软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software [doi: 10.13328/j.cnki.jos.007218]

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

分组密码结构的低数据量子密钥恢复攻击*

许琅松[1], 罗宜元[2], 董晓阳[3], 袁 征[4]

[1](北京邮电大学 网络空间安全学院, 北京 100876)

[2](惠州学院 计算机科学与工程学院, 广东 惠州 516007)

[3](清华大学 高等研究院, 北京 100190)

[4](北京电子科技学院, 北京 100070)

通信作者: 罗宜元, E-mail: luoyy@hzu.edu.cn

摘　要: 在 Q1 量子模型下, 针对 Lai-Massey 结构、Misty 结构、Type-1 型广义 Feistel 结构、类 SMS4 广义 Feistel 结构和类 MARS 广义 Feistel 结构, 提出了低数据量子密钥恢复攻击. 该攻击仅需选择常数项级别规模的明密文, 通过分析分组密码结构的加密过程, 利用 Grover 算法对某些中间态进行搜索计算, 从而恢复密钥. 且该攻击属于 Q1 模型, 相比于 Q2 模型, 无需量子叠加查询, 更具有实际意义. 对于 3 轮 Lai-Massey 结构, 相比于其他量子攻击, 该攻击仅需 O(1) 数据, 且属于 Q1 模型, 在复杂度乘积 (时间×数据×经典存储×量子比特) 评估上降低了 $n2^{n/4}$ 因子. 对于 6 轮 Misty 结构, 该方法依然保留着低数据复杂度的优势, 尤其是 6 轮 Misty L/R-FK 结构, 在复杂度乘积评估上降低了 $2^{n/2}$ 因子. 对于 9 轮 3 分支 Type-1 型广义 Feistel 结构, 与其他量子攻击在复杂度乘积评估上保持一致, 该攻击依然保留着低数据复杂度的优势, 且属于选择明文攻击. 此外, 也给出了针对类 SMS4 广义 Feistel 结构和类 MARS 广义 Feistel 结构的低数据量子密钥恢复攻击, 补充了其在 Q1 模型下的安全性评估.

关键词: Lai-Massey 结构; Misty 结构; Type-1 型广义 Feistel 结构; 类 SMS4 广义 Feistel 结构; 类 MARS 广义 Feistel 结构; 密钥恢复攻击

中图法分类号: TP309

中文引用格式: 许琅松, 罗宜元, 董晓阳, 袁征. 分组密码结构的低数据量子密钥恢复攻击. 软件学报. http://www.jos.org.cn/1000-9825/7218.htm

英文引用格式: Xu YS, Luo YY, Dong XY, Yuan Z. Low-data Quantum Key-recovery Attack on Block Cipher Structures. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7218.htm

Low-data Quantum Key-recovery Attack on Block Cipher Structures

XU Yin-Song[1], LUO Yi-Yuan[2], DONG Xiao-Yang[3], YUAN Zheng[4]

[1](School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[2](School of Computer Science and Engineering, Huizhou University, Huizhou 516007, China)

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

[4](Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: In the Q1 model, this paper proposes a low-data quantum key-recovery attack against Lai-Massey structures, Misty structures, Type-1 generalized Feistel structures, SMS4-like generalized Feistel structures and MARS-like generalized Feistel structures. This attack only needs to select constant-sized plain-ciphertexts, analyze the encryption process of block cipher structures, and recover the key by searching and calculating some intermediate states and round keys using Grover's algorithm. This attack belongs to the Q1 model, which is more practical than the Q2 model since no quantum superposition query is required. For the 3-round Lai-Massey structure, compared

* 基金项目: 国家自然科学基金 (62072207); 广东省基础与应用基础研究基金 (2022A1515140090); 北京邮电大学博士创新基金 (CX2022140)
收稿时间: 2023-08-04; 修改时间: 2024-04-03; 采用时间: 2024-04-24; jos 在线出版时间: 2024-09-30

with other quantum attacks, this attack requires only O(1) data and belongs to the Q1 model, and is even reduced by the $n2^{n/4}$ factor on the evaluation of the complexity product (time×data×classical memory×quantum bits). For the 6-round Misty structure, this attack still retains the advantage of low data complexity, and especially for the 6-round Misty L/R-FK structure, this attack is reduced by the $2^{n/2}$ factor on the evaluation of the complexity product. For the 9-round 3-branch Type-1 generalized Feistel structure, in line with other quantum attacks on the evaluation of the complexity product, this attack still retains the advantage of low data complexity and belongs to the chosen plaintext attack. In addition, a low-data quantum key-recovery attack for SMS4-like generalized Feistel structures and MARS-like generalized Feistel structures are also given in this study, complementing their security evaluation in the Q1 model.

Key words: Lai-Massey structure; Misty structure; Type-1 generalized Feistel structure; SMS4-like generalized Feistel structure; MARS-like generalized Feistel structure; key-recovery attack

分组密码作为一种底层加密手段, 在网络空间安全中扮演着重要角色. 分组密码结构作为分组密码的底层设计, 对分组密码结构的分析研究是对具体分组密码的安全性考量, 也是对分组密码设计的参考. 分组密码包含着诸多结构, 如 Feistel 结构[1]、Even-Mansour 结构[2]、Lai-Massey 结构[3]等. 其中, Feistel 结构又包含着一些变体结构, 如 Misty 结构[4]、Type-1/2/3 型广义 Feistel 结构 (generalized feistel structure, GFS)[5]、类 SMS4 广义 Feistel 结构[6]、类 MARS 广义 Feistel 结构[6]等等.

随着量子计算机和量子计算理论的发展, 人们也迫切需要了解分组密码在未来量子计算环境下的安全性, 越来越多的工作开始评估分组密码, 尤其是其底层结构的后量子安全性. 2010 年, Kuwakado 等人[7]提出了 3 轮 Feistel 结构的量子区分器, 利用 Simon 算法[8]可在多项式时间区分是否为随机置换, 结果证明在量子选择明文攻击下 (qCPA), 3 轮 Feistel 结构将不再安全. 2012 年, Kuwakado 等人[9]又利用 Simon 算法对 Even-Mansour 结构在多项式时间内实现密钥恢复攻击. 2016 年美密会上, Kaplan 等人[10]依然利用 Simon 算法对不同加密结构和工作模式的消息认证密码实现伪造攻击. 2017 年亚密会上, Leander 等人[11]将 Grover 算法[12]和 Simon 算法结合起来提出了“Grover Meets Simon”方法, 并应用在 FX 结构上. 后续, “Grover Meets Simon”方法被不断应用在 Feistel 结构[13]、Type-1/2/3 型广义 Feistel 结构[14,15]等结构. 为了优化基于“Grover Meets Simon”方法的量子攻击, 研究者们试图寻找更长的量子区分器. 例如, Ito 等人[16]提出了新的 4 轮 Feistel-F/KF 结构和 6 轮 Feistel-FK 的量子区分器, 在相同轮数 Feistel 结构的密钥恢复攻击条件下, 其复杂度将更低.

以上量子攻击都属于 Q2 模型, 即攻击者可以对加密黑盒 (量子选择明文攻击, qCPA) 或解密黑盒 (量子选择密文攻击, qCCA) 进行量子叠加查询. 而研究者们更希望攻击者能仅对黑盒做经典查询, 再辅以量子计算机做离线计算, 即 Q1 模型. 可以看出, Q2 模型需要攻击者能够访问量子加密或解密黑盒这一理想情况, 一旦被禁止访问, 则攻击将无法进行, 并且在现实情况中数据都被经典计算机进行加密, 所以只需要经典查询的 Q1 模型更具有实际意义. 2018 年, Hosoyamada 等人[17]在 Guo 等人[18]的工作基础上, 提出了针对 6 轮 Feistel 结构的量子中间相遇攻击. 该工作无需量子叠加查询, 且复杂度低于 Guo 等人的工作. 2022 年, Daiza 等人[19]提出了 3 轮 Feistel 结构的新型简洁高效的密钥恢复攻击方法, 在已知明文或选择明文攻击环境下, 仅需几个明密文, 再辅以 Grover 算法进行搜索计算, 即可实现密钥恢复攻击.

受 Daiza 等人的工作启发, 本文针对不同分组密码结构, 包含 Lai-Massey 结构、Misty 结构、Type-1 型 GFS 结构、类 SMS4 GFS 结构和类 MARS GFS 结构, 提出了新型低数据密钥恢复攻击方法, 即仅需选择常数项级别的明密文, 分析分组密码结构的加密过程, 利用 Grover 算法对某些中间态和轮密钥进行搜索计算, 从而恢复密钥. 本文所提方法与其他量子攻击方法的复杂度比较见表 1. 相比于其他量子攻击, 本文的攻击无需量子叠加查询, 且数据复杂度仅为 O(1) . 对于 3 轮 Lai-Massey 结构 , 虽然本文的方法时间复杂度为 $O(2^{n/4})$, 高于文献 [20], 但是仅需 O(1) 明密文, 无需量子叠加查询, 且在所有复杂度乘积 (时间×数据×经典存储×量子比特) 的评估上, 更少了 $n2^{n/4}$ 因子. 对于 6 轮 Misty L- KF 结构, 相比于文献 [21], 本文的方法仅需 O(1) 明密文. 而对于 6 轮 Misty L- FK 结构, 本文与文献 [21] 保持相同的时间复杂度, 但数据复杂度仅为 O(1) , 且复杂度乘积更低了 $2^{n/2}$ 因子, 甚至更优于文献 [6] 的 qCPA 方法. 对于 6 轮 Misty R- KF 结构, 本文的方法相比于文献 [21] 属于选择明文攻击, 而非选择密文攻击. 对于 6 轮 Misty R- FK 结构, 本文的方法相比于文献 [21], 只需 O(1) 明密文, 且属于选择明文攻击. 当 $d = 3$

时, 针对 9 轮 Type-1 GFS-KF 的密钥恢复攻击, 本文的方法可与文献 [21] 在复杂度乘积指标上保持一致, 但属于选择明文攻击且仅需 O(1) 明密文. 对于类 SMS4 GFS-FK 和类 MARS GFS-FK, 本文给出了在 Q1 模型下, 仅需选择常数项级别规模的明密文即可恢复密钥的方案.

