软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(9):4239−4255 [doi: 10.13328/j.cnki.jos.006636]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于周期性质的新型密钥恢复攻击方法*

邹 剑[1,2], 邹宏楷[1,2], 董晓阳[3], 吴文玲[4], 罗宜元[5]

[1](福州大学 计算机与大数据学院, 福建 福州 350108)

[2](网络系统信息安全福建省高校重点实验室 (福州大学), 福建 福州 350108)

[3](清华大学 高等研究院, 北京 100190)

[4](中国科学院 软件研究所 可信计算与信息保障实验室, 北京 100190)

[5](惠州学院 信息科学技术学院, 广东 惠州 516007)

通信作者: 邹剑, E-mail: fzuzoujian15@163.com

摘　要: 针对 Feistel, Misty 与 Type-1/2 型广义 Feistel 等结构, 创新性地将 Simon 算法的周期性质与生日攻击思想相结合, 提出一种新型传统密钥恢复攻击. 与 Simon 算法可以在多项式时间内恢复周期值不同, 在传统计算环境下至少需要生日攻击界才能恢复出对应的周期值. 利用所提方法, 可以在 $O(2^{n/4})$ 的选择明文和密文条件下, 以 $O(2^{3n/4})$ 的时间复杂度恢复出 5 轮 Feistel-F 结构的密钥, 对应的存储复杂度为 $O(2^{n/4})$. 上述结果比 Isobe 和 Shibutani 的工作结果多扩展 1 轮, 并且所需的存储复杂度也更少. 对于 Feistel-FK 结构, 构造 7 轮密钥恢复攻击. 此外, 还将上述方法应用于构造 Misty 结构和 Type-1/2 型广义 Feistel 结构的密钥恢复攻击. 对于不同的 Misty 密码方案, 分别给出 5 轮 Misty L-F 和 Misty R-F 结构的密钥恢复攻击, 以及 6 轮 Misty L-KF/FK 和 Misty R-KF/FK 结构的密钥恢复攻击. 对于 d 分支 Type-1 型广义 Feistel 结构, 给出 d^2 轮的密钥恢复攻击. 当 $d\geqslant 6$ 时, 对于 d 分支 Type-2 型广义 Feistel 结构的新型密钥恢复攻击轮数会优于现有密钥恢复攻击轮数.

关键词: Feistel; Misty; Type-1/2 型广义 Feistel 结构; 密钥恢复攻击; Simon 算法; 周期性质; 生日攻击

中图法分类号: TP309

中文引用格式: 邹剑, 邹宏楷, 董晓阳, 吴文玲, 罗宜元. 基于周期性质的新型密钥恢复攻击方法. 软件学报, 2023, 34(9): 4239–4255. http://www.jos.org.cn/1000-9825/6636.htm

英文引用格式: Zou J, Zou HK, Dong XY, Wu WL, Luo YY. New Key Recovery Attack Based on Periodic Property. Ruan Jian Xue Bao/Journal of Software, 2023, 34(9): 4239–4255 (in Chinese). http://www.jos.org.cn/1000-9825/6636.htm

New Key Recovery Attack Based on Periodic Property

ZOU Jian[1,2], ZOU Hong-Kai[1,2], DONG Xiao-Yang[3], WU Wen-Ling[4], LUO Yi-Yuan[5]

[1](College of Computer and Data Science, Fuzhou University, Fuzhou 350108, China)

[2](Key Lab of Information Security of Network Systems (Fuzhou University), Fuzhou 350108, China)

[3](Institute for Advanced Study, Tsinghua University, Beijing 100190, China)

[4](Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[5](School of Information Sciences and Technology, Huizhou University, Huizhou 516007, China)

Abstract: This study proposes a new classical key recovery attack against schemes such as Feistel, Misty, and Type-1/2 generalized Feistel schemes (GFS), which creatively combines the birthday attack with the periodic property of Simon's algorithm. Although Simon's algorithm can recover the periodic value in polynomial time, this study requires the birthday bound to recover the corresponding periodic value in the classical setting. By this new attack, the key to a 5-round Feistel-F scheme can be recovered with the time complexity of

* 基金项目: 国家自然科学基金 (61902073, 62072445, 62072207, 62072109, U1804263); 福建省自然科学基金 (2021J01623, 2021J06013)
收稿时间: 2021-11-01; 修改时间: 2021-12-02; 采用时间: 2021-12-23; jos 在线出版时间: 2022-03-24
CNKI 网络首发时间: 2023-02-23

$O(2^{3n/4})$ under the chosen plaintexts and ciphertexts of $O(2^{n/4})$, and the corresponding memory complexity is $O(2^{n/4})$. Compared with the results of Isobe and Shibutani, the above result not only increases one round but also requires lower memory complexity. For the Feistel-FK scheme, a 7-round key recovery attack is constructed. In addition, the above approach is applied to construct the key recovery attacks against Misty schemes and Type-1/2 GFS. Specifically, the key recovery attacks against the 5-round Misty L-F and Misty R-F schemes and those against the 6-round Misty L-KF/FK and Misty R-KF/FK schemes are given; for the d-branch Type-1 GFS, a d^2-round key recovery attack is presented, and when $d\geqslant 6$, the number of rounds of the key recovery attack is superior to those of the existing key recovery attacks.

Key words: Feistel; Misty; Type-1/2 GFS; key recovery attack; Simon's algorithm; periodic property; birthday attack

分组密码是一种重要的底层加密技术, 在网络空间安全中扮演关键角色. Feistel 结构[1]是一种广泛应用于分组密码设计中的对称结构. 很多密码标准算法都采用了 Feistel 结构, 包括 DES, GOST[2], Camellia[3]等分组密码. Feistel 结构不仅具有加解密相似的特点, 而且对底层轮函数没有太多限制. 由于上述设计优点, Feistel 结构受到许多密码设计者的关注, 并衍生出多个相似密码结构的设计, 如 Misty[4], Type-1 型广义 Feistel 结构[5]等. 对于这些 Feistel 结构的变体, 也都有对应的设计方案. 例如, 分组密码 Kasumi[6]的设计采用了 Misty 结构, CAST-256[7]的设计则是基于 Type-1 型广义 Feistel 结构.

对于 Feistel 结构, 研究人员目前已经做了许多研究工作. 在 SAC2012 会议上, Isobe 等人[8]利用扩展的中间相遇攻击方法, 对 Feistel 结构构造了对应的子密钥恢复攻击. 在 Asiacrypt2013 会议上, Isobe 等人[9]利用中间相遇攻击、切割缝合与函数约简等方法, 对 Feistel 结构给出了改进的密钥恢复攻击. 此外, 目前关于 Feistel 及其衍生结构还有一系列传统攻击结果, 有兴趣的读者请参阅文献[10−14].

近年来, 借助 Grover[15]、Simon[16]等高效的量子算法, 许多研究者也分析了 Feistel 结构在量子环境下的安全性. 在 2010 年, Kuwakado 等人[17]提出了 3 轮 Feistel 结构的量子区分器. 借助 Simon 算法, 他们可以在多项式的时间内将 3 轮的 Feistel 结构和随机置换区分开来. 上述结果表明 3 轮的 Feistel 结构在量子选择明文攻击 (qCPA) 下不再安全. 随后, Dong 等人利用 Grover 与 Simon 的组合算法[18], 对于 r 轮 Feistel 结构构造了对应的量子密钥恢复攻击[19]. 此外, Ito 等人[20]在量子选择密文攻击 (qCCA) 场景下对 Feistel 类结构构造了相应的量子区分器.

Misty[4]结构可以细分为 Misty L 与 Misty R 两种结构. 在文献 [21] 中, Luo 等人利用 Simon 算法分别对 Misty L 和 Misty R 结构构造了 3 轮 qCPA 区分器. 2020 年, Gouget 等人[22]改进了这一结果, 给出了一个 4 轮 Misty L 结构的 qCPA 区分器. 随后, Cui 等人[23]对 Misty 结构进行了更详细的量子密码分析. 在 qCPA 攻击假设下, 他们对 Misty L-KF 和 Misty L-FK 分别构造了 5 轮的量子区分器. 在 qCCA 攻击假设下, 他们对 Misty R 结构构造了 4 轮的量子区分器. 此外, Cui 等人还对 Misty R-KF 和 Misty R-FK 构造了 5 轮的量子区分器.

Type-1/2 型广义 Feistel 结构 (Type-1/2 GFS)[5]是 Feistel 结构的一个推广, 近些年也备受研究人员的关注. 基于中间相遇攻击的方法, Deng 等人[24]对 d 分支数 Type-1 GFS 提出了 $(5d-3)$ 轮传统密钥恢复攻击. 在量子环境下, Dong 等人[25]对于 Type-1 GFS 构造了 $(2d-1)$ 轮的 qCPA 区分攻击. 随后, Ni 等人[26]进一步改进了这一结果, 对 Type-1 GFS 分别提出了 $(3d-3)$ 轮的 qCPA 区分器和 (d^2-d+1) 轮的 qCCA 区分器. 对于 d 分支数 Type-2 GFS (d 为偶数), 邓元豪[27]利用中间相遇攻击的方法, 对 d 分支数 Type-2 GFS 提出了 $(d+3)$ 轮传统密钥恢复攻击. 在量子环境下, Dong 等人[25]对于 d 分支数 Type-2 GFS 构造了 $(d+1)$ 轮的 qCPA 区分攻击, 后面 Luo 等人[21]修正了他们的结果. 我们将对于 Feistel、Misty 与 Type-1/2 GFS 等结构的量子区分器攻击结果总结在表 1 中.

本文的创新点可以总结如下. 虽然在传统环境下我们无法使用 Simon 算法来恢复周期值, 但是借助生日攻击界, 我们仍然能以低于穷举攻击的代价对于 Feistel、Misty 与 Type-1 GFS 等结构构造新的密钥恢复攻击. 与以往传统密钥恢复攻击不同, 我们新型密钥恢复攻击是将目标结构量子区分器的周期函数与生日攻击思想相结合, 通过寻找碰撞恢复对应的周期值, 并以此作为区分器进行密钥恢复攻击. 基于本文提出的新方法, 攻击者可以在 $O(2^{3n/4})$ 时间复杂度和 $O(2^{n/4})$ 的存储复杂度下, 恢复出 5 轮 Feistel-F 结构的密钥. 相比于文献 [9] 中的攻击结果, 本文的密钥恢复攻击结果不仅增加了一轮, 而且所需的存储复杂度也更少. 与文献 [10] 的结果对比, 本文所需的攻击时间复杂度和存储复杂度都要更少. 本文还将上述思想扩展到 Feistel-FK 结构, Misty 结构以及 Type-1 GFS

的密钥恢复攻击中, 攻击结果详见表 2 中. 由表 2 的结果可得, 我们攻击均优于现有分析结果. 此外, 需要注意的是, 表 2 中仅展示了当目标结构的轮函数为随机函数时, 本文攻击所需的复杂度. 若目标结构的轮函数为随机置换时, 本文的密钥恢复攻击所需复杂度则更低.

