高斯 Wiretap 模型下基于部分陪集的无线物理层强安全编码

易 鸣* 季新生 黄开枝 钟 州 郭淑明
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：针对无线物理层安全编码不能保证信息在有噪信道下进行强安全传输的问题，该文提出一种基于部分陪集的强安全编码方法。首先证明了当且仅当陪集母码的对偶码的最小汉明距离大于信息泄露位数时，利用部分陪集编码能够保证信息的强安全传输；然后证明了陪集编码的一系列性质，基于这些性质可以将陪集间最小汉明距离计算降低为1次查表运算，进而设计了一种基于树形深度优先的最大可用陪集集合搜索算法；最后分析得出一些典型线性分组码的抗窃听信道信息泄露和抗合法信道传输噪声的能力，以及相应的最大可用陪集集合。当陪集母码为BCH(15,11)的对偶码时，与传统陪集编码方案相比，该方法对合法信道的信道质量要求降低了5 dB，同时能够保证信息传输的强安全性。

关键词：强安全编码；无线物理层；高斯 Wiretap；陪集
中图分类号：TN929.53 **文献标识码**：A **文章编号**：1009-5896(2014)04-0780-07
DOI: 10.3724/SP.J.1146.2013.00778

A Wireless Physical Layer Coding Method Achieving Strong Security Based on Partitioning Coset for the Gaussian Wiretap Model

Yi Ming Ji Xin-sheng Huang Kai-zhi Zhong Zhou Guo Shu-ming
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: To solve the problem of that the wireless physical layer secrecy coding can not achieve strong security while the legal channel is noisy, a strong security coding method is proposed based on partitioning coset. First, it is proved that if and only if the minimum Hamming distance of the dual code of the coset mother code is larger than the number of leak bits, the method can keep strong security. It is also proved that many properties of partitioning coset can help to decrease the calculation complexity to one time table search to get the Hamming distance among cosets, and a search algorithm is proposed based on tree deep priority to get maximum available coset set. Finally, the abilities of anti-information leakage in eavesdropper channel, the anti-noise in legal channel, and the corresponding maximum available coset set of typical linear block codes is presented. Compared with the traditional method, the proposed method reduces the requirement of the legal channel quality with 5 dB while keeping strong security when the mother code is the dual code of BCH(15,11).

Key words: Strong security coding; Wireless physical layer; Gaussian Wiretap; Coset

1 引言

无线物理层安全编码是一种在保证授权双方信息传输可靠性的基础上，进一步考虑信息传输安全性的信道编码技术。其目的是使授权双方的私密信息能够正常传输，而使窃听方无法获得任何私密信息。其优点是不需要通信双方事先分配或协商密钥加密，在物理底层直接防止第3方窃听。

1975年 Wyner[1]针对有线通信网络首次提出了基于信息理论安全的 Wiretap 模型，证明了当合法信道质量优于窃听信道时存在安全容量，文献[2]进一步将该模型拓展到广播信道，并利用典型序列理论，证明了在该模型下逼近安全容量的码字是存在的。文献[3]首次给出了一种合法信道无噪，窃听信道为二进制纯擦除信道(Binary Eraser Channel, BEC)Wiretap 模型下的具体物理层安全编码方式——陪集编码。合法信道无噪使得安全编码不需要考虑纠错性能，只需要重点关注安全性。有线通信网络中物理层的信息传输错误率较低，通过校验、重传等机制可以实现合法信道无噪，然而无线信道必定有噪，尽管可以利用功率控制等技术实现合法信道的近似无噪，但这种方法能效比很差。针对无线通信中合法信道噪声不易消除的问题所设计的安全编码，需要既能保证安全又要有一定的纠错能力。文献[4]将陪集编码和纠错码级联，具有较好的纠错能力，但安全性能很差，例如码字中存在某个比特

2013-05-31 收到，2013-10-08 改回
国家自然科学基金(61171108)和国家 863 计划项目(2011AA010604)资助课题
*通信作者：易鸣 ymwlcaq@gmail.com

为奇偶校验，一旦该比特泄露给窃听者，窃听者就获得了一半的信息。为了保证信息传输过程中的强安全性，文献[5]和文献[6]将陪集的概念扩展到格码，研究了合法信道为高斯和瑞利信道下的安全编码，但此类方法在维数较高时实现复杂度非常大。文献[7]以低密度奇偶校验码为基础进行陪集编码，并从降低复杂度的角度进行了深入讨论，但该方法要求合法信道无噪，实用性不强。文献[8–10]以具有良好纠错性能的码为母码，在此基础上不传私密信息或者加入随机冗余来增加私密信息的不确定度，然后利用合法及窃听信道质量差异和母码良好的纠错性能，实现合法信道上私密信息的正确恢复，而窃听信道无法获得私密信息；文献[11]和文献[12]证明了此类编码本质上是属于窃听信道容量可达码，不能保证信息的强安全传输，且安全级别不高。针对多天线系统，文献[13]提出了一种基于信道特征随机投影的物理层安全编码方式，文献[14]提出了一种分布式天线跳空收发技术，它们都是通过增加一个随机变化的预编码矩阵实现合法者正确接收，而窃听者无法收到任何信息，但合法通信双方都需要精确知道每个传输时刻的信道状态信息。文献[15]首先利用合法通信双方的交替反馈和低密度奇偶校验码的纠错能力，使合法信道转化为基本无噪，窃听信道仍然保持较高误比特率，然后利用陪集编码实现安全传输，随着合法信道质量变差，其信息交互量也随之增大。

