基于 DFT-S-OFDM 传输方式的物理层双矩阵密钥加密算法

高宝建 黄士亚 景 利 胡 云

(西北大学信息科学与技术学院 西安 710127)

摘 要 现有基于 OFDM 调制的物理层加密算法的安全性普遍依赖于较大的子载波个数,且不能抵抗明文密文攻击,当子载波个数比较少时,其密钥空间快速变小,安全性急剧下降,因此,很难适应资源受限终端的安全通信需求.针对这一共性问题,文中利用 LTE 上行链路采用的 DFT-S-OFDM 传输方式以及资源块划分方式,提出了一种基于双矩阵变换的物理层加密算法.该算法主要包含两个步骤:一是通过 AES 计数器模式控制产生两个对角密钥矩阵;二是通过密钥矩阵控制 N 点 DFT 变换前后的数据,使得密文、明文和密钥之间形成非线性方程组关系.通过这个加密过程,实现两个目的,一是利用 DFT-S-OFDM 传输方式的特点,实现对输入的明文和输出的密文分别加密的目的,保证算法具备抵抗明文密文攻击能力;二是实现明文、密文和密钥三者之间的非线性关系,保证算法的安全.算法设置了两种密钥工作模式,第一种为每加密 $N-1$ 组明文就改变一次子密钥,第二种为每加密大于等于 N 组明文才改变一次子密钥.在无噪的理想情况和有噪的非理想情况下,详细分析了两种密钥工作模式的安全性.理论分析结果表明,在子载波数大于等于 12 的情况下,第一种密钥工作模式无论在理想条件还是有扰信道条件下,均可以抵抗穷举攻击和明文密文攻击,保证算法的安全性,第二种密钥工作模式只有在有扰信道条件下才可以抵抗穷举攻击和明文密文攻击,保证算法安全;在两种密钥工作模式下,算法均不会改变 DFT-S-OFDM 系统中的峰均功率比.分别仿真分析了加密前后系统的峰均比、误码率等参数的变化,仿真数据证实了理论分析所得的结论,表明算法对系统的峰均比、功率以及误码特性等固有性能影响较小,能够在子载波数比较小的情况下,很好的保证通信数据的安全性,满足资源受限终端的安全通信需求.

关键词 LTE;物理层加密;DFT-S-OFDM;非线性方程组;峰均功率比

中图法分类号 TN918 **DOI 号** 10.11897/SP.J.1016.2018.00368

Physical Layer Double Key Matrix Encryption for DFT-S-OFDM Transmission Mode

GAO Bao-Jian HUANG Shi-Ya JING Li HU Yun

(*Department of Information Science and Technology, Northwest University, Xi'an* 710127)

Abstract The security of the existing physical layer encryption algorithm based on OFDM (Orthogonal Frequency Division Multiplexing) modulation is generally dependent on the large number of subcarriers, and can not resist the plaintext ciphertext attack. When the number of subcarriers is relatively small, the key space becomes smaller and the security is abruptly decreased, so it can not adapt to the secure communication demand of the resource limited terminal. Aiming at solving this common problem, a physical layer encryption algorithm is proposed in this paper based on double matrix transformation using DFT-S-OFDM (Discrete Fourier Transform-Spread-Orthogonal Frequency Division Multiplexing) transmission scheme and resource block partitioning

收稿日期:2016-06-23;在线出版日期:2017-06-30.本课题得到国家自然科学基金(61501372)和陕西省自然科学基金(2017JM6012)资助.**高宝建**,男,1963 年生,副教授,主要研究方向为物理层安全、通信信号处理.E-mail:esu7031@sina.com.**黄士亚**(通信作者),男,1990 年生,硕士,主要研究方向为物理层安全.E-mail:452241899@qq.com.**景 利**,女,1991 年生,硕士,主要研究方向为物理层安全.**胡 云**,女,1990 年生,硕士,主要研究方向为物理层安全.

method adopted by LTE(Long Term Evolution) uplink. The algorithm mainly consists of two steps: one is to generate two diagonal key matrices by AES(Advanced Encryption Standard) counter mode; the other is to control the data before and after the N-point DFT(Discrete Fourier Transform) transform by the key matrix, so that the ciphertext, plaintext and key are formed Nonlinear equations. Through the encryption process, we can achieve two purposes that one is using the features of DFT-S-OFDM transmission mode to achieve that the input of the plaintext and output ciphertext were encrypted to ensure that the algorithm has resistance to clear plaintext ciphertext attack; the other is to achieve the three non-linear relationship among the plaintext, ciphertext and the key to ensure the security of the algorithm. The algorithm sets two operation modes of the key. The first one is to change the sub-key once for each encrypted $N-1$ group, and the second one is to change the sub-key for each encryption greater than or equal to the N group. In the case of non-noise ideal situation and noisy non-ideal situation, the security of the two key modes of operation is analyzed in detail. The results of theoretical analysis show that under the condition of the number of subcarriers is greater than or equal to 12, the first kind of key operation mode can resist the exhaustive attack and the plaintext ciphertext attack both in the ideal and the disturbed channel condition to ensure the security of the algorithm, the second kind of key operation mode can only resist the exhaustive attack and the plaintext ciphertext attack under the condition of disturbing channel to ensure the security of the algorithm. In both key operation modes proposed in the paper, the algorithm does not change the PAPR(Peak-to-Average Power Ratio) in DFT-S-OFDM systems. The changes of the parameters such as peak to average ratio and bit error rate are analyzed in simulation, the simulation data confirm the conclusions of the theoretical analysis. It is shown that the algorithm has little influence on the inherent performance of the system, such as PAPR, power and error characteristics, and can ensure the security of communication data and satisfy to meet the safe communication demand of resource-limited terminal in the case of small number of subcarriers.

Keywords　Long Term Evolution(LTE); physical layer encryption; discrete Fourier transform-spread-orthogonal frequency division multiplexing; nonlinear equations group; peak to average power ratio

1　引　言

LTE(Long Term Evolution)技术已经在移动通信等领域得到了广泛应用,其上行链路采用离散傅里叶变换扩展正交频分复用(DFT-S-OFDM)技术,通过资源块划分和调度实现带宽资源的分配,每个资源块包括 12 个子载波,系统带宽的不同决定了资源块(Resource Block)的个数不同,在最小带宽 1.4MHz 情况下,资源块个数为 6 个,子载波总个数为 72 个,在其它带宽情况下,资源块和子载波总个数更多[1].

DFT-S-OFDM 技术原理如图 1 所示[1],该技术与 OFDM 技术的主要区别是对 OFDM 系统的输入数据进行了基于傅里叶变换的预编码.这种改进可以使 OFDM 系统的峰均比(PAPR)降低 3 dB,在相同误码率的条件下,其发射能量降低 1 dB[2].其 NLT(Non-Linear Tolerance)性能也优于原始的 OFDM 系统[3].从以上几点容易看出,DFT-S-OFDM 技术不仅保持了 OFDM 系统的原有优点,又具备了低峰均功率比和低发射功率的特点,并且对于系统的非线性失真具有更高的容忍度,这些优点使其可以有效降低终端设备的成本和实现复杂度,不仅可以满足移动通信上行链路的通信需求,也可以广泛应用在终端能源、成本和实现复杂度受限的各种宽带无线通信系统.

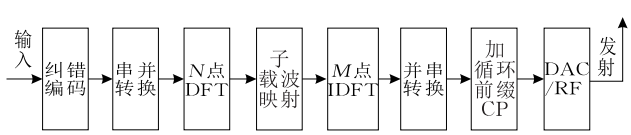


图 1　DFT-S-OFDM 系统发送端框图

随着无线通信系统的宽带化、融合化、智能化以及广泛应用,其面临的窃听、非法基站等恶意攻击情

况越来越严重,传统的基于链路层的数据加密算法受到了越来越严重的挑战.首先,传统安全算法为了保证算法安全性,一般都具有很高的计算复杂度,随着无线通信系统的宽带化,信息传输速率将高达每秒几百兆比特,使其应用和实现非常困难[4],如果直接将其在 DFT-S-OFDM 系统上使用,必然会较大幅度地增加终端设备的成本、功耗及实现复杂度,破坏该系统原本的优点;其次,链路层的加密算法只能保护数据,无法对无线通信过程中的信令控制和标志信息实现有效保护[5],从而难以防止非法基站等的攻击.

物理层加密可以在一定程度上弥补链路层加密存在的问题.首先物理层加密是对符号进行运算,在保证安全性的同时可以降低加密算法的复杂度,例如文献[4]的物理层加密算法有效降低了加密复杂度;其次,物理层加密不仅可以保护数据,而且可以保护信息的交互过程;最后,从通信系统的角度看,物理层加密处于信道编码之后,非法用户通过无线信道获取的密文都带有噪声,该噪声在解密前无法消除,也就是说,物理层加密可以利用信道噪声,提高算法安全性.

基于以上原因,本文提出了一种基于 LTE 上行链路 DFT-S-OFDM 传输方式和资源块划分方式的物理层双矩阵加密方法.该方法充分利用 DFT-S-OFDM 传输方式的物理层调制过程,在不影响安全性、不影响系统固有性能的同时,降低了加密算法的实现复杂度,实现了对无线数据链路的有效保护.

2 相关工作

物理层加密相对于链路层加密具有比较明显的优点.近年来,物理层安全算法的研究越来越受到人们的重视,研究人员已提出了一些典型物理层加密算法.