表 1　目标结构的最优量子区分器

目标	轮数	量子区分器类型	文献来源
Feistel-F	4	qCCA	[20]
Feistel-FK	6	qCCA	[20]
Misty L-F	4	qCPA	[22,23]
Misty R-F	4	qCCA	[23]
Misty L-KF/Misty L-FK	5	qCPA	[23]
Misty R-KF/Misty R-FK	5	qCCA	[23]
Type-1 GFS (d分支)	(d^2-d+1)	qCCA	[26]
Type-2 GFS (d分支, d为偶数)	d+1	qCPA	[21,25]

表 2　对于 Feistel、Misty 和 Type-1 GFS 结构的传统密钥恢复攻击

目标	轮数	时间复杂度	数据复杂度	存储复杂度	文献来源
Feistel-F	4	$O(2^{3n/4+2})$	$O(2^{n/4})$ CP	$O(2^{3n/4+2})$	[9]
	5	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CP和CC	$O(2^{(n+2)/4})$	本文
	5	$O(2^n)$	3 KP	$O(2^{n/2})$	[10]
Feistel-FK	7	$O(2^{n/2})$	$O(2^{n/3+1})$ CP和CC	$O(2^{n/2+1})$	[13]
	7	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CP和CC	$O(2^{(n+2)/4})$	本文
Misty L-F	5	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CP	$O(2^{(n+2)/4})$	本文
Misty R-F	5	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CC	$O(2^{(n+2)/4})$	本文
Misty L-KF/-FK	6	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CP	$O(2^{(n+2)/4})$	本文
Misty R-KF/-FK	6	$O(2^{(3n+2)/4})$	$O(2^{(n+2)/4})$ CC	$O(2^{(n+2)/4})$	本文
Type-1 GFS	$5d-3$	$O(2^{\frac{(d-1)n}{d}})$	$O(2^{\frac{3}{d}n})$ CP	$O(2^{\frac{(d-1)n}{d}})$	[24]
	d^2	$O(2^{\frac{(2d-1)n+d}{2d}})$	$O(2^{\frac{n+d}{2d}})$ CC	$O(2^{\frac{n+d}{2d}})$	本文

注: CP为选择明文, KP为已知明文, CC为选择密文

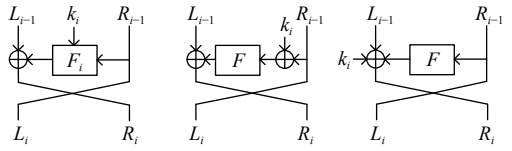
本文第 1 节介绍一些预备知识, 包括本文攻击的各类目标结构等. 第 2 节梳理总结 Simon 问题及其应用, 包含 3 轮 Feistel 结构量子区分器的构造过程, 以及对 Even-Mansour 结构滑动攻击的构造过程. 第 3 节提出对 5 轮 Feistel-F 结构和 7 轮 Feistel-FK 结构的新型密钥恢复攻击. 在第 4 节和第 5 节中, 我们分析 Misty 结构和 Type-1/2 GFS 的密钥恢复攻击. 最后第 6 节总结全文, 并提出后续研究的方向.

1　基础知识

1.1　Feistel 结构

本文假设 Feistel 结构的输入为 n 比特, 并且采用平衡结构, 即其左右分支状态均为 $n/2$ 比特. 下文中我们将 Feistel 结构的轮函数记为 F_i, 并设其输入轮密钥 k_i 的长度也为 $n/2$ 比特. 根据输入密钥注入位置的不同, Feistel 结构可以细分为 3 种类型. 本文遵循了 Ito 等人在文献 [20] 中的命名方式. 如图 1(a) 所示, 当密钥在轮函数中时, 即轮函数为 $F_i(R_{i-1})=F_{k_i}(R_{i-1})$ 时, 我们将其命名为 Feistel-F 结构; 当密钥 k_i 在公开置换 F 之前时, 即轮函数为

$F_i(R_{i-1}) = F(R_{i-1} \oplus k_i)$ 时, 我们将其记为 Feistel-KF 结构 (见图 1(b)); 当密钥 k_i 在公开置换 F 之后时, 即轮函数为 $F_i(R_{i-1}) = F(R_{i-1}) \oplus k_i$, 我们将其记为 Feistel-FK 结构 (见图 1(c)).

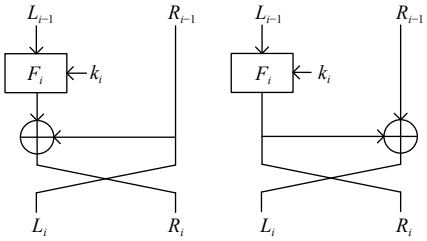


(a) Feistel-F结构 (b) Feistel-KF结构 (c) Feistel-FK结构

图 1 3 种 Feistel 结构

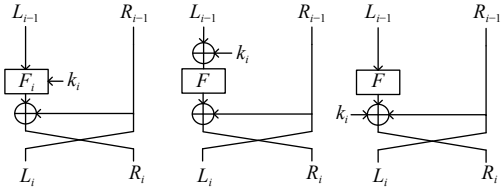
1.2 Misty 结构

本文假设 Misty 结构的输入是 n 比特, 则其左右分支均为 $n/2$ 比特. 下文我们将 Misty 结构的轮函数记为 F_i, 并设其轮密钥 k_i 的长度为 $n/2$ 比特. 根据异或位置的不同, Misty 可以分为 L 和 R 两种结构. 如图 2(a) 所示, 设 Misty L 结构第 i 轮的输入状态为 (L_{i-1}, R_{i-1}), 则其第 i 轮的输出状态 (L_i, R_i) 可以表示为 $(L_i, R_i) \leftarrow (R_{i-1}, F_i(k_i, L_{i-1}) \oplus R_{i-1})$. 类似地, 如图 2(b) 所示, Misty R 结构第 i 轮的输出状态 (L_i, R_i) 可以表示为 $(L_i, R_i) \leftarrow (R_{i-1} \oplus F_i(k_i, L_{i-1}), F_i(k_i, L_{i-1}))$.



(a) Misty L (b) Misty R

图 2 Misty L 和 Misty R 结构



(a) Misty L-F (b) Misty L-KF (c) Misty L-FK

图 3 3 种 Misty L 方案

根据密钥注入的方式, 我们可以将 Misty L 结构分为 3 种方案, 分别为 Misty L-F, Misty L-KF 和 Misty L-FK, 如图 3 所示.

类似地, Misty R 结构也可以分为 Misty R-F, Misty R-KF 和 Misty R-FK.

1.3 Type-1 GFS

文中假设 n 比特的 Type-1 GFS 可以划分成 d 个分支 ($d \geqslant 3$), 每个分支输入与轮密钥 k_i 的大小都为 n/d 比特. 如图 4 所示, 假设第 i 轮 Type-1 GFS 的输入状态是 $(x_0^{i-1}, x_1^{i-1}, \ldots, x_{d-1}^{i-1}) \in (\{0,1\}^{n/d})^d$, 则它的输出状态可以表示为: $(x_0^i, x_1^i, \ldots, x_{d-1}^i) \leftarrow (F_i(x_0^{i-1}, k_i) \oplus x_1^{i-1}, x_2^{i-1}, \ldots, x_{d-1}^{i-1}, x_0^{i-1})$. Type-1 GFS 的解密函数是通过反转分支移位的方向来实现的.

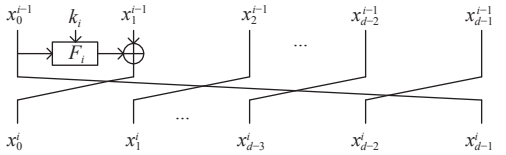


图 4 第 i 轮 Type-1 型广义 Feistel 结构

1.4 Type-2 GFS

文中假设 n 比特的 Type-2 GFS 可以划分成 d 个分支, 其中 d 为偶数. 如图 5 所示, d 个分支 Type-2 GFS 在第 i 轮包含 $d/2$ 个轮函数, 其每个输入分支大小都为 n/d 比特, 且需要 $d/2$ 个输入大小为 n/d 比特轮密钥 k_{ij}. 假设第 i 轮的输入状态是 $(x_1^{i-1}, x_2^{i-1}, \ldots, x_d^{i-1}) \in (\{0,1\}^{n/d})^d$, 则它对应的输出状态 $(x_1^i, x_2^i, \ldots, x_d^i) \in (\{0,1\}^{n/d})^d$ 可以表示为: $(x_1^i, x_2^i, \ldots, x_d^i) \leftarrow (F_1^i(x_1^{i-1}, k_{i1}) \oplus x_2^{i-1}, x_3^{i-1}, \ldots, F_{d/2}^i(x_{d-1}^{i-1}, k_{id/2}) \oplus x_d^{i-1}, x_1^{i-1})$.

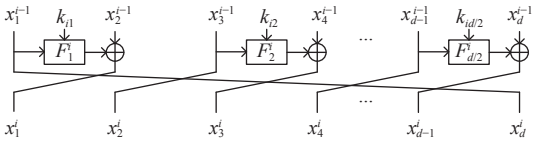


图 5　第 i 轮 Type-2 型广义 Feistel 结构

2　Simon 算法周期性质及其应用

2.1　Simon 算法及其应用

Simon 算法[16]能用于求解隐藏周期问题, 具体如下.

Simon 问题. 给定一个布尔函数 $f:\{0,1\}^n\to\{0,1\}^n$, 假设该函数 f 要么是单射函数, 要么会满足如下承诺: 存在 $s\in\{0,1\}^n$, 使得对于任意的 $x,y\in\{0,1\}^n$, 有 $f(x)=f(y)\Leftrightarrow x=y$ 或 $x=y\oplus s$. 敌手的目标是找到周期值 s.

在量子环境下, 敌手可以利用 Simon 算法在 $O(n)$ 的量子查询复杂度下找到周期 s. 不同于量子环境, 敌手在传统环境下只用找碰撞的方法来解决 Simon 问题, 即至少需要 $O(2^{n/2})$ 的时间复杂度.

在文献 [17] 中, Kuwakado 等人发现 3 轮 Feistel-F 具有周期性质, 并以此构造了一个 qCPA 量子区分器攻击. 如图 6 所示, 假设 3 轮 Feistel-F 的输入为 (x,α_b), 其中包含轮密钥 k_i 的轮函数用 F_i 简化表示, 则对应的 3 轮输出为 (L_3,R_3). 利用 L_3 的输出值, Kuwakado 等人可以按下式构造周期函数: $f(b,x)=\alpha_b\oplus L_3=F_2(x\oplus F_1(\alpha_b))$, 其中 $b\in\{0,1\}$, $x,\alpha_b\in\{0,1\}^{n/2}$, 而且 α_0 和 α_1 是两个不同的常数. 由于 $f(b,x)=f(b\oplus 1,x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))$, 函数 $f(b,x)$ 至少存在一个周期 $s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$. 当轮函数 F_i 是随机置换时, 上述 3 轮周期函数完全满足 Simon 承诺. 因为随机置换是一一对应的, 所以只有当输入差分为 0 时输出差分才为 0. 换句话说, 给定 3 轮周期函数 f 的任意一个碰撞对 $f(x)=f(y)$, 则敌手一定能恢复出对应的周期值 $s=x\oplus y$. 利用 Simon 算法, Kuwakado 等人可以在多项式时间内获得周期 s.

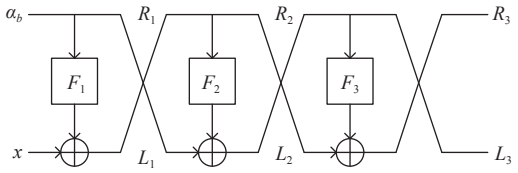


图 6　3 轮 Feistel-F 结构的量子区分器

注意到, 当轮函数 F_i 是随机函数时, 则上述 3 轮周期函数 f 不完全满足 Simon 承诺. 因为随机函数可以满足多对一的关系, 所以当随机函数的输入差分不为 0 时, 输出差分也有可能为 0. 此时, 对于周期函数 f, 可能存在 $t\neq F_1(\alpha_0)\oplus F_1(\alpha_1)$, 使得 $f(b,x)=f(b\oplus 1,x\oplus t)$. 在这种情况下, 敌手从一个碰撞对 $f(x_1)=f(y_1)$ 所恢复出的周期值 $s_1=x_1\oplus y_1$ 不一定是对应的周期值. 针对上述问题, Kaplan 等人[28]提出可以通过多次调用 Simon 算法来提高获得正确周期值的成功率.

