文章编号:1671-4598(2024)06-0242-06 DOI:10.16526/j.cnki.11-4762/tp.2024.06.035 中图分类号:TP391.4 文献标识码:A

基于加密模式的协同式激光敌我识别技术

唐大宇,潘向荣
(中国西南电子技术研究所,成都 610036)

摘要:为了解决普通的激光敌我识别中,信号容易被侦收后破解的问题,提出了一种基于加密模式的协同式激光敌我识别技术,对激光敌我识别系统工作原理进行了研究与分析,采用通过时间信息产生一组伪随机数,利用一组高强度的改进加密算法对这组伪随机数进行变换产生加密数据,并经过扩频函数对变换后的加密数据进行扩频,结合RS纠错码产生最终编码的方法,增强数据的抗干扰能力,经实验测试实现了提高信号保密性和安全性的目的,为激光敌我识别的发展提供了新的思路。

关键词:激光敌我识别;协同;伪随机数;扩频;加密算法

Cooperative Laser IFF Technology Based on Encryption Mode

TANG Dayu, PAN Xiangrong
(Southwest China Institute of Electronic Technology, Chengdu 610036, China)

Abstract: In order to solve the problem that the signal is easily detected and deciphered in general laser Identification, Friend or Foe (IFF), a cooperative laser IFF technology based on encryption mode is proposed. The working principle of laser IFF system is studied and analyzed. The time information is used to generate a set of pseudo-random numbers. A set of high-strength improved encryption algorithm is used to transform the pseudo-random numbers to generate encrypted data, and the encrypted data is spread by the spread-spectrum function. Combined with the Reed-Solomon (RS) error correction code, the final code is generated to enhance the anti-jamming ability of the data. Experimental results show that the signal confidentiality and security are enhanced, and it provides a new idea for the laser IFF development.

Keywords: laser IFF; cooperation; pseudo-random data; spread-spectrum; encryption algorithm

0 引言

现代战争越来越体现出复杂化、多元化的特点,已经不是传统战争的单一兵种作战模式,是海、陆、空一体化战场,同时各国也在大力发展超视距的技术发展,这种多兵种协同作战战场的特点是:无明显、固定的战线,目标速度快、机动性强,战况瞬息万变。这种敌我交织的现代战场中,已不同于传统敌我识别概念,敌我混淆程度更大,对敌我识别提出了更高的要求,如何快速、精准地对各平台进行识别,已成为一个迫切的需求。

目前在战争中使用比较广泛的敌我识别技术有雷达敌我识别系统、毫米波敌我识别系统和激光敌我识别系统[1]。雷达敌我识别器主要用在大型战场上,它具有完备的收发信道和天线系统,北约各国现使用先进的MARKXIIA系统,具有作用距离远,战场适应高等特点,但体积较大,角分辨率相对较低、抗干扰性差、定位精度不高;毫米波敌我识别器主要使用STANAG-4579号标准协议,用于密集战场环境下的敌我识别,虽然在设备体积和抗干扰性方面较雷达敌我识别器有所提升,但仍然存在分辨率和定位精度方面的不足。而激光敌我识别[2-5]在这方面有着先天的优势,激光具有良好的方向性、定位精度高、抗干扰能力强、信号传递通道窄、系统结构紧凑、体积小等特点。依靠这些独特优势,激光敌我识别技术作为一个新的思路和体制受到广泛重视,在近年来在美国、英国、法国和德国等西方国家都得到飞速发展。比如德国的ZFFF激光敌我识别系统,它使用的是激光询问、D波段应答,可以装载在直升机、战车等战场平台上,可完成空地、空空等识别任务;美军研制的LW—CID(陆地勇士作战识别系统)和HDSID(直升机对单兵识别系统)等激光敌我识别系统,装备M1A2、BLOCKⅢ坦克和各种武装直升机。

随着激光敌我识别的深入研究,对其干扰和对抗的技术也随之发展起来,传统的依靠友方目标上反射棱镜装置进行简单调制的方法已经变得很不安全了,因此本文提出了一种基于加密模式的协同式激光敌我识别技术来提高抗干扰能力和保密性。

1 协同式激光敌我识别技术工作原理

敌我识别技术根据体制不同可分为协同式敌我识别、非协同式敌我识别和综合敌我识别。激光敌我识别主要使用协同式敌我识别方式。

激光敌我识别从本质上来说就是利用激光作为载波发射敌我识别信号,通过对敌我识别信号的编解码来进行目标属性识别。根据应答方的使用设备形态不同,又可以分为协同式有源应答识别和协同式无源识别。

收稿日期:2023-12-27; **修回日期**:2024-02-02。
作者简介:唐大宇(1978-),男,大学本科,高级工程师。
引用格式:唐大宇,潘向荣.基于加密模式的协同式激光敌我识别技术[J].计算机测量与控制,2024,32(6):242-247,255.

