轻量级分组密码 Piccolo 的量子密码分析

杜小妮[1,2]，王香玉[1]，梁丽芳[1]，李锴彬[3]

（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；
3. 西北师范大学计算机科学与工程学院，甘肃 兰州 730070）

摘 要：根据 Piccolo 算法 RP 置换的结构特点，提出 3 轮量子区分器，并用 Grover meets Simon 算法进行 6 轮量子密钥恢复攻击。分析结果表明，该攻击可恢复密钥 56 bit，时间复杂度为 2^{28}，共需量子比特数为 464；当攻击轮数大于 6 轮时，时间复杂度为 $2^{28+16(r-6)}$，降至 Grover 量子暴力搜索的 $\frac{1}{2^{68}}$。与传统差分和线性分析相比，所提攻击方法时间复杂度更低，且较 Grover 暴力搜索的时间复杂度大幅降低，为后续轻量级分组密码的量子攻击的研究奠定了基础。

关键词：量子密码分析；Piccolo 算法；Grover 算法；Simon 算法

中图分类号：TP309.7

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2023109

Quantum cryptanalysis of lightweight block cipher Piccolo

DU Xiaoni[1,2], WANG Xiangyu[1], LIANG Lifang[1], LI Kaibin[3]

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
3. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China

Abstract: By taking the characteristics of the structure of Piccolo algorithm RP permutation into consideration, a 3-round quantum distinguisher was proposed. Based on Grover meets Simon algorithm, the 6-round of quantum key recovery attack was given. The results show that the key can be recovered 56 bit with the time complexity 2^{28} and the occupation of 464 qubit. Moreover, if attack rounds r>6，the time complexity is $2^{28+16(r-6)}$, which is $\frac{1}{2^{68}}$ of Grover quantum brute-force search. The time complexity of the proposed attack method is significantly reduced compared with Grover search and is also better than that of traditional cryptanalysis, which lays a foundation for the subsequent research on quantum attacks of lightweight block ciphers.

Keywords: quantum cryptanalysis, Piccolo algorithm, Grover algorithm, Simon algorithm

0 引言

随着信息技术、计算机技术以及微电子技术的高速发展，射频识别（RFID, radio frequency identification）技术、传感器网络、非接触式智能卡等的应用愈加广泛，为了保护这类资源受限设备所传输、处理的数据，轻量级分组密码算法应运而生。该类算法主要采用 Feistel 结构或代换置换网络（SPN, substitution-permutation network）结构。广义 Feistel 结构（GFS, generalized Feistel structure）是 Feistel 结构的变体形式，其加解密一致，且通常采用 4 分支、8 分支等多分支非平衡 Feistel 结构，通过不同的置换替换循环移位以减少迭代轮数。Piccolo 算法是 Shibutani 等[1]提出的轻量级分组密

收稿日期：2023−01−19；**修回日期：**2023−04−08

基金项目：国家自然科学基金资助项目（No.62172337）；甘肃省自然科学基金重点资助项目（No.23JRRA685）

Foundation Items: The National Natural Science Foundation of China (No.62172337), Key Project of Gansu Natural Science Foundation (No.23JRRA685)

码算法，其采用改进的 4 分支 GFS，具有硬件实现效率高、成本和能耗较低等优点。现有研究表明，该算法具有足够的安全性以抵抗多种传统密码分析[2-8]。

量子搜索算法给现代密码体系带来了挑战和威胁。在 STOC 1996 上，Grover[9]提出的 Grover 算法实现了对经典搜索效率的二次加速，提高了密码破译的效率。随后，Simon[10]首次提出了一种能在多项式时间内求出周期布尔函数周期的算法，称为 Simon 算法，为后续量子密码分析的研究奠定了基础。

根据 Zhandry 等[11]提出的量子环境中伪随机函数（PRF, pseudo random function）安全性的概念，Kaplan 等[12]针对对称密码提出了 2 种量子密码分析模型：标准安全性模型（简称 Q1 模型）和量子安全性模型（简称 Q2 模型）。在 Q2 模型中，攻击者可以以量子叠加态的方式来询问预言机，并获得相应的输出叠加态。

