doi:10.11887/j.cn.202101009 http://journal.nudt.edu.cn

NORX算法中非线性组件的移位参数选取准则研究*

沈 璇,何 俊
(国防科技大学 信息通信学院,湖北 武汉 430010)

摘 要:NORX算法是进入凯撒竞赛第三轮的15个认证加密候选算法之一,该算法的唯一非线性组件由异或、与和移位操作组成。从非线性逼近和循环分析两个密码学性质研究移位参数的选取准则,证明了可变移位函数的非线性逼近概率为三值函数,并得到了移位参数取1时具有最佳的非线性逼近性质;给出了可变移位函数的循环概率表达式,并证明了对于任意非零的移位参数其最大循环概率均相同。由上述分析结果可知,NORX算法中非线性组件的移位参数取1时达到了最佳的非线性逼近和循环性质。该结果可应用于NORX算法的安全性分析中,同时也能为设计类似算法提供理论指导。

关键词:认证加密算法;凯撒竞赛;NORX算法;非线性逼近;循环分析
中图分类号:TN918 **文献标志码**:A **文章编号**:1001-2486(2021)01-066-06

Research on design rationale of the shift parameter in nonlinear component of NORX

SHEN Xuan, *HE Jun*
(College of Information and Communication, National University of Defense Technology, Wuhan 430010, China)

Abstract: NORX is one of the fifteen candidates selected for the third round of the CAESAR (authenticated encryption: security, applicability, and robustness) competition. And its only nonlinear component is made up of XOR, AND and shift operations. The design rationale of the shift parameter of NORX from the perspective of nonlinear approximation and rotational properties were studied. On the one hand, the nonlinear approximation probability of the shift function is theoretically proved to be a three-valued function. When the shift parameter is 1, this function possesses the best nonlinear property. On the other hand, the rotational probability of the shift function is formulated. And it is proved that the maximal rotational probability is the same for all nonzero shift parameters. From the above results, the NORX has the best nonlinear approximation and rotational properties when the shift parameter takes 1. The results can be of reference to the analysis of NORX and can give theoretical guidance when designing similar ciphers.

Keywords: authenticated encryption cipher; CAESAR; NORX algorithm; nonlinear approximation; rotational cryptanalysis

凯撒竞赛(Competition for Authenticated Encryption: Security, Applicability, and Robustness, CAESAR)[1]是由著名密码学家Bernstein发起的一项寻求安全高效认证加密算法的全球性活动。该竞赛得到了美国国家标准技术研究所(National Institute of Standard and Technology, NIST)的大力支持。CAESAR于2014年开始,第一轮共收到了来自全球各个密码团队提交的57个候选算法,其中有29个候选算法进入了第二轮,15个候选算法进入了第三轮,并最终在2018年针对不同的应用场景评选出了7个获胜算法。NORX算法[2]是进入该竞赛第三轮的候选算法。

自NORX算法发布以来,许多密码学者从不同角度对其安全性进行了研究。Aumasson等[3]在Latincrypt 2014上首先分析了其内部置换函数的差分特性。进一步,Das等[4]给出了内部置换函数的高阶差分特性。接着,Bagheri等[5]在FSE 2016上给出了NORX置换函数缩减到2轮的密钥恢复攻击。后来,Biryukov等[6]在2017年给出了NOXR置换函数的一些非随机特性。最近,Chaigneau等[7]利用NORX算法置换函数的对称性质构造了唯密文伪造攻击和密钥恢复攻击。

在密码算法中,非线性组件的选择对于密码算法的安全强度具有至关重要的作用[8]。为了提高硬件的实现效率,NORX算法的唯一非线性

* **收稿日期**:2019-03-26
基金项目:国家自然科学基金资助项目(62002370, 61702537)
作者简介:沈璇(1990—),男,湖北荆门人,讲师,博士,E-mail: shenxuan_08@163.com;
何俊(通信作者),男,教授,博士,硕士生导师,E-mail: hejun17c@nudt.edu.cn

组件采用异或、与和移位操作的组合来代替模加操作。在这种组合中,移位参数的选取具有十分重要的作用。为了研究的方便,称 NORX 算法中非线性组件移位参数任取的函数为可变移位函数。在 NORX 算法的设计文档中,设计者将移位参数选取为 1,但是并没有从算法安全性的角度进行说明。因此,本文通过研究可变移位函数的密码学性质来探讨 NORX 算法中非线性组件移位参数的选取准则。