协同式有源激光敌我识别系统由询问系统和应答系统组成。询问系统主要负责询问信号的编码和应答信号的解码，应答系统主要负责询问信号的解码和应答信号的编码。战场中的我方作战单位都需要配装相应的激光敌我识别系统，用于身份属性判别，防止在战场中被误伤。

协同式无源激光敌我识别系统在询问方和有源激光敌我识别差不太多，但在应答方不再产生新的应答信号，而是在接收到询问信号后，通过调制器对反射棱镜上的光栅进行控制，将询问信号的部分信号进行遮挡，只反射其它信号，从而产生可识别的应答信号，这种方式对定位精度要求不高，且反应速度快，但缺少灵活性，抗截获性也较差。

一般来说询问系统装载于有火力打击能力的平台，如坦克、武装直升机、单兵以及导弹等平台；应答系统装载于无攻击能力的平台，如运输机、装甲车等，而对于在战场中机动性比较强，且经常在战场中穿梭的平台则应该同时装载询问系统和应答系统，以便在敌我双方进行混战时，分辨战场中的我方目标，避免误伤。

2　协同式激光敌我识别系统组成

协同式激光敌我识别系统主要激光询问分系统和激光应答分系统组成。它们由激光发射光学系统、激光器、激光接收光学系统、激光探测器、伺服转台、识别器主机、授时天线组成，如图 1 所示。

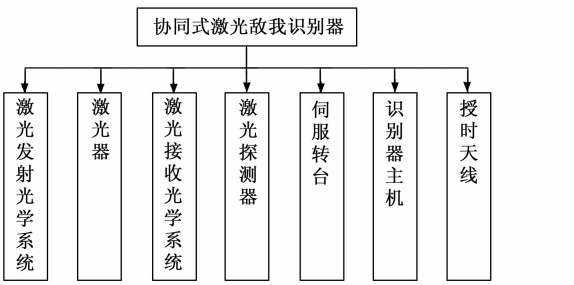

图 1　协同式激光敌我识别系统组成

其中激光发射光学系统和激光器主要完成激光信号的产生和发射；激光接收光学系统和激光探测器主要完成激光信号的发现与接收；伺服和转台控制激光发射与接收的方向；识别器主机用于信号的编解码；授时天线接收时间信息。

基于加密模式的协同式激光敌我识别，其核心在于识别器主机内的加密系统，一个稳定、高强度的加密系统是提高系统抗干扰能力、提高保密性的关键。

3　加密系统介绍

加密系统是通过时间信息产生一组伪随机数，并利用一组高强度的加密算法对这组伪随机数进行变换产生加密数据，最后通过扩频函数对变换后的加密数据进行扩频产生该时刻的脉冲控制码，并产生相应的检验码。

加密系统的核心由伪随数产生、扩频、加密算法及校验码组成。

3.1　伪随机数产生

伪随机数是指使用一个已知的算法来产生的随机数，而且它是在使用这个算法产生的一个随机序列里的一个数。这个数在一定范围内是具有随机性的，它的随机性体现在这个随机序列中。

伪随机数的产生方法有很多，比如同余法[6]、D－序列法[7]、随机分布法[8]、陶斯沃斯法（Tausorthe）等。本方采用同余法中的线性同余法。

线性同余法产生的伪随机数序列有着很好的伪随机性和安全性，是一种伪随机性能好的一种伪随机数产生器。而且如果其重复周期足够长，那么产生的随机数在一定范围内就可以视作一个真正的随机数序列。

