# 改进的Type-1型广义Feistel结构的量子攻击及其在分组密码CAST-256上的应用

倪博煜[①②] 董晓阳*[③]

[①](山东大学密码技术与信息安全教育部重点实验室 济南 250100)

[②](山东大学网络空间安全学院 青岛 266237)

[③](清华大学高等研究院 北京 100084)

**摘 要**：广义Feistel结构(GFS)是设计对称密码算法的重要基础结构之一，其在经典计算环境中受到了广泛的研究。但是，量子计算环境下对GFS的安全性评估还相当稀少。该文在量子选择明文攻击(qCPA)条件下和量子选择密文攻击(qCCA)条件下，分别对Type-1 GFS进行研究，给出了改进的多项式时间量子区分器。在qCPA条件下，给出了$3d-3$轮的多项式时间量子区分攻击，其中$d(d\geq 3)$是Type-1 GFS的分支数，攻击轮数较之前最优结果增加$d-2$轮。得到更好的量子密钥恢复攻击，即相同轮数下攻击的时间复杂度降低了$2^{(d-2)n/2}$。在qCCA条件下，对于Type-1 GFS给出了$3d-2$轮的多项式时间量子区分攻击，比之前最优结果增加了$d-1$轮。该文将上述区分攻击应用到CAST-256分组密码中，得到了12轮qCPA多项式时间量子区分器，以及13轮qCCA多项式时间量子区分器，该文给出19轮CAST-256的量子密钥恢复攻击。

**关键词**：分组密码；广义Feistel结构；量子攻击；CAST-256加密算法

**中图分类号**：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)02-0295-12

**DOI**: 10.11999/JEIT190633

# Improved Quantum Attack on Type-1 Generalized Feistel Schemes and Its Application to CAST-256

NI Boyu[①②] DONG Xiaoyang[③]

[①](*Key Laboratory of Cryptologic Technology and Information Security*, *Ministry of Education*, *Shandong University*, *Jinan* 250100, *China*)

[②](*School of Cyber Science and Technology*, *Shandong University*, *Qingdao* 266237, *China*)

[③](*Institute for Advanced Study*, *Tsinghua University*, *Beijing* 100084, *China*)

**Abstract**: Generalized Feistel Schemes (GFS) are important components of symmetric ciphers, which have been extensively researched in classical setting. However, the security evaluations of GFS in quantum setting are rather scanty. In this paper, more improved polynomial-time quantum distinguishers are presented on Type-1 GFS in quantum Chosen-Plaintext Attack (qCPA) setting and quantum Chosen-Ciphertext Attack (qCCA) setting. In qCPA setting, new quantum polynomial-time distinguishers are proposed on $3d-3$ round Type-1 GFS with branches $d\geq 3$, which gain $d-2$ more rounds than the previous distinguishers. Hence, key-recovery attacks can be obtained, whose time complexities gain a factor of $2^{\frac{(d-2)n}{2}}$. In qCCA setting, $3d-3$ round quantum distinguishers can be obtained on Type-1 GFS, which gain $d-1$ more rounds than the previous distinguishers. In addition, given some quantum attacks on CAST-256 block cipher. 12-round and 13-round polynomial-time quantum distinguishers are obtained in qCPA and qCCA settings, respectively. Hence, the quantum key-recovery attack on 19-round CAST-256 is derived.

**Key words**: Block cipher; Generalized Feistel Scheme (GFS); Quantum attack; CAST-256 cipher algorithm

收稿日期：2019-08-26；改回日期：2019-11-26；网络出版：2019-11-29

*通信作者： 董晓阳 xiaoyangdong@tsinghua.edu.cn

基金项目：国家重点研发计划(2017YFA0303903)，国家自然科学基金(61902207)，国家密码发展基金(MMJJ20180101, MMJJ20170121)

Foundation Items: The National Key Research and Development Program of China (2017YFA0303903), The National Natural Science Foundation of China (61902207), The National Cryptography Development Fund (MMJJ20180101, MMJJ20170121)

## 1 引言

Feistel分组密码采用高效的Feistel网络，其加密和解密过程基于类似的操作。这种结构已被广泛研究[1–4]并被许多人采用作为标准分组密码，例如DES, Triple-DES, Camellia[5], GOST[6]。Feistel网络的一般形式称为广义Feistel网络(Generalized Feistel Network, GFN)，它采用更多的分支和不同的分支之间的操作。在1989年美密，Zheng等人[7]将一些广义Feistel网络总结为3种，即Type-1, Type-2和Type-3型。另外一些广义Feistel结构包括Anderson等人[8], Lucks[9]以及Schneier等人[10]发明的。很多重要密码算法基于广义Feistel网络设计，例如分组密码CAST-256(Type-1)[11], CLEFIA(Type-2)[12], Simpira(Type-2)[13]以及哈希函数MD5和SHA-1的压缩函数(Type-1)。广义Feistel结构继承了Feistel结构的优势，即加解密一致性。另外，广义Feistel结构可以利用更小的轮函数来设计大状态分组的密码算法，这对于轻量级密码算法的设计大有裨益。

在标准安全模型下，Luby等人[14]证明了3轮Feistel方案是一种安全的伪随机置换。在2000年亚密，Moriai等人[15]研究了一些广义Feistel算法(Generalized Feistel Scheme, GFS)并证明了7轮4分支Type-1型GFS和5轮4分支Type-2型GFS是安全的伪随机置换。后来，Hoang等人[16]改进Type-1, Type-2和Type-3 GFS的可证明安全性。对这些结构的攻击也被广泛研究，例如生日攻击[17]，中间相遇攻击[18]，差分攻击[19,20]和Patarin等人[21–23]的攻击。

最近，在量子计算环境下的对称密码的安全性评估成为一个研究热点。在2000年左右，人们普遍认为对称密码的量子攻击威胁不大，因为它们主要是使用Grover算法[24]来加速密钥的搜索。然而，Kuwakado等人[25]发现了3轮Feistel第1个多项式时间的量子区分器，即Simon的算法[26]。随后，产生了各种针对对称密码的量子攻击，例如针对Even-Mansour构造的密钥恢复攻击[27]，针对基于分组密码工作模式构造的消息认证码的伪造或密钥恢复攻击[28,29]，对FX结构的密钥恢复攻击[30]等。

Zhandry[31]对于对称密码的量子分析方法主要基于两种分析模型，即标准安全模型(Q1)和量子安全模型(Q2)。在Q1模型中，攻击者只能使用经典方法查询预言机来收集数据，然后用量子计算机来处理这些数据。在Q2模型中，攻击者可以通过以量子叠加态的方式来询问预言机，并获得相应的输出叠加态。如Ito等人[32]所述，“如果敌手可以访问密码算法的白盒实现，那么Q2模型下的攻击将变得尤为重要。因为任意经典电路都可以转换成量子电路，敌手可以将白盒实现给出的经典源代码构造出对应的量子电路”。本文假设敌手来自Q2模型。

目前，在Q2模型下，已经出现了一些研究Feistel结构或GFS安全性的分析成果。除了Kuwakado等人[25]的工作，在量子选择密文攻击(quantum Chosen-Ciphertext Attack, qCCA)条件下，Ito等人[32]等将量子区分器扩展为4轮Feistel。基于Leander等人[30]的工作，Hosoyamada等人[33]和Dong等人[34]对Feistel结构构造了一些量子密钥恢复攻击。Dong等人[35]还给出了GFS的一些量子区分器和密钥恢复攻击。另外，Dong等人[36]和Bonnetain等人[37]分别研究了量子高级滑动攻击，并给出了2K-/4K-Feistel等的密钥恢复攻击。值得注意的是，Hosoyamada和Iwata[38]最近给出了4轮Luby-Rackoff结构量子安全性证明。

本文，在Q2攻击模型下，给出了Type-1 GFS的选择明文攻击(quantum Chosen-Plaintext Attack, qCPA)和qCCA攻击。首先，在qCPA条件下，给出了$3d-3$轮的多项式时间量子区分攻击，比之前的区分器增加$d-2$轮，在这里设Type-1 GFS有$d(d\geq 3)$个分支。基于Leander等人[30]算法，可以获得更好的密钥恢复攻击，时间复杂度降低了$2^{(d-2)n/2}$。其次，当考虑选择明文攻击时，得到$3d-2$轮量子区分器，较之前的区分器增加$d-1$轮。表1和表2总结了对Type-1型GFS的区分攻击和密钥恢复攻击。表2中$T=(d^2/4-3d/4+1)\cdot n$。