文献[4]通过对 IFFT 变换后的 OFDM 符号的实部和虚部分别进行流密码加密,设计了一种物理层安全算法,在保证安全性的同时,降低了算法实现复杂度;文献[5-6]通过引入混沌序列设计物理层加密方案,并将其成功应用于 OFDM-PON 系统,取得了良好的实验结果;文献[7-8]通过在 OFDM 的 IFFT 之前添加一个干扰矩阵,扰码矩阵通过对 OFDM 符号的原始位置进行打乱,实现对信号的加密;文献[9-10]通过 AES(Advanced Encryption Standard)产生的密钥来控制星座映射后符号的旋转角度,并将噪声插入处理后的符号来实现对数据的加密;文献[11]将用于预处理的酉矩阵作为密钥实现物理层加密,在保证 OFDM 通信系统安全的同时降低系统的 PAPR;文献[12]通过密钥控制产生一个与正常 OFDM 同带宽的干扰噪声信号,将其与正常 OFDM 信号相叠加,实现对正常信号的隐藏,从而保证了数据的安全传送.

通过对这些算法进行分析,可以看出主要存在两个方面的问题:(1)所有算法都是针对 OFDM 体制提出的,并且算法的密钥长度通常与子载波数成正比,但 DFT-S-OFDM 系统的有效子载波数比较小,当子载波数为 12 时,这些算法的密钥空间都会大幅度下降;(2)大部分算法抵抗明文密文对攻击能力比较弱或者不能抵抗,例如文献[4]只能有条件抵抗,而文献[13]则完全不能抵抗.

基于以上两个方面的问题,本文设计了一种基于 DFT-S-OFDM 的双矩阵加密算法.算法在主密钥控制下生成一组二进制的密钥序列,在其控制下产生两个复对角密钥矩阵,在 N 点 DFT 变换的前后分别乘以这两个矩阵,实现对数据的加密.通过这种设计,希望在子载波数比较小的情况下保证算法的安全性,提高算法抵抗明文密文攻击的能力,降低算法的实现复杂度,并尽可能降低算法对原系统固有性能的影响.理论分析和仿真实验均证明算法达到了设计目的.

3 加密算法模型

DFT-S-OFDM 系统的组成框图如图 2 所示.由图可见,系统中包含了一个 N 点 DFT 变换,和一个 M 点 IDFT 变换,且 $M>N$.为了降低算法的复杂度,算法围绕 N 点 DFT 变换进行加密工作.算法主要包含两个步骤:一是产生对角密钥矩阵;二是通过密钥矩阵控制 N 点 DFT 变换前后的数据,实现对物理层数据符号的加密.具体加解密算法模型如图 2 所示.

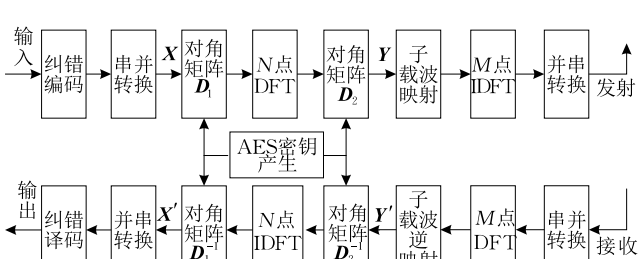


图 2 加密算法模型

3.1　对角密钥矩阵产生方法

首先采用文献[10]提出的基于 AES 算法的加密序列产生方法产生一串二进制数. 选定长度为 128 bit 的密钥 e，在计数器模式下产生 $N(L_1+L_2)$ 比特二进制数，如果计数器工作一次产生 128 bit，则计数器只要计数 $\left\lceil \frac{N(L_1+L_2)}{128} \right\rceil$ 次，就可以完成子密钥的产生过程.

假设在主密钥 e 控制下，产生的子密钥为 a_i，$i=0,1,\cdots,N(L_1+L_2)-1$. 将 a_i 中的 0、1 依次以 L_1 位为一组，转换为由 $0,1,\cdots,2^{L_1}-1$ 组成的序列 $d_1(n)$，$n=1,2,\cdots,N$，然后通过式(1)生成对角密钥矩阵 $\boldsymbol{D}_1$.

$$\boldsymbol{D}_1(m,n)=\begin{cases}\exp(j2\pi d_1(n)/2^{L_1}), & m=n\\ 0, & m\neq n\end{cases} \tag{1}$$

将 a_i 中剩余的 0、1 序列依次以 L_2 位为一组，转换为由 $0,1,\cdots,2^{L_2}-1$ 组成的序列 $d_2(n)$，$n=1,2,\cdots,N$，然后通过式(2)生成对角密钥矩阵 $\boldsymbol{D}_2$. 其中，N 为系统的子载波个数，L_1 和 L_2 作为密钥.

$$\boldsymbol{D}_2(m,n)=\begin{cases}\exp(j2\pi d_2(n)/2^{L_2}), & m=n\\ 0, & m\neq n\end{cases} \tag{2}$$

3.2　加解密过程

加密过程就是对输入信息 C 经过串并转换和星座映射后的明文复数向量 $\boldsymbol{X}$ 先乘以对角密钥矩阵 $\boldsymbol{D}_1$，然后做 N 点 DFT 变换，对变换后的向量再乘以对角矩阵 $\boldsymbol{D}_2$，完成加密过程，得到密文向量 $\boldsymbol{Y}$ 为

$$\boldsymbol{Y}=\boldsymbol{X}\cdot\boldsymbol{D}_1\cdot\boldsymbol{T}\cdot\boldsymbol{D}_2 \tag{3}$$

其中，明文 $\boldsymbol{X}=(x_1,x_2,\cdots,x_N)$，密文 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_N)$，$\boldsymbol{T}$ 为 DFT 变换矩阵，该矩阵为对称矩阵.

在解密时，合法接收者首先通过主密钥 e、L_1 和 L_2 计算出 $\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$ 的逆矩阵 $\boldsymbol{D}_1^{-1}$ 和 $\boldsymbol{D}_2^{-1}$，然后进行逆运算，获得明文.

$$\boldsymbol{X}'=\boldsymbol{Y}'\cdot\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\cdot\boldsymbol{D}_1^{-1} \tag{4}$$

其中 $\boldsymbol{X}'$ 为已经恢复的明文，$\boldsymbol{Y}'$ 为接收到的密文，$\boldsymbol{T}^{-1}$ 为 N 点 IDFT 变换矩阵.

通过以上加解密过程，我们可以实现两个目的：一是利用 DFT-S-OFDM 传输方式的特点，实现对输入的明文和输出的密文分别加密，保证算法具备抵抗明文密文攻击能力；二是实现明文、密文和密钥三者之间的非线性关系，保证算法的安全性.

3.3　密钥工作模式

为了保证密钥安全性的同时，减小密钥交换开销，这里的主密钥 e 固定不变. 通过约定计数器的工作模式，可以改变子密钥，改变前和改变后的子密钥之间相互独立[10]. 具体改变模式包括如下两种：

(1) 每加密 $N-1$ 组明文就改变一次子密钥，保证一组加密矩阵 $\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$ 的使用时间不超过 $N-1$ 组明文. 这种模式的计算开销相对较大.

(2) 每加密大于等于 N 组明文才改变一次子密钥. 这种模式计算开销相对较小.

下面我们将依据这两种密钥工作模式，分别分析加密算法的安全性.

4　理想情况下算法安全性分析

对攻击者来说，不考虑信道噪声的影响，属于理想情况.

综合分析由式(1)～(4)所示的算法原理和加密过程，我们可以考虑到的对算法的攻击方法主要有 3 种：

(1) 攻击者通过穷举法获取密钥.

(2) 攻击者通过明文密文攻击获取算法的密钥.

(3) 攻击者通过明文密文攻击获取算法的解密矩阵.

依据上面给定的两种密钥工作模式，我们主要围绕算法对这 3 种攻击方法的抵抗能力展开详细的分析.

4.1　密钥空间分析

由算法密钥产生过程容易看出，两种密钥工作模式具有相同的密钥空间.

本文算法的主密钥为 128 bit，其密钥空间为 2^{128}. 由主密钥到子密钥产生过程的安全性由 AES 加密算法的安全性来保证. 由于产生两个密钥矩阵需要的二进制比特数为 $(L_1+L_2)N$，所以两个密钥矩阵可能的组合共有 $2^{(L_1+L_2)N}$ 种. 因此，当子载波数 N 较小时，可以通过调节映射参数 L_1+L_2 来改变密钥矩阵空间的大小，当 $N=12$，$L_1+L_2=16$ 时，加密矩阵的可能组合将达到 2^{192} 个；而当 $N=72$，$L_1+L_2=4$，加密矩阵的可能组合将达到 2^{288} 个. 以上分析表明，在上述两种密钥工作模式下，本文算法无论是针对单个 RB 的 12 个子载波数进行加密，还是在特定的 LTE 系统带宽下的所有子载波数进行加密，都具有很大的密钥空间和较好的适应性.

4.2　第一种密钥工作模式下算法安全性分析

在这种密钥工作模式下，攻击者每次获取相同

子密钥控制的明文密文对不会超过 $N-1$ 对.

