doi:10.3969/j.issn.1000-436x.2013.z1.001

轻型的 RFID 安全认证协议 LAP

陈兵，郑嘉琦
(南京航空航天大学 计算机科学与技术学院，江苏 南京 210016)

摘 要：RFID 标签存在着处理能力弱、存储空间小和电源供给有限等局限性，传统的公钥算法或散列函数等复杂运算不能满足实际应用的需求。针对现有轻量级 RFID 认证协议的不足，设计了基于广义逆矩阵的 RFID 安全认证协议 LAP。该协议采用了硬件复杂度较低的 CRC 校验及计算量较小的矩阵运算。通过安全隐私和性能分析，LAP 协议适用于低成本、存储与计算受限的 RFID 标签。

关键词：RFID；广义逆矩阵；Gen2 标准；认证协议
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0001-07

Lightweight authentication protocol for RFID

CHEN Bing, ZHENG Jia-qi
(Institute of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: Radio frequency identification (RFID) is a technique using radio frequency to object identification and access to relevant data in the open system enviroment with the limits of process, storage, power and so on. The traditional tag authentication protocols taking complicated algorithms into account can't meet the demand. In view of the existing security and privacy problems of RFID , a lightweight authentication protocol for RFID named LAP was proposed. LAP is based on the generalized inverse matrix and only uses CRC checksum, some matrix and simple logic operations to satisfy the principles of balancing security, privacy and cost. The comparisons of security, privacy and performance with other authentication protocols show that LAP is feasible for RFID tags with requirements of low cost and resource-constrained.
Key words: RFID; generalized inverse matrix; Gen2 standard; authentication protocol

1 引言

射频识别技术(RFID, radio frequency identification)是一种利用射频通信实现的非接触式自动识别技术，目前被广泛应用于物流、防伪、交通等诸多领域。RFID 系统中的安全性和隐私性关系到个人信息、商业机密和军事秘密，如果被攻击者窃取或被不法分子利用将会严重地影响经济、军事和国家的安全。缺乏有效的 RFID 认证手段，就无法保护 RFID 电子标签中的数据及用户的隐私信息，所以，RFID 的安全和隐私问题目前已经成为制约其进一步推广应用的重要因素。

另一方面，RFID 电子标签设备本身存在着不足，如处理能力有限、存储空间小、电源供给受限等。传统保护安全和隐私所采用的较为成熟的公钥算法或散列函数等需要强大的运算处理能力，这将导致标签成本的增加。而广义逆矩阵的运算或变换的计算量很小，能够很好地满足 RFID 加解密的需求。

目前，针对 RFID 安全认证的研究，Chien 在文献[1]中分为 4 类：重量级认证、简单认证、轻量认证和超轻量认证。轻量级认证协议合理地平衡了安全、隐私保护和成本的要求，成为 RFID 安全认证研究的重点。RFID 标准组织 EPC Global 所提出的 EPC Class1 Gen2 标准（简称为 Gen2 标准）是一种轻量级认证协议，使用 CRC 来代替简单认证协议中的散列函数，不支持公钥加密和私钥加密。

收稿日期：2013-06-29
基金项目：国家自然科学基金资助项目(61139002)
Foundation Item: The National Natural Science Foundation of China (61139002)

Duc 等人在文献[2]中提出的安全认证协议不具有前向安全性，也容易导致拒绝服务攻击。Chen 和 Deng 在文献[3]中提出的协议要求标签和读写器在认证前向后端数据库注册，而此注册过程假定是在安全的环境中进行。因此该协议不能有效地保护用户隐私，易被攻击者追踪和伪造。Li 等人提出的协议[4]在标签端只使用了异或运算、截取函数和伪随机数生成器，虽然开销小，但攻击者容易窃听到标签和读写器之间的信息，并进行篡改和伪装。Choi 等人提出的协议[5]较为复杂，标签端 PRNG 运算次数以及与后端数据库交互步骤较多，并存在安全漏洞。Sun 等人在文献[6]中提出了 Gen2$^+$协议，标签和后端数据库共享一个密钥缓冲池 *keypool*，每 14 轮成功认证之后更新 *keypool* 以避免复制攻击，但易受重放攻击的威胁。

本文针对现有轻量级 RFID 认证协议的不足，设计了一种基于广义逆矩阵的 RFID 安全认证协议 LAP（lightweight authentication protocol）。该协议符合 Gen2 标准，采用了硬件复杂度较低的 CRC 校验和 PRNG 函数及运算量较小的矩阵运算。

2 RFID 认证协议 LAP

2.1 基于广义逆的加解密

美国学者 MOORE E H 将逆矩阵的概念推广到一般矩阵，称之为广义逆[7]。

定义 1 设矩阵 $\boldsymbol{A}\in\boldsymbol{C}^{m\times n}$，如果矩阵 $\boldsymbol{X}\in\boldsymbol{C}^{n\times m}$ 满足以下 4 个 Penrose 方程的部分或全部，则称 $\boldsymbol{X}$ 为 $\boldsymbol{A}$ 的广义逆矩阵，简称为广义逆。本文提到的广义逆是指自反减号逆，记为 $\boldsymbol{A}^-$。