除了 3 轮 Feistel-F 结构外, 2 轮 Feistel-F 结构同样具有周期性质. 下面给出引理 1.

引理 1. 2 轮的 Feistel-F 结构也具有周期性质.

证明: 与 3 轮 Feistel-F 结构类似, 敌手需已知第 2 轮状态值 (L_2,R_2) 来构造 2 轮 Feistel-F 结构的周期函数.

给定第 2 轮状态值 (L_2,R_2), 敌手可按如下方法构造 2 轮 Feistel-F 结构的周期函数: $f_2(b,x)=L_2=x\oplus F_1(\alpha_b)$. 因为 f_2 满足如下关系: $f_2(b\oplus 1,x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))=x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1)\oplus F_1(\alpha_{b\oplus 1})=x\oplus F_1(\alpha_b)=f_2(b,x)$.

因此, 函数 f_2 具有周期 $s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$, 也即 2 轮 Feistel-F 结构具有周期性.

综上, 引理 1 成立.

2.2 对 Even-Mansour 结构的滑动攻击

Even-Mansour (EM) 算法[29]由一个 n 比特的公开置换 F 和两个 n 比特密钥 k_1 和 k_2 组成, 如图 7 所示. 设 E 表示 EM 结构的加密算法, 则 EM 结构可描述为: $E(x)=F(x\oplus k_1)\oplus k_2$. 在文献 [30] 中, Biryukov 等人对 EM 结构构造了一种新型滑动攻击, 其主要思想如下. 假设 E 以两个明文 x,x' 作为输入, 并满足 $x\oplus x'=k_1$. 因为 $E(x)=F(x\oplus k_1)\oplus k_2=F(x')\oplus k_2$, 且 $E(x')=F(x'\oplus k_1)\oplus k_2=F(x)\oplus k_2$, 易得 $E(x)\oplus F(x)=E(x')\oplus F(x')$. 利用上述关系, 敌手可以构造以下攻击.

(1) 随机挑选 $2^{(n+1)/2}$ 个已知明文 $x_1,x_2,x_3,\ldots$ 访问查询 E 函数和 F 函数, 并将结果 $(E(x_i)\oplus F(x_i),i)$ 存储在一个哈希表中.

(2) 根据哈希表中的每个碰撞: $E(x_i)\oplus F(x_i)=E(x_j)\oplus F(x_j)$, 敌手可以得到正确猜测的密钥值 $k_1=x_i\oplus x_j$ 和 $k_2=E(x_i)\oplus F(x_j)$.

根据生日悖论, 敌手大概率可以找到一个碰撞对 $E(x_i)\oplus F(x_i)=E(x_j)\oplus F(x_j)$. 利用该滑动对, 敌手可以得到 k_1 和 k_2 的正确值. 攻击需要 $2^{(n+1)/2}$ 个已知明文和 $2^{(n+1)/2}$ 次对 E 函数和 F 函数的查询. 上述攻击可以视为是用生日攻击恢复 EM 结构的 Simon 周期值, 因此可以看作是对 EM 结构 Simon 算法找周期的传统化.

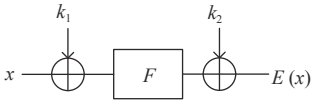


图 7 Even-Mansour 结构

3 对 Feistel 结构的密钥恢复攻击

受 Biryukov 等人[30]工作的启发, 本文通过结合 Simon 算法的周期函数和生日攻击的思想, 提出了针对 Feistel-F 和 Feistel-FK 结构的新型密钥恢复攻击.

3.1 4 轮 Feistel-F 结构的 qCCA 区分器

Ito 等人在文献 [20] 中提出了一个具有周期性质的 4 轮 Feistel-F 结构 qCCA 区分器, 比 Kuwakado 等人[17]的 3 轮区分器结果多扩展了一轮. 他们 4 轮 Feistel-F 结构的 qCCA 区分器如图 8 所示, 其中 EF_4 表示 4 轮 Feistel-F 结构的加密算法, DF_4 表示 4 轮 Feistel-F 结构的解密算法. 设 $\alpha_0,\alpha_1\in\{0,1\}^{n/2}$ 是两个任意且不同的常数. EF_4 以 (x,α_b) 作为输入明文, 其中 $b\in\{0,1\}$, $x\in\{0,1\}^{n/2}$, 则输出的密文 (L_4,R_4) 可以描述如下:

$$L_4=x\oplus F_1(\alpha_b)\oplus F_3(\alpha_b\oplus F_2(x\oplus F_1(\alpha_b))),\quad R_4=\alpha_b\oplus F_2(x\oplus F_1(\alpha_b))\oplus F_4(x\oplus F_1(\alpha_b)\oplus F_3(\alpha_b\oplus F_2(x\oplus F_1(\alpha_b)))).$$

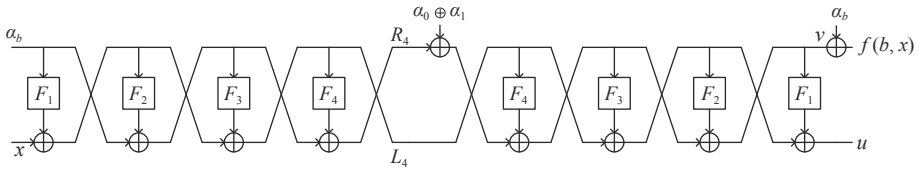


图 8 4 轮 Feistel-F 结构的 qCCA 区分器

由上式, 敌手若以 $(L_4,R_4\oplus\alpha_0\oplus\alpha_1)$ 作为 DF_4 的输入, (u,v) 作为输出, 则有:

$$u=L_4\oplus F_3(R_4\oplus\alpha_0\oplus\alpha_1\oplus F_4(L_4))\oplus F_1(R_4\oplus\alpha_0\oplus\alpha_1\oplus F_4(L_4)\oplus F_2(L_4\oplus F_3(R_4\oplus\alpha_0\oplus\alpha_1\oplus F_4(L_4)))),$$

$$v=R_4\oplus\alpha_0\oplus\alpha_1\oplus F_4(L_4)\oplus F_2(L_4\oplus F_3(R_4\oplus\alpha_0\oplus\alpha_1\oplus F_4(L_4))).$$

假设敌手有量子查询问答机 O 和 O^{-1}, 其中 O 要么是 EF_4, 要么是一个随机置换. 为了区分上述两种情形, 敌手可以构造如下函数:

$$\begin{cases} f:\{0,1\}\times\{0,1\}^{n/2}\to\{0,1\}^{n/2} \\ (b,x)\mapsto v\oplus\alpha_b \end{cases}.$$

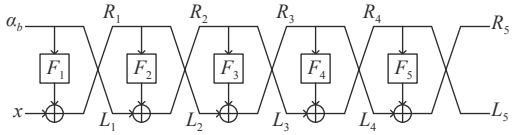
如果O是EF_4, O^{-1}是DF_4, 则函数f可以描述为:

$f(b,x)=\alpha_0\oplus\alpha_1\oplus F_2(x\oplus F_1(\alpha_b))\oplus F_2(x\oplus F_1(\alpha_b)\oplus F_3(\alpha_b\oplus F_2(x\oplus F_1(\alpha_b))))\oplus F_3(\alpha_b\oplus\alpha_0\oplus\alpha_1\oplus F_2(x\oplus F_1(\alpha_b)))$.

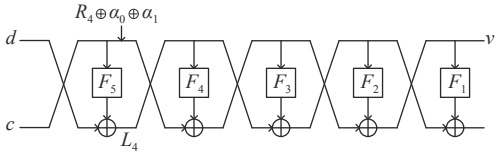
在文献 [20] 中, Ito 等人证明了函数f满足如下关系: $f(b,x)=f(b\oplus 1,x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))$. 详细证明过程可以参见文献 [20]. 因此, 当O是EF_4时, f是一个周期函数, 周期为$s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$. 当$O$是一个随机置换时, 对应的函数$f$则没有周期. 基于上述性质, 敌手可以利用 Simon 算法在多项式时间内将 4 轮 Feistel-F 结构和一个随机置换区分开来.

3.2 5 轮 Feistel-F 结构的密钥恢复攻击

本节通过结合 Simon 周期函数和生日攻击的思想, 针对 Feistel-F 结构构造了 5 轮传统选择密文恢复密钥攻击, 具体的攻击过程详见图 9. 假设EF_5表示 5 轮 Feistel-F 结构的加密算法 (详见图 9(a)), DF_5表示其解密算法 (详见图 9(b)). EF_5以(x,α_b)作为输入, 其中$b\in\{0,1\}$, $x\in\{0,1\}^{n/2}$. 设(L_i,R_i)表示第i轮的输出, 第 5 轮的输出$(L_5,R_5)=EF_5(x,\alpha_b)$. 依据图 9(a), $L_4=R_5\oplus F_5(L_5)$, $R_4=L_5$. 若给定一个密钥值k_5和第 5 轮的输出(L_5,R_5), 敌手便可以解密得到对应的第 4 轮状态值(L_4,R_4).



(a) 加密过程



(b) 解密过程

图 9 5 轮 Feistel-F 结构的密钥恢复攻击

对于给定的(L_4,R_4), 我们可以利用第 3.1 节的 4 轮 qCCA 区分器, 并以如下步骤检验密钥k_5的正确性. 首先, 我们要以$c=L_5\oplus\alpha_0\oplus\alpha_1$和$d=R_5\oplus F_5(L_5)\oplus F_5(L_5\oplus\alpha_0\oplus\alpha_1)$作为解密算法$DF_5$的输入. 当密钥$k_5$的猜测值是正确值时, 我们能解密出正确的$(L_4,R_4)$. 由第 3.1 节, 我们有$(L_4,R_4)=EF_4(x,\alpha_b)$, $(u,v)=DF_4(L_4,R_4\oplus\alpha_0\oplus\alpha_1)$以及$f(b,x)=v\oplus\alpha_b$ (详见图 8). 基于上述关系式与正确的(L_4,R_4), 我们不但能得到正确的输出值v, 而且能得到周期函数f的正确输出值. 注意, 我们可以通过选取新的明文输入对验证函数f的周期值是否正确, 并以此判定密钥k_5的值是否正确. 如果密钥k_5猜测错误, 我们将得到函数f的错误值, 且很大概率没有周期. 根据上述观察, 我们可以通过 4 轮 Feistel-F 结构量子区分器的周期函数来构造 5 轮的密钥恢复攻击.

需要注意的是, 在恢复上述 4 轮 Feistel-F 结构中函数f的周期值时, 我们会遇到轮函数是随机置换与随机函数这两种情形. 如第 2.1 节所述, 我们有如下结论: 当EF_4的轮函数是随机置换时, 第 3.1 节中构造的 4 轮周期函数完全满足 Simon 承诺, 即存在唯一周期s. 当轮函数是随机函数时, 构造的周期函数则不完全满足 Simon 承诺, 可能存在不想要的碰撞, 即可能存在$t\neq F_1(\alpha_0)\oplus F_1(\alpha_1)$, 使得$f(b,x)=f(b\oplus 1,x\oplus t)$. 因此, 本文将对轮函数$F_i$为随机置换和随机函数两种情况分别进行讨论.

情形 1: 当轮函数F_i为随机置换时, 上述 4 轮周期函数f只存在唯一周期s. 此时, 我们 5 轮 Feistel-F 结构密钥恢复攻击的详细过程可以描述如下:

步骤 1. 穷举密钥$k_5\in\{0,1\}^{n/2}$的值. 对于每个猜测的k_5, 循环执行步骤 2 到步骤 5.

步骤 2. 初始化两个空表T_1和T_2.