4.2.1 密钥安全性分析

(1)已知 $m\leq N-1$ 组明文密文对时的等效非线性方程组

假设 $\boldsymbol{D}_1=\mathrm{diag}(b_1,b_2,\cdots,b_N)$,$\boldsymbol{D}_2=\mathrm{diag}(b'_1,b'_2,\cdots,b'_N)$,$\boldsymbol{T}=[t_{ij}]$,$i,j=1,2,\cdots,N$,明文密文对为$[\boldsymbol{X}_m,\boldsymbol{Y}_m]$,$\boldsymbol{X}_m=(x_{1m},x_{2m},\cdots,x_{Nm})$,$\boldsymbol{Y}_m=(y_{1m},y_{2m},\cdots,y_{Nm})$,$m=1,2,3,\cdots,N-1$. 当已知 m 组明文密文对时,则由式(3)所示的算法加密过程容易得到以密钥 b_i 和 b'_j 为变量的非线性方程组如式(5)所示,其矩阵表示如式(6)所示;将式(5)中的变量 $b_ib'_j$ 看作一个整体用 u_{ij} 表示,可得方程组如式(7)所示.

$$\begin{cases}b_1b'_1x_{11}t_{11}+b_1b'_2x_{21}t_{21}+\cdots+b_1b'_Nx_{N1}t_{N1}=y_{11}\\ b_2b'_1x_{11}t_{12}+b_2b'_2x_{21}t_{22}+\cdots+b_2b'_Nx_{N1}t_{N2}=y_{21}\\ \ddots\\ b_Nb'_1x_{11}t_{1N}+b_Nb'_2x_{21}t_{2N}+\cdots+b_Nb'_Nx_{N1}t_{NN}=y_{N1}\\ \ddots\\ b_1b'_1x_{1m}t_{11}+b_1b'_2x_{2m}t_{21}+\cdots+b_1b'_Nx_{Nm}t_{N1}=y_{1m}\\ b_2b'_1x_{1m}t_{12}+b_2b'_2x_{2m}t_{22}+\cdots+b_2b'_Nx_{Nm}t_{N2}=y_{2m}\\ \ddots\\ b_Nb'_1x_{1m}t_{1N}+b_Nb'_2x_{2m}t_{2N}+\cdots+b_Nb'_Nx_{Nm}t_{NN}=y_{Nm}\end{cases}\tag{5}$$

$$\begin{cases}\boldsymbol{D}_2\cdot\boldsymbol{T}\cdot\boldsymbol{D}_1\cdot\boldsymbol{X}_1^{\mathrm{T}}=\boldsymbol{Y}_1^{\mathrm{T}}\\ \boldsymbol{D}_2\cdot\boldsymbol{T}\cdot\boldsymbol{D}_1\cdot\boldsymbol{X}_2^{\mathrm{T}}=\boldsymbol{Y}_2^{\mathrm{T}}\\ \ddots\\ \boldsymbol{D}_2\cdot\boldsymbol{T}\cdot\boldsymbol{D}_1\cdot\boldsymbol{X}_m^{\mathrm{T}}=\boldsymbol{Y}_m^{\mathrm{T}}\end{cases}\tag{6}$$

$$\begin{cases}u_{11}x_{11}t_{11}+u_{12}x_{21}t_{21}+\cdots+u_{1N}x_{N1}t_{N1}=y_{11}\\ u_{21}x_{11}t_{12}+u_{22}x_{21}t_{22}+\cdots+u_{2N}x_{N1}t_{N2}=y_{21}\\ \ddots\\ u_{N1}x_{11}t_{1N}+u_{N2}x_{21}t_{2N}+\cdots+u_{NN}x_{N1}t_{NN}=y_{N1}\\ \ddots\\ u_{11}x_{1m}t_{11}+u_{12}x_{2m}t_{21}+\cdots+u_{1N}x_{Nm}t_{N1}=y_{1m}\\ u_{21}x_{1m}t_{12}+u_{22}x_{2m}t_{22}+\cdots+u_{2N}x_{Nm}t_{N2}=y_{2m}\\ \ddots\\ u_{N1}x_{1m}t_{1N}+u_{N2}x_{2m}t_{2N}+\cdots+u_{NN}x_{Nm}t_{NN}=y_{Nm}\end{cases}\tag{7}$$

容易看出,方程组(7)为线性欠定方程组,容易求出其无穷多个解. 假设其解为$(z_1^k,z_2^k,\cdots,z_{N\times N}^k)$,$k=1,2,\cdots$,则可得如式(8)所示的以密钥 b_i 和 b'_j 为变量的非线性方程组,式(9)为该非线性方程组的矩阵表示.

$$\begin{cases}b_1b'_1=z_1^k\\ \ddots\\ b_1b'_N=z_N^k\\ b_2b'_1=z_{N+1}^k\\ \ddots\\ b_Nb'_N=z_{N\times N}^k\end{cases},\ k=1,2,\cdots\tag{8}$$

$$\begin{bmatrix}b_1 & & & & & & \\ & \cdots & & & & & \\ & & b_1 & & & & \\ & & & \cdots & & & \\ & & & & b_N & & \\ & & & & & \cdots & \\ & & & & & & b_N\end{bmatrix}\begin{bmatrix}b'_1 & & & & & & \\ & \cdots & & & & & \\ & & b'_N & & & & \\ & & & \cdots & & & \\ & & & & b'_1 & & \\ & & & & & \cdots & \\ & & & & & & b'_N\end{bmatrix}=\begin{bmatrix}z_1^k\\ z_2^k\\ \cdots\\ z_{N\times N}^k\end{bmatrix}\tag{9}$$

当攻击者知道 $m\leq N-1$ 组明文密文对时,密钥 b_i 和 b'_j、明文和密文三者之间将满足如式(5)和式(8)所示非线性方程组. 要获取算法的密钥,就必须求解该非线性方程组,这样算法抵抗明文密文对攻击的问题就转换为非线性方程组求解问题.

(2)等效非线性方程组解的分布

定理 1. 假设 $\boldsymbol{T}=[t_{ij}]$,$i,j=1,2,\cdots,N$ 为满秩矩阵,$\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$ 为对角矩阵,则对任意的 $m\leq N-1$,方程(5)和其等效方程(8)均有无穷多个解.

证明. 假设 v_i 和 v'_i 为方程(5)和(8)任意一组解,对于任意的非零实数 β 和任意的弧度 θ,将 $\beta v_i\mathrm{e}^{j\theta}$ 和 $\frac{1}{\beta}v'_i\mathrm{e}^{-j\theta}$ 分别代入其矩阵表示式(6)和(9),由于矩阵方程的特殊结构,容易验证,式(6)和(9)一定成立,$i=1,2,\cdots,N$. 由此证明方程(5)和(8)如果在复平面上有一组解,则其在复平面必然有无穷多个解. 证毕.

以上分析说明,在没有信道噪声的理想情况下,当攻击者得到明文密文对 $m\leq N-1$,其获取算法密钥的最佳途径都绕不开式(5)和式(8)所示的非线性方程组的求解问题,而式(5)方程具有无穷多个解,式(8)的方程组有无穷多个,且每个都有无穷多个解.

(3)式(5)和(8)所示非线性方程组求解复杂度

目前典型的非线性方程组的解法主要包括牛顿迭代法、同伦法和吴消元法. 由上分析可知,以密钥 b_i 和 b'_j 为变量的式(5)和式(8)所示的非线性方程组都具有无穷多个解,求解该方程组,不仅要解决求解问题,同时还要解决解的甄别问题. 下面我们重点分析采用这 3 种方法求解式(5)和(8)所示的非线性方程组解的关键步骤的计算复杂度,并结合多解甄别

计算复杂度，综合给出攻击者通过明文密文攻击获取密钥的计算复杂度.

虽然牛顿迭代法的收敛速度比较快，但其成功求解的关键是初值估计的准确性[14]. 在本文算法模型中，式(5)、(8)所示的非线性方程组真正的解是由128 bit 密钥控制产生，其可能的选择等于密钥矩阵的个数，即 $2^{(L_1+L_2)N}$. 同时定理 1 的结论说明该方程组有无穷多个解，所以即使其准确选择了初值，得到的解也有很大的概率是错的. 所以正确选择初值的计算复杂度最低为 $O(2^{(L_1+L_2)N})$，当不考虑牛顿迭代法的其它计算过程，取 $N=12, L_1+L_2=16$ 时，仅正确选取初值的最低计算复杂度就高达 $O(2^{192})$. 因此通过牛顿迭代法求解上述非线性方程组来得到密钥是非常困难的.

同伦法指的是同伦延拓法，或称连续同伦法[15]. 同伦方法就是跟踪不同的同伦路径从而得到目标问题的解. 同伦法所得多项式方程组孤立解个数的上限是 Bezout 数，即对于 V 个变量的方程组，其得到的可能的孤立解的个数最大有 V^V 个. 在本文算法模型中，当式(5)所示的非线性方程组的变量取 $V=24$ 时(即 $N=12$)，其孤立解的个数最大为 $24^{24}\approx 2^{110}$，而其中正确的解只有一个，由于本文算法密钥选取没有任何物理背景且是伪随机的，所以在对解的选取上不存在任何参考，从而保证正确选取路径和得到正确解的计算复杂度在 $N=12$ 时即可达到 $O(2^{110})$. 因此通过同伦法求解上述非线性方程组来得到密钥是非常困难的.