此外，本文还评估了qCPA和qCCA条件下的CAST-256分组密码。在qCPA和qCCA条件下分别找到12轮和的13轮多项式时间量子区分器，而之前最多的轮数是7轮。因此，本文对19轮CAST-256进行量子密钥恢复攻击，之前最好的量子密钥恢复攻击是16轮。结果详见表3。另外，表4还将量子攻击与经典攻击进行了比较。

**表 1 Type-1 GFS的量子区分器的轮数**

| 来源 | 攻击条件 | $r$ | $d=3$ | $d=4$ | $d=5$ | $d=6$ | $d=7$ |
|---|---|---|---|---|---|---|---|
| 文献[35] | qCPA | $2d$–1 | 5 | 7 | 9 | 11 | 13 |
| 4.1节 | qCPA | $3d$–3 | 6 | 9 | 12 | 15 | 18 |
| 4.2节 | qCCA | $3d$–2 | 7 | 10 | 13 | 16 | 19 |

**表 2　在量子环境下对Type-1 GFS的密钥恢复攻击**

| 来源 | 区分器轮数 | 密钥恢复轮数 | 复杂度(log) | 穷搜复杂度(log) |
|---|---|---|---|---|
| 文献[35] | $2d-1$ | $r \geq d^2$ | $T+(r-d^2+d-2)n/2$ | $rn/2$ |
| 4.1节 | $3d-3$ | $r \geq d^2$ | $T+(r-d^2)n/2$ | $rn/2$ |

**表 3　CAST-256的量子攻击**

| 来源 | 攻击条件 | 区分器轮数 | 密钥恢复攻击轮数 | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | $r=14$ | $r=15$ | $r=16$ | $r=17$ | $r=18$ | $r=19$ |
| 文献[35] | qCPA | 7 | $2^{74}$ | $2^{92.5}$ | $2^{111}$ | – | – | – |
| 5.1节 | qCPA | 12 | $2^{37}$ | $2^{55.5}$ | $2^{74}$ | $2^{92.5}$ | $2^{111}$ | – |
| 5.2节 | qCCA | 13 | $2^{18.5}$ | $2^{37}$ | $2^{55.5}$ | $2^{74}$ | $2^{92.5}$ | $2^{111}$ |

**表 4　针对CAST-256的经典攻击和量子攻击的比较**

| 来源 | 密钥长度 | 攻击 | 轮数 | 数据 | 时间 |
|---|---|---|---|---|---|
| 文献[39] | 128 | 飞去来器 | 16 | $2^{49.3}$ | – |
| 5.2节 | 128 | qCCA | 16 | – | $2^{55.5}$ |
| 文献[40] | 192 | 线性攻击 | 24 | $2^{124.1}$ | $2^{156.52}$ |
| 5.2节 | 192 | qCCA | 17 | – | $2^{74}$ |
| 文献[41] | 256 | 多维零相关 | 28 | $2^{98.8}$ | $2^{246.9}$ |
| 5.2节 | 256 | qCCA | 19 | – | $2^{111}$ |

## 2　符号说明

$x_j^i$：第$i$轮第$j$分支的输出；

$d$：Type-1型GFS的分支数；

$R^i$：Type-1型GFS的第$i$轮的轮函数，它的输入和输出都是$n$ bit的串；

## 3　预备知识

### 3.1　Simon算法

给定一个函数$f:\{0,1\}^n \to \{0,1\}^n$，它在某个$n$ bit周期$a$异或下不变。即找到一个给定的$a: f(x)=f(y) \leftrightarrow x \oplus y=\{0^n, a\}$。

在经典计算环境下，解决这个问题的最优时间复杂度是$2^{n/2}$。然而，Simon[26]给出了一个可以进行指数级加速的算法，它只需要$O(n)$次询问就能找到$a$。这个算法包括以下5个步骤：

(1) 将两个$n$ bit量子寄存器的状态初始化为$|0\rangle^{\otimes n}|0\rangle^{\otimes n}$，将Hadamard变换应用于第1个寄存器得到相应的叠加态

$$H^{\otimes n}|0\rangle|0\rangle=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \tag{1}$$

(2) 对函数$f$进行一个量子询问并将其映射到当前的状态

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle \tag{2}$$

(3) 测量第2个寄存器，第1个寄存器坍缩成以下状态

$$\frac{1}{\sqrt{2}}(|z\rangle+|z\oplus a\rangle) \tag{3}$$

(4) 将Hadamard变换应用于第1个寄存器得到

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{y\cdot z}(1+(-1)^{y\cdot a})|y\rangle \tag{4}$$

(5) 该叠加态中满足$y\cdot a=1$的振幅为0。因此，测量所有$y$都有$y\cdot a=0$。

重复$O(n)$次，可以得到一组线性方程组，通过求解该线性方程组可以得到$a$。在2017年亚密，Leander等人[30]假设$f(x)$是一个周期为$a$的随机函数，他们证明重复$l=2(n+\sqrt{n})$次Simon算法就可以以高概率找到$a$，详见文献[30]引理4。

在ISIT 2010上，Kuwakado等人[25]介绍了一个使用Simon算法构造的3轮Feistel的量子区分攻击。如下图1，$\alpha_0$和$\alpha_1$是任意的常数

$$\left.\begin{aligned} &f:\{0,1\}\times\{0,1\}^n\to\{0,1\}^n\\ &b,x\to\alpha_b\oplus x_2^3,(x_1^3,x_2^3)=E(\alpha_b,x)\\ &f(b,x)=R^2(R^1(\alpha_b)\oplus x)\end{aligned}\right\} \tag{5}$$

其中$f$是周期函数，满足$f(b,x)=f(b\oplus 1, x\oplus R^1(\alpha_0)\oplus R^1(\alpha_1))$。然后运用Simon算法，在多项式时间里可以得到周期$s=1||R^1(\alpha_0)\oplus R^1(\alpha_1)$。

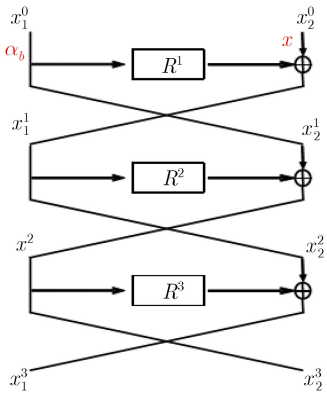


图 1 3轮的量子区分器

### 3.2 Hosoyamada和Sasaki量子叠加态截断算法

如图1所示，在Kuwakado等人[25]的量子区分器中，必须得到$E$的右半边的$n$ bit输出，即$x_2^3$。然而Kaplan等人[28]和Hosoyamada等人[33]指出在量子环境中，从$2n$ bit叠加态中截断得到$n$ bit叠加态是非平凡的，因为截断通常会破坏掉量子纠缠。

在SCN 2018, Hosoyamada等人[33]介绍了一种在不破坏量子纠缠的情况下模拟量子预言机输出截断的方法。令$O:|x\rangle|y\rangle|z\rangle|w\rangle\mapsto|x\rangle|y\rangle|z\oplus O_{\mathrm{L}}(x,y)\rangle|w\oplus O_{\mathrm{R}}(x,y)\rangle$为加密预言机$E$，其中$O_{\mathrm{L}}$, $O_{\mathrm{R}}$分别定义为完整加密的左边$n$ bit和右边$n$ bit。本文的目标是模拟预言机$O_{\mathrm{R}}:|x\rangle|y\rangle|w\rangle\mapsto|x\rangle|y\rangle|w\oplus O_{\mathrm{R}}(x,y)\rangle$。Hosoyamada等人[33]首先模拟了一个略微调整的$O_{\mathrm{R}}$，即$O'_{\mathrm{R}}:|x\rangle|y\rangle|w\rangle|0^n\rangle\mapsto|x\rangle|y\rangle|w\oplus O_{\mathrm{R}}(x,y)\rangle|0^n\rangle$。令$|+\rangle:=H^n|0\rangle^{\otimes n}$，其中$H^n$是一个$n$ bit的Hadamard门。因此，$O'_{\mathrm{R}}:|x\rangle|y\rangle|+\rangle|w\rangle\mapsto|x\rangle|y\rangle|+\rangle|w\oplus O_{\mathrm{R}}(x,y)\rangle$。然后，他们定义了$O'_{\mathrm{R}}:=(I\otimes H^n)\circ S\circ O\circ S\circ(I\otimes H^n)$，其中$S$是一个交换最后$2n$ bit的操作：$|x\rangle|y\rangle|z\rangle|w\rangle\mapsto|x\rangle|y\rangle|w\rangle|z\rangle$。所以，可以利用完整的加密预言机$O$以及一些附加的量子比特来模拟$O_{\mathrm{R}}$。