表 1　几类分组密码结构的密钥恢复攻击复杂度比较

目标结构	环境	轮数	时间 (T)	数据 (D)	经典存储 (M)	量子比特 (Q)	复杂度乘积 ($TDMQ$)	文献
Lai-Massey	Q2, qCPA	3	$O(n)$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{n/2})$	[20]
	Q2, qCCA	4	$O(n)$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{n/2})$	[20]
	Q1, CPA	3	$O(2^{n/4})$	$O(1)$	—	$O(n)$	$O(n2^{n/4})$	本文
Misty L- KF	Q1, CPA	6	$O(2^{3n/4})$	$O(2^{n/4})$	$O(2^{n/4})$	$O(n)$	$O(n2^{5n/4})$	[21]
	Q2, qCPA	6	$O(n2^{n/4})$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{3n/4})$	[6]
	Q1, CPA	6	$O(2^{5n/4})$	$O(1)$	—	$O(n)$	$O(n2^{5n/4})$	本文
Misty L-FK	Q1, CPA	6	$O(2^{3n/4})$	$O(2^{n/4})$	$O(2^{n/4})$	$O(n)$	$O(n2^{5n/4})$	[21]
	Q2, qCPA	6	$O(n2^{n/4})$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{3n/4})$	[6]
	Q1, CPA	6	$O(2^{3n/4})$	$O(1)$	—	$O(n)$	$O(n2^{3n/4})$	本文
Misty R-KF	Q1, CCA	6	$O(2^{3n/4})$	$O(2^{n/4})$	$O(2^{n/4})$	$O(n)$	$O(n2^{5n/4})$	[21]
	Q2, qCPA	6	$O(n2^{n/4})$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{3n/4})$	[6]
	Q1, CPA	6	$O(2^{5n/4})$	$O(1)$	—	$O(n)$	$O(n2^{5n/4})$	本文
Misty R-FK	Q1, CCA	6	$O(2^{3n/4})$	$O(2^{n/4})$	$O(2^{n/4})$	$O(n)$	$O(n2^{5n/4})$	[21]
	Q2, qCPA	6	$O(n2^{n/4})$	$O(2^{n/2})$	—	$O(n)$	$O(n^2 2^{3n/4})$	[6]
	Q1, CPA	6	$O(2^{3n/4})$	$O(1)$	—	$O(n)$	$O(n2^{3n/4})$	本文
Type-1 GFS-KF	Q1, CCA	d^2	$O(2^{(2d-1)n/2d})$	$O(2^{n/2d})$	$O(2^{n/2d})$	$O(n)$	$O(n2^{(2d+1)n/2d})$	[21]
	Q2, qCCA	d^2-d+3	$O(n/d)$	$O(2^{n/d})$	—	$O(n)$	$O(n^2/d\cdot 2^{n/d})$	[6]
	Q1, CPA	$3d-3$	$O(2^{n/2d})$	$O(1)$	—	$O(n)$	$O(n2^{n/2d})$	本文
类SMS4 GFS-FK	Q2, qCPA	$2d+1$	$O(n/d)$	$O(2^{n/d})$	—	$O(n)$	$O(n^2/d\cdot 2^{n/d})$	[6]
	Q1, CPA	$2d-1$	$O(2^{n/2d})$	$O(1)$	—	$O(n)$	$O(n2^{n/2d})$	本文
类MARS GFS-FK	Q2, qCPA	$2d+1$	$O(n/d)$	$O(2^{n/d})$	—	$O(n)$	$O(n^2/d\cdot 2^{n/d})$	[6]
	Q1, CPA	$2d-1$	$O(2^{n/2d})$	$O(1)$	—	$O(n)$	$O(n2^{n/2d})$	本文

注: 分组长度为 n 比特; d 为分支数; qCPA和CPA为(量子)选择明文攻击; qCCA和CCA为(量子)选择密文攻击

本文第 1 节将介绍 Lai-Massey 结构、Misty 结构、Type-1 型 GFS、类 SMS4 GFS 和类 MARS GFS 的分析研究现状. 第 2 节介绍本文所攻击分组密码结构的基础知识和概念. 第 3 节介绍 Grover 算法及其应用. 第 4–8 节分别介绍了 Lai-Massey 结构、Misty 结构、Type-1 型 GFS、类 SMS4 GFS 和类 MARS GFS 的密钥恢复攻击. 最后总结全文.

1　分组密码结构的密钥恢复攻击相关工作

在 1990 年欧密会上, Lai 等人[3]提出了 IDEA 算法. Vaudenay 推广了 IDEA 所采用的加密结构, 并称其为 Lai-Massey 结构. 3 轮和 4 轮 Lai-Massey 结构已被 Vaudenay 等人[22]分别证明可以抵抗选择明文攻击 (CPA) 和选择密文攻击 (CCA). Luo 等人[23]证明了多轮 Lai-Massey 结构是超生日界限 CCA 安全的. 在量子选择明文攻击 (qCPA) 环境下, Mao 等人[20]提出了 3 轮 Lai-Massey 结构的量子区分器, 且在量子选择密文攻击环境下, 提出了 4 轮 Lai-Massey 结构的量子区分器. 借助于 Simon 算法, Mao 等人提出的量子区分器可在多项式时间内进行区分. 他们还利用 Grover Meets Simon 方法对 Lai-Massey 结构的攻击轮数进行拓展.

Misty 结构[4]作为 Feistel 结构的变体, 由 Matsui 在 1997 年 FSE 会议上提出的分组密码 Misty 推广而来, 可分为 Misty L 和 Misty R 结构. 2019 年, Luo 等人[24]分别提出了 Misty L 和 Misty R 结构的 3 轮量子区分器, 并在

qCPA 环境下利用 Simon 算法在多项式时间区分是否随机. 随后, Gouget 等人[25]改进了这一结果, 给出了一个 4 轮 Misty L 结构的 qCPA 区分器. 而 Cui 等人[6]则更进一步, 分别提出了 Misty L-FK 结构的 5 轮 qCPA 区分器和 Misty R-FK 结构的 5 轮 qCCA 区分器. Zou 等人[21]通过结合 Simon 算法的周期函数和生日攻击的思想, 在 Q1 模型下提出了对 5 轮 Misty L/R-F 结构和 6 轮 Misty L/R-KF/FK 结构的密钥恢复攻击.

Type-1 型广义 Feistel 结构是 Feistel 结构的一个推广, CAST-256[26]则是基于该结构设计出来的. Deng 等人[27]基于中间相遇方法提出了 $5d-3$ 轮 d 分支 Type-1 型广义 Feistel 结构的密钥恢复攻击方法. 在量子环境 Q2 模型下, Dong 等人[14]基于 Simon 算法提出了 $2d-1$ 轮 Type-1 型广义 Feistel 结构的量子区分器. 随后, Ni 等人[28]进一步改进了这一结果, 提出了 $3d-3$ 轮 qCPA 区分器和 d^2-d+1 轮 qCCA 区分器. Zou 等人[21]在 d^2-d+1 轮 qCCA 区分器基础上, 在 Q1 模型下提出了 d^2 Type-1 型广义 Feistel 结构的密钥恢复攻击.

SMS4 是中国公布的商用分组密码[29]. You 等人[30]提出了 6 轮 SMS4 的 qCPA 区分器. Cid 等人[31]进一步证明了 7 轮 SMS4 在量子环境下也是不安全的. Cui 等人[6]为了更一般化地评估 SMS4 底层结构, 将 SMS4 所使用的加密结构称为类 SMS4 广义 Feistel 结构, 并提出了 $2d-1$ 轮类 SMS4 广义 Feistel-F/KF 结构的 qCPA 区分器和 $2d+1$ 类 SMS4 广义 Feistel-FK 结构的 qCPA 区分器.

Cui 等人[6]称呼 MARS 分组密码所用的底层结构为类 MARS 广义 Feistel 结构. Moriai 等人[32]已证明 5 轮 MARS 方案是伪随机的且 8 轮 MARS 方案是超伪随机的. 在 Q2 模型下, Cui 等人[6]提出了 $2d-1$ 轮类 MARS 广义 Feistel-F/KF 结构的 qCPA 区分器和 $2d+1$ 类 MARS 广义 Feistel-FK 结构的 qCPA 区分器.

2 相关密码结构

本文主要针对 Lai-Massey 结构、Misty 结构、Type-1 型广义 Feistel 结构、类 SMS4 广义 Feistel 结构和类 MARS 广义 Feistel 结构, 下面就相关概念予以介绍.

2.1 Lai-Massey 结构

本文中被攻击的 Lai-Massey 结构使用 XOR 运算代替一般的加法和减法运算, 且置换 σ 满足 $\sigma(x_L,x_R)=(x_R, x_L\oplus x_R)$, 如图 1(a) 所示. 第 i 轮 Lai-Massey 结构的输入为 (x_{i-1},y_{i-1}), 则输出为 $(x_i,y_i)\leftarrow(\sigma(x_{i-1}\oplus F_i(\Delta_{i-1})),y_{i-1}\oplus F_i(\Delta_{i-1}))$, 其中 $\Delta_{i-1}=x_{i-1}\oplus y_{i-1}$, F_i 为第 i 轮轮函数. 在最后一轮, 左半分支将无须置换 σ, 即输出为 $(x_i,y_i)\leftarrow(x_{i-1}\oplus F_i(\Delta_{i-1}),y_{i-1}\oplus F_i(\Delta_{i-1}))$. 本文中设 Lai-Massey 结构的输入为 n 比特, 则其左右分支状态均为 $n/2$ 比特.

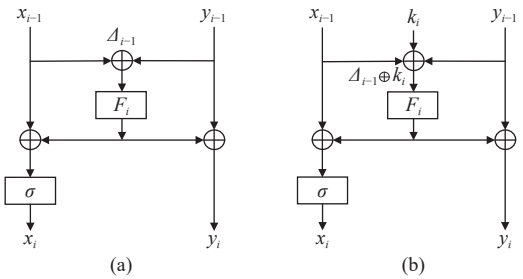


图 1 Lai-Massey 结构

类似于 Ito 等人在文献 [16] 中的命名方式, 我们根据密钥注入的方式, 即将轮密钥 k_i 与中间态 Δ_{i-1} 异或后作为轮函数 F_i 的输入, 称其为 Lai-Massey-KF 结构, 如图 1(b) 所示.

2.2 Misty 结构

由于 XOR 运算位置不同, Misty 结构可分为 L 和 R 两种结构, 如图 2 所示. 设 Misty L 结构第 i 轮的输入状态为 (x_{i-1},y_{i-1}), 则其第 i 轮的输出状态为 $(x_i,y_i)\leftarrow(y_{i-1},F_i(k_i,x_{i-1})\oplus y_{i-1})$. 类似地, 如图 2(b) 所示, Misty R 结构第 i 轮的输出状态为 $(x_i,y_i)\leftarrow(y_{i-1}\oplus F_i(k_i,x_{i-1}),F_i(k_i,x_{i-1}))$. 同样地, 本文假设 Misty 结构的输入为 n 比特, 则其左右分支状态均为 $n/2$ 比特.

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.

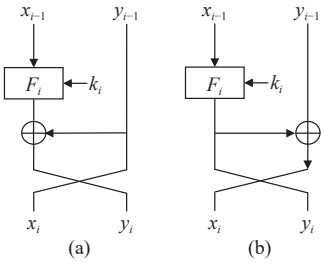


图 2　Misty L 和 Misty R 结构

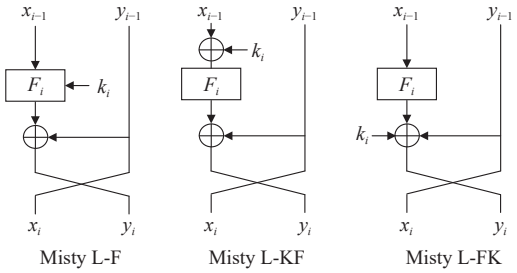


图 3　3 种 Misty L 方案: Misty L-F、Misty L-KF 和 Misty L-FK

2.3　Type-1 型广义 Feistel 结构

本文中设 Type-1 型广义 Feistel 结构有 d 个分支, 整个分组长度为 n 比特且轮密钥 k_i 的比特长度为 n/d. 设其第 i 轮的输入为 $(x_0^{i-1},x_1^{i-1},\ldots,x_{d-1}^{i-1})$, 则对应的输出状态为 $(x_0^i,x_1^i,\ldots,x_{d-1}^i) \leftarrow (F_i(x_0^{i-1},k_i)\oplus x_1^{i-1},x_2^{i-1},\ldots,x_{d-1}^{i-1},x_0^{i-1})$, 如图 4 所示.

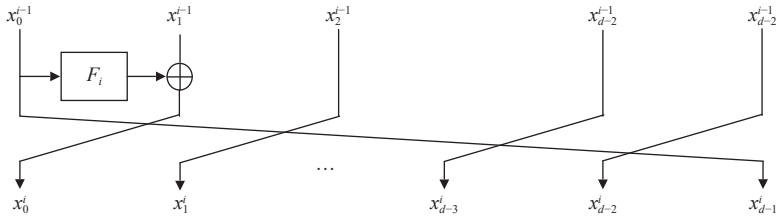


图 4　第 i 轮 Type-1 型广义 Feistel 结构

2.4　类 SMS4 广义 Feistel 结构

本文中设类 SMS4 广义 Feistel 结构有 d 个分支, 分组长度为 n 比特, 则轮密钥 k_i 的比特长度为 n/d. 设其第 i 轮的输入为 $(x_0^{i-1},x_1^{i-1},\ldots,x_{d-1}^{i-1})$, 则对应的输出状态为 $(x_0^i,x_1^i,\ldots,x_{d-1}^i) \leftarrow (x_1^{i-1},\ldots,x_{d-1}^{i-1},F_i(x_1^{i-1}\oplus\ldots\oplus x_{d-1}^{i-1},k_i)\oplus x_0^{i-1})$, 如图 5 所示.

