldsymbol{b}=\boldsymbol{b}']\leqslant q/2^{2l}$.

因此,当 $\bar{\boldsymbol{r}}=\boldsymbol{r}$ 时,攻击者 $A^{\#}$ 成功通过认证的概率可以忽略不计.在这种情况下,攻击者 A 所提供的模拟环境和真实的攻击环境是计算不可区分的.

(2)$\bar{\boldsymbol{r}}\neq\boldsymbol{r}$,即攻击者 $A^{\#}$ 给出的冒充消息 $\bar{\boldsymbol{r}}$ 与真实信息 $\boldsymbol{r}$ 不相等的情况.在模拟的攻击环境中,攻击者 A 首先验证 $\boldsymbol{r}$,如果 $\boldsymbol{r}\neq\boldsymbol{0}$ 则继续计算 $\boldsymbol{b}'=h(\bar{z})\oplus\bar{y}$,并验证 $\mathrm{wt}(\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')})\leqslant\mu$ 是否成立.$\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}$ 展开为:

$$\boldsymbol{r}^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b})}\oplus\boldsymbol{e}\oplus\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}}\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}=$$

$$(\boldsymbol{r}_L\|\boldsymbol{r}_R)^{\mathrm{T}}\cdot\begin{bmatrix}\boldsymbol{X}_u\\ \boldsymbol{X}_d\end{bmatrix}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b})}\oplus\boldsymbol{e}\oplus(\bar{\boldsymbol{r}}_L\|\bar{\boldsymbol{r}}_R)^{\mathrm{T}}\cdot\begin{bmatrix}\boldsymbol{X}_u\\ \boldsymbol{X}_d\end{bmatrix}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}=$$

$$((\boldsymbol{r}_L)^{\mathrm{T}}+(\bar{\boldsymbol{r}}_L)^{\mathrm{T}})\cdot(\boldsymbol{X}_u)_{\downarrow\boldsymbol{v}}\oplus(\boldsymbol{r}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}}\oplus(\bar{\boldsymbol{r}}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}\oplus\boldsymbol{e}.$$

①设定 $(\boldsymbol{r}_L)^{\mathrm{T}}+(\bar{\boldsymbol{r}}_L)^{\mathrm{T}}=(a_1,\cdots,a_l)\ (a_i\leftarrow Z_2)$,则 $((\boldsymbol{r}_L)^{\mathrm{T}}+(\bar{\boldsymbol{r}}_L)^{\mathrm{T}})\cdot(\boldsymbol{X}_u)_{\downarrow\boldsymbol{v}}=a_1\cdot\boldsymbol{x}_1+\cdots+a_l\cdot\boldsymbol{x}_l$.如果 $\boldsymbol{r}_L\neq\bar{\boldsymbol{r}}_L$,则必定存在 1 个元素 $a_i\in(a_1,\cdots,a_l)$ 满足 $a_i\cdot\boldsymbol{x}_i=\boldsymbol{x}_i$ $(i\in(1,\cdots,l))$.由于 $\boldsymbol{x}_i$ 服从均匀分布,根据引理 1 可得 $\{a_1\cdot\boldsymbol{x}_1,\cdots,a_l\cdot\boldsymbol{x}_l\}$ 为均匀随机分布,即 $((\boldsymbol{r}_L)^{\mathrm{T}}+(\bar{\boldsymbol{r}}_L)^{\mathrm{T}})\cdot(\boldsymbol{X}_u)_{\downarrow\boldsymbol{v}}$ 服从均匀分布. 攻击者 $A^{\#}$ 成功通过认证的概率是忽略不计的.

②设定 $(\bar{\boldsymbol{r}}_R)^{\mathrm{T}}=(\bar{r}_{l+1},\cdots,\bar{r}_{2l})\ (\bar{r}_i\in Z_2)$,则

$$(\boldsymbol{r}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}}\oplus(\bar{\boldsymbol{r}}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}=$$

$$(r_{l+1}\cdot\boldsymbol{x}_{l+1}+\cdots+r_{2l}\cdot\boldsymbol{x}_{2l})\oplus(\bar{r}_{l+1}\cdot\boldsymbol{x}'_{l+1}+\cdots+\bar{r}_{2l}\cdot\boldsymbol{x}'_{2l})=$$

$$\beta_1\cdot\hat{\boldsymbol{x}}_1+\cdots+\beta_k\cdot\hat{\boldsymbol{x}}_k,$$