### 3.3 Grover算法

给定一个有$N=2^n$个元素的无序集，Grover算法是用来找到满足某些条件的唯一元素。换句话说，给定一个量子预言机$O$执行操作$O|x\rangle=(-1)^{f(x)}|x\rangle$，其中$f(x)=0$除$x_0$外对$0\le x<2^n$成立，对$f(x_0)=1$，找到$x_0$。用于搜索这个无序数据的最佳经典算法时间复杂度为$O(N)$，而Grover算法在量子计算机上置信这个搜索只需要$O(\sqrt{N})$次操作，算法的步骤如下：

(1) 初始化一个$n$ bit的寄存器$|0\rangle^{\otimes n}$，将Hadamard变换应用于第1个寄存器得到相应的叠加态，如式(6)。

$$H^{\otimes n}|0\rangle=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle=|\varphi\rangle \tag{6}$$

(2) 构造一个预言机$O:|x\rangle\to(-1)^{f(x)}|x\rangle$，如果$x$是正确的状态，那么；否则，$f(x)=0$。

(3) 定义Grover迭代：$(2|\varphi\rangle\langle\varphi|-I)O$，并且将其迭代$R\approx\pi\sqrt{2^n}/4$次

$$[(2|\varphi\rangle\langle\varphi|-I)O]^R|\varphi\rangle\approx|x_0\rangle \tag{7}$$

(4) 返回$x_0$。

### 3.4 Grover算法和Simon算法的结合

在2017年亚密，Leander等人[30]提出了一个对FX结构的量子密钥恢复攻击，如图2所示。满足

$$\mathrm{Enc}(x)=E_{k_0}(x+k_1)+k_2 \tag{8}$$

文献[30]构造函数$f(k,x)=\mathrm{Enc}(x)+E_k(x)=E_{k_0}(x+k_1)+k_2+E_k(x)$，对于正确密钥的猜测$k=k_0$，满足$f(k,x)=f(k,x+k_1)$。然而，对于$k\ne k_0$, $f(k,\cdot)$不是周期的。在qCPA条件下，文献[30]结合Simon算法和Grover算法来攻击FX结构。

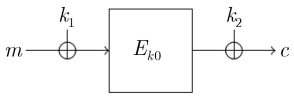


图 2 FX结构

基于Leander[30]的工作，Hosoyamada等人[33]，以及Dong等人[34]在图1所示3轮的Feistel区分器后面添加了几轮用来恢复$r$轮的Feistel加密算法的密钥，时间复杂度为$O(2^{(r-3)n/2})$[33,34]。

### 3.5 Ito等人[32]对Feistel密码的量子攻击

在RSA 2019, Ito等人[32]在qCCA条件下给出了一个4轮Feistel密码的量子区分器，详见图3，明文$(\alpha_\beta,x)$先用4轮的Feistel加密得到密文$(d,c)$，利用该密文构造一个新的密文$(d\oplus\alpha_0\oplus\alpha_1,c)$，并用逆向的4轮Feistel解密得到一个新的明文。Ito等人[32]定义函数

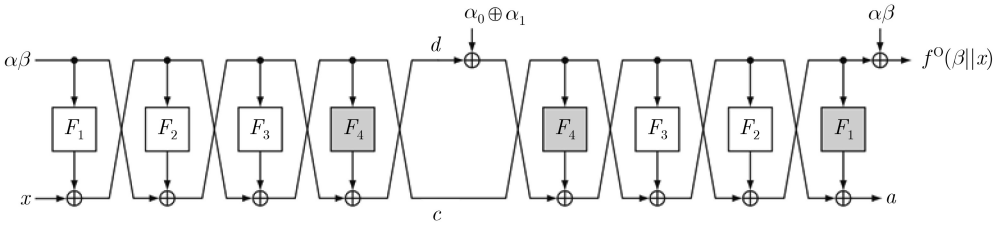


图 3 Ito等人在Feistel上的4轮量子区分器

$$f^O=\alpha_0\oplus\alpha_1\oplus F_2(x\oplus F_1(\alpha_\beta))\\ \oplus F_2(x\oplus F_1(\alpha_\beta)\oplus F_3(\alpha_\beta\oplus F_2(x\oplus F_1(\alpha_\beta))))\\ \oplus F_3(\alpha_\beta\oplus\alpha_0\oplus\alpha_1\oplus F_2(x\oplus F_1(\alpha_\beta))) \tag{9}$$

其中$\beta$的取值是0或1，并且$\alpha_\beta$是一个常数。因此，$f^O$的周期为$s=1||F_1(\alpha_0)\oplus F(\alpha_1)$。

结合Leander等人[30]算法，还有Ito等人[32]利用新的区分器给出了Feistel结构的密钥恢复攻击。另外，在密钥恢复攻击中，并没有实际地计算出$f^O$的周期，相反地，通过检查空间的维数来区分$f$，这里的空间是由Simon算法计算出的向量所张成的。因此，存在几个局部周期或者周期不同于$s$都不是问题。因为不计算$s$就可以区分$f$。仍使用这个方法对Type-1 GFS和CAST-256采用密钥恢复攻击。

## 4　Type-1 GFS的量子攻击

图4给出，Type-1密码的输入被分成了$d$个分支，即$x_j^0$，每一个都是$n$ bit，所以分组长度是$d\times n$。$R^i$是轮函数，吸收$n$ bit的密钥$k_i$和$n$ bit的输入。

Dong等人[35]首先给出了Type-1 GFS的一些量子区分器和密钥恢复攻击。本节在qCPA条件下和qCCA条件下分别给出了改进的多项式时间的量子区分器，基于这些区分器，给出了一些改进的密钥恢复攻击。

### 4.1　在qCPA条件下，Type-1 GFS的量子区分器

首先给出了一个$d=4$的攻击示例，然后扩展到任意类型$d\ge3$的情况。最后，给出密钥恢复攻击。

**在qCPA条件下$d=4$的Type-1**

当$d=4$时，可以得到一个9轮的量子区分器，如图5所示。9轮Type-1 GFS加密过程为$E(x_1^0,x_2^0,\alpha_b,x)=(x_1^9,x_2^9,x_3^9,x_4^9)$，其中$x_1^0$和$x_2^0$是常数，并且$b=0$或1，$\alpha_0,\alpha_1$也是常数，$\alpha_0\ne\alpha_1$。令$h(\alpha_b)=R^3(R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b)$。

定义$f(b,x)=x_2^9\oplus\alpha_b=R^6(R^5(R^4(h(\alpha_b)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\oplus R^2(R^1(x_1^0)\oplus x_2^0)$，因此，推断

$$f(0,x)=R^6(R^5(R^4(h(\alpha_0)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\\ \oplus R^2(R^1(x_1^0)\oplus x_2^0)\\ =f(1,x\oplus h(\alpha_0)\oplus h(\alpha_1)), \tag{10}$$

$$f(1,x)=R^6(R^5(R^4(h(\alpha_1)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\\ \oplus R^2(R^1(x_1^0)\oplus x_2^0)\\ =f(0,x\oplus h(\alpha_0)\oplus h(\alpha_1)), \tag{11}$$

所以，$f(b,x)=f(b\oplus1,x\oplus h(\alpha_0)\oplus h(\alpha_1))$是一个周期函数，周期为$s=1||h(\alpha_0)\oplus h(\alpha_1)$。

**在qCPA条件下，$d(d\ge3)$分支Type-1的推广**

在$3d-3$轮密码上构造量子区分器。第$i$轮之后的中间状态为$x_j^i,1\le j\le d$，其中第$3d-3$轮的输出表示成$x_1^{3d-3}||x_2^{3d-3}||\cdots||x_d^{3d-3}$。

