对简化轮数的SNAKE(2)算法的碰撞攻击

邱丰品 卫宏儒 潘锦航
(北京科技大学数理学院 北京 100083)

摘 要 为了研究简化轮数的SNAKE(2)算法抵抗碰撞攻击的能力,根据算法的一个等价结构,给出了SNAKE(2)算法的一个6轮区分器。通过在此区分器前后加适当的轮数,对7/8/9轮的SNAKE(2)算法实施了攻击。其攻击的数据复杂度依次为$O(2^6)$、$O(2^{6.52})$、$O(2^{15})$,时间复杂度依次为$O(2^{9.05})$、$O(2^{18.32})$、$O(2^{26.42})$,攻击结果优于对SNAKE(2)算法的Square攻击。

关键词 SNAKE(2)算法,碰撞攻击,等价结构,区分器,复杂度
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.9.028

Collision Attack on Reduced-round SNAKE(2)

QIU Feng-pin WEI Hong-ru PAN Jin-hang
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract In order to research the ability of SNAKE(2) algorithm against the collision attack, a 6-round distinguisher of SNAKE(2) algorithm based on an equivalent structure of it was proposed. Attacks on 7/8/9 rounds of SNAKE(2) were performed by adding proper rounds before or after the 6-round distinguisher. The data complexities are $O(2^6)$, $O(2^{6.52})$, $O(2^{15})$, and the time complexities are $O(2^{9.05})$, $O(2^{18.32})$, $O(2^{26.42})$. The results are better than that of Square attack.

Keywords SNAKE(2) algorithm, Collision attack, Equivalent structure, Distinguisher, Complexity

1 引言

碰撞攻击[1]最早由Gilbert等在分析Rijndael算法[2]的安全性时提出,该攻击主要利用了生日悖论的原理。近年来,该攻击成功分析了Camellia[3]、FOX[4]、CLEFIA[5]和Zodiac[6]等分组密码算法,并取得了较好的分析结果。

SNAKE(2)算法是由Lee等学者在JW-ISC1997上提出的一个Feistel型分组密码,有SNAKE(1)和SNAKE(2)两个版本。两个版本的算法对差分分析、线性分析都是可证明安全的,且对高阶差分攻击和插值攻击是免疫的[7,8]。孙兵等分析了SNAKE(2)算法抵抗不可能差分攻击的能力,利用算法的9轮不可能差分,对简化轮数的SNAKE(2)应用了不可能差分攻击[9]。张鹏等利用SNAKE(2)算法的等价结构构造了5轮区分器,对6轮SNAKE(2)算法应用SQUARE攻击[10]。2012年魏悦川等人对简化轮数的SNAKE(2)算法进行了中间相遇攻击[11]。2014年郑雅菲指出文献[10]中的错误5轮Square区分器,利用算法原结构与其等价结构,构造了一个新的6轮Square区分器,并对7轮、8轮、9轮的SNAKE(2)算法进行了攻击[12]。

本文研究了SNAKE(2)算法抵抗碰撞攻击的能力。在等价结构的基础上构造了该算法的一个6轮区分器,利用该区分器对7、8、9轮的SNAKE(2)算法进行了攻击。

2 SNAKE(2)算法

SNAKE是Feistel型分组密码,在提交的算法中,设计者给出了具有不同轮函数的两个版本:SNAKE(1)和SNAKE(2)。SNAKE(i)有4个参数(m,s,w,r),其中m为S盒的输入输出比特数,s表示轮函数中S盒的个数,w表示算法的分组长度,r表示算法的轮数。

本文只研究SNAKE(2)算法,并且参数的具体值为:$m=8$,$s=4$,$w=64$。算法的轮函数如图1所示。

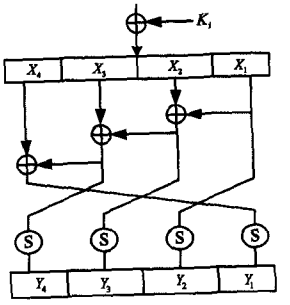

图1 SNAKE(2)算法的轮函数

算法通过迭代i次轮变换构成,设第i轮的输入为(L_{i-1},R_{i-1}),轮密钥为$K_i=(K_{i,1},K_{i,2},K_{i,3},K_{i,4})$,则一轮轮变换可定义如下:

到稿日期:2014-09-22 返修日期:2014-12-13 本文受国家自然科学基金(61272476),内蒙古自治区科技创新引导奖励资金(2012)资助。
邱丰品(1990-),女,硕士,主要研究方向为密码学,E-mail:1206472106@qq.com;卫宏儒(1963-),男,副教授,主要研究方向为数学、信息安全与密码学、物联网关键技术,E-mail:weihr@ustb.edu.cn(通信作者)。

$$\begin{cases} L_i = R_{i-1} \oplus F(L_{i-1} \oplus K_i) \\ R_i = L_{i-1} \end{cases}$$

其中，轮函数 F 将 (X_4, X_3, X_2, X_1) 映射为 (Y_4, Y_3, Y_2, Y_1)，具体定义如下：

$$\begin{cases} Y_1 = S(X_1 \oplus X_2 \oplus X_3 \oplus X_4) \\ Y_2 = S(X_1) \\ Y_3 = S(X_1 \oplus X_2) \\ Y_4 = S(X_1 \oplus X_2 \oplus X_3) \end{cases}$$

S 为有限域上的逆函数，定义如下：

$$S(x) = \begin{cases} x^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

本文不考虑密钥扩展算法的影响，因此这里不详细介绍密钥扩展算法，相关细节请参见文献[7]。

3 SNAKE(2)算法的6轮区分器

2010年，张鹏等给出了 Zodiac 算法的 4 种等价结构。2014年，刘青等利用其中的一个等价结构对 Zodiac 算法进行了碰撞攻击并取得了比较好的攻击结果。由于 SNAKE(2)算法与 Zodiac 算法结构相同，也属于 KPS 型 Feistel 密码，因此可得到 SNAKE(2)算法与 Zodiac 算法相同的 4 种等价结构。本文利用文献[6]中对 Zodiac 算法进行碰撞攻击所构造的区分器用到的等价结构来构造 SNAKE(2)算法的 6 轮区分器。

由于 SNAKE(2)算法轮函数的具体结构为 $K \to P \to S$ 型，设轮函数的输入为 A，则其输出为：

$$F(A) = S(P(A \oplus K)) = S(P(A) \oplus P(K)) = S(P(A) \oplus K')$$

其中，$K' = P(K)$。此时，可以将轮函数的原结构看为 $P \to K \to S$ 型(这里也用 K 来记以上的等价密钥 K')。

利用上述等价结构构造 SNAKE(2)算法的 6 轮区分器，以下是 SNAKE(2)算法 6 轮区分器的详细计算过程：

令 L_{i-1} 和 R_{i-1} 为第 i 轮 SNAKE(2)的输入，选取

$L_0 = (c_8, c_7, c_6, c_5)$，$R_0 = (x, x, c_2, c_1)$

其中，变量 x 取自 F_2^8，且取相同的值进行遍历，$c_i \in F_2^8 (i = 1, 2, 5, 6, 7, 8)$ 表示任意选定的常值字节。

第一轮的输出为：

$L_1 = (x \oplus a_4, x \oplus a_3, a_2, a_1)$

$R_1 = L_0 = (c_8, c_7, c_6, c_5)$

其中，$a_i (1 \leqslant i \leqslant 4)$ 仅和 $c_i (i = 1, 2, 5, 6, 7, 8)$ 及轮密钥 K_1 有关，因此在密钥取定时，a_i 均是常数。

令 $y = S(x \oplus a_3 \oplus a_2 \oplus a_1 \oplus K_{2,1}) = S(x \oplus a_0)$，第二轮的输出为：

$L_2 = (y \oplus c_8, b_3, b_2, b_1)$

$R_2 = L_1 = (x \oplus a_4, x \oplus a_3, a_2, a_1)$

其中，$b_i (1 \leqslant i \leqslant 3)$ 仅和 $a_i (1 \leqslant i \leqslant 4)$、$c_i (5 \leqslant i \leqslant 7)$ 及轮密钥 K_2 有关，因此在密钥取定的情况下，b_i 均是常数。

