·通信与信息工程·

基于LDPC码的安全可靠通信方法研究

史治平[1,2]，任亚军[1]，吕凤橙[1]

(1. 电子科技大学通信抗干扰技术国家级重点实验室 成都 611731；2. 通信网信息传输与分发技术重点实验室 石家庄 050081)

【摘要】LDPC码是一类由校验矩阵确定的线性分组码，具有逼近香农限的纠错能力。该文基于纠错码的对称密码体制以及性能等价编码矩阵提出了一类基于LDPC码的安全通信方法，该方法在几乎不改变通信可靠性的情况下，极大地提高了系统的抗截获能力。编码矩阵可以使线性分组码的生成矩阵或校验矩阵。该文通过构造大量性能等价的编码矩阵，以及通信时收发双方同时随机改变编码矩阵的方法来提高通信系统的抗截获能力。另外，由于这些性能等价的编码矩阵产生的LDPC码不仅具有相同的编码参数和可靠性，而且具有非常强的纠错能力，因此该方案是一种安全可靠的一体化通信方法。

关 键 词 LDPC码；线性同余；奇偶校验矩阵；安全通信

中图分类号 TN911.22 **文献标志码** A doi:10.3969/j.issn.1001-0548.2017.05.001

Research on Secure and Reliable Communications Method Based on LDPC Codes

SHI Zhi-ping [1,2], REN Ya-jun[1], and LÜ Feng-cheng[1]

(1. National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China Chengdu 611731;
2. Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory Shijiazhuang 050081)

Abstract Low-density parity-check (LDPC) codes are a class of linear block codes defined by the check matrix, which have the error-correcting capability of approaching Shannon limit. Based on the symmetric cryptosystem with error correcting codes as well as performance equivalent coding matrix, this paper proposes a secure communication method based on LDPC codes. This method greatly improves the anti-intercept capability of system and keeps the reliability almost unchanged by constructing a large number of performance equivalent coding matrixes and by simultaneously and randomly shifting the coding matrixes by the sender and receiver. Thus the proposed method has better error-correcting capability and can be applied as a secure and reliable integrated communication solution.

Key words LDPC codes; linear congruence; parity check matrix; secure communication

信道编码盲识别技术是一种根据侦收到的数据快速有效地识别出信道编码体制的方法，实现了对信源信息的获取，为通信对抗提供更多可靠的依据。这种方式是非合作信号处理从信号层向信息层的扩展，这在非合作通信领域具有重要的价值。因此，信道编码盲识别技术受到国内外研究人员的高度重视，并取得了很多研究成果。按照信道编码类型，信道盲识别技术分为卷积码参数盲估计和分组码参数盲估计，其中分组码主要是线性分组码参数的盲识别。

LDPC码是一种由稀疏校验矩阵定义的线性分组码[1]，在码长较长时其性能逼近香农限。自LDPC码被发现以来，研究人员从LDPC码的构造、编码、译码方法等方面展开了深入的研究，当前LDPC码在卫星、深空、移动、无线等通信系统中已被广泛应用，成为最有潜力的信道编码解决方案。对LDPC码的盲识别算法也逐渐成为研究热点[2-4]。LDPC码盲识别的最终目标是实现稀疏校验矩阵的正确重建。LDPC码的盲识别是为了解决误码条件下的LDPC码开集识别问题。通过综合利用列消元运算、校验向量判定准则以及渐进行变换等方法，将发现正确校验向量和剔除含误码码组作为手段，最终把原问题成功地退化为无误码条件下对LDPC码接收序列进行高斯消元，获取码字空间的一组基，即生成矩阵$\boldsymbol{G}$，进而方便地获取至少一个非稀疏校验矩阵$\boldsymbol{H}_d$。在此基础上，利用足够多次数的线性行变换

收稿日期：2016－10－27；修回日期：2017－05－09
基金项目：国家863项目(2014AA01A704)
作者简介：史治平(1972－)，女，博士，教授，主要从事无线通信与纠错编码的研究.

运算，可最终实现稀疏校验矩阵的正确重建。

虽然LDPC码盲识别技术的计算难度较大，且该技术目前还存在很多亟待解决的问题，但LDPC码的盲识别技术研究给传统的保密通信方案敲响了警钟。通过保密校验矩阵$\boldsymbol{H}$(或生成矩阵$\boldsymbol{G}$)实现LDPC码的安全通信已经显得越来越脆弱，因此需要新的增强系统安全性的保密方案。

