ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 36,No. 6,Nov. 2021,pp. 1125－1136
DOI:10. 16337/j. 1004-9037. 2021. 06. 006

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

面向物理层信息安全的QC-LDPC跳码设计

李　广，朱宏鹏，李　聪，葛瑞星，李广侠

（陆军工程大学通信工程学院，南京 210007）

摘　要：低密度奇偶校验（Low density parity check，LDPC）跳码可以在物理层基于跳变的校验矩阵进行差错控制编译码。准循环低密度奇偶校验码（Quasi-cyclic low density parity check code，QC-LDPC）因其良好的纠错性能和易于工程实现的优点而得到广泛应用。本文提出了一种简单且易于工程实现的QC-LDPC跳码设计方法。首先采用有限域的两类子群设计跳变的基矩阵，再通过基模图码的外信息转移算法对基矩阵散列的校验矩阵进行掩模，使跳变矩阵具有统一架构和快速编码结构。仿真和分析表明，设计的QC-LDPC跳码具有超大的跳变码集和良好的纠错性能，码集中LDPC码数目可达10^{34}个，随着码长增加，码集中的LDPC码数目呈指数倍增加，其平均性能可与诸多协议中的LDPC码相当，可用于提升通信系统的可靠性和安全性。

关键词：物理层信息安全；准循环低密度奇偶校验；跳码；有限域；基模图码的外信息转移算法

中图分类号：TN92　　**文献标志码：**A

QC-LDPC Code Hopping Design for Physical Layer Information Security

LI Guang，ZHU Hongpeng，LI Cong，GE Ruixing，LI Guangxia

（School of Communication Engineering，Army Engineering University of PLA，Nanjing 210007，China）

Abstract：Low density parity check（LDPC）code hopping can improve the security and reliability of information transmission through error control coding based on the hopping check matrix at the physical layer. Quasi-cyclic low density parity check code（QC-LDPC）is widely used because of its good error correction performance and easy engineering implementation. This paper proposes a QC-LDPC code hopping design method. Firstly two kinds of subgroups in finite field are used to design the hop-basis matrix，and then the check matrix of the hashed basis matrix is masked by the protograph-based external information transfer（PEXIT），so that the hop matrix has a unified architecture and a fast coding structure，which is easy to implement in engineering. Simulation and analysis show that the designed QC-LDPC codehopping has a huge code hopping set and good error-correcting performance. The number of LDPC codes in a code hopping set can be up to 10^{34}. With the increase of code length，the number of LDPC codes in a code hopping set increases exponentially，and the average performance of LDPC codes is comparable to that of many protocols. It can be used to improve the reliability and security of the communication system.

Key words: physical layer information security; quasi-cyclic low density parity check (QC-LDPC); code hopping; finite field; protograph-based external information transfer (PEXIT) algorithm

---

基金项目：国家自然科学基金（61971440）资助项目。
收稿日期：2021-05-12；**修订日期：**2021-10-19

引　言

随着无线通信网络的快速发展，其隐私和安全变得越来越重要。传统观念下的通信安全性被视为物理层之上的独立特性。如图1所示，目前广泛使用的加密协议（如RSA和AES）都是在物理层已经建立并提供无错误连接的假设下设计和实现的。随着通信破译端计算力的大幅度提升，传统加密面临着巨大的挑战和威胁。例如：2019年法国国家计算机科学与应用数学研究所在高速计算机上利用大数分解算法成功破译迄今最长的RSA密钥。

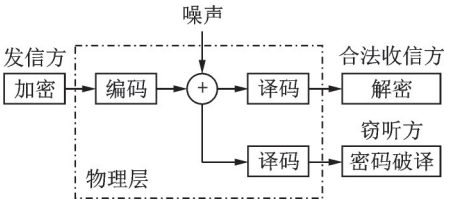


图1　传统加密编码图

Fig.1　Code diagram for traditional encryption

近年来，物理层安全技术在学术领域引起了广泛关注[1-2]，它是一种通过物理层上信号处理技术来提高通信安全的有效方法。物理层安全的基本原理[3]表明：当合法通信的信噪比优于窃听信道时，绝对安全是可行的，可达的安全通信速率上界称为保密容量。例如合法通信方在其信噪比（Signal to noise ratio, SNR）下可收到的信息量为I_B，窃听方在其SNR下可收到的信息量为I_E，此时保密容量$C_S=\max(I_B-I_E)$。但是这种安全的稳定性很差，保密容量随着信道质量而频繁变化，某些情况下甚至为0，仅依据保密容量限定进行系统设计存在局限性。因此，本文提出一种不受制于信道质量的物理层加密的方式，以解决窃听方的接收信噪比高于译码门限时的安全通信问题。

如图2所示，本文将加密方案与信道编码技术相融合，基于差错控制编码的随机跳变来增加窃听方侦收和破译的难度，提高安全等级。文献[4-5]证明了与加密融合的信道编码可保障传输信息的可靠性与安全性。文献[6]将线性分组码与加密结合，提升合法通信的可靠性与安全性。文献[7-8]证明了广义窃听信道下编码加密的可行性。文献[9]则论证了基于低密度奇偶校验（Low desity parity check, LDPC）码加密的可行性，根据校验矩阵是否私有分为两类。当校验矩阵公有时，要求合法信道质量要优于窃听信道；当校验矩阵私有时，在不影响可靠性的情况下也可保障安全性。但LDPC码是线性分组码，信息比特与编码比特的映射关系是固定的，当采用选择明文攻击时，LDPC码的校验矩阵可被恢复[10]。

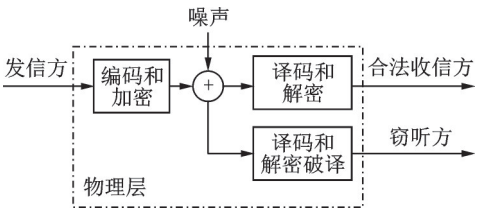


图2　物理层联合编码加密

Fig.2　Physical layer code encryption

本文参考文献[10]提出的跳码加密思想，采用私有跳变LDPC校验矩阵对明文进行编码加密，每帧明文采用不同的LDPC校验矩阵编码，在不牺牲纠错性能的情况下提高系统的安全性。合法通信的双方通过某种方式同步校验矩阵，如事先约定、伪随机数发生器或者十分可靠的信令信道等。与文献[10]所提出的架构不同，本文采用基于有限域两类子群混合构造准循环低密度奇偶校验码（Quasi-cyclic low density parity check code, QC-LDPC）的校验矩阵，并通过基模图码的外信息转移（Protograph-based external information transfer, PEXIT）算法对校验矩阵进行掩模，使校验矩阵编码快、密度更低、译码性能更好，更易于工程实现。

1　面向物理层信息安全的LDPC跳码设计

1.1　LDPC跳码设计目标

信息安全是指窃听方无法还原非法获取的信号中的真实信息。本文拟采用文献[11]提出的误比特率度量信息安全。当窃听方误比特率接近0.5时，认为窃听方无法窃听，可进行安全通信。由于无线

