软件学报 ISSN 1000-9825, CODEN RUXUEW
[doi: 10.13328/j.cnki.jos.007448] [CSTR: 32375.14.jos.007448]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

三类非平衡广义 Feistel 结构的量子中间相遇攻击*

杜小妮[1,2], 吴家辉[1], 徐 莹[1], 孙 瑞[1]

[1](西北师范大学 数学与统计学院, 甘肃 兰州 730070)
[2](西北师范大学 密码技术与数据分析重点实验室, 甘肃 兰州 730070)
通信作者: 杜小妮, E-mail: 2023221866@nwnu.edu.cn

摘 要: 研究 3 类非平衡广义 Feistel 结构的中间相遇攻击, 并在 Q1 模型下对这 3 类结构进行量子中间相遇攻击. 首先, 采用多重集和差分枚举技术对 3 分支 Type-III 型广义 Feistel 结构构建 4 轮中间相遇区分器, 分别向前向后扩展 1 轮进行 6 轮中间相遇攻击, 并利用 Grover 算法和量子爪搜索算法对该结构进行 6 轮量子密钥恢复攻击, 该攻击所需的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询, 其中ℓ为广义 Feistel 结构的分支长度. 其次, 对 3 分支 Type-I 型广义 Feistel 结构的 9 轮区分器分别向前向后扩展 1 轮进行 11 轮中间相遇攻击及量子密钥恢复攻击, 相应的时间复杂度分别为 $O(2^{2\ell})$ 次 11 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 最后, 以 3-cell 型广义 Feistel 结构为例探讨了 n-cell 型广义 Feistel 结构的量子中间相遇过程, 对 n-cell 型广义 Feistel 结构构建 $2n$ 轮中间相遇区分器, 并进行 $2(n+1)$ 轮中间相遇攻击及量子密钥恢复攻击, 且时间复杂度分别为 $O(2^{2\ell})$ 次 $2(n+1)$ 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 结果表明, 相比于经典环境, Q1 模型下消耗的时间复杂度更低.

关键词: 广义 Feistel 结构; 量子中间相遇攻击; Q1 模型; 量子爪搜索算法; Grover 算法
中图法分类号: TP309

中文引用格式: 杜小妮, 吴家辉, 徐莹, 孙瑞. 三类非平衡广义Feistel结构的量子中间相遇攻击. 软件学报. http://www.jos.org.cn/1000-9825/7448.htm

英文引用格式: Du XN, Wu JH, Xu Y, Sun R. Quantum Meet-in-the-middle Attacks on Three Types of Unbalanced Generalized Feistel Structures. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7448.htm

Quantum Meet-in-the-middle Attacks on Three Types of Unbalanced Generalized Feistel Structures

DU Xiao-Ni[1,2], WU Jia-Hui[1], XU Ying[1], SUN Rui[1]

[1](College of Mathematics and Statistic, Northwest Normal University, Lanzhou 730070, China)
[2](Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou 730070, China)

Abstract: This study investigates meet-in-the-middle attacks on three types of unbalanced generalized Feistel structures and conducts quantum meet-in-the-middle attacks in Q1 model. First, for the 3-branch Type-III generalized Feistel structure, a 4-round meet-in-the-middle distinguisher is constructed using multiset and differential enumeration techniques. By expanding one round forward and one round backward, a 6-round meet-in-the-middle attack is conducted. With the help of Grover's algorithm and the quantum claw finding algorithm, a 6-round quantum key recovery attack is performed, requiring $O(2^{3\ell/2}\cdot\ell)$ quantum queries, where ℓ is the branch length of the generalized Feistel structure. Then, for the 3-branch Type-I structure, a 9-round distinguisher is similarly extended by one round in both directions to conduct an 11-round meet-in-the-middle attack and a quantum key recovery attack with time complexities of $O(2^{2\ell})$ 11-round encryptions and $O(2^{3\ell/2}\cdot\ell)$ quantum queries. Finally, taking the 3-cell generalized Feistel structure as a representative case, this study explores a quantum meet-in-the-middle attack on an n-cell structure. A $2n$-round meet-in-the-middle distinguisher is constructed, enabling a $2(n+1)$-round meet-in-the-middle attack and quantum key recovery attack. The associated time complexities are $O(2^{2\ell})$ $2(n+1)$-round encryptions

* 基金项目: 国家自然科学基金 (62172337); 甘肃省自然科学基金重点项目 (23JRRA685); 甘肃省基础研究创新群体基金 (23JRRA684)
收稿时间: 2025-01-11; 修改时间: 2025-03-08; 采用时间: 2025-04-19; jos 在线出版时间: 2025-08-20

and $O(2^{3\ell/2}\cdot\ell)$ quantum queries. The results demonstrate that the time complexity in Q1 model is significantly reduced compared with classical scenarios.

Key words: generalized Feistel structure; quantum meet-in-the-middle attack; Q1 model; quantum claw finding algorithm; Grover's algorithm

分组密码在网络通信和信息安全领域发挥着极其重要的作用. 1970 年, Feistel 等人[1]在设计 Lucifer 算法时提出 Feistel 结构, 该结构因 DES 算法[2]的广泛使用而流行. 广义 Feistel 结构 (generalized Feistel structure, GFS) 是 Feistel 结构的变体形式, 通常采用多分支非平衡 Feistel 结构, 通过不同的置换操作 (如非线性替换与循环移位) 来增强算法的混淆与扩散效果, 且保留了 Feistel 结构加解密一致的优点, 如: Type-I/III 型 GFS[3], *n*-cell 型 GFS[4]等. 这 3 类 GFS 都通过将输入数据划分为多个子块, 允许在单轮操作中对多个子块进行并行处理, 有效提升了加解密效率.

1977 年, Diffie 等人[5]在对 DES 算法进行安全性分析时首次提出了中间相遇攻击, 其思想是利用存储复杂度来降低攻击过程中所需的时间复杂度. Demirci 等人[6]在 FSE 2008 利用中间相遇攻击的思想, 构造了 AES 算法[7]的 4 轮中间相遇区分器, 并提出了该算法的 8 轮中间相遇攻击, 被称为 Demirci-Selçuk 中间相遇 (Demirci-Selçuk meet-in-the-middle, DS-MITM) 攻击. 随后, 研究者们基于文献 [6] 的工作开展了大量抵抗分组密码算法中间相遇攻击的安全性研究[7−11]. 2010 年, Dunkelman 等人[8]改进了文献 [6] 的工作, 结合多重集、差分枚举和密钥桥技术, 有效提高了 AES 算法 DS-MITM 攻击效率. 2014 年, Guo 等人[12]首次针对 Feistel 结构提出了 6 轮 DS-MITM 攻击. 2017 年, Dong 等人[13]构造了 3 分支 Type-I 型 GFS 的 9 轮中间相遇区分器, 向后扩展 1 轮实现了该结构的 10 轮 DS-MITM 攻击. 2019 年, 邓元豪等人[14]构造了 Type-III 型 GFS 的 d+1 轮中间相遇区分器, 向前扩展 1 轮实现了该结构的 d+2 轮密钥恢复攻击.

随着量子计算的发展, 为设计后量子时代的分组密码算法, 研究者需要考虑分组密码算法在量子环境下的安全性. Grover 算法[15]是一种在无序数据库中搜索目标条目的标准搜索算法, 相较于经典环境, 它实现了搜索目标条目所需时间的二次加速. 2000 年, Brassard 等人[16]在文献 [15] 的基础上提出了量子振幅放大 (quantum amplitude amplification, QAA) 技术, 并指出 Grover 算法可以看作是量子振幅放大算法的一种特例. 随后, Buhrman 等人[17]采用 QAA 技术提出了量子爪搜索算法, 用于解决碰撞问题. 这些算法的提出为后续量子 DS-MITM 攻击的发展提供了理论基础.

根据 Zhandry 等人[18]提出的量子环境中伪随机函数 (pseudo random function, PRF) 安全性的概念, Kaplan 等人[19]针对密码算法的量子分析提出了两种模型: 标准安全模型 (Q1 模型) 和量子安全模型 (Q2 模型). 在 Q1 模型中, 攻击者可以访问量子计算机执行任何离线计算, 但只能以经典的方式执行在线查询; 而在 Q2 模型中, 攻击者除了进行离线量子计算外, 还可以利用量子叠加态对量子预言机进行在线查询. 在量子环境下, 分组密码的安全性分析成为学者们关注的焦点, 出现了大量针对 Feistel 结构以及 GFS 的量子安全性分析成果. 2010 年, Kuwakado 等人[20]构造了 3 轮 Feistel 结构的周期函数, 将其作为量子区分器, 同时利用 Simon 算法[21]搜索该函数的周期, 研究表明, 3 轮 Feistel 结构在量子环境下不再安全. 2019 年, Dong 等人[22]结合 Grover 算法和 Simon 算法给出 Feistel 结构以及两类 GFS 的量子区分器的构造方法, 证明了针对这些结构的量子安全性分析所需的时间复杂度均优于 Grover 量子暴力搜索的时间复杂度. 在 PQCrypto 2020, Hodžić等人[23]对 Type-III 型 GFS 进行了分析, 构造了该结构的 5 轮量子区分器. 随后, 于博等人[24]提出了针对若干非平衡 GFS 的量子密码分析, 相较于暴力穷举搜索, 该攻击的效率更高. 同年, 李艳俊等人[25]在考虑轮函数内部结构的情况下对 MIBS 算法进行了 7 轮量子密钥恢复攻击, 该攻击不仅使用了较少的量子比特, 而且时间复杂度更低. 2023 年, 邹剑等人[26]将 Simon 量子区分器的周期函数和生日攻击的思想相结合, 提出了一种针对 Feistel、Misty 等结构的新型密钥恢复攻击, 该攻击所需的存储复杂度和时间复杂度相较于现有的密钥恢复攻击更低.

近年来, 学者们将传统分析方法和量子分析方法相结合, 提出了量子差分密码分析[27]、量子 DS-MITM 攻击[28]等. 2018 年, Hosoyamada 等人[28]针对 Feistel 结构进行了 6 轮量子 DS-MITM 攻击, 结果表明, 相较于文献 [12] 中给出的 6 轮 DS-MITM 攻击的结果, 量子计算机可以显著提升 DS-MITM 攻击的效率. 2022 年, Wang 等人[29]利用

Grover 和量子爪搜索算法对 7 轮 AES 进行量子 DS-MITM 攻击时, 提出了 3 种权衡数据/内存/时间复杂度的量子方案, 进一步降低了攻击的时间复杂度. 次年, 受文献 [28] 的启发, Xu 等人[30]提出了 Feistel 结构的 7 轮量子 DS-MITM 攻击, 改进了文献 [12] 的工作. 2024 年, Zou 等人[31]构建了 Misty L-KF 结构[32]的 5 轮区分器, 并向前扩展 1 轮实现了 6 轮量子 DS-MITM 攻击, 结果表明, 相较于经典环境下的 DS-MITM 攻击, 该攻击所需的时间复杂度更低.

通过对文献 [13,14,22−24] 的研究发现, 不仅 Type-I/Type-III 型 GFS 在经典 DS-MITM 攻击下的轮数有待提高, 而且 n-cell 型 GFS 的 DS-MITM 攻击尚为空白. 虽然已有相关的量子密码分析结果, 但有关三者的抗量子 DS-MITM 攻击的研究仍是空白. 作为一种新的攻击方式, 量子 DS-MITM 攻击结合量子计算的优势和中间相遇的思想, 相较于经典 DS-MITM 攻击, 能够显著提升攻击效率. 因此, GFS 量子 DS-MITM 攻击的安全性有必要进一步研究. 鉴于此, 本文首先对 3 分支 Type-III 型、3 分支 Type-I 型和 n-cell 型 GFS 进行更长轮数的 DS-MITM 攻击, 其次在 Q1 模型下对这 3 类 GFS 进行量子 DS-MITM 攻击, 最后给出相应的复杂度分析, 具体结果见表 1. 主要贡献如下.