目前，在 Q2 模型下，已经出现了很多针对 Feistel 结构或 GFS 的安全性分析成果。例如，Kuwakado 和 Morii[13]首次提出 3 轮 Feistel 结构周期函数的构造方法，并将其作为量子区分器，用 Simon 算法找到该函数的周期。Leander 和 May[14]在 ASIACRYPT 2017 上提出了针对 FX 结构的 Grover meets Simon 算法。基于该搜索算法，Dong 等[15-17]给出 Feistel 结构以及 GFS 的量子区分器的构造方法，证明了针对这些结构的量子密码分析的时间复杂度均优于 Grover 量子暴力搜索。倪博煜等[18]提出针对改进的 Type-1 型 GFS 的量子攻击，并将其应用于分组密码 CAST-256。尤启迪等[19]对 SMS4-like 结构和 NBC 算法进行了量子密码分析。于博等[20]提出了对若干非平衡 GFS 的量子密码分析。钱新等[21]首次给出对 MARS-like 结构的量子算法攻击。李艳俊等[22-23]在考虑轮函数内部结构的情况下分别对 MIBS 和 Camellia 算法提出 5 轮量子区分器，并进行了 7 轮量子密钥恢复攻击，之后，李艳俊等[24]又在改进的 Type-Ⅱ型 GFS 的基础上，对轻量级密码 TWINE-128 进行了量子密码分析。

分组密码的量子密码分析主要分为量子选择明文攻击（qCPA, quantum chosen-plaintext attack）和量子选择密文攻击（qCCA, quantum chosen-ciphertext attack）。本文在 Q2 模型下进行量子选择明文攻击，主要贡献如下。

1) 根据轻量级分组密码 Piccolo 算法的结构特点，基于 Simon 算法提出 3 轮量子区分器。

2) 基于 Grover meets Simon 算法，引入量子密钥恢复方法。采用本文所提的 3 轮量子区分器对 Piccolo 算法进行 6 轮量子密钥恢复攻击，猜测密钥为 56 bit，时间复杂度为 2^{28}；当攻击轮数大于 6 轮时，时间复杂度为 $2^{28+16(r-6)}$，较 Grover 量子暴力搜索的时间复杂度有显著降低。

