对 NBC-128 的安全性分析

杨江帅[1],陈怀凤[1],鲍金凤[2],康潇文[3]
(1.中国电子信息产业集团有限公司第六研究所,北京 100083;
2.北京联合大学旅游学院,北京 110101;3.61428 部队,北京 100097)

摘 要:NBC 算法是由徐洪等人设计的基于广义 Feistel 结构的分组密码算法,支持 128/128、128/256 和 256/256 3 种分组和密钥尺寸,其非线性部分采用 16 bit S 盒。对分组长度为 128 bit 的两个 NBC 版本算法进行了改进的安全性分析。针对不可能差分攻击,修正了原有分析过程,可以分析 17 轮 NBC-128/256、15 轮 NBC-128/128;对于多维零相关攻击,扩展了攻击轮数,可以分析 19 轮 NBC-128/256、16 轮 NBC-128/128,针对 NBC-128/256 的结果在轮数上是已知最长的;对于积分攻击,给出了新的 12 轮积分路线,需要的数据量低于原有结果。

关键词:NBC-128 算法;不可能差分分析;零相关线性分析;积分分析
中图分类号:TN918;TP309.7　　**文献标识码**:A　　**DOI**:10.16157/j.issn.0258-7998.201005

中文引用格式:杨江帅,陈怀凤,鲍金凤,等. 对 NBC-128 的安全性分析[J].电子技术应用,2021,47(4):91-96.
英文引用格式:Yang Jiangshuai,Chen Huaifeng,Bao Jinfeng,et al. Cryptanalysis of NBC-128[J]. Application of Electronic Technique,2021,47(4):91-96.

Cryptanalysis of NBC-128

Yang Jiangshuai[1],Chen Huaifeng[1],Bao Jinfeng[2],Kang Xiaowen[3]
(1.The 6th Research Institute of China Electronics Corporation,Beijing 100083,China;
2.The Institute of Tourism,Beijing Union University,Beijing 110101,China;3.61428 Military,Beijing 100097,China)

Abstract:NBC is a family of block ciphers using Generalized Feistel structure, designed by Xu Hong et al. There are three block and key sizes,i.e.,128/128, 128/256 and 256/256. A 16-bit Sbox is involved in the cipher as the non-linear component. This paper makes improved cryptanalysis on the two NBC versions with block size 128.Using impossible differential cryptanalysis, the corrected results are given which cover 17-round NBC-128/256 and 15-round NBC-128/128. The attack rounds of multi-dimensional zero-correlation linear cryptanalysis are expanded, which covers 19-round NBC-128/256 and 16-round NBC-128/128. The 19-round attack is the longest as far as we know. Also, new 12-round integral distinguishers are proposed, which require less data compared to the existing integral attacks.

Key words:NBC-128;impossible differential cryptanalysis;zero-correlation linear cryptanalysis;integral cryptanalysis

0 引言

为推动我国密码算法的设计及实现技术发展,培养密码学人才,中国密码学会于 2018 年启动了全国密码算法设计竞赛,共 22 个分组密码算法进入第一轮评估,有 10 个算法进入第二轮评估[1]。其中 ublouk[2]、FESH[3]、TANGRAM[4]和 SPRING[5]算法采用 SPN 结构,ANT[6]、SMBA[7]和 Raindrop[8]算法采用 Feistel 结构,NBC[9-10]和 FBC[11]算法采用广义 Feistel 结构。最终,uBlock 和 Ballet 获得一等奖,FESH、ANT 和 TANGRAM 获得二等奖,Raindrop、NBC、FBC、SMBA 和 SPRING 获得三等奖。

本文将针对 NBC 算法进行安全性分析,NBC 算法由徐洪等人设计并提出,支持 128/128 bit、128/256 bit、256/256 bit 3 种分组和密钥尺寸。该算法的非线性 F 函数部分采用 16 bit S 盒,由 16 级非线性反馈移位寄存器迭代而成,具有较低的硬件实现成本。差分分析[12]、线性分析[13]、不可能差分分析[14]、零相关线性分析[15-17]和积分分析[18]等是分析分组密码算法安全性的主要方法,算法设计者针对 NBC 算法的各个版本给出了初步分析结果。