表 1　3 类 GFS 的 (量子) DS-MITM 攻击结果

结构类型	环境	轮数	时间复杂度	数据复杂度	存储复杂度	参考来源
Type-III型*	经典	5	$O(2^{2\ell})$	$O(2^{3\ell/2})$	$O(2^{2\ell})$	文献[14]
	经典	6	$O(2^{3\ell})$	$O(2^{\ell})$	$O(2^{2\ell})$	第2.2节
	Q1	6	$O(2^{3\ell/2}\cdot\ell)$	$O(2^{\ell})$	$O(2^{2\ell}\cdot\ell)$	第2.3节
Type-I型*	经典	10	$O(2^{2\ell})$	$O(2^{2\ell})$	$O(2^{2\ell})$	文献[13]
	经典	11	$O(2^{2\ell})$	$O(2^{\ell})$	$O(2^{2\ell})$	第3节
	Q1	11	$O(2^{3\ell/2}\cdot\ell)$	$O(2^{\ell})$	$O(2^{2\ell}\cdot\ell)$	第3节
n-cell型	经典	$2(n+1)$	$O(2^{2\ell})$	$O(2^{\ell})$	$O(2^{2\ell})$	第4.2节
	Q1	$2(n+1)$	$O(2^{3\ell/2}\cdot\ell)$	$O(2^{\ell})$	$O(2^{2\ell}\cdot\ell)$	第4.2节

注: *表示本文仅探讨3分支Type-III型与Type-I型GFS

(1) 研究 3 分支 Type-III 型 GFS 的 (量子) DS-MITM 攻击. 首先, 结合多重集和差分枚举技术构建 4 轮中间相遇区分器, 分别向前向后扩展 1 轮进行 6 轮 DS-MITM 攻击; 其次, 在 Q1 模型下利用 Grover 和量子爪搜索算法进行 6 轮量子 DS-MITM 攻击, 所需要的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询, 比经典环境下 DS-MITM 攻击所需的时间复杂度更低.

(2) 与 (1) 的原理类似, 利用文献 [13] 的 9 轮中间相遇区分器, 对 3 分支 Type-I 型 GFS 进行 (量子) DS-MITM 攻击. 首先, 在经典环境下, 进行 11 轮 DS-MITM 攻击, 相较文献 [13], 攻击轮数更高, 且降低了所需的数据复杂度; 其次, 在量子环境下, 实现 3 分支 Type-I 型 GFS 的 11 轮量子 DS-MITM 攻击, 相应的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询.

(3) 与 (1) 的原理类似, 研究 n-cell 型 GFS 的 (量子) DS-MITM 攻击方案. 首先, 以 3-cell 型 GFS 为例, 构建 6 轮中间相遇区分器, 并对其进行 8 轮 DS-MITM 攻击和量子 DS-MITM 攻击, 攻击的时间复杂度分别为 $O(2^{2\ell})$ 次 8 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 其次, 将该结论扩展到 n-cell 型 GFS, 对其构建 $2n$ 轮中间相遇区分器, 并进行 $2(n+1)$ 轮 DS-MITM 攻击和量子 DS-MITM 攻击. 相应地, 攻击的时间复杂度分别为 $O(2^{2\ell})$ 次 $2(n+1)$ 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询.

本文第 1 节给出了必要的符号说明, DS-MITM 攻击的基本原理以及相关量子算法的基础知识. 第 2 节对 3 分支 Type-III 型 GFS 进行了 6 轮 (量子) DS-MITM 攻击, 并给出了相应的复杂度分析. 第 3 节对 3 分支 Type-I 型 GFS 进行了 11 轮 (量子) DS-MITM 攻击. 第 4 节以 3-cell 型 GFS 为例分析了 n-cell 型 GFS 的 (量子) DS-MITM 攻击方案. 最后总结全文.

1 基础知识

本节首先给出必要的符号说明, 其次简要叙述 DS-MITM 攻击的基本原理, 最后介绍本文使用的量子算法和量子随机存储器的相关知识.

1.1 符号说明

$\mathbb{N}^+$: 正整数集; $\mathbb{F}_2^n$: 二元有限域 $\mathbb{F}_2$ 上的 n 维向量空间, $n \in \mathbb{N}^+$;

$[s]$: 集合 $\{1,2,\ldots,s\}, s \in \mathbb{N}^+$; $\mathbf{0}_\ell$: 长度为 ℓ 的全零比特, $\ell \in \mathbb{N}^+$;

P/C: 明/密文; $\Delta P/\Delta C$: 明/密文差分.

1.2 DS-MITM 攻击

本节介绍 DS-MITM 攻击的相关定义和基本原理.

定义 1. 令 $b, n \in \mathbb{N}^+$, 且 $b < n$, 若集合 W 满足 $\{r = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n | x_{i_k} \in \mathbb{F}_2, 1 \leqslant i_1 < i_2 < \ldots < i_k < \ldots < i_b \leqslant n$, 其余 $(n-b)$ 个比特取值分别固定为 0 或 1$\}$, 则称集合 W 为一个 b-δ-集. 一般地, 取连续的 b 比特遍历.

性质 1. S 盒的性质[33]. 若给定 S 盒的非零输入差分 Δx 和输出差分 Δy, 则方程 $S(t) \oplus S(t \oplus \Delta x) = \Delta y$ 平均有一个解.

DS-MITM 攻击由构造区分器的预计算阶段和进行密钥恢复攻击的在线阶段组成. 攻击的具体过程如下.

1) 预计算阶段

(1.1) 假设存在 N_c 个满足 $\Delta A \to \Delta B$ 的差分特征.

(1.2) 选取步骤 (1.1) 中的一条差分特征, 构造满足差分 ΔA 的输入对 (A_0, A), 根据定义 1, 利用 A_0 生成一个 b-δ-集, 记为 $W = \{A_0, A_1, A_2, \ldots, A_{2^b-1}\}$, 如图 1(a) 所示, 其中, $A_r = A_0 \oplus r$, $r \in [2^b - 1]$.

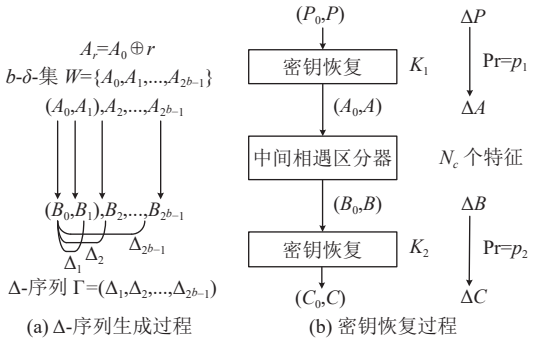


图 1 DS-MITM 攻击概述

(1.3) 将输入对 (A_0, A_r) 进行加密得到输出对 (B_0, B_r), 并计算 $\Delta_r = B_0 \oplus B_r$, $r \in [2^b - 1]$.

(1.4) 由 Δ_r 生成 Δ-序列 $\Gamma = (\Delta_1, \Delta_2, \ldots, \Delta_{2^b-1}) \in \mathbb{F}_2^{(2^b-1)\times\lambda}$, λ 为Δ_r 的比特长度, 并删除此差分特征.

(1.5) 重复步骤 (1.2)–(1.4), 以 Δ_r 为索引, 将 N_c 个序列存储在表 T_δ 中.

2) 在线阶段

(2.1) 选择足够多的明文对进行加密, 使得其中至少存在一对明密文 (P_0, P) 和(C_0, C) 同时满足$\Delta P \to \Delta A$, $\Delta C \to \Delta B$, 如图 1(b) 所示.

(2.2) 根据 P_0 构造对应的 b-δ-集, 由此得到 2^b 个明文, 对其依次进行加密得到相应的密文.

(2.3) 分别猜测子密钥 K_1, K_2 的值, 并利用 K_2 对步骤 (2.2) 的密文进行部分解密, 可得区分器输出处的 Δ-序列 Γ'.

(2.4) 将 Γ' 与 Γ 进行匹配, 若匹配成功, 则猜测的子密钥为正确密钥; 否则, 匹配不成功, 另外选取一对明文重复上述步骤 (2.1)–(2.4).

需要说明的是, 当 $(p_1 p_2)^{-1} N_c \times 2^{-(2^b-1)\times\lambda} \ll 1$, 即 $b \gg \log_2[1 - \log_2(p_1 p_2 / N_c)/\lambda]$ 时, 一定存在正确密钥.

1.3 量子基础知识

量子 DS-MITM 攻击的主要思想是使用量子爪搜索算法寻找 DS-MITM 攻击中预计算阶段和在线阶段所获得的 Δ-序列 之间的碰撞, 并通过 Grover 算法实现对经典搜索效率的二次加速.

考虑搜索问题: 给定布尔函数 $f:\mathbb{F}_2^n\to\mathbb{F}_2$, $n\geqslant 1$, 如果存在唯一的 $x_0\in\mathbb{F}_2^n$ 满足 $f(x_0)=1$, 目标是找到满足条件的 x_0 (下称目标条目). 在总条目数量为 $N=2^n$ 的无序数据库中, Grover 算法将搜索目标条目的时间复杂度从经典算法的 $\mathrm{O}(2^n)$ 降至 $\mathrm{O}(2^{n/2})$, 实现了平方加速, 算法详见文献 [15].

定义 2. 给定两个函数 $f:X\to Z$, $g:Y\to Z$, 其中 $X=[s]$, $Y=[t]$, $s,t\in\mathbb{N}^+$. 如果存在一对 $(x_0,y_0)\in X\times Y$, 使得 $f(x_0)=g(y_0)$, 则称 (x_0,y_0) 为函数 f 和 g 的爪.

2001 年, Buhrman 等人[17]首次提出量子环境下的爪搜索算法, 由于该算法在量子 DS-MITM 攻击的在线阶段起到了重要作用, 故在本节详细介绍, 见算法 1.

算法 1. 量子爪搜索算法.

输入: $f:X\to Z$, $g:Y\to Z$;
输出: 爪 (a_0,b_0).

(1) 分别随机选取大小为 l 和 l^2 的子集 $A\subseteq[s]$ 和 $B\subseteq[t]$, 其中 $l\leqslant\min\left\{s,\ \left\lfloor\sqrt{t}\right\rfloor\right\}$, $\lfloor\rfloor$ 为向下取整函数.
(2) 根据 f 值的大小对条目 $(f(a_i),\ a_i)$ 进行排序, 并将其存储在列表 L 中, 其中, $a_i\in A$, $1\leqslant i\leqslant l$.
(3) 构造量子预言机 U_h: $|b\rangle|1\rangle\to|b\rangle|h(b)\oplus 1\rangle$, 进行测量判断是否存在一对 (a,b) 满足 $f(a)=g(b)$, 其中,

$$h(b)=\begin{cases}1, & \text{存在 } a\in A, b\in B \text{ 使得 } f(a)=g(b)\\ 0, & \text{否则}\end{cases}$$

(4) 若 (3) 的测量结果为 $|b\rangle|0\rangle$, 则进行下一步, 并记 $b_0=b$, 否则, 重复步骤 (1)–(3), 直至测量结果为 $|b\rangle|0\rangle$.
(5) 使用经典二分法搜索列表 L, 找到与步骤 (3) 对应的 a, 并记 $a_0=a$, 输出爪 (a_0,b_0).

算法 1 步骤 (2) 需要 $\mathrm{O}(l\cdot\log l)$ 次经典排序, 步骤 (3)–(5) 共需要 $\mathrm{O}(\sqrt{|B|}\cdot\log|A|)=\mathrm{O}(l\cdot\log l)$ 次量子搜索, 而步骤 (1) 所需要的时间复杂度相较于步骤 (2)–(5) 可以忽略, 故运行步骤 (1)–(5) 所需要的时间复杂度为 $\mathrm{O}(l\cdot\log l)$ 次量子查询. 由于运行一次步骤 (1)–(5) 获得爪 $(a_0,b_0)\in A\times B$ 的成功概率为 $p=l^3/2st$, 故运行算法 1 需要的时间复杂度为 $\mathrm{O}(\sqrt{st/l^3}\cdot l\log l)=\mathrm{O}(\sqrt{st/l}\cdot\log l)$ 次量子查询, 存储复杂度为 $\mathrm{O}(l\cdot\log l)$ 个量子比特.

此外, 量子 DS-MITM 攻击使用了量子随机存储器 (quantum random access memory, qRAM), 它是经典随机存储器 (RAM) 在量子环境下的对应产物. 对于给定的存储在量子计算机的数据列表 $D=\{x_i|i\in[2^k],\ x_i\in\mathbb{F}_2^n,\ k\in\mathbb{N}^+\}$ 和常值 $y\in\mathbb{F}_2^n$, 使用 qRAM 访问 D 的过程定义为酉变换 U_{qRAM}:

$$U_{\mathrm{qRAM}}(D):\sum_i a_i|i\rangle|D\rangle|y\rangle\to\sum_i a_i|i\rangle|D\rangle|y\oplus x_i\rangle,$$

其中, $\sum_i a_i|i\rangle$ 是查询地址的叠加, $|D\rangle|y\oplus x_i\rangle$ 是第 i 个存储单元的内容.