信道的开放特性,窃听信道的信道质量无法获知,因此本文拟设计一种物理层加密的信道编码方案。该方案不受制于窃听信道的信道质量,且当窃听方的信道质量比合法通信信道质量差时,该方案还可以利用噪声的随机性和信道编码的增益来构建保密容量以达到信息论上的安全。图3所示为合法信道质量优于窃听信道场景下系统SNR的关系。图中$\mathrm{SNR}_{\mathrm{E,max}}$为窃听信道可获取的最大SNR,对应接收信号的最小误比特率$P^{\mathrm{E}}_{\mathrm{e,min}}$(接近0.5);$\mathrm{SNR}_{\mathrm{B,min}}$为合法信道可靠通信阈值,对应接收信号的最大误比特率$P^{\mathrm{B}}_{\mathrm{e,max}}$(符合通信要求,接近0)。安全间隔为$\mathrm{SNR}_{\mathrm{B,min}}$与$\mathrm{SNR}_{\mathrm{E,max}}$的SNR差值。在该场景下,当合法通信方采用私有LDPC码,可以有效缩小安全间隔,从而降低可靠通信所需的$\mathrm{SNR}_{\mathrm{B,min}}$。因此,本文拟构造一种不受制于信道质量的加密通信的信道编码方案,该方案的加密能力在与窃听信道质量呈负相关性,并能在窃听信道质量劣于合法信道质量时实现信息论上的安全。

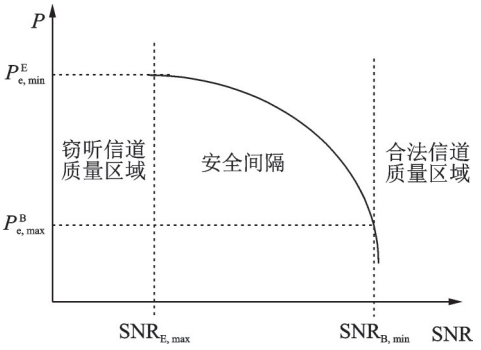


图3　通信质量图

Fig.3　Communication quality chart

文献[10]所提出的跳码架构虽然具有统一的译码架构,易于工程上译码器的实现,但是不具有统一的编码架构,编码复杂度较高,不利于工程实现。本文拟利用PEXIT算法和有限域QC-LDPC码来设计具有快速编码架构且密度更低、性能更好的加密跳码,更易于工程实现和整个系统吞吐量的提升。面向物理层信息安全的QC-LDPC跳码设计目标是具有统一编译码架构、译码性能良好的QC-LDPC跳码。

1.2　基于基模图和有限域的QC-LDPC跳码

LDPC码是Gallager于1962年发明,1999年MacKay首次利用计算机仿真出接近香农极限的二进制对称信道(Binary symmetric channel, BSC)和二元输入加性高斯白噪声(Binary input additive white Gaussian noise, BI-AWGN)信道容量的LDPC码。但当时的码字都缺乏足够的结构性,这给编码和译码的硬件设计带来了极大的不便。一种降低复杂度的方法是在LDPC码校验矩阵中引入一些额外的有助于编译码的结构。基模图码[12]是目前最流行的结构化码字,它是一种易于设计、实现和分析的LDPC码,其构造技术是基于小矩阵(基矩阵)生成大矩阵(校验矩阵)。

1.2.1　基模图LDPC码构造原理

基模图是小矩阵的Tanner图,通过对该图的复制和对图中独立边置换得到较大的图。首先将基模图复制Q次,然后在Q个独立的副本间置换边得到单个大图。如果置换矩阵为循环置换矩阵(Cyclic permutation matrix, CPM),最终得到的大图所对应的阵列为由循环阵构成的阵列,生成的码字为准循环码。本文中的CPM是以$q-1$维的单位阵为基础,循环右移c位,c为循环移位因子($0\leqslant c<q-1$)。

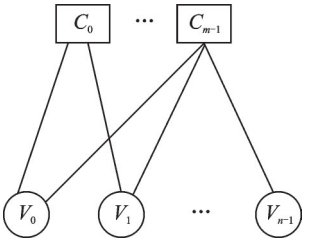


图4　基模图示例

Fig.4　Example protograph

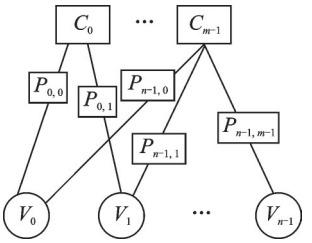


图5　基模图扩展后得到的Tanner图示例

Fig.5　Extend Tanner graph

图4给出了基模图的例子。图4中$C_0,\cdots,C_{m-1}$代表m个校验节点;$V_0,\cdots,V_{n-1}$代表n个变量节点。图5给出了扩展之后的Tanner图,该图通过将每个基模图节点用1簇Q个节点代替,将每条基模图的边用

1簇Q条边代替，每簇节点间采用$Q\times Q$的置换矩阵$\boldsymbol{P}_{i,j}$置换。扩展之后的校验矩阵维度就变成了$(m\times Q)\times(n\times Q)$。基模图中可以存在平行边，但是扩展的图中不应存在平行边。本文为了简化译码器实现的复杂度，所设计的基模图中不存在平行边。

码字的性能不仅与基矩阵的连接关系有关，还与基矩阵的CPM有关。基于有限域设计的基矩阵，不仅设计简单，而且散列得到校验矩阵具有良好的译码性能。

1.2.2 有限域LDPC码

有限域$GF(q)$中含有q个元素，q为素数幂。设α为$GF(q)$的本原元(Primitive element)，$GF(q)$中的q个元素为$\alpha^{-\infty}=0,\alpha^{0}=1,\alpha^{1},\alpha^{2},\cdots,\alpha^{q-2}$。令基矩阵$\boldsymbol{B}=[b_{i,j}](0\leqslant i<m,0\leqslant j<n)$为$GF(q)$上的$m\times n$矩阵。设$b_{i,j}=\alpha^{c_{i,j}}$，当$b_{i,j}\neq 0$时，将$b_{i,j}$替换成维度为$q-1$，移位值为$c_{i,j}$的二元CPM；当$b_{i,j}=0$时，将$b_{i,j}$替换为维度为$q-1$的零矩阵，由此可得基矩阵$\boldsymbol{B}$的二元CPM的散列矩阵$\boldsymbol{H}$，维度为$m(q-1)\times n(q-1)$，其零空间定义了一个码长为$n(q-1)$的二元QC-LDPC码$C_{qc}$[13]。

1.2.3 跳码设计

跳码设计流程如图6所示。收发双方通过某种方式(如可靠的信令信道、伪随机序列或事先约定)同步生成因子，根据生成因子得到基矩阵中CPM的循环因子，再根据PEXIT算法对基矩阵进行掩模确定基矩阵的连接关系，最后由基矩阵散列成校验矩阵。待编码的明文使用校验矩阵直接进行编码，得到的密文为非系统码LDPC。

图6 跳码设计流程图

Fig.6 Flow chart of code hopping design

跳码通过生成因子来同步校验矩阵$\boldsymbol{H}$，为了简化工程实现的复杂度，基矩阵生成器和掩模矩阵为固定架构。简而言之，基矩阵中CPM依据生成因子而跳变，但是基矩阵的连接关系不变。