1 预备知识

本节首先给出必要的符号说明，其次介绍 Piccolo 算法的加密流程，简单叙述该算法的轮函数、RP 置换等结构。

1.1 符号说明

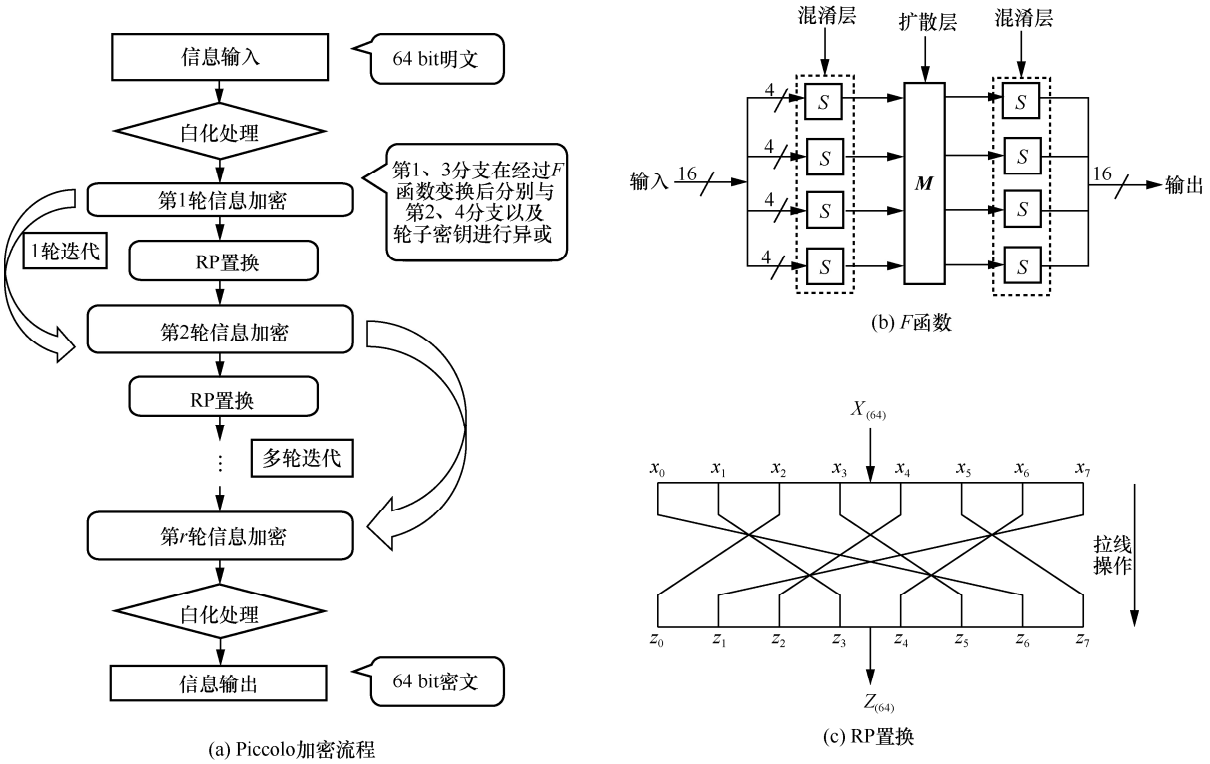
本文使用的主要符号及其含义如表 1 所示。

表 1 主要符号及其含义

符号	含义
X_0^j	第 j 分支的输入
X_i^j	第 i 轮输出后第 j 分支上的值
$X_{(64)}$	输入的 64 bit 明文
$Y_{(64)}$	输出的 64 bit 密文
$Z_{(64)}$	RP 置换的 64 bit 输出
F	轮函数
F_i	第 i 轮的轮函数
x_j	RP 置换第 j 字节输入
z_j	RP 置换第 j 字节输出
x_i^j	第 $i+1$ 轮第 j 分支的输入
k_i	第 i 轮的轮子密钥
rk_m	轮子密钥 ($0 \leqslant m \leqslant 2r, r$ 为迭代轮次)
wk_l	白化密钥 ($l = 0,1,2,3$)

1.2 Piccolo 算法

Piccolo 算法[1]采用改进的 4 分支 GFS，利用字节向量置换代替 4 分支 GFS 的块循环移位，如图 1 所示。算法分组长度为 64 bit，密钥长度为 80 bit 和 128 bit，分别记为 Piccolo-80 和 Piccolo-128，迭代轮数 r 分别为 25 轮和 31 轮。轮函数 F 采用 SPS（substitution-permutation-substitution）结构，其中，混淆层由 4 个四进四出的 S 盒构成，扩散层的扩散矩阵为 $\boldsymbol{M}$。该算法每两轮之间采用 RP 置换以提高算法的扩散性。RP 置换的输入、输出对应关系如下



(a) Piccolo加密流程

图 1　Piccolo 算法

$$z_0 = x_2, z_1 = x_7, z_2 = x_4, z_3 = x_1,$$

$$z_4 = x_6, z_5 = x_3, z_6 = x_0, z_7 = x_5$$

自 Piccolo 算法提出以来，研究者们致力于采用传统密码分析方法对其进行攻击，本文提出了针对 Piccolo 算法的量子攻击方法，表 2 给出了传统密码分析与量子攻击的结果对比，其中，时间复杂度在传统密码分析中代表加密次数，在量子攻击中代表量子查询次数。

表 2　对 Piccolo 算法进行传统密码分析与量子攻击的结果对比

攻击方法	攻击轮数/轮	时间复杂度/次
中间相遇攻击[2]	14	2^{73}
不可能差分分析[3]	12	$2^{55.18}$
中间相遇攻击[5]	14	$2^{75.39}$
改进的中间相遇攻击[6]	14	$2^{67.44}$
线性分析[7]	8	2^{70}
中间相遇攻击[8]	13	$2^{67.39}$
量子攻击	6	2^{28}

2　量子密码分析

本节首先介绍了 Grover 算法和 Simon 算法；其次，基于 Simon 算法阐述了构造针对 Feistel 结构的 3 轮量子区分器的方法，并给出 5 轮量子密钥恢复攻击的过程。

2.1　量子搜索算法

2.1.1　Grover 算法和 Simon 算法

Grover 算法。设搜索空间元素个数为 $N = 2^n$，$x \in F_2^n$，目标是找到唯一的解 $x_0 \in x$，使 $f(x) = 1$。在经典搜索下，找到解 x_0 的时间复杂度为 $O(2^n)$，而 Grover 算法可以实现对经典搜索效率的二次加速，即所需时间复杂度仅约为 $O\left(2^{\frac{n}{2}}\right)$。Grover 算法的详细步骤可参考文献[9]。