线性同余法基本概念是数论中的线性同余方程，运用同余运算来产生随机数。它的基本公式为：

$$x_{n+1} = (ax_n + c) \bmod m$$

式中，x_0 为初始值；a 为乘法器，取值为≥0 的正整数；c 为增值，取值为大于等于 0 的正整数；m 为模数，大于 x_0、a、c 的正整数；mod 为运算符，表示取余运算。

使用递推公式得到新的解析式：

$$x_1 = (ax_0 + c) \bmod m$$

$$x_i = (ax_{i-1} + c) \bmod m$$

$$u_i = x_i \div m$$

式中，u_i 就是我们要使用的伪随机数，u_1，u_2，u_3，…，u_r，就是这一组随机序列。

其中：$1 \leqslant r \leqslant m$。

公式中的各参数选择对伪随机序列的均匀性、独立性和循环周期有着直接的影响。

x_0 这里使用时间作为初始值，格式为年月日时分秒，比如时间为 2023 年 1 月 12 日 17 点 23 分 16 秒时，x_0 取值为 20230112171216，x_0 的值每秒钟变换一次，这样也可以有效避免随机序列中的数被取完，出现随机数重复的情况。

m 的大小直接限制了随机序列中随机数的重复周期，所有 m 的取值应该尽可能地大，由于本技术的实现平台为单片机或者 DSP 芯片，这类平台大多的字长为 16 位，所以这里我们可以取得 m 的最大值为 $2^{16}-1$ 。

a 和 c 的选择也是决定线性同余随机数序列重复周期的重要因素，如果想要这个随机数序列的重复周期达到最大，即为 m 的话，首先 c 必须和是 m 是同质的，即同时能被 c 和 m 正整数只有 1。而 a 的选择应为（$a-1$）是每一个能整除 m 的质数的位数，即如果 m 能被 7 整除，那么（$a-1$）也应该能被 7 整除。

在工程实现时，基于单片机或者 DSP 芯片的伪随机数产生流程如图 2 所示。

这种随机数产生方法在工程实现时有几点需要注意：第一点是种子在使用时不可以重复，这里使用时间作为种子可以有效避免重复，也可以在时间信息上再进行一次变换，来加强其保密性；第二点是 a、c、m 共 3 个参数要慎重选择，这 3 个参数是决定整个伪随机序列质量的关键。

伪随机数的产生是加密系统中的一个重要环节，对加密系统的抗干扰能力和保密性有着直接的影响。本人给出

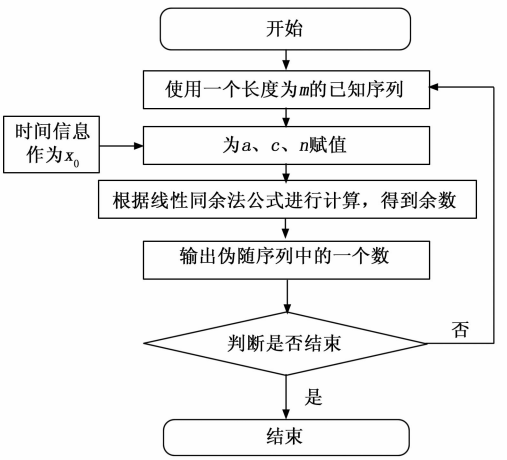

图 2 伪随机数产生流程图

的线性同余伪随机数产生方法是基于单片机或者 DSP 芯片产生的，除了具有很高的随机性外，也有利于工程实现。

3.2 扩频

扩频是提高数据抗干扰能力，提高灵敏度的有效手段。

$$\begin{bmatrix} w(0,t) \\ w(1,t) \\ w(2,t) \\ w(3,t) \\ w(4,t) \\ w(5,t) \\ w(6,t) \\ w(7,t) \\ w(8,t) \\ w(9,t) \\ w(10,t) \\ w(11,t) \\ w(12,t) \\ w(13,t) \\ w(14,t) \\ w(15,t) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix}$$

在进行 Walsh 变换[10-11]时，将产生的数据按固定长度进行划分，平分为多个数据块，再根据这些数据块里的数据从 Walsh 码表里选择一个相应的码元进行变换，最后再将这些变换后的数据组合在一起，得到最终的扩频数据。

Walsh 码在完全同步时具有最好的同步正交性，即自相关函数 $R_a(0)=1$，互相关函数 $R_c(0)=1$。但随着正交性的变化，非同步的情况会越来越强，会产生较大的旁瓣值，这就会使得 Walsh 码的自相关性和互相关性也随之变差。