针对 NBC-128 算法的两个版本,设计者的研究表明[9-10]:NBC-128 算法不存在 9 轮有效的线性特征和差分特征。对于不可能差分攻击和零相关线性攻击,设计者在第二轮的提交文档[9]中给出了 10 轮的区分器及详细的攻击过程,后来在新版本中[10]将两类路线各扩展一轮,并相应地将可攻击轮数扩展了一轮。利用不可能差分分析方法,设计者攻击 19 轮 NBC-128/256、17 轮 NBC-128/128,利用零相关线性分析方法,可以攻击 16 轮 NBC-128/256、15 轮 NBC-128/128。对于积分分析方法,设计者给出了 12 轮的积分路线,数据复杂度为 2^{127},

可以攻击 18 轮 NBC-128/256、16 轮 NBC-128/128。

本文将针对 NBC-128/256 和 NBC-128/128 两个版本进行独立的安全分析，主要从不可能差分分析、零相关分析和积分分析 3 种分析方法出发开展研究，相关的攻击结果比较见表 1。主要贡献如下：

(1)给出 NBC-128 算法的两类 11 轮不可能差分路线，利用其中一类不可能差分路线进行了 NBC-128/256 和 NBC-128/128 算法的不可能差分攻击。本文认为文献[9]中的密钥猜测过程少猜了几个子密钥，达到预期攻击轮数的计算复杂度将超过穷搜密钥复杂度。表 1 给出了修正后的数据和计算复杂度估计。

(2)给出 NBC-128 算法的两类 11 轮零相关线性路线，基于其中一类零相关线性路线构造多维零相关区分器，在卡方统计法多维零相关攻击模型下进行了 NBC-128/256 和 NBC-128/128 算法的密钥恢复攻击，对于 NBC-128/256 算法可以攻击到 19 轮，对于 NBC-128/128 算法可以攻击到 16 轮，比已知的多维零相关攻击分别扩展了 3 轮和 1 轮。

(3)给出了 NBC-128 算法基于分离特性的新型 12 轮积分路线，并进行了积分攻击，需要的数据复杂度仅为 2^{125}，优于原有积分攻击的数据复杂度。

表 1 对 NBC-128 的攻击结果比较

算法版本	攻击类型	攻击轮数	数据复杂度	时间复杂度	参考文献
NBC-128/256	ID	18、19	--	--	[9],[10]
	ID	17	2^{102}CP	$2^{210.5}$	本文
	MDZC	15、16	$2^{114.8}$KP	2^{236}	[9],[10]
	MDZC	19	$2^{124.6}$KP	$2^{249.9}$	本文
	Integral	18	2^{127}CP	$2^{206.15}$	[9],[10]
	Integral	18	2^{125}CP	2^{240}	本文
NBC-128/128	ID	16、17	--	--	[9],[10]
	ID	15	2^{100}CP	$2^{116.51}$	本文
	MDZC	14、15	$2^{114.8}$KP	$2^{109.1}$	[9],[10]
	MDZC	16	$2^{123.3}$KP	$2^{124.11}$	本文
	Integral	16	2^{127}CP	$2^{93.9}$	[9],[10]
	Integral	16	2^{125}CP	2^{112}	本文

注：(1)攻击类型中，ID 表示不可能差分攻击，MDZC 表示多维零相关攻击，Integral 表示积分攻击；(2)数据复杂度中，CP 表示选择明文，KP 表示已知明文。

1 NBC-128 算法描述

NBC-128 算法采用 8 分支广义 Feistel 结构，迭代 32 轮。每个分支 16 bit，每轮存在 4 个 F 函数，F 函数的输入为输入分支与轮密钥的异或值，经过 1 个 16 bit 的 S 盒查表，输出与另外一个分支异或，最后经过一个分支位置变换操作。在 NBC-128 算法的最后一轮，F 函数的输出与相邻分支异或后，不再进行分支位置变换操作。设第 i 轮的输入为 $\boldsymbol{X}^i=(X_0^i,X_1^i,\cdots,X_7^i)$，输出为 $\boldsymbol{X}^{i+1}=(X_0^{i+1},X_1^{i+1},\cdots,X_7^{i+1})$，第 i 轮的子密钥为 $\boldsymbol{K}^i=(K_0^i,K_1^i,\cdots,K_3^i)$，其一轮变换的结构如图 1 所示。

NBC-128 算法存在256 bit 和 128 bit 两个密钥尺寸，本文的主要研究与密钥扩展算法关联不大，此处不再给出 NBC-128 算法的密钥扩展算法。

2 对 NBC-128 算法的不可能差分分析

2.1 NBC-128 算法的 11 轮不可能差分路线

本节给出 NBC-128 算法的两类新型 11 轮不可能差分路线，其中第一类不可能差分路线在文献[10]中已被提出。

命题 1：(NBC-128 的第一类 11 轮不可能差分路线)