模加操作是密码算法常用的非线性组件,它具有良好的密码学性质。因此,本文将研究可变移位函数对模加函数的非线性逼近性质。当可变移位函数取不同移位参数时,若其逼近概率越高,则说明它越接近模加操作,其非线性逼近性质也越好。此外,循环分析方法[9-10]是近些年来针对模加循环异式(Addition, Rotation, XDR, ARX)型密码算法十分有效的一种分析方法,它对包括 BLAKE2[11]、Keccak[12]、Skein[13] 等在内的许多 Hash 函数具有十分显著的攻击效果。不仅如此,由循环分析方法发展而来的循环异或分析方法[14-15]也是最近针对 ARX 型密码算法进行安全性分析的热点。循环分析方法的关键是研究循环对通过算法非线性组件的循环概率。因此,本文还将研究可变移位函数的循环概率表达式。若其最大循环概率越低,则它抵抗循环攻击的能力越强。

在非线性逼近性质方面,本文证明了随着移位参数 k 的变化,可变移位函数的逼近概率是一个关于移位参数 k 的三值函数。其中:当 $k=0$ 时,逼近概率最小;当 $k=1$ 时,逼近概率最大;当 $k\geqslant 2$ 时,逼近概率是与移位参数 k 无关的常值。在循环性质方面,本文从理论上给出了不同移位参数下可变移位函数循环概率的显性表达式,并且证明了对于任意非零移位参数而言,可变移位函数均能够取得相同的最大循环概率。这两类密码学性质的研究在一定程度上揭示了移位参数的选取准则,对设计类似非线性组件的算法具有较强的指导意义。

1　预备知识

1.1　符号标记

表 1 给出了后文涉及的符号标记。

表 1　文中涉及的符号含义

Tab. 1　Some notations used in this paper

符号	含义
X,Y	n 比特串
$X\oplus Y$	逐比特异或
$X+Y$	模 2^n 加
$X\ll k$	X 向左移位 k 比特
$X\ggg r$	X 向右循环移位 r 比特
$\#M$	集合 M 的元素个数

1.2　NORX 算法简介

NORX 算法是由密码学者 Aumasson 等在 2014 年提交给 CAESAR 竞赛的一个轻量级认证加密算法,该算法的整体框架采用海绵结构。NORX 算法的内部置换函数是基于 ARX 设计的,它的算法设计思路来源于密码算法 ChaCha[16] 和 BLAKE2[17]。为了实现轻量化,NORX 算法并没有采用密码学性能良好的模加操作,而是采用异或、与和移位操作的组合来代替,即用 $X\oplus Y\oplus XY\ll 1$ 代替 $X+Y$。考虑到本文的研究只涉及 NORX 算法中的非线性组件,有关算法其他细节的描述参见文献[2]。另外,设计者在算法文档中只给出了非线性组件 $X\oplus Y\oplus XY\ll 1$ 来源于等式

$$X+Y=(X\oplus Y)+(XY)\ll 1$$

但并未从密码安全的角度对 $X\oplus Y\oplus XY\ll 1$ 中移位参数的选择进行说明。本文主要从密码学角度对 NORX 算法中非线性组件移位参数的选择进行探讨。为了在后文中描述方便,令可变移位函数为:

$$f_k(X,Y)=(X\oplus Y)\oplus((XY)\ll k)$$

注意到当 $k=1$ 时,$f_1(X,Y)$ 即是 NORX 算法中的非线性组件 $X\oplus Y\oplus XY\ll 1$。

2　可变移位函数的非线性逼近性质分析

本节主要研究了可变移位函数的非线性逼近性质。在这一节中,先研究了可变移位函数与模加函数相等时的等价条件,然后利用该条件计算可变移位函数逼近模加函数的精确概率值,最后对本节进行了总结。

