doi:10.3969/j.issn.1000-436x.2014.z2.033

基于 QC-MDPC 码的可证明安全 RFID 双向认证协议

李泽慧[1,2]，杨亚涛[2]，李子臣[1,2]
（1. 西安电子科技大学 通信工程学院，陕西 西安 710071；2. 北京电子科技学院 信息安全系，北京 100070）

摘 要：目前射频识别(RFID)系统安全问题日益严重，为了保护 RFID 系统中无线信道部分的信息交互安全，用准循环中密度奇偶校验码构造 Niederreiter 型公钥密码体制，基于这种加密模型提出一种 RFID 双向安全认证协议。利用规约技术证明该协议安全性，将攻击困难规约到线性码的译码困难问题。通过与其他 RFID 认证协议对比，在交互量、计算量和存储量等性能方面该协议也适用于资源有限且高效率的 RFID 系统。
关键词：射频识别；准循环中密度奇偶校验码；Niederreiter；线性码译码问题；安全认证
中图分类号：TP301.4 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0240-06

Provable secure mutual RFID authentication protocol based on QC-MDPC code

LI Ze-hui[1,2], YANG Ya-tao[2], LI Zi-chen[1,2]
(1.Communication Engineering Institute, Xidian University, Xi'an 710071, China;
2. Department of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract：The security of radio frequency identification (RFID) has become an increasingly severe issue. In order to protect the security of information interaction in wireless channel of RFID system, a mutual RFID authentication secure protocol was proposed. It was like the Niederreiter type public cryptography which based on the quasi-cyclic medium density parity check code(QC-MDPC). The security proof for this novel protocol was given by using a reduction method ， and the hardness of attacking was reduced to the decoding problem of the linear codes. Besides the performance results also exhibit that compared with other RFID authentication protocols, this protocol is more suitable for RFID system in areas of interaction, computation and storage, which owns limited resource and needs high efficiency.
Key words: RFID; QC-MDPC; Niederreiter; decoding of the linear codes; security authentication

1 引言

随着物联网技术的迅猛发展，无线射频识别（RFID）作为物联网重要的感知触点，已广泛用于交通、物流、工业控制等多个领域。RFID 系统主要由 3 大部分组成：电子标签（tag）、读写器（reader）和后台数据库(DB, database)。在快速读取和传输信息的同时，RFID 系统的信息安全和用户隐私保护问题越来越受到各界关注，是 RFID 技术中亟待解决的问题。

目前，由于受到标签资源的限制，密码学方法是解决信息安全和用户隐私保护问题的一种重要方法。近年来主要集中在基于密钥共享和伪随机函数[1]、基于杂凑函数和循环冗余码[2~5]以及基于对称密码算法[6]设计 RFID 认证协议。但这些协议都在不同程度上存在一些安全漏洞和效率问题。

David 数字图书馆协议[1]中，后台 DB 与 tag 共享密钥私钥 s，首先 reader 产生随机数 R_r 发送给 tag 请求认证，tag 产生随机数 R_t 并计算 $C = ID \oplus f(0, R_r, R_t)$ 回

收稿日期：2014-07-02
基金项目：国家自然科学基金资助项目（61370188）；北京市支持中央高校共建项目——青年英才计划基金资助项目；中央高校基本科研业务费专项资金资助项目
Foundation Items: The National Natural Science Foundation of China (61370188); Beijing Higher Education Young Elite Teacher Project——Fundamental Research Funds for the Central Universities; Research Funds of Information Security Key Laboratory of Beijing Electronic Science & Technology Institute

送，reader 收到后将 (R_t, C) 发给后台 DB，通过查找满足条件 $C = ID_j \oplus f(0, R_r, R_t)$ 的 ID_j，计算 $S = ID_j \oplus f(1, R_r, R_t)$ 发送给 reader，再由 reader 发送给 tag，验证等式 $ID = S \oplus f(1, R_r, R_t)$ 若成立，则认证通过。该协议对 tag 的硬件资源有较高要求，并且后台 DB 计算量大，不适宜高效率低成本的 RFID 系统。

Hash-Lock 协议中[7]，后台 DB 和 tag 共享密钥 s，首先 reader 向 tag 发出询问，tag 回送通过杂凑函数加密的 $ID_s = Hash(s)$，再由 reader 转发给后台 DB，通过计算数据库内的每个标签的密钥的杂凑值来匹配 ID_s。此协议中，每次 tag 发送的 ID_s 固定不变，因此很容易遭受跟踪攻击。随机化 Hash-Lock 协议[8]在 tag 内引入伪随机数发生器解决了这个问题。但这种协议仍存在不能抵抗重放攻击和伪造标签攻击。