2 QC-LDPC跳码构造算法和快速编码方法

2.1 基于有限域两类子群的QC-LDPC跳码构造算法

采用迭代译码的LDPC码性能和校验矩阵$\boldsymbol{H}$的围长、陷阱集、停止集以及环外信息量等性质有关。校验矩阵所对应的Tanner图中环长为$2d$的定义是：在d个变量节点和d个校验节点所组成的集合中，存在1条经过每个节点且只经过1次的闭合路径。Tanner图围长是指图中的最小环长。根据外部信息传递的Turbo原理可知，当环长小于当前迭代次数的1/2时，外信息的可靠度会下降。围长为6或8可以保证码字有较好的性能，增加围长可扩大停止集，提升码字的最小距离以降低错误平层[14]。由基矩阵散列所构造的QC-LDPC码，其环长与基矩阵的选择有关。下面2个定理给出围长为6或8的QC-LDPC码基矩阵的充要条件[13]。

定理1 Tanner图围长为6及以上原理：基矩阵$\boldsymbol{B}$中每个2×2的子矩阵中包含至少1个0项或为非奇异矩阵。

定理2 Tanner图围长为8及以上原理：基矩阵$\boldsymbol{B}$中每个2×2和3×3的矩阵中不存在相同非0的

行列式展开项。

为方便表述,下文称定理1为2×2 SM(Submatrices)约束,定理2为3×3 SM约束。

有限域的加法群和乘法群可以用来构造满足行列(Row column, RC)约束(不含4环)的CPM阵列,进而可以用以构造QC-LDPC校验矩阵。令α为$GF(q)$的一个本原元,设

$$\boldsymbol{S}_1=\left\{\alpha^{i_0},\alpha^{i_1},\alpha^{i_2},\cdots,\alpha^{i_{m-1}}\right\},\boldsymbol{S}_2=\left\{\alpha^{j_0},\alpha^{j_1},\alpha^{j_2},\cdots,\alpha^{j_{n-1}}\right\}\quad 1\leqslant m,n<q$$
$$i_k,j_l\in\left\{0,1,2,\cdots,q-2\right\}\quad 0\leqslant k<m,0\leqslant l<n \tag{1}$$

η为$GF(q)$中非0元素,$m\times n$矩阵为

$$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)=[\eta\alpha^{i_k}+\alpha^{j_l}]\quad 0\leqslant k<m,0\leqslant l<n \tag{2}$$

从式(1)可知:(1)$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$为有限域$GF(q)$上的矩阵;(2)矩阵的$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$的每1行或每1列不存在相同的元素;(3)任意两行或两列在任何位置都不存在相同的元素,因此满足2×2 SM约束,由$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$所散列的校验矩阵$\boldsymbol{H}$围长最小为6。通过枚举不满足3×3 SM约束项可找出所有6环。

将$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$作为基矩阵,$\boldsymbol{H}$为其二元CPM散列矩阵,CPM的维度为$q-1$。因此$\boldsymbol{H}$的维度为$m(q-1)\times n(q-1)$,其零空间代表长度为$n(q-1)$,围长至少为6的QC-LDPC码$C_{qc}$。如图6所示,本文根据生成因子快速生成式(1)中的$\boldsymbol{S}_1$和$\boldsymbol{S}_2$,乘法因子η为有限域某一固定值,根据式(2),可得基矩阵$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$,散列成校验矩阵$\boldsymbol{H}$。通过切换生成因子可得到不同的校验矩阵,根据这种方式可得校验矩阵总数目为$C_{q-1}^{m}\times C_{q-1}^{n}$。当窃听方可做到无噪窃听或者其信道质量较高时,系统码很容易暴露明文,因此本文采用非系统码提高通信的安全性,通过对低码率信息位打孔来获取目标码率。例如目标码率为1/2,通过设计1/3码率的系统码,然后将信息位全部打孔,只保留校验位来获得1/2码率的LDPC码。

2.2　PEXIT掩模算法

影响QC-LDPC码性能的因素除了2.1节中的环长外,还有变量节点和校验节点的度分布、矩阵的连通性以及校验矩阵的行冗余等。2.1节基于有限域两类子群所设计的QC-LDPC码虽然不含4环,但含有大量的6环和8环,几乎未考虑矩阵的连接性和度分布,当合法信道的SNR较低时,译码成功所需的迭代次数增加,外信息真实可靠度下降,因此码字瀑布区性能较差,即图3中的安全间隔将会变大。而且这种码字没有快速编码结构,只能通过高斯消元算法或者文献[15]中的QC-LDPC通用编码算法得到生成矩阵后再进行编码,这两种在线编码的时间复杂度都是$O(n^2)$,这种复杂度很不利于工程实现。因此本节优化了矩阵的连接性和度分布,并融入了快速编码结构,研究基于PEXIT算法掩模的有限域QC-LDPC码。

矩阵掩模是指利用与CPM相同大小的零矩阵取代校验矩阵中的某些CPM,使得校验矩阵更加稀疏,掩模操作可以在基矩阵上进行。对校验矩阵$\boldsymbol{H}$的掩模操作可以表示为Hadamard矩阵乘积。设掩模矩阵为$\boldsymbol{Z}=[Z_{i,j}]_{0\leqslant i<m,0\leqslant j<n}$,$\boldsymbol{B}_{\text{mask}}=\boldsymbol{B}\otimes\boldsymbol{Z}=[b_{i,j}\cdot z_{i,j}]_{0\leqslant i<m,0\leqslant j<n}$,$b_{i,j}$为$GF(q)$上的元素,$z_{i,j}$为$GF(2)$上的元素,当$z_{i,j}=1$时,$b_{i,j}\cdot z_{i,j}=b_{i,j}$;当$z_{i,j}=0$时,$b_{i,j}\cdot z_{i,j}=0$,其表明变量节点$i$和校验节点$j$之间不存在边。

基于度分布的不规则外信息转移(External information transfer, EXIT)图[16]凭借其简单性、准确性被广泛用于LDPC码的度分布设计,但是其没有考虑矩阵的连接性。文献[17]在文献[16]基础上提出多维EXIT技术,适用于较小的基模图,可以准确地预测基矩阵的译码门限。此外PEXIT算法还可用于计算具有某些特殊节点类型的基模图码的译码门限,例如度为2的变量节点和打孔的变量节点。首先根据不规则EXIT图设计掩模矩阵的度分布,再采用PEXIT算法计算掩模矩阵的译码门限,选择相