首先,给出如下引理。

引理　令 $X=(x_{n-1},x_{n-2},\cdots,x_1,x_0)$, $Y=(y_{n-1},y_{n-2},\cdots,y_1,y_0)$, 这里 $x_i,y_i\in F_2$。并且设 $g(X,Y)=X+Y$, $f_k(X,Y)=(X\oplus Y)\oplus((XY)\ll k)$,则有:

$$g(X,Y)=$$
$$\begin{cases} f_0(X,Y)\Leftrightarrow x_iy_i=0, i=0,1,2,\cdots,n-1 \\ f_1(X,Y)\Leftrightarrow x_iy_i(x_{i+1}\oplus y_{i+1})=0, i=0,1,\cdots,n-3 \\ f_k(X,Y)\Leftrightarrow x_iy_i=0, k\geqslant 2, i=0,1,2,\cdots,n-2 \end{cases} \tag{1}$$

证明：因为 $g(X,Y)=X+Y=X\oplus Y\oplus C$，这里 $C=(c_{n-1},\cdots,c_1,c_0)$ 且有：

$$\begin{cases} c_0=0 \\ c_i=c_{i-1}(x_{i-1}\oplus y_{i-1})\oplus x_{i-1}y_{i-1}, 1\leqslant i\leqslant n-1 \end{cases} \tag{2}$$

因此，$f_k(X,Y)=g(X,Y)\Leftrightarrow C=(XY)\ll k$。下面通过逐比特比较的方法，分 $k=0$，$k=1$，$k\geqslant 2$ 三种情况进行讨论。

情形 1：当 $k=0$ 时，$C=XY$，即

$$\begin{cases} c_0=0=x_0y_0 \\ c_1=c_0(x_0\oplus y_0)\oplus x_0y_0=x_1y_1 \\ c_2=c_1(x_1\oplus y_1)\oplus x_1y_1=x_2y_2 \\ \vdots \\ c_{n-1}=c_{n-2}(x_{n-2}\oplus y_{n-2})\oplus x_{n-2}y_{n-2}=x_{n-1}y_{n-1} \end{cases} \tag{3}$$

则有 $x_iy_i=0, i=0,1,2,\cdots,n-1$。

情形 2：当 $k=1$ 时，$C=(XY)\ll 1$，即

$$\begin{cases} c_0=0=0 \\ c_1=c_0(x_0\oplus y_0)\oplus x_0y_0=x_0y_0 \\ c_2=c_1(x_1\oplus y_1)\oplus x_1y_1=x_1y_1 \\ \vdots \\ c_{n-1}=c_{n-2}(x_{n-2}\oplus y_{n-2})\oplus x_{n-2}y_{n-2}=x_{n-2}y_{n-2} \end{cases} \tag{4}$$

则有 $x_iy_i(x_{i+1}\oplus y_{i+1})=0, i=0,1,2,\cdots,n-3$。

情形 3：当 $2\leqslant k\leqslant n-1$ 时，$C=(XY)\ll k$，即

$$\begin{cases} c_0=0=0 \\ c_1=c_0(x_0\oplus y_0)\oplus x_0y_0=0 \\ \vdots \\ c_{k-1}=c_{k-2}(x_{k-2}\oplus y_{k-2})\oplus x_{k-2}y_{k-2}=0 \\ c_k=c_{k-1}(x_{k-1}\oplus y_{k-1})\oplus x_{k-1}y_{k-1}=x_0y_0 \\ c_{k+1}=c_k(x_k\oplus y_k)\oplus x_ky_k=x_1y_1 \\ \vdots \\ c_{n-1}=c_{n-2}(x_{n-2}\oplus y_{n-2})\oplus x_{n-2}y_{n-2}=x_{n-1-k}y_{n-1-k} \end{cases} \tag{5}$$

则有 $x_iy_i=0, i=0,1,2,\cdots,n-2$。因此，上述引理成立。 □

利用上述引理，可以得到如下定理。

定理 1 对于 $0\leqslant k\leqslant n-1$，令 $a=2+\sqrt{2}$，$b=2-\sqrt{2}$ 并且

$$\begin{cases} T_k^n\triangleq\#\{(X,Y)\in F_2^{2n}\mid X+Y=(X\oplus Y)\oplus((XY)\ll k)\} \\ p_k\triangleq\dfrac{T_k^n}{2^{2n}} \end{cases} \tag{6}$$

