基于叠加扩频频谱中心技术的抗欺骗干扰研究

安巧静[1],孙志成[1],马丽丽[1],王 磊[1],高喜俊[2],胡爱兰[3]
(1.中国人民解放军 63861 部队,吉林 白城 137000;2.陆军工程大学石家庄校区,河北 石家庄 050003;
3.中国电子信息产业集团有限公司第六研究所,北京 100083)

摘 要:针对机载多天线收发系统(Multiple Input Multiple Output,MIMO)面临存在虚假指令的欺骗干扰威胁导致性能下降甚至失锁问题,提出了一种基于叠加扩频频谱中心技术检测欺骗干扰方案,最后通过试验验证了该方案的可行性,对 MIMO 抗虚假指令欺骗干扰性能的提升具有实际意义。

关键词:机载 MIMO;虚假指令;欺骗干扰;扩频频谱中心
中图分类号:TN97 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.201107

中文引用格式:安巧静,孙志成,马丽丽,等. 基于叠加扩频频谱中心技术的抗欺骗干扰研究[J].电子技术应用,2021,47(4):87-90,96.
英文引用格式:An Qiaojing,Sun Zhicheng,Ma Lili,et al. Research on a method of center of spreading spectrum testing deception jamming[J]. Application of Electronic Technique,2021,47(4):87-90,96.

Research on a method of center of spreading spectrum testing deception jamming

An Qiaojing[1],Sun Zhicheng[1],Ma Lili[1],Wang Lei[1],Gao Xijun[2],Hu Ailan[3]
(1.Unit 63861,PLA,Baicheng 137000,China;2.Ordnance Engineering College,Shijiazhuang 050003,China;
3.The 6th Research Institute of China Electronics Corporation,Beijing 100083,China)

Abstract:According to the problem of performance reduction even losing lock for the MIMO system threatened by deception jamming with pseudo-command,this paper presents a technology can test the deception jamming based on central part of spreading spectrum. And this method realizes the deception interference prevention. Finally it verifies the feasibility by experiment,which is importance to promote the capacity of resisting deception jamming.
Key words:MIMO;pseudo-command;deception jamming;center of spreading spectrum

0 引言

干扰问题一直是 MIMO 系统领域研究的热点,其抗干扰能力直接关系着 MIMO 系统的性能。在电子对抗中,欺骗干扰及防欺骗干扰多用于雷达系统中,尤其是 DRFM 技术的出现和发展加深了研究人员对欺骗干扰的研究[1-3]。目前欺骗干扰的研究热点多集中在欺骗干扰信号的特征提取识别研究,文献[4]、[5]中阐述了雷达欺骗干扰的多普勒识别方法,文献[6]~[9]介绍了基于距离、角度、速度等参数的欺骗干扰识别方法,文献[10]介绍了 MIMO 雷达利用回波信号相关性差异识别欺骗干扰的方法。

目前根据常见的欺骗干扰类型,其干扰特征主要表现为三方面,即欺骗干扰信号大于遥控信号、两者存在时延差以及虚假遥控指令 3 种情况。因为前两种情况容易识别,本文将重点研究存在虚假指令的欺骗干扰,对完善机载多天线收发系统的欺骗干扰系统具有重要意义。

本文通过分析基于机载 MIMO 系统虚假指令欺骗干扰的特征,阐述了虚假指令欺骗干扰的形成原理,并制定了相应的欺骗干扰预防方案。最后通过搭建试验平台,验证了该方法的可行性。

1 虚假指令的欺骗干扰分析

欺骗干扰信号中存在虚假遥控指令的实现方法通常表现为敌方在伪码序列中加入虚假遥控指令产生欺骗干扰信号。若被机载多天线接收解算后,按照敌方操控意图致使试验装备渐渐脱离地面控制站对设备的控制操作,达到欺骗干扰的目的。

一般情况下存在虚假指令的欺骗干扰会结合高信号强度欺骗干扰对遥控设备进行实施,首先利用干扰信号强度的优势到达机载多天线接收端的捕获解算链路,然后利用错误的遥控指令致使机载设备运行轨迹脱离地面控制站,最后实现对设备的控制或摧毁。