对最优的连接关系作为基模图掩模矩阵。

文献[17]并没有依据度分布计算平均互信息而是充分地考虑了矩阵的连接性。首先令$I_{\mathrm{E,V}}^{j\to i}$为“类型$j$”变量节点关联的码字比特与从这些变量节点发给“类型i”校验节点的对数似然信息(Logarithmic likelihood information, LLR)$L_{j\to i}$之间的外信息。同理,$I_{\mathrm{E,C}}^{i\to j}$是“类型$i$”校验节点发送给“类型$j$”变量节点关联码字比特的LLR$L_{i\to j}$的外信息。文献[17]根据文献[16]中的结论得出,当校验节点j与变量节点i之间有边时,即当$z_{i,j}\neq 0$时,有

$$I_{\mathrm{E,V}}^{j\to i}=J\left(\sqrt{\sum_{c=0}^{m-1}(z_{cj}-\delta_{ci})(J^{-1}(I_{\mathrm{E,C}}^{c\to j}))^2+\sigma_{\mathrm{ch},j}^2}\right) \tag{3}$$

$I_{\mathrm{E,C}}^{i\to j}$作为$I_{\mathrm{E,V}}^{j\to i}$的先验信息,当$c=i$时,$\delta_{ci}=1$,否则$\delta_{ci}=0$。$J$函数为输入输出均为高斯分布的互信息值,自变量为高斯输入的方差。如果码字比特j被删除,则置$\sigma_{\mathrm{ch},j}^2=0$。同理有

$$I_{\mathrm{E,C}}^{i\to j}=1-J\left(\sqrt{\sum_{v=0}^{n-1}(z_{iv}-\delta_{vj})(J^{-1}(1-I_{\mathrm{E,V}}^{v\to i}))^2}\right) \tag{4}$$

$I_{\mathrm{E,V}}^{j\to i}$作为$I_{\mathrm{E,C}}^{i\to j}$的先验信息,当$v=j$时,$\delta_{vj}=1$,否则$\delta_{vj}=0$。根据文献[16],$J$函数可拟合为

$$J(\sigma)\approx\begin{cases}A_{J,1}\sigma^3+B_{J,1}\sigma^2+C_{J,1}\sigma & 0\leqslant\sigma\leqslant 1.636\,3\\ 1-\mathrm{e}^{A_{J,2}\sigma^3+B_{J,2}\sigma^2+C_{J,2}\sigma+D_{J,2}} & 1.636\,3<\sigma<10\\ 1 & \sigma\geqslant 10\end{cases} \tag{5}$$

式(5)中参数A、B、C参照表1。由于$J(\sigma)$为σ的单调函数,所以$J(\sigma)$的反函数$J^{-1}(*)$一定存在,有

$$\sigma=J^{-1}(I)\approx\begin{cases}A_{\sigma,1}I^3+B_{\sigma,1}I^2+C_{\sigma,1}\sqrt{I} & 0\leqslant I\leqslant 0.364\,6\\ -A_{\sigma,2}\ln[B_{\sigma,2}(1-I)]-C_{\sigma,2} & 0.364\,6<I<1\end{cases} \tag{6}$$

式(6)中参数A、B、C参照表2。采用这种近似计算方式与密度进化计算的门限差距在0.05 dB之内。

表1 $J(\sigma)$中参数

Table 1 Parameters in $J(\sigma)$

$A_{J,1}$	$A_{J,2}$	$B_{J,1}$	$B_{J,2}$	$C_{J,1}$	$C_{J,2}$	$D_{J,2}$
−0.042 106 1	0.001 814 91	0.209 252	−0.082 205 4	−0.006 400 8	−0.082 205 4	0.054 960 8

表2 $J^{-1}(I)$中参数

Table 2 Parameters in $J^{-1}(I)$

$A_{\sigma,1}$	$A_{\sigma,2}$	$B_{\sigma,1}$	$B_{\sigma,2}$	$C_{\sigma,1}$	$C_{\sigma,2}$
1.095 42	0.706 692	0.214 217	0.386 013	2.337 27	−1.750 17

算法 PEXIT算法

(1) 初始化:选择E_{b}/N_0,初始化信道LLR值的方差$\sigma_{\mathrm{ch},j}^2=8R(E_{\mathrm{b}}/N_0)|_{v_j}$,当输入$x_j$被打孔时,$\sigma_{\mathrm{ch},j}^2=0$。对$I_{\mathrm{E,V}}^{j\to i}$初始化,$0\leqslant i<m$,$0\leqslant j<n$,有

$$I_{\mathrm{E,V}}^{j\to i}=\begin{cases}\sigma_{\mathrm{ch},j}^2 & b_{i,j}\neq 0\\ 0 & b_{i,j}=0\end{cases} \tag{7}$$

(2) 校验节点到变量节点的PEXIT函数:对于$0\leqslant i<m$,$0\leqslant j<n$,计算式(3)。

(3) 变量节点到校验节点的PEXIT函数:对于$0\leqslant i<m$,$0\leqslant j<n$,计算式(4)。

(4) 累积变量节点的后验信息,$0\leqslant j<n$,有

$$I_{\mathrm{CMI}}^{j}=J\left(\sqrt{\sum_{c=0}^{m-1}z_{cj}\left(J^{-1}\left(I_{\mathrm{E,C}}^{c\to j}\right)\right)^{2}+\sigma_{\mathrm{ch},j}^{2}}\right) \tag{8}$$

(5) 停止规则:对于$0\leqslant j<n$,$I_{\mathrm{CMI}}^{j}=1$或达到精度要求,否则跳到步骤(2);或者达到最高迭代次数,输出在该E_{b}/N_0下,译码无法收敛。

基于PEXIT算法掩模的有限域QC-LDPC码的设计分为两步:

(1)基矩阵设计。仍采用2.1节中的基于有限域两类子群的QC-LDPC的设计方式,因为它所设计的QC-LDPC具有以下特点:(a) 构造的跳码可以很好地避免4环;(b) 自适应码长,因为校验矩阵中的CPM维度是有限域集合的长度,因此可以根据需求适当地调整有限域大小。

(2)掩模矩阵的设计。本文参考了文献[18-19]中快速编码的校验位设计方法,采用双对角的方式来设计校验位(详见2.3节快速编码方法),然后利用EXIT算法设计具有较低译码门限的度分布,并且保证每个信息位的变量节点有充足的外信息,再利用PEXIT算法找出信息位打孔后译码门限较低的掩模矩阵。信息位打孔比例和安全性有关,信息位打孔比例越高,窃听方破译越困难,但随着打孔比例的增加,掩模矩阵设计会变得更加困难,译码的收敛速度也会变慢。