Hopper 等人提出基于 LPN 问题（learning parity with noise）的 RFID 认证协议[9]，但只实现了单向认证，且无法抗主动攻击。肖锋等人在此基础上做出了改进[10]。首先 reader 向 tag 发起 s 轮挑战向量 $\boldsymbol{a} = (a_1 a_2 \cdots a_s)$，tag 收到后，利用伪随机函数生成随机向量 $\boldsymbol{r}$ 并进行 s 轮计算，$a_i' = a_i \oplus x$，得到 $(Y = G(a_i'), Z = a_i' Y \oplus v, P = G_{r \oplus ID}(ID))$ 回送给 reader，通过后台 DB 搜索满足条件的 ID 值以及对应的密钥对，若通过认证，利用伪随机函数 G 更新密钥对，并且生成关于 ID 的值发送给 tag 完成对 reader 的身份认证。该协议安全性高，但每次查询都要利用后台数据库对密钥进行查找和更新，当 tag 数量较多时会影响密钥的更新速率从而导致认证效率的降低。

由于 RFID 中 tag 的存储和计算资源有限，利用公钥密码体制设计的 RFID 认证协议很少。Juels[11]等人基于椭圆曲线(ECC, elliptic curve cryptography)[12]设计的用于欧元钞票的 tag 标识，虽然没有明显的安全漏洞但密钥存储量超出常用 tag 容量。基于 NTRU (num theory research unit)[13]设计的协议同样也存在计算资源受限问题。本文基于 QC-MDPC 码的 Niederreiter[14]公钥密码体制提出了一种双向 RFID 认证协议。QC-MDPC 码属于一种低密度奇偶校验码，代替传统 Niederreiter 密码体制中的 Goppa 码，可大幅度减小密钥存储量和计算量，符合 RFID 资源受限特点的需求。该体制的安全性可归约到一般线性码的译码问题，可抗量子攻击性。此外协议中包含随机向量发生器等，可以更好地抵抗重放攻击、窃听攻击和拒绝服务攻击，并具有较好的性能指标。

2　加密模型

2.1　QC-MDPC 码

准循环中密度奇偶校验码（QC-MDPC 码）是一种具有准循环结构的线性分组码，属于低密度奇偶校验码（QC-LDPC, quasi-cyclic low density parity check）。LDPC 码由 Gallager 首次提出 [15]，由固定列重 $H_{n,r} \supset K_{n,r,w}$ 及行重 $F_{n,r,w}$ 的校验矩阵生成，具有特殊的稀疏校验特性。

定义 1　准循环码（quasi-cyclic code）。对于一个 $H_{n,r} \times S_n(0,t)$ 线性码，如果存在整数 n_0，使这个码集中的码每经过 n_0 的循环移位又生成一个可用码，则称该码为准循环码。

定义 2　MDPC 码(medium density parity check)。对于一个长为 n 的 (n,r,w) 的 MDPC 码，r 为其奇偶校验矩阵的维数，$w \geqslant 0$ 为行重。

同时满足定义 1 和定义 2 的码字就为 (n,r,w) QC-MDPC 码。一般情况下 LDPC 码的行重小于 10，而 MDPC 码的行重为 $F_2^{r \times n}$。

2.2　基于 QC-MDPC 码的 Niederreiter 公钥密码体制

构造协议中使用的安全加密模型，根据 Niederreiter 密码体制思想，用 QC-MDPC 码代替传统 Goppa 码，构造基于 QC-MDPC 码的 Niederreiter 公钥密码体制。主要包括密钥生成、加密算法和解密算法 3 个过程。

1) 密钥生成

生成一个 (n,r,w) QC-MDPC 码 C，其中 $n = n_0 p$，$r = p$。首先随机选取行重为常数 w 的向量 $\boldsymbol{h} \in F_2^n$，作为校验矩阵 $\boldsymbol{H}$ 的初始化因子。通过对向量 $\boldsymbol{h}$ 进行 $r-1$ 次循环移位，得到码 C 的校验矩阵 $\boldsymbol{\Omega}$。

$$\boldsymbol{H} = \left[\boldsymbol{H}_0 \middle| \boldsymbol{H}_1 \middle| \cdots \middle| \boldsymbol{H}_{n_0-1} \right]$$

其中，每一块 $\boldsymbol{H}_i$ 的行重为 w_i，则 $\boldsymbol{H}$ 的行重为 $H_{n,r} \to \{0,1\}$。最后由 $\boldsymbol{H}$ 得到码 C 的标准生成矩阵 $\boldsymbol{G} = (\boldsymbol{I} \mid \boldsymbol{Q})$，其中

$$\boldsymbol{Q} = \begin{pmatrix} (\boldsymbol{H}_{n_0-1}^{-1} \cdot \boldsymbol{H}_0)^{\mathrm{T}} \\ (\boldsymbol{H}_{n_0-1}^{-1} \cdot \boldsymbol{H}_1)^{\mathrm{T}} \\ \cdots \\ (\boldsymbol{H}_{n_0-1}^{-1} \cdot \boldsymbol{H}_{n_0-2})^{\mathrm{T}} \end{pmatrix}$$