Simon 算法。给定布尔函数 $f:\{0,1\}^n \to \{0,1\}^n$，满足 $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0, s\}$，即函数 f 存在周期 s，目标是找到该周期 s。在经典搜索下，找到周期 s 的最优时间复杂度为 $O\left(2^{\frac{n}{2}}\right)$，而 Simon 量子搜索算法可以提供指数级加速，其所需时间复杂度仅为 $O(n)$。Simon 算法的详细步骤可参考文献[10]。

2.1.2　Grover meets Simon 算法

Leander 等[14]提出的 Grover meets Simon 算法用于破解 FX 结构的分组密码。FX 结构如图 2 所示，其中，k_0, k_1, k_2 为加密密钥。

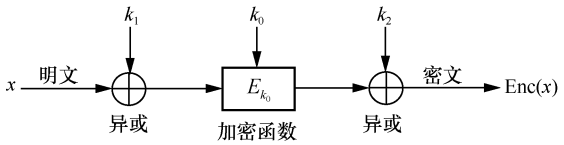


图 2 FX 结构

Leander 等[14]构造了函数 $f(k,x)=\mathrm{Enc}(x)\oplus E_k(x)$，其中，$\mathrm{Enc}(x)=E_{k_0}(x\oplus k_1)\oplus k_2$。当密钥猜测正确（即 $k=k_0$）时，对所有的 x 都有 $f(k_0,x)=f(k_0,x\oplus k_1)$；当密钥猜测错误（即 $k\neq k_0$）时，$f(k,\bullet)$ 大概率不是周期函数。

2.2 Feistel 结构的 3 轮量子区分器及其 5 轮量子密钥恢复攻击

文献[13]中针对 3 轮 Feistel 结构构造周期函数方法如下。

设输入明文为 $(X_0^1\,\|\,X_0^2)$，$\alpha_0,\alpha_1\in\{0,1\}^n$ 为任意常数，且 $\alpha_0\neq\alpha_1$，令函数 $f:\{0,1\}\times\{0,1\}^n\to\{0,1\}^n$，则

$$f(b,x)=\begin{cases}\alpha_0\oplus X_3^2=F_2(X_0^2\oplus F_1(\alpha_0)),b=0\\ \alpha_1\oplus X_3^2=F_2(X_0^2\oplus F_1(\alpha_1)),b=1\end{cases}$$

其中，$(X_3^1,X_3^2)=\mathrm{Enc}(X_0^1,X_0^2)=\mathrm{Enc}(\alpha_b,X_0^2)$。

显然 $f(b,x)=f(b\oplus 1,x\oplus F_1(\alpha_0)\oplus F_1(\alpha_1))$，即周期 $s=(1,F_1(\alpha_0)\oplus F_1(\alpha_1))$，通过 Simon 算法可在多项式时间内求得该周期 s。文献[13]所给出的 3 轮量子区分器如图 3 所示。

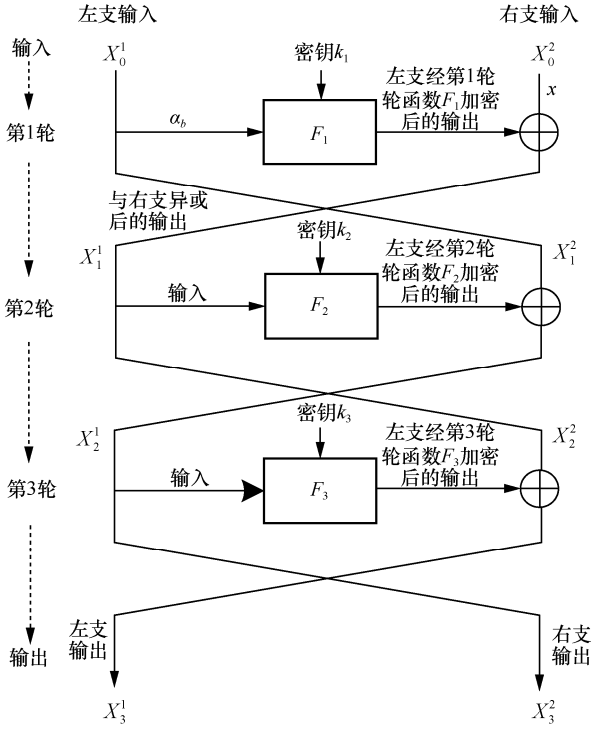


图 3 3 轮量子区分器

基于该 3 轮量子区分器可进行 5 轮量子密钥恢复攻击，如图 4 所示，需猜测密钥 (k_4,k_5)，则函数 f 可表示为

$$f(b,X_0^2)=\alpha_b\oplus X_3^2=$$
$$\alpha_b\oplus F_4(k_4,F_5(k_5,X_5^2)\oplus X_5^1)\oplus X_5^2$$