利用PEXIT算法生成的掩模矩阵对2.1节中的校验矩阵进行掩模,可以得到密度更低、性能更好、更有利于编译码设计的跳码校验矩阵。

2.3　快速编码方法

2.3.1　快速编码算法

基于PEXIT掩模的有限域QC-LDPC码具有双对角结构[19],可使用校验矩阵直接编码,避免额外的资源消耗。校验矩阵$\boldsymbol{H}$的结构如式(9),当$\boldsymbol{C}_{i,j}(0\leqslant i<m,0\leqslant j<k)$被掩模时表示$q-1$维零矩阵,否则表示维度为$q-1$、循环移位$c_{i,j}$的CPM。$\boldsymbol{C}_{i,j}(0\leqslant i<m,k\leqslant j<m+k)$表示维度为$q-1$、循环移位$c_{i,j}$的CPM,$-1$代表维度为$q-1$的零矩阵。子矩阵$\boldsymbol{D}_0$表示一个大小为$m(q-1)\times k(q-1)$的矩阵,对应信息比特部分,子矩阵$\boldsymbol{D}_1$表示一个大小为$m(q-1)\times m(q-1)$的双对角循环矩阵,对应校验比特部分。设$\boldsymbol{\mu}=\left\{\boldsymbol{\mu}_0^{\mathrm{T}},\boldsymbol{\mu}_1^{\mathrm{T}},\cdots,\boldsymbol{\mu}_{k-1}^{\mathrm{T}}\right\}^{\mathrm{T}}$为待编码信息,其中$\boldsymbol{\mu}_i(0\leqslant i<k)$为列向量,包含$q-1$个信息比特,$\boldsymbol{c}=\left\{\boldsymbol{c}_0^{\mathrm{T}},\boldsymbol{c}_1^{\mathrm{T}},\cdots,\boldsymbol{c}_{m-1}^{\mathrm{T}}\right\}^{\mathrm{T}}$为码字(不含信息比特),其中$\boldsymbol{c}_i(0\leqslant i<m)$为列向量,包含$q-1$个编码比特。

根据$\boldsymbol{H}$结构,可先求得$\boldsymbol{c}_0$,再通过递推的形式得到$\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_{m-1}$。将$\boldsymbol{H}$中所有块矩阵(按照CPM的维度分块)按列在$GF(2)$上累加,考虑到$\boldsymbol{H}\cdot\begin{bmatrix}\boldsymbol{\mu}\\ \boldsymbol{c}\end{bmatrix}=\boldsymbol{0}$,则有

$$\boldsymbol{H}=[\boldsymbol{D}_0\quad\boldsymbol{D}_1]=\begin{bmatrix}
\boldsymbol{C}_{0,0} & \boldsymbol{C}_{0,1} & \cdots & \boldsymbol{C}_{0,k-1} & \boldsymbol{C}_{0,k} & \boldsymbol{C}_{0,k+1} & -\boldsymbol{1} & \cdots & \cdots & \cdots & \cdots & \cdots & -\boldsymbol{1}\\
\boldsymbol{C}_{1,0} & \boldsymbol{C}_{1,1} & \cdots & \boldsymbol{C}_{1,k-1} & -\boldsymbol{1} & \boldsymbol{C}_{0,k+1} & \boldsymbol{C}_{1,k+2} & -\boldsymbol{1} & \cdots & \cdots & \cdots & \cdots & -\boldsymbol{1}\\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots\\
\boldsymbol{C}_{t,0} & \boldsymbol{C}_{t,1} & \cdots & \boldsymbol{C}_{t,k-1} & \boldsymbol{C}_{t,k} & -\boldsymbol{1} & \cdots & -\boldsymbol{1} & \boldsymbol{C}_{t-1,p} & \boldsymbol{C}_{t,p+1} & -\boldsymbol{1} & \cdots & -\boldsymbol{1}\\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots\\
\boldsymbol{C}_{m-1,0} & \boldsymbol{C}_{m-1,1} & \cdots & \boldsymbol{C}_{m-1,k-1} & \boldsymbol{C}_{0,k} & -\boldsymbol{1} & \cdots & \cdots & \cdots & \cdots & \cdots & -\boldsymbol{1} & \boldsymbol{C}_{m-2,m+k-1}
\end{bmatrix} \tag{9}$$

$$\boldsymbol{C}_{t,k}\cdot\boldsymbol{c}_0^{\mathrm{T}}=\sum_{i=0}^{m-1}\sum_{j=0}^{k-1}\boldsymbol{C}_{i,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}} \tag{10}$$

因为$\boldsymbol{C}_{t,k}$为CPM,所以$\boldsymbol{C}_{t,k}^{-1}=\boldsymbol{C}_{t,k}^{\mathrm{T}}$,推得

$$\boldsymbol{c}_0^{\mathrm{T}}=\boldsymbol{C}_{t,k}^{\mathrm{T}}\cdot\left(\sum_{i=0}^{m-1}\sum_{j=0}^{k-1}\boldsymbol{C}_{i,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}}\right) \tag{11}$$

再利用$\boldsymbol{D}_1$的双对角循环结构推得

$$\boldsymbol{c}_i^{\mathrm{T}}=\boldsymbol{C}_{i-1,k+i+1}^{\mathrm{T}}\cdot\left(\sum_{j=0}^{k-1}\boldsymbol{C}_{i-1,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}}+\sum_{j=k}^{k+i}\boldsymbol{C}_{i-1,j}\cdot\boldsymbol{c}_j^{\mathrm{T}}\right)\quad 0<i<m \tag{12}$$

当$\boldsymbol{C}_{i,j}$不为零矩阵时，根据CPM的性质可知，$\boldsymbol{C}_{i,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}}$（或$\boldsymbol{C}_{i,j}\cdot\boldsymbol{c}_j^{\mathrm{T}}$）为$\boldsymbol{\mu}_j$（或$\boldsymbol{c}_j$）循环右移$c_{i,j}$位。

2.3.2 *编码结构和复杂度分析*

跳码编码结构如图7所示。先进行行信息累加计算每块校验位的缓存值，再通过递推输出部分得到校验位，只需要简单的移位和异或操作便可完成编码。其中行信息累加器模块根据式(10)计算得$\boldsymbol{c}_{\mathrm{sum}}^{\mathrm{tmp}}=\sum_{i=0}^{m-1}\sum_{j=0}^{k-1}\boldsymbol{C}_{i,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}}=\boldsymbol{C}_{t,k}\cdot\boldsymbol{c}_0^{\mathrm{T}}$，$\boldsymbol{c}_i^{\mathrm{tmp}}=\sum_{j=0}^{k-1}\boldsymbol{C}_{i,j}\cdot\boldsymbol{\mu}_j^{\mathrm{T}}(0\leqslant i<m-1)$的值，共需要位宽为$q-1$的移位寄存器$m$块，二输入异或门$m(k-1)(q-1)+m-1$个。递推输出模块根据式(11～12)得$\boldsymbol{c}_0^{\mathrm{T}}=\boldsymbol{C}_{t,k}^{\mathrm{T}}\cdot\boldsymbol{c}_{\mathrm{sum}}^{\mathrm{tmp}}$，即$\boldsymbol{c}_{\mathrm{sum}}^{\mathrm{tmp}}$循环左移$c_{t,k}$位，$\boldsymbol{c}_i^{\mathrm{T}}=\boldsymbol{C}_{i-1,k+i}^{\mathrm{T}}(\boldsymbol{c}_{i-1}^{\mathrm{tmp}}+\boldsymbol{C}_{i-1,k+i-1}\cdot\boldsymbol{c}_{i-1}^{\mathrm{T}})(0<i<m-1,i\neq t+1)$，$\boldsymbol{c}_{t+1}^{\mathrm{T}}=\boldsymbol{C}_{t,k+t+1}^{\mathrm{T}}(\boldsymbol{c}_{\mathrm{sum}}^{\mathrm{tmp}}+\boldsymbol{C}_{t-1,k+t}\cdot\boldsymbol{c}_t^{\mathrm{T}}+\boldsymbol{c}_t^{\mathrm{tmp}})$。整个编码模块共需要位宽为$q-1$的移位寄存器$2m+1$块，二输入异或门$m(k-1)(q-1)+2m-2$块，编码复杂度与基矩阵行数$m$近似呈线性关系。