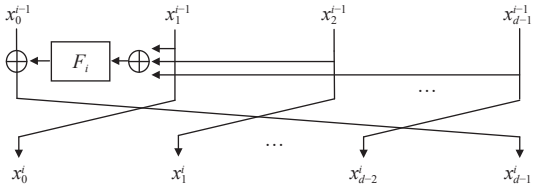


图 5　第 i 轮类 SMS4 广义 Feistel 结构

2.5　类 MARS 广义 Feistel 结构

本文中设类 MARS 广义 Feistel 结构有 d 个分支, 分组长度为 n 比特, 则轮密钥 k_i 的比特长度为 n/d. 设其第 i 轮的输入为 $(x_0^{i-1},x_1^{i-1},\ldots,x_{d-1}^{i-1})$, 则对应的输出状态为 $(x_0^i,x_1^i,\ldots,x_{d-1}^i) \leftarrow (F_i(x_0^{i-1},k_i)\oplus x_1^{i-1},\ldots,F_i(x_0^{i-1},k_i)\oplus x_{d-1}^{i-1},x_0^{i-1})$, 如图 6 所示.

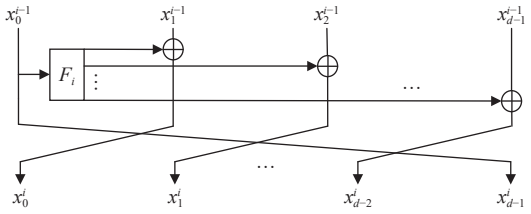


图 6 第 i 轮类 MARS 广义 Feistel 结构

3 Grover 算法及其应用

对于从 N 个无序元素列表中搜索出一个目标元素的问题, 一般情形下, 经典算法平均需要 $N/2$ 次查询列表. 而基于量子计算的并行计算特性, Grover 算法仅需要 $\sqrt{N}$ 次查询, 相比于经典搜索进行了二次加速. Grover 算法具体过程如算法 1 所示. 此外, Brassard 等人又在 Grover 算法的基础上拓展出幅度放大算法[33], 并且针对密码分析中常见的碰撞问题, 提出了 BHT 碰撞搜索算法[34].

算法 1. Grover 算法[12].

输入: 量子 Oracle O_f 可执行变换 $O_f|x\rangle|q\rangle=|x\rangle|q\oplus f(x)\rangle$, 其中, 布尔函数 $f(x)=1$ 仅当 $x=x_0$, $0\leqslant x\leqslant 2^n-1$; $n+1$ 个量子比特;

输出: x_0.

1. 制备初始态 $|\varphi_1\rangle=|0\rangle^{\otimes n}|0\rangle$.

2. 在前 n 个量子比特上执行 $H^{\otimes n}$, 以及在最后一个量子比特上执行 HX, 得到态 $|\varphi_2\rangle=\dfrac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$.

3. 执行 $R\approx\left\lceil\pi\sqrt{2^n}/4\right\rceil$ 次 Grover 迭代算子 $G=[(2|\varphi_2\rangle\langle\varphi_2|-I)O_f]$ 得到态 $|\varphi_3\rangle=[(2|\varphi_2\rangle\langle\varphi_2|-I)O_f]^R\dfrac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\approx|x_0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$.

4. 测量前 n 个量子比特, 得到 x_0.

在量子密码分析中, 通常利用 Grover 算法直接穷举搜索正确密钥, 因此复杂度由密钥空间大小决定, 但是该方法的复杂度不一定低于利用经典分析方法 (不利用量子计算机) 来恢复密钥. 但是, 利用 Grover 算法直接穷举搜索正确密钥的方法仅需要几个已知明文与其对应的密文, 这也是该方法相比于其他量子密码分析方法的另一优势, 只需要经典查询且数据复杂度仅为常数项级别. 为了发挥这一优势, Daiza 等人[19]针对 3 轮 Feistel-KF 结构 (或称为 Feistel-2 结构) 提出了新的量子密钥恢复攻击, 而不需要量子查询. 其基本思想是根据 3 轮 Feistel-KF 结构的一些特性, 利用 Grover 算法搜索出所需的中间状态值, 并根据这些中间状态值搜索出正确轮密钥. 相比于其他量子攻击, 该攻击仅需要经典查询且数据复杂度为 O(1). 尽管需要 $O(2^{n/4})$ 时间 (n 为分组长度), 但依然优于经典分析的 $O(2^{n/2})$.

4 对 Lai-Massey 结构的密钥恢复攻击

受 Daiza 等人[19]工作的启发, 本文将分析 3 轮 Lai-Massey 结构, 并利用 Grover 算法辅助进行搜索计算, 提出新型量子密钥恢复攻击.

如图 7 所示的 3 轮 Lai-Massey 结构, 其中 F_1、F_2 和 F_3 为轮函数, $\sigma(x_L,x_R)=(x_R,x_L\oplus x_R)$ (x_L 和 x_R 分别表示 x_i 的左半部分和右半部分比特). 设 $[a,b]\in\{0,1\}^n$, 其中 a, b 分别表示高位 $n/2$ 比特和低位 $n/2$ 比特. 设 $[x_i^0,x_i^1]$, $[y_i^0,y_i^1]\in\{0,1\}^n$, $i=0,1,2,3$. $[x_0^0,x_0^1]$, $[y_0^0,y_0^1]$ 为 3 轮 Lai-Massey 结构的输入, $[x_3^0,x_3^1]$, $[y_3^0,y_3^1]$ 作为输出.

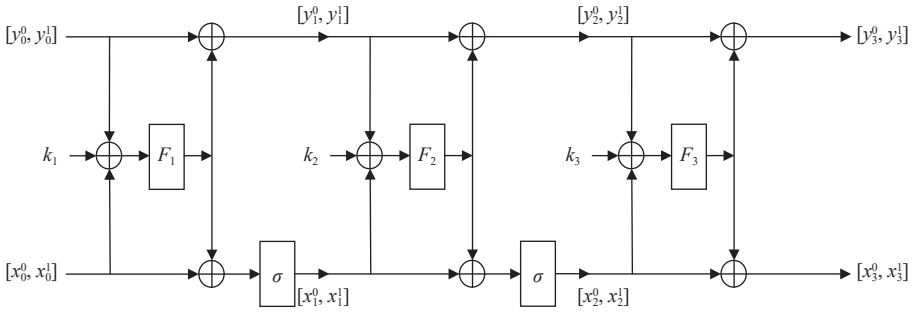


图 7　3 轮 Lai-Massey 结构

根据 3 轮 Lai-Massey 结构的计算, 可以得到中间状态:

$$
\begin{aligned}
&x_1^0 = x_0^1 \oplus F_{1R}(\Delta_1),\\
&x_1^1 = x_0^0 \oplus x_0^1 \oplus F_{1L}(\Delta_1) \oplus F_{1R}(\Delta_1),\\
&y_1^0 = y_0^0 \oplus F_{1L}(\Delta_1),\\
&y_1^1 = y_0^1 \oplus F_{1R}(\Delta_1),\\
&x_2^0 = x_0^0 \oplus x_0^1 \oplus F_{1L}(\Delta_1) \oplus F_{1R}(\Delta_1) \oplus F_{2R}(\Delta_2),\\
&x_2^1 = x_0^0 \oplus F_{1L}(\Delta_1) \oplus F_{2L}(\Delta_2) \oplus F_{2R}(\Delta_2),\\
&y_2^0 = y_0^0 \oplus F_{1L}(\Delta_1) \oplus F_{2L}(\Delta_2),\\
&y_2^1 = y_0^1 \oplus F_{1R}(\Delta_1) \oplus F_{2R}(\Delta_2),\\
&x_3^0 = x_0^0 \oplus x_0^1 \oplus F_{1L}(\Delta_1) \oplus F_{1R}(\Delta_1) \oplus F_{2R}(\Delta_2) \oplus F_{3L}(\Delta_3),\\
&x_3^1 = x_0^0 \oplus F_{1L}(\Delta_1) \oplus F_{2L}(\Delta_2) \oplus F_{2R}(\Delta_2) \oplus F_{3R}(\Delta_3),\\
&y_3^0 = y_0^0 \oplus F_{1L}(\Delta_1) \oplus F_{2L}(\Delta_2) \oplus F_{3L}(\Delta_3),\\
&y_3^1 = y_0^1 \oplus F_{1R}(\Delta_1) \oplus F_{2R}(\Delta_2) \oplus F_{3R}(\Delta_3).
\end{aligned}
$$

其中:

$$
\begin{aligned}
&\Delta_1 = [x_0^0 \oplus y_0^0, x_0^1 \oplus y_0^1] \oplus k_1,\\
&\Delta_2 = [x_0^1 \oplus y_0^0 \oplus F_{1L}(\Delta_1) \oplus F_{1R}(\Delta_1), x_0^0 \oplus x_0^1 \oplus y_0^1 \oplus F_{1L}(\Delta_1)] \oplus k_2,\\
&\Delta_3 = [x_0^0 \oplus x_0^1 \oplus y_0^0 \oplus F_{1R}(\Delta_1) \oplus F_{2L}(\Delta_2) \oplus F_{2R}(\Delta_2), x_0^0 \oplus y_0^1 \oplus F_{1L}(\Delta_1) \oplus F_{1R}(\Delta_1) \oplus F_{2L}(\Delta_2)] \oplus k_3,
\end{aligned}
$$

且 $F_{iL}(\cdot)$ 和 $F_{iR}(\cdot)$ ($i = 1,2,3$) 表示轮函数 $F_i(\cdot)$ 输出结果的左半部分和右半部分比特. 依据上述这些公式, 我们可以推导出 x_3^0 与 y_3^0 之间的关系, 如公式 (1) 所示.

$$
x_3^0 \oplus y_3^0 = x_0^0 \oplus x_0^1 \oplus y_0^0 \oplus F_{1R}(\Delta_1) \oplus F_{2L}(\Delta_2) \oplus F_{2R}(\Delta_2) \tag{1}
$$

在了解了 3 轮 Lai-Massey 结构以后, 我们给出如下选择明文攻击环境下的密钥恢复攻击过程.

(1) 选择明文 $P_0 = [\alpha_0, \alpha_0] \| \| [\alpha_0, \alpha_0]$ 和 $P_1 = [\alpha_1, \alpha_1] \| \| [\alpha_1, \alpha_1]$, 查询出其对应的密文, 根据公式 (1) 可计算出:

$$
\begin{aligned}
x_3^0(P_0) \oplus y_3^0(P_0) =& \alpha_0 \oplus F_{1R}([0,0] \oplus k_1) \oplus F_{2L}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_0 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)\\
&\oplus F_{2R}([f_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_0 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2),\\
x_3^0(P_1) \oplus y_3^0(P_1) =& \alpha_1 \oplus F_{1R}([0,0] \oplus k_1) \oplus F_{2L}([f_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_1 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)\\
&\oplus F_{2R}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_1 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2),
\end{aligned}
$$

则可推出以下公式:

$$
\begin{aligned}
x_3^0(P_0) \oplus y_3^0(P_0) \oplus x_3^0(P_1) \oplus y_3^0(P_1) =& \alpha_0 \oplus \alpha_1 \oplus F_{2L}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_0 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)\\
&\oplus F_{2R}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_0 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)\\
&\oplus F_{2L}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_1 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)\\
&\oplus F_{2R}([F_{1L}([0,0] \oplus k_1) \oplus F_{1R}([0,0] \oplus k_1), \alpha_1 \oplus F_{1L}([0,0] \oplus k_1)] \oplus k_2)
\end{aligned} \tag{2}
$$

(2) 假设:

$$\beta_0 = [F_{1L}([0,0]\oplus k_1)\oplus F_{1R}([0,0]\oplus k_1), \alpha_0 \oplus F_{1L}([0,0]\oplus k_1)]\oplus k_2,$$

$$\beta_1 = [F_{1L}([0,0]\oplus k_1)\oplus F_{1R}([0,0]\oplus k_1), \alpha_1 \oplus F_{1L}([0,0]\oplus k_1)]\oplus k_2.$$

则公式 (2) 可简写成:

$$x_3^0(P_0)\oplus y_3^0(P_0)\oplus x_3^0(P_1)\oplus y_3^0(P_1) = \alpha_0\oplus\alpha_1\oplus F_{2L}(\beta_0)\oplus F_{2R}(\beta_0)\oplus F_{2L}(\beta_1)\oplus F_{2R}(\beta_1) \tag{3}$$

且 $\beta_0\oplus\beta_1 = [0, \alpha_0\oplus\alpha_1]$. 设 $\beta_0 =: x$, $x\in\{0,1\}^n$, 根据公式 (3) 构造函数:

$$G(x) = \alpha_0\oplus\alpha_1\oplus F_{2L}(x)\oplus F_{2R}(x)\oplus F_{2L}(x\oplus[0,\alpha_0\oplus\alpha_1])\oplus F_{2R}(x\oplus[0,\alpha_0\oplus\alpha_1]) \tag{4}$$

由于函数 F_2 公开已知, 且已知 $x_3^0(P_0)\oplus y_3^0(P_0)\oplus x_3^0(P_1)\oplus y_3^0(P_1)$ 值和 α_0、α_1 值, 则可通过 Grover 算法搜索出 x 使得 $G(x) = x_3^0(P_0)\oplus y_3^0(P_0)\oplus x_3^0(P_1)\oplus y_3^0(P_1)$, 即 β_0 值.