1) $\boldsymbol{AXA}=\boldsymbol{A}$

2) $\boldsymbol{XAX}=\boldsymbol{X}$

3) $(\boldsymbol{XA})^{\mathrm{T}}=\boldsymbol{XA}$

4) $(\boldsymbol{AX})^{\mathrm{T}}=\boldsymbol{AX}$

定理 1 设矩阵 $\boldsymbol{A}\in\boldsymbol{C}^{m\times n}$，则 $\boldsymbol{A}$ 的 Moore-Penrose 逆存在且唯一。

证明 先证存在性，即 Penrose 方程组有解。若 $\boldsymbol{A}=0$，则 $\boldsymbol{X}=0\in\boldsymbol{C}^{n\times m}$ 显然满足 1)~4)。若 $\boldsymbol{A}\neq 0$，设 $\boldsymbol{A}$ 有一个满秩分解 $\boldsymbol{A}=\boldsymbol{FG}$，并令 $\boldsymbol{X}=\boldsymbol{G}^{\mathrm{T}}(\boldsymbol{GG}^{\mathrm{T}})^{-1}\cdot(\boldsymbol{F}^{\mathrm{T}}\boldsymbol{F})^{-1}\boldsymbol{F}^{\mathrm{T}}$，则容易验证 $\boldsymbol{X}$ 满足 1)~4)。再证唯一性即 Penrose 方程组有唯一解。设 $\boldsymbol{X}_1,\boldsymbol{X}_2$ 均满足 1)~4)，则

$$\begin{aligned}\boldsymbol{X}_1&=\boldsymbol{X}_1\boldsymbol{AX}_1=\boldsymbol{X}_1\boldsymbol{AX}_2\boldsymbol{AX}_1=\boldsymbol{X}_1(\boldsymbol{AX}_2)^{\mathrm{T}}(\boldsymbol{AX}_1)^{\mathrm{T}}\\&=\boldsymbol{X}_1(\boldsymbol{AX}_1\boldsymbol{AX}_2)^{\mathrm{T}}=\boldsymbol{X}_1(\boldsymbol{AX}_2)^{\mathrm{T}}=\boldsymbol{X}_1\boldsymbol{AX}_2\end{aligned}$$

类似地，可证 $\boldsymbol{X}_1\boldsymbol{AX}_2=\boldsymbol{X}_2$。故 $\boldsymbol{X}_1=\boldsymbol{X}_2$。

引理 1 对于任意矩阵 $\boldsymbol{A}\in\boldsymbol{C}^{m\times n}$，它的 Moore-Penrose 逆存在并且唯一。其中，$\boldsymbol{A}^+=\boldsymbol{C}^{\mathrm{T}}(\boldsymbol{CC}^{\mathrm{T}})^{-1}\cdot(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B})^{-1}\boldsymbol{B}^{\mathrm{T}}$，$\boldsymbol{A}=\boldsymbol{BC}$ 是 $\boldsymbol{A}$ 的满秩分解式。

相关参数约定如表 1 所示。

表 1 LAP 协议中定义的符号和术语

符号	术语	符号	术语
T_q	RFID 标签	$\boldsymbol{K}$	矩阵 $\boldsymbol{K}$ 的广义逆
R_k	RFID 阅读器	R_r	阅读器产生的随机数
B	数据库	R_{ij}	标签产生的随机数
K_{ij}	标签密钥	l	RFID 标签标识的比特长度
$\boldsymbol{ID}_{ij}$	标签的密钥在矩阵中的编号	$\in_R$	随机数选择器
$\boldsymbol{S}$	满足条件 $\boldsymbol{K}\cdot\boldsymbol{S}=0$ 的矩阵（n 行 m 列）	$\oplus$	异或运算
$\boldsymbol{E}$	单位矩阵（n 行 n 列）	T_q	替换操作符
$\boldsymbol{K}$	满足条件 $\boldsymbol{K}\cdot\boldsymbol{S}=0$ 的矩阵（m 行 n 列）		

在 RFID 应用中，如果电子标签的响应值为常量，那么电子标签就容易被攻击者追踪。因此标签端的响应值应具有随机性特点。同时，后端数据库应能从随机数中提取出标签的标识符，否则随机性就失去了意义。本文利用矩阵的广义逆理论来解决。

图 1 是 RFID 标签加密过程。输入参数为 R_t，R_r 和 ID，加密密钥为 $\boldsymbol{K}^+$ 和 $\boldsymbol{S}$，输出密文为 $\boldsymbol{M}_1$。为了排除恶意读写器每次发出相同的随机数，将标签产生的随机数 R_t 参与运算，因此加密运算为

$$(R_r\oplus R_t)\cdot\boldsymbol{K}^+ + (R_r\oplus ID)\cdot\boldsymbol{S} \tag{1}$$

其中，$(R_r\oplus R_t)\cdot\boldsymbol{K}^+$ 使加密结果随机化。

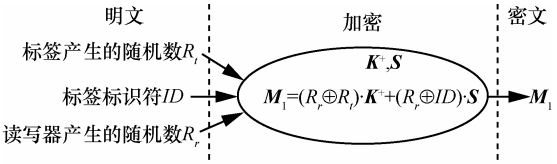

图 1 加密过程

图 2 是 RFID 标签解密过程。解密的目标是求出 $(R_r\oplus ID)\cdot\boldsymbol{S}$。在等式 M_1 两边左乘 $\boldsymbol{K}^+\boldsymbol{K}$ 得

$$(\boldsymbol{K}^+\boldsymbol{K})\cdot\boldsymbol{M}_1=(R_r\oplus R_t)(\boldsymbol{K}^+\boldsymbol{K})\cdot\boldsymbol{K}^+ + (R_r\oplus ID)\cdot(\boldsymbol{K}^+\boldsymbol{K})\cdot\boldsymbol{S} \tag{2}$$