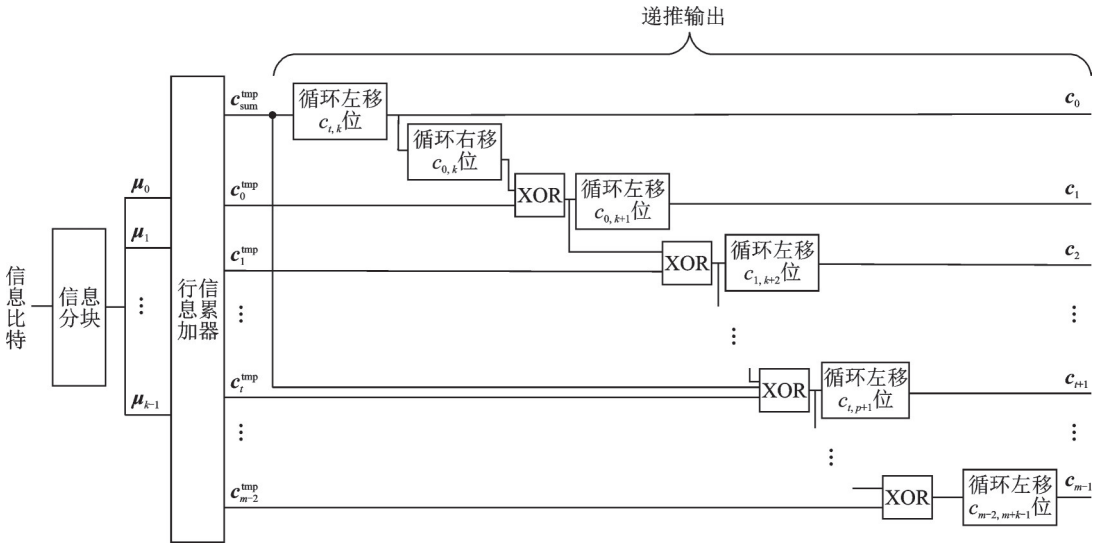


图7 跳码编码架构图

Fig.7 Architecture diagram of code hopping coding

3 解密分析

明文攻击是目前破译LDPC码生成矩阵或校验矩阵的最常用手段，因此本节重点分析明文攻击下跳码的安全性。

基于单校验矩阵编码加密系统[20]本质上是一种线性加密过程，即明文和密文一一对应。只需要找出明文到密文的线性映射空间，即可破译该加密系统。为了评估单一校验矩阵破译的复杂度，设满秩单校验矩阵为$\boldsymbol{H}_s$，其维度为$m_s\times n_s$，$\boldsymbol{G}_s$为生成矩阵，其维度为$k_s\times m_s$，$k_s=n_s-m_s$，$m_s>k_s$。设待编码的信息列向量和编码列向量分别为$\boldsymbol{\mu}$和$\boldsymbol{c}$，维度分别为k_s和m_s，即$\boldsymbol{c}=\boldsymbol{G}_s^{\mathrm{T}}\cdot\boldsymbol{\mu}$。设$k_s$组二元信息矢量分别为$\boldsymbol{\mu}_0=[1,0,\cdots,0]^{\mathrm{T}}$，$\boldsymbol{\mu}_1=[0,1,\cdots,0]^{\mathrm{T}}$，$\cdots$，$\boldsymbol{\mu}_{k_s-1}=[0,0,\cdots,1]^{\mathrm{T}}$信息矢量对应的编码矢量分别为$\boldsymbol{c}_0,\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{k_s-1}$，维度为$m_s$。根据线性分组码的编码原理，可得

$$\boldsymbol{G}_s^{\mathrm{T}}\cdot[\boldsymbol{\mu}_0,\boldsymbol{\mu}_1,\cdots,\boldsymbol{\mu}_{k_s}]=[\boldsymbol{c}_0,\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{k_s}]\Rightarrow\boldsymbol{G}_s^{\mathrm{T}}=[\boldsymbol{c}_0,\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{k_s}] \tag{13}$$

因为$[\boldsymbol{\mu}_0,\boldsymbol{\mu}_1,\cdots,\boldsymbol{\mu}_{k_s}]$为$[\boldsymbol{c}_0,\boldsymbol{c}_1,\cdots,\boldsymbol{c}_{k_s}]$的子空间,且$[\boldsymbol{\mu}_0,\boldsymbol{\mu}_1,\cdots,\boldsymbol{\mu}_{k_s}]$满秩,所以$\boldsymbol{G}_s$矩阵的右逆矩阵一定存在,有

$$\boldsymbol{G}_R=\boldsymbol{G}_s^{\mathrm{T}}(\boldsymbol{G}_s\cdot\boldsymbol{G}_s^{\mathrm{T}})^{-1} \tag{14}$$

则明文$\boldsymbol{\mu}=\boldsymbol{c}^{\mathrm{T}}\boldsymbol{G}_R$,加密破译的复杂度为$O(k_s^2)$,所需要的存储空间为$k_s\times m_s$个比特。因此,在明文攻击下,单矩阵编译码系统很容易被破解。

为了攻击跳码,窃听方需要弄清楚矩阵$\boldsymbol{H}_i$跳变的规律以及码集中的矩阵数目。矩阵的跳变规律主要取决于合法通信双方都已知的伪随机序列,码集中的矩阵数目则取决于有限域和基矩阵的大小。根据上文可知,单矩阵编译码系统可以根据k_i(待编码信息比特数)组$(\boldsymbol{\mu}_i,\boldsymbol{c}_i)$明文-密文对来获取编码矩阵$\boldsymbol{G}_i$。但在本文设计的跳码系统中,每一组待编码的明文信息对应的编码矩阵都不同,尽管窃听方可从一组$(\boldsymbol{\mu}_i,\boldsymbol{c}_i)$中获得$\boldsymbol{G}_i$的某些行的异或值,但无法获得完整的$\boldsymbol{G}_i$。设定明文$\boldsymbol{\mu}_i=[0,\cdots,1,\cdots,0]^{\mathrm{T}}$,根据$\boldsymbol{c}_i=\boldsymbol{G}_i^{\mathrm{T}}\cdot\boldsymbol{\mu}_i$可得$\boldsymbol{G}_i$中的第$i$行为$\boldsymbol{c}_i$,但无法得到$\boldsymbol{G}_i$矩阵的其他行数据。本文所设计的码集规模庞大,随着码长的增加,码集的数目呈阶乘的数量增加。例如:当基矩阵的维度为8×12,采用的有限域为$GF(2^8)$时,此时码集中的校验矩阵数目为$\mathrm{C}_{255}^{8}\times\mathrm{C}_{255}^{12}\approx4.81\times10^{34}$。从码集的角度,当窃听方想要破译该码字,需要将整个码集的生成矩阵$\boldsymbol{G}_i$全部存储下来,就上述例子而言,$\boldsymbol{G}_i$的维度为$(4\times255)\times(12\times255)$,该矩阵一般稠密矩阵。因此单个矩阵需要的存储空间为$(4\times255)\times(12\times255)=2.98$ Mb,而存储整个码集的映射矩阵所需空间约为$2.98\times4.81\times10^{34}=1.432\times10^{35}$ Mb,其所需存储容量趋近于无穷。即使窃听方具备这样的存储能力,也很难破解基于周期无限大的同步混沌序列,因此其破译的复杂度趋近于无穷。