文献[5]证明了纠错码(信道编码)的一般线性分组码译码问题是一个NPC问题。文献[6]利用这一理论基础并结合Goppa码，首次提出了一类基于纠错码的公钥密码体制，称为McEliece公钥密码体制(M体制)。该体制的基本思想是首先接收方选择一个具有快速译码算法的特定码作为私钥，然后使用一个陷门函数将这个特定码隐藏起来，而敌手看到的只是一个一般的线性码。而且该密码体制具有抗量子攻击的特性，因为密码学界普遍认为量子计算机无法攻破NPC问题，所以该密码体制在量子计算机时代仍然是安全的。但该密码体制存在明显的缺点：密钥开销大、信息速率低且没有考虑有扰信道的情况。

针对M体制密钥开销大、信息速率低等缺点，研究者们相继提出了很多改进方案，其中大部分都是利用LDPC码等具有紧致生成矩阵或校验矩阵的码来代替Goppa码[7]；而针对有扰信道的情况，文献[8]对该密码体制进行了修正，使其具有一定的纠错能力，并将修正后的密码体制称为M_s公钥体制，但这种修正会损失一定的安全性，需要在安全性和可靠性之间进行折中。为了解决该问题，文献[9]提出了基于M公钥体制的分组加密纠错体制，但密钥开销大依旧是该方案的弱点，而且后续研究证明该方案可以被一些选择明文攻击攻破。因此，研究新的M对称密码体制改进方案来降低密钥开销、提高系统的安全性，显得非常重要。

本文基于纠错码的对称密码体制以及性能等价矩阵的概念，提出了一类基于LDPC码的安全通信方法，设计了大量等价的编码矩阵，通过通信双方随机改变编码矩阵，在不改变LDPC码纠错能力的前提下，提高了非合作方识别或破获信息的难度。同时针对密钥开销问题，给出了一种低复杂度密钥控制的同步实现方案。

1 系统模型

1.1 LDPC码

LDPC码是基于稀疏校验矩阵的线性分组码，因此构造LDPC码实际上就是构造一个稀疏的校验矩阵$\boldsymbol{H}$。根据生成矩阵$\boldsymbol{G}$与校验矩阵$\boldsymbol{H}$之间的关系$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=0$，可以得到生成矩阵$\boldsymbol{G}$。因此，发送端可以基于$\boldsymbol{G}$对信息序列$m$进行编码，得到码字$\boldsymbol{c}=m\boldsymbol{G}$。在接收端，译码器基于校验矩阵$\boldsymbol{H}$，利用置信传播算法从带有噪声的接收序列中恢复出原始信息序列。

对于LDPC码$\boldsymbol{H}$矩阵的生成，主要有以下几种方法：1) 随机生成$\boldsymbol{H}$后经过仿真挑选[10]，这种方式是早期取得最佳性能LDPC码所采用的方式；2) 通过PEG等方法[11]，从双边图的角度构造$\boldsymbol{H}$矩阵，可以得到性能比较稳定的$\boldsymbol{H}$矩阵。以上两种方法都是从性能的角度出发构造$\boldsymbol{H}$矩阵，通常情况下硬件实现复杂度较高。目前使用较多的是结构化$\boldsymbol{H}$矩阵[12]，如准循环LDPC码(QC-LDPC码)。这种类型的LDPC码从实现角度出发，结构特殊，利于编码或译码实现。

1.2 系统模型

设m为待加密编码的信息序列，通信双方均已知参数$\boldsymbol{H}$、$\boldsymbol{S}$、$\boldsymbol{P}$，其中$\boldsymbol{H}$是$(n-k)\times n$阶线性分组码的奇偶校验矩阵，$\boldsymbol{G}$为$\boldsymbol{H}$对应的线性分组码的$k\times n$阶生成矩阵，$\boldsymbol{S}$为$k\times k$阶密集可逆矩阵，$\boldsymbol{P}$为$n\times n$阶置换矩阵(即$\boldsymbol{P}^{\mathrm{T}}=\boldsymbol{P}^{-1}$)。

1) 发送端编码和加密算法为：

$$\boldsymbol{c}=m\boldsymbol{S}\boldsymbol{G}\boldsymbol{P} \tag{1}$$

接收端的接收向量为：

$$\boldsymbol{r}=\boldsymbol{c}+\boldsymbol{n} \tag{2}$$

式中，n表示信道引入的噪声。

2) 解密与解码的具体步骤如下：

首先将接收到的序列$\boldsymbol{r}$右乘$\boldsymbol{P}^{\mathrm{T}}$得到：

$$\boldsymbol{r}'=\boldsymbol{r}\boldsymbol{P}^{\mathrm{T}}=\boldsymbol{c}\boldsymbol{P}^{\mathrm{T}}+\boldsymbol{n}\boldsymbol{P}^{\mathrm{T}}=m\boldsymbol{S}\boldsymbol{G}+\boldsymbol{n}' \tag{3}$$