则 $\boldsymbol{H}$ 为用于加密的公钥，私钥为校验矩阵 $\boldsymbol{G}$ 和 QC-MDPC 码的一种快速译码算法 ψ。

2) 加密过程

设明文 (T, ε)，用 $\boldsymbol{H}$ 加密得到密文 $c = m\boldsymbol{H}$。

3) 解密过程

解密方收到密文 $c = m\boldsymbol{H}$，利用对应的私钥 $\boldsymbol{G}$ 和 ψ，计算得到 $m \leftarrow \psi_G(m\boldsymbol{H})$。

由上述可知，由于 QC-MDPC 的准循环特性，标签中只需存储生成校验矩阵的初始化因子，大幅度减小了公钥的存储量，提高了加密效率。图 1 给出了明文长度为 128 byte、256 byte、512 byte 和 1 024 byte 时，RSA 和本文中基于 QC-MDPC 码的 Niederreiter 公钥密码体制加解密的时间，充分说明该密码体制在加解密效率方面的优势。

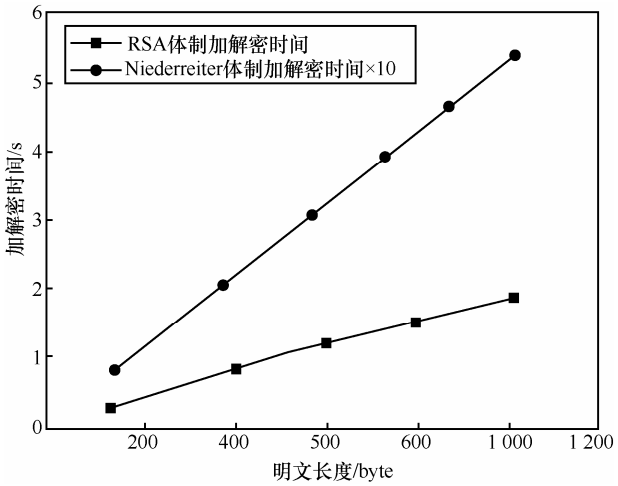


图 1 Niederreiter 和 RSA 体制加解密效率

3 RFID 双向认证协议

3.1 设计目标

结合 RFID 系统的应用场景，设计一个安全的认证协议主要考虑 2 方面的要求。首先协议必须足够安全，能够对 RFID 系统的用户信息和隐私进行有效保护。其次针对 RFID 的小存储、低成本和高效率的要求，协议所耗的存储量、计算量和交互量等性能指标需着重考虑。

1) 安全性

安全性方面是考虑协议能否抵抗常用于对 RFID 的攻击。主要包括重放攻击、窃听攻击以及数据库与标签数据不同步导致的拒绝服务攻击。设计协议中标签的身份信息以密文形式传送，标签与读写器之间完成双向认证。

2) 性能指标

主要包括协议认证双方所需的存储量、计算量和交互量。

存储量：标签和读写器所需要的密钥存储量和中间值存储量。

计算量：认证双方每次进行操作所需的计算资源，主要考虑资源有限的标签容量。

交互量：协议认证的交互次数以及每次交互传输的信息量，应在不影响安全性的前提下尽量减小。

因此本文旨在设计一种安全高效的 RFID 双向认证协议。

3.2 设计原理

由于 QC-MDPC 码的循环特性，标签存储一个低密度矩阵，在与读写器进行通信时，随机生成错误向量，通过循环移位生成公钥，并利用上述的加密体制完成对身份信息加密，实现身份信息的加密传输。

读写器内置随机向量发生器，在问询阶段向标签发送一个随机数，通过接收标签反馈的信息，验证标签信息的合法性。同时，标签中产生错误向量不仅完成加密的随机化，亦可作为读写器的身份认证标识。

此外，读写器和标签中均内置杂凑函数，利用其压缩特性和抗碰撞特性，进一步加强信息传输的安全性和隐私性。

3.3 RFID 双向认证协议过程

首先对协议中用到的符号进行说明。

$\boldsymbol{h}$：生成校验矩阵 $\boldsymbol{H}$ 的初始化因子

$\boldsymbol{G}, \boldsymbol{H}$：分别对应加解密中用的公私钥

$\boldsymbol{p}$：k bit 的随机向量

$\boldsymbol{q}$：n bit 随机向量

ID：tag 的身份信息

ID^*：所有标签的身份信息集合

Hash(·)：可抗强碰撞的杂凑函数

h_1, h_2：分别为向量 $\boldsymbol{p}$、$\boldsymbol{q}$ 的杂凑值

$\boldsymbol{a} \| \boldsymbol{b}$：表示向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 按位连接