$(0,\Delta,0,0,0,0,0,0)/\!\rightarrow(0,0,0,\Delta,0,\Gamma,0,0)$是 NBC-128 算法的一条 11 轮不可能差分路线，最后一轮不包括位置置换，其中 $\Delta,\Gamma\neq 0,\Delta\neq\Gamma$，图 2 给出了该不可能差分路线的矛盾产生过程，图中 * 表示差分非零，?表示差分不确定，空白位置表示差分为 0。

命题 2：(NBC-128 的第二类 11 轮不可能差分路线)

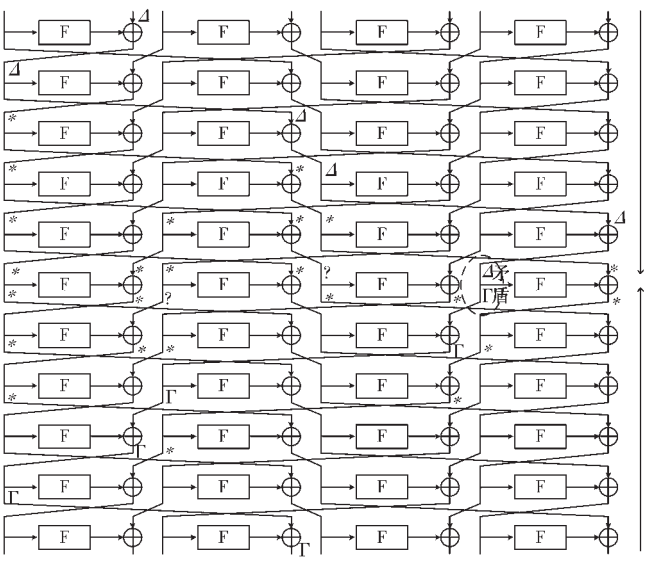

图 2 NBC-128 的第一类 11 轮不可能差分路线

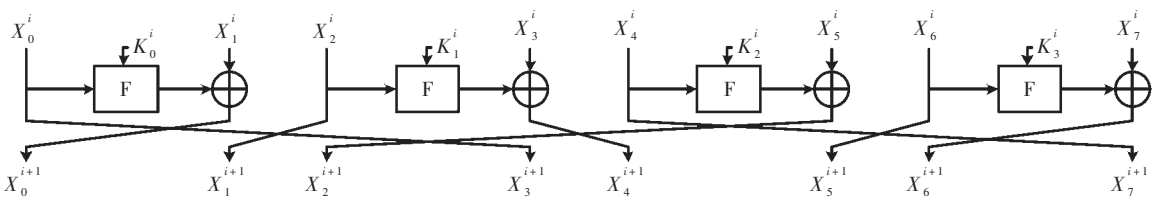

图 1 NBC-128 的轮函数

$(0,\Delta,0,0,0,0,0,0)/\!\rightarrow(0,0,0,\Delta,0,\Gamma,0,0)$是 NBC-128 算法的一条 11 轮不可能差分路线，最后一轮不包括位置置换，其中 $\Delta,\Gamma\neq 0$，且 Δ 与 Γ 相互独立，图 3 给出了该不可能差分路线的矛盾产生过程，图中 * 表示差分非零，? 表示差分不确定，空白位置表示差分为 0。

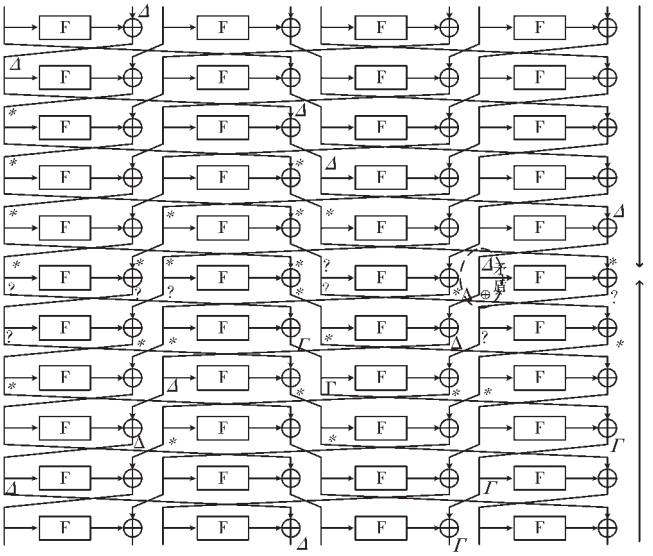

图 3 NBC-128 的第二类 11 轮不可能差分路线

实际上，NBC-128 算法为每一轮具有 4 个 F 函数的广义 Feistel 结构，通过移动输入差分、输出差分中非零差分的位置，可以构造一系列类似的 11 轮不可能差分路线，从结构以及攻击能力方面考虑与上述路线等价，此处不再给出具体细节。