上述分析建立在窃听方无噪的条件下,然而实际中窃听方几乎无法做到无噪窃听,因此本文进一步分析AWGN噪声下所提加密方案的安全性。在噪声信道下,合法通信双方可根据同步的校验矩阵准确地译码解密,而窃听方在不知道校验矩阵的情况下,只能通过硬判决得到密文比特,假设在二进制相移键控(Binary symmetric keying, BPSK)的调制下,误比特率为$p_{\mathrm{e}}=Q(\sqrt{2RE_{\mathrm{b}}/N_0})$,其中$Q(\cdot)$为$Q$函数,$R$为编码码率。受噪声的影响,窃听方很难判断密文的正确性,因此跳码的安全性在噪声信道下得到进一步加强。

4　仿真与分析

设α为$GF(256)$本原元,$\eta=1$,$\boldsymbol{S}_1$和$\boldsymbol{S}_2$是$GF(256)$的两个任意平凡子集,大小分别为m和n,根据式(2)可得$m\times n$的有限域$GF(256)$上的基矩阵$\boldsymbol{B}(\boldsymbol{S}_1,\boldsymbol{S}_2)$,其CPM散列的二元矩阵为$\boldsymbol{H}$,其维度为$255m\times255n$。

为了检验掩模打孔对可靠性的影响,本文对比了相同码长、码率下未掩模、未打孔和掩模打孔后的QC-LDPC跳码性能。设未掩模、未打孔的基矩阵$\boldsymbol{B}_{\mathrm{unmp}}$中$\boldsymbol{S}_1$和$\boldsymbol{S}_2$的大小分别为4和8,即$m=4$,$n=8$。$\boldsymbol{B}_{\mathrm{unmp}}$维度为$4\times8$,其CPM散列矩阵为$\boldsymbol{H}_{\mathrm{unmp}}$,其维度为$1\,020\times2\,040$,零空间是码率为1/2的$(1\,020,2\,040)$码字$\boldsymbol{c}_{\mathrm{unmp}}$,Tanner图中平均6环数目为1 122.73,8环数目为21 321.69,跳码的校验矩阵总数为$\mathrm{C}_{255}^{4}\times\mathrm{C}_{255}^{8}\approx6.93\times10^{22}$。设掩模打孔的基矩阵$\boldsymbol{B}_{\mathrm{mp}}$中$\boldsymbol{S}_1$和$\boldsymbol{S}_2$的大小分别为8和12,即$m=8$,$n=12$。$\boldsymbol{B}_{\mathrm{mp}}$维度为$8\times12$,其CPM散列矩阵为$\boldsymbol{H}_{\mathrm{mp}}$,其维度为$2\,040\times3\,060$,零空间是码率为1/3的$(1\,020,3\,060)$系统码$\boldsymbol{c}_{\mathrm{mask}}$,Tanner图中平均6环数目为73.9,8环数目为731.06。将$\boldsymbol{c}_{\mathrm{mask}}$的信息位全部打孔后得到码率为1/2的$(1\,020,2\,040)$非系统码$\boldsymbol{c}_{\mathrm{mp}}$,跳码的校验矩阵总数约为$\mathrm{C}_{255}^{8}\times\mathrm{C}_{255}^{12}\approx4.81\times10^{34}$。掩模之后,Tanner图中短环数目骤减。

在表3的仿真条件下，码字$\boldsymbol{c}_{\mathrm{mp}}$和$\boldsymbol{c}_{\mathrm{unmp}}$的误比特率(Bit error rate, BER)性能如图8所示。图中横坐标为比特能量比噪声密度E_{b}/N_0；纵坐标Pb为误比特率。当E_{b}/N_0为1～1.4 dB时，此时跳码$\boldsymbol{c}_{\mathrm{mp}}$未达译码门限，误码率曲线随$E_{\mathrm{b}}/N_0$呈现平缓下降，当过$E_{\mathrm{b}}/N_0$超过1.6 dB之后，跳码$\boldsymbol{c}_{\mathrm{mp}}$到达译码门限，误码率随$E_{\mathrm{b}}/N_0$呈现瀑布式下降。当BER为$10^{-6}$时，码字$\boldsymbol{c}_{\mathrm{mp}}$的性能优于$\boldsymbol{c}_{\mathrm{unmp}}$约0.6 dB。图8还包含国际空间数据系统咨询委员会(Consultative Committee for Space Data Systems, CCSDS)标准中的AR4JA码[21]$\boldsymbol{c}_{\mathrm{AR4JA}}$和IEEE 802.16标准中的QC-IRA码[22]$\boldsymbol{c}_{\mathrm{IRA}}$。码字$\boldsymbol{c}_{\mathrm{mp}}$的性能略差于$\boldsymbol{c}_{\mathrm{AR4JA}}$ 0.1 dB，略优于$\boldsymbol{c}_{\mathrm{IRA}}$0.05 dB，这是因为$\boldsymbol{c}_{\mathrm{mp}}$代表的是整个码集的平均性能，其中不乏短环较多、性能较差的码字，但本文的主旨是在不牺牲太多译码性能的前提下尽可能地提高码字的抗破译性。

表3 仿真参数

Table 3 Parameters in simulation

码字类型	码长	码率	译码算法	调制方式	信道
$\boldsymbol{c}_{\mathrm{unmp}}$	2 040	1/2	NMSA	BPSK	AWGN
$\boldsymbol{c}_{\mathrm{mp}}$	2 040	1/2			
$\boldsymbol{c}_{\mathrm{AR4JA}}$	2 048	1/2			
$\boldsymbol{c}_{\mathrm{IRA}}$	2 044	约1/2			

当采用去短环算法从整个码集中筛选出一个围长至少为12的校验矩阵$\boldsymbol{H}_0$，其性能如图9所示，图中$\boldsymbol{c}_0$为$\boldsymbol{H}_0$所对应的LDPC码。分析图中曲线可以发现该码字性能比传统码字性能提高0.2～0.5 dB，比码集的平均性能提高约0.3 dB。