2 基于干扰认知的抗欺骗干扰

结合欺骗干扰的信号特征,MIMO 系统测控链路可以采用相应的方法进行预防。

针对欺骗干扰信号中存在虚假遥控指令，文献[11]中采用叠加扩频 MIMO 抗干扰方法，已使得敌方干扰机产生相似遥控指令难度增大。为了进一步遏制虚假欺骗干扰信息的侵入，本文提出一种基于 Walsh 序列的叠加扩频频谱中心检测法。

Walsh 序列一种“±1”为元素的二值完备正交序列，因其具有较好的正交和完备性在通信系统中得到广泛应用[12-13]。Walsh 序列具有多个不同的描述和表示方式，这里主要采用 Hadamard 矩阵得到的 Walsh 序列[14]。Hadamard 矩阵的每一行或者每一列均可以作为一个 Walsh 序列，表示为 $\mathbf{Wal}_{\mathrm{H}}(m)$，$m$ 为 Hadamard 矩阵的行序号或者列序号。Walsh 序列的列率是指序列中码元组合的重复周期数。具有相同列率的不同 Walsh 序列除了时间延迟不同，其具有相同的周期延拓波形。2 阶矩阵可表示为 $\boldsymbol{H}_2$，可递推出 $2N$ 阶 Hadamard 矩阵[15]为：

$$\boldsymbol{H}_2=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\boldsymbol{H}_4=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix},\cdots,\boldsymbol{H}_{2N}=\begin{bmatrix}\boldsymbol{H}_N & \boldsymbol{H}_N\\ \boldsymbol{H}_N & -\boldsymbol{H}_N\end{bmatrix}。$$

在 Hadamard 矩阵中，任意两行(或两列)的对应元素相乘之和等于零，即互相关函数为零。Hadamard 矩阵的每一行或每一列代表一个 Walsh 序列，这 N 个 Walsh 序列构成一个 Walsh 序列组。以 8 阶 Hadamard 矩阵产生的 Walsh 序列为例，Hadamard 有：

$$\boldsymbol{H}_8=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1\\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1\\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1\\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1\\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1\end{bmatrix} \tag{1}$$

可见，在行序中，$\mathbf{Wal}_{\mathrm{H}}(3)$与 $\mathbf{Wal}_{\mathrm{H}}(4)$具有相同的列率，$\mathbf{Wal}_{\mathrm{H}}(5)$与 $\mathbf{Wal}_{\mathrm{H}}(7)$具有相同的列率，$\mathbf{Wal}_{\mathrm{H}}(6)$与 $\mathbf{Wal}_{\mathrm{H}}(8)$具有相同的列率。8 阶 Hadamard 矩阵产生的 Walsh 序列的归一化频谱结构如图 1 所示，定义该 Walsh 序列频谱结构中谱线幅值最高点对应的频率为其中心频率。可见，不同列率的 Walsh 序列具有不同的频谱结构和不同的中心频率。$\mathbf{Wal}_{\mathrm{H}}(1)$序列虽然具有与其他序列不同的列率，但其码元的平衡性较差，不适宜应用。因此，可将不同列率且平衡性较好的 Walsh 序列集 W 作为叠加扩频序列用于欺骗干扰预防，实现方法为：无人机测控链路两端约定采用某一频率中心的 Walsh 序列作为扩频码，在接收端检测收到的 Walsh 序列中心频率来识别出有效信号，当中心频率不满足所约定的序列中心频率时，则可认为是欺骗的干扰信息。采用这种方法实现对欺骗干扰信号预防的同时，也增大了敌方实施欺骗干扰的难度。