2.2 对 NBC-128/256 算法的不可能差分攻击

在文献[9]、[10]中的不可能差分分析过程中，认为作者漏猜了几个子密钥，因此实际攻击效果达不到预期的那么好。利用第一类 11 轮不可能差分路线，本文对 NBC-128/256 算法进行修正的不可能差分攻击，图 4 给出了攻击过程中的差分及符号，主要攻击过程如下：

(1)构造 Structure：$S_c=\{X=(X_0,X_1,X_2,X_3,X_4,X_5,X_6,X_7)\mid(X_0,X_4,X_5)\}=c$，其他位置遍历}，则每个 Structure 中有 2^{80} 个元素，可以构造约 2^{159} 组符合$(0,*,*,*,0,0,\Delta,*)$的差分对(Δ 取遍非零可能值)。

(2)通过构造 m 个 Structure，可以构造 $2^t=2^{159}\times m\times 2^{-48}$ 个明文差分符合$(0,*,*,*,0,0,\Delta,*)$，相应的密文差分符合$(0,*,0,0,*,*,\Gamma,*)$，$\Gamma\neq\Delta$，$\Gamma\neq 0$ 的正确数据对。

(3)按照表 2 进行密钥猜测及错误对筛除，对于每一个错误密钥，每一个正确对被留下的概率为 $2^{-16\times 8}=2^{-128}$。对于错误密钥，没有差分对留下的概率为$p=(1-2^{-128})2^t\approx 2^{-114\times(t-128)}$，即剩余约 $2^{256}\times p$ 个候选正确密钥。

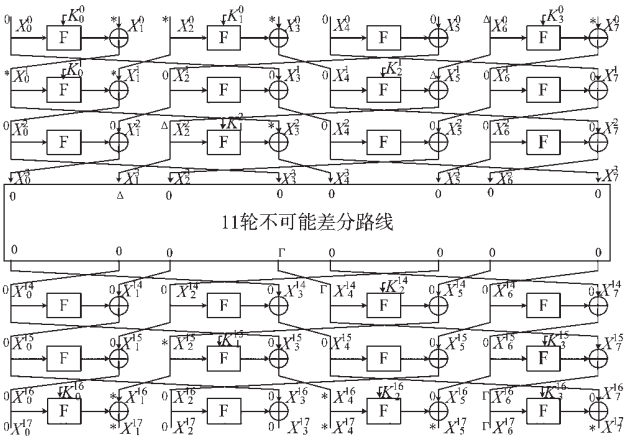

图 4 NBC-128/256 的 17 轮不可能差分攻击

(4)利用两个明文对进行候选正确密钥的穷搜，完成密钥恢复攻击。

复杂度估计：选取 $m=2^{22}$ 个 Structure，共需要 2^{102} 个选择明文。此时，步骤(3)的总计算复杂度约为 $2^{t+80}=2^{159+22-48+80}=2^{213}$ 次简单计算，步骤(4)的穷搜复杂度为 $2^{256}\times p\approx 2^{209.82}$ 次 17 轮加密。总时间复杂度约为 $2^{210.5}$ 次 17 轮加密。