令 $z = S(y \oplus c_8 \oplus b_3 \oplus b_2 \oplus b_1 \oplus K_{3,4}) = S(y \oplus d_0)$，则第三轮的输出为：

$L_3 = (x \oplus d_4, x \oplus d_3, d_2, z \oplus a_1)$

$R_3 = L_2 = (y \oplus c_8, b_3, b_2, b_1)$

其中，$d_i (2 \leqslant i \leqslant 4)$ 仅和 $b_i (1 \leqslant i \leqslant 3)$、$a_i (2 \leqslant i \leqslant 4)$ 及轮密钥 K_3 有关，因此在密钥取定的情况下，d_i 均是常数。

第四轮的输出为：

$L_4 = (\Delta, \Delta, \Delta, S(z \oplus d_4 \oplus d_3 \oplus d_2 \oplus a_1 \oplus K_{4,4}) \oplus b_1) = (\Delta, \Delta, \Delta, S(z \oplus c_0) \oplus b_1)$

$R_4 = L_3$

其中，Δ 表示本文不关心的字节，下同。

第五轮的输出为：

$L_5 = (\Delta, \Delta, S(S(z \oplus c_0) \oplus d_0) \oplus d_2, \Delta) = (\Delta, \Delta, u, \Delta)$

$R_5 = L_4$

其中，d_0 仅和 b_1、$K_{5,3}$ 有关，因此在密钥取定的情况下，d_0 是常数。

此时，第六轮输出的右半部分为：

$R_6 = L_5 = (\Delta, \Delta, u, \Delta)$

具体的 6 轮区分器如表 1 所列。

表 1 SNAKE(2)算法的 6 轮区分器

L ‖ R	L	R
$L_0 \| R_0$	c_8, c_7, c_6, c_5	x, x, c_2, c_1
$L_1 \| R_1$	$x \oplus a_4, x \oplus a_3, a_2, a_1$	c_8, c_7, c_6, c_5
$L_2 \| R_2$	$y \oplus c_8, b_3, b_2, b_1$	$x \oplus a_4, x \oplus a_3, a_2, a_1$
$L_3 \| R_3$	$x \oplus d_4, x \oplus d_3, d_2, z \oplus a_1$	$y \oplus c_8, b_3, b_2, b_1$
$L_4 \| R_4$	$\Delta, \Delta, \Delta, S(z \oplus c_0) \oplus b_1$	$x \oplus d_4, x \oplus d_3, d_2, z \oplus a_1$
$L_5 \| R_5$	$\Delta, \Delta, u, \Delta$	$\Delta, \Delta, \Delta, S(z \oplus c_0) \oplus b_1$
$L_6 \| R_6$	$\Delta, \Delta, \Delta, \Delta$	$\Delta, \Delta, u, \Delta$

性质 令明文输入形如 $(c_8, c_7, c_6, c_5, x, x, c_2, c_1)$，其中 $c_i \in F_2^8 (i = 1, 2, 5, 6, 7, 8)$ 表示任意选定的常值字节，x 表示变量且取相同的值进行遍历。如果明文输入仅有 x 不同，其余参数字节均相同，将此明文加密 6 轮，得到 $R_{6,2}$ 是两两互异的字节。

证明：因为 SNAKE(2)算法的 S 盒是双射，所以当 x 取不同值且其余参数字节均相同时，$y = S(x \oplus a_3 \oplus a_2 \oplus a_1 \oplus K_{2,1}) = S(x \oplus a_0)$ 也互不相同；进一步可知 $z = S(y \oplus d_0)$ 也取不同的值，所以 $R_{6,2} = u = S(S(z \oplus c_0) \oplus d_0) \oplus d_2$ 是两两互异的字节。

4 对 7/8/9 轮 SNAKE(2)算法的碰撞攻击

原结构中的轮函数为 $K \to P \to S$ 型结构，验证猜测密钥时，密钥后面有 P 置换进行扩散，因此会使复杂度大大增加。如果采用等价的 $P \to K \to S$ 型结构，则每个字节均可单独验证相应的密钥字节。因此，在攻击时将 $K \to P \to S$ 型结构等价成 $P \to K \to S$ 型结构，会使复杂度大大降低。