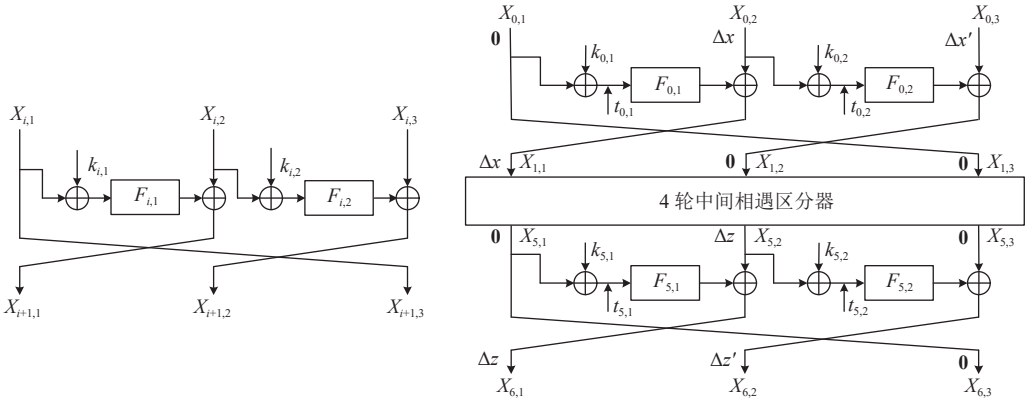
2 3 分支 Type-III 型 GFS 的 6 轮 (量子) DS-MITM 攻击

本节首先简要说明 3 分支 Type-III 型 GFS 的结构特征, 其次, 构造该结构的 4 轮中间相遇区分器, 最后, 基于该区分器分别向前向后扩展 1 轮, 实现 6 轮 (量子) DS-MITM 攻击, 并给出该攻击的复杂度分析.

设该结构的分组长度为 3ℓ 比特, 每个分支的输入长度为 ℓ 比特, 如图 2(a) 所示. 设第 i 轮的两个轮函数分别为 $F_{i,1}:\mathbb{F}_2^\ell\to\mathbb{F}_2^\ell$ 和 $F_{i,2}:\mathbb{F}_2^\ell\to\mathbb{F}_2^\ell$, 两个轮密钥分别为 $k_{i,1}\in\mathbb{F}_2^\ell$ 和 $k_{i,2}\in\mathbb{F}_2^\ell$, 第 i 轮的输入为 $X_i=(X_{i,1},X_{i,2},X_{i,3})\in\mathbb{F}_2^{3\ell}$, 其中, $X_{i,j}$ 表示第 i 轮第 j 个分支的输入, $i\in\mathbb{N}$ 且 $1\leqslant j\leqslant 3$, 则有:

$$(X_{i+1,1},X_{i+1,2},X_{i+1,3})=(X_{i,2}\oplus F_{i,1}(k_{i,1}\oplus X_{i,1}),X_{i,3}\oplus F_{i,2}(k_{i,2}\oplus X_{i,2}),X_{i,1}).$$

另外, 记 $F_{i,j}$ 的输入输出分别为 $F_{i,j}^I$ 和 $F_{i,j}^O$, 相应的输入输出差分分别记为 $\Delta F_{i,j}^I$ 和 $\Delta F_{i,j}^O$.



(a) 第 i 轮结构 (b) 6 轮 DS-MITM 攻击

图 2 3 分支 Type-III 型 GFS 第 i 轮结构和 6 轮 DS-MITM 攻击

2.1 3 分支 Type-III 型 GFS 的 4 轮中间相遇区分器

为研究 Type-III 型 GFS 各轮轮函数内部状态的所有可能值, 引入 Guo 等人[12]对于经典 5 轮 Feistel 结构内部状态所有可能值的相关结论, 具体见引理 1.

引理 1[12]. 对于一个经典的 5 轮 Feistel 结构, 若给定 $\Delta x \neq \Delta z \in \mathbb{F}_2^\ell$, 选取一个输入对 $(A_0, A) \in \mathbb{F}_2^{2\ell\times 2}$ 满足 $\Delta A = A_0 \oplus A = (\mathbf{0}_\ell, \Delta x)$, 进行加密后得到输出对 $(B_0, B) \in \mathbb{F}_2^{2\ell\times 2}$ 且 $\Delta B = B_0 \oplus B = (\mathbf{0}_\ell, \Delta z)$, 则满足截断差分 $\Delta A \to \Delta B$ 的中间 3 轮内部状态值的数量平均为 2^ℓ.

类似地, 可以得到下述 3 分支 Type-III 型 GFS 中间相遇区分器的相关结论.

命题 1. 对于 3 分支 Type-III 型 GFS, 若给定 Δx, $\Delta z \in \mathbb{F}_2^\ell$, 选取一个输入对 $(A_0, A) \in \mathbb{F}_2^{3\ell\times 2}$ 满足 $\Delta A = A_0 \oplus A = (\Delta x, \mathbf{0}_\ell, \mathbf{0}_\ell)$, 进行加密后得到输出对 $(B_0, B) \in \mathbb{F}_2^{3\ell\times 2}$ 且 $\Delta B = B_0 \oplus B = (\mathbf{0}_\ell, \Delta z, \mathbf{0}_\ell)$, 记 Δy 为 $F_{1,1}$ 的输出差分, 则当 $(\Delta x \to \Delta y)$ 为 $F_{3,2}$ 的一条有效差分传播时:

(1) 存在 $(\Delta x, \mathbf{0}_\ell, \mathbf{0}_\ell) \to (\mathbf{0}_\ell, \Delta z, \mathbf{0}_\ell)$ 的一条 4 轮中间相遇区分器;

(2) 满足区分器前 3 轮内部状态值的数量平均为 2^ℓ.

证明:

(1) 如图 3(a) 所示, 从加密方向考虑, 当该结构的输入差分为 $(\Delta x, \mathbf{0}_\ell, \mathbf{0}_\ell)$ 时, 根据差分传播规律, 有 $\Delta F_{3,2}^I = \Delta F_{1,1}^I = \Delta x$. 从解密方向考虑, 根据差分传播规律, 当输出差分为 $(\mathbf{0}_\ell, \Delta z, \mathbf{0}_\ell)$ 时, 有 $\Delta F_{3,1}^O = \Delta x$, $\Delta F_{2,1}^O = (\Delta F_{1,2}^O \oplus \mathbf{0}_\ell) \oplus (\Delta F_{4,2}^O \oplus \Delta z) = \Delta z \neq \mathbf{0}_\ell$, 显然 $\Delta F_{2,1}^I \neq \mathbf{0}_\ell$, 记 $\Delta y = \Delta F_{2,1}^I$, 则 $\Delta F_{3,2}^O = \Delta F_{1,1}^O = \Delta y$. 由此可得一条满足 $(\Delta x, \mathbf{0}_\ell, \mathbf{0}_\ell) \to (\mathbf{0}_\ell, \Delta z, \mathbf{0}_\ell)$ 的 4 轮中间相遇区分器.

(2) 下面讨论前 3 轮内部状态的可能值, 令 $t_{i,j}$ 为第 i 轮第 j 个轮函数的输入, 从加密方向可得:

$$\begin{cases} F_{1,1}(t_{1,1}) \oplus F_{1,1}(t_{1,1} \oplus \Delta x) = \Delta y,\ F_{2,1}(t_{2,1}) \oplus F_{2,1}(t_{2,1} \oplus \Delta y) = \Delta z \\ F_{3,1}(t_{3,1}) \oplus F_{3,1}(t_{3,1} \oplus \Delta z) = \Delta x,\ F_{3,2}(t_{3,2}) \oplus F_{3,2}(t_{3,2} \oplus \Delta x) = \Delta y \end{cases} \tag{1}$$

由于轮函数内部的线性运算不影响差分, 只有非线性运算 S 盒会影响差分, 根据性质 1, 当公式 (1) 中的 Δx, Δz 给定, Δy 取固定值时, 轮函数的内部状态值 $t_{1,1}$, $t_{2,1}$, $t_{3,1}$ 和 $t_{3,2}$ 平均只有 1 个解. 由于 Δy 最多可取 2^ℓ 个值, 所以上述 4 个内部状态值的数量平均为 2^ℓ. 证毕.

下面基于区分器的输入对讨论 3 分支 Type-III 型 GFS 的 Δ-序列 Γ_1 可能值的个数.

定理 1. 若输入对 $(A_0, A) \in \mathbb{F}_2^{3\ell\times 2}$ 满足命题 1 中区分器的输入, 利用 A_0 构造 b-δ-集 $M = \{(A_0 \oplus (r, \mathbf{0}_\ell, \mathbf{0}_\ell)) \in \mathbb{F}_2^{3\ell} | r \in \{0, 1, \ldots, 2^b - 1\}\}$, 则可得 Δ-序列 $\Gamma_1 = (\Delta_1, \Delta_2, \ldots, \Delta_{2^b-1})$ 有 2^ℓ 个可能值.

证明: 如图 3(b) 所示, 设 $X_{1,1} \in \mathbb{F}_2^\ell$ 的 b 比特活跃, 输入对 $(A_0, A) \in \mathbb{F}_2^{3\ell\times 2}$ 的差分 $\Delta A = A_0 \oplus A = (r, \mathbf{0}_\ell, \mathbf{0}_\ell)$, 根据集合 M 可得输入对 $(A_0, A_0 \oplus (r, \mathbf{0}_\ell, \mathbf{0}_\ell))$, $r \in [2^b - 1]$, 将其加密 4 轮得到差分为 $\Delta X_5^r = (\Delta X_{5,1}^r, \Delta X_{5,2}^r, \Delta X_{5,3}^r)$ 的输出对. 则 $\Delta_r =$

$\Delta X_{5,3}^{r}$ 的具体计算过程如下.

由加密流程可知:

第 1 轮: $\Delta F_{1,1}^{O} = F_{1,1}(t_{1,1}) \oplus F_{1,1}(t_{1,1} \oplus r)$.

第 2 轮: $\Delta F_{2,1}^{O} = F_{2,1}(t_{2,1}) \oplus F_{2,1}(t_{2,1} \oplus \Delta F_{1,1}^{O})$.

第 3 轮: $\Delta F_{3,1}^{O} = F_{3,1}(t_{3,1}) \oplus F_{3,1}(t_{3,1} \oplus \Delta F_{2,1}^{O})$, $\Delta F_{3,2}^{O} = F_{3,2}(t_{3,2}) \oplus F_{3,2}(t_{3,2} \oplus r)$.

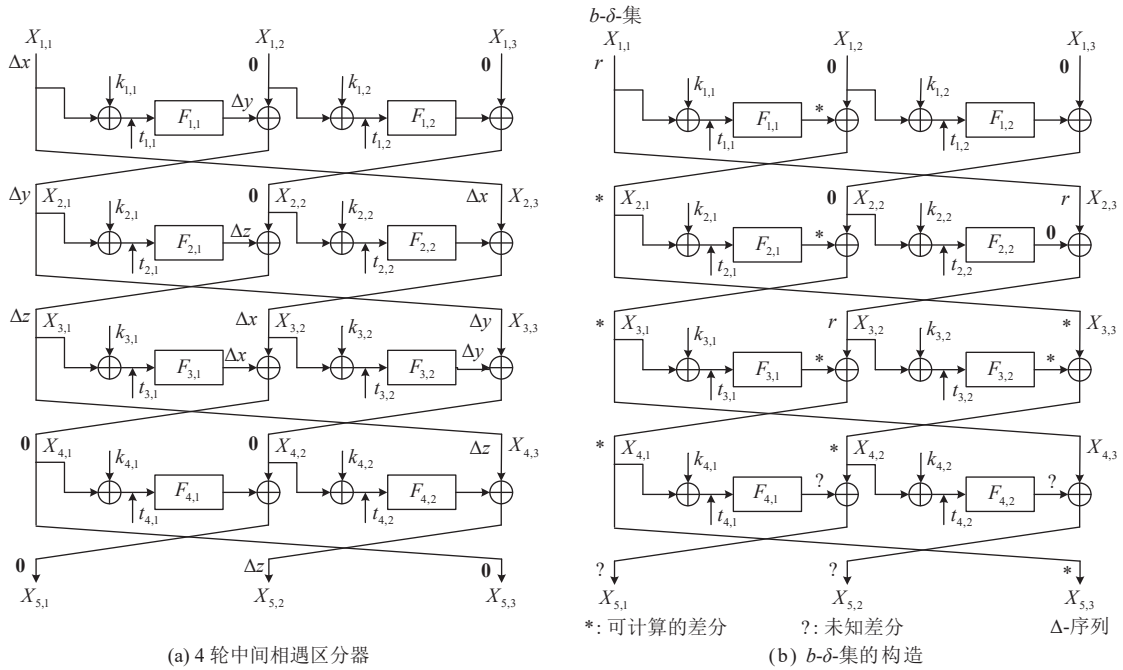


图 3　3 分支 Type-III 型 GFS 的 4 轮中间相遇区分器和 b-δ-集 的构造

由此可得:

$$\begin{aligned}\Delta_r &= \Delta X_{5,3}^{r} = \Delta F_{3,1}^{O} \oplus r \\ &= (F_{3,1}(t_{3,1}) \oplus F_{3,1}(t_{3,1} \oplus \Delta F_{2,1}^{O})) \oplus r \\ &= (F_{3,1}(t_{3,1}) \oplus F_{3,1}(t_{3,1} \oplus F_{2,1}(t_{2,1}) \oplus F_{2,1}(t_{2,1} \oplus \Delta F_{1,1}^{O}))) \oplus r \\ &= (F_{3,1}(t_{3,1}) \oplus F_{3,1}(t_{3,1} \oplus F_{2,1}(t_{2,1}) \oplus F_{2,1}(t_{2,1} \oplus F_{1,1}(t_{1,1}) \oplus F_{1,1}(t_{1,1} \oplus r)))) \oplus r \end{aligned} \tag{2}$$

当 r 取遍 $[2^b - 1]$ 时, 可得到 Δ-序列 $\Gamma_1 = (\Delta_1, \Delta_2, \ldots, \Delta_{2^b-1})$.