然后根据线性分组码的生成矩阵$\boldsymbol{G}$或校验矩阵$\boldsymbol{H}$，对$\boldsymbol{r}'$进行译码，得到：$\boldsymbol{u}'=m\boldsymbol{S}$

最后将$\boldsymbol{u}'$右乘$\boldsymbol{S}$的逆，还原明文信息$\boldsymbol{m}$：

$$\boldsymbol{u}'\boldsymbol{S}^{-1}=m\boldsymbol{S}\boldsymbol{S}^{-1}=m \tag{4}$$

该模型与基于纠错编码的公钥密码体制[13-14]类似，但与之不同的是，这里的矩阵$\boldsymbol{S}$、$\boldsymbol{P}$、$\boldsymbol{H}$、$\boldsymbol{G}$都是随机可变的，它们既可以单独变化，也可以联合改变。本文只考虑两种变化方式($\boldsymbol{H}$和$\boldsymbol{P}$)，通信时基于性能等价的海量编码矩阵随机改变，提高破解难度。

1) 海量置换矩阵$\boldsymbol{P}$在收发双方同时跳变

不同于传统的M对称密码体制中矩阵$\boldsymbol{P}$始终不发生变化，本文方案中，每次通信发送端和接收端同步选用与之前通信不同的置换矩阵$\boldsymbol{P}$进行加解密操作，矩阵$\boldsymbol{P}$的变化空间为$n!$。当n=100时，矩阵$\boldsymbol{P}$的个数可以大于2^{512}，可见矩阵数量巨大，可以达到理论上的一次一密，提高了通信系统的安全性。

2) 基于海量校验矩阵$\boldsymbol{H}$跳变的安全通信

本文采用随机循环差集(RDF)的方法构造大量等价的LDPC码的校验矩阵$\boldsymbol{H}$，通信双方通过随机选择编码矩阵，提高系统的抗截获能力。

研究显示，基于RDF的LDPC码在相同的参数下可以形成大量的等价码[13]，根据RDF构造的校验矩阵$\boldsymbol{H}$的特性，发送端和接收端可以同步改变校验矩阵$\boldsymbol{H}$，有效地提高破译的难度。另外，RDF-LDPC码的奇偶校验矩阵$\boldsymbol{H}$为准循环结构，且可以由基组向量$\boldsymbol{B}$唯一确定，因此，基于RDF-LDPC码构造的安全体制可以减少密钥存储量。

为降低密钥开销和同步难度，基于线性同余思想产生置换矩阵$\boldsymbol{P}$和校验矩阵$\boldsymbol{H}$。发送端和接收端都不用存储$\boldsymbol{P}$矩阵和$\boldsymbol{H}$矩阵，只选用线性同余方法产生的密钥便可使$\boldsymbol{P}$和$\boldsymbol{H}$同步变化，这样能够有效地降低密钥量。

2　基于LDPC码的安全通信方案

下面给出两种基于LDPC码的安全可靠的通信方案，一种是随机改变置换矩阵$\boldsymbol{P}$，另外一种是改变校验矩阵$\boldsymbol{H}$。两种方案都不降低LDPC码的纠错性能，同时具有很高的安全性。

2.1　海量置换矩阵$\boldsymbol{P}$的生成与同步

下面基于线性同余思想，给出收发双方同步产生置换矩阵$\boldsymbol{P}$的方法。

2.1.1　密钥生成

将基于线性同余方法(linear congruence, LCG)产生的伪随机序列作为通信双方的密钥，然后基于这个密钥同步控制编码矩阵的变化。下面给出密钥的生成过程。