4.1 对 7 轮 SNAKE(2)算法的碰撞攻击

利用 6 轮区分器对 7 轮到 9 轮的 SNAKE(2)算法进行碰撞攻击，7 轮攻击的具体过程如图 2 所示。

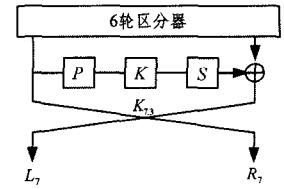

图 2 SNAKE(2)算法的 7 轮攻击

第 1 步 选取 58 个明文 $Pi (1 \leqslant i \leqslant 58)$，使得 $Pi = (c_8,$

$c_7, c_6, c_5, x_i, x_i, c_2, c_1$)。其中，$c_i \in F_2^8 (i=1,2,5,6,7,8)$表示任意选定的常值字节，$x_i$ 取自 F_2^8，且取相同的值进行遍历，相应的密文记为 $Ci(1 \leqslant i \leqslant 58)$。

第 2 步　猜测 $K_{7,3}$，对密文集合进行解密，得到 $R_{6,2}$ 的 58 个值 $Ri_{6,2}(1 \leqslant i \leqslant 58)$。检查这些值是否有碰撞，如果有，则丢弃相应的候选密钥；否则，输出相应的候选密钥。

第 3 步　对第 2 步输出的候选密钥，选择其他的明文，重复第 2 步，直到输出值唯一。

根据碰撞攻击的概率统计模型可知，部分解密 58 个密文得到对应的 $Ri_{6,2}(1 \leqslant i \leqslant 58)$ 产生碰撞的概率大于 $1-e^{-58\times57/2^9} > 1-2^{-9}$，因此，第 2 步输出错误子密钥的概率小于 2^{-9}。因为正确密钥肯定通过，而 2^8-1 个错误密钥中通过碰撞检测的个数平均为 $(2^8-1)\times2^{-9} \approx 0.5$，故通过检测的候选密钥的个数约为 1.5，因此，第 3 步只需几个明文即可。综上，攻击需 2^6 个选择明文，攻击的时间复杂度主要是由第 2 步根据猜测密钥进行部分解密运算决定的，由于一次部分解密需要计算 1 个 S 盒，因此攻击的时间复杂度约为 $58\times2^8/(7\times4) \approx 2^{9.05}$。

4.2　对 8 轮 SNAKE(2)算法的碰撞攻击

8 轮攻击是在 7 轮攻击的基础上，在算法的后面再加上一轮。为部分解密得到 $R_{6,2}$，需要猜测密钥 $K_{7,3}$ 和 $K_{8,4}$。这里选取 80 个明文，相应的密文记为 $Ci(1 \leqslant i \leqslant 80)$。部分解密 80 个密文，得到对应的 $Ri_{6,2}(1 \leqslant i \leqslant 80)$，它们产生碰撞的概率大于 $1-e^{-80\times79/2^9} > 1-2^{-17}$，因此，第 2 步输出错误子密钥的概率小于 2^{-17}。而 $2^{16}-1$ 个错误密钥中通过碰撞检测的个数平均为 $(2^{16}-1)\times2^{-17} \approx 0.5$，故通过检测的候选密钥的个数约为 1.5，因此，第 3 步只需几个明文即可。综上，攻击需 $2^{6.52}$ 个选择明文，由于一次部分解密需要计算 2 个 S 盒，因此攻击的时间复杂度约为 $80\times2^{16}\times2/(8\times4) \approx 2^{18.32}$。

4.3　对 9 轮 SNAKE(2)算法的碰撞攻击

9 轮攻击是在 8 轮攻击的基础上，在算法的前面再加上一轮，需要额外猜测一个字节的密钥，即猜测的密钥为 $K_{1,1}$、$K_{8,3}$ 和 $K_{9,4}$，攻击具体步骤如下。

第 1 步　对 $K_{1,1}$ 的每个候选值 t，选取 96 个明文 $Pi^t = (Li_0^t, Ri_0^t)(1 \leqslant i \leqslant 96)$，形如：

$$Pi^t = (Li_0^t, Ri_0^t)$$
$$= (x_i, x_i, c_2, c_1, S(x_i \oplus c_0 \oplus K_{1,1}) \oplus c_8, a_7, a_6, a_5)$$