(3) 选择明文 $P_2 = [0,0]\|\|[\alpha_0,\alpha_1]$ 和 $P_3 = [\alpha_0,0]\|\|[0,\alpha_1]$, 查询它们对应的密文, 与步骤 (1) 一样, 求出以下值:

$$\begin{aligned}x_3^0(P_2)\oplus y_3^0(P_2) =&\alpha_0\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{2L}([\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\\ &\oplus F_{2R}([\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2),\\ x_3^0(P_3)\oplus y_3^0(P_3) =&\alpha_0\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{2L}([f_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_0\oplus\alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\\ &\oplus F_{2R}([f_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_0\oplus\alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2),\end{aligned}$$

再异或相加得到:

$$\begin{aligned}x_3^0(P_2)\oplus y_3^0(P_2)\oplus x_3^0(P_3)\oplus y_3^0(P_3) =&F_{2L}([\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\\ &\oplus F_{2R}([\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\\ &\oplus F_{2L}([F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_0\oplus\alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\\ &\oplus F_{2R}([F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_0\oplus\alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2)\end{aligned} \tag{5}$$

(4) 同样设:

$$\beta_2 = [\alpha_0\oplus f_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus f_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_1\oplus f_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2,$$

$$\beta_3 = [f_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus f_{1R}([\alpha_0,\alpha_1]\oplus k_1), \alpha_0\oplus\alpha_1\oplus f_{1L}([\alpha_0,\alpha_1]\oplus k_1)]\oplus k_2.$$

则公式 (5) 可以简写成:

$$x_3^0(P_2)\oplus y_3^0(P_2)\oplus x_3^0(P_3)\oplus y_3^0(P_3) = F_{2L}(\beta_2)\oplus F_{2R}(\beta_2)\oplus F_{2L}(\beta_3)\oplus F_{2R}(\beta_3) \tag{6}$$

且 $\beta_3\oplus\beta_2 = [\alpha_0,\alpha_0]$. 依然设 $\beta_2 =: x$, $x\in\{0,1\}^n$, 根据公式 (6) 构造函数:

$$G'(x) = F_{2L}(x)\oplus F_{2R}(x)\oplus F_{2L}(x\oplus[\alpha_0,\alpha_0])\oplus F_{2R}(x\oplus[\alpha_0,\alpha_0]) \tag{7}$$

由于函数 F_2 公开已知, 且已知 $x_3^0(P_2)\oplus y_3^0(P_2)\oplus x_3^0(P_3)\oplus y_3^0(P_3)$ 和 α_0、α_1 值, 则可通过 Grover 算法搜索出 x 使得 $G'(x) = x_3^0(P_2)\oplus y_3^0(P_2)\oplus x_3^0(P_3)\oplus y_3^0(P_3)$, 即 β_2 值.

(5) 得到 β_0 和 β_2 值后, 异或可得:

$$\beta_0\oplus\beta_2 = [\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus k_1)\oplus F_{1L}(k_1)\oplus F_{1R}(k_1), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus k_1)\oplus\alpha_0\oplus F_{1L}(k_1)].$$

令 $k_1 =: x$, 构造函数:

$$H(x) = [\alpha_0\oplus F_{1L}([\alpha_0,\alpha_1]\oplus x)\oplus F_{1R}([\alpha_0,\alpha_1]\oplus x)\oplus F_{1L}(x)\oplus F_{1R}(x), \alpha_1\oplus F_{1L}([\alpha_0,\alpha_1]\oplus x)\oplus\alpha_0\oplus F_{1L}(x)] \tag{8}$$

由于已知公开函数 F_1, $\beta_0\oplus\beta_2$, α_0 和 α_1 值, 可通过 Grover 算法搜索出 x 满足 $H(x) = \beta_0\oplus\beta_2$, 即为 k_1 值.

(6) 获得 k_1 值, 可通过 β_0 求出 k_2, 最后计算出 k_3.

复杂度分析. 通过上述密钥恢复攻击过程可知, 在选择明文攻击环境下, 我们提出的攻击仅需 4 个明文 $\{P_0,P_1,P_2,P_3\}$ 及其对应的密文则可恢复密钥. 并且在第 (2)、(4)、(5) 步中利用 Grover 算法搜索解时所需时间分别为 $O(2^{n/2})$, 所以总的时间复杂度也为 $O(2^{n/2})$. 此外, 数据复杂度仅为 $O(1)$, 经典存储复杂度可忽略不计.

5 对 Misty 结构的密钥恢复攻击

本文针对 Lai-Massey 结构的新型量子密钥恢复攻击思想同样可以被应用到 Misty 结构上.

5.1 对 Misty L-KF 结构的密钥恢复攻击

在本节中, 我们将主要以 Misty L-KF 结构作为攻击目标. 如图 8 所示的 4 轮 Misty L-KF 结构, 其中 $F_i(x_{i-1}\oplus k_i)$ $(i=1,2,3,4)$ 为轮函数, k_i 为轮密钥且 $|k_i|=n/2\,(i=1,2,3,4)$, (x_0,y_0) 为 4 轮 Misty L-KF 结构的明文输入且 $|(x_0,y_0)|=n$, (x_4,y_4) 作为密文输出.

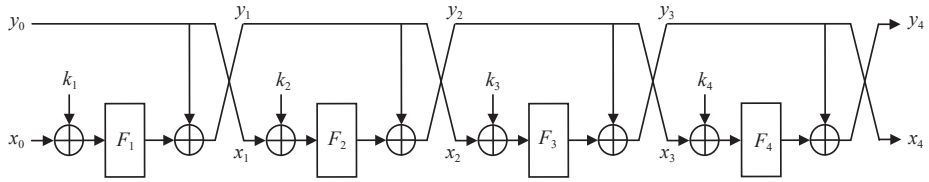


图 8　4 轮 Misty L-KF 结构

根据 Misty L-KF 结构的加密过程, 我们可以得到密文 (x_4,y_4) 的值为:

$$x_4=y_0\oplus F_1(x_0\oplus k_1)\oplus F_2(y_0\oplus k_2)\oplus F_3(y_0\oplus F_1(x_0\oplus k_1)\oplus k_3),$$

$$y_4=y_0\oplus F_1(x_0\oplus k_1)\oplus F_2(y_0\oplus k_2)\oplus F_3(y_0\oplus F_1(x_0\oplus k_1)\oplus k_3)\oplus F_4(y_0\oplus F_1(x_0\oplus k_1)\oplus F_2(y_0\oplus k_2)\oplus k_4),$$

将密文的左半部分 x_4 与右半部分 y_4 异或后可得:

$$x_4\oplus y_4=F_4(y_0\oplus F_1(x_0\oplus k_1)\oplus F_2(y_0\oplus k_2)\oplus k_4) \tag{9}$$

根据公式 (9) 可设函数:

$$G(x,y)=F_4(y\oplus F_1(x\oplus k_1)\oplus F_2(y\oplus k_2)\oplus k_4) \tag{10}$$

其中, 变量 x 和 y 分别对应明文 x_0 和 y_0; $x,y\in\{0,1\}^{n/2}$ 且 $G(x,y)\in\{0,1\}^{n/2}$. 在公式 (10) 的基础上, 我们可以构建新的 4 轮 Misty L-KF 结构密钥恢复攻击, 具体过程如下.

(1) 选择明文 (x_0^1,y_0^1) 和 (x_0^1,y_0^2), 并查询其对应的密文. 根据公式 (9)、(10) 可得:

$$G(x_0^1,y_0^1)=F_4(y_0^1\oplus F_1(x_0^1\oplus k_1)\oplus F_2(y_0^1\oplus k_2)\oplus k_4),G(x_0^1,y_0^2)=F_4(y_0^2\oplus F_1(x_0^1\oplus k_1)\oplus F_2(y_0^2\oplus k_2)\oplus k_4).$$

设 $\beta_1=y_0^1\oplus F_1(x_0^1\oplus k_1)\oplus F_2(y_0^1\oplus k_2)\oplus k_4$, $\beta_2=y_0^2\oplus F_1(x_0^1\oplus k_1)\oplus F_2(y_0^2\oplus k_2)\oplus k_4$, 则$G(x_0^1,y_0^1)=F_4(\beta_1)$ 且$G(x_0^1,y_0^2)=F_4(\beta_2)$. 由于已知公开函数$F_4$, $G(x_0^1,y_0^1)$ 和$G(x_0^1,y_0^2)$ 值, 利用 Grover 算法可搜索出 β_1 和 β_2 值.

(2) β_1 和β_2 异或后可得$\beta_1\oplus\beta_2=y_0^1\oplus y_0^2\oplus F_2(y_0^1\oplus k_2)\oplus F_2(y_0^2\oplus k_2)$. 由于已知公开函数 F_2, $\beta_1\oplus\beta_2$, y_0^1 和 y_0^2 值, 依然可利用 Grover 算法搜索出轮密钥 k_2.

(3) 对于剩下的轮密钥 k_1, k_4 和 k_3, 可依次通过 Grover 算法搜索出来.

复杂度分析. 通过上述密钥恢复攻击过程可知, 我们的攻击仅需 4 个明文, 且每一步中的 Grover 搜索时间为 $O(2^{n/4})$, 则总的时间复杂度依然为 $O(2^{n/4})$. 其数据复杂度仅为 $O(1)$, 经典存储复杂度可忽略不计.

如果扩展 $r-4$ 轮构成 r 轮 Misty L-KF 结构, 则可先穷举 k_5-k_r, 对每一次猜测的 k_5-k_r, 重复以上 3 个步骤, 若得到的所有轮密钥 k_1-k_r 都能使明密文正确地加解密, 则所有轮密钥 k_1-k_r 计算正确. 整个密钥恢复过程的时间复杂度为 $O(2^{n/4+(r-4)n/2})$, 数据复杂度同样仅为 $O(1)$, 且经典存储复杂度可忽略不计.

5.2 对 Misty L-FK 结构的密钥恢复攻击

在本节中, 我们将先给出针对 5 轮 Misty L-FK 结构 (如图 9 所示) 的密钥恢复攻击过程.