则有

$$\begin{cases} p_0=\left(\dfrac{3}{4}\right)^n \\ p_k=\left(\dfrac{3}{4}\right)^{n-1}, 2\leqslant k\leqslant n-1 \end{cases} \tag{7}$$

且

$$p_1=\frac{(7+5\sqrt{2})a^{n-3}+(7-5\sqrt{2})b^{n-3}}{2^{2(n-1)}} \tag{8}$$

证明：根据引理得到如下情形。

情形 1：当 $k=0$ 时，$X+Y=(X\oplus Y)\oplus XY\Leftrightarrow x_iy_i=0, i=0,1,2,\cdots,n-1$。对于任意的 $x_iy_i=0$，(x_i,y_i) 可取 $(0,0)$、$(0,1)$、$(1,0)$ 这 3 种情况，因此

$$\begin{cases} T_0^n=3^n \\ p_0=\dfrac{3^n}{2^{2n}}=\left(\dfrac{3}{4}\right)^n \end{cases} \tag{9}$$

情形 2：当 $2\leqslant k\leqslant n-1$ 时，$X+Y=(X\oplus Y)\oplus((XY)\ll k)\Leftrightarrow x_iy_i=0$，这里 $i=0,1,\cdots,n-2$。当 $0\leqslant i\leqslant n-2$ 时，对于任意的 $x_iy_i=0$，(x_i,y_i) 可取 $(0,0)$、$(0,1)$、$(1,0)$ 这三种情况。当 $i=n-1$ 时，x_i、y_i 无限制，可取所有可能的 4 种情况。因此

$$\begin{cases} T_k^n=4\times 3^{n-1} \\ p_k=\dfrac{4\times 3^{n-1}}{2^{2n}}=\left(\dfrac{3}{4}\right)^{n-1} \end{cases} \tag{10}$$

情形 3：当 $k=1$ 时，因为

$$X+Y=(X\oplus Y)\oplus((XY)\ll 1)\Leftrightarrow$$
$$\begin{cases} x_0y_0(x_1\oplus y_1)=0 \\ x_1y_1(x_2\oplus y_2)=0 \\ \vdots \\ x_{n-3}y_{n-3}(x_{n-2}\oplus y_{n-2})=0 \end{cases} \tag{11}$$

令 $F_n(x_0,\cdots,x_{n-3},x_{n-2},y_0,\cdots,y_{n-3},y_{n-2})=0$ 表示上述方程组，并且令

$$\begin{cases} N_{(0,0)}^n=\#\{F_n(x_0,x_1,\cdots,x_{n-3},0,y_0,y_1,\cdots,y_{n-3},0)=0\} \\ N_{(0,1)}^n=\#\{F_n(x_0,x_1,\cdots,x_{n-3},0,y_0,y_1,\cdots,y_{n-3},1)=0\} \\ N_{(1,0)}^n=\#\{F_n(x_0,x_1,\cdots,x_{n-3},1,y_0,y_1,\cdots,y_{n-3},0)=0\} \\ N_{(1,1)}^n=\#\{F_n(x_0,x_1,\cdots,x_{n-3},1,y_0,y_1,\cdots,y_{n-3},1)=0\} \end{cases} \tag{12}$$

因为 $0\oplus 0=1\oplus 1, 0\oplus 1=1\oplus 0$，所以

$$\begin{cases} N_{(0,0)}^n=N_{(1,1)}^n \\ N_{(0,1)}^n=N_{(1,0)}^n \end{cases} \tag{13}$$

记方程组 $F_n(x_0,x_1,\cdots,x_{n-2},y_0,y_1,\cdots,y_{n-2})=0$ 解的数目为 N^n,则有:

$$\begin{aligned}N^n &= N^n_{(0,0)}+N^n_{(0,1)}+N^n_{(1,0)}+N^n_{(1,1)}\\ &=2N^n_{(0,0)}+2N^n_{(0,1)}\end{aligned}\tag{14}$$