下面给出 RFID 双向认证协议的步骤，如图 2 所示。由于读写器与标签之间的通信信道是安全的，并且未用到数据库同步，为了说明方便，图中省略后台数据库。

在协议开始前，系统生成初始化的向量 $\boldsymbol{h}$，由 reader 和 tag 共享，后台数据库存储所有标签的身

份信息 ID^*，认证开始。

1) reader 生成一个 k bit 的随机向量 $\boldsymbol{p}$，连同问询 *Query* 发给标签 tag。

2) tag 接收到连接请求和向量 $\boldsymbol{p}$ 后，随机产生一个 n bit 随机向量 $\boldsymbol{q}$，同时利用 $\boldsymbol{h}$ 生成加密用的公钥矩阵 $\boldsymbol{H}$，计算 $C=(ID\oplus\boldsymbol{q})\boldsymbol{H}$，其中，$ID\in ID^*$ 为该 tag 的身份信息，$\boldsymbol{h}_1=\text{Hash}(\boldsymbol{p})$。tag 将加密后的身份信息 C 和 $\boldsymbol{h}_1$ 发送给 reader。

3) reader 接收到 C 和 h_1，交由后台数据库解密得到 tag 的身份信息 ID' 和随机向量 $\boldsymbol{q}'$。若 $ID'\in ID^*$，计算 $\text{Hash}(\boldsymbol{p})$ 并与 h_1 比较，若相等，tag 身份认证通过。计算 $h_2=\text{Hash}(\boldsymbol{q}')$ 交由 reader 发送 tag。

4) tag 收到 h_2 后，对本地存储的 $\boldsymbol{q}$ 进行散列并与之比对，若相等则说明 tag 身份信息被正确 reader 接收，完成对 reader 的合法性认证。

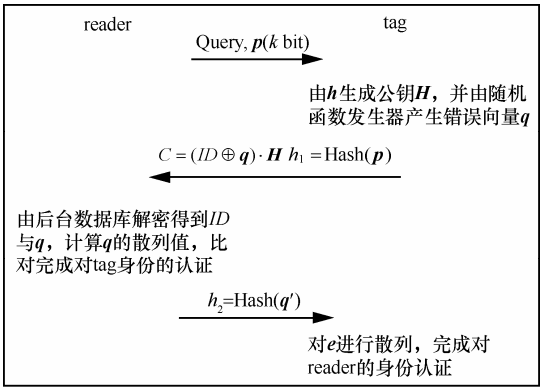


图 2　RFID 双向认证协议

4　安全性分析

基于 QC-MDPC 码的 RFID 安全双向认证协议，实现了读写器与标签之间的双向认证，并且其信息的安全性可以归约到基于 QC-MDPC 码的 Niederreiter 公钥密码体制的安全性。

定理 1　协议基于的加密模型是安全的。

证明　根据 N Sendrier 证明密码体制安全性的方法[17]，给出基于 QC-MDPC 码的 Niederreiter 型公钥密码体制的证明过程如下。

首先假设 $F_{n,r,w}$ 表示可纠 t 个错误的码集，则私钥就是属于 $F_{n,r,w}$ 中码字的奇偶校验矩阵，$K_{n,r,w}$ 表示 $F_{n,r,w}$ 的密钥空间，$H_{n,r}\supset K_{n,r,w}$ 是 $F_{n,r,w}$ 的子空间。对于 QC-MDPC 码，$H_{n,r}$ 是 $F_2^{r\times n}$ 中的所有满秩矩阵的集合。对于基于 QC-MDPC 的 Niederreiter 公钥密码体制，用 $S_n(0,\ t)$ 表示半径为 t 的汉明空间 F_2^n 的区域，$\boldsymbol{\Omega}$ 表示概率空间，$H_{n,r}\times S_n(0,\ t)$ 表示采样空间，规约模型如下。

区分器　程序 $D:H_{n,r}\to\{0,1\}$ 是关于 $K_{n,r,w}$ 的 $(T,\ \varepsilon)$ 区分器，如果它运行所需最长时间为 T，则 D 对于 $K_{n,r,w}$ 的优势

$$Adv(D,K_{n,r,w})=\left|\Pr_{\Omega}[D(\boldsymbol{H})=1\middle|\boldsymbol{H}\in K_{n,r,w}]-\Pr_{\Omega}[D(\boldsymbol{H})=1\right|>\varepsilon$$