为了保证编码强安全性的同时提高其在合法信道的抗噪性能，本文在二元域上，针对合法信道为高斯噪声信道，窃听信道为 BEC 信道的 Wiretap 模型，提出一种基于部分陪集的强安全编码方法。为了保证编码方法的强安全性，本文证明了部分陪集强安全编码的充分必要条件：当且仅当陪集母码的对偶码的最小码字距离大于信息泄露位数时，利用部分陪集编码可以保证私密信息的强安全传输。为了提高部分陪集编码的可靠性和有效性，本文在全体陪集集合中尽量多地选取陪集间最小汉明距离尽量大的陪集作为可用陪集进行安全编码，并利用部分陪集间的汉明距离提高码字的抗噪声性能。为解决该问题，首先需要计算两两陪集间的最小汉明距离，本文通过深入分析陪集编码的性质，当陪集母码为 $C(n,n-k)$ 时，将其计算量从 $2^{2(n-k)}n$ 次异或运算降低为 1 次查表运算，同时将陪集编码器的内存需求从 $2^n n$ bit 减少为 $2^k n$ bit；然后将问题等效为搜索无向图的最大完全子图问题，并设计了基于树形深度优先的搜索算法，得到了给定距离冗余下势最大的部分陪集集合。

2　无线物理层安全编码模型与相关定义

总结现有Wiretap模型，无线物理层安全编码的基本模型如图1所示。图1中所示的合法信道和窃听信道均是易受干扰的无线信道。

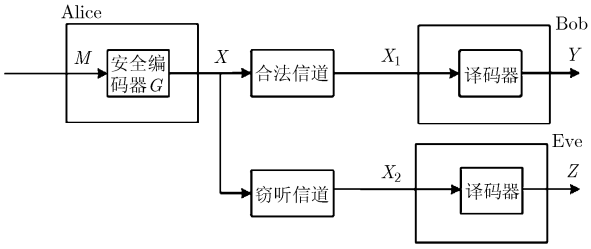


图1 无线物理层安全编码模型

假设发送者Alice通过安全编码器 G 后将 s_m bit 私密信息 M 映射成为 n bit的码字 X，经无线信道传输后分别到达合法接收者Bob和窃听者Eve，接收到的信号分别为 X_1 和 X_2，对接收信号译码得到 Y 和 Z。Alice希望Bob能够克服噪声影响，从 Y 中恢复出 M，同时不希望Eve获得任何私密信息，如式(1)：

$$\left.\begin{array}{ll} P_e^B \le P_{e,\min}^B, & \text{可靠性} \\ \lim\limits_{n\to\infty}\dfrac{1}{n}I(M;Z)=0, & \text{弱安全性} \\ \lim\limits_{n\to\infty}I(M;Z)=0, & \text{强安全性} \end{array}\right\} \tag{1}$$

其中，P_e^B 为Bob译码后的比特错误率，$P_{e,\min}^B$ 为Bob端所允许的最高误比特率；$I(M;Z)$ 为Eve在收到消息Z后对原有私密信息不确定度的减少量，$\lim\limits_{n\to\infty}\dfrac{1}{n}I(M;Z)=0$ 表示Eve从平均意义上无法获得任何关于 M 的信息量，是一种弱安全性；$\lim\limits_{n\to\infty}I(M;Z)=0$ 表示Eve绝对意义上无法获得任何关于 M 的信息量，是一种强安全性[16]。物理层安全编码的本质要求Eve接收到的信息与私密信息统计独立，本文以强安全性为目标，针对合法信道高斯有噪窃听信道为BEC信道的无线Wiretap模型进行研究，以提高安全编码的安全性和实用性。