吴方法是一种具有全局收敛性的方法，也是求得多项式方程组全部解的有效计算方法之一[16-17]. 但是该方法的计算复杂度高，仅仅在吴方法的伪除法运算中，对于含有 n 个变元的多项式方程组，计算复杂度高达 $O((n-1)!)$，如果应用于本文中的 $N=12$，其计算复杂度将达到 $O(23!)\approx O(2^{75})$. 因此通过吴方法求解上述非线性方程组得到密钥也是非常困难的.

综上分析，在不考虑多解甄别复杂度的情况下，我们可得，在取 $N=12, L_1+L_2=16$ 时，攻击者为获取密钥，求解(5)和(8)所示非线性方程组的最低计算复杂度如表 1 所示.

表 1　明文密文攻击获取密钥的计算复杂度

方法	求解复杂度
牛顿迭代法	$O(2^{192})$
同伦法	$O(2^{110})$
吴消元法	$O(2^{75})$

如果考虑多解甄别，当攻击者获取 $m\leq N-1$ 组明文密文对，它将得到如式(5)所示的方程组，或者如式(8)所示的无穷多个方程组，这里每个方程组都有无穷多个解，而真正的密钥只是其中的一个解，所以从概率的角度看，攻击者通过解方程获取真正密钥的概率为无穷小.

综上(1)、(2)和(3)部分的分析，我们可以得到结论：第一种密钥工作模式可以保证密钥安全.

4.2.2　算法安全性分析

如果将加密矩阵看成一个整体，用 $\boldsymbol{D}=\boldsymbol{D}_1\cdot\boldsymbol{T}\cdot\boldsymbol{D}_2$ 表示，则其解密矩阵可写为 $\boldsymbol{D}^{-1}=\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\cdot\boldsymbol{D}_1^{-1}$，这样式(3)、(4)所示的加解密过程可以等效为 $\boldsymbol{Y}=\boldsymbol{X}\cdot\boldsymbol{D}, \boldsymbol{X}'=\boldsymbol{Y}'\cdot\boldsymbol{D}^{-1}$. 容易看出，攻击者不用获取密钥，只要获取算法的解密矩阵 $\boldsymbol{D}^{-1}=\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\cdot\boldsymbol{D}_1^{-1}$，同样可以实现对密文的解密.

在第一种密钥工作模式下，攻击者要获取算法解密密钥，只能通过式(6)所示方程组来完成. 将式(6)所示方程组写成如下矩阵形式，其中 $\boldsymbol{A}_{m\times N}$ 表示明文矩阵，$\boldsymbol{B}_{m\times N}$ 表示密文矩阵.

$$\boldsymbol{D}_2\cdot\boldsymbol{T}\cdot\boldsymbol{D}_1\cdot[\boldsymbol{X}_1^{\mathrm{T}},\cdots,\boldsymbol{X}_m^{\mathrm{T}}]=[\boldsymbol{Y}_1^{\mathrm{T}},\cdots,\boldsymbol{Y}_m^{\mathrm{T}}],$$
$$\boldsymbol{A}_{m\times N}\cdot\boldsymbol{D}_{N\times N}=\boldsymbol{B}_{m\times N} \tag{10}$$

由于 $m\leq N-1$，所以密文矩阵 $\boldsymbol{B}_{m\times N}$ 总是秩不等于 N 的非满秩矩阵，其逆矩阵不存在，所以攻击者很难通过式(10)矩阵方程求得解密矩阵 $\boldsymbol{D}^{-1}$.

以上分析表明，第一种密钥工作模式也能保证算法安全.

4.3　第二种密钥工作模式下算法安全性分析

在这种密钥工作模式下，攻击者每次获取相同子密钥控制的明文密文对 $m\geq N$.

4.3.1　密钥安全性分析

在这种密钥工作模式下，尤其是当 $m=N$ 时，方程(7)将变成一个有 $N\times N$ 个变量，$N\times N$ 个方程的确定性线性方程组，攻击者可以方便求得这个线性方程组的唯一解如下式所示：

$$\begin{cases} b_1 b_1' = z_1^1 \\ \quad\ddots \\ b_1 b_N' = z_N^1 \\ b_2 b_1' = z_{N+1}^1 \\ \quad\ddots \\ b_N b_N' = z_{N\times N}^1 \end{cases} \tag{11}$$

虽然这个方程组是密钥 b_i 和 b_j' 的非线性方程组，具有无穷多个解，但是不同于第一种密钥工作模

式中式(8)方程组有无穷多个,这时只有唯一的一个方程组式(11).

这种情况下攻击者不用求解式(11)所示的方程组,而可以通过猜测的方法获取密钥.如方程(11)所示,当攻击者猜测到了 b_i 中任意一个,例如 b_1,就可以由方程(11)方便的得到所有 b'_j,进而得到其余的 b_i,这样攻击者就可以得到所有密钥.容易计算,$L_1=L_2=8$ 时,其猜对 b_1 的概率为 $\frac{1}{2^8}$;$L_1=L_2=4$ 时,其猜对 b_1 的概率为 $\frac{1}{2^4}$,而且此时和子载波数无关.

由此可见,在不考虑信道噪声的理想情况下,第二种密钥工作模式不能保证密钥安全.

4.3.2 算法安全性分析

在这种密钥工作模式下,尤其是当 $m=N$ 时,式(10)矩阵方程将变为

$$\boldsymbol{A}_{N\times N}\cdot\boldsymbol{D}_{N\times N}=\boldsymbol{B}_{N\times N} \tag{12}$$

这时,$\boldsymbol{B}_{N\times N}$ 矩阵将变成方阵,其逆矩阵有可能存在,当其逆矩阵存在时,攻击者很容易求解式(12)所示的矩阵方程,得到解密矩阵 $\boldsymbol{D}^{-1}$.

$$\boldsymbol{D}^{-1}=\boldsymbol{B}^{-1}_{N\times N}\cdot\boldsymbol{A}_{N\times N} \tag{13}$$

由此可见,在不考虑信道噪声的理想情况下,第二种密钥工作模式不能保证算法安全.

4.4 举 例

不失一般性,为了简化运算,选取 $L_1=L_2=2$,$N=3$,选取 $(b_1,b_2,b_3)=(a,b,c)=(1,j,-1)$,选取 $(b'_1,b'_2,b'_3)=(e,d,f)=(-1,1,j)$ 作为密钥,选取满秩对称矩阵 $\begin{pmatrix}1&1&-1\\1&-1&1\\-1&1&1\end{pmatrix}$ 代替 DFT 矩阵 $\boldsymbol{T}$.

依据这些参数,得到 3 组明文密文对如下:

$(X_1;Y_1)=(1,j,-1;2j-1,2-j,-1)$,

$(X_2;Y_2)=(-1,j,-j;j,2j+1,-j)$,

$(X_3;Y_3)=(1,-j,-1;-1,-j,2j-1)$.

将前两组明文密文对代入方程组(5)可得式(14)所示方程组;将三组明文密文对全部代入方程组(5),可以得到式(15)所示的方程组.

如果将 ae、ad、af、be 等变量乘积看作一个未知量,那么式(14)就可以等效为一个 6 个方程,9 个未知量的线性欠定方程组,该方程组一定有无穷多个解,难以从中猜测出密钥.

式(15)可以等效为一个 9 个方程,9 个未知量的线性确定方程组,对其进行求解,可得到唯一解如式(16)所示.

$$\begin{cases}ae+adj+af=2j-1\\be-bdj-bf=2-j\\-ce+cdj-cf=-1\\-ae+adj+afj=j\\-be-bdj-bfj=2j+1\\ce+cdj-cfj=-j\end{cases} \tag{14}$$

$$\begin{cases}ae+adj+af=2j-1\\be-bdj-bf=2-j\\-ce+cdj-cf=-1\\-ae+adj+afj=j\\-be-bdj-bfj=2j+1\\ce+cdj-cfj=-j\\ae-adj+af=-1\\be+bdj-bf=-j\\-ce-cdj-cf=2j-1\end{cases} \tag{15}$$

$$\begin{cases}ae=-1,be=-j,ce=1\\ad=1,\quad bd=j,\quad cd=-1\\af=j,\quad bf=-1,cf=-j\end{cases} \tag{16}$$

容易验证,当攻击者猜出 $a=1$,则由式(16)很容易就可以算出其它正确的密钥 $b=j$,$c=-1$,$d=1$,$e=-1$,$f=j$.由于 a 只有 ±1 和 $\pm j$ 这 4 种选择,所以很容易猜对.

同样式(14)和(15)都可以写成矩阵形式.容易看出通过式(17)无法获取 $\boldsymbol{D}^{-1}_{3\times3}$,而通过(18)可以获取.

$$\begin{bmatrix}1&j&-1\\-1&-j&-1\end{bmatrix}\cdot\boldsymbol{D}_{3\times3}=\begin{bmatrix}2j-1&2-j&-1\\j&2j+1&-j\end{bmatrix} \tag{17}$$

$$\begin{bmatrix}1&j&-1\\-1&-j&-1\\1&-j&-1\end{bmatrix}\cdot\boldsymbol{D}_{3\times3}=\begin{bmatrix}2j-1&2-j&-1\\j&2j+1&-j-1\\-1&-j&2j-1\end{bmatrix} \tag{18}$$

5 信道噪声对算法安全性影响分析

对于传统的链路层加密,非法用户通过无线信道截获受到噪声干扰的密文信息,然后通过解调和信道译码,可以去除噪声,恢复没有噪声干扰的密文.对于物理层加密,非法用户同样可以通过无线信道截获受到噪声干扰的密文信息,不同的是,这时他无法去除密文上的噪声.