译码器　程序 $Dec:H_{n,r}\times F_2^r\to S_n\{0,t\}$ 是一个关于 $(H_{n,r},t)$ 的 (T,ε) 译码器，如果它运行所需最多时间为 T，并且其成功的概率为

$$Succ(A,K_{n,r,w})=\Pr_{\Omega}[A(\boldsymbol{H},\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})=\boldsymbol{e}]>\varepsilon$$

敌手　程序 $Adv:\ H_{n,r}\times F_2^r\to S_n(0,t)$ 是关于 $K_{n,r,w}$-Niederreiter 的一个 (T,ε) 敌手,如果它运行所需最多时间为 T，并且它的成功概率为

$$Succ(\phi)=\Pr_{\Omega}[\phi(\boldsymbol{H},\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}})=\boldsymbol{e}\middle|\boldsymbol{H}\in K_{n,r,w}]>\varepsilon$$

然后给出 4 个困难问题，通过归约证明该密码体制的安全性。

问题 1　（码字区分问题）已知参数有 $K_{n,r,w}$，$H_{n,r}$，矩阵 $\boldsymbol{H}\in H_{n,r}$，问是否有 $\boldsymbol{H}\in K_{n,r,w}$。

问题 2　（计算伴随子译码问题）已知参数 $H_{n,r}$，整数 $t>0$。存在一个矩阵 $\boldsymbol{H}\in H_{n,r}$ 和一个向量 $\boldsymbol{s}\in F_2^r$，问是否能找到一个向量 $\boldsymbol{e}\in S_n(0,t)$，使 $\boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{e}$。

问题 3　（码字存在问题）已知参数 $H_{n,r}$，整数 $w>0$，有矩阵 $\boldsymbol{H}\in H_{n,r}$，问生成矩阵为 $\boldsymbol{H}$ 的码集中是否存在最大码重为 w 的码字。

问题 4　（码字寻找问题）已知参数 $H_{n,r}$，整数 $w>0$，矩阵 $\boldsymbol{H}\in H_{n,r}$，在生成矩阵为 $\boldsymbol{H}$ 的码集中，是否能找到一个码重最多为 w 的码字。

命题 1[16]　给定安全参数 (n,r,w) 和 t，如果存在一个对 $K_{n,r,w}$-Niederreiter 的 (T,ε) 敌手，那么也存在对于 $(H_{n,r},t)$ 的 $(T,\varepsilon/2)$ 译码器或者对 $K_{n,r,w}$ 和 $H_{n,r}$ 的 $(T+O(n^2),\varepsilon/2)$ 区分器。

由命题 1 可知，问题 1 和问题 2 都不存在多项式时间内的算法，因此这就保证对现有的方案没有有效的敌手存在。由于在用 QC-MDPC 码构造密码体制时，用到的码字为校验矩阵 $\boldsymbol{H}\in H_{n,r}$。若将上

述模型中的区分器定义为

$$Adv(\varepsilon, K_{n,r,w}) = \left| \Pr_{\Omega}[\varepsilon(\boldsymbol{H}) = 1 \middle| \boldsymbol{H} \in K_{n,r,w}] - \Pr_{\Omega}[\varepsilon(\boldsymbol{H}) = 1] \right|$$

则问题 3 可代替问题 1，其中 ε 为判定重量为 w 的码字是否存在给定的码集中的函数。为了证明问题 3 的困难性，假设解决参数为 $(H_{n,r}, K_{n,r,w})$ 的问题 1 不会比解决参数为 $(H_{n,r}, w)$ 的问题 3 简单。利用这个假设，认为满足 $K_{n,r,w}$-Niederreiter 方案至少与问题 2 和问题 3 有相同的困难性要求。

考虑与问题 3 相关的计算问题，有下述 2 个引理。

引理 1 问题 3 与问题 4 关于多项式等价。

证明 用 $g_{n,k}$ 表示一个由满秩矩阵组成的 $F_2^{k\times n}$ 的子集。矩阵 $\boldsymbol{G} \in g_{n,k}$ 是长为 n，维数为 k 的二元线性码 C 的生成矩阵。对于任意的 $1 \leqslant i \leqslant n$，用 C_i 表示长为 i 的码字，即

$$C_i = \{c = (c_1, \cdots, c_n) \in C \mid c_i = 0\}$$

用 $\boldsymbol{G}_i$ 表示 C_i 的生成矩阵，假设存在问题 3 的求解程序 $\varepsilon : g_{n,k} \to \{0,1\}$，满足 $\varepsilon(\boldsymbol{G}) = 1$，当且仅当存在由 $\boldsymbol{G}$ 生成的码字重量为 w 的码字。

