

基于 QC-LDPC 码的 Niederreiter 公钥密码体制

杨磊鑫,杜伟章

(长沙理工大学 计算机与通信工程学院,长沙 410114)

(ylx2010000@163.com)

摘要:提出基于准循环低密度奇偶校验(QC-LDPC)码构造的 Niederreiter 公钥密码体制。由于 QC-LDPC 的校验矩阵具有稀疏和分块循环的特性,且 QC-LDPC 的纠错能力大,与以往基于纠错码构造的公钥密码体制相比,该体制密钥量大大减少,提高了传信率。同时引入对角形式的可逆变换矩阵 Q ,通过线性变换产生新的校验矩阵 H' ,隐藏了码字的校验矩阵,可以抵消矩阵 H' 稀疏易攻击的弱点,增加了体制的安全性。并且通过对现有的攻击方法分析,证明了体制的安全性。

关键词:低密度奇偶校验码;准循环低密度奇偶校验码;循环矩阵;Niederreiter 公钥密码体制;安全分析

中图分类号:TP309 **文献标志码:**A

Niederreiter public-key cryptosystem based on QC-LDPC

YANG Lei-xin, DU Wei-zhang

(College of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha Hunan 410114, China)

Abstract: A Niederreiter public-key cryptosystem based on Quasi-Cyclic Low-Density Parity Check (QC-LDPC) Code was proposed. As the check matrix of QC-LDPC is sparse, and has the structure of circulative blocks and high error correction capability, compared with other public-key cryptosystem, the key sizes of the new cryptosystem were reduced and transmission rate was improved. A new parity-check matrix was mapped by invertible transformation matrix Q with diagonal form. The sparse characteristic of H' is countervailed. Through analyzing the existing attacking methods, security of the cryptosystem has been confirmed.

Key words: Low-Density Parity Check (LDPC) Code; Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) Code; cyclic matrices; niederreiter public-key cryptosystem; security analysis

0 引言

1978年,McEliece利用一般线性码的译码问题是一个NP完全问题^[1]和Goppa码有快速译码算法的特点首次提出了基于纠错码的公钥密码体制,简称M公钥体制^[2]。1986年,Niederreiter提出了另一个基于纠错码的公钥密码体制^[3],简称N公钥密码体制。虽然基于纠错码的公钥密码体制加解密算法简单,安全性高,但是也存在一些弱点,比如需要存储的密钥量大,传信率低等,这也是该公钥体制很少在实际中应用的原因。随着计算机技术的不断发展,对公钥密码体制的安全性提出了更高的要求,由此对纠错码的纠错能力和传信率也提出了更高的要求,许多高性能的纠错码相继诞生。如何利用高性能的纠错码来构造实用安全的公钥密码体制成为众多学者研究的内容。

低密度奇偶校验(Low-Density Parity Check, LDPC)码由Gallager在1962年首次提出^[4],在近年来受到广泛关注,并且有了很多新的研究成果。它可以说是在纠错码领域继Turbo码后的又一重大发现,研究发现LDPC码的性能优于Turbo码,如译码复杂度低于Turbo码,且可实现完全的并行操作,硬件实现复杂度低,有较好的纠错能力,尤其是其简单实用,且接近于Shannon限,成为下一代通信纠错编码的首选。

2000年,Monico等人用LDPC码构造了McEliece公钥密码体制^[5],虽然减少了密钥量增加了传信率,但是却是以牺

牲安全性为代价的。准循环低密度奇偶校验(Quasi-Cyclic Low-Density Parity-Check, QC-LDPC)码是利用代数学或者组合理论构造的一类非常重要的LDPC码,能够接近于Shannon限,在基于置信传播原则上有很好的软判决译码算法^[6]。与其他LDPC码相比,QC-LDPC码具有非常低的线性编码复杂度,实用性更强。2007年,Baldi等人使用QC-LDPC码构造新的McEliece公钥密码体制,并进行了安全分析^[7]。