$3d-3$轮的Type-1 GFS加密过程为$E(x_1^0,\cdots,x_{d-2}^0,\alpha_b,x)$，其中$b=0$或1，$\alpha_0,\alpha_1$也是常数，$\alpha_0\ne\alpha_1$，并且$x_d^0=x$。所有剩余的分支$x_1^0,x_2^0,\cdots,x_d^0$都为常数。和$d=4$情况的攻击相同，定义$h(\alpha_b)=R^{d-1}(R^{d-2}(\cdots R^3(R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0)\cdots\oplus x_{d-2}^0)\oplus\alpha_b)$，然后，我们定义：

$$f(b,x)=x_2^{3d-3}\oplus\alpha_b=R^{2d-2}(R^{2d-3}(\cdots(h(\alpha_b)\oplus x)\cdots)\\ \oplus R^{d-3}(\cdots(R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0\cdots)\oplus x_{d-2}^0))\\ \oplus R^{d-2}(R^{d-3}(\cdots(R^2(R^1(x_1^0)\oplus x_2^0)x_3^0)\cdots)\\ \oplus x_{d-2}^0) \tag{12}$$

通过计算，推导出$f(b,x)=f(b\oplus1,x\oplus g(\alpha_0)\oplus g(\alpha_1))$。因此，利用Simon算法，求解周期$s=1||g(\alpha_0)\oplus g(\alpha_1)$。在本文第3.2节，利用Hosoyamada等人[33]的成果，可以截断量子预言机的输出，因此$f$可以当做量子预言机使用。

**在qCPA条件下，对Type-1 GFS的量子密钥恢复攻击**

给出一个$d=4$分支的密钥恢复攻击的例子。结合Simon算法[33]和Grover算法[34]来攻击Feistel结构，在9轮区分器后面添加了7轮进行攻击。如图6所示，Grover算法需要猜测$4n$ bit密钥来计算$x_2^9$。注意到，在这里不需要Hosoyamada等人[33]的方法来截断加密预言机的输出，只需要实现一个函数$h_D(k_{10},k_{13},k_{14},k_{16},x_1^{16},x_2^{16},x_3^{16},x_4^{16})=x_2^9$，其中$k_{10},k_{13},k_{14},k_{16}$分别是$R^{10},R^{13},R^{14},R^{16}$的轮密钥，通过猜测密钥$k_{10},k_{13},k_{14},k_{16}$，用$h_D$解密$x_1^{16},x_2^{16},x_3^{16},x_4^{16}$得到$x_2^9$。

因此，16轮的量子密钥恢复攻击需要$2^{2n}$次询问和$O(n^2)$量子比特。如果攻击$r(r>16)$轮，那么

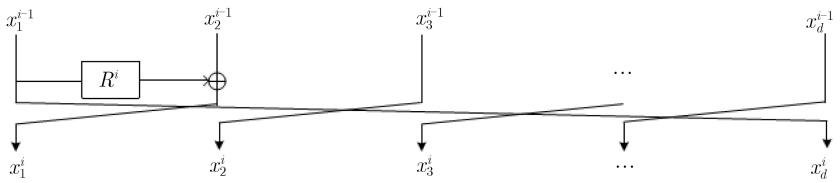


图 4 $d$分支Type-1 GFS的第$i$轮

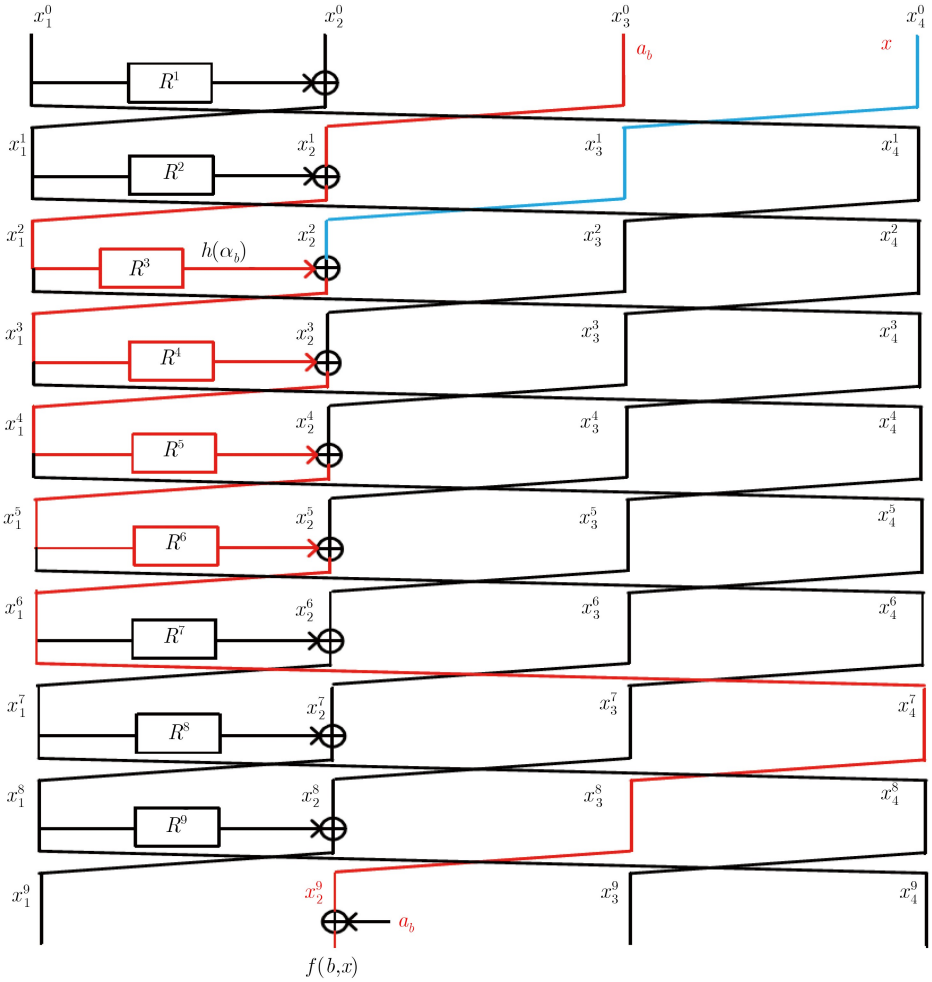


图 5 4分支Type-1 GFS的选择明文量子区分器

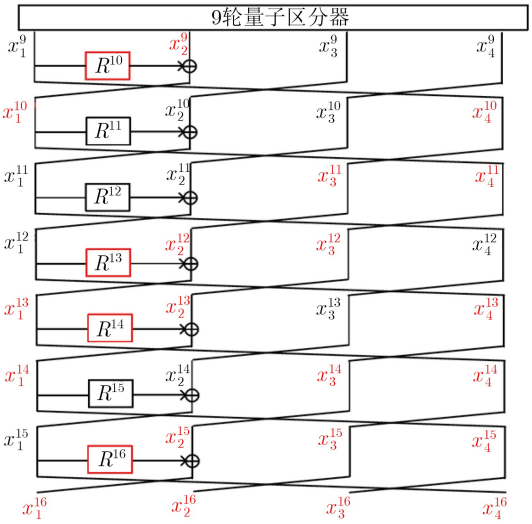


图 6 4分支Type-1 GFS的16轮密钥恢复攻击

需要猜测$(r-12)n$ bit密钥。所有，时间复杂度为$2^{(r-12)n/2}$。

一般来说，对于$d \geq 3$，可以得到$(3d-3)$轮的量子区分器，并在量子区分器后面添加上$d^2-3d+3$轮来攻击$r_0=d^2$轮。同理，需要猜测$(d^2/2-3d/2+2)n+(r-r_0)n$ bit密钥。因此，时间复杂度为$2^{(d^2/4-3d/4+1)n+(r-r_0)n/2}$。

$n$ bit密钥。所以，对于$r_0$轮Type-1 GFS，时间复杂度为$2^{(d^2/4-3d/4+1)n}$，并且需要$O(n^2)$量子比特。如果攻击$r(r>r_0)$轮，那么需要猜测$(d^2/2-3d/2+2)n+(r-r_0)n$ bit密钥。因此，时间复杂度为$2^{(d^2/4-3d/4+1)n+(r-r_0)n/2}$。