线性同余产生器的递推公式为：

$$N_{i+1}=aN_i+b \pmod{M} \quad i=0,1,2,\cdots,M-1 \tag{5}$$

式中，a、b、M是产生器设定的常数，分别是乘数、增量和模数；N_0为产生器的初始值。

LCG的最大周期为M，但大部分情况都会小于M。为了确保LCG达到最大周期，式(5)中的参数应满足以下5个条件：

1) M与b互质；

2) M的所有质因子的积能整除$a-1$；

3) 若M是4的倍数，则$a-1$也应该是4的倍数；

4) a、b、N_0都比M小；

5) a、b都是正整数。

若式(5)的参数满足以上条件，则该递推公式在重复之前可以产生0～M之间的所有整数。

根据以上线性同余的思想，本文方案的密钥选取步骤如下：

1) 可信第三方根据LCG达到最大周期的条件，合理地选择乘数a和增量b，并将选好的a，b作为密钥分发给通信的收发两方；

2) 可信第三方随机选取大随机数N作为密钥分发到通信双方；

3) 可信第三方随机选择一个密集的可逆矩阵$\boldsymbol{S}$作为密钥分发给通信双方；

4) 通信双方根据收到的密钥(a，b，N，$\boldsymbol{S}$)产生同步控制序列，其中$\boldsymbol{S}$用于编译码。

① 通信双方统一选取模数M，M是LDPC码的码长；

② 收发双方根据随机数密钥N，计算$N_0=N \bmod M$，得到初始值N_0；

③ 收发双方根据线性同余产生器的递推公式得到长度为M的整数序列为：

$$n=(N_0,N_1,N_2,\cdots,N_{M-1}) \quad i=0,1,2,\cdots,M-1 \tag{6}$$

2.1.2　生成同步置换矩阵$\boldsymbol{P}$

基于上述方法产生密钥后，通信双方每次通信时得到同步置换矩阵$\boldsymbol{P}$的步骤如下：

1) 根据密钥产生时得到的整数序列$n=(N_0, N_1,\cdots,N_{M-1})$，确定初始置换矩阵$\boldsymbol{P}$；

由于置换矩阵中每一行每一列都只有一个1，如果将置换矩阵$\boldsymbol{P}$第i行的非零位置设为l_i，计算：

$$l_i=N_{i-1}+1 \quad i=1,2,3,\cdots,M \tag{7}$$

则初始置换矩阵$\boldsymbol{P}$可以由序列$l=(l_1,l_2,\cdots,l_M)$唯一确定。

2) 根据前面得到的整数序列$n=(N_0, N_1,\cdots, N_{M-1})$，通信双方对置换矩阵$\boldsymbol{P}$做同步变化。

由1)可知，置换矩阵$\boldsymbol{P}$由整数序列n唯一确定，收发双方每次通信时，可以采用相同的规则对序列n重新排列。本文采用邻位对换法依次得到基于序列n的每一个新的序列n'，由n'确定新的置换矩阵$\boldsymbol{P}'$，并且用$\boldsymbol{P}'$进行下次通信的加解密操作。

邻位对换法可以由已知序列以非递归的方式，依次得到该序列的全排列序列。

邻位对换法得到全排列的主要思想：

1) 邻位对换法中下一个排列总是上一个排列中某相邻的两位对换得到的，以4个元素的排列1 3 4 2为例，将第一个元素1逐次与其后面的元素交换，可以生成3个新的排列：3 1 4 2，3 4 1 2，3 4 2 1；

2) 将最后一个排列的前面的两个元素交换，再逐次将末尾的1与其前面的元素交换，又生成4个新

排列：4 3 2 1，4 3 1 2,，4 1 3 2，1 4 3 2；

3) 将最后一个排列的末尾的两个元素交换，将1从前往后移：1 4 2 3，4 1 2 3，4 2 1 3，4 2 3 1；

4) 如此循环即可求出已知序列的全排列。

对于长度为M的序列n，根据邻位对换，可以获得该序列的全排列，共有$M!$种不同的序列，对应$M!$种不同的置换矩阵$\boldsymbol{P}$。

本通信方案中的置换矩阵由线性同余参数控制变化，因此在进行LDPC译码前需要根据每次通信的矩阵$\boldsymbol{P}$进行反交织，然后再进行LDPC译码。由于本文方案中的校验矩阵始终不发生变化，因此可以使用相同的译码器实现。

2.2 基于海量校验矩阵$\boldsymbol{H}$的LDPC安全通信

本文基于RDF生成的性能等价校验矩阵数量巨大的特点，设计了基于海量校验矩阵随机变化的LDPC码安全通信方案。下面介绍该方法的基本原理与通信过程。

为了方便叙述，先给出模p的差的定义。

定义 设$\mathbb{Z}_p$是一个整数模p的集合，对于给定的两个元素$x,y\in\mathbb{Z}_p$模p的差定义为[13]：

$$\delta_{xy}^{p}=\begin{cases}x-y & x\geqslant y\\ p-(y-x)=p-\delta & x<y\end{cases} \tag{8}$$

2.2.1 基于RDF算法生成校验矩阵$\boldsymbol{H}$

假设QC-LDPC的奇偶校验矩阵的形式为：

$$\boldsymbol{H}=[\boldsymbol{H}_0 \quad \boldsymbol{H}_1 \quad \cdots \quad \boldsymbol{H}_{n_0-1}] \tag{9}$$

$\boldsymbol{H}$由n_0个基本块$\boldsymbol{H}_i$组成，其中$\boldsymbol{H}_i$是大小为$p\times p$的循环行移位方阵，$\boldsymbol{H}_i$中的第k+1行元素可由第k行元素排列的循环左(右)移1位所得。形如：

$$\boldsymbol{H}_i=\begin{bmatrix}a_0 & a_1 & a_2 & \cdots & a_{p-1}\\ a_1 & a_2 & a_2 & \cdots & a_0\\ a_2 & a_3 & a_4 & \cdots & a_1\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ a_{p-1} & a_0 & a_1 & \cdots & a_{p-2}\end{bmatrix}_{p\times p} \tag{10}$$