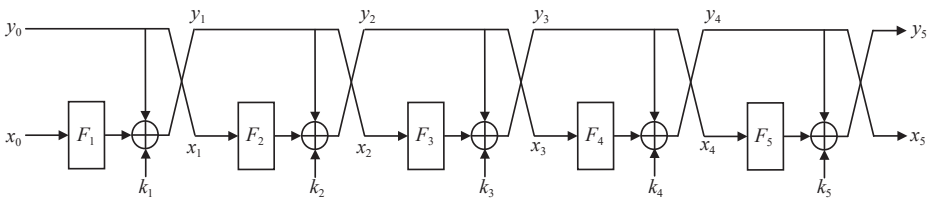


图 9　5 轮 Misty L-FK 结构

根据 Misty L-FK 结构的加密过程, 可得到密文 (x_5,y_5) 的值为:

$$x_5 = y_0 \oplus F_1(x_0) \oplus k_1 \oplus F_2(y_0) \oplus k_2 \oplus F_3(y_0 \oplus F_1(x_0) \oplus k_1) \oplus k_3 \oplus F_4(y_0 \oplus F_1(x_0) \oplus k_1 \oplus F_2(y_0) \oplus k_2) \oplus k_4,$$

$$y_5 = x_5 \oplus F_5(y_0 \oplus F_1(x_0) \oplus k_1 \oplus F_2(y_0) \oplus k_2 \oplus F_3(y_0 \oplus F_1(x_0) \oplus k_1) \oplus k_3) \oplus k_5.$$

将密文的左半部分 x_5 和右半部分 y_5 异或后可得:

$$x_5 \oplus y_5 = F_5(y_0 \oplus F_1(x_0) \oplus k_1 \oplus F_2(y_0) \oplus k_2 \oplus F_3(y_0 \oplus F_1(x_0) \oplus k_1) \oplus k_3) \oplus k_5 \tag{11}$$

根据公式 (11) 可设函数:

$$G(x,y) = F_5(y \oplus F_1(x) \oplus k_1 \oplus F_2(y) \oplus k_2 \oplus F_3(y \oplus F_1(x) \oplus k_1) \oplus k_3) \oplus k_5 \tag{12}$$

其中, 变量 x 和 y 分别对应明文 x_0 和 y_0, $x,y \in \{0,1\}^{n/2}$ 且 $G(x,y) \in \{0,1\}^{n/2}$. 在公式 (12) 的基础上, 我们可以构建新的 5 轮 Misty L-FK 结构密钥恢复攻击, 具体过程如下.

(1) 选择明文 $(x_0^1, y_0^1 = F_1(x_0^1))$, $(x_0^2, y_0^2 = F_1(x_0^2))$, 并查询其密文. 根据公式 (11)、(12) 分别进行计算, 并对输出进行异或可得:

$$G(x_0^1, y_0^1) \oplus G(x_0^2, y_0^2) = F_5(k_1 \oplus F_2(y_0^1) \oplus k_2 \oplus F_3(k_1) \oplus k_3) \oplus F_5(k_1 \oplus F_2(y_0^2) \oplus k_2 \oplus F_3(k_1) \oplus k_3).$$

(2) 设 $\beta_1 = k_1 \oplus F_2(y_0^1) \oplus k_2 \oplus F_3(k_1) \oplus k_3$, $\beta_2 = k_1 \oplus F_2(y_0^2) \oplus k_2 \oplus F_3(k_1) \oplus k_3$, 则 $\beta_1 \oplus \beta_2 = F_2(y_0^1) \oplus F_2(y_0^2)$, $G(x_0^1, y_0^1) \oplus G(x_0^2, y_0^2) = F_5(\beta_1) \oplus F_5(\beta_1 \oplus F_2(y_0^1) \oplus F_2(y_0^2))$. 由于已知公开函数 F_5 和 F_2, $G(x_0^1, y_0^1) \oplus G(x_0^2, y_0^2)$ 值, y_0^1 和 y_0^2 值, 可通过 Grover 算法求出 β_1 值.

(3) 根据 β_1 值和公式 (12), 可计算出 k_5.

(4) 在计算出 k_5 后, 可使用步骤 (1)–(3) 类似的方法依次恢复出轮密钥 k_4, k_3, k_2 和 k_1.

复杂度分析. 在对 5 轮 Misty L-FK 结构的密钥恢复攻击过程中, 我们仅需选择 2 个明密文对, 且在依次恢复轮密钥 $k_5 - k_1$ 的时间复杂度分别都为 $O(2^{n/4})$. 综上, 我们的攻击总体时间复杂度为 $O(2^{n/4})$, 数据复杂度为 $O(1)$ 且经典存储复杂度可忽略不计.

若在 5 轮 Misty L-FK 结构的基础上再增加 $r-5$ 轮, 则可先穷举轮密钥 $k_6 - k_r$, 再重复以上步骤恢复其他轮密钥, 并用明密文进行验证正确性. 则整体时间复杂度为 $O(2^{n/4+(r-5)n/2})$, 数据复杂度依然仅为 $O(1)$ 且经典存储复杂度可忽略不计.

5.3 对 Misty R-KF 结构的密钥恢复攻击

如图 10 所示的 4 轮 Misty R-KF 结构, 其中 $F_i(i=1,2,3,4)$ 为轮函数, k_i 为轮密钥且 $|k_i| = n/2(i=1,2,3,4)$, (x_0,y_0) 为 4 轮 Misty R-KF 结构的明文输入且 $|(x_0,y_0)| = n$, (x_4,y_4) 作为密文输出.

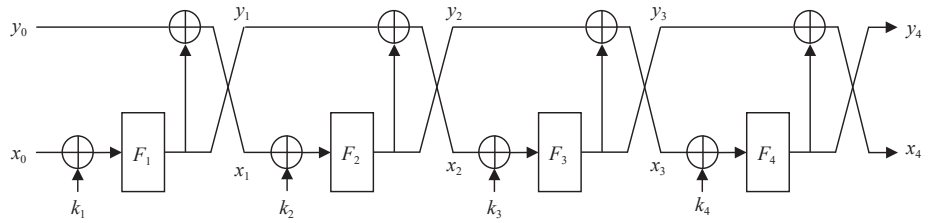


图 10 4 轮 Misty R-KF 结构

根据 Misty R-KF 结构的加密过程, 得到密文 (x_4,y_4), 并将左半部分 x_4 和右半部分 y_4 异或后可得:

$$x_4 \oplus y_4 = F_3(F_1(x_0 \oplus k_1) \oplus F_2(F_1(x_0 \oplus k_1) \oplus y_0 \oplus k_2) \oplus k_3) \tag{13}$$

由公式 (13) 可设函数:

$$G(x,y) = F_3(F_1(x \oplus k_1) \oplus F_2(F_1(x \oplus k_1) \oplus y \oplus k_2) \oplus k_3) \tag{14}$$

其中, 变量 x 和 y 分别对应 x_0 和 y_0, $x,y \in \{0,1\}^{n/2}$ 且 $G(x,y) \in \{0,1\}^{n/2}$. 依据公式 (14), 我们提出以下针对 4 轮 Misty R-KF 结构的密钥恢复过程.

(1) 选择明文 (x_0^1,y_0^1), (x_0^1,y_0^2), 并查询其对应的密文, 根据公式 (13)、(14) 计算出:

$$G(x_0^1,y_0^1)=F_3(F_1(x_0^1\oplus k_1)\oplus F_2(F_1(x_0^1\oplus k_1)\oplus y_0^1\oplus k_2)\oplus k_3),$$

$$G(x_0^1,y_0^2)=F_3(F_1(x_0^1\oplus k_1)\oplus F_2(F_1(x_0^1\oplus k_1)\oplus y_0^2\oplus k_2)\oplus k_3).$$

(2) 设 $\beta_1=F_1(x_0^1\oplus k_1)\oplus F_2(F_1(x_0^1\oplus k_1)\oplus y_0^1\oplus k_2)\oplus k_3$, $\beta_2=F_1(x_0^1\oplus k_1)\oplus F_2(F_1(x_0^1\oplus k_1)\oplus y_0^2\oplus k_2)\oplus k_3$, 则 $G(x_0^1,y_0^1)=F_3(\beta_1)$, $G(x_0^1,y_0^2)=F_3(\beta_2)$, 利用 Grover 算法求出 β_1 和 β_2 值.

(3) 将 β_1 和 β_2 异或后可得 $\beta_1\oplus\beta_2=F_2(F_1(x_0^1\oplus k_1)\oplus y_0^1\oplus k_2)\oplus F_2(F_1(x_0^1\oplus k_1)\oplus y_0^2\oplus k_2)$, 设 $\delta_1=F_1(x_0^1\oplus k_1)\oplus y_0^1\oplus k_2$, $\delta_2=F_1(x_0^1\oplus k_1)\oplus y_0^2\oplus k_2$, 则 $\delta_1\oplus\delta_2=y_0^1\oplus y_0^2$. 可利用 Grover 算法求 $\beta_1\oplus\beta_2=F_2(\delta_1)\oplus F_2(\delta_1\oplus y_0^1\oplus y_0^2)$ 中未知量 δ_1.

(4) 选择明文 (x_0^2,y_0^1), (x_0^2,y_0^2), 并查询其对应的密文, 计算出:

$$G(x_0^2,y_0^1)=F_3(F_1(x_0^2\oplus k_1)\oplus F_2(F_1(x_0^2\oplus k_1)\oplus y_0^1\oplus k_2)\oplus k_3),$$

$$G(x_0^2,y_0^2)=F_3(F_1(x_0^2\oplus k_1)\oplus F_2(F_1(x_0^2\oplus k_1)\oplus y_0^2\oplus k_2)\oplus k_3).$$

(5) 设 $\beta_3=F_1(x_0^2\oplus k_1)\oplus F_2(F_1(x_0^2\oplus k_1)\oplus y_0^1\oplus k_2)\oplus k_3$, $\beta_4=F_1(x_0^2\oplus k_1)\oplus F_2(F_1(x_0^2\oplus k_1)\oplus y_0^2\oplus k_2)\oplus k_3$, 则 $G(x_0^2,y_0^1)=F_3(\beta_3)$, $G(x_0^2,y_0^2)=F_3(\beta_4)$, 利用 Grover 算法求出 β_3 和 β_4 值.

(6) 将 β_3 和 β_4 异或后可得 $\beta_3\oplus\beta_4=F_2(F_1(x_0^2\oplus k_1)\oplus y_0^1\oplus k_2)\oplus F_2(F_1(x_0^2\oplus k_1)\oplus y_0^2\oplus k_2)$, 设 $\delta_3=F_1(x_0^2\oplus k_1)\oplus y_0^1\oplus k_2$, $\delta_4=F_1(x_0^2\oplus k_1)\oplus y_0^2\oplus k_2$, 则 $\delta_3\oplus\delta_4=y_0^1\oplus y_0^2$. 可利用 Grover 算法求 $\beta_3\oplus\beta_4=F_2(\delta_3)\oplus F_2(\delta_3\oplus y_0^1\oplus y_0^2)$ 中未知量 δ_3.

(7) 将得到的 δ_1 和 δ_3 异或后可得 $\delta_1\oplus\delta_2=F_1(x_0^1\oplus k_1)\oplus F_1(x_0^2\oplus k_1)$. 再利用 Grover 算法求出其中的未知量 k_1.

(8) 恢复出轮密钥 k_1 后, 可依次求出轮密钥 k_2, k_3 和 k_4.

复杂度分析. 在对 4 轮 Misty R-KF 结构的密钥恢复攻击过程中, 我们仅需选择 4 个明密文对, 且在步骤 (2)、(3)、 (5)–(8) 中利用 Grover 算法搜索未知量, 每一个未知量的规模为 $2^{n/2}$, 所以每一步的时间复杂度都分别为 $O(2^{n/4})$. 综上, 该密钥恢复攻击的总体时间复杂度为 $O(2^{n/4})$, 数据复杂度为 $O(1)$ 且经典存储复杂度可忽略不计.

若在 4 轮 Misty R-KF 结构上再增加 $r-4$ 轮, 则可先穷举轮密钥 k_5-k_r, 再重复以上步骤恢复其他轮密钥, 并用明密文验证正确性. 则整体时间复杂度为 $O(2^{n/4+(r-4)n/2})$, 数据复杂度依然仅为 $O(1)$ 且经典存储复杂度可忽略不计.