由公式 (2) 的最后一行可知, Δ_r 依赖于 $t_{1,1}$, $t_{2,1}$ 和 $t_{3,1}$ 的值, 又由公式 (1) 可知, $t_{2,1}$ 和 $t_{3,1}$ 由 $t_{1,1}$ 决定. 而根据命题 1, $t_{1,1}$ 有 2^{ℓ} 个可能值, 故 Δ-序列 Γ_1 有 2^{ℓ} 个可能值. 证毕.

2.2　3 分支 Type-III 型 GFS 的 6 轮 DS-MITM 攻击及复杂度分析

本节基于命题 1 构造的 4 轮中间相遇区分器, 分别向前向后扩展 1 轮, 实现 3 分支 Type-III 型 GFS 的 6 轮 DS-MITM 攻击, 攻击包括预计算阶段和在线阶段, 具体过程见图 2(b).

预计算阶段: 详细过程如定理 1 所示, 并将 Δ-序列 Γ_1 的 2^{ℓ} 种可能值存储在以 Δ_r 为索引的表 T_1 中, 其中 $r \in [2^b - 1]$.

在线阶段: 包括数据收集和密钥恢复两部分.

1) 数据收集. 包括如下 3 个步骤.

(1.1) 任意选取两个向量 m, $a \in \mathbb{F}_2^{\ell}$, 如图 2(b) 所示, 构造满足区分器第 1 分支输入差分为 Δx 的两个明文集

$\{(a,m,0),(a,m,1),\ldots,(a,m,2^\ell-1)\}$, $\{(a,m\oplus\Delta x,0),(a,m\oplus\Delta x,1),\ldots,(a,m\oplus\Delta x,2^\ell-1)\}$, 相应的明文差分 $\Delta P=(\mathbf{0}_\ell,\Delta x,\Delta x')\in\mathbb{F}_2^{\ell\times 3}$, 将这 $2^{2\ell}$ 个明文对存储在列表 T_P 中.

(1.2) 对任意 u_1, $u_2\in\mathbb{F}_2^\ell$, 将差分为 ΔP 的明文对 (a,m,u_1) 和 $(a,m\oplus\Delta x,u_2)$ 分别进行 6 轮加密得到 $2^{2\ell}$ 个差分为 $\Delta C=(\Delta z,\Delta z',\mathbf{0}_\ell)\in\mathbb{F}_2^{\ell\times 3}$ 的密文对, 并将其存储在列表 T_C 中. 对于给定的 Δx, Δz, 由于明密文差分 ΔP 和 ΔC 均以概率 $p_1=p_2=2^{-\ell}$ 分别传播到区分器的输入差分 $(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)$ 和输出差分 $(\mathbf{0}_\ell,\Delta z,\mathbf{0}_\ell)$, 则 6 轮截断差分传播概率为 $p=p_1p_2=2^{-2\ell}$. 因此, 至少有 $2^{-2\ell}\times 2^{2\ell}=1$ 个明密文对 $(P_0,P)\in\mathbb{F}_2^{3\ell\times 2}$ 和 $(C_0,C)\in\mathbb{F}_2^{3\ell\times 2}$ 满足图 2(b) 所示的 6 轮差分特征 $(\mathbf{0}_\ell,\Delta x,\Delta x')\to(\Delta z,\Delta z',\mathbf{0}_\ell)$.

(1.3) 根据步骤 (1.2) 得到的明文对 (P_0,P), 利用 $P_0=(X_{0,1}^0,X_{0,2}^0,X_{0,3}^0)$ 构造 b-δ-集 $G=\{P_r=X_{0,1}^0,X_{0,2}^0\oplus r,X_{0,3}^0\oplus\Delta F_{0,2}^O)|r\in\{0,1,\ldots,2^b-1\},\ \Delta F_{0,2}^O\in\mathbb{F}_2^\ell\}$, 利用 G 构造明文对 (P_0,P_r), $r\in[2^b-1]$, 并依次进行 6 轮加密得到对应的密文对 (C_0,C_r), 因此得到 2^b-1 个明密文对满足图 2(b) 所示的 6 轮差分特征 $(\mathbf{0}_\ell,\Delta x,\Delta x')\to(\Delta z,\Delta z',\mathbf{0}_\ell)$.

2) 密钥恢复. 包括如下 4 个步骤.

(2.1) 选取步骤 (1.3) 中的一个明文对 (P_0,P_r), 对应差分 $P_0\oplus P_r=(\mathbf{0}_\ell,\Delta x,\Delta x')$, 根据性质 1, 利用 $F_{0,2}(t_{0,2})\oplus F_{0,2}(t_{0,2}\oplus\Delta x)=\Delta x'$ 确定 $t_{0,2}$ 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 $t_{0,2}$ 的 2^b-1 个可能值存储在以 $(\mathbf{0}_\ell,\Delta x,\Delta x')$ 为索引的表 T_2 中, 再由 $k_{0,2}=t_{0,2}\oplus(X_{0,2}^0\oplus r)$ 确定子密钥 $k_{0,2}$ 的 2^b-1 个可能值.

(2.2) 对每个 $r\in[2^b-1]$, 依次选取密文对 (C_0,C_r), $C_r=(X_{6,1}^r,X_{6,2}^r,X_{6,3}^r)$, 显然 $C_0\oplus C_r=(\Delta z,\Delta z',\mathbf{0}_\ell)$. 猜测子密钥 $k_{5,1}$ 的值, 根据性质 1 和 $X_{6,1}^r\oplus F(X_{6,3}^r\oplus k_{5,1})=X_{5,2}^r$ 确定 $X_{5,2}^r$ 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 $X_{5,2}^r$ 的 2^b-1 个可能值. 类似地, 利用 $F_{5,2}(t_{5,2})\oplus F_{5,2}(t_{5,2}\oplus\Delta z)=\Delta z'$ 确定 $t_{5,2}$ 的 2^b-1 个可能值, 并将其存储在以 $(\Delta z,\Delta z',\mathbf{0}_\ell)$ 为索引的表 T_3 中, 再由 $k_{5,2}=t_{5,2}\oplus X_{5,2}^r$ 确定子密钥 $k_{5,2}$ 的 2^b-1 个可能值.

(2.3) 根据 $k_{5,1}$ 和 $k_{5,2}$ 的猜测值, 对步骤 (1.3) 得到的密文集 $\{C_0,C_1,\ldots,C_{2^b-1}\}$ 分别进行部分解密, 得到区分器输出处的可能值 $X_5^r=(X_{5,1}^r,X_{5,2}^r,X_{5,3}^r)\in\mathbb{F}_2^{\ell\times 3}$, $r\in\{0,1,\ldots,2^b-1\}$, 从而得到 Δ-序列 $\Gamma_2=(\Delta_1,\Delta_2,\cdots,\Delta_{2^b-1})$, 其中, $\Delta_r=X_{5,3}^0\oplus X_{5,3}^r$, $r\in[2^b-1]$.

(2.4) 将步骤 (1.3) 中的 2^b-1 个明密文对 (P_0,P_r) 和 (C_0,C_r), 步骤 (2.1)–(2.3) 中的 2^b-1 组子密钥 $(k_{0,2},k_{5,1},k_{5,2})$ 以及相应的 Δ-序列 $\Gamma_2=(\Delta_1,\Delta_2,\ldots,\Delta_{2^b-1})$ 存储在以 Δ_r 为索引的表 T_4 中. 当 $b\geqslant 3$ 时, 检查表 T_1 和 T_4 中的 Δ-序列是否匹配, 若匹配, 则猜测的子密钥 $(k_{0,2},k_{5,1},k_{5,2})$ 为正确密钥; 否则, 匹配不成功, 另外选取一对明文重复上述步骤 (2.1)–(2.4).

下面给出攻击的复杂度分析.

(1) 由于在线阶段构造了两个大小分别为 2^ℓ 的明文集, 故该攻击的数据复杂度为 $\mathrm{O}(2^\ell+2^\ell)\approx\mathrm{O}(2^\ell)$ 个选择明文.

(2) 由于预计算阶段构造表 T_1 所需的时间复杂度为 $\mathrm{O}(2^{2\ell})$ 次 6 轮加密, 在线阶段猜测子密钥所需的时间复杂度为 $\mathrm{O}(2^{3\ell})$ 次 6 轮加密, 因此, 攻击所需的时间复杂度为 $\mathrm{O}(2^{3\ell})$ 次 6 轮加密.

(3) 由于存储的是 Δ-序列, 而 Δ-序列中有 2^b-1 个 Δ_i, 且每个 Δ_i 的长度为 ℓ 比特, 故存储表 T_1 和 T_4 所需的存储复杂度为 $\mathrm{O}(2^{2\ell}+2^{2\ell})\approx\mathrm{O}(2^{2\ell})$ 个长度为 $(2^b-1)\ell$ 的比特块.

2.3 3 分支 Type-III 型 GFS 的 6 轮量子 DS-MITM 攻击及复杂度分析

本节首先基于命题 1 构造的 4 轮中间相遇区分器, 分别向前向后扩展 1 轮, 实现 3 分支 Type-III 型 GFS 的 6 轮量子 DS-MITM 攻击; 其次, 对攻击的复杂度进行分析.

攻击过程包括预计算阶段和在线阶段.

1) 预计算阶段. 通过量子并行叠加, 将经典环境下的时间复杂度从 $\mathrm{O}(2^{2\ell})$ 次 6 轮加密降低到 $\mathrm{O}(2^\ell)$ 次量子查询, 具体步骤如下.

(1.1) 根据区分器第 1 分支差分 Δx 制备量子叠加态:

$$|\varphi_1\rangle=\sum_{\Delta z=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta z\rangle\sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle|\Delta x\rangle.$$

(1.2) 依据公式 (1) 利用 Grover 算法搜索 $|\varphi_1\rangle$ 得到图 3(a) 中的状态 $t_{1,1}$, $t_{2,1}$, $t_{3,1}$ 和 $t_{3,2}$, 即:

$$\begin{cases}\sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle|\Delta x\rangle\sum_{t_{1,1}=0}^{2^\ell-1}\left|t_{1,1}\right\rangle\xrightarrow{\text{Grover}}\sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle|\Delta x\rangle\left|t_{1,1}\right\rangle\\ \sum_{\Delta z=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta z\rangle\sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle\sum_{t_{2,1}=0}^{2^\ell-1}\left|t_{2,1}\right\rangle\xrightarrow{\text{Grover}}\sum_{\Delta z,\Delta y=0}^{\Delta z,\Delta y=2^\ell-1}\frac{1}{\sqrt{2^{2\ell}}}|\Delta z\rangle|\Delta y\rangle\left|t_{2,1}\right\rangle\\ \sum_{\Delta z=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta z\rangle|\Delta x\rangle\sum_{t_{3,1}=0}^{2^\ell-1}\left|t_{3,1}\right\rangle\xrightarrow{\text{Grover}}\sum_{\Delta z=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta z\rangle|\Delta x\rangle\left|t_{3,1}\right\rangle\\ \sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle|\Delta x\rangle\sum_{t_{3,2}=0}^{2^\ell-1}\left|t_{3,2}\right\rangle\xrightarrow{\text{Grover}}\sum_{\Delta y=0}^{2^\ell-1}\frac{1}{\sqrt{2^\ell}}|\Delta y\rangle|\Delta x\rangle\left|t_{3,2}\right\rangle\end{cases},$$

从而得到叠加态:

$$|\varphi_2\rangle=\sum_{\Delta z,\Delta y=0}^{\Delta z,\Delta y=2^\ell-1}\frac{1}{\sqrt{2^{2\ell}}}|\Delta z\rangle|\Delta y\rangle|\Delta x\rangle\left|t_{1,1}\right\rangle\left|t_{2,1}\right\rangle\left|t_{3,1}\right\rangle\left|t_{3,2}\right\rangle.$$

(1.3) 将 $\otimes_{r=0}^{2^b-1}|r\rangle$ 作为输入, 根据定理 1 中的 b-δ-集 M 计算 Δ-序列 Γ_1, 制备叠加态:

$$|\varphi_3\rangle=\sum_{\Delta z,\Delta y=0}^{\Delta z,\Delta y=2^\ell-1}\frac{1}{\sqrt{2^{2\ell}}}|\Delta z\rangle|\Delta y\rangle|\Delta x\rangle|\Gamma_1\rangle,$$

并将其存储在量子寄存器的 $\mathrm{O}(\ell\cdot 2^b)$ 个比特中.