对系统线性分组码 $C(n,n-k)$，假设其码字长度为 n，其前 $(n-k)$ 位为信息位，生成矩阵为 $\boldsymbol{G}$，码字集合为 $C=\{C^1,C^2,\cdots,C^{2^{n-k}}\}$。以码字集合 C 为基础将二元域上的 n 维空间 $S_c(2^n)$ 划分为 2^k 个互不相交的子空间，其中每一个子空间称为一个陪集，码字集合 C 称为该陪集划分的母码，如果将陪集母码 C 本身也看做一个陪集 CO_1，则共有 2^k 个陪集，详见文献[3]。所有陪集的集合记为 $SC=\{CO_p,p=1,2,\cdots,2^k\}$，第 p 个陪集 CO_p 的第 i 个元素记为

$CO_p^i=[CO_p^{i_1},CO_p^{i_2},\cdots,CO_p^{i_{2^k}}]$, $i=1,2,\cdots,2^k$，其陪集首元素记为CL_p。下面给出文中相关术语的定义。

陪集间最小汉明距离$DO_{p,q}$是陪集CO_p和CO_q所有元素间汉明距离的最小值，记为$DO_{p,q}=\min\limits_{i,j}(\mathrm{Hm}(CO_p^i,CO_q^j))$, $i=1,2,\cdots,2^k$, $j=1,2,\cdots,2^k$。显然，当可用陪集间的最小汉明距离越大时，陪集编码的抗噪声性能越好。

陪集的最小汉明重量是陪集中所有元素的最小汉明重量。

接收矢量与陪集间的距离$d(\boldsymbol{r},CO_p)$是接收矢量$\boldsymbol{r}$与第p个陪集中所有元素间的最小汉明距离，记为$d(\boldsymbol{r},CO_p)=\min\limits_{i}(\mathrm{Hm}(\boldsymbol{r},CO_p^i))$, $i=1,2,\cdots,2^k$。按照最小陪集汉明距离准则译码，记为$\boldsymbol{r}\to CO_i, iff(d(\boldsymbol{r},CO_i)\le d(\boldsymbol{r},CO_j), j\ne i)$，即当且仅当接收到的码字$\boldsymbol{r}$与陪集$CO_i$间的最小陪集汉明距离最小时，将其译为$CO_i$对应的私密信息$s_i$。

记$H(\bullet)$表示熵函数，$|\bullet|$表示集合的势，$+$表示按二进制位异或。

3 基于部分陪集的强安全编码方法

现有的强安全编码方案抗干扰性差，不适用于无线通信系统，而合法信道有噪情形下的物理层安全编码又不能满足信息传输的强安全性要求，为此本文提出了基于部分陪集的强安全编码方法。该方法的基本思想是利用陪集内的随机冗余保证强安全性，利用陪集间的距离冗余保证可靠性，通过寻找给定距离冗余下势最大的可用陪集集合保证编码的有效性。该方法首先根据系统的安全性要求选择合适的陪集母码，得到能够保证强安全性的全体陪集集合，然后计算所有陪集间最小汉明距离，再搜索给定陪集间最小汉明距离下势最大的部分陪集集合，最后利用所得的部分陪集进行编码映射。具体编码步骤如下：

步骤 1 根据系统安全性要求，选择合适母码进行陪集划分。假设系统强安全性所允许的最高信息泄露比例为λ，当且仅当码$C(n,n-k)$的对偶码$C^{\perp}(n,k)$的最小码字距离$d^*>\lambda n+1$时，由步骤4的陪集映射能够保证信息传输的强安全性，本文第3.1节将对该方法的强安全性进行证明；

步骤 2 计算陪集间的最小汉明距离$DO_{p,q}$，获得陪集间的距离矩阵$\boldsymbol{G_Nei}$。由陪集间最小汉明距离的定义，遍历方案首先需要$2^{2(n-k)}n$次异或运算得到任意两元素之间的距离，再在$2^{2(n-k)}$值中寻找最小值，当n,k较大时，计算量将激增。在3.2节将明，CO_p中一定包含一个$\{\underbrace{0,0,\cdots,0}_{n-k},\underbrace{p_1,p_2,\cdots,p_k}_{k}\}$的元证素，令$p$为$\{p_1,p_2,\cdots,p_k\}$的十进制值，则陪集$CO_p$与$CO_q$间的距离是陪集$CO_m$的最小汉明重量，其中$m$为$\{p_1,p_2,\cdots,p_k\}+\{q_1,q_2,\cdots,q_k\}$的十进制值，此时只需要1次查表运算即可；

步骤 3 计算陪集间的最小汉明距离限为d_c^*时势最大的部分陪集集合。如果将每个陪集看作一个节点，该问题等价于求一个无向图的最大完全子图，在本文3.3节设计了一种基于树形深度部分陪集搜索算法；