由前面的分析可知,在理想无噪声情况下,第一种密钥工作模式能保证密钥和算法安全,那么在有噪声情况下,它们会更安全.而在理想无噪声情况下,第二种密钥工作模式不安全.所以我们下面就重点分析信道噪声对第二种密钥工作模式的影响,也

就是 $m=N$ 时的情况.

假设信道噪声为加性噪声，和密文向量 $\boldsymbol{Y}_i$ 对应的复噪声向量为 $\boldsymbol{W}_i=(w_{1,i},w_{2,i},\cdots,w_{N,i})$，则其截获的密文为

$$\overline{\boldsymbol{Y}}_i=\boldsymbol{Y}_i+\boldsymbol{W}_i=\boldsymbol{X}_i\cdot\boldsymbol{D}+\boldsymbol{W}_i \tag{19}$$

为了便于分析，从对攻击者有利的角度，对和 $\overline{\boldsymbol{Y}}_i$ 对应的复噪声 $\boldsymbol{W}_i$ 作如下假设：在同一个 OFDM 符号内，$\boldsymbol{W}_i$ 的相位不变且为 θ_i，其每个元素的模值是原密文 $\boldsymbol{Y}_i$ 对应元素模值的 $\frac{1}{\sqrt{a}}$. 这样可得

$$\boldsymbol{W}_i=\left(\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}y_{1,i},\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}y_{2,i},\cdots,\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}y_{N,i}\right) \tag{20}$$

$$\begin{aligned}\overline{\boldsymbol{Y}}_i&=\left(\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right)y_{1,i},\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right)y_{2,i},\cdots,\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right)y_{N,i}\right)\\&=\mathrm{diag}\left(\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right),\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right),\cdots,\left(1+\frac{\mathrm{e}^{j\theta_i}}{\sqrt{a}}\right)\right)\cdot\boldsymbol{Y}_i^{\mathrm{T}}\end{aligned} \tag{21}$$

其中 a 为信号与噪声的功率比，$\theta_i\in[0,2\pi]$为由噪声类型决定的随机相位. 假设在第二种密钥工作模式下，攻击者获取的 N 组明文密文对为$[\boldsymbol{X}_i,\overline{\boldsymbol{Y}}_i]$，$i=1,2,\cdots,N$，$\overline{\boldsymbol{Y}}_i$ 如式(21)所示.

5.1　信道噪声对算法安全性的影响

由于攻击者获取如上假设的 N 组带有噪声的明文密文对$[\boldsymbol{X}_i,\overline{\boldsymbol{Y}}_i]$，$i=1,2,\cdots,N$，他就可以获取相应的明文矩阵和密文矩阵，将其代入式(12)可得

$$\mathrm{diag}\left(\left(1+\frac{\mathrm{e}^{j\theta_1}}{\sqrt{a}}\right),\left(1+\frac{\mathrm{e}^{j\theta_2}}{\sqrt{a}}\right),\cdots,\left(1+\frac{\mathrm{e}^{j\theta_N}}{\sqrt{a}}\right)\right)\boldsymbol{B}=\boldsymbol{A}\cdot\overline{\boldsymbol{D}} \tag{22}$$

进而可得

$$\overline{\boldsymbol{D}}^{-1}=\boldsymbol{B}^{-1}\cdot\mathrm{diag}\left(\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_1}},\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_2}},\cdots,\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_N}}\right)\cdot\boldsymbol{A} \tag{23}$$

比较式(13)和(23)，我们不难看出，信道噪声确实对非法接收者获取解密矩阵带来了影响，在我们的合理假设下，其影响为在 $\boldsymbol{B}^{-1}$ 和 $\boldsymbol{A}$ 之间多了一个对角矩阵 $\mathrm{diag}\left(\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_1}},\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_2}},\cdots,\frac{\sqrt{a}}{\sqrt{a}+\mathrm{e}^{j\theta_N}}\right)$. 容易看出，这种影响和信噪比密切相关，随着信噪比的增加，影响强度下降.

在 7.3 节我们仿真了高斯噪声下，攻击者获取解密密钥 $\overline{\boldsymbol{D}}^{-1}$ 并利用其解密的误符号率，并将其和合法用户利用 $\boldsymbol{D}^{-1}$ 解密的误符号率进行了比较. QPSK 映射时的具体数据如表 2 所示.

表 2　合法用户和非法用户解调误符号率

信噪比/db	$N=12$ 合法	$N=12$ 非法	$N=72$ 合法	$N=72$ 非法
11.5	10^{-5}	0.4	1.73×10^{-4}	0.59
12	0	0.39	6.17×10^{-5}	0.58
14.5	0	0.3	0	0.5
16	0	0.22	0	0.47
18	0	0.14	0	0.4
28.5	0	0	0	0.02
38.5	0	0	0	0

由表 2 数据可以看出，当合法用户解密误符号为 0 时，在子载波数 $N=12$ 时，非法用户为 0.39；在子载波数 $N=72$ 时，非法用户高达 0.5. 这一数据说明，在子载波数 $N=72$ 时，合法用户可以在保证自己正常解密和解调的情况下，通过控制发射功率，使非法用户的误符号率始终保持在 0.5 以上.

以上分析结果表明，虽然在理想情况下第二种密钥工作模式是不安全的，但是在实际的有扰信道下，通过适当控制发射功率，可以保证 $N=72$ 时第二种密钥工作模式的安全性，大幅提高 $N=12$ 时第二种密钥工作模式下算法的破解难度和安全性.

5.2　信道噪声对密钥安全性的影响

由于攻击者获取了如上假设的 N 组带有噪声的明文密文对$[\boldsymbol{X}_i,\overline{\boldsymbol{Y}}_i]$，$i=1,2,\cdots,N$，将其代入式(7)所示的线性方程组，这时该方程组为确定性线性方程组，容易算出其形如式(11)的唯一解如下：

$$\begin{cases}b_1b_1'=z_1^1\cdot\left(1+\dfrac{\mathrm{e}^{j\theta_1}}{\sqrt{a}}\right)\\\quad\ddots\\b_1b_N'=z_N^1\cdot\left(1+\dfrac{\mathrm{e}^{j\theta_1}}{\sqrt{a}}\right)\\b_2b_1'=z_{N+1}^1\cdot\left(1+\dfrac{\mathrm{e}^{j\theta_2}}{\sqrt{a}}\right)\\\quad\ddots\\b_Nb_N'=z_{N\times N}^1\cdot\left(1+\dfrac{\mathrm{e}^{j\theta_N}}{\sqrt{a}}\right)\end{cases} \tag{24}$$

由于受到 N 组不同的随机噪声 $\boldsymbol{W}_i$ 的影响，使得式(24)右边的值和式(11)比较，均乘上了不同的系数，变化比较大，忽略相位影响，其每一个方程右边取值的绝对误差为 $\left|\frac{z_i^1}{\sqrt{a}}\right|$.

由表 2 可知，在子载波数 $N=12$ 时，合法用户解密误符号为 0 所需的信噪比为 12 dB，相当于$\sqrt{a}=4$，绝对误差为 $0.25|z_i^1|$；在子载波数 $N=72$ 时，合法用户解密误符号为 0 所需的信噪比为 14.5 dB，相当于

$\sqrt{a}=5.3$,绝对误差为 $0.19|z_i^1|$. 这说明在合法用户能够正常解密和解调时,非法用户获取的如式(24)所示的唯一解具有比较大的误差. 这样攻击者只能通过受到噪声严重干扰,具有较大误差的式(24)来猜测密钥. 容易看出,当其猜对某个 b_i 时,只能得到错误的 b_j',从而无法正确获取其他密钥.

由此证明在有噪情况下,4.3.1 节的攻击方法将失效,第二种密钥工作模式可以保证密钥安全.

综合以上分析,我们看到本文算法在第一种密钥工作模式下,始终是安全的;而第二种密钥工作模式在理想无噪声情况下是不安全的,但是在有噪声干扰情况下,通过适当控制发射功率可保证其安全. 本文算法设置在物理层,噪声干扰是不可避免的,所以总体上看,本文算法第一和第二两种密钥工作方式都是安全的,只是安全强度不同. 在算法实际使用过程中,可以依据安全级别的不同,选择不同的密钥工作模式. 具体实现方法为通信双方首先交换主密钥,依据信息的安全级别约定子密钥的工作模式(绝对安全选择第一种模式,基本安全选择第二种模式),生成子密钥并加密明文,送入采用 DFT-S-OFDM 传输方式的通信系统,在保证正常解密和解调的情况下适当控制发射功率,实现加密信息的安全传输. 合法接收者按照约定的密钥方式完成解密和解调,恢复信息.

6 算法对原系统固有性能影响分析

6.1 系统 PAPR 影响分析

峰均比(PAPR)被定义为系统信号的最大峰值功率与其平均值之比. 假设图 1 所示的 DFT-S-OFDM 系统中,M 点 IDFT 变换后输出的信号表示为 $\{x_m, m=1,2,\cdots,M\}$,那么此时的峰均功率比可表示为

$$PAPR=\frac{\max|x_m|^2}{E\{|x_m|^2\}} \tag{25}$$

文献[18]给出了一种预编码 OFDM 系统方案,该方案通过对 IFFT 变换前的复数符号乘上一个预编码酉矩阵 $\boldsymbol{D}$,实现峰均比的抑制,具有良好的效果. DFT-S-OFDM 体制通过对星座映射后的复数向量乘上一个 DFT 矩阵,实现峰均比的 3 dB 下降,由于 DFT 矩阵也是一个酉矩阵,所以 DFT-S-OFDM 体制实际上是文献[18]方案的一个特例,文献[18]的结论完全适合 DFT-S-OFDM 体制.