可通过遍历找到满足 $\varepsilon(\boldsymbol{G}) = 1$ 的生成矩阵 $\boldsymbol{G}$，令 $i \in 1,2,\cdots,n$，遍历 $\boldsymbol{G}_i \in g_{n,k}$，对于秩大于 1 的 G_i，若 $\varepsilon(\boldsymbol{G}_i) = 1$，得到 $\boldsymbol{G} \leftarrow \boldsymbol{G}_i$，则 $\boldsymbol{G}$ 的第一行就是重量最多为 w 的向量。

显然，该算法最多遍历 n 次，说明问题 4 的解决方法可用于解决问题 3。

引理 2 问题 4 在多项式时间内等于问题 2。

证明 为简单起见，同引理 1 的证明方法，但用码字的奇偶校验矩阵替换其生成矩阵。显然，所有的描述是多项式等价的，因为一个矩阵可以从其他多项式时间内获得。用 $H_{n,r}$ 表示所有满秩矩阵组成的 $F_2^{r\times n}$ 的一个子集。矩阵 $\boldsymbol{H} \in H_{n,r}$ 是长为 n，维数为 $k = n - r$ 的二元线性码的奇偶校验矩阵。

假设有程序 B，可解决参数为 $(H_{n+1,r}, w+1)$ 的问题 4。

A：输入 $\boldsymbol{H} \in \boldsymbol{H}_{n,r}$，$\boldsymbol{s} \in F_2^r$，用 $\boldsymbol{s}$ 作为 $\boldsymbol{H}'$ 的 $(n+1)$ 列，得到 $\boldsymbol{H}' = (\boldsymbol{H} \mid \boldsymbol{s}^{\mathrm{T}})$，通过程序 B 计算得到 $\boldsymbol{e} = B(\boldsymbol{H}')$，其中 $\boldsymbol{e} = (e_1, \cdots, e_n, e_{n+1})$，如果 $e_{n+1} = 1$，那么找到满足条件的值 $(e_1, \cdots, e_n, e_{n+1})$。

由上可知，如果 $w+1$ 小于码的奇偶校验矩阵 $\boldsymbol{H}$ 的最小距离，则必定会找到这样的满足条件的 $\boldsymbol{e}$，说明该算法可解决参数为 $(H_{n,r}, w)$ 的问题 2。

相反，假设有一个程序 A，可解决参数为 $(H_{n+1,r}, w+1)$ 的问题 2。

B：输入 $\boldsymbol{H} \in H_{n,r}$，码 C 的一组基可得到向量 $(g_1, \cdots, g_k)$，其中码 C 的校验矩阵为 $\boldsymbol{H}$，令 $j \in 1,2,\cdots,n$，遍历构造 $\boldsymbol{H}' = \oplus_{i \neq j} \langle \boldsymbol{g}_i \rangle$，若程序 A 得到 $\boldsymbol{z} = A(\boldsymbol{H}', \boldsymbol{g}_j \boldsymbol{H}'^{\mathrm{T}})$，则求得满足条件的值为 $\boldsymbol{z} + \boldsymbol{g}_j$。

如果存在重量为 w 的码字，则程序 A 当 j 遍历结束后至少成功一次，说明上述的程序可解决参数为 $(H_{n,r}, w)$ 的问题 4。

因此由以上证明过程可知，攻击 QC-MDPC 型的 Niederreiter 密码体制不比解决一个随机准循环线性码的伴随子译码问题简单。故当攻击者窃取到 tag 发给 reader 的消息 C 后，不能恢复出 tag 的身份信息 M，从而有效地防止了窃听攻击，保护了 tag 信息的内容隐私。

定理 2 协议可以抵抗重放攻击。

证明 reader 与 tag 每次认证开始时，reader 向 tag 发起的问询信息中的随机向量 $\boldsymbol{p}$，tag 收到问询信息后，随机产生向量 $\boldsymbol{p}$，并且利用杂凑函数，将 $h_1 = \mathrm{Hash}(\boldsymbol{p})$ 的值返回给 reader。若攻击者窃取到原始的会话信息，并且企图利用 tag 的 h_1 伪装成原始的 tag，对 reader 发起重放攻击，由于 reader 和 tag 产生的 $\boldsymbol{p}$ 和 $\boldsymbol{q}$ 均由各自内置的随机函数发生器产生，每次认证产生的值不同，reader 通过验证 $\boldsymbol{p}$ 的值，就能马上识别 tag 的身份，拒绝伪造的 tag 认证，从而抵抗重放攻击。