步骤 4 陪集映射。将每个待传的私密消息M_p映射到一个陪集整体CO_p，编码时随机选择陪集中的任何一个元素$CO_p{}^i$作为实际传送的码字X，当每个陪集中都至少有一个元素与窃听者所得到的码字一致时，窃听者无法区分所接收到的码字属于哪个陪集，即没有获得任何关于私密消息的信息。传统信道编码将k bit信息映射到n bit码字，即从一个包含2^k元素的空间S_m映射到一个包含2^n个元素的空间S_c，但是仅选取了S_c中的部分元素作为可用码字，剩余的2^{n-k}码字作为禁用码字不发挥任何作用。为此，我们在整个S_c空间内重新考虑，将编码的研究对象从传统的码字扩展为“码字云”，即一组码字的集合(陪集)，由于实际传送的码字X是随机选取的，本质上是利用陪集内部的随机冗余保证私密信息的安全传输。

3.1 部分陪集编码的强安全性证明

为了说明部分陪集编码可以保证私密信息的强安全传输，本节给出定理1。

定理 1 当且仅当码$C(n,n-k)$的对偶码$C^{\perp}(n,k)$的最小码字距离$d^*>\lambda n+1$时，由码C生成的陪集进行安全编码时，能够保证窃听端收到任意不多于λn bit时仍然无法获得关于M的任何信息。

证明 令C的生成矩阵$\boldsymbol{G}=[\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_n]$,Eve通过BEC信道后所得码字$\boldsymbol{Z}=[z_1,z_2,\cdots,z_n]$, $z_i\in\{'0','1','?'\}$，其中$\boldsymbol{a}_i$表示生成矩阵的第i列，z_i表示$\boldsymbol{Z}$的第i个bit，'?'表示擦除符号。假设信息泄露位$\{i:z_i='0'\text{或}'1'\}=\{i_1,i_2,\cdots,i_s\}$，即所传递的私密信息$\boldsymbol{M}$中的$\boldsymbol{Z}^s=[z^{i_1},z^{i_2},\cdots,z^{i_s}]$位bit泄露给Eve，信息泄露比例$\lambda=s/n$。因为，当且仅当$C^{\perp}$的最小距离为$d^*$时，$C$的生成矩阵$\boldsymbol{G}$的任意$d^*-1$列线性无关，而有$d^*$列线性相关，并且当且仅当$\boldsymbol{G}$中泄露位相对应列构成的子矩阵$\boldsymbol{G}_s=[\boldsymbol{a}_{i_1},\boldsymbol{a}_{i_2},\cdots,\boldsymbol{a}_{i_s}]$中各列线性无关时，码字集合$C$中第$j$个码字$C_j$的$s$位bit$\boldsymbol{C}_j^s=[c_j^{i_1},c_j^{i_2},\cdots,c_j^{i_s}]$的取值可能性为$2^s$个。

所以，(1)当且仅当生成矩阵中泄露位相对应列构成的子矩阵$\boldsymbol{G}_s=[\boldsymbol{a}_{i_1},\boldsymbol{a}_{i_2},\cdots,\boldsymbol{a}_{i_s}]$中各列线性无关

时，对任意 CO_i，存在 $CO_i^j = CL_i + C_j$ 相应的 s 位 $\boldsymbol{CO}_i^{j,s} = [CO_i^{j,i_1}, CO_i^{j,i_2}, \cdots, CO_i^{j,i_s}] = \boldsymbol{Z}^s$，即每个陪集中都至少存在一个元素去除擦除符号后与 $\boldsymbol{Z}^s$ 一致。(2)当且仅当 $C^{\perp}$ 的最小距离 $d^* > \lambda n + 1$ 时，每个陪集中至少存在一个元素去除擦除符号后与 $\boldsymbol{Z}^s$ 一致，使得式(2)成立：

$$I(\boldsymbol{M};\boldsymbol{Z}) = H(\boldsymbol{Z}) - H(\boldsymbol{M} \mid \boldsymbol{Z}) = \log_2 |SC| - \log_2 |SC| = 0 \tag{2}$$

式(2)成立即满足式(1)所描述的强安全性。定理1是构造强安全性陪集的基础。显然当陪集集合 SC 满足定理1时，从其中选取的部分陪集也能保证信息传输的强安全性。　　证毕

3.2 计算陪集间最小汉明距离方法的可行性证明

陪集间的最小汉明距离决定编码的抗噪声性能。为了得到给定距离冗余下势最大的可用陪集集合，首先需要计算任意陪集间的最小汉明距离。为了减少其计算量，本节给出定理2至定理5。