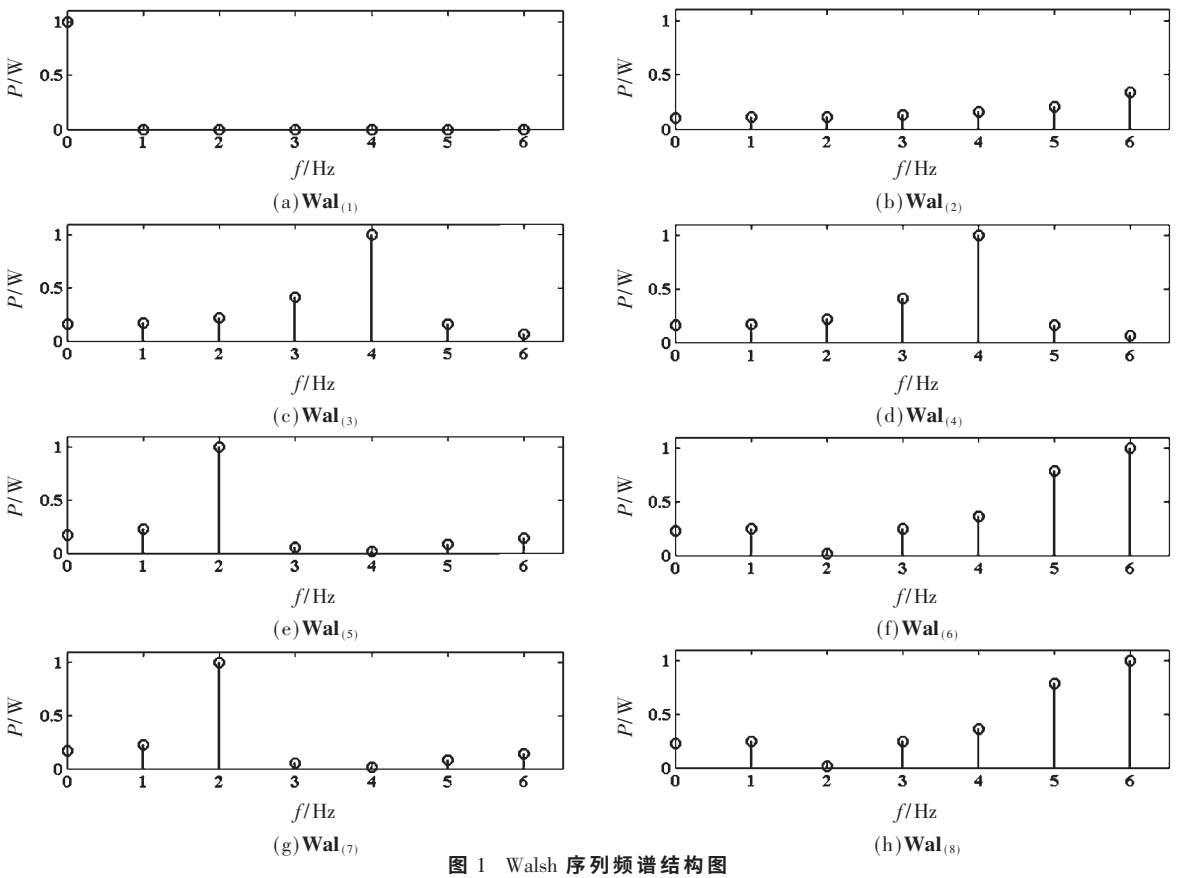


图 1 Walsh 序列频谱结构图

3 基于 MIMO 的抗干扰性能理论分析

根据欺骗干扰特征分析，接收信干比并能不反映出欺骗干扰和抗欺骗干扰的性能。本文主要根据系统误码率来说明机载多天线的抗欺骗干扰性能。

在一般机载多天线系统抗干扰方法中，干扰、噪声及信道估计是影响系统误码性能的主要因素。下面分析信道对系统误码性能的影响。

结合机载天线测控链路的通信特点，其信道主要包括直射分量和散射分量，因此可以假设信道 H 为莱斯衰落信道，则 h_{ji} 可以看作实部和虚部均值分别为 $\bar{\varepsilon}_{\mathrm{I}}$、$\bar{\varepsilon}_{\mathrm{Q}}$，方差为 σ^2 的复高斯变量，则 $\Phi=\|\boldsymbol{H}\|_F^2$ 服从自由度为 $2Num^2$ 的非中心 χ^2 分布，结合概率密度函数 $f(\varphi)$、ML 译码中 BPSK 信号瞬时负载差错概率等定义(推导过程参考文献[11])，获得理论上的系统误码率：