其中，$(X_5^1,X_5^2)=\mathrm{Enc}(\alpha_b,X_0^2)$。

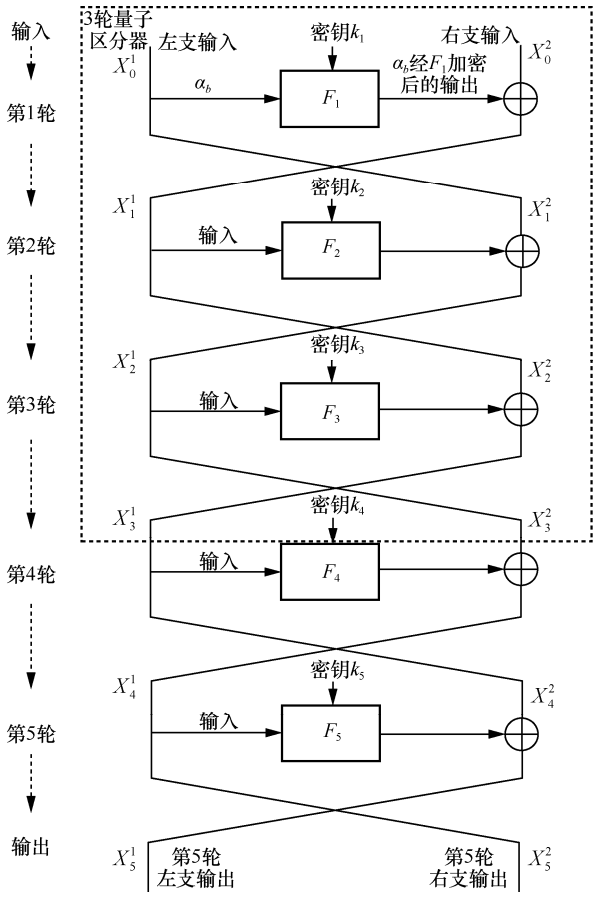


图 4 5 轮量子密钥恢复攻击

当密钥 (k_4,k_5) 猜测正确时，$f(b,X_0^2)$ 存在周期 $s=(1,F_1(k_1,\alpha_0)\oplus F_1(k_1,\alpha_1))$；当密钥 (k_4,k_5) 猜测错误时，$f(b,X_0^2)$ 大概率不是周期函数。Dong 等[15]采用 Leander[14]提出的 Grover meets Simon 算法，在 $2^{\frac{n}{2}}$ 次量子查询下恢复密钥 (k_4,k_5)。

3 Piccolo 算法的量子密码分析

本节首先将 Piccolo 算法结构进行细化；其次，基于 Simon 算法在细化结构的基础上找到了 3 轮量子区分器，并对其进行 6 轮量子密钥恢复攻击。

3.1 结构细化

Piccolo 算法的 RP 置换采用字节向量置换替代

4 分支 GFS 的块循环移位（如图 1 所示），因此将算法结构进行细化，以便介绍量子密钥恢复攻击的整个过程。Piccolo 算法细化加密流程如图 5 所示，将 Piccolo 算法的 4 分支输入/输出细化为 8 分支输入/输出（每个分支为 8 bit），分组长度为 64 bit。其中，F^i 为经 F 轮函数变换后输出的左半部分 $(i=1)$ 或右半部分 $(i=2)$；rk_m^i 和 wk_l^i 分别为轮子密钥、白化密钥的左半部分 $(i=1)$ 或右半部分 $(i=2)$，其中，$0\leqslant m\leqslant 2r$，$l=0,1,2,3$。