由广义逆矩阵的定义 $\boldsymbol{K}^+\boldsymbol{K}\boldsymbol{K}^+=\boldsymbol{K}^+$ 和初始条件 $\boldsymbol{K}\cdot\boldsymbol{S}=0$ 可得

$$(\boldsymbol{K}^+\boldsymbol{K})\cdot\boldsymbol{M}_1=(R_r\oplus R_t)(\boldsymbol{K}^+) \tag{3}$$

因此 $(R_r \oplus ID)\cdot \boldsymbol{S} = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_1$。

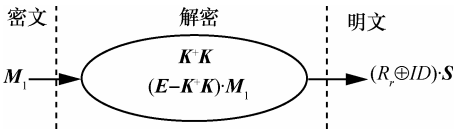

图 2　解密过程

2.2　LAP 协议描述

在RFID工作环境中，RFID电子标签是符合Gen2标准的低成本标签，拥有一个伪随机数发生器，并能执行 CRC 运算、矩阵运算和异或操作。RFID 读写器通过多天线可并行处理多标签响应信息，拥有一个伪随机数发生器，能够存储和传输数据库与标签之间的交互信息。读写器和标签的密钥信息以及标签标识信息是在协议初始化阶段由数据库进行分配。后端数据库执行 CRC 运算、矩阵运算和异或操作。

在初始状态下，为每一个标签在后端数据库中存储一条记录 $(\mu, ID, \boldsymbol{S}, \boldsymbol{K}, \boldsymbol{K}^+, DATA)$，其中，$\mu$ 是上一次认证成功后矩阵 $\boldsymbol{S}$ 更新时的列偏移量(初始状态 $\mu = 0$)，ID 是标签的唯一标识符。n 行 m 列矩阵 $\boldsymbol{S}$ 和 m 行 n 列矩阵 $\boldsymbol{K}$ 满足条件 $\boldsymbol{K}\cdot\boldsymbol{S} = 0$，矩阵 $\boldsymbol{K}^+$ 为 $\boldsymbol{K}$ 的广义逆，$DATA$ 是关于该电子标签的详细信息。标签端存储 $(ID, \boldsymbol{S}, \boldsymbol{K}^+)$，与数据库中相关记录对应。标签和后端数据库可执行 CRC 运算、矩阵运算和异或操作。RFID 认证过程如图 3 所示。

1) 读写器产生随机数 R_r，并向该电子标签发出查询命令以及 R_r。

2) 标签利用其产生的随机数 R_t、读写器产生的随机数 R_r 以及存储在标签中的 ID、矩阵 $\boldsymbol{S}$ 和矩阵 $\boldsymbol{K}^+$ 计算 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$，并将其作为响应值返回给读写器。

$$\boldsymbol{M}_1 = (R_r \oplus R_t)\cdot \boldsymbol{K}^+ + (R_r \oplus ID)\cdot \boldsymbol{S} \tag{4}$$

$$\boldsymbol{M}_2 = (R_t \oplus ID)\cdot \boldsymbol{K}^+ + (R_r \oplus R_t)\cdot \boldsymbol{S} \tag{5}$$

3) 读写器将 $\boldsymbol{M}_1$、$\boldsymbol{M}_2$ 和 R_r 转发给后端数据库。

4) 后端数据库对电子标签进行认证，包括 4 个步骤。

a) 查询

在后端数据库中查看是否存在某条记录，其 ID、$\boldsymbol{S}$、$\boldsymbol{K}$ 和 $\boldsymbol{K}^+$ 满足

$$(R_r \oplus ID)\cdot \boldsymbol{S} = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_1 \tag{6}$$

或

$$(R_r \oplus ID)\cdot \lambda_{-\mu}(\boldsymbol{S}) = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_1 \tag{7}$$

如果存在，则说明该标签是合法标签，转至 b)；否则该标签为非法标签，停止读写器认证过程。

b) 计算 R_t、i 和 $\boldsymbol{M}_3$

由于 $(R_r \oplus R_t)\cdot \boldsymbol{S} = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_2$，$R_r$ 和 $\boldsymbol{S}$ 的