步骤 3. 随机选取$2^{n/4}$个不同的$x\in\{0,1\}^{n/2}$, 并以(x,α_0)作为EF_5的明文输入, 则敌手可以得到$2^{n/4}$个不同的输

出 (L_5^0,R_5^0). 对于每个输出值 (L_5^0,R_5^0), 敌手可以计算对应的输出状态值 (c^0,d^0), 其中 $c^0=L_5^0\oplus\alpha_0\oplus\alpha_1$, $d^0=R_5^0\oplus F_5(L_5^0)\oplus F_5(L_5^0\oplus\alpha_0\oplus\alpha_1)$. 通过将上述状态值 (c^0,d^0) 作为 DF_5 的输入, 敌手可以得到 $2^{n/4}$ 个不同的 v^0 值与对应的 $f(0,x)$ 值, 其中 $(x,f(0,x))$ 将被存储在表 T_1 中.

步骤 4. 随机选取 $2^{n/4}$ 个不同的 $y\in\{0,1\}^{n/2}$, 再以 (y,α_1) 作为 EF_5 的明文输入, 则敌手可以得到 $2^{n/4}$ 个不同的输出 (L_5^1,R_5^1). 对于每个输出值 (L_5^1,R_5^1), 敌手需要计算对应的输出状态值 (c^1,d^1), 其中 $c^1=L_5^1\oplus\alpha_0\oplus\alpha_1$, $d^1=R_5^1\oplus F_5(L_5^1)\oplus F_5(L_5^1\oplus\alpha_0\oplus\alpha_1)$. 通过将上述状态值 (c^1,d^1) 作为 DF_5 的输入, 敌手可以得到 $2^{n/4}$ 个不同的 v^1 值与对应的 $f(1,y)$ 值, 其中 $(y,f(1,y))$ 将被存储在表 T_2 中. 因为周期函数 f 的输出为 $n/2$ 比特, 根据生日悖论, 我们可以期望表 T_1 和 T_2 之间存在 1 个碰撞: $f(0,x')=f(1,y')$. 由上述碰撞, 敌手可以恢复出函数 f 的周期候选值 $s'=x'\oplus y'$.

步骤 5. 对于每个猜测的 k_5, 敌手都能得到一个对应的周期候选值 s'. 为了检验猜测的 k_5 与候选值 $s'=x'\oplus y'$ 的正确性, 敌手需要随机选取若干个明文对 (m,α_0) 和 $(m\oplus x'\oplus y',\alpha_1)$ 进行检验. 如果猜测的密钥 k_5 与周期候选值 $s'=x'\oplus y'$ 是正确的, 则对于所检验的明文对都会有 $f(0,m)=f(1,m\oplus x'\oplus y')$ 成立. 此时, 程序输出正确的密钥值 k_5 并退出循环. 否则, 判定密钥 k_5 猜测错误, 并返回第 1 步.

步骤 6. 在恢复出密钥 k_5 后, 敌手可恢复任意输入所对应的第 4 轮的状态值 (L_4,R_4). 利用第 2.1 节中的 3 轮 Simon 算法 qCPA 区分器, 并通过结合 3 轮周期性质与生日攻击, 敌手可以恢复出密钥 k_4. 由于该过程类似于恢复 k_5, 因此我们省略了具体过程.

步骤 7. 依据引理 1 所述, 2 轮的 Feistel-F 结构也具有周期性质. 因此, 在恢复出密钥 k_5 和 k_4 后, 敌手可以恢复任意输入所对应的 (L_3,R_3). 通过结合 2 轮 Feistel-F 结构的周期性质与生日攻击, 敌手可以恢复出密钥 k_3. 该过程同样类似于恢复 k_5.

步骤 8. 由图 9 可知, 在恢复出正确的 (k_3,k_4,k_5) 后, 敌手利用 EF_5 的一个明文输入 (x,α_b) 以及对应的密文 (L_5,R_5), 就可以很容易计算出第 2 轮的输出状态值 (L_2,R_2). 如图 9 所示, 我们有: $F_1(\alpha_b)=x\oplus L_2$ 和 $F_2(L_2)=\alpha_b\oplus R_2$. 换句话说, 我们可以通过输入 (x,α_b) 与状态值 (L_2,R_2) 分别恢复出函数 F_1 与 F_2 的输出值. 再利用函数 F_1 与 F_2 的输出值, 敌手可以通过穷举密钥来恢复 k_1 和 k_2 的值.

上述攻击的整体复杂度可分析如下.

第 1 步穷举密钥 k_5 需要 $O(2^{n/2})$ 的时间复杂度. 第 2 步建表只需要 $O(1)$ 的时间复杂度. 第 3 步和第 4 步收集数据都需要 $O(2^{n/4})$ 的计算与存储复杂度. 根据生日悖论, 从第 3 步和第 4 步收集的数据中找到一个碰撞需要 $O(2^{n/4})$ 的时间. 第 5 步的检验仅需常数次的访问 EF_5 和 DF_5. 因此, 猜测出正确的密钥 k_5 总共需要 $O(2^{n/2}\cdot 2^{n/4})=O(2^{3n/4})$ 的时间以及 $O(2^{n/4})$ 的存储复杂度.

与求解 k_5 的过程类似, 在第 6 步中, 我们是将 3 轮 Feistel-F 结构的周期性质与生日攻击结合, 因此恢复出 k_4 所需的复杂度与 k_5 一样. 同理, 第 7 步恢复 k_3 所需的复杂度也与 k_5 一样. 所以第 6 步和第 7 步都需要 $O(2^{3n/4})$ 的时间和 $O(2^{n/4})$ 的存储复杂度. 在第 8 步中, 敌手需要常数量级的计算和存储来收集若干个第 2 轮的状态值. 同时, 敌手还需 $O(2^{n/2})$ 的时间来对密钥 k_1 和 k_2 分别进行穷举操作.

综上所述, 敌手恢复 5 轮密钥 (k_1,k_2,k_3,k_4,k_5) 需要的时间复杂度为 $O(2^{3n/4})$, 存储复杂度为 $O(2^{n/4})$. 整个攻击过程还需要 $O(2^{n/4})$ 的选择明文和密文.

情形 2: 当轮函数 F_i 是随机函数时, 由第 2.1 节可知, 敌手从一个碰撞对 $f(x_1)=f(y_1)$ 所恢复出的 $s_1=x_1\oplus y_1$ 不一定是对应的周期值. 我们在后续将不满足周期性的碰撞称为错误碰撞, 并假设 p 为错误碰撞在总碰撞中所占比例. 注意到, 我们需要避免出现由于错误碰撞使得正确密钥 k_5 被排除的情形. Kaplan 等人在文献 [28] 中提出可以通过多次调用 Simon 算法来提高恢复周期的正确率. 与文献 [28] 类似, 我们的攻击过程需要做出如下调整.

第 1 步. 穷举密钥 $k_5\in\{0,1\}^{n/2}$ 的值. 对于每个猜测的 k_5, 循环执行第 2 到 5 步.

第 2 步. 初始化两个空表 T_1 和 T_2.

在第 3 步和第 4 步中, 敌手需要收集 $2^{n/4+c}$ 个 $(x,f(0,x))$ 和 $2^{n/4+c}$ 个 $(y,f(1,y))$, 分别存入表 T_1 和 T_2 中. 根据生日悖论, 我们可以期望表 T_1 和 T_2 之间存在 $(2^{n/4+c}\cdot 2^{n/4+c})\Big/2^{n/2}=2^{2c}$ 个碰撞. 因为 $1-p$ 是包含周期值的正确碰撞在总

碰撞中所占比例, 所以当$2^{2c} \geqslant 1/(1-p)$时, 我们可以期望上述碰撞中存在一个正确碰撞.

在第 5 步中, 对于2^{2c}个碰撞中的每一个碰撞$f(0,x_i)=f(1,y_j)$, 敌手可以通过如下操作恢复出正确的密钥和周期值. 首先, 将每一个$x_i \oplus y_j$的值都作为函数f周期值的候选值, 再随机选取常数多个明文对(m,α_0)和$(m\oplus x_i \oplus y_j, \alpha_1)$进行检验. 若恢复的周期值以及猜测的密钥值$k_5$是正确的, 则对于所检验的明文对都有$f(0,m)=f(1,m\oplus x_i \oplus y_j)$成立. 此时, 程序输出正确的密钥值$k_5$并退出循环. 否则, 密钥值$k_5$猜测错误, 并返回第 1 步.

第 6 步. 敌手可以利用 3 轮周期性质与生日攻击, 恢复出正确的k_4. 与恢复k_5类似, 敌手需要收集多个碰撞以避免错误碰撞对于恢复k_4的影响.

第 7 步. 敌手可以利用 2 轮周期性质与生日攻击, 恢复出正确的k_3. 与恢复k_5和k_4的过程类似, 敌手同样需要收集多个碰撞来恢复密钥k_3.

第 8 步. 通过前面恢复的正确密钥(k_3,k_4,k_5), 敌手需要利用常数个明密文对, 来计算得到对应的第 2 轮输出状态值. 再依据关系式$F_1(\alpha_b)=x\oplus L_2$和$F_2(L_2)=\alpha_b \oplus R_2$, 敌手可以分别对密钥$k_1$和$k_2$进行穷举, 以恢复出正确的$k_1$和$k_2$密钥值.

由于我们在上述攻击过程中需要收集多个碰撞, 情形 2 所需的复杂度与情形 1 相比略有增加, 对应的攻击复杂度可计算如下.

第 1 步穷举密钥k_5需要$O(2^{n/2})$的时间复杂度. 第 3 步和第 4 步收集数据都需要$O(2^{n/4+c})$的计算与存储复杂度. 根据生日悖论, 从第 3 步和第 4 步收集的数据中得到2^{2c}个碰撞需要$O(2^{n/4+c})$的时间. 第 5 步的检验只需要对EF_5和DF_5进行常数次的访问. 因此, 猜测出正确的密钥值k_5总共需要$O(2^{n/2}\cdot 2^{n/4+c})=O(2^{3n/4+c})$的时间以及$O(2^{n/4+c})$的存储, 其中$2^{2c} \geqslant 1/(1-p)$.

第 6 步恢复k_4和第 7 步恢复k_3的过程都与恢复k_5类似, 因此所需的复杂度也相同, 即均需要$O(2^{3n/4+c})$的时间和$O(2^{n/4+c})$的存储. 第 8 步对k_1和k_2进行穷举均需要$O(2^{n/2})$的时间复杂度.

综上所述, 在轮函数F_i为随机函数的情形下, 恢复出EF_5的全部密钥需要$O(2^{3n/4+c})$的时间以及$O(2^{n/4+c})$的存储. 此外, 整体攻击需要$O(2^{n/4+c})$的选择明文和密文. 注意到, 随机函数中错误碰撞出现的比例较低, 一般可以假设$p \leqslant 0.5$. 此时, $c \geqslant (\log_2 1/(1-p))/2 \geqslant 0.5$. 所以上述攻击所需的时间复杂度为$O(2^{3n/4+0.5})=O(2^{(3n+2)/4})$, 存储复杂度为$O(2^{(n+2)/4})$.