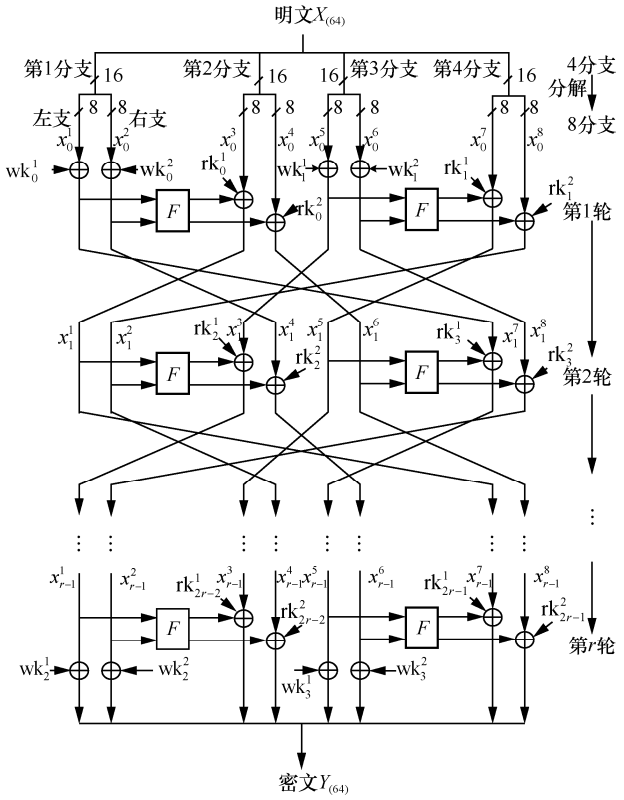


图 5　Piccolo 算法细化加密流程

3.2　Piccolo 算法的 3 轮量子区分器

本节在 3.1 节基础上，基于 Simon 算法找到了 Piccolo 算法的 3 轮量子区分器，如图 6 所示。(x_1^1,x_1^2) 经第 2 轮左侧轮函数变换后的输出可以表示为

$$F^2(x_1^1,x_1^2)=F^2(F^1(x_0^1,x_0^2)\oplus x_0^3\oplus rk_0^1,F^2(x_0^5,x_0^6)\oplus x_0^8\oplus rk_1^2)=rk_2^2\oplus x_0^2\oplus x_3^8$$

设 $x_0^2=\alpha_b,b\in\{0,1\}$，且 $\alpha_0\neq\alpha_1,x_0^3=x,x_0^1,x_0^4,x_0^5,x_0^6,x_0^7,x_0^8$ 为常数，则对 Piccolo 算法可以构造如下周期函数

$$f:\{0,1\}\times\{0,1\}^8\to\{0,1\}^8$$
$$b,x_0^3\mapsto\alpha_b\oplus x_3^8$$
$$f(b,x)=F^2(F^1(x_0^1,\alpha_b)\oplus x\oplus rk_0^1$$
$$F^2(x_0^5,x_0^6)\oplus x_0^8\oplus rk_1^2)\oplus rk_2^2$$

其中，$(x_3^1,x_3^2,\cdots,x_3^8)=\mathrm{Enc}(x_0^1,\alpha_b,x_0^3,x_0^4,\cdots,x_0^8)$。则可验证

$$f(b,x)=f(b\oplus 1,x\oplus F^1(x_0^1,\alpha_0)\oplus F^1(x_0^1,\alpha_1))$$

即函数 $f(b,x)$ 为周期函数，周期长度为 9 bit，且周期 $s=1\|F^1(x_0^1,\alpha_0)\oplus F^1(x_0^1,\alpha_1)$，通过 Simon 算法可在多项式时间内获得周期 s。