虽然M公钥和N公钥密码体制是等价的^[8],但在相同的参数下,N公钥却有着公钥存储量低,传信率高的优点,并且学者对N公钥的研究相比M公钥较少,所以本文着重研究N公钥密码体制。本文首先介绍QC-LDPC码的概念,指出其特点,在此基础上提出基于QC-LDPC码的Niederreiter公钥密码体制,由于QC-LDPC码的校验矩阵是稀疏矩阵且具有分块循环的特点,大大减少了密钥存储量;并且QC-LDPC码设计简单,使得传信率有所提高;由于QC-LDPC码具有结构稀疏的特点,容易通过寻找低重量码字获得明文,本文使用可逆变换矩阵代替原始方案中的置换矩阵,增强了方案的安全性,证明该体制可以抵抗现有的攻击方法。

1 基本概念

1.1 LDPC码

LDPC码是一种由稀疏矩阵定义的线性分组码,它的校验矩阵是“稀疏”矩阵。一个二元 (n, k) LDPC码 C 是通过 $(n -$

收稿日期:2011-01-14;修回日期:2011-02-22。

作者简介:杨磊鑫(1984-),男,安徽阜阳人,硕士研究生,主要研究方向:信息安全;杜伟章(1965-),女,湖南长沙人,教授,博士,主要研究方向:密码学、信息安全、信道编码。

$k) \times n$ 的奇偶校验矩阵 H 来定义的, 即: $C = \{c \in GF(2)^n : H \cdot c^T = 0\}$, 其中 n 为码长, k 为信息位个数, $n - k$ 为校验个数, 码率 $R = k/n$ 。

二元 LDPC 码的校验矩阵 H 须满足:

- 1) H 矩阵每行有 p 个“1”;
- 2) H 矩阵每列有 q 个“1”;
- 3) H 矩阵的任意两行(或两列) 共同“1” 的个数不超过1。
- 4) 与行列数相比, p 和 q 很小, 即矩阵中除少数元素为 1 外, 其余大部分元素都为零, 就是说矩阵 H 为稀疏矩阵。

满足以上四个条件的 H 校验矩阵对应的 LDPC 码一般表示为 (n, p, q) 。

对 LDPC 码研究的一个质的跨越就是使用 Tanner 图来表示 LDPC 码, 它和校验矩阵是一一对应的^[9]。Tanner 图可以用 $G = (V, E)$ 来描述, 其中 V 是节点的集合, $V = V_b \cup V_c$ 。对于校验矩阵 H , $V_b = (b_1, b_2, \dots, b_n)$ 称为比特节点, 对应校验矩阵的列, 也对应码字中的比特。 $V_c = (c_1, c_2, \dots, c_{n-k})$ 是校验节点, 对应校验矩阵的行, 也对应校验方程。 E 是比特节点和校验节点之间相邻边的集合, 设 h_{ij} 为矩阵 H 的元素。当 $h_{ij} = 1$ 时, 对应的节点 c_i 和 b_j 之间有一条边相连。与节点相连的边的数目称为该节点的度 (degree), 从某个节点出发又回到此节点的路径为一循环 (cycle), 所经过的边的条数成为循环的长度。

如一个二元的 $(10, 2, 4)$ LDPC 码的校验矩阵为:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