定理 2　任意陪集中有且仅有一个元素的前 $(n-k)$ bit为0，且该元素的后 k bit为从全0到全1。

证明　因为同一陪集中不同元素的伴随式是相同的，不同陪集的伴随式不同，令 $\boldsymbol{S}_p$ 表示第 p 个陪集的伴随式，它是一个 k 维的向量，取值从全0到全1。假设 C 的校验矩阵经过初等行变换为 $\boldsymbol{H} = [\boldsymbol{P}_{k\times(n-k)} \mid \boldsymbol{I}_{k\times k}]_{k\times n}$，$\boldsymbol{I}_{k\times k}$ 为单位阵。所以，存在 $\boldsymbol{CO}_p^i = \begin{bmatrix} \boldsymbol{0}_{(n-k)\times 1} \\ \boldsymbol{X}_{k\times 1} \end{bmatrix}$，使得式(3)成立：

$$\boldsymbol{H} \times \boldsymbol{CO}_p^i = [\boldsymbol{P}_{k\times(n-k)} \mid \boldsymbol{I}_{k\times k}]_{k\times n} \times \begin{bmatrix} \boldsymbol{0}_{(n-k)\times 1} \\ \boldsymbol{X}_{k\times 1} \end{bmatrix} = \boldsymbol{S}_p \tag{3}$$

因为 $\boldsymbol{S}_p$ 的取值从全0到全1只有 2^k 中可能，且 $\boldsymbol{I}_{k\times k}$ 为单位矩阵，所以，每个陪集中有且只有一个前 $(n-k)$ bit为0的元素，且该元素的后 k bit从全0到全1，即各陪集中有且仅有一个元素是矩阵 $\boldsymbol{A}$ 中的行矢量：

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{CL}_0 \\ \boldsymbol{CL}_1 \\ \vdots \\ \boldsymbol{CL}_{2^k-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{bmatrix} \tag{4}$$

（$0\ 0\ \cdots\ 0$ 为 $n-k$ 列，$1\ 1\ \cdots\ 1$ 为 k 列）

证毕

定理 3　线性陪集安全编码的性能是由码字 C 唯一确定。

证明　由于陪集中的任意元素都可以作为该陪集的首，即矩阵 $\boldsymbol{A}$ 中的行矢量可以作为相应陪集的首元素，则当码字 C 确定后，关于该码字的陪集划分也随之确定，不同陪集首对应的只有陪集内的元素顺序和陪集间次序的不同，不影响陪集间距离的计算，即线性陪集安全编码的性能由码字 C 唯一确定。　　证毕

定理 4　陪集 CO_p, CO_q 间的最小汉明距离等于 CO_p 的任一元素与 CO_q 中所有元素汉明距离的最小值。

证明　假设 $CO_p{}^i = CL_p + C_i$，$CO_q{}^j = CL_q + C_j$，则有式(5)：

$$\begin{aligned} DO_{p,q} &= \min_{i,j}(\mathrm{Hm}(CO_p^i, CO_q^j)) \\ &= \min_{i,j}(CL_p + C_i + CL_q + C_j) \\ &= \min_{j'}(CL_p + CL_q^{j'}) \end{aligned} \tag{5}$$

因为陪集中的任意元素都可以作为陪集首，所以陪集 CO_p, CO_q 间的最小汉明距离等于 CO_p 的任一元素与 CO_q 中所有元素汉明距离的最小值。　证毕

定理 5　任意两个不同陪集间元素的异或一定构成另一陪集。

证明　假设 $CO_p^i = CL_p + C_i$，$CO_q{}^j = CL_q + C_j$，且 $CL_p \neq CL_q$，则有式(6)：

$$CO_p^i + CO_q^j = CL_p + C_i + CL_q + C_j = CO_m + C_{j'} \tag{6}$$

因为陪集中的任意元素都可以作为陪集首，所以，任意两个不同陪集间元素的异或一定构成另一陪集。　　证毕

推论 1　任意两个不同陪集间的最小距离一定是另一个陪集的最小汉明重量。

证明　结合定理4，由陪集间最小距离和陪集最小汉明重量的定义可得。　　证毕

根据定理2和定理3，不妨选取各陪集中前 $(n-k)$ bit为0的元素作为陪集首，并以其对应的十进制值作为相应的陪集序号。安全编码时，只需要将私密信息映射到陪集首，然后动态生成相应的陪集进行随机映射，而不再需要静态存储所有的陪集元素，即将陪集编码器的内存需求从 $2^n n$ bit减少为 $2^k n$ bit。综合定理4和定理5，可得所提部分安全编码方案中步骤2的正确性。

3.3 基于树形深度优先搜索的部分陪集计算算法

将每一个陪集看作一个节点，其距离矩阵为 $\boldsymbol{G\_Nei}$，求势最大的可用陪集集合就是求一个无向图的最大子图。由于一个无向图可能含有多个最大完全子图，为了进一步简化计算复杂度，定理6证明只需要考虑包含码字集合 C 的最大完全子图即可。