在文献[18]中给出了预编码 OFDM 系统峰均比与预编码矩阵元素取值的关系,如式(26)所示,该结果表明,通过调节和选择预编码矩阵的列向量元素,可以降低峰均比,从而实现峰均比的抑制. 其中 $p_m^{\boldsymbol{D}}(t)$ 是预编码矩阵 $\boldsymbol{D}$ 第 m 列元素 $d_{i,m}$ 的函数.

$$PAPR=\frac{1}{N}\max_{0\le t\le T}\left(\sum_{m=1}^{N}|p_m^{\boldsymbol{D}}(t)|\right)^2 \tag{26}$$

$$p_m^{\boldsymbol{D}}(t)=\begin{cases}\sum_{i=1}^{N}d_{i,m}\,\mathrm{e}^{j2\pi it/T}, & 0\le t<T\\ 0, & \text{其它}\end{cases} \tag{27}$$

下面我们利用文献[18]的结论,证明本文加密算法不会对式(26)所示的峰均比造成影响,进而说明算法不会增加系统峰均比.

由图 1 及式(3)可知本文算法的加密过程为 $\boldsymbol{Y}=\boldsymbol{X}\cdot\boldsymbol{D}_1\cdot\boldsymbol{T}\cdot\boldsymbol{D}_2$. 因为对角密钥矩阵 $\boldsymbol{D}_1$ 相当于对输入信号 $\boldsymbol{X}$ 进行随机角度的旋转,不会影响系统的 PAPR,我们这里可以不考虑 $\boldsymbol{D}_1$,这样对系统峰均比产生影响的因素就只有 $\boldsymbol{T}\cdot\boldsymbol{D}_2$ 了.

由加密算法容易知道,这里的 $\boldsymbol{T}$ 表示 DFT 变换矩阵,结合文献[18]算法,我们可以将其看作加密前的预编码矩阵,则 $\boldsymbol{T}\cdot\boldsymbol{D}_2$ 可看作加密后的预编码矩阵. 容易计算其为

$$\boldsymbol{T}\cdot\boldsymbol{D}_2=\begin{bmatrix}b_1't_{11} & b_2't_{12} & \cdots & b_N't_{1N}\\ b_1't_{21} & b_2't_{22} & \cdots & b_N't_{2N}\\ \cdots & \cdots & \cdots & \cdots\\ b_1't_{N1} & b_2't_{N2} & \cdots & b_N't_{NN}\end{bmatrix} \tag{28}$$

由式(2),我们知道:

$$|b_m'|=|\exp(j2\pi d_2(m)/2^{L_2})|=1 \tag{29}$$

结合式(27)、(28)和式(29),我们容易得到

$$p_m^{\boldsymbol{T}\cdot\boldsymbol{D}_2}(t)=b_m'p_m^{\boldsymbol{T}}(t) \tag{30}$$

$$|p_m^{\boldsymbol{T}\cdot\boldsymbol{D}_2}(t)|=|b_m'||p_m^{\boldsymbol{T}}(t)|=|p_m^{\boldsymbol{T}}(t)| \tag{31}$$

这样由式(31)容易看出,加密算法对式(26)中的 $|p_m^{\boldsymbol{D}}(t)|$ 没有影响,所以对系统峰均比没有任何影响,这就从理论上证明了本文加密算法不会增加原系统的峰均比,后面的仿真结果也验证了这一结论.

6.2 系统误码率影响分析

由式(4)可知,算法的解密过程为 $\boldsymbol{X}'=\boldsymbol{Y}'\cdot\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\cdot\boldsymbol{D}_1^{-1}$. 如果假设信道噪声为加性噪声 n_0,则 $\boldsymbol{Y}'=\boldsymbol{Y}+n_0$,可以得出没有加密算法和有加密算法的解调结果如下:

$$\boldsymbol{X}'_{\text{无加密算法}}=\boldsymbol{Y}'\cdot\boldsymbol{T}^{-1}=(\boldsymbol{Y}+n_0)\cdot\boldsymbol{T}^{-1}=\boldsymbol{X}+n_0\boldsymbol{T}^{-1} \tag{32}$$

$$\begin{aligned}\boldsymbol{X}'_{\text{有加密算法}}&=(\boldsymbol{Y}+n_0)\cdot\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\boldsymbol{D}_1^{-1}\\&=\boldsymbol{X}+n_0\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\boldsymbol{D}_1^{-1}\end{aligned} \tag{33}$$

比较式(32)和(33)，容易看出，加密算法对原系统的噪声产生了一定的影响，由原来的 $n_0\boldsymbol{T}^{-1}$ 变成了 $n_0\boldsymbol{D}_2^{-1}\cdot\boldsymbol{T}^{-1}\boldsymbol{D}_1^{-1}$，也就是对原来的 IDFT 矩阵左右各乘了一个满秩对角矩阵，这种变换都是线性的，所以不会改变噪声性质.后面的仿真实验结果表明，其对系统误码率的影响是非常小的.

6.3　算法复杂度分析

由图 1 的 DFT-S-OFDM 系统框图可以看出，该系统主要由一个 N 点 DFT 和一个 M 点 DFT 串接而成，如果采用快速傅里叶变换 FFT 实现，其时间复杂度为 $O(N\log_2 N+M\log_2 M)$. 由图 2 的加密算法模型可以看出，加密算法对 N 点 DFT 的输入数据乘了一个 $N\times N$ 对角密钥矩阵，对其输出乘了一个不同的 $N\times N$ 对角密钥矩阵，其他不变. 由于乘的是对角矩阵，所以其时间复杂度为 $O(N)$，加之密钥产生过程可以事先完成，不影响复杂度，所以可以得到加密系统总的时间复杂度为 $O(N+N\log_2 N+M\log_2 M)$. 与原系统的时间复杂度比较，容易看出，加密算法增加的复杂度只有 $O(N)$，对原系统的影响很小，加密算法容易实现.

7　仿真实验结果

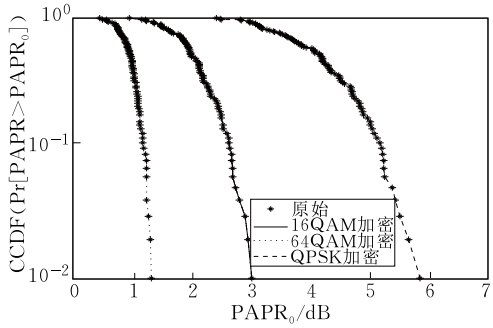
7.1　算法对系统固有性能影响的仿真分析

为了验证加密算法对原系统的峰均比和误码率的影响，我们使用 MATLAB 软件对加密前后的 DFT-S-OFDM 系统进行仿真测试.

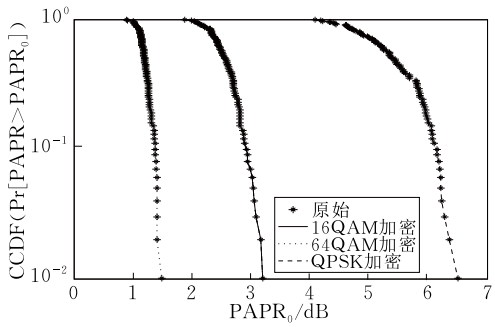
仿真参数的选择以 LTE 上行链路协议的规定[1] 为准. 具体包括 QPSK、16QAM 和 64QAM 这 3 种调制方式，12 和 72 两种子载波以及子载波分布式的映射方式. 主密钥为 128 bit 二进制数，$L_1=L_2=8$.

图 3 为在以上参数下，DFT-S-OFDM 原始系统和加密系统的 PAPR 对比曲线，其中(a)、(b)分别对应子载波数 $N=12$ 和 $N=72$. 观察图 3(a)，可以清楚的看出，加密系统在 QPSK、16QAM 和 64QAM 这 3 种调制方式下的峰均比曲线和原始系统在相同调制方式下的峰均比曲线几乎完全重合；观察图 3(b)可以得到相同的结果. 这说明加密算法没有对系统的 PAPR 造成影响，从而证明了我们理论分析的结果.