其中 $k>l+1$.如果 $\boldsymbol{r}_R\neq\bar{\boldsymbol{r}}_R$,那么 $(\beta_1,\cdots,\beta_k)\neq\boldsymbol{0}$. 则必定存在 1 个元素 $\beta_i\in(\beta_1,\cdots,\beta_k)$ 满足 $\beta_i\cdot\boldsymbol{x}_i=\boldsymbol{x}_i$ $(i\in(1,\cdots,k))$.由于 $\boldsymbol{x}_i$ 服从均匀分布,由引理 1 得 $\{\beta_1\cdot\hat{\boldsymbol{x}}_1,\cdots,\beta_k\cdot\hat{\boldsymbol{x}}_k\}$ 为均匀分布,即 $(\boldsymbol{r}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}\oplus(\bar{\boldsymbol{r}}_R)^{\mathrm{T}}\cdot(\boldsymbol{X}_d)_{\downarrow\boldsymbol{b}'}$ 服从均匀分布.因此攻击者 $A^{\#}$ 通过阅读器认证的概率 $P[\mathrm{wt}(\bar{z}\oplus(\bar{\boldsymbol{r}})^{\mathrm{T}})\cdot\boldsymbol{X}_{\downarrow(\boldsymbol{v}\|\boldsymbol{b}')}\leqslant\mu]\leqslant\varepsilon$ (ε 可忽略不计).

因此,当 $\bar{\boldsymbol{r}}\neq\boldsymbol{r}$ 时,攻击者 A 所提供的模拟环境和真实的攻击环境也是计算不可区分的.

通过上述分析可知,攻击者 A 以压倒性的优势成功地为攻击者 $A^{\#}$ 模拟了攻击环境.因此,如果存在攻击者 $A^{\#}$ 以不可忽略的优势 $\delta^{\#}$ 对 LPNAP 协议进行中间人攻击,则必然存在另一个攻击者 A 以 $\delta\geqslant\delta^{\#}-q/2^{2l}$ 的概率对 $\mathrm{Auth}^{\#}$ 协议进行主动攻击.

3　LPNAP 协议的改进版本

LPNAP 协议要求标签存储 $4l\times n$ 比特的矩阵 $\boldsymbol{X}$,这一存储开销很难满足 RFID 标签的低成本要求. 为了降低存储成本,用 Toeplitz 矩阵代替 LPNAP 协议中的随机矩阵,得到了 LPNAP 协议的改进版本,其存储复杂度为 $o(n)$.

由于 Toeplitz 矩阵是广对称矩阵,其对角线元素是固定的,因此 1 个 Toeplitz 矩阵可以用其矩阵中首行和首列的元素来表示.相对于 $4l\times n$ 的随机矩阵的存储量为 $4l\times n$ 比特,$(4l\times n)$-Toeplitz 矩阵其存储需求仅为 $4l+n-1$ 比特,由此说明优化版本对密钥的存储需求大大降低.假设用 $\boldsymbol{s}\in Z_2^{4l+n-1}$ 表示 $(4l\times n)$-Toeplitz 矩阵 $\boldsymbol{T}$ 的存储向量,则对应 $(4l\times n)$-Toeplitz 矩阵可表示为 $\boldsymbol{T}_s$. LPNAP 协议的优化版本如图 3 所示.