注意到 (x_{n-1},y_{n-1}) 可以取 (0,0)、(0,1)、(1,0)、(1,1)这 4 种情况,因此有

$$T^n_1=4\times N^n=8(N^n_{(0,0)}+N^n_{(0,1)})\tag{15}$$

因为 $F_n(x_0,x_1,\cdots,x_{n-2},y_0,y_1,\cdots,y_{n-2})=0$ 当且仅当

$$\begin{cases}F_{n-1}(x_0,x_1,\cdots,x_{n-3},y_0,y_1,\cdots,y_{n-3})=0\\ x_{n-3}y_{n-3}(x_{n-2}\oplus y_{n-2})=0\end{cases}\tag{16}$$

所以

$$\begin{cases}N^n_{(0,0)}=N^{n-1}_{(0,0)}+N^{n-1}_{(0,1)}+N^{n-1}_{(1,0)}+N^{n-1}_{(1,1)}\\ \quad\quad=2N^{n-1}_{(0,0)}+2N^{n-1}_{(0,1)}\\ N^n_{(0,1)}=N^{n-1}_{(0,0)}+N^{n-1}_{(0,1)}+N^{n-1}_{(1,0)}\\ \quad\quad=N^{n-1}_{(0,0)}+2N^{n-1}_{(0,1)}\\ N^n_{(1,0)}=N^{n-1}_{(0,0)}+N^{n-1}_{(0,1)}+N^{n-1}_{(1,0)}\\ \quad\quad=N^{n-1}_{(0,0)}+2N^{n-1}_{(0,1)}\\ N^n_{(1,1)}=N^{n-1}_{(0,0)}+N^{n-1}_{(0,1)}+N^{n-1}_{(1,0)}+N^{n-1}_{(1,1)}\\ \quad\quad=2N^{n-1}_{(0,0)}+2N^{n-1}_{(0,1)}\end{cases}\tag{17}$$

化简上述方程组得:

$$\begin{aligned}\begin{pmatrix}N^n_{(0,1)}\\ N^n_{(0,0)}\end{pmatrix}&=\begin{pmatrix}2&1\\2&2\end{pmatrix}\begin{pmatrix}N^{n-1}_{(0,1)}\\ N^{n-1}_{(0,0)}\end{pmatrix}\\ &=\begin{pmatrix}2&1\\2&2\end{pmatrix}^{n-3}\begin{pmatrix}N^3_{(0,1)}\\ N^3_{(0,0)}\end{pmatrix}\end{aligned}\tag{18}$$

注意当 $n=3$ 时,方程组即为 $x_0y_0(x_1\oplus y_1)=0$。因此

$$\begin{cases}N^3_{(0,1)}=3\\ N^3_{(0,0)}=4\end{cases}\tag{19}$$

则

$$\begin{pmatrix}N^n_{(0,1)}\\ N^n_{(0,0)}\end{pmatrix}=\begin{pmatrix}2&1\\2&2\end{pmatrix}^{n-3}\begin{pmatrix}3\\4\end{pmatrix}\triangleq\boldsymbol{A}^{n-3}\begin{pmatrix}3\\4\end{pmatrix}\tag{20}$$

令

$$\begin{cases}\boldsymbol{Q}=\begin{pmatrix}1&1\\\sqrt{2}&-\sqrt{2}\end{pmatrix}\\ \boldsymbol{\Lambda}=\begin{pmatrix}2+\sqrt{2}&0\\0&2-\sqrt{2}\end{pmatrix}\end{cases}\tag{21}$$

则有 $\boldsymbol{A}=\boldsymbol{Q}\boldsymbol{\Lambda}\boldsymbol{Q}^{-1}$。因此

$$\begin{aligned}\begin{pmatrix}N^n_{(0,1)}\\ N^n_{(0,0)}\end{pmatrix}&=\boldsymbol{A}^{n-3}\begin{pmatrix}3\\4\end{pmatrix}=\boldsymbol{Q}\boldsymbol{\Lambda}\boldsymbol{Q}^{-1}\boldsymbol{Q}\boldsymbol{\Lambda}\boldsymbol{Q}^{-1}\cdots\boldsymbol{Q}\boldsymbol{\Lambda}\boldsymbol{Q}^{-1}\begin{pmatrix}3\\4\end{pmatrix}\\ &=\boldsymbol{Q}\boldsymbol{\Lambda}^{n-3}\boldsymbol{Q}^{-1}\begin{pmatrix}3\\4\end{pmatrix}\\ &=\frac{1}{2}\begin{pmatrix}(3+2\sqrt{2})a^{n-3}+(3-2\sqrt{2})b^{n-3}\\ (4+3\sqrt{2})a^{n-3}-(3\sqrt{2}-4)b^{n-3}\end{pmatrix}\end{aligned}\tag{22}$$