5.4 对 Misty R-FK 结构的密钥恢复攻击

如图 11 所示的 5 轮 Misty R-FK 结构, 其中 F_i ($i=1,2,3,4,5$) 为轮函数, k_i 为轮密钥且 $|k_i|=n/2$ ($i=1,2,3,4$), (x_0,y_0) 为 5 轮 Misty R-FK 结构的明文输入且 $|(x_0,y_0)|=n$, (x_5,y_5) 作为密文输出.

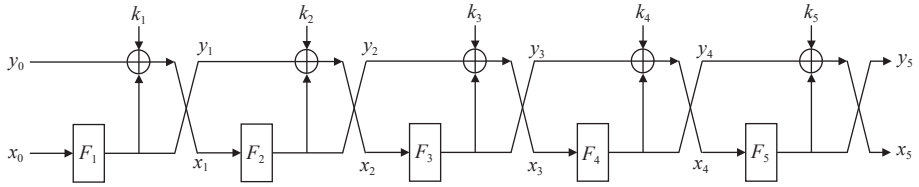


图 11 5 轮 Misty R-FK 结构

根据 Misty R-KF 结构的加密过程, 得到密文 (x_5,y_5), 并将左半部分 x_5 和右半部分 y_5 异或后可得:

$$x_5\oplus y_5=F_4(x_3)\oplus k_5 \tag{15}$$

对右半部分密文 y_5 经过函数 F_5 的逆可以求得:

$$x_4=F_5^{-1}(y_5)=y_3\oplus F_4(x_3)\oplus k_4 \tag{16}$$

将公式 (15)、(16) 异或后可得:

$$F_5^{-1}(y_5)\oplus x_5\oplus y_5=y_3\oplus k_5\oplus k_4 \tag{17}$$

其中, $y_3=F_3(F_1(x_0)\oplus F_2(F_1(x_0)\oplus y_0\oplus k_1)\oplus k_2)$. 可设函数:

$$G(x,y)=F_3(F_1(x)\oplus F_2(F_1(x)\oplus y\oplus k_1)\oplus k_2)\oplus k_4\oplus k_5 \tag{18}$$

其中, 变量 x 和 y 分别对应 x_0 和 y_0, $x,y\in\{0,1\}^{n/2}$ 且 $G(x,y)\in\{0,1\}^{n/2}$. 依据公式 (18), 我们提出以下针对 5 轮 Misty R-FK 结构的密钥恢复过程.

(1) 选择明文 $(x_0^1,y_0^1=F_1(x_0^1))$ 和 $(x_0^2,y_0^2=F_1(x_0^2))$, 并查询其对应的密文. 根据公式 (15)–(18), 可计算求得:

$$G(x_0^1,y_0^1)=F_3(F_1(x_0^1)\oplus F_2(F_1(x_0^1)\oplus y_0^1\oplus k_1)\oplus k_2)\oplus k_4\oplus k_5,$$

$$G(x_0^2,y_0^2)=F_3(F_1(x_0^2)\oplus F_2(F_1(x_0^2)\oplus y_0^2\oplus k_1)\oplus k_2)\oplus k_4\oplus k_5.$$

(2) 将 $G(x_0^1,y_0^1)$ 和 $G(x_0^2,y_0^2)$ 异或后可得:

$$G(x_0^1,y_0^1)\oplus G(x_0^2,y_0^2)=F_3(F_1(x_0^1)\oplus F_2(k_1)\oplus k_2)\oplus F_3(F_1(x_0^2)\oplus F_2(k_1)\oplus k_2).$$

(3) 设 $\beta_1=F_1(x_0^1)\oplus F_2(k_1)\oplus k_2$, $\beta_2=F_1(x_0^2)\oplus F_2(k_1)\oplus k_2$, 则 $\beta_1\oplus\beta_2=F_1(x_0^1)\oplus F_1(x_0^2)$, $G(x_0^1,y_0^1)\oplus G(x_0^2,y_0^2)=F_3(\beta_1)\oplus F_3(\beta_1\oplus F_1(x_0^1)\oplus F_1(x_0^2))$. 由于已知公开函数 F_3 和 F_1, $G(x_0^1,y_0^1)$, $G(x_0^2,y_0^2)$, x_0^1 和 x_0^2 值, 可利用 Grover 算法搜索出未知量 β_1.

(4) 选择明文 (x_0^1,y_0^3) ($y_0^3\neq F_1(x_0^1)$), 并查询器对应的密文. 根据公式 (15)–(18), 可计算求得:

$$G(x_0^1,y_0^3)=F_3(F_1(x_0^1)\oplus F_2(F_1(x_0^1)\oplus y_0^3\oplus k_1)\oplus k_2)\oplus k_4\oplus k_5.$$

(5) 将 $G(x_0^1,y_0^1)$ 和 $G(x_0^1,y_0^3)$ 异或后可得:

$$G(x_0^1,y_0^1)\oplus G(x_0^1,y_0^3)=F_3(\beta_1)\oplus F_3(F_1(x_0^1)\oplus F_2(F_1(x_0^1)\oplus y_0^3\oplus k_1)\oplus k_2).$$

同样地, 可用 Grover 算法搜索出未知量 $F_1(x_0^1)\oplus\ F_2(F_1(x_0^1)\oplus y_0^3\oplus k_1)\oplus k_2$ 值.

(6) 将 β_1 和 $F_1(x_0^1)\oplus F_2(F_1(x_0^1)\oplus y_0^3\oplus k_1)\oplus k_2$ 异或后可得 $F_2(k_1)\oplus F_2(F_1(x_0^1)\oplus y_0^3\oplus k_1)$, 依然可用 Grover 算法搜索出未知量 k_1.

(7) 搜索出 k_1 后, 可依次计算出剩余轮密钥 k_2-k_5.

复杂度分析. 在对 5 轮 Misty R-FK 结构的密钥恢复攻击过程中, 我们仅需选择 3 个明密文对即可恢复密钥, 且在步骤 (3)、(5)、(6) 中利用 Grover 算法搜索未知量, 每一个未知量的规模为 $2^{n/2}$, 所以每一步的时间复杂度都分别为 $O(2^{n/4})$. 综上, 该密钥恢复攻击的总体时间复杂度为 $O(2^{n/4})$, 数据复杂度为 $O(1)$ 且经典存储复杂度可忽略不计.

若在 5 轮 Misty R-FK 结构上再增加 $r-5$ 轮, 则可先穷举轮密钥 k_6-k_r, 再重复以上步骤恢复其他轮密钥, 并用明密文进行验证正确性. 则整体时间复杂度为 $O(2^{n/4+(r-5)n/2})$, 数据复杂度依然仅为 $O(1)$ 且经典存储复杂度可忽略不计.

6 对 Type-1 型广义 Feistel 结构的密钥恢复攻击

如图 12 所示的 $3d-3$ 轮 Type-1 型广义 Feistel-FK 结构, 分组长度为 n 比特, 其中每个分支与轮密钥 k_i ($i=1,2,\ldots,3d-3$) 的比特长度为 n/d, F_i 为轮函数, x_j^i 的上标 i 表示第 i ($i=0,1,\ldots,3d-3$) 轮, 下标 j 表示第 j ($j=0,1,\ldots,d-1$) 个分支. 明文 $(x_0^0,x_1^0,\ldots x_{d-1}^0)$ 作为其输入, 经过 $3d-3$ 轮加密后得到密文 $(x_0^{3d-3},x_1^{3d-3},\ldots x_{d-1}^{3d-3})$.

根据 Type-1 型广义 Feistel-FK 结构加密过程, 我们选择密文中的 x_1^{3d-3} 和 x_2^{3d-3} 部分, 由于存在 $x_0^i=x_{d-1}^{i+1}=x_{d-2}^{i+2}=\ldots=x_1^{i+d-1}$ 性质, 有:

$$x_1^{3d-3}=x_{d-1}^{2d-1}=F_{2d-2}(x_{d-1}^{2d-2})\oplus x_{d-2}^d\oplus k_{2d-2},x_2^{3d-3}=F_{2d-1}(F_{2d-2}(x_{d-1}^{2d-2})\oplus x_{d-2}^d\oplus k_{2d-2})\oplus x_{d-1}^d\oplus k_{2d-1}\tag{19}$$

我们发现 x_2^{3d-3} 中函数 F_{2d-1} 的输入正好是 x_1^{3d-3} 值, 则可利用公开函数 F_{2d-1} 计算 $F_{2d-1}(x_1^{3d-3})$, 并与 x_2^{3d-3} 异或后可得:

$$F_{2d-1}(x_1^{3d-3})\oplus x_2^{3d-3}=x_{d-1}^d\oplus k_{2d-1}\tag{20}$$

由于 $x_0^i=x_{d-1}^{i+1}=x_{d-2}^{i+2}=\ldots=x_1^{i+d-1}$, 则:

$$F_{2d-1}(x_1^{3d-3})\oplus x_2^{3d-3}=x_0^{d-1}\oplus k_{2d-1}\tag{21}$$

由于 $x_0^{d-1}=F_{d-1}(F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-2}^0\oplus k_{d-2})\oplus x_{d-1}^0\oplus k_{d-1}$, 则:

$$F_{2d-1}(x_1^{3d-3})\oplus x_2^{3d-3}=F_{d-1}(F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-2}^0\oplus k_{d-2})\oplus x_{d-1}^0\oplus k_{d-1}\oplus k_{2d-1} \tag{22}$$

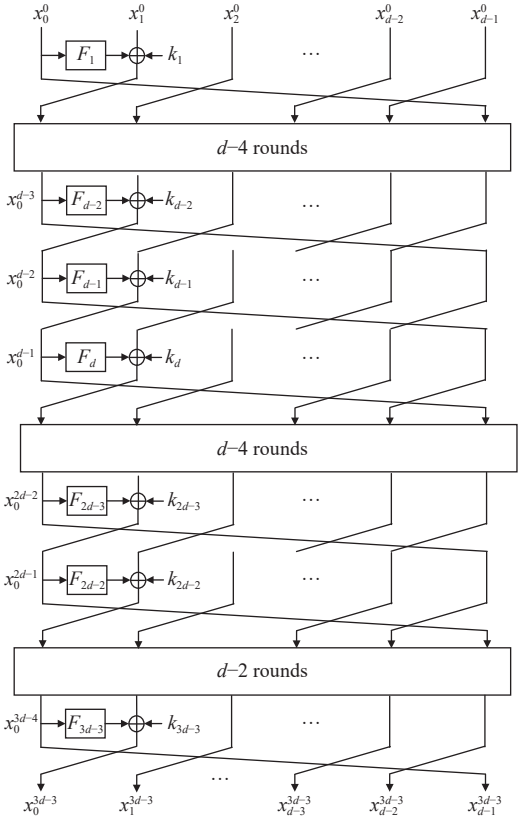


图 12 $3d-3$ 轮 Type-1 型广义 Feistel-FK 结构

可根据公式 (22) 设函数:

$$G(P)=F_{d-1}(F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-2}^0\oplus k_{d-2})\oplus x_{d-1}^0\oplus k_{d-1}\oplus k_{2d-1} \tag{23}$$

其中 $P=(x_0^0,x_1^0,\ldots,x_{d-3}^0,x_{d-2}^0,x_{d-1}^0)$, $P\in\{0,1\}^n$ 且 $G(P)\in\{0,1\}^{n/d}$. 依据公式 (19)–(23), 我们提出以下针对 $3d-3$ 轮 Type-1 型广义 Feistel-FK 结构的密钥恢复过程:

(1) 选择明文 $P=(x_0^0,x_1^0,\ldots,x_{d-3}^0,x_{d-2}^0,x_{d-1}^0)$ 和 $P'=(x_0^0,x_1^0,\ldots,x_{d-3}^0,(x_{d-2}^0)',x_{d-1}^0)$ ($x_{d-2}^0\neq(x_{d-2}^0)'$), 查询其对应的密文. 根据公式 (19)–(23) 可求得:

$$\begin{aligned}G(P)\oplus G(P')=&F_{d-1}(F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-2}^0\oplus k_{d-2})\\&\oplus F_{d-1}(F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-2}^0)'\oplus k_{d-2}).\end{aligned}$$

(2) 设 $\beta_1=F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-2}^0\oplus k_{d-2}$, $\beta_2=F_{d-2}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-2}^0)'\oplus k_{d-2}$, 则 $\beta_1\oplus\beta_2=x_{d-2}^0\oplus(x_{d-2}^0)'$, $G(P)\oplus G(P')=F_{d-1}(\beta_1)\oplus F_{d-1}(\beta_1\oplus x_{d-2}^0\oplus(x_{d-2}^0)')$, 可利用 Grover 算法求出 β_1 值.