另假设集合B由n_0个基本块B_i组成：

$$B=\{B_0,B_1,\cdots,B_{n_0-1}\} \tag{11}$$

每个基本块B_i都是$\mathbb{Z}_p$的一个子集，且与$\boldsymbol{H}$中的循环块$\boldsymbol{H}_i$一一对应，$B_i\leftrightarrow\boldsymbol{H}_i$，其对应方式为：$B_i$包含$\boldsymbol{H}_i$中第一行非零元素的位置，若将$\boldsymbol{H}_i$的第一行表示为多项式，基块$B_i$包含变量$x$在该多项式$A_i(x)$的指数，即：

$$B_i\leftrightarrow A_i(x)=\sum_{j=0}^{d_v}x^{d_{ij}} \qquad i\in[0,n_0-1] \tag{12}$$

式中，d_{ij}为基块B_i的第j个元素。

由$\boldsymbol{H}_i$的结构特点知，当$\boldsymbol{H}_i$的第一行元素确定之后整个矩阵$\boldsymbol{H}_i$也将被确定。

对于规则矩阵，假设d_v即为矩阵$\boldsymbol{H}$的列重，则行重$d_c=n_0d_v$。在这种情况下，为了定义整个矩阵$\boldsymbol{H}$，每个基本块B_i必须包含d_v个不同的元素，由式(8)可知这d_v个元素可以产生$d_v(d_v-1)$个差值δ_{xy}^{p}。

根据Tanner图中4环的结构特点，为了避免该类型码对应的Tanner图中存在4环，其奇偶校验矩阵基本块$\boldsymbol{H}_i$相对应的B_i必须满足特性[13]：

$$\begin{aligned}&\delta_{ab}^{p}\neq\delta_{cd}^{p} \quad \forall a,b\in B_i,\forall c,d\in B_j\\ &\forall i,j\in[0,n_0-1]\end{aligned} \tag{13}$$

随机地选择每个基本块B_i中的元素，验证是否满足式(13)，即码的Tanner图中不存在4环的条件。如果不满足，再重试直到找到满足条件的基本块组$B_0,B_1,\cdots,B_{n_0-1}$，然后根据$B=\{B_0,B_1,\cdots,B_{n_0-1}\}$构造QC-LDPC码的校验矩阵$\boldsymbol{H}=[\boldsymbol{H}_0 \quad \boldsymbol{H}_1 \quad \cdots \quad \boldsymbol{H}_{n_0-1}]$。

由此可见，该方法构造的LDPC码的校验矩阵$\boldsymbol{H}$由基本块组B唯一决定。因此通信双方只需要存储B便可以唯一确定出该LDPC码的校验矩阵$\boldsymbol{H}$，基于这种结构进行安全可靠通信，可以大大降低密钥量。

2.2.2 QC-LDPC码校验矩阵$\boldsymbol{H}$的数量分析

假设$\boldsymbol{H}_{n_0-1}$循环矩阵是可逆的，其逆矩阵$\boldsymbol{H}_{n_0-1}^{-1}$仍然是循环矩阵，则校验矩阵$\boldsymbol{H}$对应的生成矩阵：

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I} & (\boldsymbol{H}_{n_0-1}^{-1}\boldsymbol{H}_0)^{\mathrm{T}}\\ & (\boldsymbol{H}_{n_0-1}^{-1}\boldsymbol{H}_1)^{\mathrm{T}}\\ & \vdots\\ & (\boldsymbol{H}_{n_0-1}^{-1}\boldsymbol{H}_{n_0-2})^{\mathrm{T}}\end{bmatrix} \tag{14}$$

则由矩阵$\boldsymbol{G}$便可生成一类QC-LDPC码。

对于LDPC码的参数，码长$n=pn_0$，码率$R=(n_0-1)/n_0$，列重d_v，基于RDF算法可以构造出的无4环的不同QC-LDPC码的平均数量为[13]：

$$\begin{aligned}N(n_0,d_v,p)\geqslant&\frac{1}{p}\binom{p}{d_v}^{n_0}\prod_{l=0}^{n_0-1}\prod_{j=1}^{d_v-1}\frac{p}{p-j}-\\ &\frac{j[2-p\bmod 2+(j^2-1)/2+ld_v(d_v-1)]}{p-j}\end{aligned} \tag{15}$$