$$P_{\mathrm{e}}=\int_0^{+\infty}Q\left(\sqrt{\frac{2\varepsilon\varphi}{n_0}}\right)f(\varphi)\mathrm{d}\varphi$$
$$=\sum_{m=0}^{\infty}\frac{(KNum^2)^m\mathrm{e}^{-KNum^2}}{\Gamma(m+1)}\times$$
$$\left[\sigma^2-\sqrt{\frac{2\varepsilon\sigma^6}{n_0+2\varepsilon\sigma^2}}-\sqrt{\frac{\varepsilon\sigma^2}{2\pi n_0}}\sum_{l=0}^{Num^2+m-1}\frac{n_0^{Num^2+m-l-1/2}\Gamma(Num^2+m-l-1/2)}{\Gamma(Num^2+m-l)(n_0+2\varepsilon\sigma^2)^{Num^2+m-l-1/2}}\right] \tag{2}$$

其中，n_0 为信号样本量；K 为莱斯参数，表示为：

$$K=(\bar{\varepsilon}_{\mathrm{I}}^2+\bar{\varepsilon}_{\mathrm{Q}}^2)/(2\sigma^2) \tag{3}$$

$$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\mathrm{e}^{-(t^2/2)}\mathrm{d}t \tag{4}$$

伽马(Γ)函数为：

$$\Gamma(n)=\int_0^{+\infty}t^{n-1}\mathrm{e}^{-t}\mathrm{d}t \tag{5}$$

4 仿真试验

为进一步验证本文方法的可行性，基于本方法搭建了 2×2 MIMO 抗干扰系统试验环境，进行了欺骗干扰试验。

首先对 MIMO 分集收发实验的相关参数进行说明：随机生成 6 000 个“0”、“1”数据，数据包保护头为 38 bit 数据，数据包头中编号和总数据包大小均为 16 bit 数据，每次发送1 500 个数据 (6 000 个数据要经 4 次发送)，数据包保护尾 200 bit 数据(这样，每次发送1 770 个数据)。采用 8PSK 方式调制，发射、接收频率均为 4.95 GHz，IQ 速率为 500 kHz，误码率采用蒙特卡罗方式统计，次数为 100，总体观测统计 20 次的误码率 (每次为 6×10^6 个数据)，总计为 1.2×10^7 个数据的统计结果。信源经星座映射后得出发射数据的复信号星座，其频谱和时域波形分别如图 2(a)、图 2(b)所示，图中两组发射信号分别由黑色和灰色线表示。其中，图 2(a)所示的频谱是射频发射频谱映射到基带的频谱图。

为验证系统对欺骗干扰的预防“警惕性”，干扰端生成了一组与发射序列例似的随机数，并采用不同于发射端的扩频码对欺骗干扰数据进行扩频，定义欺骗干扰的 IQ 速率同样为 500 kHz，干信比为 10 dB，其发射欺骗干扰两组信号的频谱如图 3(a)所示，分别由黑色和灰色线表示。在欺骗干扰下，MIMO 综合抗干扰系统接收到的两组射频信号的频域和时域波形分别如图 3(b)、图 3(c)所示，两组接收信号分别由黑色和灰色线表示。由图 3(c)可见，该欺骗干扰会导致时域一定程度的“紊乱”，且在时域中，会明显存在某一段信号被干扰所掩埋。

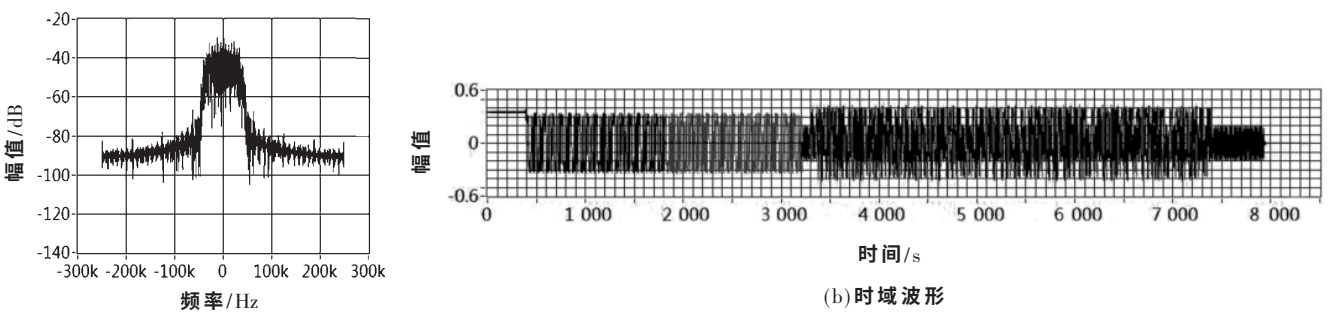
为了观测欺骗干扰对系统的影响，通过持续的欺骗干扰，观测了整个 20 次误码率统计时间内的抗干扰情况，图 4 为该欺骗干扰情况下的误码率统计值。从误码率统计结成果整体看来，只存在两次“尖峰”，即被干扰功入侵，该系统基本能够有效剔除欺骗干扰的影响，整体误码率稳定保持在 1×10^{-5} 左右。