(3) 选择明文 $P^*=(x_0^0,x_1^0,\ldots,(x_{d-3}^0)^*,x_{d-2}^0,x_{d-1}^0)$ 和 $P^{*\prime}=(x_0^0,x_1^0,\ldots,(x_{d-3}^0)^*,(x_{d-2}^0)',x_{d-1}^0)$, 查询其对应的密文. 根据公式 (19)–(23) 可求得:

$$\begin{aligned}G(P^*)\oplus G(P^{*\prime})=&F_{d-1}(F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-3}^0)^*\oplus k_{d-3})\oplus x_{d-2}^0\oplus k_{d-2})\\&\oplus F_{d-1}(F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-3}^0)^*\oplus k_{d-3})\oplus(x_{d-2}^0)'\oplus k_{d-2}).\end{aligned}$$

(4) 设 $\beta_3=F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-3}^0)^*\oplus k_{d-3})\oplus x_{d-2}^0\oplus k_{d-2}$, $\beta_4=F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus(x_{d-3}^0)^*\oplus k_{d-3})\oplus(x_{d-2}^0)'\oplus k_{d-2}$, 则 $\beta_3\oplus\beta_4=x_{d-2}^0\oplus(x_{d-2}^0)'$, $G(P^*)\oplus G(P^{*\prime})=F_{d-1}(\beta_3)\oplus F_{d-1}(\beta_3\oplus x_{d-2}^0\oplus(x_{d-2}^0)')$, 可利用 Grover 算法求出 β_3 值.

(5) 已知β_1和β_3值, 异或后可得:

$$\begin{aligned}\beta_1\oplus\beta_3 =&F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-3}^0\oplus k_{d-3})\\&\oplus F_{d-2}(F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus (x_{d-3}^0)^*\oplus k_{d-3}).\end{aligned}$$

(6) 设$\delta_1 = F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus x_{d-3}^0\oplus k_{d-3}$, $\delta_2 = F_{d-3}(\ldots F_1(x_0^0)\oplus x_1^0\oplus k_1\ldots)\oplus (x_{d-3}^0)^*\oplus k_{d-3}$, 则$\delta_1\oplus\delta_2 = x_{d-3}^0\oplus(x_{d-3}^0)^*$, $\beta_1\oplus\beta_3 = F_{d-2}(\delta_1)\oplus F_{d-2}(\delta_1\oplus x_{d-3}^0\oplus(x_{d-3}^0)^*)$, 可利用 Grover 算法求出$\delta_1$值.

(7) 已知δ_1, β_1和x_{d-2}^0值, 可计算出轮密钥$k_{d-2} = \beta_1\oplus F_{d-2}(\delta_1)\oplus x_{d-2}^0$.

(8) 可重复以上类似步骤, 依次恢复出其他剩余轮密钥.

复杂度分析. 在对$3d-3$轮 Type-1 型广义 Feistel-FK 结构的密钥恢复攻击过程中, 我们仅需选择 4 个明密文对即可恢复轮密钥k_{d-2}, 且在步骤 (2)、(4)、 (6) 中利用 Grover 算法搜索未知量, 每一个未知量的规模为$2^{n/d}$, 所以每一步的时间复杂度都分别为$O(2^{n/2d})$. 对于恢复其他轮密钥的过程所需时间和明文数量, 我们相信与恢复轮密钥k_{d-2}所需时间和明文数量基本保持一致, 甚至可能更低, 例如, 可以重复利用明文. 综上, 该密钥恢复攻击的总体时间复杂度为$O(2^{n/2d})$, 数据复杂度为$O(1)$且经典存储复杂度可忽略不计. 需要注意的是, Zou 等人[21]同样提出了在 Q1 模型下对 Type-1 型广义 Feistel-FK 结构的量子密钥恢复攻击, 其复杂度详见表 1. 然而, 由于他们使用了d^2-d+1轮的量子选择密文区分器, 他们的攻击属于选择密文攻击, 而我们的攻击仅需要加密 Oracle, 即选择明文攻击. 当分支数$d=3$时, 我们的攻击在复杂度乘积方面与 Zou 等人的攻击保持一致, 并且, 我们的攻击仅可以将数据复杂度和存储复杂度从$O(2^{n/2d})$降低到$O(1)$. 不过, 当$d>3$时, 我们的攻击相比于 Zou 等人的攻击将不具备明显优势.

7 对类 SMS4 广义 Feistel 结构的密钥恢复攻击

如图 13 所示的$2d-1$轮类 SMS4 广义 Feistel-FK 结构, 其中每个分支与轮密钥k_i ($i=1,2,\ldots,2d-1$)的比特长度为n/d, F_i为轮函数, x_j^i的上标i表示第i ($i=0,1,\ldots,2d-1$)轮, 下标j表示第j ($j=0,1,\ldots,d-1$)个分支. 明文$(x_0^0,x_1^0,\ldots x_{d-1}^0)$作为其输入, 经过$2d-1$轮加密后得到密文$(x_0^{2d-1},x_1^{2d-1},\ldots x_{d-1}^{2d-1})$. 假设$d$为偶数.

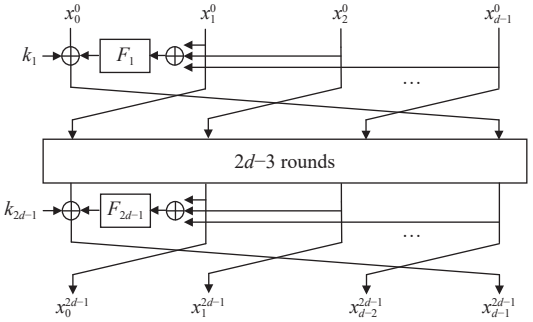


图 13 $2d-1$轮类 SMS4 广义 Feistel-FK 结构

根据$2d-1$轮类 SMS4 广义 Feistel-FK 结构的加密过程可知:

$$x_0^{2d-1} = x_{d-1}^0\oplus F_d \tag{24}$$

其中,

$$\begin{cases}F_1 = F_1(\mathop{\oplus}\limits_{j=1}^{d-1} x_j^0)\oplus k\\ F_2 = F_2(x_0^0\oplus\mathop{\oplus}\limits_{j=2}^{d-1} x_j^0\oplus F_1)\oplus k_2\\ \cdots\\ F_d = F_d(\mathop{\oplus}\limits_{j=1}^{d-2} x_j^0\oplus\mathop{\oplus}\limits_{i=1}^{d-1} F_i)\oplus k_d\end{cases} \tag{25}$$

根据公式 (24)、(25) 可设函数:

$$G(P)=x_{d-1}^{0}\oplus F_d(\bigoplus_{j=1}^{d-2}x_j^0\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d \tag{26}$$

其中 $P=(x_0^0,x_1^0,\ldots,x_{d-3}^0,x_{d-2}^0,x_{d-1}^0)$, $P\in\{0,1\}^n$ 且 $G(P)\in\{0,1\}^{n/d}$. 依据公式 (24)–(26), 我们提出以下针对 $2d-1$ 轮类 SMS4 广义 Feistel-FK 结构的密钥恢复过程.

(1) 选择明文 $P=(c,\ldots,c,\alpha)$, $P'=(c',\ldots,c',\alpha)$ ($c\neq c'$), 查询其对应的密文. 并计算出 $G(P)=\alpha\oplus F_d(c\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d$, $G(P')=\alpha\oplus F_d(c'\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d$.

(2) 设 $\beta_1=c\oplus\bigoplus_{i=1}^{d-1}F_i$, $\beta_2=c'\oplus\bigoplus_{i=1}^{d-1}F_i$, 则 $\beta_1\oplus\beta_2=c\oplus c'$, $G(P)\oplus G(P')=F_d(\beta_1)\oplus F_d(\beta_1\oplus c\oplus c')$, 可利用 Grover 算法求出未知量 β_1.

(3) 已知 β_1 值, 可根据公式 (26) 求出轮密钥 k_d.

(4) 其他轮密钥可通过以上类似的方式依次求出来.

复杂度分析. 在对 $2d-1$ 轮类 SMS4 广义 Feistel-FK 结构的密钥恢复攻击过程中, 我们仅需选择 2 个明密文对即可恢复轮密钥 k_d, 且在步骤 (2) 中利用 Grover 算法搜索未知量, 时间复杂度为 $O(2^{n/2d})$. 对于恢复其他轮密钥的过程所需时间和明文数量, 我们相信与恢复轮密钥 k_d 所需时间和明文数量基本保持一致. 综上, 该密钥恢复攻击的总体时间复杂度为 $O(2^{n/2d})$, 数据复杂度为 $O(1)$ 且经典存储复杂度可忽略不计. Cui 等人[6]也提出了对类 SMS4 广义 Feistel-FK 结构的量子密钥恢复攻击, 具体复杂度可见表 1. 但是, 他们的攻击属于 Q2 模型, 对攻击者的能力要求较高. 此外, 当攻击轮数都为 $r=r_0$ 时, 我们的攻击在复杂度乘积方面相比于他们的攻击可从 $O(2n^2/(r_0-1)\cdot 2^{2n/(r_0-1)})$ 降低为 $O(n2^{n/(r_0+1)})$. 但是, 当分支数 d 和攻击轮数相同时, 我们的攻击在复杂度乘积方面将提高 $O(2^{3n/2d})$ 因子.

8 对类 MARS 广义 Feistel 结构的密钥恢复攻击

如图 14 所示的 $2d-1$ 轮类 MARS 广义 Feistel-FK 结构, 其中每个分支与轮密钥 k_i ($i=1,2,\ldots,2d-1$) 的比特长度为 n/d, F_i 为轮函数, x_j^i 的上标 i 表示第 i ($i=0,1,\ldots,2d-1$) 轮, 下标 j 表示第 j ($j=0,1,\ldots,d-1$) 个分支. 明文 $(x_0^0,x_1^0,\ldots x_{d-1}^0)$ 作为其输入, 经过 $2d-1$ 轮加密后得到密文 $(x_0^{2d-1},x_1^{2d-1},\ldots x_{d-1}^{2d-1})$. 假设 d 为偶数.