定理 6　假设全体陪集的集合 SC 中最多存在 n_p 个陪集组成的部分陪集集合 SC_p，其陪集间的最

小汉明距离不小于 d_c^*，则一定存在包含码字集合 C 的 n_p 个陪集组成的部分陪集集合 SC_p'，其陪集间的最小汉明距离不小于 d_c^*。

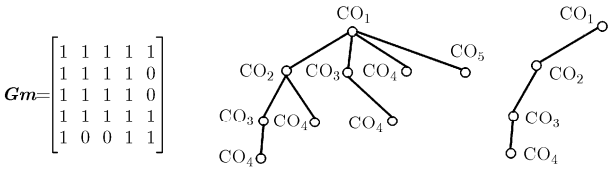
证明 假设 SC_p 中的各陪集不包含 C，且包含某一陪集 C_p，不妨将 SC_p 中各陪集与 C_p 相加，由定理5可知，一定构成一个新的由 n_p 个陪集组成的部分陪集集合 SC_p'，由于每个陪集都是与 C_p 相加，则 SC_p' 中两两陪集间的距离仍然不小于最小距离限 d_c^*，且 SC_p' 中一定存在 C。 证毕

求一个无向图的最大完全子图是图论中的经典问题，相应地有各种确定性或启发式求解算法，为了获得全局最优解，本文提出一种基于树形深度优先的搜索算法。算法步骤见表1。

表1 树形深度优先搜索算法

输入：	图的距离矩阵 $\boldsymbol{G\_Nei}$，陪集间汉明距离下限 d_c^*，初始最大可用陪集集合 MaxPath = Null。
步骤1	将 $\boldsymbol{G\_Nei}$ 转化为布尔矩阵 $\boldsymbol{Gm}$。当 $\boldsymbol{G\_Nei}(p,q) \ge d_c^*$ 时 $\boldsymbol{Gm}(p,q)=1$，称陪集 CO_p 与陪集 CO_q 相互为邻居陪集；否则，$\boldsymbol{Gm}(p,q)=0$。若 $p>q$ 且 $\boldsymbol{Gm}(p,q)=1$，则称陪集 CO_p 是陪集 CO_q 的右邻居，陪集 CO_q 是陪集 CO_p 的左邻居；
步骤2	以母码 C 为根节点，生成邻居关系树(Neighborhood Relation Tree, NRT)。若陪集 CO_p 是陪集 CO_q 及 CO_q 所有父辈陪集共同的右邻居，则称 CO_p 为 CO_q 的孩子陪集，根据此规则生成NRT。在构造NRT的同时，用 Path 记录从根节点 C 到当前节点 CO_p 的路径；如果 CO_p 是叶子节点，则比较 Path 和 MaxPath 的长度，若 Length (Path) > Length(MaxPath)，则更新 MaxPath = Path；
步骤3	NRT构造完毕，获得 MaxPath；
输出：	MaxPath 为最大完全子图，即最大可用陪集集合。

算法示例如图2所示。在图2示布尔矩阵下，构造NRT时，由于陪集 CO_4 是陪集 CO_3 及其所有父辈陪集(CO_1,CO_2)的右邻居，所以 CO_4 可以作为 CO_3 的子陪集，而 CO_5 尽管是 CO_4 的右邻居但不是 CO_4 所有父辈节点的右邻居，所以不能作为 CO_4 的子陪集。最终，将长度最大的 MaxPath 作为势最大的可用陪集集合。



(a)步骤1，生成布尔矩阵 (b)步骤2，生成NRT (c)步骤3，获得势最大的可用陪集集合MaxPath

图2 树形深度优先搜索算法示意图

4 典型结果及性能仿真

根据上述方法，表2给出了典型母码下的最小陪集间汉明距离和抗比特泄露能力，及最小陪集间汉明距离下的最多可用陪集集合。其中 e^* 为允许泄露的最多bit数，其值越大抗窃听信道信息泄露能力越强；d_c^* 为陪集间最小汉明距离，其值越大抗合法信道噪声性能越好；Max_Part_Coset* 为在给定 e^* 和 d_c^* 条件下，势最大的部分陪集集合；$|\bullet|$ 为该部分陪集集合的势，即所包含的陪集数量。

将Wyner安全编码与基于部分陪集编码强安全编码进行仿真对比。以BPSK调制为例，假设合法信道为高斯白噪无线信道，功率谱密度为 N_0，窃听信道为二进制纯擦除无线信道，擦除概率为 ε，待传私密信息量 m 分别为3 bit, 4 bit。以本原BCH