其中 10 表示校验矩阵的列数, 2 为行重, 4 为列重, 则该校验矩阵对应的 Tanner 图如图 1 所示。

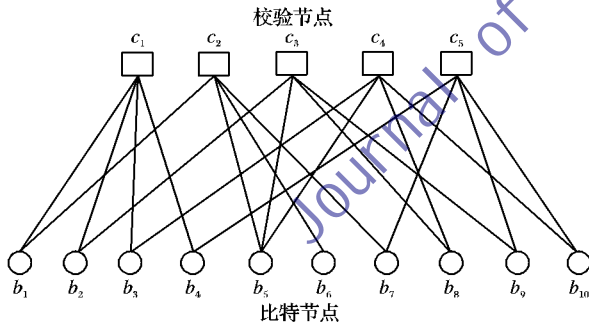


图 1 $(10, 2, 4)$ LDPC 码的校验矩阵对应的 Tanner 图

一般情况下, 校验矩阵是随机构造的, 因此是非系统化的, 在编码时, 将校验矩阵 H 进行高斯消元, 可得: $H = [I | P]$, 则生成矩阵 $G = [-P^T | I]$, 其中 I 为单位矩阵。

1.2 QC-LDPC 码

定义 1 循环矩阵。一个 $L \times L$ 阶的右移循环矩阵如下:

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{L-1} \\ a_{L-1} & a_0 & \cdots & a_{L-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$$

将矩阵中每一行向右循环移动一个单位, 就得到矩阵的下一行; 将矩阵最后一行向右循环移动一个单位, 就得到矩阵的第一行; 同理将矩阵中每一列向下循环移动一个单位, 就得到矩阵的下一列; 将矩阵最后一列向下循环移动一个单位, 就

得到了矩阵的第一列。可以看出循环矩阵 A 可以由矩阵的其中一行或者一列来描述。

一个二进制循环码是模 $x^L - 1$ 多项式剩余类线性组合代数中的一个理想, 在理想中可以找到一个次数最低的非零首一多项式 $a(x)$, 由它的一切倍式可以生成的一个循环码, 我们称多项式 $a(x)$ 为该循环码的生成多项式, 可以表示为 $a(x) = x^r + x^{r-1} + \cdots + x + x^0$, 其中每一项前面的系数为 0 或是 1。

QC-LDPC 码是一种特殊结构化的 LDPC 码, 其校验矩阵具有分块循环特性, 每个循环子矩阵的行重或列重可以大于 1, 也可以等于 1。QC-LDPC 码对应的奇偶校验矩阵的一般形式为:

$$H_{QC} = \begin{bmatrix} A_{s_{11}} & A_{s_{12}} & \cdots & A_{s_{1n}} \\ A_{s_{21}} & A_{s_{22}} & \cdots & A_{s_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ A_{s_{m1}} & A_{s_{m2}} & \cdots & A_{s_{mn}} \end{bmatrix}$$

其中: $A_{s_{ij}}$ ($1 \leq i \leq m, 1 \leq j \leq n, 0 \leq s_{ij} \leq L$) 是大小为 $L \times L$ 的循环矩阵, s_{ij} 为右移因子, 表示对循环矩阵 $A_{s_{ij}}$ 右移 s_{ij} 个单位。当 s_{ij} 为零时, 表示 $A_{s_{ij}}$ 为零矩阵。之所以叫准循环, 是因为它不是真正的循环, 仅仅是局部的分块循环。鉴于 QC-LDPC 码具有分块循环的特性, 可以利用移位寄存器对它实现线性编码。由于只需要存储校验矩阵中每一个非零循环子矩阵的位置和循环移位位数, 所以可以明显地减少存储空间, 大大降低公钥存储量。

2 基于 QC-LDPC 码的公钥密码方案

2.1 方案构造

设二元 (n, k) 线性码 C 是 $GF(2)$ 上的 QC-LDPC 码, 生成矩阵 G 的阶数为 $k \times n$, 校验矩阵 H 的阶数为 $(n - k) \times n$, 纠错能力为 t 。随机选取 $k \times k$ 阶非奇异矩阵 S 和 $n \times n$ 阶可逆变换矩阵 Q , 且 Q 为对角矩阵, Q 的行重和列重都为 $m > 1$ 。这里设 $n = Ln_0, k = L(n_0 - 1)$, 则校验矩阵转换为如下格式: $H = [H_0 | H_1 | \cdots | H_{n_0-1}]$, 其中 H_i 是 $L \times L$ 阶的稀疏循环矩阵, 循环因子为 n_0 。校验矩阵 H 的每一列码重为 $d_c \ll n$, 且 H_{n_0-1} 是满秩矩阵, 那么校验矩阵可化为:

$$H = [H_{n_0-1}^{-1} \cdot H_0 | H_{n_0-1}^{-1} \cdot H_1 | \cdots | H_{n_0-1}^{-1} \cdot H_{n_0-2} | I_{n-k}] \quad (1)$$