(1.4) 基于 Grover 算法, 对 $|\varphi_3\rangle$ 使用 $2^{2\ell}$ 个并行的单量子处理器进行搜索, 以获得 $(\Delta z,\Delta y)$ 对应的所有可能的 $|\Gamma_1\rangle$, 并将其存储在以 $(\Delta z,\Delta y)$ 为索引的表 T_1' 中.

2) 在线阶段. 在经典环境中, 确定第 3.2 节步骤 (2.2) 的 Δ-序列 Γ_2 需要使用 $\mathrm{O}(2^{2\ell})$ 经典内存进行 $\mathrm{O}(2^{2\ell})$ 次计算, 而在量子环境下可使用以下步骤降低时间复杂度.

(2.1) 将 2ℓ 个量子比特初始化为 $|0\rangle^{\otimes 2\ell}$, 并制备叠加态:

$$|\psi_1\rangle=\sum_{I_1\in T_P,I_2\in T_C}\frac{1}{\sqrt{2^{2\ell}}}|I_1\rangle|I_2\rangle,$$

其中, 长度均为 6ℓ 个量子比特的叠加态 $|I_1\rangle$ 和 $|I_2\rangle$ 分别表示第 3.2 节步骤 (1.1) 和 (1.2) 所得的 $2^{2\ell}$ 组明密文对, 并将其存储在表 T_{PC} 中, 以 (I_1,I_2) 为索引.

(2.2) 将 $|\psi_1\rangle$ 作为地址, 使用 qRAM 从表 T_{PC} 中查询一组明密文对 (P_0,C_0) 和 (P,C), 得到 $|\psi_2\rangle$, 即:

$$|\psi_1\rangle|T_{PC}\rangle|\mathbf{0}_{6\ell}\rangle|\mathbf{0}_{6\ell}\rangle\xrightarrow{U_{\text{qRAM}}}|\psi_1\rangle|T_{PC}\rangle|P_0,C_0\rangle|P,C\rangle=|\psi_2\rangle.$$

(2.3) 计算 b-δ-集 M 对应的明文集 $\{P_0,P_1,\ldots,P_{2^b-1}\}$, 得到叠加态:

$$|\psi_3\rangle=|\psi_2\rangle|P_0,P_1,\ldots,P_{2^b-1}\rangle.$$

(2.4) 将 $|\psi_3\rangle$ 作为地址, 使用 qRAM 查询明文集得到对应的密文集, 可得:

$$|\psi_4\rangle=|\psi_3\rangle|C_0,C_1,\ldots,C_{2^b-1}\rangle.$$

(2.5) 对每个 $r\in[2^b-1]$, 依次执行以下 3 个步骤.

(2.5.1) 选取一组明密文对 (P_0,C_0) 和 (P_r,C_r), 计算相应的差分 $(\Delta x,\Delta x')$ 和 $(\Delta z,\Delta z')$, 得到叠加态:

$$|\psi_5\rangle=|\psi_4\rangle|\Delta x,\Delta x'\rangle|\Delta z,\Delta z'\rangle.$$

(2.5.2) 对叠加态 $|\psi_5\rangle$ 使用 Grover 算法搜索 $t_{0,2}$, $t_{5,1}$ 和 $t_{5,2}$, 即:

$$|\psi_5\rangle\sum_{t_{0,2}=0}^{2^\ell-1}\left|t_{0,2}\right\rangle\sum_{t_{5,2}=0}^{2^\ell-1}\left|t_{5,2}\right\rangle\sum_{t_{5,1}=0}^{2^\ell-1}\left|t_{5,1}\right\rangle\xrightarrow{\text{Grover}}|\psi_5\rangle\left|t_{0,2}\right\rangle\left|t_{5,1}\right\rangle\left|t_{5,2}\right\rangle,$$

从而获得叠加态:

$$|\psi_6\rangle=|\psi_5\rangle\left|t_{0,2}\right\rangle\left|t_{5,1}\right\rangle\left|t_{5,2}\right\rangle.$$

(2.5.3) 猜测子密钥 $k_{0,2}$, $k_{5,1}$ 和 $k_{5,2}$, 得到叠加态:

$$|\psi_7\rangle = |\psi_6\rangle\left|k_{0,2}\right\rangle\left|k_{5,1}\right\rangle\left|k_{5,2}\right\rangle.$$

(2.6) 根据 2^b-1 组候选子密钥 $(k_{5,1},k_{5,2})$ 和密文集 $\{C_0,C_1,\ldots,C_{2^b-1}\}$, 解密 1 轮得到 Δ-序列 Γ_2, 可得:

$$|\psi_8\rangle = |\psi_7\rangle|\Gamma_2\rangle,$$

再利用量子删除操作, 仅保留 $|\psi_1\rangle$ 和 $|\Gamma_2\rangle$, 得到最终的叠加态:

$$|\psi_9\rangle = \sum_{I_1\in T_P, I_2\in T_C} \frac{1}{\sqrt{2^{2\ell}}}|I_1\rangle|I_2\rangle|\Gamma_2\rangle,$$

同时, 将 Γ_2 存储在以 $(I_1,\ I_2)$ 为索引的表 T_4' 中.

(2.7) 利用量子爪搜索算法将表 T_1' 和 T_4' 进行匹配, 以获得正确密钥.

下面分析攻击的时间和存储复杂度.

在预计算阶段, 步骤 (1.2) 和 (1.4) 所需的时间复杂度分别为 $\mathrm{O}(2^{\ell/2})$ 和 $\mathrm{O}(2^{\ell})$ 次量子查询, 故所消耗的总时间为 $\mathrm{O}(2^{\ell/2}+2^{\ell})\approx\mathrm{O}(2^{\ell})$ 次量子查询. 此外, 该阶段还需要 $\mathrm{O}(2^{2\ell}\cdot\ell)$ 个量子比特存储表 T_1'.

在线阶段的复杂度主要由步骤 (2.7) 决定, 即使用量子爪搜索算法, 从表 T_1' 和 T_4' 中搜索爪 $((\Delta z,\Delta y),(I_1,I_2))$ 使得函数 $f(\Delta z,\Delta y)=g(I_1,I_2)$, 其中, 函数 $f:\Delta z\times\Delta y\to\Gamma_1$, $\Delta z,\Delta y\in\mathbb{F}_2^{\ell}$, 函数 $g:I_1\times I_2\to\Gamma_2$, $I_1,I_2\in\mathbb{F}_2^{6\ell}$, $\Gamma_1,\Gamma_2\in\mathbb{F}_2^{(2^b-1)\times\ell}$. 根据算法 1, 当 $l=2^{\ell}$ 时, 该阶段的时间复杂度为 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询.

综上所述, 在 Q1 模型下对 3 分支 Type-III 型 GFS 进行 6 轮量子 DS-MITM 攻击所需要的复杂度如下.

(1) 数据复杂度为 $\mathrm{O}(2^{\ell})$ 个选择明文.

(2) 由于构造表 T_1' 和运行爪搜索算法 $(l=2^{\ell})$ 的时间复杂度分别为 $\mathrm{O}(2^{\ell/2}+2^{\ell})\approx\mathrm{O}(2^{\ell})$ 和 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询, 因此, 总的时间复杂度为 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询.

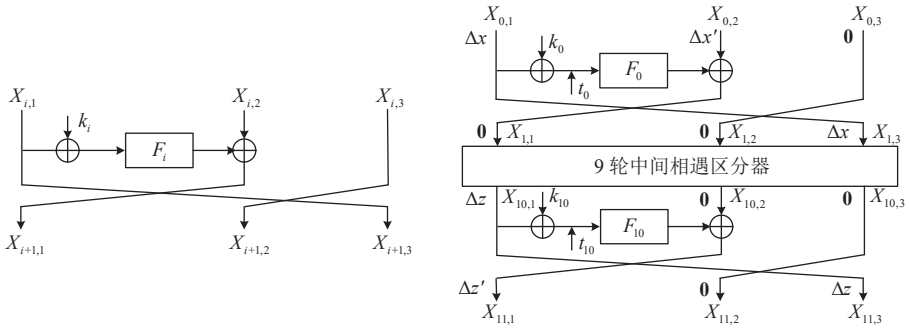
(3) 构造表 T_1' 和运行爪搜索算法筛选密钥 $(l=2^{\ell})$ 需要 $\mathrm{O}(2^{2\ell}\cdot\ell+2^{\ell}\cdot\ell)\approx\mathrm{O}(2^{2\ell}\cdot\ell)$ 个量子比特.

3 3 分支 Type-I 型 GFS 的 11 轮 (量子) DS-MITM 攻击及其复杂度分析

本节首先简要介绍 3 分支 Type-I 型 GFS 的结构特征, 其次, 利用文献 [13] 构造的 3 分支 Type-I 型 GFS 的 9 轮中间相遇区分器对该结构实施 11 轮 DS-MITM 攻击和量子 DS-MITM 攻击, 并进行复杂度分析.

设该结构的分组长度为 3ℓ 比特, 每个分支的输入长度为 ℓ 比特, 如图 4(a) 所示. 设第 i 轮的轮函数为 $F_i:\mathbb{F}_2^{\ell}\to\mathbb{F}_2^{\ell}$, 轮密钥为 $k_i\in\mathbb{F}_2^{\ell}$, 第 i 轮的输入为 $X_i=(X_{i,1},X_{i,2},X_{i,3})\in\mathbb{F}_2^{\ell\times 3}$, $i\in\mathbb{N}$, 则有:

$$(X_{i+1,1},X_{i+1,2},X_{i+1,3})=(X_{i,2}\oplus F_i(k_i\oplus X_{i,1}),X_{i,3},X_{i,1}).$$



(a) 第 i 轮结构 (b) 11 轮 DS-MITM 攻击

图 4 3 分支 Type-I 型 GFS 第 i 轮结构和 11 轮 DS-MITM 攻击

另外, 记 F_i 的输入输出分别为 F_i^I 和 F_i^O, 相应的输入输出差分分别记为 ΔF_i^I 和 ΔF_i^O.

接下来, 我们利用文献 [13] 构造的 9 轮中间相遇区分器对 11 轮 3 分支 Type-I 型 GFS 进行 DS-MITM 攻击及复杂度分析.

预计算阶段: 将文献 [13] 构造区分器阶段 $(\mathbf{0}_{\ell},\mathbf{0}_{\ell},\Delta x)\to(\Delta z,\mathbf{0}_{\ell},\mathbf{0}_{\ell})$ 得到的 Δ-序列 Γ_3 的 2^{ℓ} 种可能值存储在表 T_5 中.

在线阶段: 包括数据收集和密钥恢复两部分.

1) 数据收集. 包括如下 3 个步骤.

(1.1) 任意选取两个向量 c, $a \in \mathbb{F}_2^\ell$, 如图 4(b) 所示, 构造满足区分器第 1 分支输出差分为 Δz 的两个密文集 $\{(0,a,c),(1,a,c),\ldots,(2^\ell-1,a,c)\},\{(0,a,c\oplus\Delta z),(1,a,c\oplus\Delta z),\ldots,(2^\ell-1,a,c\oplus\Delta z)\}$, 相应的密文差分 $\Delta C = (\Delta z',\mathbf{0}_\ell,\Delta z) \in \mathbb{F}_2^{\ell\times 3}$, 将这 $2^{2\ell}$ 个密文对存储在列表 T_C 中.

(1.2) 对任意 u_1, $u_2 \in \mathbb{F}_2^\ell$, 将差分为 ΔC 的密文对 (u_1,a,c) 和 $(u_2,a,c\oplus\Delta z)$ 分别进行 11 轮解密得到 $2^{2\ell}$ 个差分为 $\Delta P = (\Delta x,\Delta x',\mathbf{0}_\ell) \in \mathbb{F}_2^{\ell\times 3}$ 的明文对, 并将其存储在列表 T_P 中. 对于给定的 Δx, Δz, 由于明密文差分 ΔP 和 ΔC 均以概率 $p_1 = p_2 = 2^{-\ell}$ 分别传播到区分器的输入差分 $(\mathbf{0}_\ell,\mathbf{0}_\ell,\Delta x)$ 和输出差分 $(\Delta z,\mathbf{0}_\ell,\mathbf{0}_\ell)$, 则 11 轮截断差分传播概率为 $p = 2^{-2\ell}$. 因此, 至少有 $2^{-2\ell}\times 2^{2\ell} = 1$ 个明密文对 (P_0,P) 和 (C_0,C) 满足图 4(b) 所示 $(\Delta x,\Delta x',\mathbf{0}_\ell) \to (\Delta z',\mathbf{0}_\ell,\Delta z)$ 的 11 轮差分特征.