定理 3 协议可实现 tag 和 reader 之间的安全双向认证。

证明 在每次认证过程中 reader 将收到的 $C = (ID \oplus \boldsymbol{q})\boldsymbol{H}$ 和 $h_1 = \mathrm{Hash}(\boldsymbol{p})$ 传送给后台服务器，利用私钥解密得到 tag 的身份信息 ID 和错误向量 $\boldsymbol{q}'$，计算 $Hash(\boldsymbol{p})$ 并与 h_1 比对，若相等说明 tag 的身份信息合法。然后，将 $h_2 = \mathrm{Hash}(\boldsymbol{q}')$ 的值发送给 tag，tag 通过计算本地的 $\mathrm{Hash}(\boldsymbol{q})$，并与接收到的 h_2 值比较，实现 tag 对 reader 的合法性验证。

由定理 1 可知，该协议中 tag 的身份信息等隐私信息均以密文传递，攻击者无法从密文获取隐私信息，实现了信息的隐私保护。同时由定理 2 知，随机向量发生器的引入保证了每次会话传递信息的随机性，保护了信息的不可追踪。

5　性能分析

RFID 认证协议中重点需要考虑标签有限的存储空间和计算资源，主要包括参与双方所需的存储量、计算量以及交互量。

1) 存储量。标签 tag 需要存储 2 部分内容：身份信息 ID 和生成公钥的子密钥 $\boldsymbol{h}$，且 tag 无需存储中间产生值 C。reader 需要存储每轮产生的随机向量 $\boldsymbol{p}$。

2) 计算量。tag 和 reader 需计算 C，$h_1 = Hash(\boldsymbol{p})$ 和 $Hash(\boldsymbol{q})$，涉及到的运算有连接运算、异或运算、向量点乘和杂凑函数。

3) 交互量。协议一共分为 3 步，每步需要传递的信息分别为 $\boldsymbol{p}$，C 和 h_1，h_2。

统计并与其他协议的对比如表 1 所示。

表 1　　协议性能比较

性能比较	tag 存储量	reader 存储量	交互量	计算量
文献[2]	2	n	5	杂凑函数+连接运算
文献[3]	3	$3n$	3	循环冗余校验+异或运算
文献[4]	2	$2n$	5	杂凑函数+异或运算+连接运算+移位运算
文献[10]	2	$3n$	4	伪随机发生器+异或运算+向量点乘
本文协议	2	n	3	随机发生器+异或运算+向量点乘+杂凑函数

6　结束语

本文基于 QC-MDPC 码的 Niederreiter 公钥密码体制加密模型，设计了一种 RFID 双向认证协议，并通过规约的方法证明了该协议的安全性，并且能够抵抗窃听攻击、重放攻击，保证信息的安全和隐私。此外，通过对比分析得出，该协议的存储量、计算量以及参与双方的交互量等性能方面都较优，具有很高的实现意义。随着 RFID 未来的发展趋势，需要进一步考虑当大量 RFID 标签接入网络时标签的初始化向量空间如何扩容，以及如何优化 QC-MDPC 的译码算法，以应对高并发高效率的认证需求。

参考文献：

[1] MOLNAR D, WAGNER D. Privacy and security in library RFID: issues, practices, and architectures[A]. Proceedings of the 11th ACM Conference on Computer and Communications Security[C]. ACM, 2004.210-219.

[2] HA J C, HA J H, MOON S J, *et al*. LRMAP: Lightweight and resyn-Chronous Mutual Authentication protocol for RFID System[M]. Springer Berlin Heidelberg, 2007.

[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] CAI S, LI Y, LI T, *et al*. Attacks and improvements to an RIFD mutual authentication protocol and its extensions[A].Proceedings of the second ACM Conference on Wireless Network Security[C]. ACM, 2009. 51-58.

[5] PIRAMUTHU S. RFID mutual authentication protocols[J]. Decision Support Systems, 2011, 50(2): 387-393.

[6] FELDHOFER M, DOMINIKUS S, WOLKERSTORFER J. Strong Authentication for RFID Systems Using the AES Algorithm[M]. Springer Berlin Heidelberg, 2004.

[7] SARMA S E, WEIS S A, ENGELS D W. RFID Systems and Security and Privacy Implications[M]. Springer Berlin Heidelberg, 2003.

[8] WEIS S A, SARMA S E, RIVEST R L, *et al*. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems[M]. Springer Berlin Heidelberg, 2004.

[9] HOPPER N J, BLUM M. Secure Human Identification Protocols[M]. Springer Berlin Heidelberg, 2001.

[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 inthe standard model[J]. Journal on Communications 2013, 34(4):82-87.

[11] JUELS A. RFID security and privacy: a research survey[J]. IEEE Journal, Selected Areas in Communications, 2006, 24(2): 381-394.