那么生成矩阵为:

$$G = \begin{bmatrix} I & \begin{bmatrix} (H_{n_0-1}^{-1} \cdot H_0)^T \\ (H_{n_0-1}^{-1} \cdot H_1)^T \\ \vdots \\ (H_{n_0-1}^{-1} \cdot H_{n_0-2})^T \end{bmatrix} \end{bmatrix}$$

其中: I_{n-k} 是 $(n - k) \times (n - k)$ 阶的单位矩阵, I 是 $k \times k$ 阶的单位矩阵。

2.2 加密

公钥:

$$H' = S^{-1} \cdot H \cdot Q^{-1} \quad (2)$$

私钥: S, H, Q ;

由于 LDPC 码的矩阵是稀疏矩阵, 可以通过密度降低攻击 (density reduction attack) 来获得 LDPC 码的密钥。所以在这里与之前的 McEliece 公钥体制不同, 我们用可逆变换矩阵

Q 代替置换矩阵 P , 不是简单地将原校验矩阵进行坐标的变换, 而是将矩阵 H 映射为一个新的矩阵, 加强了码字的结构, 通过改 m 的值, 可以提高该体制的安全性。

密文 $c = y \cdot H'$, 其中 S^{-1}, Q^{-1} 分别是 S 和 Q 的逆矩阵, c 是密文, y 是 $GF(2)$ 上的 n 比特的明文, 码重为 $t' (t' \geq t'm)$ 。 c 与 y 的关系实质上就是伴随式与错误图样的关系, 因为码 C 能纠正 t 个错误, 因此 c 与 y 之间必然存在一一对应关系, 从而保证了解密的唯一性。

2.3 解密

当接收者收到密文 c 后, 可通过如下步骤计算得到明文 M :

将密文右乘 Q , 有 $c \cdot Q = y \cdot S^{-1} \cdot H \cdot Q^{-1} \cdot Q$, 得到 $c \cdot Q = y \cdot S^{-1} \cdot H$, 由于 $t \geq t'm$, 即在可纠正错误范围之内, 然后通过 QC-LDPC 码译码算法得到 $y \cdot S^{-1}$, 右乘 S , 则恢复出明文 y 。

3 安全性分析

对基于 LDPC 码的公钥密码系统的攻击, 是针对 LDPC 码本身的特点来进行攻击的, 常见的有以下几种攻击。

首先, c 与 y 的关系实质上就是伴随式与错误图样的关系, 根据密文 c 和公钥 H' , 直接解方程 $c = y \cdot H'$, 可是由纠错码理论可知, 它是一个 NP 完全问题, 故该攻击不可行。

其次是通过寻找码字对该体制直接攻击。由于构造新的公钥密码体制的纠错码是由 H' 生成的, 它包含了低码重码字, 攻击者可以通过概率算法获取明文。目前最著名的寻找低码重码字的概率算法就是 Stern 算法^[10], 文献^[11] 给出了 (n, k) LDPC 码的 Stern 算法。我们可知, 经过一次迭代, 寻找码重为 $\omega (\leq n_0 d_v m)$, 个数为 A_ω 的码字的概率是:

$$P_{\omega, A_\omega} = A_\omega \cdot \frac{\binom{\omega}{g} \binom{n-\omega}{\frac{k}{2}-g}}{\binom{n}{\frac{k}{2}}} \cdot \frac{\binom{\omega-g}{g} \binom{n-\frac{k}{2}-\omega+g}{\frac{k}{2}-g}}{\binom{n}{\frac{k}{2}}} \cdot \frac{\binom{n-k-\omega+2g}{l}}{\binom{n-k}{l}}$$