Walsh 码的各码元序列的频谱[12-13]是离散的，它的谱分布取决于码元序列中的码字的重复周期，重复周期越大，谱线的分布越密集，反之，重复周期越小，谱线分布越稀疏。而 Walsh 码的各谱线包络形状有点类似于 Sa 函数，它的主要能量集中在中心频率附近，如果把中心频率做主瓣，与之相在这里使用 Walsh 变换[9]进行扩频，Walsh 函数是美国科学家 Walsh 在 1923 年提出的一类完备的正交函数系，Walsh 码具有良好的同步正交性。Walsh 函数序列里的数字由+1 和−1 组成，这使得它更适合在数字信号处理、数字图像处理、数据加密及数字通信中使用。

Walsh 码的行和列可由哈达马矩阵映射构成，其中码的种类等于码的长度。

$$H_1 = 1$$

$$H_1 = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_N = \begin{bmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & H_{N/2} \end{bmatrix}$$

用 $W(0)$ 表示 Walsh 序列 0，$W(k)$ 表示 Walsh 序列 k 即哈达马矩阵的第 $k+1$ 行。那么 N 阶 Walsh 函数（$N=2n$，$n=0$，1，2 ...）对应于 Walsh 序列 $W(0)$，$W(1)$ ... $W(N-1)$，每个 Walsh 序列的长度均为 N。Walsh 码的矩阵其实就是一种矩形波，例如 16 阶 Walsh 码的各码元序列如下所示：

邻的两个零点作为边界，那么所有的谱线都应该在这个范围之内，这个范围也称之为这个码元序列的频带宽度。

当知道了一个 Walsh 码序列频谱的中心频率、谱线间隔和频带宽度后，这个 Walsh 码序列在频域上的频谱结构也可以推算出来。Walsh 码各码元序列的频谱分布是有规律性的。N 阶的 Walsh 码所包含的 N 个码元序列一共有 $N/2+1$ 种频谱结构，每个序列的中心频率可由下列公式计算得出。

$$q = k \times \frac{fw}{2^{p+1}}$$

式中，q 为中心频率，fw 为码元速率，k 为系数，P 为码元序号。

N 个码元的频谱结构分布序号如下：

$$\begin{cases} 2^p + q \\ 2^p + 2^{p-1} + q \end{cases}$$

式中，$P=0,1,2,\cdots,N-1$；$q=0,1,2,\cdots,2^{p-1}-1$。

通过 Walsh 码在频域上频谱分布特性的分析，可以看出，不同的码元序列，其中心频率和带宽都不是相同的，主瓣的能量分布也是随之变化的，所以这些码元序列的频谱结构也是不相同的。因此，合理地选择 Walsh 变换进行扩频，除了可以增加信号数据长度、增加扩频增益、提高传输速率外，还可以根据频谱分布的特点结合系统使用的环境及频率范围进行选择 Walsh 码，以此来解决远近效应和窄带干扰给系统带来的问题。

3.3　加密算法

加密算法是整个加密系统的核心，它的性能直接影响整个激光敌我识别系统的抗干扰能力、保密性以及识别率。加密算法包括密钥产生、询问机生成加密询问包；应答机处理询问包（解密、判别）等关键部分。

3.3.1　密钥产生

密钥产生的基本思想是：自主设计的密钥流产生器产生合格的大数量密钥材料，从中提取密钥加密密钥 K2 和 100 条（或指定条数）适合轮换使用的短期密钥 K1（包括互不相同的 ID，和由日期和序号确定的密钥批号 No），每条（包括 ID 和 No）364 比特。用装定密钥 K2 的 AES[14-15] 算法等方法加密每条 K1、再用汉明码编码、最后按 SHA-1[16]（可将该数据分为较小的组）计算以上数据的 Hash 值（若分组，各组 Hash 值做异或）作为认证码，再将以上数据存入 Card1；将重复的 K2 存入 Card2。