3.3 7 轮 Feistel-FK 结构的密钥恢复攻击

与第 3.1 节描述的 4 轮 Feistel-F 结构的区分器类似, Ito 等人[20]通过将 6 轮 Feistel-FK 加密结构和解密结构相连接, 构造了具有周期性质的 6 轮 Feistel-FK 结构 qCCA 区分器, 具体周期函数f构造可描述如下:

$$\begin{aligned} f(b,x) =& \alpha_0 \oplus \alpha_1 \oplus F(x\oplus F(\alpha_b \oplus k_1)\oplus k_2)\oplus \\ & F(x\oplus F(\alpha_b\oplus k_1)\oplus k_2 \oplus F(\alpha_0 \oplus F(x\oplus F(\alpha_b\oplus k_1)\oplus k_2)\oplus k_3)\oplus F(\alpha_1 \oplus F(x\oplus F(\alpha_b\oplus k_1)\oplus k_2)\oplus k_3)). \end{aligned}$$

函数f的周期为$s=(1,F(\alpha_0\oplus k_1)\oplus F(\alpha_1\oplus k_1))$. 此外, 针对 Feistel-FK 结构, Ito 等人还构造了具有周期性质的 5 轮 qCPA 区分器. 他们将$(\alpha_b \oplus F(x),x)$作为 5 轮 Feistel-FK 的输入, 得到输出密文(c,d). 利用输出密文, 敌手可以构造 5 轮周期函数$f'(b,x)=d\oplus F(c)\oplus \alpha_b$, 其周期也为$s=(1,F(\alpha_0\oplus k_1)\oplus F(\alpha_1\oplus k_1))$. 对具体构造过程感兴趣的读者可以参考文献 [20].

与 5 轮 Feistel-F 结构密钥恢复攻击类似, 我们新型 7 轮 Feistel-FK 结构密钥恢复攻击过程可总结如下.

第一, 利用上述 6 轮具有周期性质的 qCCA 区分器, 敌手可以通过如下方式恢复密钥k_7的值. 首先, 通过穷举密钥k_7的值, 敌手可以计算出对应的第 6 轮状态值以及对应函数f的值; 其次, 敌手可以通过生日攻击得到函数f的周期候选值; 此外, 敌手还需要选取若干个明文对以验证周期候选值和k_7的正确性. 注意到, 上述恢复密钥k_7的过程与第 3.2 节中恢复密钥k_5的过程类似.

第二, 我们可以利用上述 5 轮具有周期性质的 qCPA 区分器来恢复密钥k_6. 由于具体过程与恢复密钥k_7的过程类似, 我们省略相关细节. 恢复了密钥k_7与k_6之后, 我们还需要恢复密钥$k_5,\ldots,k_1$.

最后, 由于 Feistel-FK 结构可以看成是特殊的 Feistel-F, 所以我们可以利用第 3.2 节 Feistel-F 结构的 5 轮密钥

恢复攻击来恢复 Feistel-FK 结构的剩余密钥 $k_5,\ldots,k_1$.

由于上述 7 轮密钥恢复攻击与 3.2 节的攻击过程类似, 我们在本节中只给出结论而忽略相关细节. 当 Feistel-FK 结构的轮函数为随机置换时, 7 轮密钥恢复攻击的时间复杂度为 $O(2^{3n/4})$, 存储复杂度为 $O(2^{n/4})$, 并且需要 $O(2^{n/4})$ 的选择明文和密文. 当 Feistel-FK 结构的轮函数为随机函数, 并且错误碰撞出现的比例 $p \leqslant 0.5$ 时, 攻击的时间复杂度变为 $O(2^{(3n+2)/4})$, 存储复杂度为 $O(2^{(n+2)/4})$, 且需要 $O(2^{(n+2)/4})$ 的明文和密文. 与 Yang 等人[13]的结果相比, 本文的攻击使用了更低的存储和数据复杂度.

4 对 Misty 结构的密钥恢复攻击

由于 Misty 结构具有周期性, 本文的新型密钥恢复攻击方法也能被应用到 Misty 结构上.

4.1 4 轮 Misty L-F 结构的 qCPA 区分器

Gouget 等人[22]构造了一个具有周期性质的 4 轮 Misty L-F 结构的 qCPA 区分器, 如图 10 所示. 假设 4 轮 Misty L-F 的加密算法 MF_4 以 (α_b,x) 作为明文输入, 其中 F_i 是包含 $n/2$ 比特轮密钥 k_i 的轮函数. 设 (L_i,R_i) 表示第 i 轮的输出状态, 则输出的密文 (L_4,R_4) 可以表述为:

$$L_4 = x\oplus F_1(\alpha_b)\oplus F_2(x)\oplus F_3(x\oplus F_1(\alpha_b)), R_4 = F_4(x\oplus F_1(\alpha_b)\oplus F_2(x))\oplus L_4.$$

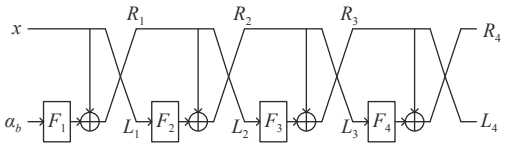


图 10 4 轮 Misty L-F 结构

给定一个量子查询问答机 O, O 要么是 4 轮的 Misty L-F 结构, 要么是一个随机置换. 为了区分上述两种情形, 敌手需要构造一个函数 $f:\{0,1\}^{n/2}\to\{0,1\}^{n/2}$, $f(x)=L_4^0\oplus L_4^1$, 其中 $L_4^0=O(\alpha_0,x)$, $L_4^1=O(\alpha_1,x)$. 当 O 是 MF_4 时, 由函数 f 的定义, 我们能将函数 f 改写为 $f(x)=L_4^0\oplus L_4^1=F_1(\alpha_0)\oplus F_1(\alpha_1)\oplus F_3(x\oplus F_1(\alpha_0))\oplus F_3(x\oplus F_1(\alpha_1))$. 由于 $f(x)=f(x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))$, 函数 f 有一个周期 $s=F_1(\alpha_0)\oplus F_1(\alpha_1)$. 当 O 是随机置换时, 由定义函数 f 则没有上述周期性质. 通过函数 f 和 Simon 算法, 攻击者可以构造一个多项式时间的 4 轮 Misty L-F 结构 qCPA 区分器.

此外, 通过观察 Misty L-F 结构的性质特点, 我们有如下引理.

引理 2. 3 轮和 2 轮的 Misty L-F 结构均具有周期性质.

证明: 与 4 轮周期函数类似, 为了构造 3 轮 Misty L-F 结构的周期函数, 敌手需要知道第 3 轮状态 (L_3,R_3). 与 4 轮周期函数类似, 敌手可以用 (α_b,x) 作为明文输入, 获得对应的输出状态值 (L_3^b,R_3^b), 其中 $b\in\{0,1\}$. 如图 10 所示, 我们有 $R_3^b=L_4^b$. 由上述状态值 R_3^0 与 R_3^1, 敌手可以构造 3 轮周期函数 $f_3(x)=R_3^0\oplus R_3^1=L_4^0\oplus L_4^1$. 注意到, 上述 3 轮周期函数 $f_3(x)$ 与 Gouget 等人的 4 轮周期函数相等, 因此其周期为 $s=F_1(\alpha_0)\oplus F_1(\alpha_1)$.

与 3 轮周期函数类似, 敌手可以通过利用状态值 L_2 来构造 2 轮周期函数. 注意到, 第 2 轮的输出值 L_2 可以表述为 $L_2=F_1(\alpha_b)\oplus x$. 若给定状态值 L_2, 敌手便可以构造 2 轮的周期函数 $f_2(b,x)=L_2=F_1(\alpha_b)\oplus x$. 很容易验证 $f_2(b\oplus 1,x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))=f_2(b,x)$. 因此函数 f_2 具有一个周期 $s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$.

综上所述, 我们可以分别为 3 轮和 2 轮的 Misty L-F 构造相应的周期函数, 因此引理 2 成立.

4.2 对 5 轮 Misty L-F 结构的密钥恢复攻击

与 Feistel-F 结构不同, 我们发现对 Misty L-F 结构 qCCA 攻击中的周期函数轮数并不能超过 4 轮. 因此, 我们直接利用 Gouget 等人 4 轮 qCPA 区分器的周期函数[22]来构造 5 轮 Misty L-F 结构的密钥恢复攻击, 具体攻击如图 11 所示, 其中虚线框部分表示 4 轮 Misty L-F 的量子区分器.

如图 11 所示, 5 轮 Misty L-F 的加密算法 MF_5 以 (α_b,x) 作为明文输入, 设 (L_i,R_i) 表示第 i 轮的输出状态, 则输出密文 (L_5,R_5). 依据 Misty L-F 加密算法, 敌手可以得到以下关系: $L_4=F_5^{-1}(L_5\oplus R_5)$, $R_4=L_5$, 其中 F_5^{-1} 是 F_5 的逆.

随机猜测密钥 k_5 的值, 敌手便可以通过 (k_5, L_5, R_5) 来计算对应出 (L_4, R_4), 而后再由 L_4 计算出第 4.1 节周期函数 f 值. 若密钥 k_5 猜测正确, 则函数 f 具有周期 s. 否则, 函数 f 将没有周期性质.

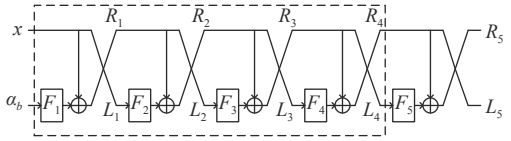


图 11 5 轮 Misty L-F 结构

与 Feistel-F 类似, 我们需要将 MF_5 的轮函数分为随机置换和随机函数两种情况分别进行处理.

情形 1: 当 MF_5 的轮函数为随机置换时, 对于 Misty L-F 结构的 4 轮周期函数 f 完全满足 Simon 承诺, 即存在唯一周期 s. 此时, 对于 Misty L-F 结构 5 轮密钥恢复攻击思路可以描述如下.

第 1 步. 敌手可以利用 Misty L-F 结构的 4 轮周期函数 f 来恢复密钥 k_5 的值, 具体如下. 首先, 敌手可以通过穷举密钥 k_5 的值, 计算出对应第 4 轮状态值 (L_4, R_4) 以及对应周期函数 f 的值. 其次, 敌手可以通过生日攻击得到函数 f 的周期候选值. 最后, 敌手需要选取若干个明文对以验证周期候选值和 k_5 的正确性.

第 2 步. 在恢复出正确的 k_5 后, 敌手可以恢复出第 4 轮的状态值 (L_4, R_4). 如引理 2 所述, 3 轮和 2 轮 Misty L-F 结构也具有周期性质. 与 k_5 类似, 敌手可以通过穷举 k_4 恢复输入 (α_b, x) 所对应的第 3 轮的状态值 (L_3^b, R_3^b). 利用上述状态值 (L_3^b, R_3^b), 敌手可以将 3 轮 Misty L-F 结构的周期性质与生日攻击相结合, 来恢复出正确的 k_4. 由于其具体过程与恢复 k_5 类似, 因此我们省略了细节.

第 3 步. 恢复出 k_4 与 k_5 后, 敌手不仅可以进一步恢复出第 3 轮的状态值 (L_3, R_3), 而且通过穷举 k_3 还可以计算出状态值 L_2. 利用 L_2, 再将 2 轮 Misty L-F 结构的周期性质与生日攻击相结合, 敌手可以恢复出正确的 k_3. 由于恢复 k_4 和 k_3 的过程与恢复 k_5 的过程类似, 因此我们省略了细节.

第 4 步. 在恢复出正确的 (k_3, k_4, k_5) 后, 敌手可以利用 MF_5 的一个明文 (α_b, x) 以及对应的密文 (L_5, R_5), 反向计算得到第 2 轮的输出状态值 (L_2, R_2). 换句话说, 我们可以按 $F_1(\alpha_b) = x \oplus L_2$ 和 $F_2(x) = R_2 \oplus L_2$ 计算出轮函数 F_1 与 F_2 的输出值. 根据上述轮函数的输出值, 敌手可以分别对密钥 k_1 和 k_2 进行穷举, 以恢复出正确的密钥值.