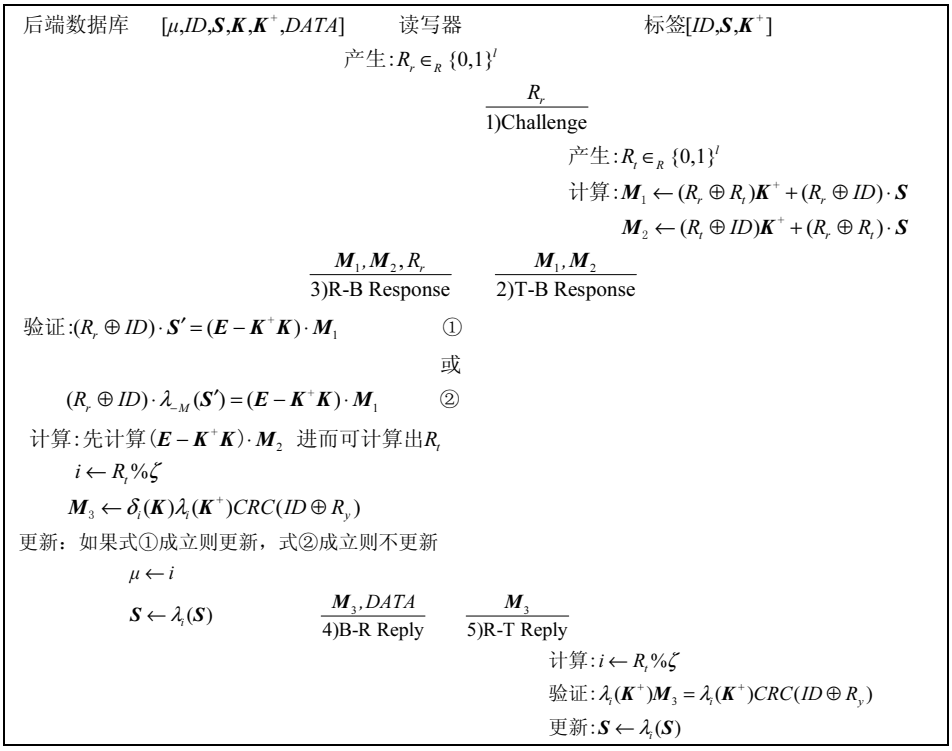

图 3　LAP 协议工作机制

值由 a)已确定，所以可求出 R_t。用 R_t 对矩阵的行数 m 和列数 n 的最小值 ξ 取模，计算出 i，用 i 分别作为矩阵 $\boldsymbol{K}$ 和 $\boldsymbol{K}^+$ 的行偏移量和列偏移量来生成新的矩阵参与计算 $\boldsymbol{M}_3$。

$$\boldsymbol{M}_3 = \delta_i(\boldsymbol{K})\lambda_i(\boldsymbol{K}^+)CRC(ID \oplus R_r) \tag{8}$$

c) 更新

若 $(R_r \oplus ID)\cdot \boldsymbol{S} = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_1$ 成立，说明标签和后端数据库的密钥矩阵 $\boldsymbol{S}$ 是同步的，此时将 b)中计算的 i 值作为新的 μ 值，$\lambda_i(\boldsymbol{S})$ 作为新的 $\boldsymbol{S}$ 值更新后端数据库。

如果 $(R_r \oplus ID)\cdot \lambda_{-\mu}(\boldsymbol{S}) = (\boldsymbol{E} - \boldsymbol{K}^+\boldsymbol{K})\cdot \boldsymbol{M}_1$ 成立，说明在前一次认证时，后端数据库中密钥矩阵 $\boldsymbol{S}$ 已更新，但标签中的矩阵 $\boldsymbol{S}$ 由于某种原因未能更新。由于后端数据库中存储了前一次矩阵 $\boldsymbol{S}$ 更新时的偏移量，因此利用 $\lambda_{-\mu}(\boldsymbol{S})$ 使得不同步的合法标签能够通过后端数据库的验证。这种情况下，后端数据库不再更新矩阵 $\boldsymbol{S}$。

d) 后端数据库将 $\boldsymbol{M}_3$ 和与此标签相关的信息 $DATA$ 发送给读写器。

5) 标签对后端数据库进行认证。标签收到来自读写器的信息 $\boldsymbol{M}_3$ 时，利用其产生的随机数 R_t 对矩阵的行数 m 和列数 n 的最小值 ξ 取模，计算出 i。根据广义逆矩阵的性质可得: $\lambda_i(\boldsymbol{K}^+) = \delta_i^+(\boldsymbol{K})$，即 $\lambda_i(\boldsymbol{K}^+)$ 是 $\delta_i(\boldsymbol{K})$ 的广义逆，故满足条件

$$\lambda_i(\boldsymbol{K}^+)\delta_i(\boldsymbol{K})\lambda_i(\boldsymbol{K}^+) = \lambda_i(\boldsymbol{K}^+) \tag{9}$$

因此可以通过比较 $\lambda_t(\boldsymbol{K}^+)\cdot \boldsymbol{M}_3$ 和 $\lambda_t(\boldsymbol{K}^+)\cdot CRC(ID \oplus R_r)$ 是否相等来判断后端数据库是否合法。若相等，则后端数据库是合法的，标签将 $\boldsymbol{S}$ 值更新为 $\lambda_t(\boldsymbol{S})$；否则，标签认为 $\boldsymbol{M}_3$ 不是由后端数据库发出的，而是攻击者伪造或重传的信息，停止认证过程。

2.3 LAP 协议数值验证

下面通过数值实验举例说明 LAP 认证协议的工作过程。假设 $m=3$，$n=4$，且电子标签标识 ID 设置为 3 759。设矩阵 $\boldsymbol{K} = \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 2 & 2 & 2 \\ -1 & 4 & 5 & 3 \end{bmatrix}$，利用满秩分解的方法来计算其 Moore-Penrose 逆 $\boldsymbol{K}^+$。矩阵 $\boldsymbol{K}$ 满秩分解为

$$\boldsymbol{K} = \begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 2 & 2 & 2 \\ -1 & 4 & 5 & 3 \end{bmatrix} = \boldsymbol{BC} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