先用择多法排除 K2 的随机错；再按 SHA-1 算法计算 Card1 数据（不包括存储的 Hash 值）的 Hash 值，与存储的 Hash 值比对，如果相等，可认证 Card1 数据无误（以接近 1 的概率）。然后，用密钥产生步骤的逆步骤还原出指定的（当日或数日使用的）那条短期密钥 K1（若纠错译码未发现不可纠差错），之后将 K1 馈入询问机或应答机。

消息加密密钥 K1 的原始随机序列材料由专门设计的一种流密码生成器产生。然后对原始随机序列进行筛选。通过严格筛选的随机序列才作为消息加密密钥提供用户。对同批的（最多 100 条）消息加密密钥，还要进一步筛选以保障各条密钥内的 12 比特识别标志 ID 彼此不同。

K1 的生成算法－cscsi _ KeyGenerator，算法流程如图 3 所示。

在图 3 的 A 点处，研究消息加密密钥生成算法的输出序列。该序列的周期等于 4 个驱动序列周期的最小公倍数：

$$p=lcm(p_1,p_2,p_3,p_4)=lcm(2^{19}-1,2^{30}-1,2^{26}-1,2^{27}-1)$$
$$=(2^{19}-1)(2^{30}-1)(2^{26}-1)(2^{27}-1)/63$$
$$=8.04856\times10^{28}>2^{96}(=7.9228162\times10^{28})$$

所以，穷搜索攻击的难度大于搜索 96 比特密钥。

GSM[17] 中的密钥流生成器 A5/1[18] 公式为：

$$P_{A5/1}=lcm(p_1,p_2,p_3)=lcm(2^{19}-1,2^{22}-1,2^{23}-1)$$
$$=(2^{19}-1)(2^{22}-1)(2^{23}-1)<2^{64}$$

A5/1 密钥流生成器工作过程：

1）预置：先将 3 个 LFSR 的初态置“0”，再将 K＝K64＋FN22（K64 为 64 比特密钥，FN22 是 frame number，已知）共 86 比特在反馈端以“模 2 加”注入（此过程择多步进逻辑不工作）。

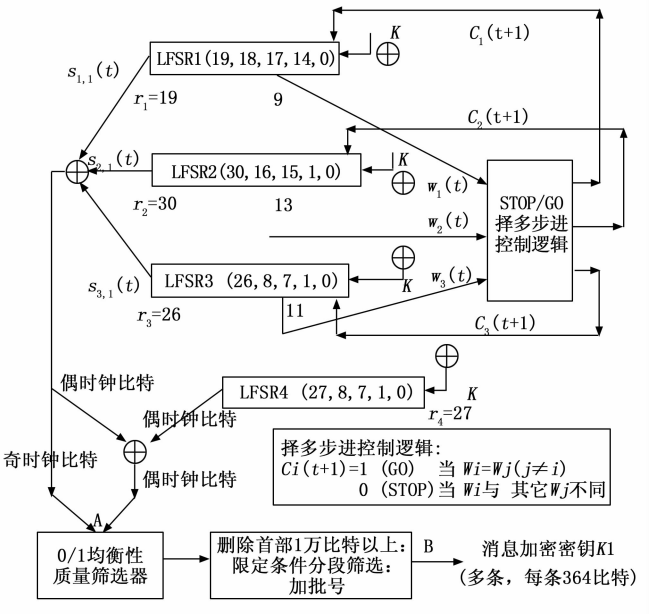

图 3　K1 算法流程图

2）置乱：（$t=0$ 计时开始）择多步进逻辑开始工作，先“空跑”100 拍，再跑 228 拍，所得 228 比特为有效密钥流 y（101－328）。

研究消息加密密钥 K1 生成算法可以发现，该生成器在 A5/1 型流密码的基础上做了以下强化：

1）增加了 LFSR1～LFSR3 的总级数（由 64 级增加到 75 级，增加了 11 级）；

2）增加了 LFSR4 用于对 A5/1 型输出序列进行“打孔式”覆盖；

3）在输出端（图 3 位置 B）删除了序列首部上万比特（随机长度）。

以上设计，完全阻止了对 A5/1 型序列生成器的所有有效攻击：目前，对 A5/1 型序列生成器的最好分析结果是 $O(2^{41.16})$，即利用生成器的反馈关系，可以把原来 $O(2^{64})$ 的复杂度降低 $O(2^{23})$，或者说将密钥量减少 23 比特。即使该方法对本密钥流生成器完全有效（由于（3），该方法对本设计其实已经失效），其攻击本设计的复杂度仍然大于 $O(2^{73})$，实际不可行。