则

$$\begin{cases}T^n_1=4\times N^n=8(N^n_{(0,0)}+N^n_{(0,1)})\\ \quad\quad=4\times[(7+5\sqrt{2})a^{n-3}+(7-5\sqrt{2})b^{n-3}]\\ p_1=\dfrac{T^n_1}{2^{2n}}=\dfrac{(7+5\sqrt{2})a^{n-3}+(7-5\sqrt{2})b^{n-3}}{2^{2(n-1)}}\end{cases}\tag{23}$$

□

从定理 1 中可得,对于任意 n 比特长的两个数据块,能够计算出不同移位参数 k 下可变移位函数的逼近概率,如表 2 所示。

表 2　可变移位函数在不同移位参数下的逼近概率

Tab. 2　Approximation probability of variable shift function when k takes different values

	$P/\%$				
	$n=4$	$n=8$	$n=16$	$n=32$	$n=64$
$k=0$	31.64	10.01	1.00	0.010	1.01×10^{-6}
$k=1$	75.00	39.84	11.23	0.891	5.61×10^{-3}
$k\geqslant2$	42.19	13.25	1.34	0.013	1.36×10^{-6}

从定理 1 和表 2 可知:当 $k=1$ 时,$f_k(X,Y)$ 的逼近概率最大;当 $k=0$ 时,$f_k(X,Y)$ 的逼近概率最小。此外,当 $k\geqslant2$ 时,不管移位参数取何值,$f_k(X,Y)$ 的逼近概率均相同,并且其概率大小为中间值。当移位参数 $f_k(X,Y)$ 给定时,数据块的规模 n 越大,$f_k(X,Y)$ 的逼近概率越小。考虑到逼近概率越高,非线性逼近的性质越好,在 NORX 算法中移位参数取 1 达到了最佳的非线性逼近。

3　可变移位函数的循环性质分析

上一节研究了可变移位函数的非线性逼近性质,本节主要研究该函数的循环性质。首先介绍关于函数的循环对概念,然后给出一个关于可变移位函数循环概率的定理,最后对本节进行总结。

定义[9]　令 $G:\mathbb{F}_2^{2n}\to\mathbb{F}_2^{n}$ 是一个向量值布尔函数并且 X、Y 均是 n 比特串,r 为任意的循环参数,$1\leqslant r\leqslant n-1$,则满足式(24)时称 $G(X,Y)$ 是一个关于函数 G 的循环对:

$$G(X,Y)\ggg r=G(X\ggg r,Y\ggg r)\tag{24}$$

下面给出一个关于可变移位函数循环概率的定理。

定理 2 令 X、Y 是 n 比特串，移位参数 k 满足 $0 \leqslant k \leqslant n-1$，循环参数 r 满足 $1 \leqslant r \leqslant n-1$，并且 $f_k(X,Y) = (X \oplus Y) \oplus ((XY) \ll k)$，则 (X,Y) 关于可变移位函数 $f_k(X,Y)$ 循环对的概率为：

$$P(f_k(X,Y) \gg r = f_k(X \gg r, Y \gg r)) = \left(\frac{9}{16}\right)^{\min(k,r)} \tag{25}$$

证明：根据 $f_k(X,Y)$ 的具体形式知

$$f_k(X,Y) \gg r = ((X \gg r) \oplus (Y \gg r)) \oplus ((XY) \ll k) \gg r \tag{26}$$

并且

$$f_k(X \gg r, Y \gg r) = (X \gg r) \oplus (Y \gg r) \oplus ((X \gg r)(Y \gg r) \ll k) \tag{27}$$

因此

$$f_k(X,Y) \gg r = f_k(X \gg r, Y \gg r) \Leftrightarrow ((XY) \ll k) \gg r = (X \gg r)(Y \gg r) \ll k \tag{28}$$

令 $Z = XY$，则

$$f_k(X,Y) \gg r = f_k(X \gg r, Y \gg r) \Leftrightarrow (Z \ll k) \gg r = (Z \gg r) \ll k \tag{29}$$