由引理 1 可得

$$\boldsymbol{K}^+ = \boldsymbol{C}^{\mathrm{T}}(\boldsymbol{C}\boldsymbol{C}^{\mathrm{T}})^{-1}(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B})^{-1}\boldsymbol{B}^{\mathrm{T}}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}^{-1}\begin{bmatrix} 2 & -4 \\ -4 & 20 \end{bmatrix}^{-1}\begin{bmatrix} 1 & 0 & -1 \\ 0 & 2 & 4 \end{bmatrix}$$

$$= \frac{1}{18}\begin{bmatrix} 5 & 2 & -1 \\ 1 & 1 & 1 \\ -4 & -1 & 2 \\ 6 & 3 & 0 \end{bmatrix}$$

由矩阵方程 $\boldsymbol{K}\cdot \boldsymbol{S} = 0$，可得

$$\boldsymbol{S} = \begin{bmatrix} 1 & 2 & 0 \\ -5 & -8 & -2 \\ 3 & 5 & 1 \\ 2 & 3 & 1 \end{bmatrix}$$

将记录 $(\mu, ID, \boldsymbol{S}, \boldsymbol{K}, \boldsymbol{K}^+, DATA)$ 存入数据库，标签初始信息如表 2 所示。

表 2 数据库中标签初始信息

偏移量 μ	标签标识 ID	矩阵 $\boldsymbol{S}$	矩阵 $\boldsymbol{K}$	矩阵 $\boldsymbol{K}^+$
0	3 759	$\begin{bmatrix} 1 & 2 & 0 \\ -5 & -8 & -2 \\ 3 & 5 & 1 \\ 2 & 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & -1 & 1 \\ 0 & 2 & 2 & 2 \\ -1 & 4 & 5 & 3 \end{bmatrix}$	$\frac{1}{18}\begin{bmatrix} 5 & 2 & -1 \\ 1 & 1 & 1 \\ -4 & -1 & 2 \\ 6 & 3 & 0 \end{bmatrix}$

假设在认证过程中，读写器产生的随机数 R_r = 2 973，电子标签产生的随机数 R_t=5 642。当读写器向标签发送随机数 2 973 时，标签计算如下

$$(R_r \oplus R_t)\cdot \boldsymbol{K}^+$$

$$= (2\,973 \oplus 5\,642)\times \frac{1}{18}\begin{bmatrix} 5 & 2 & -1 \\ 1 & 1 & 1 \\ -4 & -1 & 2 \\ 6 & 3 & 0 \end{bmatrix}$$

$$= \frac{2\,525}{6}\begin{bmatrix} 5 & 2 & -1 \\ 1 & 1 & 1 \\ -4 & -1 & 2 \\ 6 & 3 & 0 \end{bmatrix}$$

$$(R_r \oplus ID)\cdot \boldsymbol{S} = (2\,973 \oplus 3\,759)\cdot \begin{bmatrix} 1 & 2 & 0 \\ -5 & -8 & -2 \\ 3 & 5 & 1 \\ 2 & 3 & 1 \end{bmatrix}$$

$$=1\,330\begin{bmatrix}1&2&0\\-5&-8&-2\\3&5&1\\2&3&1\end{bmatrix}$$

因此，$\boldsymbol{M}_1=\frac{1}{6}\begin{bmatrix}20\,605&21\,010&-2\,525\\-37\,375&-61\,315&-13\,435\\13\,840&37\,375&8\,530\\31\,110&31\,515&7\,980\end{bmatrix}$，

同理，$\boldsymbol{M}_2=\frac{1}{2}\begin{bmatrix}18\,655&31\,702&-701\\-75\,049&-120\,499&-29\,599\\42\,646&75\,049&16\,552\\34\,506&47\,553&15\,150\end{bmatrix}$。标签将 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 发送给读写器，读写器将 $\boldsymbol{M}_1$、$\boldsymbol{M}_2$ 和 R_r 发送给后端数据库，后端数据库进行计算。

$$\boldsymbol{E}-\boldsymbol{K}^{+}\boldsymbol{K}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}-\frac{1}{18}\begin{bmatrix}5&2&-1\\1&1&1\\-4&-1&2\\6&3&0\end{bmatrix}\begin{bmatrix}1&0&-1&1\\0&2&2&2\\-1&4&5&3\end{bmatrix}$$

$$=\frac{1}{3}\begin{bmatrix}2&0&1&-1\\0&2&-1&-1\\1&-1&1&0\\-1&-1&0&1\end{bmatrix}$$

$$(\boldsymbol{E}-\boldsymbol{K}^{+}\boldsymbol{K})\boldsymbol{M}_1=1\,330\begin{bmatrix}1&2&0\\-5&-8&-2\\3&5&1\\2&3&1\end{bmatrix}$$，同理，

$$(\boldsymbol{E}-\boldsymbol{K}^{+}\boldsymbol{K})\boldsymbol{M}_2=7\,575\begin{bmatrix}1&2&0\\-5&-8&-2\\3&5&1\\2&3&1\end{bmatrix}$$。