密钥加密密钥 K2，在每批次准备的消息加密密钥材料数据（64 000 byte，每次所需要的 100 条 K1，净需求为 4 600 byte，按利用率 10％计算，最多消耗 46 000 byte，尚剩余 18 000 byte）的尾部截取。换言之 K2 与 K1 数据在序列中的位置至少相距 18 000 byte（实际距离在 50 000 byte 左右）。前面的密钥材料的随机性论证，对 K2 的生成质量保障，也同样有效。

分组密码 cscsi _ B32 是设计的一种 32 比特分组密码。由于小分组密码本身的弱点，本系统对询问包明文的加密，

并不是单独使用 cscsi _ B32 完成的，而是与特殊设计的掩码加密算法联合使用的。

cscsi _ B32 算法明/密文分组为 32 比特，用户密钥 256 比特，按迭代型分组密码设计，轮数 r 在 12～18 之间可选（不使用关联包时，推荐使用 15～18 轮）。加密算法流程如图 4 所示。

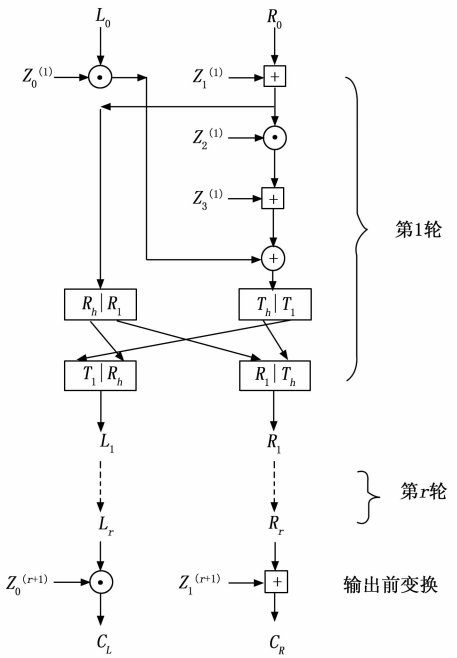

图 4 加密算法流程图

M：32 比特分组明文，$M=(L_0 \mid R_0)$，L_0、R_0 分别为 16 比特块。

L_{i-1}、R_{i-1}；L_i、R_i：第 i 轮函数的输入的左右部分，和输出的左右部分，分别为 16 比特块。

C：32 比特分组密文，$C=$ cscsi _ B32（K_{256}，M）。

K_{256}：32 比特分组密码用户密钥或会话密钥。

key1［16］，key2［16］：密钥 K_{256} 的两部分，按多个算法需要的字节存储形式。

en _ keyB32：32 比特分组密码 cscsi _ B32 加密工作密钥生成算法。

de _ keyB32：32 比特分组密码 cscsi _ B32 解密工作密钥生成算法。

$Zj^{(r)}$：由算法 en _ keyB32（key1，key2）生成的用于 cscsi _ B32 加密算法第 r 轮的第 j 块工作密钥（$j=0$～3），16 比特（word）。

Z［4］［$R+1$］：cscsi _ B32 加密工作密钥（二维数组），由 $Z_j^{(r)}=Z[j][r]$ 组成。

$Z_j^{(r)-1}$：由算法 de _ keyB32（Z［］［］）生成的用于 cscsi _ B32 解密算法第 r 轮的第 j 块工作密钥（$j=0$～3），16 比特（word）。

⊕：16 比特块——对位模 2 加。

⊙：16 比特块——模 $2^{16}+1$（65537）乘法。

＋＋：16 比特块——模 2^{16}（65536）加法。

其中，明文 $M=(L_0 \mid R_0)$，密文 $C=(C_L \mid C_R)$。cscsi _ B32 的工作密钥生成算法 en _ keyB32（key1，key2），是对 IDEA[19] 工作密钥生成算法的改进与强化，使得密钥量从 128 比特增加为 256 比特。由图 4 可见，cscsi _ B32 的轮工作密钥比特数为 64（4×16），远高于 IDEA32 的轮工作密钥比特数 48（6×8）。cscsi _ B32 解密算法按上图的逆方向进行。