表2 典型母码的部分陪集安全编码性能表

$C^{\perp}(n,k)$	e^* (bit)	d_c^*	Max_Part_Coset*	$\lvert\bullet\rvert$
本原BCH(15,5)	6	2	{0,3,5,6,9,10,12,15,17,18,20,23,24,27,29,30}	16
本原BCH(15,5)	6	3	{1,20}	2
本原BCH(15,5)	6	4	∅	0
本原BCH(15,7)	4	3	{0,19,38,53,76,95,106,121}	8
本原BCH(15,7)	4	4	{ 0,53,95,106}	4
本原BCH(15,7)	4	5	∅	0
本原BCH(15,11)	2	5	{0,95,173,465,760,796,869,930,1254,1335,1384,1434,1579,1618,1685,1999}	16
本原BCH(15,11)	2	6	{0,95,679,826,1209,1477,1652,1738}	8
本原BCH(15,11)	2	7	{0,1335}	2
汉明(15,11)	2	5	{0,79,181,371,632,667,742,908,1257,1309,1411,1534,1558,1834,1893,2000}	16
汉明(15,11)	2	6	{0,125,667,1000,1355,1457,1650,1926}	8
汉明(15,11)	2	7	{0,1894}	2
戈莱码(23,12)	6	5	{0,61}	2

(15,11)的对偶码为部分陪集母码，各陪集中前$(n-k)$ bit为0的元素作为陪集首，其对应的十进制值为相应的陪集序号。假设Bob和Eve均知道编译码方式。对于Wyner安全编码，在所有陪集中选取前2^m个陪集作为可用陪集进行安全编码。对于部分陪集编码传递3 bit私密信息选取的可用陪集集合为：{0,95,679,826,1209,1477,1652,1738}，其陪集间最小汉明距离为5；传递4 bit私密信息选取的可用陪集集合为：{0,79,181,371,632,667,742,908,1257,1309,1411,1534,1558,1834,1893,2000}，其陪集间最小汉明距离为6。仿真结果如图3和图4所示。

从图3可以看出，部分陪集编码方法的抗合法信道噪声性能优于传统的Wyner方法。这是因为传统陪集编码方案下，译码正确时当且仅当所有bit不发生传递错误，或者错成同一陪集内的码字。由于线性分组码任意码字间的汉明距离是另外一个码字的汉明重量，对于$C(n,n-k)$线性分组码，当传送的是全0码字时，其译码错误概率为

$$p_e = 1 - p_c = 1 - \left(\sum_{i=0}^{2^{n-k}-1} p_b^{w(i)} (1-p_b)^{(n-w(i))} \Big/ \binom{n}{w(i)} \right) \quad (7)$$

式中p_e为译码错误概率，p_c是译码正确概率，p_b为bit错误概率，$w(i)$为码集合中第i个元素的汉明重量。以BCH(15,11)码为例，如果使用Wyner编码方案，为了保证合法接收者译码错误概率达到10^{-6}，则要求E_b/N_0约为10 dB。部分陪集编码方案由于陪集间存在汉明距离，使得抗bit传输错误能力更强，信噪比要求更低。仿真结果表明，采用部分陪集编码方法当E_b/N_0高于5 dB时误比特率趋近于0，相对于Wyner方法，对合法信道的信噪比要求降低了5 dB。又因为传递3 bit私密信息所选用的部分陪集间的最小汉明距离大于传递4 bit私密信息所选用的部分陪集间的最小汉明距离，因此传递3 bit私密信息时合法信道误比特率下降速度更快。

由定理1可知，以本原BCH(15,11)码的对偶码为母码的部分陪集编码方法，理论上能够保证Eve获得码字中的任意2 bit信息，即当窃听信道擦除概率高于$(1-2/15)\approx 0.87$时，能够满足式(1)所描述的强安全。图4的仿真结果表明，当擦除概率为0.87，进行部分陪集编码时的误比特率为0.497，接近误比特率为0.5的理论值，即能够保证私密信息的强安全传输。对于擦除概率为ε的窃听信道，不进行安全编码时理论误比特率为$\varepsilon/2$，该值比使用部分陪集编码方案时的误比特率低，这说明本文方法可以提高安全性。部分陪集编码方案和Wyner编码方法都是将每一个陪集对应一个待发送的私密消息。当陪集母码一样时，部分陪集编码方案和Wyner编码方法的抗信息泄露能力相同。然而，由于部分陪集编码选择陪集间汉明距离最大的陪集作为可用陪集，因此部分陪集编码比Wyner编码的抗噪声性能好。另外，由于所选用的部分陪集集合是相应最小陪集汉明距离要求下陪集元素最多的集合，因此其私密信息传输有效性也最高。

5　结束语

本文在深入分析陪集编码性质的基础上，提出了基于部分陪集的强安全编码方案，在保证私密信息强安全传输的同时，提高了其抗噪声性能。研究发现，部分陪集编码的强安全性、可靠性和有效性由陪集母码决定。我们下一步将针对部分陪集编码的强安全性、可靠性及有效性的内在关系进行深入研究。