当 $k = 0$ 时，

$$f_0(X,Y) \gg r = f_0(X \gg r, Y \gg r) \tag{30}$$

始终成立，即

$$P(f_0(X,Y) \gg r = f_0(X \gg r, Y \gg r)) = 1 \tag{31}$$

当 $1 \leqslant k \leqslant n-1$ 时，分 $r \leqslant k$ 和 $r > k$ 两种情况进行讨论。

情形 1：当 $r \leqslant k$，则有

$$\begin{cases} (Z \ll k) \gg r = \\ (\overbrace{000000\cdots0}^{r}\ \overbrace{z_{n-1-k}z_{n-2-k}\cdots z_r}^{n-(k+r)}\ \overbrace{z_{r-1}z_{r-2}\cdots z_0}^{r}\ \overbrace{000000\cdots0}^{k-r}) \\ (Z \gg r) \ll k = \\ (\underbrace{z_{n-k+(r-1)}z_{n-k+(r-2)}\cdots z_{n-k}}_{r}\ \underbrace{z_{n-1-k}z_{n-2-k}\cdots z_r}_{n-(k+r)}\ \underbrace{00\cdots0}_{r}\ \underbrace{00\cdots0}_{k-r}) \end{cases} \tag{32}$$

根据式(29)可得 $z_j = 0$，这里

$$j = 0,1,\cdots,r-1,n-k,n-k+1,\cdots,n-k+(r-1) \tag{33}$$

考虑到 $P(z_j = x_j y_j = 0) = \frac{3}{4}$，则有

$$P(f_k(X,Y) \gg r = f_k(X \gg r, Y \gg r)) = \left(\frac{3}{4}\right)^{2r} = \left(\frac{9}{16}\right)^{r} \tag{34}$$

情形 2：当 $r > k$，则有

$$\begin{cases} (Z \ll k) \gg r = \\ (\overbrace{z_{r-k-1}z_{r-k-2}\cdots z_0}^{r-k}\overbrace{000\cdots0}^{k}\ \overbrace{z_{n-1-k}z_{n-2-k}\cdots z_r}^{n-(k+r)}\ \overbrace{z_{r-1}z_{r-2}\cdots z_{r-k}}^{k}) \\ (Z \gg r) \ll k = \\ (\underbrace{z_{r-k-1}z_{r-k-2}\cdots z_0}_{r-k}\ \underbrace{z_{n-1}z_{n-2}\cdots z_{n-k}}_{k}\ \underbrace{z_{n-1-k}z_{n-2-k}\cdots z_r}_{n-(k+r)}\ \underbrace{000\cdots0}_{k}) \end{cases} \tag{35}$$

根据式(29)可得 $z_j = 0$，这里

$$j = r-k, r-k+1, \cdots, r-1, n-k, \cdots, n-1 \tag{36}$$

同样 $P(z_j = x_j y_j = 0) = \frac{3}{4}$，则有

$$P(f_k(X,Y) \gg r = f_k(X \gg r, Y \gg r)) = \left(\frac{3}{4}\right)^{2k} = \left(\frac{9}{16}\right)^{k} \tag{37}$$

因此，上述定理成立。 □

由定理 2 知：当 $k = 0$ 时，$f_0(X,Y)$ 的循环概率为 1；当 $1 \leqslant k \leqslant n-1$ 时，$f_k(X,Y)$ 的循环概率在循环参数 $r = 1$ 时均能达到最大，并且最大概率均为 9/16。注意到文献[9]中引理 11 只是本文定理 2 中关于移位参数 $k = 1$ 时的推论。

在密码算法中，非线性组件的循环概率越低，越有利于抵抗循环攻击。因此，从循环概率值的分布情况看，移位参数取非零值时对应的可变移位函数具有更好的循环性质。进一步，不管非零移位参数取何值，可变移位函数在循环参数 $r = 1$ 时均能达到相同的最大循环概率。