cscsi _ B64 算法明/密文分组为 64 比特，间接使用 cscsi _ B32 用户密钥（256 比特），由 4 个 cscsi _ B32s 模块组合构成。当采用关联包方案，与 cscsi _ B32 配合使用。由于 DSP 时间限制，cscsi _ B32s 需要选定为小迭代轮数。

cscsi _ B64 加密算法结构如图 5 所示。

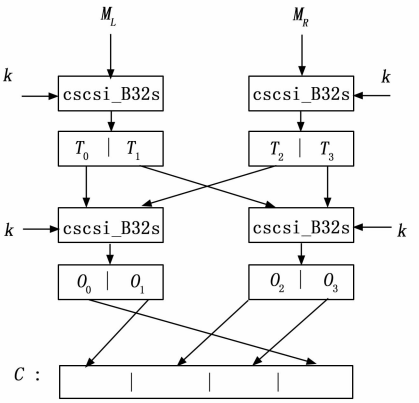

图 5 加密算法结构图

M：64 比特分组明文，$M=(M_L \mid M_R)$，M_L、M_R 分别为 32 比特块。

C：64 比特分组密文，$C=$cscsi _ B64（K_{256}，M）。

3.3.2 询问机生成加密询问包

将未加密的询问包称为原始消息 M_0，32 比特，其构成如下：

J	S	Tag	$N\neq 0$	ID

其中：J、S 各 4 比特，是指示掩码加密的参数；ID、N 见符号约定；模式标记 Tag，8 比特，它的取值将根据“模式解释表”解释询问包的模式或种类。解释表可由密钥指定。

记消息加/解密密钥为｛key1［16］，key2［16］，mask［19］｝。32 比特原始消息 M_0 到已加密询问包 C 的加密过程如图 6 所示。

其中，符号 Rot ^{5}(＞＞) 表示其后的三字节比特串循环右移 S 位。这里，原始消息 M_0 第一步被掩码加密为 M，第二步调用分组密码 cscsi _ B32 加密 M，产生的密文 C 即待发送的 32 比特密文询问包。

3.3.3 应答机处理询问包

应答机内，解密 32 比特密文询问包 C 的过程与加密中的变换过程相反：先调用分组密码 cscsi _ B32 解密 C，得到 M；再用掩码解密 M，最后得到 M_0。这里要注意的是，在

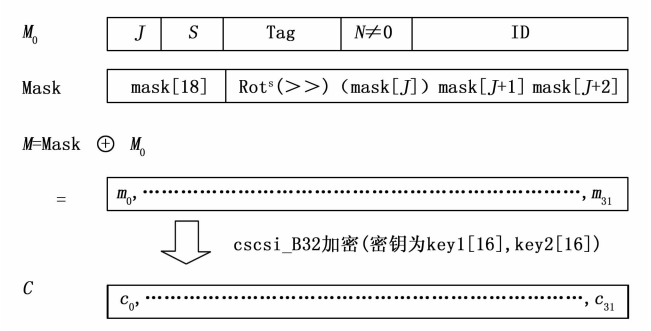

图 6　加密过程

解密 M 时，需要先用密钥字节 mask［18］同 M 的前 8 比特做模 2 加，得到 J 和 S，然后才能利用 J 和 S 解密 M 的后 24 比特。

3.4　检验码

信号在传输过程中会有各种各样的干扰，如串扰、混扰、异步干扰、同步干扰以及噪声的影响等等。这会使得信号在接收时会有可能出错。一个好的检验码除了可以判断信号是否接收正确外，还可以对一定数量的错码进行纠正。

在这里我们选择一种 Reed-Solomon（RS）纠错码[20-22]。它是一种多进制的循环纠错编码，具有很强的纠正随机误码和突发性误码的能力。

RS 纠错码的生成多项式的公式为：

$$g(x)=\prod_{i=1}^{2v}(x+a^i)=\sum_{i=1}^{2v}g_i x^i$$

一个定义在 $GF(2^m)$（伽罗瓦域）上的可纠正 v 个错误的 RS 纠错码 RS（n，k）的参数定义如下：

码长：$n=2^m-1$ 符号 或 $n(2^m-1)$ 比特。

信息段：k 符号或 km 比特。

监督段：$n-k=2v$ 符号 或 $m(n-k)$ 比特。

最小码距：$d=2v+1$ 符号 或 $m(2v+1)$ 比特。

RS 码的编码方式与一般循环码的编码方式是完全一样的。即用信息码多项式 $m_{k-1}x^{k-1}+m_{k-2}x^{k-2}+\cdots+m_0$ 升 x^{n-k} 位后去除生成多项式 $g(x)$，所得余式 $r(x)$ 为监督多项式，将监督多项式置于升 x^{n-k} 位的信息式项式后，就形成 RS 码。这样的 RS 码可以纠 v 个错误符号。