(1.3) 根据步骤 (1.2) 得到的密文对 (C_0,C), 利用密文 $C_0 = (X_{11,1}^0,X_{11,2}^0,X_{11,3}^0)$ 构造 b-δ-集 $G = \{C_r = (X_{11,1}^0\oplus\Delta F_{10}^O,\ X_{11,2}^0,\ X_{11,3}^0\oplus r) \mid r\in\{0,1,\ldots,2^b-1\},\ \Delta F_{10}^O \in \mathbb{F}_2^\ell\}$, 利用 G 构造密文对 (C_0,C_r), $r\in[2^b-1]$, 并依次进行 11 轮解密得到对应的明文对 (P_0,P_r), 因此得到 2^b-1 个明密文对满足图 4(b) 所示的 11 轮差分特征.

2) 密钥恢复. 包括如下 4 个步骤.

(2.1) 选取步骤 (1.3) 中的一个密文对 (C_0,C_r), 其差分为 $C_0\oplus C_r = (\Delta z',\mathbf{0}_\ell,\Delta z)$, 根据性质 1 和 $F(t_{10})\oplus F(t_{10}\oplus\Delta z) = \Delta z'$ 确定 t_{10} 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 t_{10} 的 2^b-1 个可能值存储在以 $(\Delta z',\mathbf{0}_\ell,\Delta z)$ 为索引的表 T_6 中, 再由 $k_{10} = t_{10}\oplus(X_{11,3}^0\oplus r)$ 确定子密钥 k_{10} 的 2^b-1 个可能值.

(2.2) 对每个 $r\in[2^b-1]$, 依次选取明文对 (P_0,P_r), $P_r = (X_{0,1}^r,X_{0,2}^r,X_{0,3}^r)$, 显然 $P_0\oplus P_r = (\Delta x,\Delta x',\mathbf{0}_\ell)$. 类似地, 利用 $F(t_0)\oplus F(t_0\oplus\Delta x) = \Delta x'$ 确定 t_0 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 t_0 的 2^b-1 个可能值存储在以 $(\Delta x,\Delta x',\mathbf{0}_\ell)$ 为索引的表 T_7 中, 再由 $k_0 = t_0\oplus X_{0,1}^r$ 确定子密钥 k_0 的 2^b-1 个可能值.

(2.3) 根据 k_0 的猜测值, 对步骤 (1.3) 得到的明文集 $\{P_0,P_1,\ldots,P_{2^b-1}\}$ 分别进行部分加密, 得到区分器输入处的可能值 $X_1^r = (X_{1,1}^r,X_{1,2}^r,X_{1,3}^r) \in \mathbb{F}_2^{\ell\times 3}, r\in\{0,1,\ldots,2^b-1\}$, 从而得到 Δ-序列 $\Gamma_4 = (\Delta_1,\Delta_2,\ldots,\Delta_{2^b-1})$, 其中, $\Delta_r = X_{1,1}^0\oplus X_{1,1}^r$, $r\in[2^b-1]$.

(2.4) 将步骤 (1.3) 中的 2^b-1 个明密文对 (P_0,P_r) 和 (C_0,C_r), 步骤 (2.1)–(2.3) 中的 2^b-1 组子密钥 (k_0,k_{10}) 以及相应的 Δ-序列 $\Gamma_4 = (\Delta_1,\Delta_2,\ldots,\Delta_{2^b-1})$ 存储在表 T_8 中. 类似地, 当 $b\geqslant 3$ 时, 检查表 T_5 和 T_8 中的 Δ-序列 是否匹配, 若匹配, 猜测的子密钥 k_0 和 k_{10} 为正确密钥; 否则, 匹配不成功, 另外选取一对明文重复上述步骤 (2.1)–(2.4).

下面给出攻击的复杂度分析.

(1) 由于在线阶段构造了两个大小分别为 2^ℓ 的密文集, 故该攻击的数据复杂度为 $\mathrm{O}(2^\ell+2^\ell)\approx\mathrm{O}(2^\ell)$ 个选择密文.

(2) 由于预计算阶段构造表 T_5 和在线阶段猜测子密钥所需的时间复杂度均为 $\mathrm{O}(2^{2\ell})$ 次 11 轮解密, 因此, 攻击所需的时间复杂度为 $\mathrm{O}(2^{2\ell})$ 次 11 轮解密.

(3) 存储表 T_5 和 T_8 所需的存储复杂度为 $\mathrm{O}(2^{2\ell}+2^{2\ell})\approx\mathrm{O}(2^{2\ell})$ 个长度为 $(2^b-1)\ell$ 的比特块.

定理 2. 利用文献 [13] 的中间相遇区分器可对 3 分支 Type-I 型 GFS 进行 11 轮量子 DS-MITM 攻击, 数据复杂度为 $\mathrm{O}(2^\ell)$ 个选择密文, 时间复杂度为 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询, 存储复杂度为 $\mathrm{O}(2^{2\ell}\cdot\ell)$ 个量子比特.

证明: 量子 DS-MITM 攻击过程与第 3.3 节类似, 不再赘述.

(1) 显然, 数据复杂度为 $\mathrm{O}(2^\ell)$ 个选择密文.

(2) 由于构造表 T_5' 和运行爪搜索算法 $(l = 2^\ell)$ 的时间复杂度分别为 $\mathrm{O}(2^{\ell/2}+2^\ell)\approx\mathrm{O}(2^\ell)$ 和 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询. 因此, 总的时间复杂度为 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询.

(3) 构造表 T_5' 和运行爪搜索算法筛选密钥 $(l = 2^\ell)$ 需要 $\mathrm{O}(2^{2\ell}\cdot\ell+2^\ell\cdot\ell)\approx\mathrm{O}(2^{2\ell}\cdot\ell)$ 个量子比特.

4 3-cell 型和 *n*-cell 型 GFS 的 (量子) DS-MITM 攻击

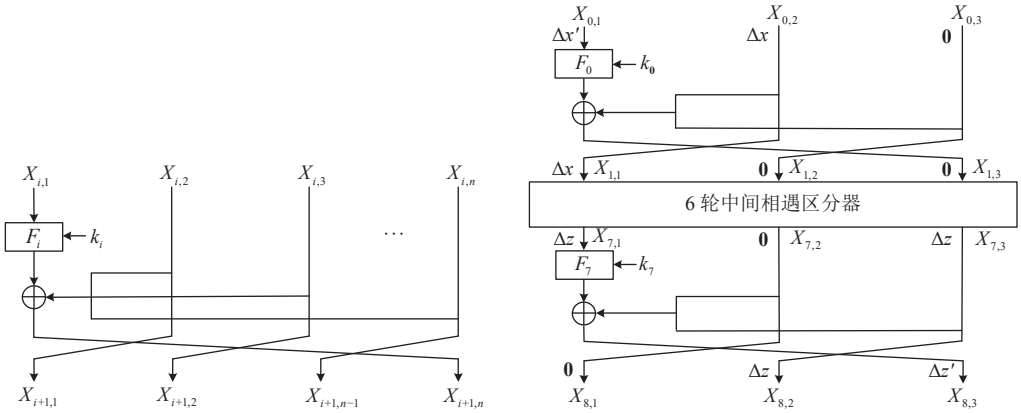
本节以 3-cell 型 GFS 为例探讨 n-cell 型 GFS 的 (量子) DS-MITM 攻击方案. 首先简要介绍 n-cell 型 GFS 的结

构特征, 其次, 利用多重集和差分枚举技术给出 3-cell 型 GFS 的 6 轮中间相遇区分器, 并在此基础上进行 8 轮 (量子) DS-MITM 攻击, 最后, 将上述相关结果推广至 n-cell 型 GFS, 并进行 $2(n+1)$ 轮 (量子) DS-MITM 攻击.

设 n-cell 型 GFS 的分组长度为 $n\ell$ 比特, 每个分支的输入长度为 ℓ 比特, 如图 5(a). 记 $X_i=(X_{i,1},X_{i,2},\ldots,X_{i,n})\in\mathbb{F}_2^{\ell\times n}$ 为第 i 轮的输入, $i\in\mathbb{N}$, 则有:

$$(X_{i+1,1},X_{i+1,2},\ldots,X_{i+1,n})=(X_{i,2},X_{i,3},\ldots,X_{i,n},F_i(k_i\oplus X_{i,1})\oplus X_{i,2}\oplus X_{i,3}\oplus\ldots\oplus X_{i,n}),$$

其中, $F_i=F(k_i\oplus X_{i,1})\in\mathbb{F}_2^{\ell}$ 为第 i 轮的轮函数, $k_i\in\mathbb{F}_2^{\ell}$ 为参与第 i 轮轮密钥.



(a) n-cell 型 GFS 的第 i 轮结构 (b) 3-cell 型 GFS 的 8 轮 DS-MITM 攻击

图 5 n-cell 型 GFS 的第 i 轮结构和 3-cell 型 GFS 的 8 轮 DS-MITM 攻击

4.1 3-cell 型 GFS 的 8 轮 (量子) DS-MITM 攻击

本节首先构造 3-cell 型 GFS 的 6 轮中间相遇区分器, 其次, 对其分别向前向后扩展 1 轮, 实现 8 轮 3-cell 型 GFS 的 (量子) DS-MITM 攻击, 并分析该攻击的复杂度.

4.1.1 3-cell 型 GFS 的 6 轮中间相遇区分器

构造 3-cell 型 GFS 的中间相遇区分器, 需要讨论在给定轮函数输入和输出差分时各轮内部状态的所有可能值, 具体见命题 2.

命题 2. 对于 6 轮 3-cell 型 GFS, 若给定 Δx, $\Delta z\in\mathbb{F}_2^{\ell}$, 选取一个输入对 $(A_0,A)\in\mathbb{F}_2^{3\ell\times 2}$ 满足 $\Delta A=A_0\oplus A=(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)$, 进行加密后得到输出对 $(B_0,B)\in\mathbb{F}_2^{3\ell\times 2}$ 且 $\Delta B=B_0\oplus B=(\Delta z,\mathbf{0}_\ell,\Delta z)$, 则有:

(1) 存在 $(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)\to(\Delta z,\mathbf{0}_\ell,\Delta z)$ 的一条 6 轮中间相遇区分器;

(2) 满足区分器第 1, 4 和 5 轮内部状态值的数量平均为 2^ℓ.

证明:

(1) 如图 6(a) 所示, 从加密方向考虑, 根据差分传播特性, 当输入差分为 $(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)$ 时, 由于 $\Delta F_1^I=\Delta x\neq\mathbf{0}_\ell$, 显然 $\Delta F_1^O\neq\mathbf{0}_\ell$, 记 $\Delta y=\Delta F_1^O$, 则 $\Delta F_4^I=\Delta F_5^I=\Delta y$. 从解密方向考虑, 当输出差分为 $(\Delta z,\mathbf{0}_\ell,\Delta z)$ 时, 根据差分传播规律, 有 $\Delta F_5^O=\Delta z$, $\Delta F_4^O=\Delta y\oplus\Delta z$. 由此可得一条满足 $(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)\to(\Delta z,\mathbf{0}_\ell,\Delta z)$ 的 6 轮中间相遇区分器.

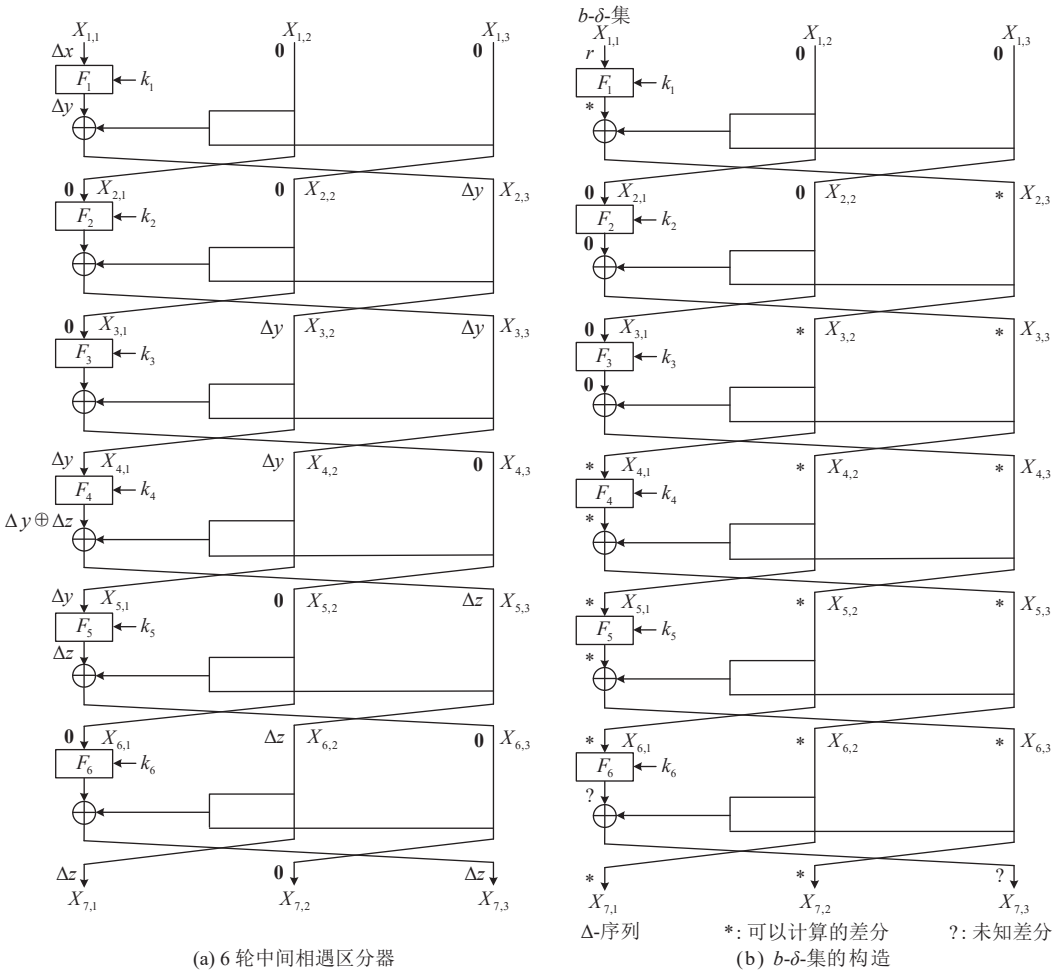
(2) 下面讨论区分器第 1、4 和 5 轮内部状态的可能值, 令 t_i 为第 i 轮轮函数的输入, 从加密方向可得:

$$\begin{cases}F_1(t_1)\oplus F_1(t_1\oplus\Delta x)=\Delta y\\ F_4(t_4)\oplus F_4(t_4\oplus\Delta y)=\Delta y\oplus\Delta z\\ F_5(t_5)\oplus F_5(t_5\oplus\Delta y)=\Delta z\end{cases}\tag{3}$$