4 结论

本文从非线性逼近和循环分析两方面研究了 NORX 算法中非线性函数的移位参数选取准则。研究结果表明：从抵抗密码攻击的角度看，当移位参数为 0 时，可变移位函数的非线性逼近和循环性质均最差；当移位参数为 1 时，其非线性逼近和循环性质均最好；当移位参数为其他值时，其具有相同效果的非线性逼近和循环性质。因此，NORX 算法中唯一非线性组件的移位参数取 1 时达到了最佳的非线性逼近和循环性质。本文对 NORX 算法中非线性函数移位参数选取准则的探讨，不仅有助于提高 NORX 算法的安全性分析结果，而且还对设计类似组件函数的算法提供了理论指导。

参考文献(References)

[1] Cryptographic Competitions. Competition for authenticated encryption: security, applicability, and robustness [EB/OL]. [2019 - 02 - 16]. http://competitions.cr.yp.to/Caesar.html.

[2] AUMASSON J P, JOVANOVIC P, NEVES S. NORX: parallel and scalable AEAD [C]// Proceedings of European Symposium on Research in Computer Security, 2014, 8713: 19 - 36.

[3] AUMASSON J P, JOVANOVIC P, NEVES S. Analysis of NORX: investigating differential and rotational properties [C]// Proceedings of International Conference on Cryptology and Information Security in Latin America, 2014, 8895: 306 -

324.

[4] DAS S, MAITRA S, MEIER W. Higher order differential analysis of NORX[EB/OL]. [2019 - 06 - 16]. http://eprint. iacr. org/2015/186.

[5] BAGHERI N, HUANG T, JIA K T, et al. Cryptanalysis of reduced NORX[C]// Proceedings of Revised Selected Papers of the 23rd International Conference on Fast Software Encryption, 2016, 9783: 554 - 574.

[6] BIRYUKOV A, UDOVENKO A, VELICHKOV V. Analysis of the NORX core permutation[EB/OL]. [2019 - 06 - 16]. http://eprint. iacr. org/2017/034.

[7] CHAIGNEAU C, FUHR T, GILBERT H, et al. Cryptanalysis of NORX v2. 0[J]. Journal of Cryptology, 2019, 32: 1423 - 1447.

[8] 赵光耀, 成磊, 李瑞林, 等. 低轮 PUFFIN 算法的积分攻击[J]. 国防科技大学学报, 2015, 37(6): 129 - 134.
ZHAO Guangyao, CHENG Lei, LI Ruilin, et al. Integral cryptanalysis on reduced-round PUFFIN[J]. Journal of National University of Defense Technology, 2015, 37(6): 129 - 134. (in Chinese)

[9] KHOVRATIOVICH D, NIKOLIC I. Rotational cryptanalysis of ARX[C]// Proceedings of International Conference on Fast Software Encryption, 2010, 6147: 333 - 346.

[10] KHOVRATOVICH D, NIKOLIĆ I, PIEPRZYK J, et al. Rotational cryptanalysis of ARX revisited[C]// Proceedings of International Conference on Fast Software Encryption, 2015, 9054: 519 - 536.

[11] GUO J, KARPMAN P, NIKOLIĆ I, et al. Analysis of BLAKE2[C]// Proceedings of the Cryptographer's Track at the RSA Conference, 2014: 402 - 423.

[12] MORAWIECKI P, PIEPRZYK J, SREBRNY M. Rotational cryptanalysis of round-reduced Keccak[C]// Proceedings of International Conference on Fast Software Encryption, 2013: 241 - 262.

[13] KHOVRATOVICH D, NIKOLIĆI, RECHBERGER C. Rotational rebound attacks on reduced Skein[C]// Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2010: 1 - 19.

[14] LIU Y, WITTE G, RANEA A, et al. Rotational-XOR cryptanalysis of reduced-round SPECK[J]. IACR Transactions on Symmetric Cryptology, 2017(3): 24 - 36.

[15] ASHUR T, LIU Y. Rotational cryptanalysis in the presence of constants[J]. IACR Transactions on Symmetric Cryptology, 2016(1): 57 - 70.

[16] BERNSTEIN D J. ChaCha, a variant of Salsa20[EB/OL]. [2019 - 06 - 26]. http://cr. yp. to/chacha. html.

[17] AUMASSON J P, NEVES S, O'HEARN Z W, et al. BLAKE2: simpler, smaller, fast as MD5[C]// Proceedings of International Conference on Applied Cryptography and Network Security, 2013, 7954: 119 - 135.