上述密钥恢复攻击的总体复杂度分析如下. 第 1 步, 对于每个密钥 k_5, 敌手不仅可以恢复出 (L_4, R_4), 而且可以进一步通过生日攻击以 $O(2^{n/4})$ 的时间和存储代价恢复对应周期函数 f 的值. 而后, 敌手需要对 MF_5 进行常数次访问来验证密钥值 k_5 和周期候选值是否正确. 由于我们需要对 $O(2^{n/2})$ 个 k_5 都重复上述过程, 因此恢复出正确的 k_5 总共需要 $O(2^{n/2} \cdot 2^{n/4}) = O(2^{3n/4})$ 的时间以及 $O(2^{n/4})$ 的存储复杂度. 与求解 k_5 类似, 敌手需要分别利用 3 轮和 2 轮 Misty L-F 结构的周期函数和生日攻击以恢复出正确的 k_4 和 k_3. 因此, 恢复 k_4 和 k_3 所需的复杂度与恢复 k_5 相同, 都需要 $O(2^{3n/4})$ 的时间以及 $O(2^{n/4})$ 的存储复杂度. 最后, 敌手需要先收集轮函数 F_1 与 F_2 的输出值, 然后以 $O(2^{n/2})$ 的时间代价对密钥 k_1 和 k_2 分别进行穷举攻击.

综上所述, 敌手恢复出 5 轮 Misty L-F 结构的密钥 $(k_1, k_2, k_3, k_4, k_5)$ 需要的时间复杂度为 $O(2^{3n/4})$, 存储复杂度为 $O(2^{n/4})$. 此外, 整个攻击还需要 $O(2^{n/4})$ 的选择明文.

情形 2: 当 MF_5 的轮函数为随机函数时. 与 Feistel-F 结构类似, Misty L-F 结构的 4 轮周期函数 f 不一定满足 Simon 承诺. 为了避免恢复正确密钥时受错误碰撞的影响, 敌手需要寻找多个碰撞, 以期从中恢复出正确周期值与密钥值. 与第 3.2 节类似, 若假设错误碰撞出现的比例 $p \leqslant 0.5$, 则敌手需要的时间复杂度变为 $O(2^{(3n+2)/4})$, 存储复杂度为 $O(2^{(n+2)/4})$, 以及需要 $O(2^{(n+2)/4})$ 个选择明文.

4.3 对 Misty L-KF 和 Misty L-FK 的密钥恢复攻击

Cui 等人[23]分别对 5 轮 Misty L-KF 和 5 轮 Misty L-FK 结构构造了具有周期性质的 qCPA 区分器. 针对 5 轮的 Misty L-KF 结构, 其第 i 轮的轮函数为 $F_i(x) = F(x \oplus k_i)$, 其中 F 为一公开函数. Cui 等人分别使用 (α_0, x) 和 (α_1, x) 作为明文输入, 并得到对应的输出密文 (L_5^0, R_5^0) 和 (L_5^1, R_5^1). 利用上述密文对, 他们构造了如下的周期函数:

$$f^{KF}(x)=F^{-1}(L_5^0\oplus R_5^0)\oplus F^{-1}(L_5^1\oplus R_5^1)=F(\alpha_0\oplus k_1)\oplus F(\alpha_1\oplus k_1)\oplus F(x\oplus k_3\oplus F(\alpha_0\oplus k_1))\oplus F(x\oplus k_3\oplus F(\alpha_1\oplus k_1)).$$

易得上述函数 $f^{KF}(x)$ 的周期值为 $F(\alpha_0\oplus k_1)\oplus F(\alpha_1\oplus k_1)$, 其中 F^{-1} 为 F 的逆函数.

针对 5 轮的 Misty L-FK 结构, 其第 i 轮的轮函数为 $F_i(x)=F(x)\oplus k_i$, 其中 F 为一公开函数. Cui 等人分别以 $(F^{-1}(\alpha_0\oplus x),\alpha_0)$ 和 $(F^{-1}(\alpha_1\oplus x),\alpha_1)$ 作为明文输入, 其中 F^{-1} 为 F 的逆函数, 并得到对应的输出密文 (L_5^0,R_5^0) 和 (L_5^1,R_5^1). 利用上述得到的左分支输出 L_5^0 和 L_5^1, 他们构造了如下周期函数:

$$f^{FK}(x)=L_5^0\oplus L_5^1=F(\alpha_0)\oplus F(\alpha_1)\oplus F(F(\alpha_0)\oplus x\oplus k_1\oplus k_2)\oplus F(F(\alpha_1)\oplus x\oplus k_1\oplus k_2).$$

该函数的周期为 $F(\alpha_0)\oplus F(\alpha_1)$.

引理 2 证明了低轮的 Misty L-F 结构也具有周期性质. 由于 Misty L-KF 和 Misty L-FK 可以看成是特殊的 Misty L-F 结构, 所以我们可以很容易验证低轮的 Misty L-KF 和 Misty L-FK 也同样具有周期性质. 因此, 与第 4.2 节类似, 我们可以将上述周期函数和生日攻击相结合, 来对 6 轮 Misty L-KF 和 6 轮 Misty L-FK 结构分别构造出对应的密钥恢复攻击. 综上所述, 当轮函数为随机置换时, 6 轮的密钥恢复攻击需要 $O(2^{n/4})$ 的选择明文, $O(2^{3n/4})$ 的时间复杂度, 以及 $O(2^{n/4})$ 的存储复杂度. 当轮函数为随机函数时, 攻击则需要 $O(2^{(3n+2)/4})$ 的时间复杂度, $O(2^{(n+2)/4})$ 的存储复杂度, 以及 $O(2^{(n+2)/4})$ 的选择明文.

4.4 对 Misty R 结构的密钥恢复攻击

针对 Misty R-F 结构, Cui 等人[23]构造了具有 4 轮周期性质的 qCCA 区分器. 此外, 他们还分别对 Misty R-KF 和 Misty R-FK 结构构造了具有 5 轮周期性质的 qCCA 区分器. 由于 Misty R 与 Misty L 结构类似, 因此低于区分器轮数的 Misty R 结构也具有相应的周期性质, 我们省略了具体细节.

通过目标结构的周期性质和生日攻击相结合的方法, 我们可以对 5 轮 Misty R-F 结构, 6 轮 Misty R-KF, 以及 6 轮 Misty R-FK 结构构造出相关的密钥恢复攻击. 当轮函数为随机置换时, 上述的每个密钥恢复攻击都需要 $O(2^{n/4})$ 的选择密文, 总体的时间复杂度均为 $O(2^{3n/4})$, 存储复杂度为 $O(2^{n/4})$. 当轮函数为随机函数时, 上述的每个攻击则需要 $O(2^{(3n+2)/4})$ 的时间复杂度, $O(2^{(n+2)/4})$ 的存储复杂度, 以及 $O(2^{(n+2)/4})$ 的选择密文. 密钥恢复攻击的过程以及复杂度分析过程可以参考第 4.2 节.

5 对 Type-1 GFS 的密钥恢复攻击

5.1 (d^2-d+1) 轮 Type-1 GFS 的 qCCA 区分器

针对 Type-1 GFS 结构, Ni 等人[26]分别提出了具有周期性质的 $(3d-3)$ 轮 qCPA 区分器和 (d^2-d+1) 轮 qCCA 区分器. 为了使得构造的密钥恢复攻击轮数尽可能高, 以下的攻击借助了 Ni 等人[26]所构造 (d^2-d+1) 轮 qCCA 区分器的周期函数. d^2 轮的 Type-1 GFS 解密结构如图 12 所示. 假设第 i 轮 Type-1 GFS 的解密算法用 Φ_i^{-1} 表示. 为了方便, 下面将解密结构的第 i 个轮函数记为 F_i. 假设 $\Phi_{d^2}^{-1}$ 以 $(x,x_1^0,\ldots,x_{d-2}^0,\alpha_b)$ 作为输入, 则第 (d^2-d+1) 轮的输出为 $(x_0^{d^2-d+1},\ldots,x_{d-1}^{d^2-d+1})$. 根据文献 [26], 用于构造 (d^2-d+1) 轮区分器的周期函数可定义如下.

$$\begin{cases} f:\{0,1\}\times\{0,1\}^{n/d}\to\{0,1\}^{n/d} \\ (b,x)\mapsto \alpha_b\oplus x_0^{d^2-d+1} \end{cases}.$$

其中, $(x_0^{d^2-d+1},\ldots,x_{d-1}^{d^2-d+1})=\Phi_{d^2-d+1}^{-1}(x,x_1^0,\ldots,x_{d-2}^0,\alpha_b)$. 由 Ni 等人的证明可知该函数是一个周期函数, 且周期值为 $s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$. 对具体过程感兴趣的读者可以参考文献 [26].

另外, 通过观察 Type-1 GFS 解密结构的性质特点, 我们有如下引理.

引理 3. 当以 $(x,x_1^0,\ldots,x_{d-2}^0,\alpha_b)$ 作为输入时, 第 i 轮的 Type-1 GFS 解密结构同样具有周期性质, 其中 $1\leqslant i\leqslant d^2-d$ 且 x_j^0 是常数 ($1\leqslant j\leqslant d-2$).

证明: 与文献 [26] 中引理 2 的证明类似, 为了构造第 i 轮 Type-1 GFS 解密结构的周期函数, 我们需要将 i 进行分段处理. 由图 12 所示, Type-1 GFS 的解密结构第 1 轮会输出 $F_1(\alpha_b)\oplus x$. 注意到, $F_1(\alpha_b)\oplus x$ 将作为第 d 轮轮函数 F_d 的输入, 有 $x_1^d=F_d(F_1(\alpha_b)\oplus x)\oplus x_1^0$. 而在前 d–1 轮 $F_1(\alpha_b)\oplus x$ 不会受到轮函数的影响.

当 $1 \leqslant i \leqslant d-1$ 时, 我们可将第 i 轮的周期函数表述为 $f_{d-1}(b,x) = F_1(\alpha_b) \oplus x$, 即挑选第 i 轮中包含 $F_1(\alpha_b) \oplus x$ 的分支作为 $f_{d-1}(b,x)$ 输出. 易得 $f_{d-1}(b,x) = f_{d-1}(b \oplus 1, x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1))$, 因此周期为 $s = (1, F_1(\alpha_0) \oplus F_1(\alpha_1))$. 当 $d \leqslant i \leqslant 2d-1$ 时, 注意到状态 $x_1^d = F_d(F_1(\alpha_b) \oplus x) \oplus x_1^0$ 不需要输入轮函数中进行变换. 此外, 由于 x_1^0 是一个常数, 我们可以将 $x_1^d = F_d(F_1(\alpha_b) \oplus x) \oplus x_1^0$ 改写为 $x_1^d = F(F_1(\alpha_b) \oplus x)$, 其中 $F(\cdot) = F_d(\cdot) \oplus x_1^0$. 与周期函数 $f_{d-1}(b,x)$ 类似, 我们可以挑选上述范围内第 i 轮中包含 $F(F_1(\alpha_b) \oplus x)$ 的分支作为此处周期函数 $f_{2d-1}(b,x)$ 的输出, 即 $f_{2d-1}(b,x) = x_1^d = F(F_1(\alpha_b) \oplus x)$. 易得 $f_{2d-1}(b,x) = f_{2d-1}(b \oplus 1, x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1))$, 则周期为 $s = (1, F_1(\alpha_0) \oplus F_1(\alpha_1))$.

当 $2d \leqslant i \leqslant 3d-1$ 时, 由于 x_2^0 为常数, 因此我们能将 $x_1^{2d-1} = F_{2d-1}(x_1^d) \oplus x_2^0 = F_{2d-1}(F(F_1(\alpha_b) \oplus x)) \oplus x_2^0$ 改写为 $x_1^{2d-1} = F'(F_1(\alpha_b) \oplus x)$. 与 $x_1^d = F(F_1(\alpha_b) \oplus x)$ 类似, 我们将此范围内第 i 轮中包含 $F'(F_1(\alpha_b) \oplus x)$ 的分支作为此处周期函数 $f_{3d-1}(b,x)$ 的输出, 易得 $f_{3d-1}(b,x) = f_{3d-1}(b \oplus 1, x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1))$, 对应周期为 $s = (1, F_1(\alpha_0) \oplus F_1(\alpha_1))$. 类似地, 对于接下来的每一个 $d-1$ 轮, 我们都可以形式化地表述出相应的周期函数.