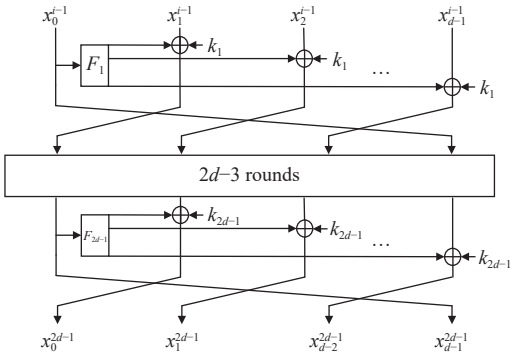


图 14 $2d-1$ 轮类 MARS 广义 Feistel-FK 结构

根据 $2d-1$ 轮类 MARS 广义 Feistel-FK 结构的加密过程可知:

$$\begin{cases} x_0^{2d-1}=x_{d-1}^0\oplus F_1\oplus k_1\oplus\ldots\oplus F_{d-1}\oplus k_{d-1}\oplus\ldots\oplus F_{2d-1}\oplus k_{2d-1}\\ x_1^{2d-1}=x_0^0\oplus F_2\oplus k_2\oplus\ldots\oplus F_d\oplus k_d\oplus\ldots\oplus F_{2d-1}\oplus k_{2d-1}\\ \cdots\\ x_{d-1}^{2d-1}=x_{d-2}^0\oplus F_1\oplus k_1\oplus\ldots\oplus F_d\oplus k_d\oplus\ldots\oplus F_{2d-2}\oplus k_{2d-2}\end{cases} \tag{27}$$

由于 d 是偶数, 则:

$$x_1^{2d-1}\oplus\ldots\oplus x_{d-1}^{2d-1}=x_0^0\oplus\ldots\oplus x_{d-2}^0\oplus F_d\oplus k_d \tag{28}$$

其中, $F_d=F_d(x_{d-1}^0\oplus\bigoplus_{i=1}^{d-1}F_i)$. 由于 $\bigoplus_{i=1}^{d-1}F_i$ 由 $x_0^0,\ldots,x_{d-2}^0$ 计算决定, 不受 x_{d-1}^0 影响, 可设函数:

$$G(P)=x_0^0\oplus\ldots\oplus x_{d-2}^0\oplus F_d(x_{d-1}^0\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d \tag{29}$$

其中, $P=(x_0^0,x_1^0,\ldots,x_{d-3}^0,x_{d-2}^0,x_{d-1}^0)$, $P\in\{0,1\}^n$ 且 $G(P)\in\{0,1\}^{n/d}$. 依据公式 (27)–(29), 我们提出以下针对 $2d-1$ 轮类 MARS 广义 Feistel-FK 结构的密钥恢复过程.

(1) 选择明文 $P=(x_0^0,\ldots,x_{d-2}^0,x_{d-1}^0)$ 和 $P'=(x_0^0,\ldots,x_{d-2}^0,(x_{d-1}^0)')$ ($x_{d-1}^0\neq(x_{d-1}^0)'$), 查询其对应的密文. 并计算出 $G(P)=x_0^0\oplus\ldots\oplus x_{d-2}^0\oplus F_d(x_{d-1}^0\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d$, $G(P')=x_0^0\oplus\ldots\oplus x_{d-2}^0\oplus F_d((x_{d-1}^0)'\oplus\bigoplus_{i=1}^{d-1}F_i)\oplus k_d$.

(2) 设 $\beta_1=x_{d-1}^0\oplus\bigoplus_{i=1}^{d-1}F_i$, $\beta_2=(x_{d-1}^0)'\oplus\bigoplus_{i=1}^{d-1}F_i$, 则 $\beta_1\oplus\beta_2=x_{d-1}^0\oplus(x_{d-1}^0)'$, $G(P)\oplus G(P')=F_d(\beta_1)\oplus F_d(\beta_1\oplus x_{d-1}^0\oplus(x_{d-1}^0)')$, 可利用 Grover 算法求出未知量 β_1 值.

(3) 已知 β_1 值, 可根据公式 (29) 求出轮密钥 k_d.

(4) 其他轮密钥可通过以上类似的方式依次求出来.

复杂度分析. 在对 $2d-1$ 轮类 MARS 广义 Feistel-FK 结构的密钥恢复攻击过程中, 我们仅需选择 2 个明密文对即可恢复轮密钥 k_d, 且在步骤 (2) 中利用 Grover 算法搜索未知量, 时间复杂度为 $O(2^{n/2d})$. 对于恢复其他轮密钥的过程所需时间和明文数量, 我们相信与恢复轮密钥 k_d 所需时间和明文数量基本保持一致. 综上, 该密钥恢复攻击的总体时间复杂度为 $O(2^{n/2d})$, 数据复杂度为 $O(1)$ 且经典存储复杂度可忽略不计. 类似于类 SMS4 广义 Feistel-FK 结构, Cui 等人[6]同样提出了对类 MARS 广义 Feistel-FK 结构的量子密钥恢复攻击, 具体复杂度可见表 1. 同样地, 他们的攻击属于 Q2 模型, 对攻击者的能力要求较高. 此外, 当攻击轮数都为 $r=r_0$ 时, 我们的攻击在复杂度乘积方面相比于他们的攻击可从 $O(2n^2/(r_0-1)\cdot 2^{2n/(r_0-1)})$ 降低为 $O(n2^{n/(r_0+1)})$. 但是, 当分支数 d 和攻击轮数相同时, 我们的攻击在复杂度乘积方面会高于他们的攻击.

9 总 结

近年来, 针对分组密码结构的量子攻击研究, 主要是在 Q2 模型下提出基于 Simon 算法的量子区分器, 并利用 Grover Meets Simon 方法拓展更多轮数. 但是对于更有实际意义的 Q1 模型, 分析分组密码结构的一些缺陷, 再辅以量子算法来加速计算, 从而实现密钥恢复攻击的研究相对较少. 本文提出的低数据密钥恢复攻击方法可以有效评估分组密码结构在 Q1 模型的安全性. 针对 3 轮 Lai-Massey 结构, 相比于其他量子攻击, 本文的方法不仅仅需 $O(1)$ 数据, 而且属于 Q1 模型, 在复杂度乘积 (时间×数据×经典存储×量子比特) 评估上降低了 $n2^{n/4}$ 因子. 针对 6 轮 Misty 结构, 本文的方法依然保留着低数据复杂度的优势, 尤其是 6 轮 Misty L/R-FK 结构, 在复杂度乘积评估上降低了 $2^{n/2}$ 因子. 对于 9 轮 3 分支 Type-1 型广义 Feistel 结构, 与其他量子攻击在复杂度乘积评估上保持一致, 本文的方法依然保留着低数据复杂度的优势且属于选择明文攻击. 此外, 本文也给出了针对类 SMS4 广义 Feistel 结构和类 MARS 广义 Feistel 结构的低数据密钥恢复攻击方法.

References:

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

[2] 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]

[3] Lai X J, Massey JL. A proposal for a new block encryption standard. In: Proc. of Workshop on the Theory and Application of Cryptographic Techniques. Aarhus: Springer, 1990. 389–404. [doi: 10.1007/3-540-46877-3_35]

[4] Matsui M. New block encryption algorithm MISTY. In: Proc. of the 4th Int'l Workshop on Fast Software Encryption. Haifa: 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. New York: Springer, 1990. 461–480. [doi: 10.1007/0-387-34805-0_42]

[6] 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]

[7] 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]

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

[9] Kuwakado H, Morii M. Security on the quantum-type Even-Mansour cipher. In: Proc. of the 2012 Int'l Symp. on Information Theory and Its Applications. Honolulu: IEEE, 2012. 312–316.

[10] Kaplan M, Leurent G, Leverrier A, Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: Proc. of the 36th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2016. 207–237. [doi: 10.1007/978-3-662-53008-5_8]

[11] Leander G, May A. Grover meets Simon-quantumly attacking the FX-construction. In: Proc. of the 23rd Int'l Conf. on the Theory and Applications of Cryptology and Information Security. Hong Kong: Springer, 2017. 161–178. [doi: 10.1007/978-3-319-70697-9_6]

[12] 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]

[13] 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]

[14] 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]

[15] Zhang ZY, Wu WL, Sui H, Wang BL. Quantum attacks on Type-3 generalized Feistel scheme and unbalanced Feistel scheme with expanding functions. Chinese Journal of Electronics, 2023, 32(2): 209–216. [doi: 10.23919/cje.2021.00.294]

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

[17] Hosoyamada A, Sasaki Y. Quantum Demiric-Selcuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In: Proc. of the 11th Int'l Conf. on Security and Cryptography for Networks. Amalfi: Springer, 2018. 386–403. [doi: 10.1007/978-3-319-98113-0_21]

[18] Guo J, Jean J, Nikoli Nikolić I, Sasaki Y. Extended meet-in-the-middle attacks on some Feistel constructions. Designs, Codes and Cryptography, 2016, 80(3): 587–618. [doi: 10.1007/s10623-015-0120-4]

[19] Daiza T, Yoneyama K. Quantum key recovery attacks on 3-Round Feistel-2 structure without quantum encryption oracles. In: Proc. of the 17th Int'l Workshop on Security. Tokyo: Springer, 2022. 128–144. [doi: 10.1007/978-3-031-15255-9_7]

[20] Mao SP, Guo TT, Wang P, Hu L. Quantum attacks on Lai-Massey structure. In: Proc. of the 13th Int'l Workshop. Springer, 2022. 205–229. [doi: 10.1007/978-3-031-17234-2_11]

[21] 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 with English abstract). http://www.jos.org.cn/1000-9825/6636.htm [doi: 10.13328/j.cnki.jos.006636]

[22] Vaudenay S. On the Lai-Massey scheme. In: Proc. of Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 1999. 8–19. [doi: 10.1007/978-3-540-48000-6_2]

[23] Luo YY, Lai XJ, Hu J. The pseudorandomness of many-round Lai-Massey scheme. Journal of Information Science and Engineering, 2015, 31(1): 1085–1096]

[24] 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]

[25] Gouget A, Patarin J, Toulemonde A. (Quantum) Cryptanalysis of Misty schemes. In: Proc. of the 23rd Int'l Conf. on Information Security and Cryptology. Seoul: Springer, 2020. 43–57. [doi: 10.1007/978-3-030-68890-5_3]

[26] Adams C, Gilchrist J. The CAST-256 encryption algorithm. RFC 2612, 1999. [doi: 10.17487/RFC2612]

[27] Deng YH, Jin CH, Li RJ. Meet in the middle attack on Type-1 Feistel construction. In: Proc. of the 13th Int'l Conf. on Information Security and Cryptology. Xi'an: Springer, 2018. 427–444. [doi: 10.1007/978-3-319-75160-3_25]

[28] Ni BY, Ito G, Dong XY, Iwata T. Quantum attacks against Type-1 generalized Feistel ciphers and applications to CAST-256. In: Proc. of the 20th Int'l Conf. on Cryptology in India. Hyderabad: Springer, 2019. 433–455. [doi: 10.1007/978-3-030-35423-7_22]

[29] Diffie W, Ledin G. SMS4 encryption algorithm for wireless networks. IACR Cryptology ePrint Archive, 2008, 2008: 329.

[30] You QD, Qian X, Zhou X, Yuan Y, Wu ZY. Research on quantum cryptanalysis on SMS4-like structure and NBC algorithm. Journal of

Cryptologic Research, 2020, 7(6): 864–874. (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000412]

[31] Cid C, Hosoyamada A, Liu YW, Sim SM. Quantum cryptanalysis on contracting Feistel structures and observation on related-key settings. In: Proc. of the 21st Int'l Conf. on Cryptology in India. Bangalore: Springer, 2020. 373–394. [doi: 10.1007/978-3-030-65277-7_17]

[32] Moriai S, Vaudenay S. On the pseudorandomness of top-level schemes of block ciphers. In: Proc. of the 6th Int'l Conf. on the Theory and Application of Cryptology and Information Security. Kyoto: Springer, 2000. 289–302. [doi: 10.1007/3-540-44448-3_22]

[33] Brassard G, Hoyer P, Mosca M, Tapp A. Quantum amplitude amplification and estimation. arXiv:quant-ph/0005055, 2000.

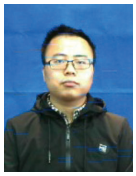
[34] Brassard G, HØyer P, Tapp A. Quantum cryptanalysis of hash and claw-free functions. In: Proc. of the 3rd Latin American Symp. on Theoretical Informatics. Campinas: Springer, 1998. 163–169. [doi: 10.1007/BFb0054319]

附中文参考文献:

[21] 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 [doi: 10.13328/j.cnki.jos.006636]

[24] 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]

[30] 尤启迪, 钱新, 周旋, 袁野, 吴兆阳. SMS4-like 结构以及 NBC 算法的量子算法攻击研究. 密码学报, 2020, 7(6): 864–874. [doi: 10.13868/j.cnki.jcr.000412]



许垠松(1996－), 男, 博士生, CCF 学生会员, 主要研究领域为对称密码的量子安全性分析.

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.

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

袁征(1968－), 女, 博士, 教授, 博士生导师, 主要研究领域为密码算法的设计与分析.