### 4.2 在qCCA条件下，Type-1 GFS的量子区分器

#### 在qCCA条件下$d=4$的Type-1 GFS

当$d=4$时，如图7所示，得到10轮量子区分器。注意到，为简单起见，省略了最后一个交换函数。

加密的过程为$E(x_1^0,x_2^0,\alpha_b,x)=(x_1^{10},x_2^{10},x_3^{10},x_4^{10})$，其中$\alpha_0,\alpha_1$也是常数，$\alpha_0 \neq \alpha_1$，并且$x_4^0=x$ 分支$x_1^0$，$x_2^0$是常数。解密的过程为$D(x_1^{10},x_2^{10}\oplus\alpha_0\oplus\alpha_1,x_3^{10},x_4^{10})=(y_1^0,y_2^0,y_3^0,y_4^0)$，注意，如图7所示，在解密阶段(图7的右侧)与加密阶段(图7的左侧)的许多中间状态相同。

在图7的右侧，按照红线和蓝线，可以定义函数

$$f(b,x)=y_1^0=R^4(R^7(g(b,x)\oplus\alpha_0\oplus\alpha_1)\oplus R^7(g(b,x))\oplus x_2^6\oplus x_2^7 \tag{13}$$

其中$g(b,x)=x_2^9$，接着计算$g(b,x)$，首先定义$h(\alpha_b)=$

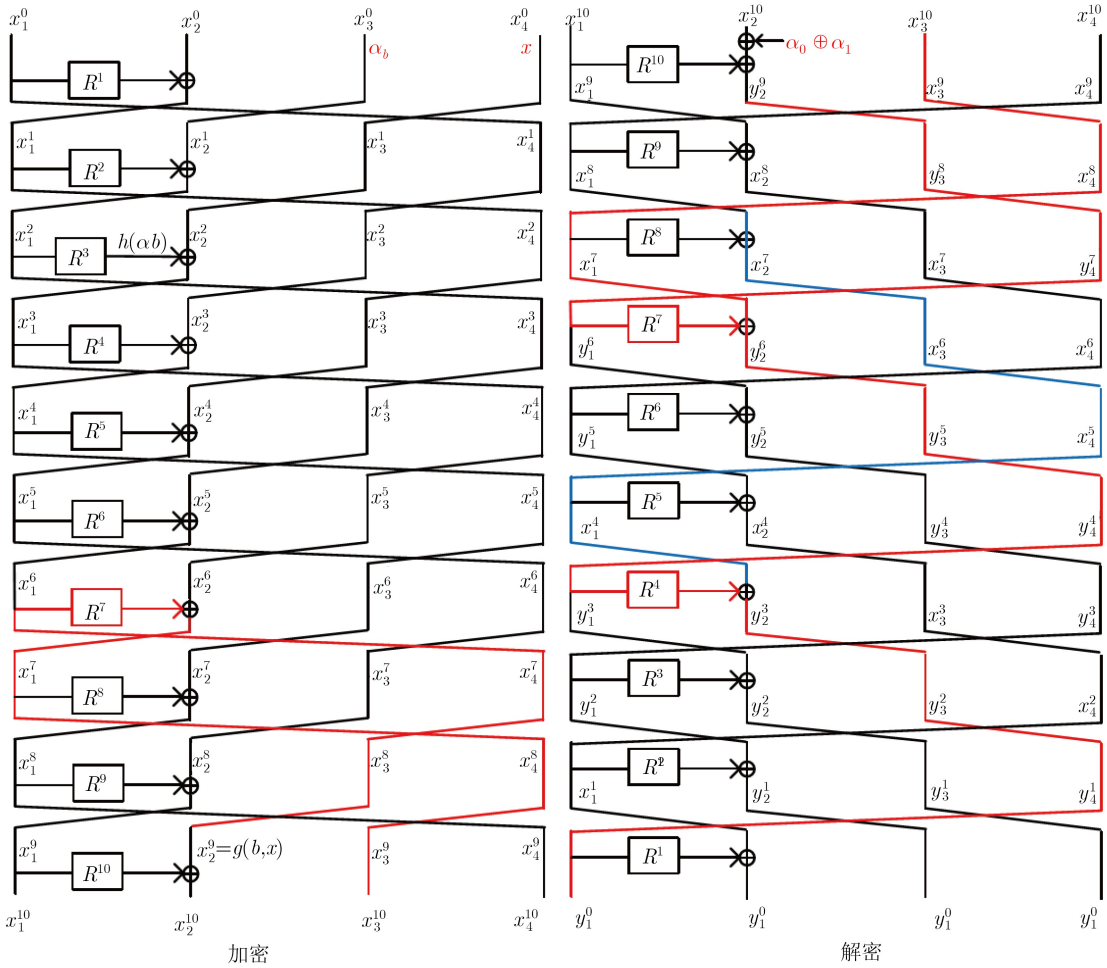


图 7 4分支CAST256-like GFS的10轮区分器

$R^3(R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b)$。所以$g(b,x)=R^6(R^5(R^4(h(\alpha_0)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\oplus R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b$。通过计算，推出$g(0,x)\oplus\alpha_0\oplus\alpha_1=g(1,x\oplus h(\alpha_0)\oplus h(\alpha_1))$和$g(1,x)\oplus\alpha_0\oplus\alpha_1=g(0,x\oplus h(\alpha_0)\oplus h(\alpha_1))$。

因此，$g'(b,x)=R^7(g(b,x)\oplus\alpha_0\oplus\alpha_1)\oplus R^7(g(b,x))$具有周期性，为$s=1||h(\alpha_0)\oplus h(\alpha_1)$。由于$x_2^6=h(\alpha_b)\oplus x_2^2=h(\alpha_b)\oplus x$成立，$x_2^6$也是一个周期函数，并且周期和$g'(b,x)$相同，即周期为$1||h(\alpha_0)\oplus h(\alpha_1)$。同样地，$x_2^7=R^4(h(\alpha)\oplus x)\oplus x_1^0$也有相同的周期，周期为$s=1||h(\alpha_0)\oplus h(\alpha_1)$。所以$f(b,x)$是一个周期函数，周期为$s=1||h(\alpha_0)\oplus h(\alpha_1)$。

**在qCCA条件下，$d(d\geq 3)$分支Type-1 GFS的推广**

在$3d-2$轮密码上构造一个新的量子区分器。第$i$轮后的中间状态记为$x_j^i$，其中$1\leq j\leq d$，特别是第$3d-2$轮的输出记为$x_1^{3d-2}||x_2^{3d-2}||\cdots||x_d^{3d-2}$。

加密的过程为$E(x_1^0,x_2^0,\cdots,x_{d-2}^0,\alpha_b,x)=(x_1^{3d-2},x_2^{3d-2},\cdots,x_d^{3d-2})$，其中$b=0$或1，$\alpha_0,\alpha_1$也是常数，$\alpha_0\neq\alpha_1$，且$x_d^0=x$。输入分支$x_1^0,x_2^0,\cdots,x_{d-2}^0$都是常数。所以定义加密过程为$E(\alpha_b,x)$。解密过程为$D(x_1^{3d-2},x_2^{3d-2}\oplus\alpha_0\oplus\alpha_1,\cdots,x_d^{3d-2})=(y_1^0,y_2^0,\cdots,y_d^0)$。定义$g(b,x)$

$$\begin{aligned}g(b,x)=x_2^{3d-3}=R^{2d-2}(\cdots(R^{d+1}(R^d(R^{d-1}&\\(\cdots R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0)\cdots\oplus\alpha_b)\oplus x)\oplus x_1^0)&\\\oplus R^1(x_1^0)\oplus x_2^0)\cdots\oplus R^{d-3}(\cdots(R^2(R^1(x_1^0)\oplus x_2^0)&\\\oplus x_3^0)\cdots\oplus x_{d-3}^0)\oplus x_{d-2}^0)\oplus R^{d-2}(R^{d-3}(\cdots&\\(R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0)\cdots\oplus x_{d-3}^0)\oplus x_{d-2}^0)&\\\oplus\alpha_b&\end{aligned}\tag{14}$$

还是以$d=4$为例，如图7，遵循加密中的过程，得到

$$\left.\begin{aligned}x_i^{3d-2}=x_i^{3d-3}=R^{2d-4+i}(x_{i-1}^{3d-3})\oplus x_2^{2d-5+i},&\\3\leq i\leq d&\\x_1^{3d-2}=x_1^{3d-3}=R^{3d-3}(x_d^{3d-3})\oplus x_2^{3d-4}&\\x_2^{3d-2}=R^{3d-2}(x_1^{3d-2})\oplus x_2^{3d-3}&\end{aligned}\right\}\tag{15}$$