图 4 为在以上参数下，DFT-S-OFDM 原始系统和加密系统在高斯噪声情况下的 BER 对比曲线，

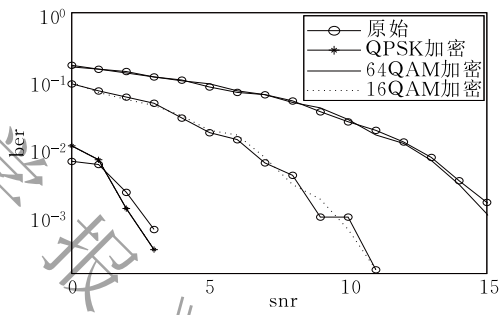


(a) 子载波数$N=12$

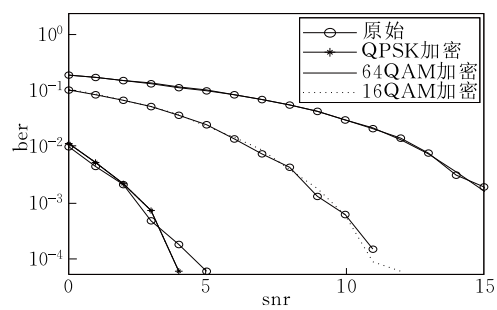


(b) 子载波数$N=72$

图 3　原始系统和加密后系统的 PAPR 比较



(a) 子载波数$N=12$



(b) 子载波数$N=72$

图 4　原始系统和加密系统的 BER 比较

其中加密系统的 BER 曲线是合法用户在已知密钥情况下取得的解密解调结果. 观察图 4(a)可以看出，加密系统在 QPSK、16QAM 和 64QAM 这 3 种调制方式下的误码率曲线和原始系统在相同调制方式下的误码率曲线几乎完全重合，而且随着信噪比的增大，误码率越来越小；观察图 4(b)可以得到相

同的结果.这一方面说明加密算法没有对原系统的误码性能造成明显影响,另一方面也说明合法用户可以和没有加密前一样,正确解调信息.

综合图 3 和图 4 的仿真结果,说明我们算法对系统的 PAPR 和 BER 等重要固有性能影响很小,对合法用户的调制解调过程几乎没有影响,具有良好的适应性.

7.2 算法安全性仿真分析

本文算法的密钥包括 128 bit 的主密钥和 L_1、L_2 取值两部分.我们分两种情况进行仿真分析,一是攻击者不知道主密钥,但知道 L_1 和 L_2 取值,二是攻击者知道主密钥,但不知道 L_1 和 L_2 取值.

从对攻击者有利的原则出发,我们选择最小的子载波数 $N=12$,星座映射分别采用 QPSK 和 16QAM,子载波映射采用分布式的映射方式,$L_1=L_2=8$.

图 5 为假设非法接收者不知道 128 位主密钥和 L_1、L_2 取值时的解调误码率曲线.观察图 5 可以看出在两种星座映射方式下,非法接收误码率不随信噪比的增加而减小;QPSK 调制方式下,其误码率在 0.56～0.59 之间波动,16QAM 调制方式下,其误码率在 0.71～0.74 之间波动.

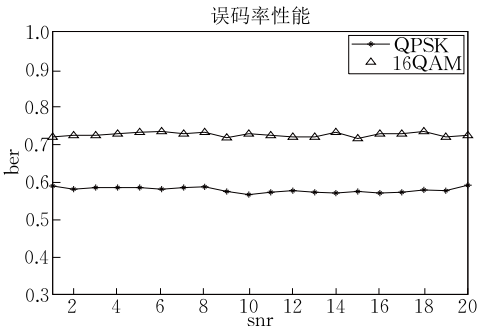
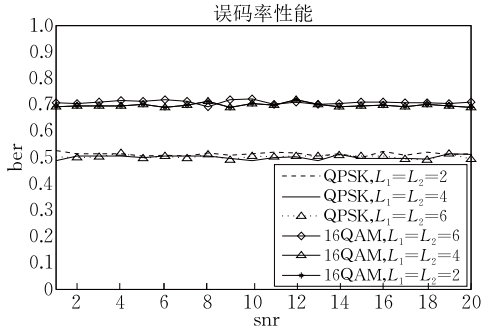


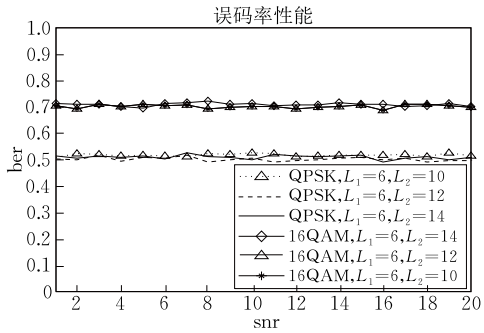
图 5 主密钥与 L 值同时错误的误码率

图 6 为假设非法接收者知道主密钥,但不知道 L_1、L_2 取值时的解调误码率曲线.观察图 6 可以看出,无论是在 QPSK 调制还是 16QAM 调制,误码率均不随信噪比的增加而减小;图 6(a)和(b)所示误码率在 QPSK 调制下在 0.48～0.53 之间波动,16QAM 调制下在 0.68～0.72 之间波动.由于图 6(c)代表攻击者知道主密钥和 L_2,知道的密钥信息最多,所以其误码率稍有下降,但其 QPSK 调制最低值也在 0.48 左右,16QAM 调制最低值为 0.67.

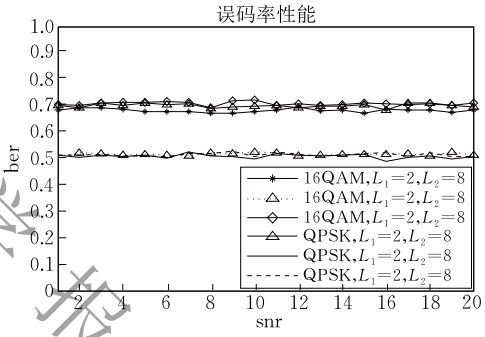
综合图 5、图 6 的仿真结果,可以得到如下结论:



(a) $L_1=L_2$且同时错误



(b) $L_1\neq L_2$且同时错误



(c) L_1错误且L_2正确

图 6 L 取值错误时的误码率

(1)攻击者不能通过增加信噪比来提高攻击的效果;

(2)当攻击者不知道密钥的所有信息时,其解调误码率高达 0.56 以上;

(3)攻击者即使知道部分密钥信息,其解调误码率最小也始终在 0.48 以上;

(4)随着调制阶数的增加,攻击者的解调误码率也随之增加,相当于算法的安全性也会越高.

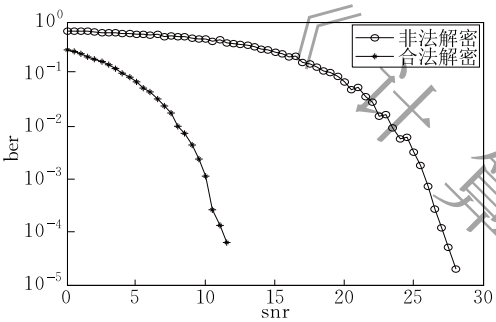
我们知道,如果攻击者随机猜测一串等概率出现的二进制信息,其猜错的概率也是 0.5.所以,以上仿真结果说明,当攻击者不知道密钥时,由于其解调误码率超过了 0.5,所以这种盲目解调的效果还不如猜测;即使当攻击者知道部分密钥的情况下,其解调误码率也很接近 0.5,所以其解调效果也和随

机猜测几乎是一样的. 这说明我们的加密算法是安全的.

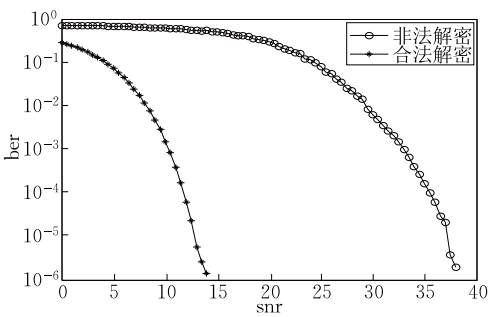
7.3　噪声影响仿真分析

为了验证 5.1 节的分析结果，我们仿真了高斯信道下的信道噪声对算法安全性的具体影响. 我们分别选择子载波数 $N=12$ 和 $N=72$，星座映射分别采用 QPSK 和 16QAM，子载波映射采用分布式的映射方式，$L_1=L_2=8$.

在此条件下，我们按照 5.1 节的方法，首先生成加解密矩阵，再生成 N 组明文密文对，在不同信噪比下，分别生成对应的被随机高斯噪声干扰的带噪密文，用其代替式(21)，计算出该信噪比下的非法解密矩阵；在相同信噪比下，计算合法用户和非法用户的解密误符号率. 具体仿真结果如图 7 和图 8 所示.



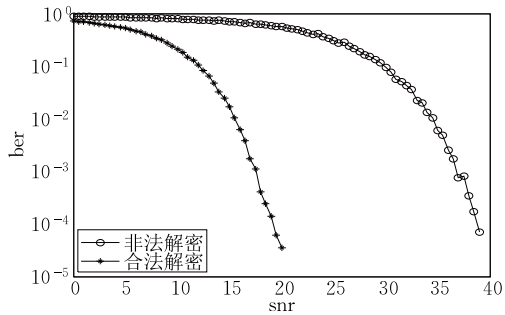
(a) 子载波数$N=12$



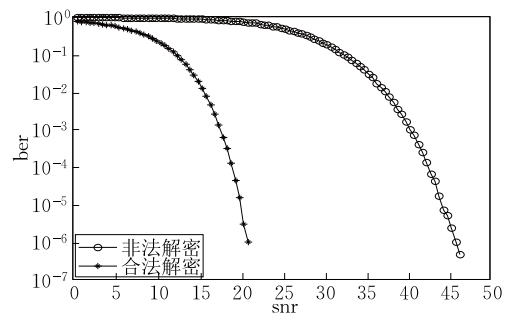
(b) 子载波数$N=72$

图 7　QPSK 调制高斯信道下的解密误符号率比较

由图可以看出，随着信噪比的增加，合法用户的解密误符号率快速下降，而非法用户的解密误符号率下降比较缓慢. 误符号率为零时，由图 7(a)曲线可看出二者信噪比相差 16.5 dB；由图 7(b)曲线可看出二者信噪比相差 24 dB；由图 8(a)曲线可看出二者信噪比相差 19 dB；由图 8(b)曲线可看出二者信噪比相差 25.5 dB. 尤其由图 7(b)和图 8(b)可以看出，在子载波数为 72，合法用户误符号为零时，非法用户的误符号仍然在 0.5 以上. 以上仿真数据和曲线说明信道噪声确实对非法用户的解密具有较大影响，随着子载波数的增多，这种影响会越来越大.