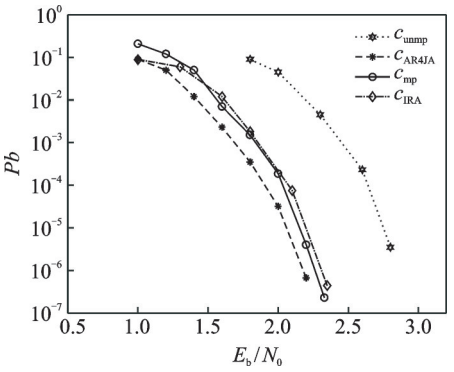


图8 跳码性能曲线图

Fig.8 Code hopping performance

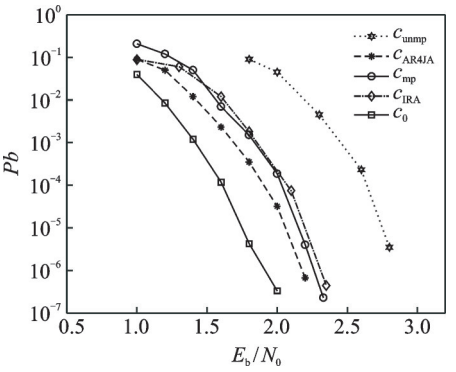


图9 单短阵性能对比图

Fig.9 Comparison diagram of single matrix performance

根据图10可以看出，采用明文攻击的窃听方误比特率与SNR的关系不大，无论是在低信噪比区还是高信噪比区域，其误比特率始终在0.5左右，而从图10或图8中则可以看出，当合法收信方的E_{b}/N_0达到译码门限时(1.5 dB左右)，便可实现可靠通信，随着E_{b}/N_0的值越高，通信的可靠性越好。

因此，对于明文攻击的窃听方式而言，采用该跳码设计在任何信噪比条件下均能保证信息传输的安全性，当$E_{\mathrm{b}}/N_0>1.5$ dB时即可保证可靠通信。

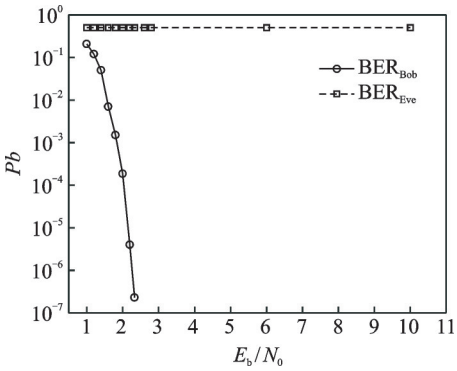


图10 窃听方和合法通信方性能对比图

Fig.10 Performance comparison between eavesdropper and legitimate communicator

5　结束语

本文采用了误比特率来衡量物理层信息安全,使用跳码技术将加密和信道编码结合,采用非系统LDPC码传输信息。该方案的加密特性不受制于信道质量,且加密能力在与窃听信道质量呈负相关性,能在窃听信道质量劣于合法信道质量时实现信息论上的安全。跳码由跳变的校验矩阵生成,跳变矩阵根据同步因子生成器可进行快速切换。跳变矩阵具有统一架构和快速编码的结构,通过对信息比特的简单移位和异或操作便可实现快速编码,易于工程实现。跳变的校验矩阵数目庞大,纠错性能良好,在不牺牲编码增益的前提下可以改善传统通信的安全性。

参考文献:

[1] MUKHERJEE A, FAKOORIAN S A A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550-1573.

[2] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: Technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[3] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[4] CSISZÁR I, KORNER J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[5] WYNER A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[6] WEI V K. Generalized Hamming weights for linear codes[J]. IEEE Transactions on Information Theory, 1991, 37(5): 1412-1418.

[7] HAYASHI M. Exponents of channel resolvability and wire-tapped channel[C]//Proceedings of IEEE Int Symp Information Theory and Its Applications (ISITA). Parma, Italy: [s.n.], 2004: 1080-1085.

[8] HAYASHI M. General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1562-1575.

[9] MURAMATSU J. Secret key agreement from correlated source outputs using low density parity check matrices[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006, 89(7): 2036-2046.

[10] CHEN Z, YIN L, PEI Y, et al. CodeHop: Physical layer error correction and encryption with LDPC-based code hopping[J]. Science China Information Sciences, 2016, 59(10): 1-15.

[11] KLINC D, HA J, MCLAUGHLIN S W, et al. LDPC codes for the Gaussian wiretap channel[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 532-540.

[12] DEHGHAN A, BANIHASHEMI A H. On the Tanner graph cycle distribution of random LDPC, random protograph-based LDPC, and random quasi-cyclic LDPC code ensembles[J]. IEEE Transactions on Information Theory, 2018, 64(6): 4438-4451.

[13] LI J, LIU K, LIN S, et al. Algebraic quasi-cyclic LDPC codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme[J]. IEEE Transactions on Communications, 2014, 62(8): 2626-2637.

[14] TIAN T, JONES C, VILLASENOR J D, et al. Construction of irregular LDPC codes with low error floors[C]//Proceedings of IEEE International Conference on Communications. [S.l.]: IEEE, 2003: 3125-3129.

[15] LI Z, CHEN L, ZENG L, et al. Efficient encoding of quasi-cyclic low-density parity-check codes[J]. IEEE Transactions on Communications, 2006, 54(1): 71-81.

[16] DIAO Q, HUANG Q, LIN S, et al. A transform approach for analyzing and constructing quasi-cyclic low-density parity-check codes[C]//Proceedings of 2011 Information Theory and Applications Workshop. [S.l.]: IEEE, 2011: 1-8.

[17] CHEN Z, GU Y, CHEN P, et al. Improved EXIT algorithm based on Gaussian mixture model and its application to LDPC construction in coding cooperative systems with hybrid fading[J]. IEEE Access, 2020, 8: 49933-49950.

[18] 徐恒舟. LDPC码:分析、设计与构造[D]. 西安:西安电子科技大学,2017.
XU Hengzhou. LDPC code: Analysis, design and construction[D]. Xi'an: Xidian University, 2017.

[19] MYUNG S, YANG K, KIM J. Quasi-cyclic LDPC codes for fast encoding[J]. IEEE Transactions on Information Theory, 2005, 51(8): 2894-2901.

[20] OTMANI A, TILLICH J P, DALLOT L. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes[J]. Mathematics in Computer Science, 2010, 3(2): 129-140.

[21] CCSDS. Tm synchronization and channel coding: 131.0-B-3[S]. [S.l.]: [s.n.], 2009.

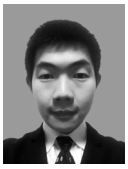
[22] GAO N, XU Y, HE D, et al. Design of LDPC codes for joint satellite and terrestrial broadcasting system[C]//Proceedings of 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB). [S.l.]: IEEE, 2018: 1-6.

作者简介:

李广(1994-),男,硕士研究生,研究方向:卫星通信、信道编码,E-mail:1216739-033@qq.com。

朱宏鹏(1982-),**通信作者**,男,博士,副教授,研究方向:卫星通信、信道编码以及调制解调等,E-mail:hongpengzhu@126.com。

李聪(1997-),男,硕士研究生,研究方向:卫星通信、物理层安全以及信息论。



葛瑞星(1993-),男,博士研究生,研究方向:多层卫星网络资源配置、非正交多址接入等。

李广侠(1964-),男,教授,研究方向:通信系统设计、卫星通信、卫星导航和抗干扰通信等。

(编辑:刘彦东)