其中，$a_i(5 \leqslant i \leqslant 7)$仅与 $c_i(i=5,6,7)$及轮密钥 K_1 有关，因此在密钥取定时，a_i 均是常数，$c_0 = c_1 \oplus c_2$ 也是常数，字节 x_i 满足 $0 \leqslant x_i \leqslant 255$。将这些明文加密 9 轮后相应的密文记为 $Ci_9^t = (Li_9^t, Ri_9^t)$。

第 2 步　猜测 $K_{8,3}$ 和 $K_{9,4}$，对 $(t, K_{8,3}, K_{9,4})$的每个候选值，解密得到 $R_{7,2}$ 的 96 个值 $Ri_{7,2}(1 \leqslant i \leqslant 96)$。检查这些值是否有碰撞，如果有，则丢弃相应的$(t, K_{8,3}, K_{9,4})$；否则，输出相应的$(t, K_{8,3}, K_{9,4})$值。

第 3 步　对第 2 步输出的每个$(t, K_{8,3}, K_{9,4})$值，选择其他的明文，重复第 2 步，直到输出的值是唯一的。

根据碰撞攻击的概率统计模型可知，部分解密 96 个密文得到对应的 $Ri_{7,2}(1 \leqslant i \leqslant 96)$ 产生碰撞的概率大于 $1-e^{-96\times95/2^9} > 1-2^{-25}$，故，第 2 步输出错误子密钥的概率小于 2^{-25}。因为正确密钥肯定通过，而 $2^{24}-1$ 个错误密钥中通过碰撞检测的个数平均为 $(2^{24}-1)\times2^{-25} \approx 0.5$，故通过检测的候选密钥的个数约为 1.5，因此，第 3 步只需几个明文即可。综上，攻击需 2^7 个选择明文，因此该 9 轮攻击的数据复杂度为 $2^7\times2^8 = 2^{15}$，时间复杂度约为 $96\times2^8\times2^{16}\times2/(9\times4) \approx 2^{26.42}$。

SNAKE(2)算法 7、8、9 轮碰撞攻击的复杂度如表 2 所列。

表 2　SNAKE(2)算法不同轮数碰撞攻击的复杂度

攻击方法	轮数	时间复杂度	数据复杂度	预计算复杂度	文献
中间相遇	7	2^6	7	2^{32}	[11]
Square 攻击	7	$2^{12.19}$	2^9	—	[12]
碰撞攻击	7	$2^{9.05}$	2^6	—	本文
中间相遇	8	2^{14}	8	2^{32}	[11]
Square 攻击	8	$2^{21.59}$	$2^{9.59}$	—	[12]
碰撞攻击	8	$2^{18.32}$	$2^{6.52}$	—	本文
中间相遇	9	2^{22}	$2^{11.2}$	2^{32}	[11]
Square 攻击	9	$2^{30.41}$	2^{10}	—	[12]
碰撞攻击	9	$2^{26.42}$	2^{15}	—	本文

结束语　本文对 SNAKE(2)算法抵抗碰撞攻击的能力进行了评估，基于 SNAKE(2)算法的等价结构构造了一个 6 轮区分器，并给出了 7 至 9 轮的攻击过程和相应的复杂度。表 2 列出了本文方法与其他方法的攻击结果比较，对于 7 轮和 8 轮 SNAKE(2)算法的攻击，本文在数据复杂度和时间复杂度方面均优于文献[12]给出的 Square 攻击；对 9 轮 SNAKE(2)算法的攻击，本文在时间复杂度方面也优于 Square 攻击。由于计算复杂度与时间复杂度是等价的，因此与中间相遇攻击相比，本文攻击不仅不需要预计算复杂度，而且计算复杂度还优于其预计算复杂度。

参 考 文 献

[1] Gilbert H, MinierM. A collision attack on 7 rounds of Rijndael [EB/OL]. 2012-10-10. http://csrc.. nist. gov/archive/aes/round2/conf3/papers/11-hgilbert. pdf

[2] Daemen J, Rijmen V. The block ciphRijndael[C]// Proceedings of the Third International Conference (CARDIS' 98). Berlin: Springer-Verlag, 2000: 277-284