后端数据库利用存储在数据库中的 $\boldsymbol{S}$ 和接收到的随机数 $R_r=2\,973$ 找到与之相匹配的标签标识符 3 759。由标签标识符 3 759 和 $(\boldsymbol{E}-\boldsymbol{K}^{+}\boldsymbol{K})\boldsymbol{M}_1$ 的结果可求出标签产生的随机数 $R_t=5\,642$。因为 $m=3$，$n=4$，所以 $\xi=3$。计算

$$i=R_t\%\xi=5\,642\%3=2$$

$$\boldsymbol{M}_3=\delta_2(\boldsymbol{K})\lambda_2(\boldsymbol{K}^{+})CRC(ID\oplus R_r)$$

$$=\begin{bmatrix}-1&4&5&3\\1&0&-1&1\\0&2&2&2\end{bmatrix}\frac{1}{18}\begin{bmatrix}2&-1&5\\1&1&1\\-1&2&-4\\3&0&6\end{bmatrix}$$

$$CRC(3\,759\oplus 2\,973)$$

$$=\frac{1}{6}\begin{bmatrix}2&5&-1\\2&-1&5\\2&2&2\end{bmatrix}CRC(1\,330)$$

后端数据库更新标签 3 759 的偏移量 μ 和矩阵 $\boldsymbol{S}$。更新后标签 3 759 各参数如表 3 所示。

表 3　　一次认证后数据库中标签信息

偏移量 μ	标签标识 ID	矩阵 $\boldsymbol{S}$	矩阵 $\boldsymbol{K}$	矩阵 $\boldsymbol{K}^{+}$
2	3 759	$\begin{bmatrix}2&0&1\\-8&-2&-5\\5&1&3\\3&1&2\end{bmatrix}$	$\begin{bmatrix}1&0&-1&1\\0&2&2&2\\-1&4&5&3\end{bmatrix}$	$\frac{1}{18}\begin{bmatrix}5&2&-1\\1&1&1\\-4&-1&2\\6&3&0\end{bmatrix}$

标签端计算 $i=R_t\%\xi=5\,642\%3=2$，并验证 $\boldsymbol{M}_3$ 的合法性，之后更新标签端的矩阵 $\boldsymbol{S}$。

3　LAP 协议证明

3.1　LAP 协议形式化描述

LAP 协议流程如图 3 所示，将消息传递顺序转换成 GNY 逻辑符号 $\boldsymbol{M}_1\sim\boldsymbol{M}_9$，符号表示及其含义如下。

$\boldsymbol{M}_1: T\lhd *R_r$ 表示标签 T 接收到随机数 R_r。*表示随机数 R_r 不是由标签发出的。

$\boldsymbol{M}_2: R\lhd *\{F(ID,R_r)\}_{\boldsymbol{K}^{+},\boldsymbol{S}}$ 表示读写器 R 接收到 ID 和 R_r 经过函数 F 运算之后并通过 $\boldsymbol{K}^{+}$ 和 $\boldsymbol{S}$ 加密后的结果。

$\boldsymbol{M}_3: R\lhd *\{F(R_t,R_r)\}_{\boldsymbol{K}^{+},\boldsymbol{S}}$ 表示读写器 R 接收到 R_t 和 R_r 经过函数 F 运算后并通过 $\boldsymbol{K}^{+}$ 和 $\boldsymbol{S}$ 加密后的结果。

$\boldsymbol{M}_4: B\lhd *\{F(ID,R_r)\}_{\boldsymbol{K}^{+},\boldsymbol{S}}$ 表示后端数据库 B 接收到 ID 和 R_r 经过函数 F 运算后并通过 $\boldsymbol{K}^{+}$ 和 $\boldsymbol{S}$ 加密后的结果。

$\boldsymbol{M}_5: B\lhd *\{F(R_t,R_r)\}_{\boldsymbol{K}^{+},\boldsymbol{S}}$ 表示后端数据库 B 接收到 R_t 和 R_r 经过函数 F 运算后并通过 $\boldsymbol{K}^{+}$ 和 $\boldsymbol{S}$ 加密后的结果。

$\boldsymbol{M}_6: B\lhd *R_r$ 表示后端数据库 B 接收到随机数 R_r。

$\boldsymbol{M}_7 : R \lhd *DATA$ 表示读写器 R 接收到标签 T 的相关信息 $DATA$。

$\boldsymbol{M}_8 : R \lhd *H(F(ID,R_r))$ 表示读写器 R 接收到 ID 和 R_r 经过函数 F 运算后的单向函数值。

$\boldsymbol{M}_9 : T \lhd *H(F(ID,R_r))$ 表示标签 T 接收到 ID 和 R_r 经过函数 F 运算后的单向函数值。

LAP 协议定义了 10 个初始假设，具体含义如下。

$A_1 : T \ni (ID,R_t)$ 假设标签 T 拥有 ID 和其产生的随机数 R_t。

$A_2 : R \ni R_r$ 假设读写器 R 拥有其产生的随机数 R_r。

$A_3 : B \ni (\boldsymbol{S},\boldsymbol{K},\boldsymbol{K}^+)$ 假设后端数据库拥有保密参数 $\boldsymbol{S}$、$\boldsymbol{K}$ 和 $\boldsymbol{K}^+$。