表 2 对 NBC-128/256 的不可能差分攻击

状态差分	猜测密钥	筛除概率	余下对数	时间
$X_0^0(0),X_1^0(*),X_2^0(*),X_3^0(*),X_4^0(0),X_5^0(0),X_6^0(\Delta),X_7^0(*)$			2^{-t}	
$X_0^0(0),X_1^0(*),X_6^0(\Delta),X_7^0(*),X_1^1(*),X_4^1(0)$	K_1^0	2^{-16}	2^{t-16}	2^{t-16}
$X_0^0(0),X_1^0(*),X_1^1(*),X_4^1(0),X_5^1(\Delta),X_6^1(0)$	K_3^0	2^{-16}	2^{t-32}	
$X_4^1(0),X_5^1(\Delta),X_0^2(0),X_3^2(*)$	K_0^0,K_0^1	2^{-16}	2^{t-48}	2^{t-16}
$X_1^2(\Delta),X_4^3(0)$	K_2^1,K_1^2	2^{-16}	2^{t-64}	$2^{t+32}\ 2^{t+48}$
$X_0^{17}(0),X_1^{17}(*),X_2^{17}(*),X_3^{17}(*),X_4^{17}(0),X_5^{17}(0),X_6^{17}(\Delta),X_7^{17}(*)$			2^{t-64}	
$X_0^{17}(0),X_1^{17}(*),X_4^{16}(*),X_5^{16}(0),X_4^{16}(*),X_5^{16}(0)$	K_2^{16}	2^{-16}	2^{t-80}	2^{t+48}
$X_0^{17}(0),X_1^{17}(*),X_4^{16}(*),X_5^{16}(0),X_6^{16}(\Gamma),X_7^{16}(0)$	K_3^{16}	2^{-16}	2^{t-96}	2^{t+48}
$X_5^{16}(0),X_6^{16}(\Gamma),X_2^{15}(*),X_3^{15}(0)$	K_0^{16},K_1^{15}	2^{-16}	2^{t-112}	2^{t+64}
$X_4^{14}(\Gamma),X_5^{14}(0)$	K_3^{15},K_2^{14}	2^{-16}	2^{t-128}	2^{t+80}

2.3 对 NBC-128/128 算法的不可能差分攻击

对于 NBC-128/128 算法，主密钥长度仅有128 bit，只能在区分器前后各添加两轮进行 15 轮密钥恢复攻击。

通过选择 2^{52} 个 $S_c=\{X=(X_0,X_1,X_2,X_3,X_4,X_5,X_6,X_7)\mid(X_2,X_3,X_4,X_6,X_7)\}=c$，其他位置遍历}类型的结构体，可以构造 $2^{52+95-80}=2^{67}$ 个输入差分符合$(*,*,0,0,0,\Delta,0,0)$、输出差分符合$(0,*,0,0,*,0,\Gamma,0)$、$\Gamma\neq\Delta$ 的数据对，用类似于上述的密钥猜测及错误对筛除，对于错误密钥，无差分对剩余的概率为 $p=(1-2^{-64})2^{67}\approx 2^{-11.52}$。错误对筛除的总计算量约为 $2^{67+48}=2^{115}$ 次简单计算，剩余约 $2^{128}\times 2^{-11.52}=2^{116.48}$，总时间复杂度约为 $2^{116.51}$ 次15 轮

加密。需要的数据量为 $2^{52+48}=2^{100}$ 个选择明文。

3 对 NBC-128 算法零相关线性分析

3.1 NBC-128 算法的 11 轮零相关线性路线

本节给出 NBC-128 算法的两类新型 11 轮零相关线性路线，其中第一类零相关线性路线在文献[10]中已被提出。

命题 3：(NBC-128 的第一类 11 轮零相关线性路线) $(\alpha,0,0,0,0,0,0,0)\rightarrow(0,0,0,0,\beta,0,0,0)$ 是 NBC-128 算法的一条 11 轮零相关路线，最后一轮不包括位置置换，其中 $\alpha,\beta\neq 0,\alpha\neq\beta$，图 5 给出了该零相关线性路线的矛盾产生过程，* 表示掩码非零，? 表示掩码不确定，空白位置表示掩码为 0。

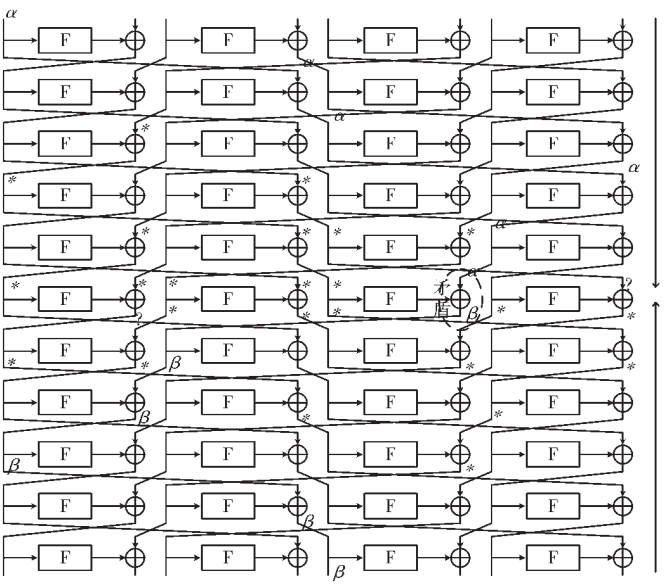

图 5 NBC-128 的第一类 11 轮零相关路线

命题 4：(NBC-128 的第二类 11 轮零相关线性路线) $(\alpha,0,0,0,0,0,0,0)\rightarrow(0,0,0,0,\alpha,0,\beta,0)$ 是 NBC-128 算法的一条 11 轮零相关线性路线，最后一轮不包括位置置换，其中 $\alpha,\beta\neq 0$，且 α 与 β 相互独立，图 6 给出了该零相关线性路线的矛盾产生过程，* 表示掩码非零，? 表示掩码不确定，空白位置表示掩码为 0。