当$n_0=4$，$d_v=11$，$p=4\,032$时，$N(n_0,d_v,p)\geqslant 2^{391}$，可见这个数字是相当大的。因此当采用这种矩阵作为LDPC码的校验矩阵进行可靠传输时，可以随机选取性能等价的$\boldsymbol{H}$进行编译码，提高通信系统的安全性。

2.2.3 基于海量校验矩阵$\boldsymbol{H}$的安全通信方案

基于RDF的校验矩阵$\boldsymbol{H}$的产生原理可知，校验

矩阵 $\boldsymbol{H}=[\boldsymbol{H}_0\ \ \boldsymbol{H}_1\ \ \cdots\ \ \boldsymbol{H}_{n_0-1}]$ 由集合 $B=\{B_0,B_1,\cdots,B_{n_0-1}\}$ 唯一确定，B_i 包含着 $\boldsymbol{H}_i$ 第一行中非零元的位置。而对于 B_i 中的每个元素的确定方法是：随机地从集合 $c=\{1,2,3,\cdots,p\}$ 中选择一个值，其中p为循环块的长度，验证该值是否满足式(13)，若满足则保留，否则重复该步骤，直到找出满足条件的基组 $B_0,B_1,\cdots,B_{n_0-1}$，再根据基组 $B=\{B_0,B_1,\cdots,B_{n_0-1}\}$ 构造QC-LDPC码的校验矩阵 $\boldsymbol{H}=[\boldsymbol{H}_0\ \ \boldsymbol{H}_1\ \ \cdots\ \ \boldsymbol{H}_{n_0-1}]$。

由此可看出，校验矩阵$\boldsymbol{H}$由每次从集合c中选取的元素确定。B_i 中元素的确定方法是从序列 $c'=(c_0,c_1,\cdots,c_{p-1})$ 中的第一个元素开始依次选取，其中 c_i 验证选取的值是否满足无4环的条件，若满足则保留，否则取序列c'中下一个值，继续验证是否满足无4环的条件，依次类推，直到找出满足条件的基组 $B_0,B_1,\cdots,B_{n_0-1}$。如果通信双方可以得到相同的唯一确定的序列c'，那么双方便可同步产生相同的校验矩阵$\boldsymbol{H}$。即确定了序列c'，也就确定了校验矩阵$\boldsymbol{H}$。

借助于线性同余的方法，收发双方可以同时得到相同的序列c'，这里采用与产生置换矩阵$\boldsymbol{P}$相同a，b，N，但模数M的值等于循环块的长度p，N_0=Nmod$M$，将这些参数代入式(5)，通信双方可以同时获得相同的序列c'，然后根据c'得到相同的校验矩阵$\boldsymbol{H}$。

第一次通信时，通信双方基于序列c'产生校验矩阵$\boldsymbol{H}$，下次通信时，通信双方可以协同产生新的递推公式初值N_0(如N_0=N_0+1)，进而得到新的序列c'和新的校验矩阵$\boldsymbol{H}$，进一步增大通信的密钥空间，增强通信的安全性。

本文通信方案中，因为校验矩阵$\boldsymbol{H}$每间隔一定时间发生改变，所以译码器也应随之改变，这在一定程度上增加了系统的复杂度。由于校验矩阵$\boldsymbol{H}$是根据密钥参数a，b，N动态生成的，因此在密钥参数发生变化后，可以使用软件定义的方式，动态同步改变LDPC译码器。为了权衡系统的复杂度和安全性，可以考虑选择合适的校验矩阵变化频率。

3　性能仿真与安全性分析

下面通过具体实例对以上算法进行说明和性能分析。

3.1　置换矩阵随机改变

LDPC码的码长为1 024比特，码率为1/2。密钥参数：N=5 197、$a=2\wedge 7+1$、b=47。校验矩阵参数：$B_1=[417,65,323,280,494]$，$B_2=[463,467,142,490,80]$，$p=512$，$d_v=5$。

设需要编码的信息序列为m，编码加密方案为$\boldsymbol{c=mSGP}$，仿真过程中每一帧都采用不同的置换矩阵$\boldsymbol{P}$，校验矩阵$\boldsymbol{H}$始终不变，仿真结果如图1所示。