最后, 当 $d^2 - 2d + 2 \leqslant i \leqslant d^2 - d$ 时, 我们可以将此时第 i 轮的周期函数形式化地表述为 $f(b,x) = \alpha_b \oplus x_{i-(d^2-2d+2)+1}^i = F''(F_1(\alpha_b) \oplus x)$, 其中 F'' 独立于输入 (b,x). 根据文献 [26], 上述构造的周期函数满足 $f(b,x) = f(b \oplus 1, x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1))$, 因而具有周期 $s = (1, F_1(\alpha_0) \oplus F_1(\alpha_1))$.

综上所述, 引理 3 成立.

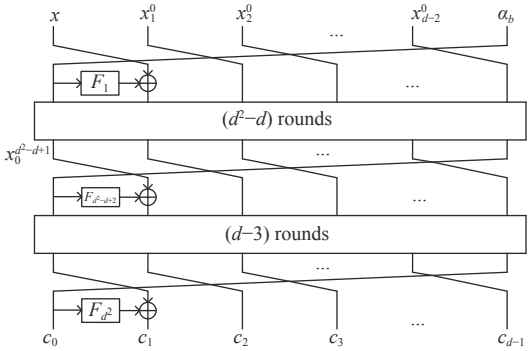


图 12 d^2 轮 Type-1 GFS 的解密结构

5.2 d^2 轮 Type-1 GFS 的密钥恢复攻击

本节通过将 (d^2-d+1) 轮的 qCCA 区分器往后扩展 $(d-1)$ 轮, 构造出 d^2 轮 Type-1 GFS 的密钥恢复攻击. d^2 轮的 Type-1 GFS 解密结构如图 12 所示, 其中 $\Phi_{d^2}^{-1}$ 以 $(x, x_1^0, x_2^0, \ldots, x_{d-2}^0, \alpha_b)$ 作为输入, $(c_0, c_1, \ldots, c_{d-1})$ 作为输出.

由图 12 可知, 若敌手随机地猜测第 (d^2-d+2) 轮到第 d^2 轮的密钥 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$, 通过 $(c_0, c_1, \ldots, c_{d-1})$ 以及猜测的密钥值 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$, 便可以解密得到 $x_0^{d^2-d+1}$ 的值, 从而得到函数 f 的值. 若密钥 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$ 均猜测正确, 则 f 会有周期 $s = (1, F_1(\alpha_0) \oplus F_1(\alpha_1))$. 否则, f 很大概率是一个非周期性的随机函数. 因此, 敌手可以通过生日攻击恢复出正确的周期值, 进而恢复出第 (d^2-d+2) 轮到第 d^2 轮 Type-1 GFS 的密钥.

固定两个不同的值 α_0 和 α_1, 以及 $(d-2)$ 个常数 $x_1^0, x_2^0, \ldots, x_{d-2}^0$, 它们都是 n/d 比特的. 与第 3.2 节中 Feistel 结构的密钥恢复攻击类似, 下面将轮函数 F_i 分为随机置换和随机函数两种情形来描述我们的攻击过程.

情形 1: 当 $\Phi_{d^2}^{-1}$ 的轮函数是随机置换时, d^2 轮 Type-1 GFS 的密钥恢复攻击思路描述如下.

首先, 敌手可以通过穷举 $d-1$ 个轮密钥 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$ 的值, 计算出对应的第 (d^2-d+1) 轮状态值以及对应函数 f 的值; 其次, 敌手可以通过生日攻击得到函数 f 的周期候选值; 最后, 敌手需要选取若干个明文对以验证周期候选值和 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$ 的正确性. 由引理 3 可得, 轮数小于 (d^2-d+1) 时 Type-1 GFS 解密结构也具有周期性. 因此, 恢复出 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$ 后, 我们可以恢复第 (d^2-d+1) 轮的轮状态值. 而后, 敌手可以用类似于恢复 $(k_{d^2-d+2}, k_{d^2-d+3}, \ldots, k_{d^2})$ 的方法来恢复其他轮密钥值. 首先, 通过穷举密钥值收集低轮函数的周期函数的多

个输出值, 再通过生日攻击来恢复对应的周期值, 并以此验证所猜测的轮密钥值的正确性. 因为攻击过程与恢复 $(k_{d^2-d+2},k_{d^2-d+3},\ldots,k_{d^2})$ 类似, 我们省略相关细节.

上述攻击的整体复杂度分析如下. 穷举密钥 $(k_{d^2-d+2},k_{d^2-d+3},\ldots,k_{d^2})$ 需要 $O(2^{(d-1)n/d})$ 的时间复杂度. 通过生日攻击找到函数 f 的周期候选值需要 $O(2^{n/2d})$ 的时间和 $O(2^{n/2d})$ 的存储复杂度. 检验轮密钥值和周期候选值的过程仅需对 $\Phi^{-1}_{d^2-d+2}$ 进行常数次的访问. 因此, 猜测出正确的 $d-1$ 个轮密钥值 $(k_{d^2-d+2},k_{d^2-d+3},\ldots,k_{d^2})$ 共需要 $O(2^{(d-1)n/d}\cdot 2^{n/2d})=O(2^{(2d-1)n/2d})$ 的时间和 $O(2^{n/2d})$ 的存储复杂度. 由于恢复其他轮密钥的过程与 $(k_{d^2-d+2},k_{d^2-d+3},\ldots,k_{d^2})$ 类似, 也是通过将周期值与生日攻击相结合来恢复轮密钥值, 因此对应的复杂度并不会超过恢复 $(k_{d^2-d+2},k_{d^2-d+3},\ldots,k_{d^2})$ 所需的复杂度. 综上, 该密钥恢复攻击需要 $O(2^{(2d-1)n/2d})$ 的时间复杂度和 $O(2^{n/2d})$ 的存储复杂度, 以及 $O(2^{n/2d})$ 的选择密文.

情形 2: 当 $\Phi^{-1}_{d^2-d+2}$ 的轮函数为随机函数时, 对于 Type-1 GFS 的周期函数 f 不一定满足 Simon 承诺. 与 Feistel-F 结构类似, 为了避免受到错误碰撞的影响, 敌手需要寻找多个碰撞. 若假设错误碰撞出现的比例 $p\leqslant 0.5$, 则整体攻击的时间复杂度变为 $O(2^{(2d-1)n/2d+0.5})=O(2^{(2d-1)n+d/2d})$, 存储复杂度为 $O(2^{(n/2d)+0.5})=O(2^{(n+d)/2d})$. 此外, 上述攻击还需要 $O(2^{(n+d)/2d})$ 个选择密文.

在文献 [24] 中, Deng 等人分析了轮密钥在轮函数前注入的 Type-1 GFS. 基于中间相遇攻击技术, 他们针对该结构提出了一个 $(5d-3)$ 轮的密钥恢复攻击. 而本文则分析了更安全的 Type-1 GFS 结构, 即轮密钥直接作用于轮函数中, 并且我们新型密钥恢复攻击的轮数能达到 d^2 轮.

5.3 Type-1 GFS 的密钥恢复攻击的推广

上述对于 Type-1 GFS 密钥恢复攻击还能推广到 Type-2 型广义 Feistel 结构上. 对于 d 分支 Type-2 GFS (d 为偶数), Deng 等人[27]利用中间相遇攻击的方法, 提出了 $(d+3)$ 轮传统密钥恢复攻击. 在文献 [25] 中, Dong 等人构造了 $(d+1)$ 轮具有周期性质的 qCPA 区分器. 但是, Dong 等人构造的周期函数需要利用内部轮函数的输出状态值, 这将使得整个量子区分攻击变为平凡攻击. Luo 等人[21]修正了这一结果, 并指出敌手只需利用第 $(d+1)$ 轮第 d 个分支的输出状态值 x_d^{d+1}, 就可以构造出 $(d+1)$ 轮量子区分器的周期函数 $f(b,x)=\alpha_b\oplus x_d^{d+1}$. 为了简便, 后续我们将 Type-2 GFS 中第 i 轮第 j 个包含轮密钥的轮函数记为 F_j^i, 则函数 f 的周期为 $s=(1,F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$. 通过观察 Type-2 GFS 的性质特点, 我们有如下引理.

引理 4. 当 Type-2 GFS 输入为 $(\alpha_b,x,x_3^0,x_4^0,\ldots,x_d^0)$ 时, 轮数低于 $(d+1)$ 轮的 Type-2 GFS 也具有周期性质, 其中 x_j^0 是常数 ($3\leqslant j\leqslant d$).

证明: 为了证明上述结论, 我们选取 Type-2 GFS 第 i 轮第 1 个分支的轮函数 F_1^i 作为分析目标.

依据图 5, Type-2 GFS 第 1 轮第 1 个分支的输出可以表示为 $x_1^1=F_1^1(\alpha_b)\oplus x$. 利用 x_1^1 我们可以对轮数为 1 的 Type-2 GFS 构造周期函数 $f_1(b,x)=x_1^1=F_1^1(\alpha_b)\oplus x$. 易证 $f_1(b,x)=f_1(b\oplus 1,x\oplus F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$, 所以 f_1 的周期为 $s=(1,F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$.

Type-2 GFS 第 2 轮第 1 个分支轮函数 F_1^2 的输入为 x_1^1, 对应的第 2 轮第 1 个分支输出可以表示为 $x_1^2=F_1^2(x_1^1)\oplus x_3^0$. 由于 x_3^0 是常数, $x_1^2=F_1^2(x_1^1)\oplus x_3^0$ 可以改写为 $x_1^2=R_2(x_1^1)=R_2(F_1^1(\alpha_b)\oplus x)$, 其中 $R_2(\cdot)=F_1^2(\cdot)\oplus x_3^0$. 利用 $x_1^2=R_2(F_1^1(\alpha_b)\oplus x)$, 我们可以对 2 轮 Type-2 GFS 构造周期函数 $f_2(b,x)=R_2(F_1^1(\alpha_b)\oplus x)$. 易得 $f_2(b,x)=f_2(b\oplus 1,x\oplus F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$, 因此对应的周期为 $s=(1,F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$.

同理, 因为 x_1^2 是第 3 轮第 1 个分支函数 F_1^3 的输入, 所以第 3 轮第 1 个分支的输出 x_1^3 可以表示为 $x_1^3=F_1^3(R_2(x_1^1))\oplus F_2^1(x_3^0)\oplus x_4^0$. 由于 $F_2^1(x_3^0)\oplus x_4^0$ 也是常数, 因此 $x_1^3=F_1^3(R_2(x_1^1))\oplus F_2^1(x_3^0)\oplus x_4^0$ 可以改写为 $x_1^3=R_3(x_1^1)$.

一般地, 当 $2\leqslant i\leqslant d-1$ 时, 第 i 轮第 1 个分支的输出都可以形式化地表示为 $x_1^i=R_i(x_1^1)$. 因此, 当 $2\leqslant i\leqslant d-1$ 时, 利用 x_1^i, 敌手可以构造出第 i 轮的 Type-2 GFS 周期函数: $f_i(b,x)=x_1^i=R_i(x_1^1)=R_i(F_1^1(\alpha_b)\oplus x)$. 易证 $f_i(b,x)=f_i(b\oplus 1,x\oplus F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$, 所以 f_i 的周期均为 $s=(1,F_1^1(\alpha_0)\oplus F_1^1(\alpha_1))$.