由于轮函数内部仅有 S 盒会影响差分, 根据性质 1, 当公式 (3) 中的 Δx, Δz 给定, Δy 取固定值时, 轮函数的内部状态值 t_1, t_4 和 t_5 平均只有 1 个解. 由于 Δy 最多可取 2^ℓ 个值, 所以上述 3 个内部状态值的数量平均为 2^ℓ. 证毕.

下面利用区分器的输入对讨论 3-cell 型 GFS 的 Δ-序列 Γ_5 可能值的个数.

定理 3. 输入对 $(A_0, A) \in \mathbb{F}_2^{3\ell\times 2}$ 满足命题 2 中区分器的输入, 利用 A_0 构造 b-δ-集 $M = \{(A_0 \oplus (r, \mathbf{0}_\ell, \mathbf{0}_\ell)) \in \mathbb{F}_2^{3\ell} \mid r \in \{0, 1, \ldots, 2^b - 1\}\}$, 则可得 Δ-序列 $\Gamma_5 = (\Delta_1, \Delta_2, \ldots, \Delta_{2^b-1})$ 有 2^ℓ 个可能值.



(a) 6 轮中间相遇区分器 (b) b-δ-集的构造

图 6 3-cell 型 GFS 的 6 轮中间相遇区分器和 b-δ-集 的构造

证明: 如图 6(b) 所示, 设 $X_{1,1} \in \mathbb{F}_2^\ell$ 的 b 比特活跃, 输入对 $(A_0, A) \in \mathbb{F}_2^{3\ell\times 2}$ 的差分 $\Delta A = A_0 \oplus A = (r, \mathbf{0}_\ell, \mathbf{0}_\ell)$, 根据集合 M 可得 $2^b - 1$ 个输入对 $(A_0, A_0 \oplus (r, \mathbf{0}_\ell, \mathbf{0}_\ell))$, $r \in [2^b - 1]$, 将其加密 6 轮得到差分为 $\Delta X_7^r = (\Delta X_{7,1}^r, \Delta X_{7,2}^r, \Delta X_{7,3}^r)$ 的输出对. 则 $\Delta_r = \Delta X_{7,1}^r$ 的具体计算过程如下.

由加密流程可知:

第 1 轮: $\Delta F_1^O = F_1(t_1) \oplus F_1(t_1 \oplus r)$.

第 4 轮: $\Delta F_4^O = F_4(t_4) \oplus F_4(t_4 \oplus \Delta F_1^O)$.

第 5 轮: $\Delta F_5^O = F_5(t_5) \oplus F_5(t_5 \oplus \Delta F_1^O)$.

由此可得:

$$\begin{aligned}\Delta_r = \Delta X_{7,1}^r &= \Delta F_4^O \oplus \Delta F_1^O = (F_4(t_4) \oplus F_4(t_4 \oplus \Delta F_1^O)) \oplus (F_1(t_1) \oplus F_1(t_1 \oplus r)) \\ &= (F_4(t_4) \oplus F_4(t_4 \oplus F_1(t_1) \oplus F_1(t_1 \oplus r))) \oplus (F_1(t_1) \oplus F_1(t_1 \oplus r))\end{aligned} \tag{4}$$

当 r 取遍 $[2^b - 1]$ 时, 可得到 Δ-序列 $\Gamma_5 = (\Delta_1, \Delta_2, \ldots, \Delta_{2^b-1})$.

由公式 (4) 的最后一行可知, Δ_r 依赖于 t_1 和 t_4 的值, 又由公式 (3) 可知, t_4 由 t_1 决定. 而根据命题 2, t_1 有 2^ℓ 个

可能值, 故 Δ-序列 Γ_5 有 2^ℓ 个可能值. 证毕.

4.1.2 3-cell 型 GFS 的 8 轮 DS-MITM 攻击及复杂度分析

本节利用命题 2 构造的 6 轮中间相遇区分器, 分别向前向后扩展 1 轮, 实现 8 轮 3-cell 型 GFS 的 DS-MITM 攻击, 攻击包括预计算阶段和在线阶段, 具体过程见图 5(b).

预计算阶段: 详细过程如定理 3 所示, 并将 Δ-序列 Γ_5 的 2^ℓ 种可能值存储在表 T_9 中.

在线阶段: 包括数据收集和密钥恢复两部分.

1) 数据收集. 包括如下 3 个步骤.

(1.1) 任意选取两个向量 m, $a \in \mathbb{F}_2^\ell$, 如图 5(b) 所示, 构造满足区分器第 1 分支差分输入差分为 Δx 的两个明文集 $\{(0,m,a),\ldots,(2^\ell-1,m,a)\}$, $\{(0,m\oplus\Delta x,a),\ldots,(2^\ell-1,m\oplus\Delta x,a)\}$, 对应差分 $\Delta P=(\Delta x',\Delta x,\mathbf{0}_\ell)\in\mathbb{F}_2^{\ell\times 3}$, 将得到的 $2^{2\ell}$ 个明文对存储在表 T_P 中.

(1.2) 对任意 u_1, $u_2\in\mathbb{F}_2^\ell$, 将差分为 ΔP 的明文对 (u_1,m,a) 和 $(u_2,m\oplus\Delta x,a)$ 分别进行 8 轮加密得到 $2^{2\ell}$ 个差分为 $(\mathbf{0}_\ell,\Delta z,\Delta z')\in\mathbb{F}_2^{\ell\times 3}$ 的密文对, 并将其存储在表 T_C 中. 对于给定的 $\Delta x,\Delta z$, 由于 ΔP 和 ΔC 均以概率 $p_1=p_2=2^{-\ell}$ 分别传播到区分器的输入差分 $(\Delta x,\mathbf{0}_\ell,\mathbf{0}_\ell)$ 和输出差分 $(\Delta z,\mathbf{0}_\ell,\Delta z)$, 则 8 轮截断差分传播概率为 $p=2^{-2\ell}$. 因此, 至少有 $2^{-2\ell}\times 2^{2\ell}=1$ 个明密文对 (P_0,P) 和 (C_0,C) 满足图 5(b) 所示 $(\Delta x',\Delta x,\mathbf{0}_\ell)\to(\mathbf{0}_\ell,\Delta z,\Delta z')$ 的 8 轮差分特征.

(1.3) 根据步骤 (1.2) 得到的明文对 (P_0,P), 利用明文 $P_0=(X_{0,1}^0,X_{0,2}^0,X_{0,3}^0)$ 构造 b-δ-集 $G=\{P_r=(X_{0,1}^0\oplus\Delta F_0^l,X_{0,2}^0\oplus r,X_{0,3}^0)|r\in\{0,1,\ldots,2^b-1\},\ \Delta F_0^l\in\mathbb{F}_2^\ell\}$, 利用 G 构造明文对 (P_0,P_r), $r\in[2^b-1]$, 并进行 8 轮加密得到对应的密文对 (C_0,C_r), 因此得到 2^b-1 个明密文对满足图 5(b) 所示的 8 轮差分特征.

2) 密钥恢复. 包括如下 4 个步骤.

(2.1) 选取步骤 (1.3) 中的一个明文对 (P_0,P_r), 根据性质 1, 利用 $F(t_0)\oplus F(t_0\oplus\Delta x')=\Delta x$ 确定 t_0 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 t_0 的 2^b-1 个可能值存储在以 $(\Delta x',\Delta x,\mathbf{0}_\ell)$ 为索引的表 T_{10} 中, 再由 $k_0=t_0\oplus(X_{0,1}^0\oplus\Delta F_0^l)$ 确定子密钥 k_0 的 2^b-1 个可能值.

(2.2) 对每个 $r\in[2^b-1]$, 依次选取密文对 (C_0,C_r), $C_r=(X_{8,1}^r,X_{8,2}^r,X_{8,3}^r)$, 显然 $C_0\oplus C_r=(\mathbf{0}_\ell,\Delta z,\Delta z')$. 猜测子密钥 k_7 的值, 根据性质 1 和 $F(k_7\oplus X_{7,1}^r)=X_{8,1}^r\oplus X_{8,2}^r\oplus X_{8,3}^r$ 确定 $X_{7,1}^r$ 的唯一值. 当 r 取遍 $[2^b-1]$ 时, 将得到 $X_{7,1}^r$ 的 2^b-1 个可能值存储在以 $(\mathbf{0}_\ell,\Delta z,\Delta z')$ 为索引的表 T_{11} 中.

(2.3) 根据 k_7 的猜测值, 对步骤 (1.3) 得到的密文集 $\{C_0,C_1,\ldots,C_{2^b-1}\}$ 分别进行部分解密, 得到区分器输出处的可能值 $X_7^r=(X_{7,1}^r,X_{7,2}^r,X_{7,3}^r)\in\mathbb{F}_2^{\ell\times 3}$, $r\in\{0,1,\ldots,2^b-1\}$, 从而得到 Δ-序列 $\Gamma_6=(\Delta_1,\Delta_2,\cdots,\Delta_{2^b-1})$, 其中, $\Delta_r=X_{7,1}^0\oplus X_{7,1}^r$, $r\in[2^b-1]$.

(2.4) 将得到的 2^b-1 个明密文对 (P_0,P_r) 和 (C_0,C_r), 2^b-1 组子密钥 (k_0,k_7) 以及相应的 Δ-序列 $\Gamma_6=(\Delta_1,\Delta_2,\ldots,\Delta_{2^b-1})$ 存储在表 T_{12} 中. 类似地, 当 $b\geqslant 3$ 时, 检查表 T_9 和 T_{12} 中的 Δ-序列 是否匹配, 若匹配, 则猜测的子密钥 k_0 和 k_7 为正确密钥; 否则, 匹配不成功, 另外选取一对明文重复上述步骤 (2.1)–(2.4).

下面给出攻击的复杂度分析.

(1) 由于在线阶段构造了两个大小分别为 2^ℓ 的明文集, 故该攻击的数据复杂度为 $\mathrm{O}(2^\ell+2^\ell)\approx\mathrm{O}(2^\ell)$ 个选择明文.

(2) 由于预计算阶段构造表 T_9 和在线阶段猜测密钥所需的时间复杂度均为 $\mathrm{O}(2^{2\ell})$ 次 8 轮加密, 因此, 攻击所需的时间复杂度为 $\mathrm{O}(2^{2\ell})$ 次 8 轮加密.

(3) 存储表 T_9 和 T_{12} 所需的存储复杂度为 $\mathrm{O}(2^{2\ell})$ 个长度为 $(2^b-1)\ell$ 的比特块.

最后, 为了降低攻击的时间复杂度, 需要在 Q1 模型下对 3-cell 型 GFS 做量子并行运算, 此处我们给出该结构的 8 轮量子 DS-MITM 攻击及复杂度分析, 具体见定理 4.

定理 4. 利用命题 2 构造的中间相遇区分器可对 3-cell 型 GFS 进行 8 轮量子 DS-MITM 攻击, 数据复杂度为 $\mathrm{O}(2^\ell)$ 个选择密文, 时间复杂度为 $\mathrm{O}(2^{3\ell/2}\cdot\ell)$ 次量子查询, 存储复杂度为 $\mathrm{O}(2^{2\ell}\cdot\ell)$ 个量子比特.

证明: 量子 DS-MITM 攻击过程与第 3.3 节类似, 不再赘述.