遵循图7解密过程中的红线，可以得到

$$\begin{aligned}y_1^0=R^d(R^{2d-1}(x_2^{3d-3}\oplus\alpha_0\oplus\alpha_1)\oplus x_3^{3d-2})&\\\oplus R^{2d}(x_3^{3d-2})\oplus x_4^{3d-2}&\end{aligned}\tag{16}$$

构造函数$f:\{0,1\}\times\{0,1\}^n\to\{0,1\}^n b,x\mapsto y_1^0$，其中$\left(x_1^{3d-2},x_2^{3d-2},\cdots,x_d^{3d-2}\right)=E(\alpha_b,x),(y_1^0,y_2^0,\cdots,y_d^0)=D\left(x_1^{3d-2},x_2^{3d-2}\oplus\alpha_0\oplus\alpha_1,\cdots,x_d^{3d-2}\right)f(b,x)=R^d\left(R^{2d-1}\left(x_2^{3d-3}\oplus\alpha_0\oplus\alpha_1\right)\oplus x_3^{3d-2}\right)\oplus R^{2d}\left(x_3^{3d-2}\right)\oplus x_4^{3d-2}$。

$f$分两步得到：第1步，加密$(x_1^0,x_2^0,\cdots,x_{d-2}^0,\alpha_b,x)$得到密文$(x_1^{3d-2},x_2^{3d-2},\cdots,x_d^{3d-2})$，第2步，解密$(x_1^{3d-2},x_2^{3d-2}\oplus\alpha_0\oplus\alpha_1,\cdots,x_d^{3d-2})$得到明文$(y_1^0,y_2^0,\cdots,y_d^0)$，定义$f=y_1^0$。

记$h(\alpha_b)=R^{d-1}(R^{d-2}(R^{d-3}(\cdots R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0)\cdots\oplus x_{d-3}^0)\oplus x_{d-2}^0)\oplus\alpha_b)$。正如式(6)所示，可以简单地推出$g(0,x)=g(1,x\oplus h(\alpha_0)\oplus h(\alpha_1))\oplus\alpha_0\oplus\alpha_1$，同时，还可以得到$g(1,x)=g(0,x\oplus h(\alpha_0)\oplus h(\alpha_1))\oplus\alpha_0\oplus\alpha_1$。所以$g(b,x)$的周期为$1||h(\alpha_0)\oplus h(\alpha_1)$。同时，$x_2^{2d-2}=R^{d-1}(R^{d-2}(R^{d-3}(\cdots R^2(R^1(x_1^0)\oplus x_2^0)\oplus x_3^0)\cdots\oplus x_{d-3}^0)\oplus x_{d-2}^0)\oplus\alpha_b)\oplus x=h(\alpha_b)\oplus x$，得到$x_2^{2d-2}$的周期是$1||h(\alpha_0)\oplus h(\alpha_1)$。同理，在函数$f$中，根据式(15)中的第一个等式，$R^{2d}(x_3^{3d-2})\oplus x_4^{3d-2}=x_2^{2d-1}=R(x_2^{2d-2})\oplus x_1^0$有相同的周期。此外，在函数$f$中，由于式(15)是周期的。所以，$f(b,x)=f(b\oplus1,x\oplus h(\alpha_0)\oplus h(\alpha_1))$，周期为$s=1||h(\alpha_0)\oplus h(\alpha_1)$

**在qCCA条件下，对Type-1 GFS的量子密钥恢复攻击**

在$3d-2$轮区分器前面添加了$r-3d+2$轮使用Leander等人[30]的算法来进行密钥恢复攻击。攻击步骤如下:

(1) 运行量子电路，用第$r-3d+2$轮后的中间状态值$(x_1^{r-3d+2},x_2^{r-3d+2},\cdots,x_{d-2}^{r-3d+2},\alpha_b,x)$和子密钥作为输入，解密前$r-3d+2$轮的到明文 然后使用加密预言机$E$加密明文$(x_1^0,x_2^0,\cdots,x_d^0)$得到密文$(x_1^r,x_2^r,\cdots,x_d^r)$。

(2) 运行量子电路，由量子解密询问$D$，用密文$(x_1^r,x_2^r\oplus\alpha_0\oplus\alpha_1,\cdots,x_d^r)$得到明文，然后再用明文与前$r-3d+2$轮的子密钥加密得到中间状态$(y_1^{r-3d+2},y_2^{r-3d+2},\cdots,y_d^{r-3d+2})$。

(3) 猜测前$r-3d+2$轮的子密钥。对每个猜测的密钥，使用$E$和$D$的$3d-2$轮区分器检查它的正确性。

如果区分器是周期的，那么判断猜测的密钥是正确的，否则猜测的密钥是错误的。

对于$r(r>3d-2)$轮，需要使用Grover算法猜测$(r-3d+2)n$ bit密钥。所以$r$轮量子密钥恢复攻击需要的时间复杂度$2^{(r-3d+2)n/2}$量子比特。

## 5 CAST-256分组密码的量子攻击

CAST-256分组密码是AES竞赛的第1轮候选者。它有48轮，包括24轮的Type-1 GFN和24轮的逆向Type-1 GFN。如图8所示，其中包含9轮的Type-1 GFN和3轮的逆向Type-1 GFN。分组长度为128 bit，分为4个分支，每个分支32 bit，密钥长度可以为128, 192或者256 bit。每个轮函数吸收37 bit密钥，本文的攻击是非常普遍的，不需要密码的其他任何细节。

在本节中，在qCPA条件下和qCCA条件下对CAST-256分组密码分别给出了量子攻击。

### 5.1 在qCPA条件下，对CAST-256的量子攻击

如图8所示，用CAST-256结构构造一个12轮的量子区分器，包含9轮的Type-1 GFN和3轮的逆向Type-1 GFN。这个区分器和4.1节中9轮的区分器非常相似。

令$h(\alpha_b)=R^3(R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b)$以及$f(b,x)=x_2^9\oplus\alpha_b=R^6(R^5(R^4(h(\alpha_b)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\oplus R^2(R^1(x_1^0)\oplus x_2^0)$，正如4.1节所示，$f(b,x)=f(b\oplus1,x\oplus h(\alpha_0)\oplus h(\alpha_1))$，所以$f(b,x)$是一个周期函数，周期为$s=1||h(\alpha_0)\oplus h(\alpha_1)$。

如图9所示，当攻击$r(r>12)$轮CAST-256时，需要猜测最后$(r-12)$轮的所有密钥，即$(r-12)\times37$ bit密钥。因此，需要$2^{(r-13)\times37/2}=2^{18.5r-240.5}$次Grover迭代。

### 5.2 在qCPA条件下，对CAST-256的量子攻击

在qCCA条件下，构造了一个13轮的量子区分器，如图10所示。这个区分器和4.2节中10轮的Type-1 GFS区分器非常相似。

加密的过程为$E(x_1^0,x_2^0,\alpha_b,x)=(x_1^{13},x_2^{13},x_3^{13},x_4^{13})$，其中$b=0$或1, $\alpha_0,\alpha_1$是常数，$\alpha_0\neq\alpha_1$，并且$x_4^0=x$分支$x_1^0,x_2^0$是常数。解密过程为$D(x_1^{10},x_2^{10}\oplus\alpha_0\oplus\alpha_1,x_3^{10},x_4^{10})=(y_1^0,y_2^0,y_3^0,y_4^0)$。如图10所示，在解密阶段(图10的右侧)与加密阶段(图10的左侧)的许多中间状态相同。

从图10的右侧，按照红、蓝线，定义$f(b,x)=y_1^0=R^4(R^7(g(b,x)\oplus\alpha_0\oplus\alpha_1)\oplus x_1^7)\oplus x_2^7$，从图10的左侧，找到$x_1^7=R^7(g(b,x)\oplus x_2^6$。

然后计算$g(b,x)$的布尔表达式。首先定义$h(\alpha_b)=R^3(R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b)$。那么，$g(b,x)=R^6(R^5(R^4(h(\alpha_b)\oplus x)\oplus x_1^0)\oplus R^1(x_1^0)\oplus x_2^0)\oplus R^2(R^1(x_1^0)\oplus x_2^0)\oplus\alpha_b$。与第4.2节相似，$g(b,x)$的周期为$1||h(\alpha_0)\oplus h(\alpha_1)$。同时，$x_1^7=R^7(g(b,x)\oplus x_2^6=R^7(g(b,x))\oplus h(\alpha_b)\oplus x$也有周期$s=1||h(\alpha_0)\oplus h(\alpha_1)$。因此，$g'(b,x)=R^7(g(b,x)\oplus\alpha_0\oplus\alpha_1)\oplus x_1^7$具有周期性，那么有$f(b,x)=R^4(g(b,x))\oplus x_2^7$。由于，$x_2^7=R^4(h(\alpha_b)\oplus x)\oplus x_1^0$具有相同的周期$1||h(\alpha_0)\oplus h(\alpha_1)$。所以$f(b,x)$是周期函数，且周期为$1||h(\alpha_0)\oplus h(\alpha_1)$。