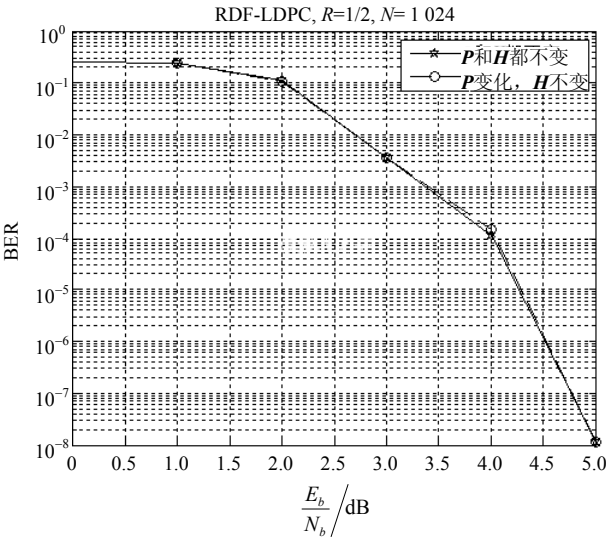

图1　置换矩阵$\boldsymbol{P}$变化与$\boldsymbol{P}$不变时的误码曲线对比图

由仿真结果可以看出，每次通信都更新置换矩阵$\boldsymbol{P}$的设计方案并不会影响系统的纠错能力，但该设计方案仅仅依靠N、a和b作为密钥，就可以产生M!种不同的编码加密方案。在此仿真中M =1 024，可以产生一个巨大的数，避免了通信双方对海量的置换矩阵$\boldsymbol{P}$的存储，极大地降低了密钥存储量，而且每次通信采用不同的置换矩阵$\boldsymbol{P}$，提高了系统的安全性。

3.2　改变校验矩阵$\boldsymbol{H}$

在仿真参数设置、加密编码方案与3.1节相同的情况下，为了模拟校验矩阵$\boldsymbol{H}$的变化，仿真时，对于每个信噪比校验矩阵$\boldsymbol{H}$改变20次，置换矩阵$\boldsymbol{P}$始终不变，结果如图2所示。

本文方案同样依靠N、a和b作为密钥，通信双方便可以同步产生多种具有相同性能的校验矩阵，不用存储这些校验矩阵就可以完成编译码操作，进一步降低了密钥存储量。由于在相同的参数下，基于RDF构造的LDPC码是等价码，所以，从该误码曲线对比图中可以看出，改变校验矩阵$\boldsymbol{H}$对误码性能的影响很小，但通信双方通过同步改变校验矩阵$\boldsymbol{H}$，可以有效增强系统的安全性。

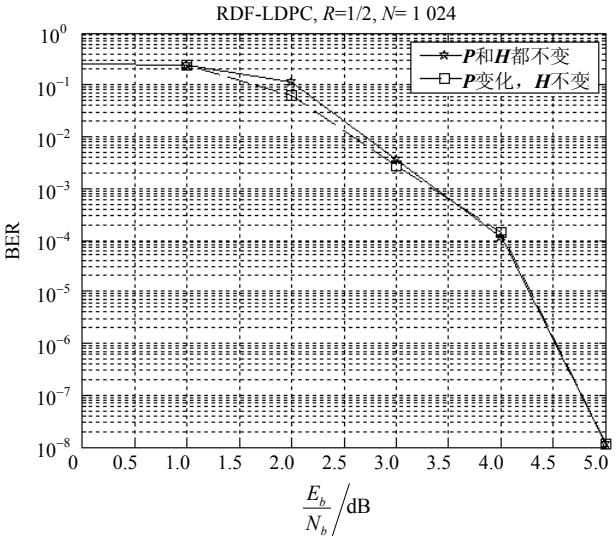

图2 校验矩阵***H***变化与***H***不变时的误码曲线对比图

3.3 校验矩阵和置换矩阵都随机改变

在仿真参数设置、加密编码方案与3.1节相同的情况下，为了模拟校验矩阵***H***的变化，仿真时每个信噪比校验矩阵***H***改变20次；仿真过程中每一帧都采用不同的置换矩阵***P***，仿真结果如图3所示。

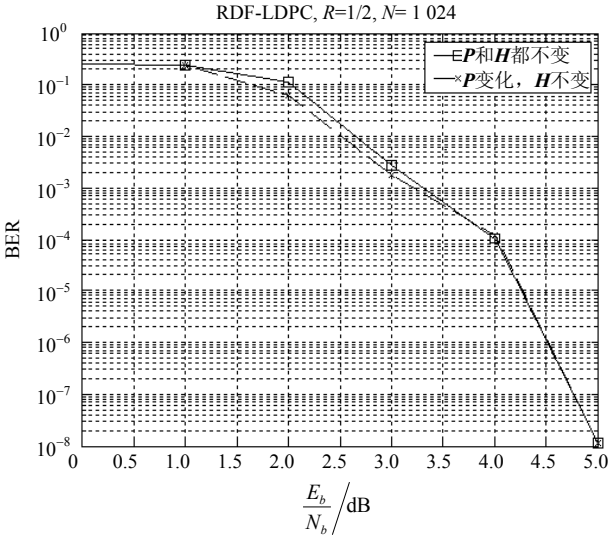

图3 置换矩阵***P***和校验矩阵***H***同时变化时的误码曲线图

将图3与图2对比可知，在校验矩阵***H***发生变化的基础上，让置换矩阵***P***在每次通信中都发生改变，不会影响编译码性能。通信过程中同时改变置换矩阵***P***和校验矩阵***H***会进一步增强系统的安全性，系统的密钥始终只是N、a、b和可逆方阵***S***，降低了密钥的存储量。