(1) 显然, 数据复杂度为 $O(2^{\ell})$ 个选择密文.

(2) 由于构造表 T'_9 和运行爪搜索算法 $(l=2^{\ell})$ 的时间复杂度分别为 $O(2^{\ell/2}+2^{\ell})\approx O(2^{\ell})$ 和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 因此, 总的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询.

(3) 构造表 T'_9 和运行爪搜索算法筛选密钥 $(l=2^{\ell})$ 需要 $O(2^{2\ell}\cdot\ell+2^{\ell}\cdot\ell)\approx O(2^{2\ell}\cdot\ell)$ 个量子比特.

4.2 *n*-cell 型 GFS 的 DS-MITM 攻击和量子 DS-MITM 攻击

本节将第 4.1 节的相关结论推广至 n-cell 型 GFS. 具体地, 在预计算阶段分别固定输入和输出差分 $(\Delta x,\mathbf{0}_{\ell},\mathbf{0}_{\ell},\mathbf{0}_{\ell},\ldots,\mathbf{0}_{\ell})$ 和 $(\Delta z,\mathbf{0}_{\ell},\Delta z,\mathbf{0}_{\ell},\ldots,\mathbf{0}_{\ell})$, Δx, $\Delta z\in\mathbb{F}_2^{\ell}$, 与命题 2 类似, 可得到一类 $2n$ 轮中间相遇区分器, 对其分别向前向后扩展 1 轮进行 $2(n+1)$ 轮 DS-MITM 攻击, 并在 Q1 模型下对该结构进行 $2(n+1)$ 轮量子 DS-MITM 攻击. 分析过程与第 4.1 节一致, 故不再详细叙述, 仅给出复杂度分析.

n-cell 型 GFS 的 $2(n+1)$ 轮 DS-MITM 攻击的复杂度:

(1) 数据复杂度为 $O(2^{\ell})$ 个选择明文.

(2) 由于预计算阶段构造的存储 Δ-序列 的表 T_{13} 和在线阶段猜测密钥所需的时间复杂度均为 $O(2^{2\ell})$ 次 $2(n+1)$ 轮加密, 因此, 攻击所需的时间复杂度为 $O(2^{2\ell})$ 次 $2(n+1)$ 轮加密.

(3) 存储表 T_{13} 和 T_{14} 所需的存储复杂度为 $O(2^{2\ell})$ 个长度为 $(2^b-1)\ell$ 的比特块, 其中, 表 T_{14} 存储在线阶段得到的 Δ-序列.

n-cell 型 GFS 的 $2(n+1)$ 轮量子 DS-MITM 攻击的复杂度:

(1) 数据复杂度为 $O(2^{\ell})$ 个选择明文.

(2) 由于构造表 T'_{13} 和运行爪搜索算法 $(l=2^{\ell})$ 的时间复杂度分别为 $O(2^{\ell/2}+2^{\ell})\approx O(2^{\ell})$ 和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询, 因此, 该攻击所需要的总的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询.

(3) 构造表 T'_{13} 和运行爪搜索算法筛选密钥 $(l=2^{\ell})$ 需要 $O(2^{2\ell}\cdot\ell+2^{3\ell/2}\cdot\ell)\approx O(2^{2\ell}\cdot\ell)$ 个量子比特.

5 总 结

本文研究了 3 类 GFS 的 DS-MITM 攻击, 并在 Q1 模型下对 3 类 GFS 进行了量子 DS-MITM 攻击. 首先, 针对 3 分支 Type-III 型 GFS, 采用多重集和差分枚举技术构造了 4 轮中间相遇区分器, 并利用 Grover 算法和量子爪搜索算法对其进行了 6 轮量子 DS-MITM 攻击, 攻击的时间复杂度为 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 其次, 对 3 分支 Type-I 型 GFS 的 9 轮中间相遇区分器分别进行了 11 轮 DS-MITM 攻击和量子 DS-MITM 攻击, 相应的时间复杂度分别为 $O(2^{2\ell})$ 次 11 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 最后, 对 n-cell 型 GFS 进行了 $2(n+1)$ 轮 DS-MITM 攻击和量子 DS-MITM 攻击, 且攻击所需要的时间复杂度分别为 $O(2^{2\ell})$ 次 $2(n+1)$ 轮加密和 $O(2^{3\ell/2}\cdot\ell)$ 次量子查询. 结果表明, 本文提出的量子 DS-MITM 攻击有效降低了经典 DS-MITM 攻击的复杂度. 然而遗憾的是, 本文的方法在应用于 n 分支 Type-I/III 型 GFS 时仍有局限性, 未来我们希望通过借助其他工具分析其 DS-MITM 攻击效果, 并通过量子算法更好地降低时间复杂度.

References

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

[2] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1): 3–72. [doi: 10.1007/BF00630563]

[3] 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]

[4] Choy J, Chew G, Khoo K, Yap H. Cryptographic properties and application of a generalized unbalanced Feistel network structure. In: Boyd C, González Nieto J, eds. Proc. of the 14th Australasian Conf. on Information Security and Privacy. Brisbane: Springer, 2009. 73–89. [doi: 10.1007/978-3-642-02620-1_6]

[5] Diffie W, Hellman ME. Special feature exhaustive cryptanalysis of the NBS data encryption standard. Computer, 1977, 10(6): 74–84. [doi: 10.1109/C-M.1977.217750]

[6] Demirci H, Selçuk AA. A meet-in-the-middle attack on 8-round AES. In: Nyberg K, ed. Proc. of the 15th Int'l Workshop on Fast Software Encryption. Lausanne: Springer, 2008. 116–126. [doi: 10.1007/978-3-540-71039-4_7]

[7] Daemen J, Rijmen V. The block cipher Rijndael. In: Quisquater JJ, Schneier B, eds. Proc. of the 3rd Int'l Conf. on Smart Card Research and Applications. Louvain-la-Neuve: Springer, 2000. 277–284. [doi: 10.1007/10721064_26]

[8] Dunkelman O, Keller N, Shamir A. Improved single-key attacks on 8-round AES-192 and AES-256. Journal of Cryptology, 2015, 28(3): 397–422. [doi: 10.1007/s00145-013-9159-4]

[9] Ren JJ, Hou ZZ, Li MM, Lin DD, Chen SZ. Improved meet-in-the-middle attacks on reduced-round MIBS-80 cipher. Journal of Electronics & Information Technology, 2022, 44(8): 2914–2923 (in Chinese with English abstract). [doi: 10.11999/JEIT210441]

[10] Du XN, Sun R, Zheng YN, Liang LF. Improved meet-in-the-middle attacks on reduced-round E2. Journal of Electronics & Information Technology, 2024, 46(6): 2655–2662 (in Chinese with English abstract). [doi: 10.11999/JEIT230655]

[11] Du XN, Zheng YN, Liang LF, Li KB. Meet-in-the-middle attack on RAIN-128. Journal of Electronics & Information Technology, 2024, 46(1): 327–334 (in Chinese with English abstract). [doi: 10.11999/JEIT221593]

[12] Guo J, Jean J, Nikolic I, Sasaki Y. Meet-in-the-middle attacks on generic Feistel constructions. In: Sarkar P, Iwata T, eds. Advances in Cryptology—ASIACRYPT 2014. Kaoshiung: Springer, 2014. 458–477. [doi: 10.1007/978-3-662-45611-8_24]

[13] Dong L, Mao YX. Meet-in-the-middle attacks on 3-line generalized Feistel networks. 2017. https://eprint.iacr.org/2017/1071.pdf

[14] Deng YH, Jin CH, Zhao JQ. Meet-in-the-middle attack on Type-3 Feistel structure. Journal of Cryptologic Research, 2019, 6(1): 27–36 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000280]

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

[17] Buhrman H, Durr C, Heiligman M, Høyer P, Magniez F, Santha M, De Wolf R. Quantum algorithms for element distinctness. In: Proc. of the 16th Annual IEEE Conf. on Computational Complexity. Chicago: IEEE, 2001. 131–137. [doi: 10.1109/CCC.2001.933880]

[18] Zhandry M. How to construct quantum random functions. In: Proc. of the 53rd IEEE Annual Symp. on Foundations of Computer Science. New Brunswick: IEEE, 2012. 679–687. [doi: 10.1109/FOCS.2012.37]

[19] Kaplan M, Leurent G, Leverrier A, Naya-Plasencia M. Quantum differential and linear cryptanalysis. IACR Trans. on Symmetric Cryptology, 2016, 2016(1): 71–94. [doi: 10.13154/tosc.v2016.i1.71-94]

[20] 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]

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

[22] 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]

[23] Hodžić S, Ramkilde LK, Kidmose AB. On quantum distinguishers for Type-3 generalized Feistel network based on separability. In: Ding JT, Tillich JP, eds. Proc. of the 11th Int'l Conf. on Post-quantum Cryptography. Paris: Springer, 2020. 461–480. [doi: 10.1007/978-3-030-44223-1_25]

[24] Yu B, Sun B, Liu GQ, Luo YY, Zhang ZY. Quantum cryptanalysis on some generalized unbalanced Feistel networks. Journal of Cryptologic Research, 2021, 8(6): 960–973 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000490]

[25] Li YJ, Lin H, Yi ZH, Xie HQ. Quantum cryptanalysis of MIBS. Journal of Cryptologic Research, 2021, 8(6): 989–998 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000492]

[26] 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]

[27] Li HW, Yang L. Quantum differential cryptanalysis to the block ciphers. In: Proc. of the 6th Int'l Conf. on Applications and Techniques in Information Security. Beijing: Springer, 2015. 44–51. [doi: 10.1007/978-3-662-48683-2_5]

[28] Hosoyamada A, Sasaki Y. Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In: Catalano D, De Prisco R, eds. 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]

[29] Wang P, Chen XM, Jiang GH. Quantum Demiric-Selçuk meet-in-the-middle attacks on reduced-round AES. Int'l Journal of Theoretical Physics, 2022, 61(1): 5. [doi: 10.1007/s10773-022-05003-2]

[30] Xu YS, Yuan Z. Quantum meet-in-the-middle attack on Feistel construction. Quantum Information Processing, 2023, 22(3): 155. [doi: 10.

1007/s11128-022-03715-2]

[31] Zou J, Huang KR, Zhu M, Zou HK, Luo YY, Liu Q. New Demiric-Selçuk meet-in-the-middle attacks on Misty and Feistel schemes. Quantum Information Processing, 2024, 23(4): 136. [doi: 10.1007/s11128-024-04349-2]

[32] Matsui M. New block encryption algorithm MISTY. In: Biham E, ed. Proc. of the 4th Int'l Workshop on Fast Software Encryption. Haifa: Springer, 1997. 54–68. [doi: 10.1007/BFb0052334]

[33] Ren JJ, Chen SZ. Meet-in-the-middle attack on 11-round 3D cipher. Journal on Communications, 2015, 36(8): 182–191 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000-436x.2015131]

附中文参考文献

[9] 任炯炯, 侯泽洲, 李曼曼, 林东东, 陈少真. 改进的减轮 MIBS-80 密码的中间相遇攻击. 电子与信息学报, 2022, 44(8): 2914–2923. [doi: 10.11999/JEIT210441]

[10] 杜小妮, 孙瑞, 郑亚楠, 梁丽芳. 改进的减轮 E2 算法中间相遇攻击. 电子与信息学报, 2024, 46(6): 2655–2662. [doi: 10.11999/JEIT230655]

[11] 杜小妮, 郑亚楠, 梁丽芳, 李锴彬. RAIN-128 算法的中间相遇攻击. 电子与信息学报, 2024, 46(1): 327–334. [doi: 10.11999/JEIT221593]

[14] 邓元豪, 金晨辉, 赵杰卿. Type-3 型广义 Feistel 结构的中间相遇攻击. 密码学报, 2019, 6(1): 27–36. [doi: 10.13868/j.cnki.jcr.000280]

[24] 于博, 孙兵, 刘国强, 罗宜元, 张志宇. 若干广义非平衡 Feistel 结构的量子分析研究. 密码学报, 2021, 8(6): 960–973. [doi: 10.13868/j.cnki.jcr.000490]

[25] 李艳俊, 林昊, 易子晗, 谢惠琴. MIBS 算法量子密码分析. 密码学报, 2021, 8(6): 989–998. [doi: 10.13868/j.cnki.jcr.000492]

[26] 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]

[33] 任炯炯, 陈少真. 11 轮 3D 密码算法的中间相遇攻击. 通信学报, 2015, 36(8): 182–191. [doi: 10.11959/j.issn.1000-436x.2015131]

作者简介

杜小妮, 博士, 教授, 博士生导师, 主要研究领域为密码学, 信息安全.

吴家辉, 硕士生, 主要研究领域为密码学, 信息安全.

徐莹, 硕士生, 主要研究领域为密码学, 信息安全.

孙瑞, 硕士生, 主要研究领域为密码学, 信息安全.