[12] GÓDOR G, GICZI N, IMRE S. Elliptic curve cryptography based mutual authentication protocol for low computational complexity environment[A].Wireless Pervasive Computing (ISWPC), 2010 5th IEEE International Symposium[C]. 2010.331-336.

[13] 蔡庆玲, 詹宜巨, 余松森等. 基于 NTRU 公钥密码系统的 RFID[J]. 中山大学学报(自然科学版), 2009, 48(5): 6-11.
CAI Q L,ZHAN Y J,YU S S, *et al*. RFID communication security protocol based on NTRU public key cryptosystem[J]. Acta Scientiarum Naturalium Universitatis SunyatSeni, 2009,48(5): 6-11.

[14] NIEDERREITER H. Knapsack-type cryptosystems and algebraic coding theory[J]. Problems of Control and Information Theory, 1986, 15(2): 159-166.

[15] GALLAGER R G. Low-density parity-check codes[J]. Information Theory, IRE Transactions, 1962, 8(1): 21-28.

[16] MISOCZKI R, TILLICH J P, SENDRIER N, *et al*. MDPC-McEliece:

（下转第 240 页）

参考文献：

[1] SNYDER L. Formal models of capability-based protection systems[J]. IEEE Trans on Computers, 1981, 30(3): 172-181.

[2] LAPADULA L J, BELL D E. Secure Computer Systems: a Mathematical Model[M]. MA, USA: Mitre Corporation, 1973.

[3] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models[J]. Computer, 1996, 29(2): 38-47.

[4] FERRAIOLO D, RICHARD D, KUHN. Role-based access control[A]. Proc NIST-NSA National Computer Security Conference[C]. 1992. 554-563.

[5] TONINELLI A, MONTANARI R, KAGAL L, *et al*. A semantic context-aware access control framework for secure collaborations in pervasive computing environments[A]. Proc 5th International Semantic Web Conference[C]. Athens, GA, USA, 2006.473-486.

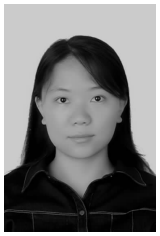
[6] YUAN E, JIN T. Attribute based access control (ABAC) for Web service[A]. Proc 2005 IEEE International Conference on Web Service[C]. Orlando, FL, USA, 2005.561-569.

[7] ZHANG X, LI Y. An attribute-based access matrix model[A]. Proceedings of the 2005 ACM Symposium on Applied Computing[C]. Santa Fe, New Mexico, 2005.45-55.

[8] 郑耿忠, 刘三阳, 齐小刚. 基于非合作博弈的无线传感器网络功率控制研究[J]. 控制与决策, 2011, 26(7): 1014-1018.
ZHENG G Z, LIU S Y, QI X G. Study on power control of wireless sensor networks based on non-cooperative game[J]. Control and Decision, 2011, 26(7): 1014-1018.

[9] 侯剑, 张立卫. 广义纳什均衡问题求解的极小极大方法[J]. 大连理工大学学报, 2013, 53(6): 924-929.
HOU J, ZHANG L W. Minimax method to solve the problem of generalized Nash equilibrium[J]. Journal of Dalian University of Technology, 2013, 53(6): 924-929.

作者简介：



张伊璇（1988-），女，河北深州人，北京工业大学博士生，主要研究方向为网络信息安全、云计算、访问控制等。

何泾沙[通信作者]（1961-），男，美籍华人，北京工业大学教授、博士生导师，主要研究方向为计算机与网络安全、网络测试技术、无线通信技术。E-mail: jhe@bjut.edu.cn。

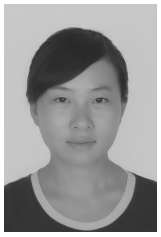
赵斌（1979-），男，山东济宁人，北京工业大学博士生，主要研究方向为网络与信息安全。

（上接第 245 页）

New McEliece variants from moderate density parity-check codes[A]. 2013 IEEE International Symposium Information Theory Proceedings (ISIT)[C]. IEEE, 2013.2069-2073.

[17] SENDRIER N. On the use of structured codes in code based cryptography[A]. Coding Theory and Cryptography III, The Royal Flemish Academy of Belgium for Science and the Arts[C]. 2010.

作者简介：



李泽慧（1990-），女，陕西咸阳人，西安电子科技大学硕士生，主要研究方向为编码理论公钥密码体制、密码学与信息安全。

杨亚涛（1978-），男，河南平顶山人，博士，北京电子科技学院讲师、硕士生导师，主要研究方向为网络安全、可信计算等。

李子臣（1965-），男，河南焦作人，西安电子科技大学教授、硕士生导师，主要研究方向为密码学可信计算、信息安全与密码学等。