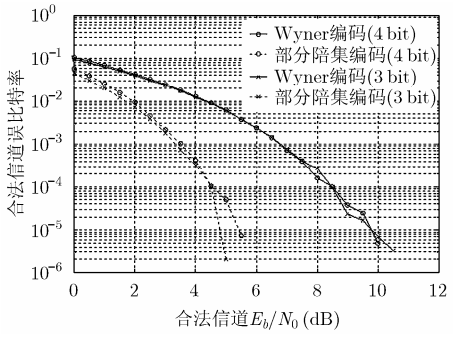


图3 合法信道误比特率随E_b/N_0变化图

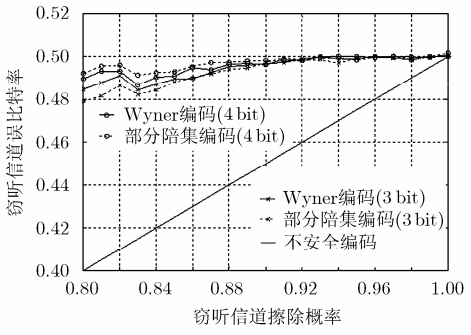


图4 窃听信道误比特率随擦除概率变化图

参 考 文 献

[1] Wyner A D. The wiretap channel[J]. *AT&T Bell Laboratories Technical Journal*, 1975, 54(8): 1355–1387.

[2] Csiszár I and Körner J. Broadcast channels with confidential messages[J]. *IEEE Transactions on Information Theory*, 1978, 24(3): 339–348.

[3] Ozarow L H and Wyner A D. Wire-tap channel Ⅱ[J]. *AT&T Bell Laboratories Technical Journal*, 1984, 63(10): 2135–2137.

[4] Cassuto Y and Bandic Z. Low-complexity wiretap codes with security and error-correction guarantees[C]. Proceedings of IEEE Information Theory Workshop, Dublin, 2010: 1–5.

[5] Belfiore J C and Oggier F. Lattice codes design for the Rayleigh fading wiretap channel[C]. Proceedings of IEEE International Conference on Communications Workshops, Kyoto, 2011: 1–5.

[6] Oggier F, Solé P, and Belfiore J C. Lattice codes for the wiretap Gaussian channel: construction and analysis[C]. Proceedings of International Worshop Coding and Cryptology (IWCC): 3th International Workshop, Qingdao, China, 2011: 47–62.

[7] Thangaraj A, Dihidar S, Calderbank A R, *et al.*. Applications of LDPC codes to the wiretap channel[J]. *IEEE Transactions on Information Theory*, 2007, 53(8): 2933–2945.

[8] Klinc D, Ha J, Mclaughlin S W, *et al.*. LDPC codes for physical layer security[C]. Proceedings of IEEE Global Telecommunications Conference, Honolulu, 2009: 1–6.

[9] Liu R, Poor H V, Spasojevic P, *et al.*. Nested codes for secure transmission[C]. Proceedings of IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, Cannes, 2008: 1–5.

[10] Andersson M. Coding for the wiretap channel[D]. [Ph.D. dissertation], Sweden: School of Electrical Engineering Royal Institute of Technology, 2011.

[11] Bloch M R. Achieving secrecy: capacity vs resolvability[C]. Proceedings of IEEE International Symposium on Information Theory, Saint Petersburg, 2011: 632–636.

[12] Luzzi L. Capacity-based random codes cannot achieve strong secrecy over symmetric wiretap channels[C]. 5th International ICST Conference on Performance Evaluation Methodologies and Tools, Paris, France, 2011: 641–647.

[13] 王亚东, 黄开枝, 吉江. 一种多天线信道特征投影物理层安全编码算法[J]. 电子与信息学报, 2012, 34(7): 1653–1658.
Wang Ya-dong, Huang Kai-zhi, and Ji Jiang. A physical layer secrecy coding algorithm using multi-antenna channel characteristics projection[J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1653–1658.

[14] 殷勤业, 贾曙乔, 左莎琳, 等. 分布式多天线跳空收发技术 I [J]. 西安交通大学学报, 2013, 47(1): 1–8.
Yin Qin-ye, Jia Shu-qiao, Zuo Sha-lin, *et al.*. A distributed multi-antenna space hopping transceiver technique I [J]. *Journal of Xi'an Jiaotong University*, 2013, 47(1): 1–8.

[15] Wen H, Ho P H, and Jiang X H. On achieving unconditional secure communications over binary symmetric channels (BSC)[J]. *IEEE Wireless Communications Letters*, 2012, 1(2): 49–52.

[16] Mahdavifar H and Vardy A. Achieving the secrecy capacity of wiretap channels using polar codes[J]. *IEEE Transactions on Information Theory*, 2011, 57(10): 6428–6443.

易 鸣： 男，1986 年生，博士生，研究方向为物理层安全编码.

季新生： 男，1968 年生，教授，博士生导师，研究方向为信息安全.

黄开枝： 女，1973 年生，副教授，硕士生导师，研究方向为无线通信安全.