[3] Wu W L, Feng D G. Collision attack on reduced-round Camellia [J]. Science in China: Series F, 2004, 48(1): 78-90

[4] 吴文玲，卫宏儒. 低轮 FOX 分组密码的碰撞-积分攻击[J]. 电子学报，2005，33(7)：1307-1310
Wu Wen-ling, Wei Hong-ru. Collision-Integral Attack of Reduced-Round FOX[J]. Acta Electronica Sinica, 2005, 33(7): 1307-1310

[5] 韩敬，张文英，徐小华. 对低轮 CLEFIA 分组密码的碰撞-Square 攻击[J]. 电子学报，2009，37(10)：2309-2313
Han Jing, Zhang Wen-ying, Xu Xiao-hua. Collision-Square Attacks on the Reduced-Round CLEFIA[J]. Acta Electronica Sinica, 2009, 37(10): 2309-2313

[6] 刘青，卫宏儒，潘伟. Zodiac 算法的碰撞攻击[J]. 计算机应用，2014，34(1)：73-77
Liu Qing, Wei Hong-ru, Pan Wei. Collision attack on Zodiac

algorithm[J]. Journal of Computer Applications, 2014, 34(1): 73-77

[7] Lee C, Cha Y. TheBlock Cipher: SNAKE with Provable Resistance against DC and LC attacks 1997[C]// Proceedings of 1997 Korea-Japan Joint Workshop on Information Security and Cryptology(JWISC'97). 1997: 3-17

[8] Moriai S, Shimoyama T, Kaneko T. Interpolation attacks of the Block Cipher: SNAKE[C]// Proc of Fast Software Encryption. 1999: 275-289

[9] Sun Bing, Qu Long-jiang, Li Chao. Impossible Differential Cryptanalysis of SNAKE[C]// Procof NSWCT'09. 2009: 63-66

[10] 张鹏,孙兵,李超. 对特殊类型 Feistel 密码的 Square 攻击[J]. 国防科技大学学报, 2010, 32(4): 137-140
Zhang Peng, Sun Bing, Li Chao. Square Attack on Some Special Feistel Ciphers[J]. Journal of National Uuniversity of Defense Technology, 2010, 32(4): 137-140

[11] 魏悦川,孙兵,李超. 对简化轮数的 SNAKE(2)算法的中间相遇攻击[J]. 计算机工程与科学, 2012, 34(6): 28-31
Wei Yue-chuan, Sun Bing, Li Chao. A Meet-in-the-Middle Attack on Reduced-Round SNAKE(2)[J]. Computer Engineering and Science, 2012, 34(6): 28-31

[12] 郑雅菲,卫宏儒. SNAKE(2)算法新的 Square 攻击[J]. 计算机科学, 2014, 41(3): 169-171
Zheng Ya-fei, Wei Hong-ru. New Square Attack on SNAKE(2)[J]. Computer Science, 2014, 41(3): 169-171

(上接第 146 页)

$|R_{1,-1}|$,$|R_0|+|R_2|+|R_4|$,$|R_{1,1}|$,$|R_{3,1}|$次。下面给出$|R_i|$($i=0,1,2,3,4$)的具体值。

根据引理 4 关于指数和的结果,有以下 4 个等式:

$$|R_0|+|R_2|+|R_4|+|R_{1,1}|+|R_{1,-1}|+|R_{3,1}|+|R_{3,-1}|=p^m-1$$

$$p^{\frac{m+e}{2}}(|R_{1,1}|-|R_{1,-1}|)+p^{\frac{m+3e}{2}}(|R_{3,1}|-|R_{3,-1}|)=p^m$$

$$p^{m+e}(|R_{1,1}|+|R_{1,-1}|)+p^{m+3e}(|R_{3,1}|+|R_{3,-1}|)=p^{2m}$$

$$p^{\frac{3(m+e)}{2}}(|R_{1,1}|-|R_{1,-1}|)+p^{\frac{3(m+3e)}{2}}(|R_{3,1}|-|R_{3,-1}|)=p^{2m+(3k,m)}$$