5 结论

为验证所研究抗干扰方法的可靠性，采用软件无线电平台，在 MIMO 分集实验平台的基础上，搭建了 2×2 MIMO 抗干扰实验验证系统，并采用虚假指令欺骗干扰对其抗干扰性能进行了测试，为完善机载多天线系统测控链路中抗欺骗研究提供了有利依据。结果表明，该系统能够实现虚假指令欺骗干扰的预防。

参考文献

[1] 曹鹏，戴国宪.一种基于数字射频存储器的欺骗干扰机[J].航天电子对抗，2004(2)：33-35.
[2] 王彩云，何志勇，宫俊.基于压缩感知的单脉冲雷达欺骗



(a)频谱　(b)时域波形

图 2　发射信号波形图

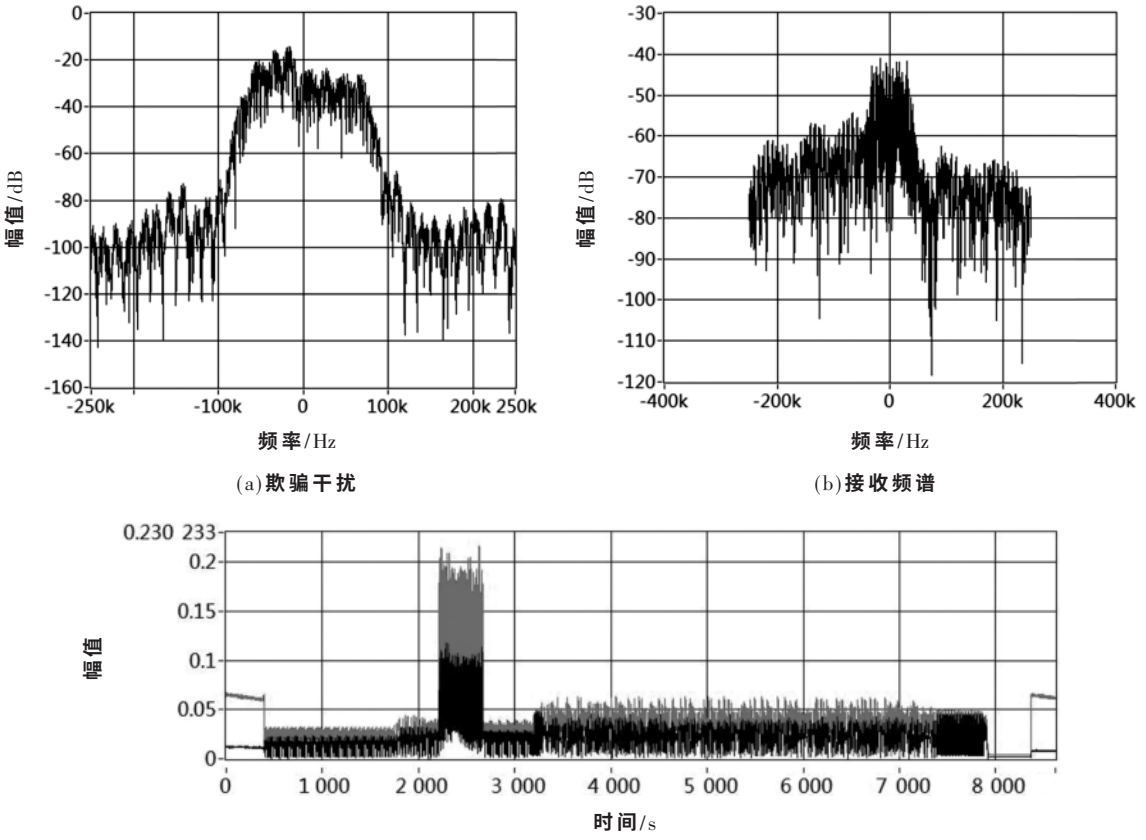


图 3 欺骗干扰及接收信号时频波形图

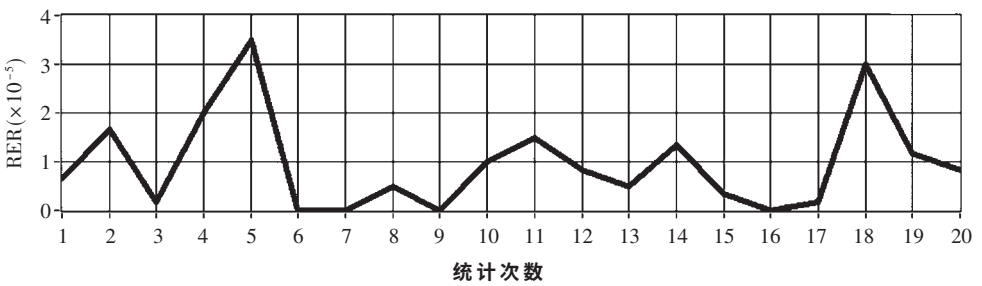


图 4 欺骗干扰下 MIMO 综合抗干扰系统误码率统计结果

干扰机研究[J].北京航空航天大学学报,2017,43(9):1789-1798.

[3] 李宏,薛冰,赵艳丽.雷达欺骗干扰的现状与困惑[J].航天电子对抗,2019(4):1-5.

[4] 单凉,张剑云,周青松.基于多普勒的欺骗干扰识别方法[J].航天电子对抗,2016,32(2):37-39.

[5] 杨少奇,田波,赵双,等.基于微多普勒特征的欺骗干扰识别[J].火力与指挥控制,2016,41(10):21-25.

[6] 张昭建,谢军伟,李欣,等.基于 FDA-MIMO 的距离欺骗干扰鉴别方法[J].北京航空航天大学学报,2017,43(4):738-747.

[7] Zhang Zhaojian,Xie Junwei,Sheng Chuan,et al.Deceptive jamming discrimination based on range-angle localization of a frequency diverse array[J].Frontiers of Information Technology & Electronic Engineering,2017,18(9):1437-1446.

[8] 段翔,刘红明,李军,等.双基地多输入多输出雷达距离欺骗干扰识别技术[J].电波科学学报,2015,30(3):517-523.

[9] 杨林,张翔宇,李林,等.基于时空频特征融合的距离-速度复合欺骗干扰识别技术研究[J].系统工程与电子技术,2019,41(12):2684-2691.

[10] 干鹏,周生龙,李贵显,等.分布式 MIMO 雷达欺骗干扰抑制算法研究[J].航天电子对抗,2019,35(2):25-32.

[11] 高喜俊,陈自力.基于 CR-MIMO 的无人机多域联合分集抗干扰方案[J].系统工程与电子技术,2015,37(9):1987-1993.

[12] 付江志,郭黎利,杨红乔.具有频谱可控特性的直扩系

(下转第 96 页)