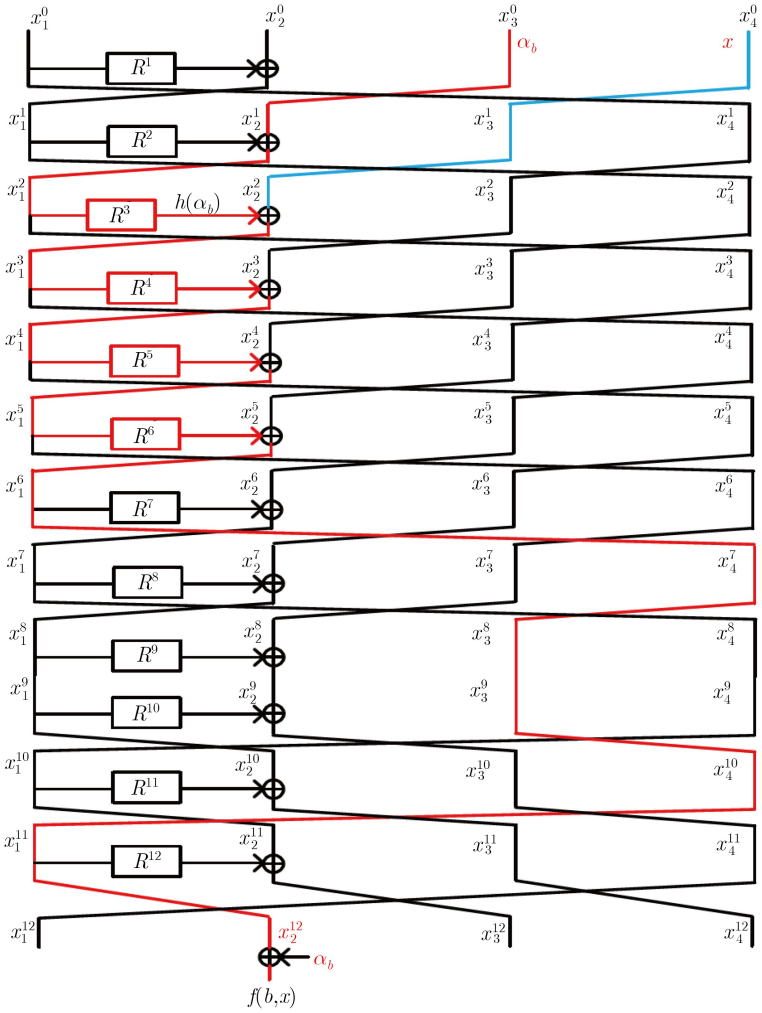


图 8 CAST-256的12轮区分器

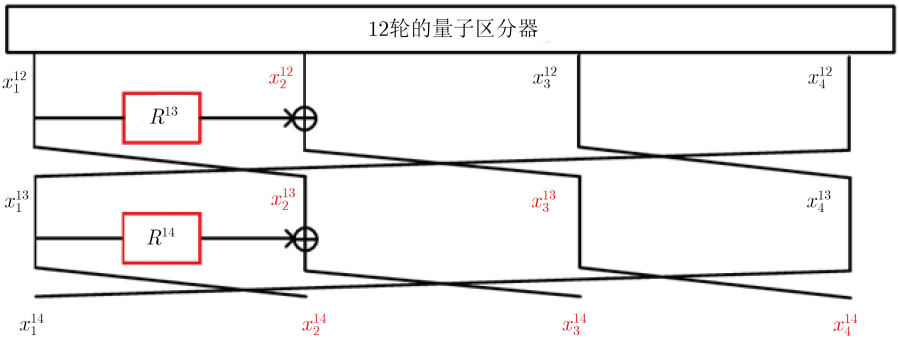


图 9 CAST-256的14轮攻击

与4.2节的密钥恢复攻击类似，当攻击$r(r>13)$轮CAST-256时，使用13轮的区分器，需要猜测前面$(r-13)$轮的所有子密钥，即$(r-13)\times 37$ bit密钥。因此，需要$2^{(r-13)\times 37/2}=2^{18.5r-240.5}$次Grover迭代。

## 6　结束语

本文在qCPA条件下和qCCA条件下，对Type-1 GFS给出了改进的多项式时间量子区分器。

本文给出了在qCPA条件下针对Type-1 GFS的$3d-3$量子区分器，比以前的多了$d-2$轮。因此，可以得到一个更好的密钥恢复攻击，时间复杂度降低了$2^{(d-2)n/2}$。也给出了在qCCA条件下针对Type-1 GFS的$3d-2$量子区分器，比以前的多了$d-1$轮。另外，还讨论了一些针对CAST-256分组密码的量子攻击。

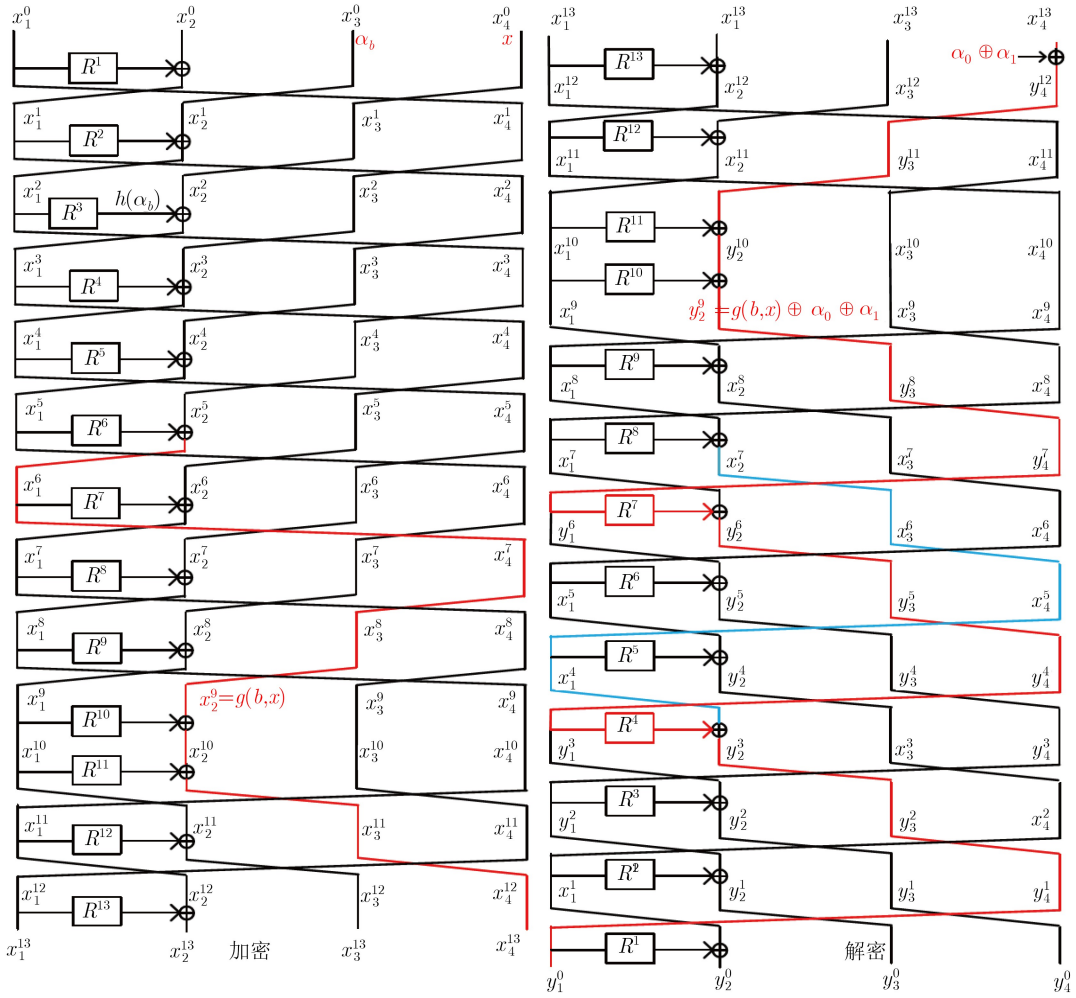


图 10 CAST-256的13轮区分器

## 参 考 文 献


[1] KNUDSEN L R. The security of Feistel ciphers with six rounds or less[J]. *Journal of Cryptology*, 2002, 15(3): 207–222. doi: 10.1007/s00145-002-9839-y.