根据以上等式、引理 5 和定理 3 的结论,可以求出

$$|R_{1,-1}|=p^{m-e-1}-p^{2e-1}(a_{n-2}-|R_4|)-\frac{p^{\frac{m+3e}{2}}-p^{\frac{m-3e}{2}+(3k,m)}}{p^{2e+1}-2}$$

$$|R_{1,1}|=p^{m-e-1}-p^{2e-1}(a_{n-2}-|R_4|)+\frac{p^{\frac{m+3e}{2}}-p^{\frac{m-3e}{2}+(3k,m)}}{p^{2e+1}-2}$$

$$|R_0|+|R_2|+|R_4|=2^m-1-2^{m-e}+(2^{2e}-1)a_{n-2}+(1-2^{2e})|R_4|$$

$$|R_{3,-1}|=\frac{a_{n-2}-|R_4|}{2}-\frac{p^{\frac{m-3e}{2}+(3k,m)}-p^{\frac{m-e}{2}}}{p^{3e+1}-p^{e+1}}$$

$$|R_{3,1}|=\frac{a_{n-2}-|R_4|}{2}+\frac{p^{\frac{m-3e}{2}+(3k,m)}-p^{\frac{m-e}{2}}}{p^{3e+1}-p^{e+1}}$$

其中,$|R_4|$和a_{n-2}如式(4)和式(5)所示。

结束语 当 p 为奇素数、k 为偶数且 m 序列的级数 $m=6s+3$ 时,本文对采样因子为 $d=(p^{2k}+1)/(p^k+1)$的 m 序列互相关函数进行了研究。避免了传统的求解有限域上多元高次方程的方法,利用有限域上二次型理论,证明了其互相关函数值为五值。通过引入矩阵结合方案,把对互相关值分布问题的研究转化为对二次型秩之间关系的研究,最终得出了该类 p 元 m 序列之间五值互相关函数的完整分布。

参 考 文 献

[1] Golomb S W. Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences [J]. Information Sciences, 1968(1): 87-109

[2] Kang J W, Whang Y, Ko H B, et al. Generalized Cross-Correlation Properties of Chu Sequences[J]. IEEE Transcations on Information Theory, 2012, 58(1): 438-444

[3] Dobbertin H, Felke P, Helleseth T, et al. Binary m-sequences with three-valued cross correlation: a proof of Welch's conjecture[J]. IEEE Transcations on Information Theory, 2000, 46(1): 4-8

[4] Dobbertin H, Felke P, Helleseth P, et al. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums [J]. IEEE Transcations on Information Theory, 2006, 52(2): 613-627

[5] Kasami T. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes[J]. Information and Control, 1971, 18(4): 369-394

[6] Dobbertin H. Another proof of Kasami's theorem[J]. Designs, Codes and Cryptography, 1999, 17(1): 177-180

[7] Johansen A, Helleseth T. A family of m-sequences with five-valued cross correlation[J]. IEEE Transcations on Information Theory, 2009, 55(2): 880-887

[8] Johansen A, Helleseth T, Kholosha A. Further results on m-sequences with five-valued cross correlation[J]. IEEE Transcations on Information Theory, 2009, 55(12): 5792-5802

[9] Bracken C. Designs, Codes, Spin Models and the Walsh Transform[D]. Nat. Univ. Ireland(NUI), Ma, 2004

[10] Helleseth T, Gong G. New Nonbinary Sequences With Ideal Two-Level Autocorrelation[J]. IEEE Transcations on Information Theory, 2002, 48(11): 2868-2872

[11] Tang X H, Udaya P, Fan P Z. A New Family of Nonbinary Sequences With Three-Level Correlation Property and Large Linear Span[J]. IEEE Transcations on Information Theory, 2005, 51(8): 2906-2914

[12] Gong G, Helleseth T, Hu H G. A Three-Valued Walsh Transform From Decimations of Helleseth-Gong Sequences[J]. IEEE Transcations on Information Theory, 2012, 58(2): 1158-1162

[13] Helleseth T. Some results about the cross-correlation function between two maximal linear sequences[J]. Discrete Mathematics, 1976, 16(3): 209-232

[14] Delsarte P, Goethals J M. Alternating bilinear forms over GF(q) [J]. Journal of Combinational Theory, Series A, 1975, 19: 26-50

[15] Egawa Y. Association schemes of quadratic forms[J]. Journal of Combinational Theory: Series A, 1985, 38: 1-14