其中: A_ω 是可用码字中码重为 ω 的个数, g 和 l 是使性能最优的两个参数, 具体的选择方法见参考文献^[11]。所以寻找一个低码重码字需要的迭代次数为 $P_{\omega, A_\omega}^{-1}$, 而每次迭代需要的工作量约为: $N \approx \frac{(n-k)^3}{2} + k(n-k)^2 + 2gl \left(\frac{k}{2} \right) +$

$\frac{2g(n-k) \left(\frac{k}{2} \right)^2}{2^l}$, 则寻找一个低码重码字的总的工作量是 $W = P_{\omega, A_\omega}^{-1} \cdot N$ 。当 $n = 4096, k = 2048, t = 82, g = 3, l = 36$ 时, 总的工作量为 $2^{98.39}$ 。可以看出, 该体制是安全的, 可以抵抗 Stern 攻击。

第三种攻击方法就是通过矩阵的稀疏结构对体制进行攻击。我们设矩阵 S 和 Q 对应的生成多项式分别是 $s_{ij}(x)$ 和

$q_{ij}(x)$, 且 Q 又是对角形式, 则 $q_{ij}(x) = 0 (i \neq j)$, Q 可表示为

$$Q = \begin{bmatrix} Q_0 & 0 & \cdots & 0 \\ 0 & Q_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q_{n_0-1} \end{bmatrix}$$

由式(1)和式(2), 我们选择 H' 的最后 $n-k$ 列就可以得到

$$H'_{n-k} = S^{-1} \cdot \begin{bmatrix} Q_0^{-1} & 0 & \cdots & 0 \\ 0 & Q_1^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q_{n_0-1}^{-1} \end{bmatrix}$$

可以看出 $(H'_{n-k})^{-1}$ 仍是循环因子为 L 的稀疏矩阵, 可以表示为: $h_{ij}(x) = q_{ij}(x) \cdot s_{ij}(x) \bmod (x^L - 1)$, 由于 S 和 Q 的列重都为 m , 所以 $h_{ij}(x)$ 的最高次最多为 m^2 , 攻击者遍历所有可能的 $h_{ij}(x)$ 多项式的子集, 求出明文。设 $q_{ij}(x) = x^{e_i} + x^{e_2} + \cdots + x^{e_m}$, $s_{ij}(x) = x^{d_1} + x^{d_2} + \cdots + x^{d_m}$, 其中 $0 \leq e_i \leq L-1, 0 \leq d_i \leq L-1 (1 \leq i \leq m)$ 。首先固定 $q_{ij}(x)$ 中一项不变, 然后依次独立均匀地将 $s_{ij}(x)$ 中所有的子集都遍历一次, 当 $g_{ij}(x)$ 的重量为 m^2 时, 恢复明文。若没有恢复明文, 继续固定 $q_{ij}(x)$ 的另一项不变, 再依将中所有的子集都遍历一次, 重复下去, 最后恢复明文。如果选取的非奇异矩阵 S 为稠密矩阵, 则该攻击的工作量十分庞大, 相当于暴力攻击, 攻击者很难获取到明文信息。

4 其他性能分析

使用其他纠错码构造的 N 体制由于存储密钥需要的存储量大, 在实际中很少得到应用。但是采用 QC-LDPC 码后, 由于循环矩阵的特性, 可以通过使用矩阵的一行或者一列来描述一个矩阵, 这就大大减少了密钥的存储空间。此外由于 QC-LDPC 码本身结构的特点, 使得码字的信息位可以很大; 并且误码率低, 纠错能力强, 大大减少重发的可能, 提高了传信率, 表 1 是不同的公钥密码体制的性能比较。