3.2 对 NBC-128/256 的多维零相关线性攻击

通过选取特定形式的输入掩码和输出掩码，可以构造 $t=12$ 维的多维零相关线性区分器，例如选取 $\alpha=0^4||0^6||*^6,\beta=0^4||*^6||0^6$ 的零相关路线。在该区分器前后各添加 4 轮进行 19 轮算法的密钥恢复攻击，相关状态及猜测的密钥情况如图 7 所示，具体攻击过程如下：

(1)对于 N 个已知明文及其相应的密文数据，猜测 128 bit 密钥 $K_0^0,K_1^0,K_2^0,K_2^1,K_0^{18},K_2^{18},K_3^{18},K_2^{17}$ 可以计算得到 $X_{0,1,2}^1,X_2^2,X_{1,5,6}^{18},X_5^{17}$，对于 X_2^2、X_5^{17}，根据区分器的输入、输出掩码表示，共需存储 t bit 即可，因此可将中间状态存储于 2^{96+t} 个计数器中。该步骤需要的计算复杂度约为 $N\times 2^{128}$ 次 8 个 S 盒的查表。

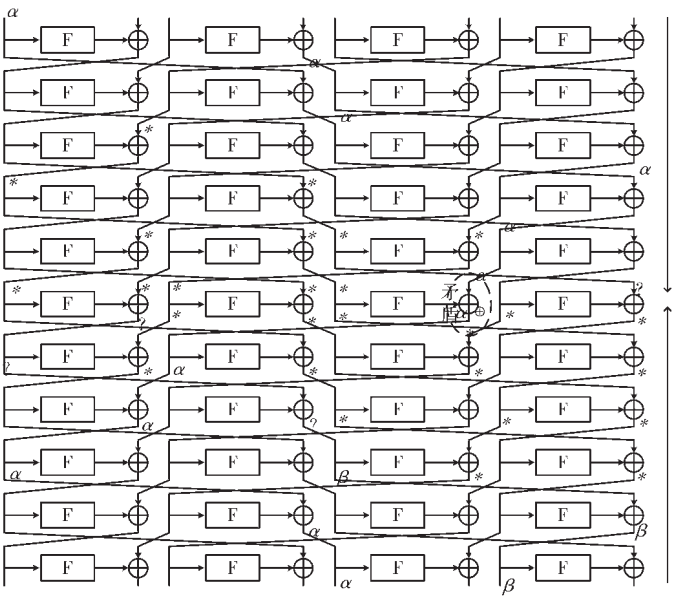

图 6 NBC-128 的第二类 11 轮零相关路线

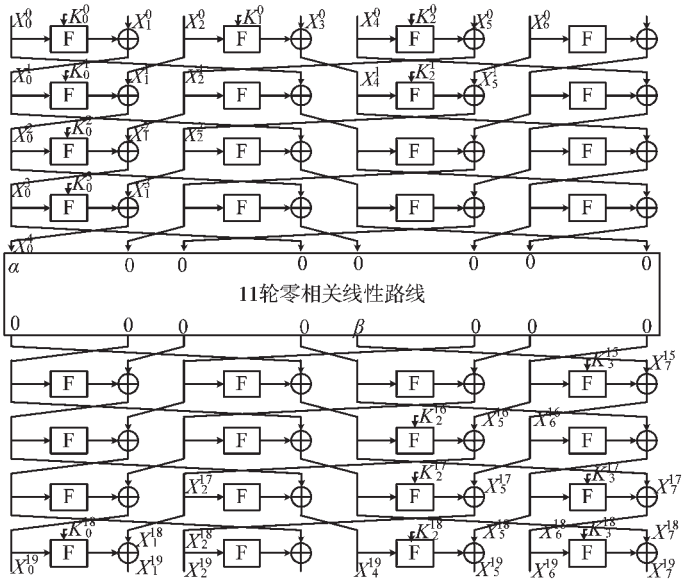

图 7 NBC-128/256 的 19 轮零相关攻击

(2)猜测 K_1^0，计算得到 $X_{0,1}^2,X_2^2,X_{1,5,6}^{18},X_5^{17}$，可存储于 2^{80+t} 个计数器中。该步骤需要的计算复杂度约为 $2^{96+t}\times 2^{128+16}=2^{240+t}$ 次 1 个 S 盒的查表。