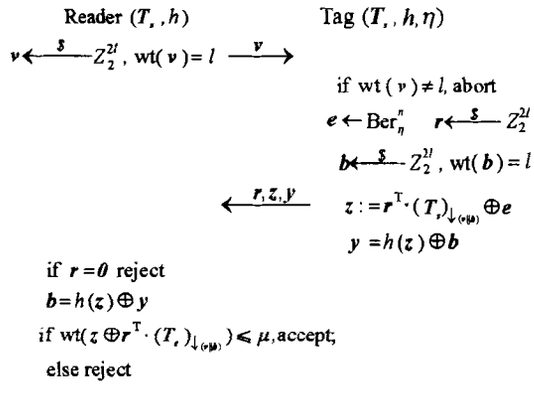

图3 LPNAP协议的优化版本

Figure 3 Extension for LPNAP Protocol

4 结束语

低成本和高安全性是射频识别技术的2个基本要求,然而目前已存在的基于LPN的认证协议均未能同时满足这2个要求.本文设计了1个新的两轮认证协议LPNAP.基于LPN的LPNAP协议不但具有很小的计算成本和较低的通信开销,而且能够抵抗一般中间人攻击.最重要的是,LPNAP协议具有可证明的紧致安全性,为进一步设计高效安全的RFID认证协议提供了建设性的指导.为进一步降低LPNAP协议的存储复杂度,本文提出了基于Toeplitz-LPN的优化版本,此版本的安全性证明可沿用LPNAP协议的证明思路.然而,Toeplitz-LPN的困难性目前仍然是一个悬而未决的问题,可作为下一步认证协议研究工作的方向.

参考文献:

[1] ZHOU J, ZHANG Q, LUO Q. Survey of privacy of radio frequency identification technology [J]. Journal of Software, 2015, 26(4): 960-976.

[2] MA C. Low cost RFID authentication protocol with forward privacy [J]. Chinese Journal of Computer, 2011, 34(8): 1387-1398.

[3] LI Y, ROBERT D, MA C. On two RFID privacy notions and their relations [J]. ACM Transaction and System Security, 2011, 14(4): 68-85.

[4] MA C, WENG J. Radio frequency identification system security proceedings of rfidsec asia workshop [M]. Netherlands: IOS Press, 2013.

[5] HOPPER N J, BLUM M. Secure human identification protocols [C]//BOYD C. Advances in Cryptology-ASIACRYPT 2001. Berlin: Springer, 2001: 52-66.

[6] JUELS A, WEIS S. Authenticating pervasive devices with human protocols [C]//SHOUP V. Advances in Cryptology-CRYPTO 2005. Berlin: Springer, 2005: 293-308.

[7] GILBERT H, ROBSHAW M, SEURIN Y. HB#: increasing the security and efficiency of HB+ [C]//SMART N. Advances in Cryptology -EUROCRYPT 2008. Berlin: Springer, 2008: 361-378.

[8] KILTZ E, PIETRZAK K, CASH D, et al. Efficient authentication from hard learning problems [C]//PATERSON K G. Advances in Cryptology- EUROCRYPT 2011. Berlin: Springer, 2011: 7-26.

[9] GILBERT H, ROBSHAW M, SILBERT H. Active attack against HB+: a provably secure lightweight authentication protocol [J]. Electronics Letters, 2005, 41(21): 1170.

[10] OUAFI K, OVERBACK R, VAUDENAY S. On the security of HB# against a man-in-the-middle attack [C]// PIEPRZYK J. Advances in Cryptology-ASIACRYPT 2008. Berlin: Springer, 2008: 108-124.

[11] RIZOMILIOTIS P, GRITZALIS S. Revisiting lightweight authentication protocols based on hard learning problems [C]//Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM, 2013: 125-130.

[12] BLUM A, KALAI A, WASSERMAN H. Noise-tolerant learning, the parity problem, and the statistical query model[J]. Journal of ACM, 2003, 50(4): 506-519.

[13] LYUBASHEVSKY V, MANSY D. Man-in-the-middle secure authentication schemes from LPN and weak PRFs [C]//CANETTI R, GARAY J A. Advances in Cryptology-CRYPTO 2013. Berlin: Springer, 2013: 308-325.

[14] EPCglobal. Class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz: Version 1.0.9 [S/OL]. (2005-01-31)[2016-03-25]. http://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_0_9-standard-20050126.pdf.

[15] DODIS Y, KILTZ E, PIETRZAK K, et al. Message authentication, revisited[C]//POINTCHEVAL D, JOHANSSON T. Advances in Cryptology-EUROCRYPT 2012. Berlin: Springer, 2012: 355-374.

[16] BERLEKAMP R, MCELIECE J, TILBORG V. On the inherent intractability of certain coding problems[J]. IEEE Transactions on Information Theory, 1978, 24(3): 385.

[17] RUBINFELD R. Randomness and computation[Z/OL]. (2012-02-22)[2016-03-25]. http://people.csail.mit.edu/ronitt/COURSE/S12/handouts/lec5.pdf.

【中文责编:庄晓琼 英文责编:肖菁】