(a) 子载波数$N=12$



(b) 子载波数$N=72$

图 8　16QAM 调制高斯信道下的解密误符号率比较

7.4　性能比较

文献[4]通过对 OFDM 符号的实部和虚部分别用流密码进行加密，设计了一种物理层加密算法，该算法和本文算法具有较多相同点，下面从实现复杂度、安全性和对原系统的影响三个方面对两种算法进行比较分析.

实现复杂度方面，本文算法需要做 $2N$ 次复数乘法运算，文献[4]算法需要做 $2N$ 次复数与 ±1 的乘法运算，虽然计算复杂度相同，但是实际计算量比本文算法小.

算法安全性方面，文献[4]算法的密钥空间和 OFDM 的子载波数 N 密切相关，当 N 较小时，密钥空间会很小，例如 $N=12$，QPSK 调制时，密钥空间只有 2^{24}，安全性会下降，限制其应用范围；同时文献[4]算法不能抵抗以本文算法中的星座映射后向量 $\boldsymbol{X}$ 作为明文组成的明文密文对$[\boldsymbol{X},\boldsymbol{Y}]$的攻击，因为这时攻击者通过一组明文密文对就可很容易的得到密钥. 由上面的理论分析可知本文算法即使在子载波数 $N=12$ 时，也能保持较大的密钥空间，同时在第一种密钥工作模式下，可以完全抵抗明文密文对攻击，在第二种密钥工作模式下，可以通过控制发射功率，利用信道噪声保证算法安全. 但是，从仿真结果来看，文献[4]的加密效果优于本文算法.

对原系统误码率和峰均比影响方面，由于文献[4]加密过程非常简单，其对原系统的影响要小于本

文算法.但是由于其算法设置在 IDFT 之后,加密过程虽然破坏了子载波的正交性,提高了加密效果,但是同样破坏了 IDFT 的循环特性,为合法接收者设置循环前缀,实现系统同步造成了困难.而本文算法设置在 IDFT 之前,不会造成这样的影响.

总之,本文算法是针对现有物理层安全算法存在的密钥空间依赖于子载波个数和不能抵抗明文密文对攻击的共性问题而提出的,算法充利用 DFT-S-OFDM 体制的调制特点,合理设置密钥,利用物理层的已有的调制环节设置加密算法,使得明文、密文和密钥之间形成非线性方程组关系,在子载波数较小的情况下,不仅保证了密钥的安全,而且也实现了数据的可靠保护.

8 结 论

本文提出了一种基于 DFT-S-OFDM 传输方式的物理层双矩阵密钥加密算法.理论分析和仿真结果说明,在较小子载波数的情况下,算法在第一种密钥工作模式下,可以有效抵抗穷举攻击和明文密文对的攻击,可以有效保护无线数据连路;在第二种密钥工作模式下,可以通过控制发射功率,利用信道噪声保证算法安全.理论分析和仿真结果表明,算法对原系统的峰均比、误码率影响很小,具有良好的适应性.从而可以有效解决终端能源、计算能力等受限的无线宽带通信系统的安全问题.

致 谢 感谢徐捷、罗永玲、王少迪等所有为本文研究给予支持和帮助的人!

参 考 文 献

[1] Wang Ying-Min, Sun Shao-Hui. TD-LTE Principle and System Design. Beijing: The People's Posts and Telecommunications Press, 2010(in Chinese)
(王映民, 孙韶晖. TD-LTE 技术原理与系统设计. 北京: 人民邮电出版社, 2010)

[2] Chen Xi, Li An, Gao Guanjun. Experimental demonstration of improved fiber nonlinearity tolerance for unique-word DFT-spread OFDM systems. Optics Express, 2011, 19(27): 26198-26207

[3] Shulkind G, Nazarathy M. An analytical study of the improved nonlinear tolerance of DFT-spread OFDM and its unitary-spread OFDM generalization. Optics Express, 2012, 20(23): 25884

[4] Huo F, Gong G. A new efficient physical layer OFDM encryption scheme//Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Toronto, Canada, 2014: 1024-1032

[5] Hu Xiannan, Yang Xuelin, Shen Zanwei, et al. Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON. IEEE Photonics Technology Letters, 2015, 27(23): 1-1

[6] Liu Bo, Zhang Lijia, Xin Xiangjun, et al. Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation. IEEE Photonics Technonlogy Letter, 2014, 26(2): 127-130

[7] Zhang Lijia, Xin Xiangjun, Liu Bo, et al. Secure OFDM-PON based on chaos scrambling. IEEE Photonics Technology Letters, 2011, 23(14): 998-1000

[8] Liu Bo, Zhang Lijia, Xin Xiangjun, et al. Physical layer security in CO-OFDM transmission system using chaotic scrambling. Optics Communications, 2011, 1: 1-8

[9] Ma Ruifeng, Dai Linglong, Wang Zhaocheng, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion. IEEE Transactions on Consumer Electronics, 2010, 56(3): 1328-1332

[10] Reilly D, Kanter G S. Noise-enhanced encryption for physical layer security in an OFDM radio//Proceedings of the 2009 IEEE Radio and Wireless Symposium, San Diego, USA, 2009: 344-347

[11] Dong Jian-E, Gao Bao-Jian, Du Min. Low-PAPR OFDM algorithm to guarantee data security. Computer Engineering, 2011, 37(2): 286-289(in Chinese)
(董建娥, 高宝建, 杜敏. 一种保证数据安全的低峰平比 OFDM 算法. 计算机工程, 2011, 37(2): 286-289)

[12] Chorti A. Masked-OFDM: A physical layer encryption for future OFDM applications//Proceedings of the IEEE Globecom 2010 Workshop on Mobile Computing and Emerging Communication Networks. Miami, USA, 2010: 1254-1258

[13] Yucek T, Arslan H. Feature suppression for physical-layer security in OFDM systems//Proceedings of the 2007 IEEE Military Communications Conference. Orlando, USA, 2007: 1-5

[14] Gallo G. Complexity Issues in Computational Algebra [Ph. D. dissertation]. Courant Institute of Mathematical Sciences, New York University, New York, USA, 1992

[15] Hansen E. Numerical methods for unconstrained optimization and nonlinear equations (J. E. Dennis, Jr. and Robert B. Schnabel). SIAM Review, 1986, 28(3): 417-419

[16] Wu W J. On the decision problem and the mechanization of theorem-proving in elementary geometry. Science in China Ser A, 1979, 21(2): 117-138

[17] Wu F F, Sadatoshi K. Steady-state security regions of power systems. IEEE Transactions on Circuits and Systems, 1982, 29(11): 703-711

[18] Slimane S B. Reducing the peak-to-average power ratio of OFDM signals through precoding. IEEE Transactions on Vehicular Technology, 2007, 56(2): 686-695

GAO Bao-Jian, born in 1963, associate professor. His research interests include physical layer security and communication signal processing.

HUANG Shi-Ya, born in 1990, M. S. His research interest is physical layer security.

JING Li, born in 1991, M. S. Her research interest is physical layer security.

HU Yun, born in 1990, M. S. Her research interest is physical layer security.

Background

This paper explored the physical layer encryption technology. With bandwidth broadening and merging of the wireless communication system, foreign scholars have been paying attention to such security problems of the physical layers encryption and algorithm studies of the physical layer. In OFDM transmitting system, some algorithms exhibiting satisfied results are born, like constellation scrambling, constellation random phase rotation, and noise cover. However, with the superb transmission performance required, the physical layer encryption algorithms are confined to simple encrypting process, which make the algorithms themselves unsafe and cannot resist plaintext to ciphertext attacking. Generally, the size of key spaces proportional to the number of subcarriers. The algorithm safety drops dramatically when the number of subcarriers become less.

The aiming at the safety problem of existing algorithms, subcarrier fewer DFT-S-OFDM system as the research object, combined with LTE's resource partitioning and scheduling model design a double matrix key physical layer encryption algorithm based on, the algorithm can effectively guarantee the security of the wireless data link. The peaks of the original system are influenced the inherent properties of ratio and bit error rate. Under the condition that the number of sub carriers is greater than or equal to 12, the larger key space can be guaranteed, which can resist the attack of the plain text cipher text, and overcome the security problems of the existing algorithms.

Our research team has undertaken the Shaanxi Natural Science Foundation Project (2011JM8034) "Data Security New Mechanism Research Combined with the Characteristics of OFDM Modulation", which was completed in 2013. And our team is committed to the National Natural Science Foundation of China (61501372) and the Shaanxi Province Natural Science Foundation (2017JM6012). The physical layer security algorithm based on the unitary matrix pre coding is proposed, which is based on the interpolation of the physical layer security algorithm. And has made the physical layer encryption aspect of the invention patent (ZL 2013 1 0337275. X).