(3)同上，依次进行密 $K_0^2,K_0^3,K_3^{17},K_2^{16},K_3^{15}$ 的猜测及状态压缩，每次猜测的密钥长度为 16 bit，计数器个数每次减少为之前的 2^{-16}，该步骤需要的计算复杂度约为 $2^{96+t}\times 2^{128+16}\times 5=2^{240+t}\times 5$ 次 1 个 S 盒的查表。

(4)最终得到 t 维的计数器向量，计算统计数并保留小于阈值 τ 的密钥，剩余约 $2^{256}\times\alpha_1$ 个候选密钥，这里 α_1 表示将错误密钥判定为正确密钥的概率。通过至多两个明密文数据进行穷搜攻击，恢复各轮密钥。

复杂度估计[19-20]：通过设置两类错误概率 $\alpha_0=2^{-2.7}$，$\alpha_1=2^{-11}$，这里 α_0 表示将正确密钥判定为错误密钥的概率，可以计算出需要的不同已知明文数据复杂度为 $N\approx 2^{124.5537}$，区分密钥使用的阈值为 $\tau=3803.173$。步骤(1)需要的计算复杂度约为 $T_1=N\times 2^{128}\times(8/(4\times 19))\approx 2^{249.3058}$；步骤(2)和步骤(3)需要的计算复杂度约为 $T_2=2^{240+t}\times 6\times(1/(4\times 19))\approx 2^{248.337}$；步骤(4)需要的计算复杂度约为 $T_3=2^{245}$。综上，总计算复杂度约为 $2^{249.9487}$ 次 19 轮加密。

3.3 对 NBC-128/128 的多维零相关线性攻击

利用类似的 $t=8$ 维的多维零相关路线，可以在前后分别添加 2 和 3 轮，针对 NBC-128/128 算法进行 16 轮的攻击。沿用图 7 的表示，进行第 3~18 轮的攻击，攻击过程如下：

(1)对于 N 个不同的已知明文及其密文数据，可压缩为存储 $X^2_{0,1}$，X^2_2，$X^{18}_{1,5,6}$，X^{18}_2 个数的计数器。对于 X^2_2、X^{18}_2，根据区分器的输入、输出掩码表示，共需存储 t bit 即可，因此可将中间状态存储于 2^{96+t} 个计数器中。

(2)猜测 16 bit 密钥 K^2_0，可计算得到 X^3_0，X^3_1，$X^{18}_{1,5,6,7}$，X^{18}_2，可存储于 2^{80+t} 个计数器中。该步骤需要的计算复杂度约为 $2^{96+t}\times 2^{16}=2^{112+t}$ 次 1 个 S 盒的查表。

(3)同上，依次进行密钥 K^3_0，K^{17}_2，K^{17}_3，K^{16}_2，K^{15}_3 的猜测及状态压缩，每次猜测的密钥长度为 16 bit，计数器个数每次减少为之前的 2^{-16}。该步骤需要的计算复杂度约为 $2^{112+t}\times 5$ 次 1 个 S 盒的查表。

(4)最终得到 t 维的计数器向量，计算统计数并保留小于阈值 τ 的密钥，剩余约 $2^{128}\times\alpha_1$ 个候选密钥。通过至多两个明密文数据进行穷搜攻击，恢复各轮密钥。

复杂度估计[9-10]：通过设置两类错误概率 $\alpha_0=2^{-2.7}$，$\alpha_1=2^{-8}$，可以计算出需要的不同已知明文数据复杂度为 $N\approx 2^{123.3548}$，区分密钥使用的阈值为 $\tau=15905.54$。步骤(1)需要的计算复杂度约为 $T_1=N$ 次状态压缩；步骤(2)和步骤(3)需要的计算复杂度约为 $T_2=2^{112+t}\times 6\times(1/(4\times 16))\approx 2^{122.585}$；步骤(4)需要的计算复杂度约为 $T_3=2^{120}$。综上，总计算复杂度不超过为 $2^{124.1069}$ 次 16 轮加密。