算法[EB/OL].(2019-xx-xx)[2020-10-13].http://sfjs.cacr-net.org.cn/site/term/list_76_1.html.
[2] 吴文玲,张蕾,郑雅菲,等.分组密码 uBlock[J].密码学报,2019,6(6):690-703.
[3] 贾珂婷,董晓阳,魏淙洺,等.分组密码算法 FESH[J].密码学报,2019,6(6):713-726.
[4] 张文涛,季福磊,丁天佑,等.TANGRAM:一个基于比特切片的适合多平台的分组密码[J].密码学报,2019,6(6):727-747.
[5] 田甜,戚文峰,叶晨东,等.基于 NFSR 的分组密码算法 SPRING[J].密码学报,2019,6(6):815-834.
[6] 陈师尧,樊燕红,付勇,等.ANT 系列分组密码算法[J].密码学报,2019,6(6):748-759.
[7] 王克,贾文义,黄念念.SMBA 分组密码算法[J].密码学报,2019,6(6):786-802.
[8] 李永清,李木舟,付勇,等.Raindrop:面向硬件设计的分组密码算法[J].密码学报,2019,6(6):803-814.
[9] 徐洪,段明,谭林,等.NBC 算法[EB/OL].(2019-12-05)[2020-10-13].http://sfjs.cacrnet.org.cn/site/content/424.html.
[10] 徐洪,段明,谭林,等.NBC 算法[J].密码学报,2019,6(6):760-767.
[11] 冯秀涛,曾祥勇,张凡,等.轻量级分组密码算法 FBC[J].密码学报,2019,6(6):768-785.
[12] BIHAM E,SHAMIR A.Dierential cryptanalysis of DES-like cryptosystems[C].CRYPTO 1990,Springer Berlin Heidelberg,1991,537:2-21.
[13] MATSUI M.Linear cryptanalysis method for DES cipher[C].EUROCRYPT 1993,Springer Berlin Heidelberg,1993,765:386-397.
[14] BIHAM E,BIRYUKOV A,SHAMIR A.Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C].EUROCRYPT 1999,Springer Berlin Heidelberg,1999,1592:12-23.
[15] BOGDANOV A,RIJMEN V.Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J].Designs Codes & Cryptography,2014,70(3):369-383.
[16] BOGDANOV A,WANG M.Zero-correlation linear cryptanalysis with reduced data complexity[C].FSE 2012,Springer Berlin Heidelberg,2012,7549:29-48.
[17] BOGDANOV A,LEANDER G,NYBERG K,et al.Integral and multidimensional linear distinguishers with correlation zero[C].ASIACRYPT 2012,Springer Berlin Heidelberg,2012,7658:244-261.
[18] KNUDSEN L R,WAGNER D.Integral cryptanslysis2[C].FSE 2002,Springer Berlin Heidelberg,2002,2365:112-127.
[19] CHEN H F,CUI T T,WANG M Q.Improving algorithm 2 in multidimensional(zero-correlation) linear cryptanalysis using χ^2-method[J].Designs Codes & Cryptography,2016,81(3):523-540.
[20] SUN L,CHEN H F,WANG M Q.Zero-correlation attacks:statistical models independent of the number of approximations[J].Designs Codes & Cryptography,2018,86(9):1923-1945.
[21] TODO Y.Structural evaluation by generalized integral property[C].EUROCRYPT 2015,Lecture Notes in Computer Science,Springer,Berlin,Heidelberg,2015,9056:287-314.

(收稿日期:2020-10-13)

作者简介:
杨江帅(1989-),男,博士研究生,工程师,主要研究方向:信息安全与密码。
陈怀凤(1990-),通信作者,男,博士研究生,工程师,主要研究方向:对称密码算法的安全性分析,E-mail:chenhf@ncse.com.cn。
鲍金凤(1969-),通信作者,女,博士研究生,讲师,主要研究方向:旅游文化、北京历史文化,E-mail:lytjinfeng@buu.edu.cn。
康潇文(1983-),女,硕士研究生,助理研究员,主要研究方向:虚拟存储、云计算、数据融合。

(上接第 90 页)

统规避窄带干扰技术[J].系统工程与电子技术,2011,33(6):1403-1406.
[13] 杜秀丽,甄旭亮,邱少明.混沌与 Walsh 复合扩频序列性能分析[J].大连大学学报,2013,34(6):13-17.
[14] WANG F H,XIE H,HUANG Z T.Blind reconstruction of convolutional code based on segmented Walsh-Hadamard transform[J].Journal of Systems Engineering and Electronics,2014,25(5):748-754.
[15] 玉苏甫江·依拉依木,任平安.基于 Hadamard 矩阵的随机网络编码[J].电子科技,2012,25(5):105-107.

(收稿日期:2020-11-12)

作者简介:
安巧静(1987-),通信作者,女,博士,工程师,主要研究方向:数据分析与处理,E-mail:anqjoec@163.com。
孙志成(1983-),男,本科,工程师,主要研究方向:数据处理。

版权声明