$A_4 : T \mid\equiv \#(R_r,R_t)$ 假设标签 T 相信随机数 R_t 和 R_r 是新鲜的。

$A_5 : R \mid\equiv \#(R_r,R_t)$ 假设读写器 R 相信随机数 R_t 和 R_r 是新鲜的。

$A_6 : B \mid\equiv \#(\boldsymbol{S},\boldsymbol{K},\boldsymbol{K}^+)$ 假设后端数据库 B 相信保密参数 $\boldsymbol{S}$、$\boldsymbol{K}$ 和 $\boldsymbol{K}^+$ 是新鲜的。

$A_7 : B \mid\equiv \phi(\boldsymbol{S},\boldsymbol{K},\boldsymbol{K}^+)$ 表示后端数据库 B 相信保密参数 $\boldsymbol{S}$、$\boldsymbol{K}$ 和 $\boldsymbol{K}^+$ 是可识别的。

$A_8 : B \mid\equiv \overset{\boldsymbol{K}^+,\boldsymbol{S}}{\mapsto} B$ 假设后端数据库 B 相信 $\boldsymbol{K}^+$ 和 $\boldsymbol{S}$ 是 B 的公钥。

$A_9 : T \mid\equiv T \overset{R_r,R_t,\boldsymbol{K}^+,\boldsymbol{S}}{\leftrightarrow} B$ 假设标签 T 相信 T 和后端数据库 B 共享保密参数 R_r、R_t、$\boldsymbol{K}^+$ 和 $\boldsymbol{S}$。

$A_{10} : B \mid\equiv B \overset{R_r,R_t,\boldsymbol{K}^+,\boldsymbol{S}}{\leftrightarrow} T$ 假设后端数据库 B 相信 B 和标签 T 共享保密参数 R_r、R_t、$\boldsymbol{K}^+$ 和 $\boldsymbol{S}$。

3.2 LAP 协议证明目标

本协议的证明目标主要有 4 个 $G_1 \sim G_4$。

$G_1 : B \ni ID$ 表示后端数据库 B 拥有电子标签 T 的 ID。

$G_2 : R \ni DATA$ 表示读写器 R 拥有电子标签 T 的相关信息 $DATA$。

$G_3 : B \mid\equiv T \mid\sim \{F(ID,R_r)\}_{\boldsymbol{K}^+,\boldsymbol{S}}$ 表示后端数据库 B 相信标签 T 发送了 ID 和 R_r 经过函数 F 运算后又通过 $\boldsymbol{K}^+$ 和 $\boldsymbol{S}$ 加密的结果。

$G_4 : T \mid\equiv B \mid\sim H(F(ID,R_r))$ 表示标签 T 相信后端数据库 B 发送了 ID 和 R_r 经过函数 F 运算后的单向函数值。

3.3 LAP 协议证明

在初始假设的基础上严格遵循 GNY 逻辑推理规则来进行证明，第 n 条形式化消息用 $\boldsymbol{M}_n$ 表示，第 n 条初始假设用 A_n 表示，告知规则、拥有规则和新鲜规则按照文献[8]的表示方法分别用符号 T、P 和 F 来表示。

由消息 $\boldsymbol{M}_4$、告知规则 T_1 可得

① $B \lhd \{F(ID,R_r)\}_{\boldsymbol{K}^+,\boldsymbol{S}}$

由①，初始假设 A_3、告知规则 T_4 可得

② $B \lhd F(ID,R_r)$

由②、拥有规则 P_1 可得

③ $B \ni F(ID,R_r)$

由消息 M_6、告知规则 T_1 可得

④ $B \lhd R_r$

由④、拥有规则 P_1 可得

⑤ $B \ni R_r$

由③、⑤、拥有规则 P_5 可得

⑥ $B \ni ID$，得到 G_1

由消息 $\boldsymbol{M}_7$、告知规则 T_1 可得

⑦ $R \lhd DATA$

由⑦、拥有规则 P_1 可得

⑧ $R \ni DATA$，得到 G_2

由初始假设 A_6、新鲜规则 F_1 可得

⑨ $B \mid\equiv \#(\{F(ID,R_r)\}_{\boldsymbol{K}^+,\boldsymbol{S}},R_r,\boldsymbol{K}^+,\boldsymbol{S})$

由初始假设 A_7、识别规则 R_1 可得

⑩ $B \mid\equiv \phi(\{F(ID,R_r)\}_{\boldsymbol{K}^+,\boldsymbol{S}},R_r,\boldsymbol{K}^+,\boldsymbol{S})$

由⑨、⑩，消息 $\boldsymbol{M}_4$、初始假设 A_3、A_8、A_{10}、消息解释规则 I_2 可得

⑪ $B \mid\equiv T \mid\sim \{F(ID,R_r)\}_{\boldsymbol{K}^+,\boldsymbol{S}}$，得到 G_3