[2] ISOBE T and SHIBUTANI K. Generic key recovery attack on Feistel scheme[C]. The 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, 2013: 464–485.

[3] GUO Jian, JEAN J, NIKOLIĆ I, *et al*. Meet-in-the-middle attacks on generic Feistel constructions[C]. The 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, China, 2014: 458–477.

[4] DINUR I, DUNKELMAN O, KELLER N, *et al*. New attacks on Feistel structures with improved memory complexities[C]. The 35th Annual Cryptology Conference, Santa Barbara, USA, 2015: 433–454.

[5] AOKI K, ICHIKAWA T, KANDA M, *et al*. *Camellia*: A 128-bit Block Cipher Suitable for Multiple Platforms - Design and Analysis[M]. Berlin, Heidelberg: Springer, 2001: 39–56.

[6] National Soviet Bureau of Standards. GOST 28147-89 Information processing systems. cryptographic protection cryptographic transformation algorithm[S]. 1989.

[7] ZHENG Yuliang, MATSUMOTO T, and IMAI H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses[C]. Conference on the Theory and Application of Cryptology, Santa Barbara, USA, 1990: 461–480.

[8] ANDERSON R and BIHAM E. Two practical and provably secure block ciphers: BEAR and LION[C]. The 3rd International Workshop on Fast Software Encryption, Cambridge, UK, 1996: 113–120.

[9] LUCKS S. Faster luby-rackoff ciphers[C]. The 3rd International Workshop on Fast Software Encryption, Cambridge, UK, 1996: 189–203.

[10] SCHNEIER B and KELSEY J. Unbalanced Feistel networks and block cipher design[C]. The 3rd International Workshop on Fast Software Encryption, Cambridge, UK, 1996: 121–144.

[11] First AES Candidate Conference[EB/OL]. http://csrc.nist.gov/archive/aes/round1/conf1/aes1conf.htm.

[12] SHIRAI T, SHIBUTANI K, AKISHITA T, *et al*. The 128-bit blockcipher CLEFIA (extended abstract)[C]. The 14th International Workshop on Fast Software Encryption, Luxembourg, Luxembourg, 2007: 181–195.

[13] GUERON S and MOUHA N. Simpira v2: A family of efficient permutations using the AES round function[C]. The 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016: 95–125.

[14] LUBY M and RACKOFF C. How to construct pseudorandom permutations from pseudorandom functions[J]. *SIAM Journal on Computing*, 1988, 17(2): 373–386. doi: 10.1137/0217022.

[15] MORIAI S and VAUDENAY S. On the pseudorandomness of top-level schemes of block ciphers[C]. The 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, 2000: 289–302.

[16] HOANG V T and ROGAWAY P. On generalized Feistel networks[C]. The 30th Annual Cryptology Conference, Santa Barbara, USA, 2010: 613–630.

[17] JUTLA C S. Generalized birthday attacks on unbalanced Feistel networks[C]. The 18th Annual International Cryptology Conference, Santa Barbara, USA, 1998: 186–199.

[18] GUO Jian, JEAN J, NIKOLIC I, *et al*. Meet-in-the-middle attacks on classes of contracting and expanding Feistel constructions[J]. *IACR Transactions on Symmetric Cryptology*, 2016(2): 307–337.

[19] NACHEF V, VOLTE E, and PATARIN J. Differential attacks on generalized Feistel schemes[C]. The 12th International Conference on Cryptology and Network Security, Paraty, Brazil, 2013: 1–19.

[20] TJUAWINATA I, HUANG Tao, and WU Hongjun. Improved differential cryptanalysis on generalized Feistel schemes[C]. The 18th International Conference on Cryptology in India, Chennai, India, 2017: 302–324.

[21] PATARIN J, NACHEF V, and BERBAIN C. Generic attacks on unbalanced Feistel schemes with contracting functions[C]. The 12th International Conference on the Theory and Application of Cryptology and Information Security, Shanghai, China, 2006: 396–411.

[22] PATARIN J, NACHEF V, and BERBAIN C. Generic attacks on unbalanced Feistel schemes with expanding functions[C]. The 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2007: 325–341.

[23] VOLTE E, NACHEF V, and PATARIN J. Improved generic attacks on unbalanced Feistel schemes with expanding functions[C]. The 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 2010: 94–111.

[24] GROVER L K. A fast quantum mechanical algorithm for database search[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, USA, 1996: 212–219.

[25] KUWAKADO H and MORII M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C]. IEEE International Symposium on Information Theory, Austin, USA, 2010: 2682–2685.

[26] SIMON D R. On the power of quantum computation[J]. *SIAM Journal on Computing*, 1997, 26(5): 1474–1483. doi: 10.1137/S0097539796298637.

[27] KUWAKADO H and MORII M. Security on the quantum-type even-mansour cipher[C]. 2012 International Symposium on Information Theory and its Applications, Honolulu, USA, 2012: 312–316.

[28] KAPLAN M, LEURENT G, LEVERRIER A, *et al*. Breaking symmetric cryptosystems using quantum period finding[C]. The 36th Annual International Cryptology Conference, Santa Barbara, USA, 2016: 207–237.

[29] BONNETAIN X. Quantum key-recovery on full AEZ[C]. The 24th International Conference on Selected Areas in Cryptography, Ottawa, Canada, 2018: 394–406.

[30] LEANDER G and MAY A. Grover meets simon - quantumly attacking the FX-construction[C]. The 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 2017: 161–178.

[31] ZHANDRY M. How to construct quantum random functions[C]. The 53rd IEEE Annual Symposium on Foundations of Computer Science, New Brunswick, USA, 2012: 679–687.

[32] ITO G, HOSOYAMADA A, MATSUMOTO R, *et al*. Quantum chosen-ciphertext attacks against Feistel ciphers[C]. The Cryptographers' Track at the RSA Conference, San Francisco, USA, 2019: 391–411.

[33] HOSOYAMADA A and SASAKI Y. Quantum demiric-selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions[C]. The 11th International Conference on Security and Cryptography for Networks, Amalfi, Italy, 2018: 386–403.

[34] DONG Xiaoyang and WANG Xiaoyun. Quantum key-recovery attack on Feistel structures[J]. *Science China Information Sciences*, 2018, 61(10): 102501. doi: 10.1007/s11432-017-9468-y.

[35] DONG Xiaoyang, LI Zheng, and WANG Xiaoyun. Quantum cryptanalysis on some generalized Feistel schemes[J]. *Science China Information Sciences*, 2019,

62(2): 22501. doi: 10.1007/s11432-017-9436-7.

[36] DONG Xiaoyang, DONG Bingyou, and WANG Xiaoyun. Quantum attacks on some Feistel block ciphers[R]. Cryptology ePrint Archive, Report 2018/504, 2018.

[37] BONNETAIN X, NAYA-PLASENCIA M, and SCHROTTENLOHER A. On quantum slide attacks[R]. Cryptology ePrint Archive, Report 2018/1067, 2018.

[38] HOSOYAMADA A and IWATA T. Tight quantum security bound of the 4-round luby-rackoff construction[R]. Cryptology ePrint Archive, Report 2019/243, 2019.

[39] WAGNER D. The boomerang attack[C]. The 6th International Workshop on Fast Software Encryption, Rome, Italy, 1999: 156–170.

[40] WANG Meiqin, WANG Xiaoyun, and HU Changhui. New linear cryptanalytic results of reduced-round of CAST-128 and CAST-256[C]. The 15th International Workshop on Selected Areas in Cryptography, Sackville, Canada, 2009: 429–441.

[41] BOGDANOV A, LEANDER G, NYBERG K, *et al*. Integral and multidimensional linear distinguishers with correlation zero[C]. The 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 2012: 244–261.

董晓阳：男，1988年生，助理研究员。研究方向为对称密码算法的安全性分析与设计.