由于 RS 码是一种线性循环分组码，因此 RS 码具有如下特性：

1）允许在一定范围内随意减少或增加冗余校验数目，当冗余度发生变化时，算法可以通过调整删除操作来进行译码；

2）RS 的最小汉明距离与冗余检验位数成正比，即校验码的纠错能力随冗余度的增加而增加。

为了提高检验的性能还可以采用 CRC 检验与 RS 纠错码相结合的方式，对接收到的信号进行循环冗余检验以及纠检错。

4　实验结果与分析

这里对核心内容算法安全性进行了分析，主要从总密钥量保证、对分组密码保护和对系统消息重放的保护 3 个方面论证了本技术的安全性。

4.1　总密钥量保证

原始询问包 M_0 的加密过程如下：

pre _ encode ()：$M_0\rightarrow M$，密钥字节组 mask［19］，密钥量 152 比特。

cscsi _ B32 ()：$M\rightarrow C$，密钥字节组 key1［16］，key2［16］，密钥量 256 比特。

如果两部分密钥无关，密钥量为 408 比特；考虑到两部分密钥有部分比特重用，实际密钥量不低于 330 比特。

攻击者在获取了两组以上密文后，可通过穷举猜测密钥破译，判据是解密出的原始询问包 M_0 包含相同的 ID。此种蛮力破译的时间复杂度将大于 $O(2^{330})$，显然不可行。

4.2　前置“掩码加密”对分组密码 cscsi _ B32 的保护

由于 cscsi _ B32 加密的明文为 M，而 M 没有 ID 这一明显特征，所以无法直接对 cscsi _ B32 实施基于已知“明文－密文”对的攻击，包括差分攻击、线性攻击、差分—线性攻击。如果要获取 M 的 ID 特征，需要猜测的掩码加密密钥，不是 12 比特，而是（mask［19］）$19\times 8=152$ 比特。这已经远远超出一般认为安全的 128 比特密钥的穷举复杂度 $O(2^{128})$。

4.3　对系统消息重放的保护

任何“询问－应答包”方案，都可能遭受敌方的“消息重放”攻击：敌方只要接收询问机的密文询问包，然后向对方的应答机发送该密文询问包并记录应答延时 $\tau=\tau_0+N$，τ_0 为固定延时，则可获得“延时 N—密文”（对）。此攻击甚至可以由敌手“主动发起”：伪造“密文询问包”，发向对手方应答机；如果无应答，则伪造失败；如果在延时 $\tau=\tau_0+N$ 收到应答，则伪造攻击成功，获得“延时 N—密文”（对）。

本算法考虑了关于消息重放攻击的对策。我们设计了一种“单包—带重放攻击检测”方案。在该方案里，我们没有将 DSP 的所有时间资源全部用于增加 cscsi _ B32 的迭代轮数，而是分出了 1/3 的资源时间用于重放攻击检测。这实际上提供了约 2 200 条指令用于重放检测，足够存储处理 400 条以上的已处理消息比如，处理策略可以是：如果在连续的 100 条密文询问包中出现重复，则对后出现的询问不予应答；或者，在三连询（三连续询问包）中，如果出现重复包，则判为攻击包。

5　结束语

敌我识别在现代战争中有着不可或缺的作用，它是明辨敌我，减少误伤，多兵种联合作战的重要手段。采用激光技术是实现运动目标间敌我识别的有效方法之一。为了提高识别准确度，减少干扰，提高保密程度，本文提出了一种基于加密模式的协同式激光敌我识别技术。

本技术通过对伪随机数产生、扩频、加密算法和检验码的研究，深入阐述了基于加密模式的协同式激光敌我识别

（下转第 255 页）