由初始假设 A_4、新鲜规则 F_1 可得

⑫ $T \mid\equiv \#F(ID,R_r)$

由消息 $\boldsymbol{M}_1$、告知规则 T_1 可得

⑬ $T \lhd R_r$

由⑬、拥有规则 P_1 可得

⑭ $T \ni R_r$

由⑭、初始假设 A_1、拥有规则 P_2 可得

⑮ $T \ni F(ID,R_r)$

由⑫、⑮、消息 $\boldsymbol{M}_9$、初始假设 A_9、消息解释规则 I_3 可得

⑯ $T \mid\equiv B \mid\sim H(F(ID,R_r))$，得到 G_4

综上所述，证明目标 G_1、G_2、G_3、G_4 分别在证明过程中的步骤⑥、⑧、⑪、⑯完成。

4　LAP 性能分析

参照文献[9~11]分析 LAP 的安全隐私和性能指标。安全隐私主要指标包括防窃听攻击、防重放攻击、防拒绝服务攻击、防复制攻击、可追踪性、前向安全性等，具体对比如表 4 所示。性能指标主要包括计算量、存储量和通信量，具体对比如表 5 所示。

表 4　　LAP 安全隐私分析对比

方案	窃听攻击	重放攻击	拒绝服务攻击	复制攻击	追踪	前向安全性
文献[2]	×	×	×	√	√	×
文献[3]	×	×	√	×	×	×
文献[4]	×	×	√	×	√	×
文献[5]	×	×	√	√	√	√
文献[11]	×	×	×	√	×	×
LAP	√	√	√	√	√	√

√：安全；×：不安全。

表 5　　LAP 性能分析对比

方案	存储量			计算量			通信量
	标签	读写器	后端数据库	标签	读写器	后端数据库	交互次数
文献[2]	L+2K	—	L+2K	3X+3C+P	—	3X+3C	3
文献[3]	L+2K	2K	L+3K	4X+2C+P	4X+2C+P	—	3
文献[4]	L	—	L	2X+2P	P	2X	4
文献[5]	4K	—	L+5K	5X+3P	3X+3P	D	8
文献[11]	3$\boldsymbol{A}$	2$\boldsymbol{A}$	$\boldsymbol{A}$	rX+3$\boldsymbol{M}$	rX+2$\boldsymbol{M}$+rP	—	3
LAP	2$\boldsymbol{A}$+L	—	3$\boldsymbol{A}$+L+K	5X+C+3$\boldsymbol{M}$+P	P	3X+6$\boldsymbol{M}$	3

$\boldsymbol{A}$：密钥矩阵；L：标签标识符；K：密钥；X：异或操作；$\boldsymbol{M}$：矩阵运算；C：CRC 运算；P：伪随机数运算；D：解密操作；r：表示若干次。

5　结束语

针对现有 RFID 轻量认证协议存在的安全和隐私问题，基于广义逆矩阵，利用 CRC 校验、矩阵运算以及简单逻辑运算设计了一个 RFID 标签和后端服务器之间的双向安全认证协议 LAP。LAP 协议符合 Gen2 标准，适用于低成本电子标签，因此具有广泛的应用前景。后续将在组环境下 RFID 的安全隐私方面继续深入研究。

参考文献：

[1] CHIEN H Y. SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(4):337-340.

[2] DUC D C, PARK J, LEE H, *et al*. Enhancing security of EPC global Gen-2 RFID tag against traceability and cloning[A]. The 2006 Symposium on Cryptography and Information Security[C]. 2006. 269-277.

[3] CHEN C L, DENG Y Y. Conformation of EPC class 1 Generation 2 standards RFID system with mutual authentication and privacy protection[J]. Engineering Applications of Artificial Intelligence, 2009, 22(8): 1284-1291.

[4] LI Y Z, CHO Y B, UM N K, *et al*. Security and privacy on authentication protocol for low-cost RFID[A]. IEEE International Conference on Computational Intelligence and Security[C]. 2006. 1101-1104.

[5] CHOI E Y, LEE D H, LIN J. Anti-cloning protocol suitable to EPC global class-1 Generation-2 RFID systems[J]. Computer Standards & Interfaces, 2009, 31(6):1124-1130.

[6] SUN H M, TING W C. A Gen2-based RFID authentication protocol for security and privacy[J]. IEEE Transactions on Mobile Computing, 2009, 8(1):1-11.

[7] 陈永林. 广义逆矩阵的理论与方法[M]. 南京:南京师范大学出版社,2005.
CHEN Y L. The Theory and Method of Generalized Inverse Matrix[M]. Nanjing: Nanjing Normal University Press, 2005.

[8] GONG L, NEEDHAM R, YAHALOM R. Reasoning about belief in cryptographic protocols[A]. IEEE Computer Society Symposium in Security and Privacy[C]. 1990. 234-248.

[9] SUN H M, TING W C, CHANG S Y. Offlined simultaneous grouping proof for RFID tags[A]. Proceedings of the 2nd International Conference on Computer Science and Its Applications[C]. Jeju, Korea, 2009. 404-409.

[10] 肖锋, 周亚建, 周景贤等. 标准模型下可证明安全的 RFID 双向认证协议[J]. 通信学报, 2013, 34(4):82-87.
XIAO F, ZHOU Y J, ZHOU J X, *et al*. Provable secure mutual authentication protocol for RFID in the standard model[J]. Journal on Communications, 2013, 34(4):82-87.

[11] KARTHIKEYAN S, NESTERENKO M. RFID security without extensive cryptography[A]. Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks[C]. 2005. 63-67.

作者简介：

陈兵（1970-），男，江苏南通人，博士，南京航空航天大学教授，主要研究方向为网络安全、无线网络等。

郑嘉琦（1986-），男，河南平顶山人，南京航空航天大学硕士生，主要研究方向为网络安全。