4 NBC-128 算法的积分攻击

4.1 NBC-128 算法的积分路线

利用 Todo 的分离特性[21]搜索方法，实现了广义 Feistel 结构的搜索算法，并对 NBC-128 进行了积分路线搜索。搜索得到的 NBC-128 算法最长积分路线为 12 轮，需要的数据复杂度为 2^{125}，基于分离特性的积分路线如表 3 所示(文献[9]、[10]中给出的数据量为 2^{127})。

第 4 条分离特性路线的积分特性见命题 5。

命题 5：(NBC-128 的一条积分路线)

$(A_{16},A_{16},A_{16},A_{16},A_{16},A_{16},A_{13},A_{16})\rightarrow(U,U,U,U,U,U,U,B)$ 是 NBC-128 算法的一条 12 轮积分路线，最后一轮包括位置置换，其中 A_n 表示 n 个比特遍历，$16-n$ 个比特取常数，U 表示异或和状态不确定，B 表示异或和为 0，对应着存在积分特性的分支。

表 3 NBC-128 的积分路线

轮数	输入分离特性 $D_{K_{in}}^{16,16,16,16,16,16,16}$	输出分离特性 $D_{K_{out}}^{16,16,16,16,16,16,16,16}$
12	$K_{in}=(13,16,16,16,16,16,16,16)$	$K_{out}=\{(0,0,0,0,0,0,0,1),(0,0,0,0,0,0,1,0),(0,0,0,0,0,1,0,0),(0,0,0,0,1,0,0,0),(0,0,0,1,0,0,0,0),(0,0,1,0,0,0,0,0),(0,2,0,0,0,0,0,0),(1,0,0,0,0,0,0,0)\}$
12	$K_{in}=(16,16,13,16,16,16,16,16)$	$K_{out}=\{(0,0,0,0,0,0,0,1),(0,0,0,0,0,0,1,0),(0,0,0,0,0,1,0,0),(0,0,0,0,1,0,0,0),(0,0,0,2,0,0,0,0),(0,0,1,0,0,0,0,0),(0,1,0,0,0,0,0,0),(1,0,0,0,0,0,0,0)\}$
12	$K_{in}=(16,16,16,16,13,16,16,16)$	$K_{out}=\{(0,0,0,0,0,0,0,1),(0,0,0,0,0,0,1,0),(0,0,0,0,0,2,0,0),(0,0,0,0,0,1,0,0),(0,0,0,1,0,0,0,0),(0,0,1,0,0,0,0,0),(0,1,0,0,0,0,0,0),(1,0,0,0,0,0,0,0)\}$
12	$K_{in}=(16,16,16,16,16,16,13,16)$	$K_{out}=\{(0,0,0,0,0,0,0,2),(0,0,0,0,0,0,1,0),(0,0,0,0,0,1,0,0),(0,0,0,0,1,0,0,0),(0,0,1,0,0,0,0,0),(0,1,0,0,0,0,0,0),(1,0,0,0,0,0,0,0)\}$

4.2 对 NBC-128/256、NBC-128/128 算法的积分攻击

对 NBC-128 的攻击过程与文献[9]中的描述大部分相同，下面不详细描述具体细节，只说明攻击中的不同点。

(1)本文采用的积分路线需要的数据量为 2^{125}，而不是 2^{127}。

(2)在使用 2^{125} 数据量的积分区分器下，只有一个分支存在积分特性，该分支状态异或和为16 bit 全 0 时对应的密钥为候选正确密钥，剩余密钥量为总密钥量的 2^{-16}。

(3)对于 NBC-128/256，利用 12 轮积分路线可以攻击 18 轮算法，计算一个分支异或和的计算复杂度约为 $2^{204.15}$。因此，使用一条积分路线攻击时，总计算复杂度为 $2^{204.15}+2^{256-16}\approx 2^{240}$。

(4)对于 NBC-128/128，利用 12 轮积分路线可以攻击 16 轮算法，计算一个分支异或和的计算复杂度约为 $2^{92.32}$。因此，使用一条积分路线攻击时，总计算复杂度为 $2^{92.32}+2^{128-16}\approx 2^{112}$。

5 结论

本文针对 NBC-128 的两个密钥尺寸版本的算法，给出改进的不可能差分分析、多维零相关线性分析和积分分析结果。其中不可能差分攻击对之前的攻击进行了修正，零相关线性分析在攻击轮数上有所扩展，积分分析则降低了攻击的数据复杂度。针对 NBC-128/256 的19 轮多维零相关线性攻击从轮数上来说是已知的最优攻击。

参考文献

[1] 中国密码学会.全国密码算法设计竞赛进入第二轮分组

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