最后, 依据图 5 可知 $x_d^{d+1}=x_1^d$. 利用第 d 轮第 1 个分支的输出状态值 x_1^d, 敌手就可以构造与 $(d+1)$ 轮相等的 d 轮周期函数. 因此, d 轮 Type-2 GFS 也具有周期性质.

综上所述, 引理 4 成立.

利用上述周期性质, 我们可以用类似 Type-1 GFS 的思路, 通过生日攻击验证猜测密钥的正确性. 此外, 我们发现在 Type-2 GFS 中恢复周期函数状态值时并不需要对所有轮子密钥都进行穷举, 而是只需要对部分轮密钥进行穷举即可, 这就给我们构造轮数超过 $(d+3)$ 的密钥恢复攻击提供了便利条件. 需要强调的是, 我们新型攻击的复杂度均小于穷举攻击, 因此是有效的. 由于篇幅受限, 且攻击过程与 Type-1 GFS 类似, 本节仅给出对于 d 分支 Type-2 型广义 Feistel 结构上的攻击轮数而忽略具体攻击过程. 如表 3 所示, 当 $d \geqslant t^2$ 时, 我们新型密钥恢复攻击的轮数至少是 $(d+2t)$. 因此, 当 $t \geqslant 2$ 时, 我们新型密钥恢复攻击的轮数要优于邓元豪[27]的密钥恢复攻击轮数.

表 3 d 分支 (d 为偶数) Type-2 GFS 密钥恢复攻击轮数的对比

分支数	d=4	d=6	d=8	d=10	d=12	d=14	d=16	…	$t(t+1) \geqslant d \geqslant t^2$或$(t+1)^2 \geqslant d \geqslant t(t+1)$	…
文献[27]攻击轮数	7	9	11	13	15	17	19	…	d+3	…
本文攻击轮数	7	10	13	16	18	21	23	…	d+2t或d+2t+1	…

6 总 结

近些年, 量子密码已经成为密码学的研究热点, 涌现出了多个新型的量子算法. 不过, 现有的研究工作都是将传统算法量子化, 而如何将量子环境中的结果转化为传统攻击却还比较少. 因此, 这将会是一个很有趣的研究方向. 基于上述想法, 本文提出了一种针对 Feistel、Misty 等结构的新型密钥恢复攻击. 通过将 Simon 量子区分器的周期函数和生日攻击的思想相结合, 本文可以在 $O(2^{3n/4})$ 的时间复杂度和 $O(2^{n/4})$ 的存储复杂度下, 恢复出 5 轮 Feistel-F 结构的密钥. 此外, 上述新型密钥恢复方法还能扩展到 Feistel-FK 结构、Misty 结构和 Type-1/2 型广义 Feistel 结构上.

除了本文分析的几个结构外, 对于其他 Feistel 类型结构, 如 Type-3 GFS、非平衡类的 Feistel 结构等, 同样可以利用本文的方法构造相应的密钥恢复攻击. 但是, 本文的攻击方法需要利用到构造量子区分器的周期函数. 而随着目标结构轮数的增加, 其周期函数的构造会越来越困难. 对于 Type-3 GFS、非平衡类的 Feistel 等结构, 本文的方法无法利用底层函数的性质特点, 这使得我们不能构造出比以往工作更有效的攻击. 因此, 如何对这些 Feistel 类型的结构构造更多轮的量子区分器也值得思考.

References:

[1] Feistel H. Cryptography and computer privacy. Scientific American, 1973, 228(5): 15–23. [doi: 10.1038/scientificamerican0573-15]

[2] GOST. GOST 28147-89 Information processing systems. Cryptographic protection cryptographic transformation algorithm. GOST, 1989.

[3] Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J, Tokita T. Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis. In: Stinson DR, Tavares S, eds. Selected Areas in Cryptography. Berlin: Springer, 2001. 39–56. [doi: 10.1007/3-540-44983-3_4]

[4] Matsui M. New block encryption algorithm MISTY. In: Biham E, ed. Fast Software Encryption. Berlin: Springer, 1997. 54–68. [doi: 10.1007/BFb0052334]

[5] Zheng YL, Matsumoto T, Imai H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard G, ed. Advances in Cryptology (CRYPTO 1989). Lecture Notes in Computer Science, vol 435. New York: Springer, 1990. 461–480. [doi: 10.1007/0-387-34805-0_42]

[6] ETSI. Universal mobile telecommunications system (UMTS); specification of the 3GPP confidentiality and integrity algorithms. Document 2: Kasumi algorithm specification (3GPP TS 35.202 version 3.1. 2 Release 1999).

[7] Adams C, Gilchrist J. The CAST-256 encryption algorithm. Reston: Internet Society 1999. http://ftp.arnes.si/packages/rfc/pdfrfc/rfc2612.txt.pdf

[8] Isobe T, Shibutani K. All subkeys recovery attack on block ciphers: Extending meet-in-the-middle approach. In: Knudsen LR, Wu H, eds. Selected Areas in Cryptography. Berlin: Springer, 2013. 202–221. [doi: 10.1007/978-3-642-35999-6_14]

[9] Isobe T, Shibutani K. Generic key recovery attack on Feistel scheme. In: Sako K, Sarkar P, eds. Proc. of the 19th Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2013). Berlin: Springer, 2013. 464–485. [doi: 10.1007/

978-3-642-42033-7_24]

[10] Dinur I, Dunkelman O, Keller N, Shamir A. New attacks on Feistel structures with improved memory complexities. In: Gennaro R, Robshaw M, eds. Proc. of the 35th Annual Cryptology Conf. Advances in Cryptology (CRYPTO 2015). Berlin: Springer, 2015. 433–454. [doi: 10.1007/978-3-662-47989-6_21]

[11] Zhao SB, Duan XH, Deng YH, Peng ZN, Zhu JH. Improved meet-in-the-middle attacks on generic Feistel constructions. IEEE Access, 2019, 7: 34416–34424. [doi: 10.1109/ACCESS.2019.2900765]

[12] Guo J, Jean J, Nikolic I, Sasaki Y. Meet-in-the-middle attacks on classes of contracting and expanding Feistel constructions. IACR Trans. on Symmetric Cryptology, 2017, 2016(2): 307–337. [doi: 10.13154/tosc.v2016.i2.307-337]

[13] Yang D, Qi WF, Tian T. All-subkeys-recovery attacks on a variation of Feistel-2 block ciphers. IET Information Security, 2017, 11(5): 230–234. [doi: 10.1049/iet-ifs.2016.0014]

[14] Guo J, Jean J, Nikolic I, Sasaki Y. Meet-in-the-middle attacks on generic Feistel constructions. In: Sarkar P, Iwata T, eds. Proc. of the 20th Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2014). Berlin: Springer, 2014. 458–477. [doi: 10.1007/978-3-662-45611-8_24]

[15] Grover LK. A fast quantum mechanical algorithm for database search. In: Proc. of the 28th Annual ACM Symp. on Theory of Computing. Philadelphia: ACM, 1996. 212–219. [doi: 10.1145/237814.237866]

[16] Simon DR. On the power of quantum computation. SIAM Journal on Computing, 1997, 26(5): 1474–1483. [doi: 10.1137/S0097539796298637]

[17] Kuwakado H, Morii M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: Proc. of the 2010 IEEE Int'l Symp. on Information Theory. Austin: IEEE, 2010. 2682–2685. [doi: 10.1109/ISIT.2010.5513654]

[18] Leander G, May A. Grover meets Simon–quantumly attacking the FX-construction. In: Takagi T, Peyrin T, eds. Proc. of the 23rd Int'l Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2017). Cham: Springer, 2017. 161–178. [doi: 10.1007/978-3-319-70697-9_6]

[19] Dong XY, Wang XY. Quantum key-recovery attack on Feistel structures. Science China Information Sciences, 2018, 61(10): 102501. [doi: 10.1007/s11432-017-9468-y]

[20] Ito G, Hosoyamada A, Matsumoto R, Sasaki Y, Iwata T. Quantum chosen-ciphertext attacks against Feistel ciphers. In: Matsui M, ed. Proc. of the 2019 Cryptographers' Track at the RSA Conf. (CT-RSA 2019). Cham: Springer, 2019. 391–411. [doi: 10.1007/978-3-030-12612-4_20]

[21] Luo YY, Yan HL, Wang L, Hu HG, Lai XJ. Study on block cipher structures against Simon's quantum algorithm. Journal of Cryptologic Research, 2019, 6(5): 561–573 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000322]

[22] Gouget A, Patarin J, Toulemonde A. (Quantum) cryptanalysis of misty schemes. In: Hong D, ed. Proc. of the 23rd Int'l Conf. on Information Security and Cryptology (ICISC 2020). Cham: Springer, 2021. 43–57. [doi: 10.1007/978-3-030-68890-5_3]

[23] Cui JY, Guo JS, Ding SZ. Applications of Simon's algorithm in quantum attacks on Feistel variants. Quantum Information Processing, 2021, 20(3): 117. [doi: 10.1007/S11128-021-03027-X]

[24] Deng YH, Jin CH, Li RJ. Meet in the middle attack on type-1 Feistel construction. In: Chen X, Lin D, Yung M, eds. Proc. of the 13th Int'l Conf. on Information Security and Cryptology. Cham: Springer, 2018. 427–444. [doi: 10.1007/978-3-319-75160-3_25]

[25] Dong XY, Li Z, Wang XY. Quantum cryptanalysis on some generalized Feistel schemes. Science China Information Sciences, 2019, 62(2): 22501. [doi: 10.1007/s11432-017-9436-7]

[26] Ni BY, Ito G, Dong XY, Iwata T. Quantum attacks against type-1 generalized Feistel ciphers and applications to CAST-256. In: Hao F, Ruj S, Sen Gupta S, eds. Proc. of the 2019 Int'l Conf. on Cryptology in India, Progress in Cryptology (INDOCRYPT 2019). Cham: Springer, 2019. 433–455. [doi: 10.1007/978-3-030-35423-7_22]

[27] Deng YH. Meet-in-the-middle attacks on three types of generalized Feistel constructions [MS. Thesis]. Zhengzhou: Information Engineering University, 2018 (in Chinese with English abstract).

[28] Kaplan M, Leurent G, Leverrier A, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: Robshaw M, Katz J, eds. Proc. of the 2016 Annual Int'l Cryptology Conf. Advances in Cryptology (CRYPTO 2016). Berlin: Springer, 2016. 207–237. [doi: 10.1007/978-3-662-53008-5_8]

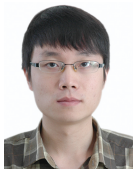
[29] Even S, Mansour Y. A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology, 1997, 10(3): 151–161. [doi: 10.1007/s001459900025]

[30] Biryukov A, Wagner D. Advanced slide attacks. In: Preneel B, ed. Proc. of the 2000 Int'l Conf. on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 2000). Berlin: Springer, 2000. 589–606. [doi: 10.1007/3-540-45539-6_41]

附中文参考文献:

[21] 罗宜元, 闫海伦, 王磊, 胡红钢, 来学嘉. 分组密码结构抗Simon量子算法攻击研究. 密码学报, 2019, 6(5): 561–573. [doi: 10.13868/j.cnki.jcr.000322]

[27] 邓元豪. 三类广义Feistel结构的中间相遇攻击 [硕士学位论文]. 郑州: 战略支援部队信息工程大学, 2018.



邹剑(1985－), 男, 博士, 副教授, 主要研究领域为对称密码分析, 量子计算.

吴文玲(1966－), 女, 博士, 教授, 博士生导师, 主要研究领域为对称密码算法分析与设计.

邹宏楷(1998－), 男, 硕士生, 主要研究领域为量子计算.

罗宜元(1986－), 男, 博士, 副教授, 主要研究领域为对称密码的安全性分析.

董晓阳(1988－), 男, 博士, 副研究员, 主要研究领域为对称密码算法安全性分析, 量子计算.