表 1 各公钥密码体制的性能比较

公钥密码体制	公钥大小/b	传信率
McEliece 体制(1 024, 524)	67 072	0.51
Niederreiter 体制(1 024, 524)	32 750	0.57
QC-LDPC 码 Niederreiter 体制 (16 384, 12 288)	6 144	0.75

可以看出, 即使选择 QC-LDPC 码的维数很大, 公钥大小仍然很小, 同时传信率相对也较高。

5 结语

可以看出, 使用 QC-LDPC 码构造公钥密码系统, 可以克服基于 Goppa 构造的公钥密码系统的密钥存储量大、传信率低等弱点。但是, 我们要注意到, 由于 QC-LDPC 码的稀疏矩阵的特征, 攻击者也许可以通过新的攻击方法来攻击该体制获得密钥。所以随着对 QC-LDPC 码研究的深入, 安全性分析需要进一步加强。

参考文献:

- [1] BERLEKAMP E R, McELIECE R J, van TILBORG H C A. On the inherent intractability of certain coding problems[J]. IEEE Transactions on Information Theory, 1978, 24(3): 384-386.

(下转第 1923 页)

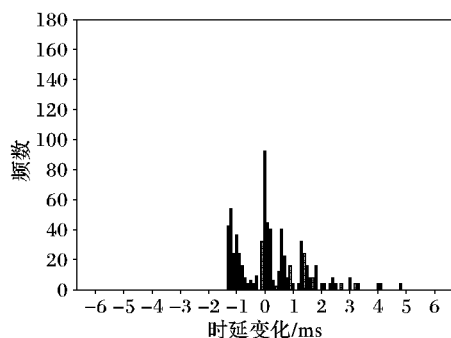
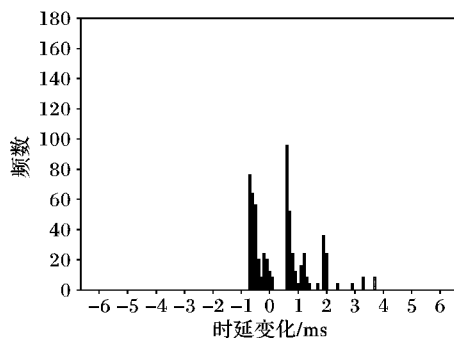
图8 时延变化分布图($R=5$ Mbps)

图9为包链发送速率为7 Mbps的时延变化分布图。与2.4节分析的多背景流量时包链排队行为特征基本一致。包链发送速率为7 Mbps时,已超过瓶颈链路可用带宽。此时包链与背景流量需竞争使用瓶颈链路,背景流量将使得包链多处排队。故图9中,频数出现若干时延变化不为0 ms的峰点。这些峰点对应时延变化值之差与背景流量包大小有关。

图9 时延变化分布图($R=7$ Mbps)

4 结语

包链测量是网络带宽指标测量的主要方法之一。对于背景流量与探测包相互作用下包链的排队行为特征,目前研究不多。本文基于单跳路由器的排队模型,分析得出了背景流量影响下,四种典型的包链排队行为特征,且仿真结果与分析基本一致。实际网络的包链排队行为可以是四种典型情况的混合。本文工作为设计合理的带宽指标测量方法,提高测量的准确性、降低开销提供参考。

本文主要考虑了单跳排队的情况,下一步将扩展到多跳

排队的情况。此外,根据本文结果,对现有带宽指标测量方法进行改进也是未来工作的方向。

参考文献:

- [1] RAVI P, CONSTANTINOS D, MARGARET M, *et al.* Bandwidth estimation: Metrics, measurement techniques, and tools [J]. IEEE Network, 2003, 17(6): 27–35.
- [2] COSTANTINOS D, PARAMESWARAN R, DAVID M. Packet dispersion techniques and a capacity estimation methodology [J]. IEEE/ACM Transactions on Networking, 2004, 12(6): 963–977.
- [3] LIU JUN, ZHANG DAFANG. Toward accurate and efficient available bandwidth measurement[J]. Telecommunication Systems, 2009, 41(3): 211–227.
- [4] HU NINGNING, STEENKISTE P. Evaluation and characterization of available bandwidth probing techniques[J]. IEEE Journal on Selected Areas in Communications, 2003, 21(6): 879–894.
- [5] LIU XILIAN, RAVINDRAN K, LOGUINOV D. A queueing-theoretic foundation of available bandwidth estimation: single-hop analysis[J]. IEEE/ACM Transactions on Networking, 2007, 15(4): 918–931.
- [6] LIU X, RAVINDRAN K, LOGUINOV D. What signals do packet-pair dispersions carry [C]// Proceedings of IEEE INFOCOM. New York: IEEE, 2005: 281–292.
- [7] HÁGA P, DIRICZI K, VATTAY G, *et al.* Understanding packet pair separation beyond the fluid model: The key role of traffic granularity[C]// Proceedings of the 25th IEEE International Conference on Computer Communications. Washington, DC: IEEE Computer Society, 2006: 1–13.
- [8] PARK K-J, LIM H, CHOI C-H. Stochastic analysis of packet-pair probing for network bandwidth estimation[J]. Computer Networks, 2006, 50(12): 1901–1915.
- [9] PASZTOR A, VEITCH D. The packet size dependence of packet pair like methods [C]// Proceedings of IEEE/IFIP International Workshop on Quality of Service. New York: IEEE, 2002: 204–213.
- [10] LEE S, WON Y, SHIN D, *et al.* On the multi-scale behavior of packet size distribution in Internet backbone network[C]// Proceedings of IEEE Network Operations and Management Symposium. New York: IEEE, 2008: 799–802.
- [11] TAQQU M S, WILLINGER W, SHERMAN R. Proof of a fundamental result in self-similar traffic modeling[J]. ACM/SIGCOMM Computer Communications Review, 1997, 27(2): 5–23.

(上接第1908页)

- [2] McELIECE R J. A public-key cryptosystem based on algebraic coding theory [EB/OL]. [2010-10-20]. <http://www.cs.colorado.edu/~jrblack/class/csci7000/f03/.../mceliece.pdf>.
- [3] NIEDERREITER H. Knapsack-type crypto-systems and algebraic coding theory[J]. Problems of Control and Information Theory, 1986, 15(2): 159–166.
- [4] GALLAGER R G. Low-density parity-check codes [J]. IRE Transactions on Information Theory, 1962, 8(1): 21–28.
- [5] MONICO C, ROSENTHAL J, SHOKROLLAHI A. Using low density parity check codes in the McEliece cryptosystem [C]// IEEE International Symposium on Information Theory. New York: IEEE, 2000: 215.
- [6] RICHARDSON T J, URBANKE R L. The capacity of low-density parity-check codes under message-passing decoding[EB/OL]. [2010-09-25]. <http://www.ldpc-codes.com/papers/capacity.pdf>.
- [7] BALDI M, CHIARALUCE F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes [C]// IEEE International Symposium on Information Theory. New York: IEEE, 2007: 2591–2595.
- [8] LI YUANXING, DEN R H, WANG XINMEI. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems[J]. IEEE Transactions on Information Theory, 1994, 40(1): 271–273.
- [9] TANNER R M. A recursive approach to low complexity codes[J]. IEEE Transactions on Information Theory, 1981, 27(5): 533–547.
- [10] STERN J. A method for finding codewords of small weight[C]// Proceedings of the 3rd International Colloquium on Coding Theory and Applications. London: Springer-Verlag, 1989: 106–113.
- [11] HIROTOMO M, MOHRI M, MORII M. A probabilistic computation method for the weight distribution of low-density parity-check codes[C]// IEEE International Symposium on Information Theory. New York: IEEE, 2005: 2166–2170.