4 结 束 语

综上所述，本文提出的基于LDPC码的海量编码矩阵传输方案是一种高效的安全可靠传输方法。通过通信双方在海量编码矩阵中的随机选取，极大地增加了系统的安全性，提高了系统抗截获能力；另一方面，由于海量编码矩阵的性能等价性，通信系统的纠错性能不受影响，保证了系统的可靠性和高效性；最后，给出了一种降低开销密钥的编译码矩阵同步控制方案，与直接传递和存储编码矩阵相比，该方案大大降低了密钥开销。

本文建议的基于LDPC码的安全可靠通信方法是一种编码域的抗干扰、抗截获通信方式，它通过信道编码矩阵的随机改变，在保证系统可靠性的同时，提高了编码被攻击者破译的难度。这对于提高基于LDPC码通信系统的安全性具有重要意义。

本文研究工作得到了通信网信息传输与分发技术重点实验室开放课题(KX152600018/ITD-U15009)的资助，在此表示感谢。

参 考 文 献

[1] MACKAY D J C, NEAL R M. Near Shannon limit performance of low density parity check codes[J]. Electronics Letters, 1996, 18(32): 1645-1646.

[2] 包昕, 周磊硐, 何可, 等. LDPC码稀疏校验矩阵的重建方法[J]. 电子科技大学学报, 2016, 45(2): 191-196.
BAO Xin, ZHOU Lei-ke, HE Ke, et al. A method of restructuring LDPC parity-check matrix[J]. Journal of University of Electronic Science and Technology of China, 2016, 45(2): 191-196.

[3] 包昕, 周磊硐, 何可, 等. 误码条件下的LDPC码盲识别算法[J]. 西安交通大学学报, 2015, 12(49): 53-58.
BAO Xin, ZHOU Lei-ke, HE Ke, et al. A recognition algorithm for LDPC codes of blind in a noisy environment[J]. Journal of Xi'an Jiaotong University, 2015, 12(49): 53-58.

[4] 刘海达, 李静, 彭华. 利用最大偏差比的LDPC码识别算法[J]. 信号处理, 2014, 8(30): 908-913.
LIU Hai-da, LI Jing, PENG Hua. Identification algorithm for LDPC codes using maximum deviation ratio[J]. Journal of Signal Processing, 2014, 8(30): 908-913.

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

[6] MCELIECE R J. A public-key cryptosystem based on algebraic coding theory[J]. DSN Progress Report, 1978, 1(9): 114-116.

[7] SHOOSHTARI M K, AHMADIAN M, PAYANDEH A. Improving the security of McEliece-like public key cryptosystem based on LDPC codes[C]//11th International Conference on Advanced Communication Technology. PhoenixPark, Korea: IEEE, 2009: 1050-1053.

[8] 王新梅. M公钥的推广及通过有扰信道时的性能分析[J]. 电子学报, 1986, 1(4): 86-92.

WANG Xin-mei. Generalization of M public key system and analysis of its performance on noisy[J]. Acta Electronica Sinica, 1986, 1(4): 84-91.

[9] RAO T N R. Joint encryption and error correction schemes [C]//Proceedings of the 11th Annual International Symposium on Computer Architecture. New York, USA: ACM Sigarch Computer Architecture News, 1984, 12(3): 240-241.

[10] RICHARDSON T J, RUDIGER L. Urbanke, effcient encoding of low-density parity check codes[J]. IEEE Trans Inf Theory, 2001, 47(2): 638-656.

[11] HU X Y, ELEFTHERIOU E. Regular and irregular progressive edge-growth tanner graphs[J]. IEEE Transactions on Information Theory, 2005, 1(51): 386-398.

[12] LEI C, IVANA D, JUN X, et al. Construction of quasi-cyclic ldpc codes based on the minimum weight codewords of reed-solomon codes[J]. ISIT, 2004, 1(1): 239.

[13]MARCO B. QC-LDPC code-based cryptography[M]. [S.l.]: Springer, 2014: 23-64.

[14] 蒋定顺, 金力军. 高速跳频通信系统同步技术研究[J].电子科技大学学报, 2005, 34(1): 48-52.
JIANG Ding-shun, JIN Li-jun. Research on synchronization technique for a high-speed FH communication system[J]. Journal of University of Electronic Science and Technology of China, 2005, 34(1): 48-52.

编 辑 叶 芳