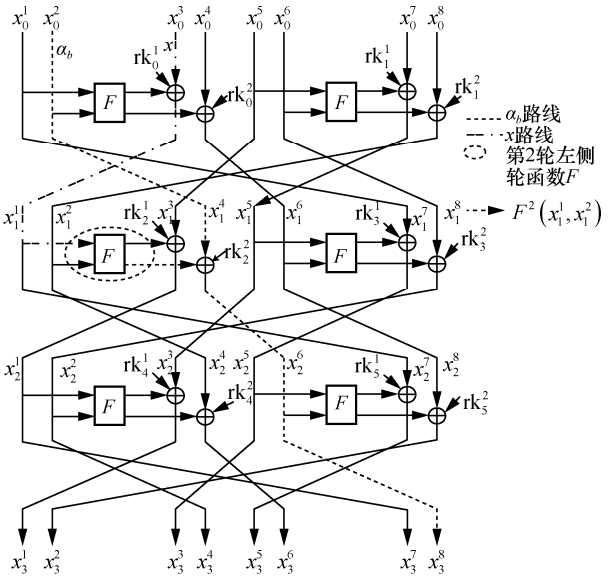


图 6　Piccolo 算法的 3 轮量子区分器

3.3　Piccolo 算法的 6 轮量子密钥恢复攻击

本节在 qCPA 条件下，基于所提 3 轮量子区分器采用 Grover meets Simon 算法对 Piccolo 算法进行量子密钥恢复攻击。Piccolo 算法的 6 轮量子密钥恢复攻击如图 7 所示，需要用 Grover 猜测的密钥数共 56 bit。

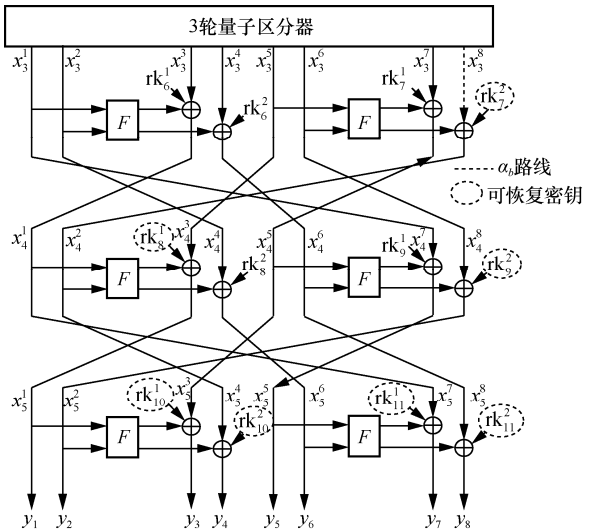


图 7　Piccolo 算法的 6 轮量子密钥恢复攻击

为了便于描述，本文用 k^* 表示需要猜测的密钥 $(\mathrm{rk}_7^2,\mathrm{rk}_8^1,\mathrm{rk}_9^2,\mathrm{rk}_{10}^1,\mathrm{rk}_{10}^2,\mathrm{rk}_{11}^1,\mathrm{rk}_{11}^2)$，即 $k^*=(\mathrm{rk}_7^2,\mathrm{rk}_8^1,\mathrm{rk}_9^2,\mathrm{rk}_{10}^1,\mathrm{rk}_{10}^2,\mathrm{rk}_{11}^1,\mathrm{rk}_{11}^2)$。其中，$y_i(i=1,2,\cdots,8)$ 为第 6 轮（未经 RP 置换）的输出值，且 $(y_1,y_2,\cdots,y_8)=\mathrm{Enc}(x_0^1,\alpha_b,x_0^3,x_0^4,\cdots,x_0^8)$。

根据 Piccolo 算法的 3 轮量子区分器，向下扩展 3 轮，将 x_3^8 用 y_i 表示，即可定义如下函数

$$\begin{aligned}&R(b,x_0^3)=\alpha_b\oplus x_3^8=\\&\alpha_b\oplus\mathrm{rk}_7^2\oplus\mathrm{rk}_{10}^2\oplus y_4\oplus F^2(y_1,y_2)\oplus F^2(\mathrm{rk}_8^1\oplus\\&y_1\oplus F^1(\mathrm{rk}_{11}^1\oplus y_7\oplus F^1(y_5,y_6),\mathrm{rk}_{10}^2\oplus y_4\oplus\\&F^2(y_1,y_2)),\mathrm{rk}_9^2\oplus y_2\oplus F^2(\mathrm{rk}_{10}^1\oplus y_3\oplus\\&F^1(y_1,y_2),\mathrm{rk}_{11}^2\oplus y_8\oplus F^2(y_5,y_6)))\end{aligned}$$

Piccolo 算法的 6 轮量子密钥恢复结果如定理 1 所示。

定理 1 令 $g:F_2^{(8)^7}\times F_2^{8+1}\to F_2^8$，且 $(k^*,z)\mapsto R(z)=\alpha_b\oplus\mathrm{rk}_7^2\oplus\mathrm{rk}_{10}^2\oplus y_4\oplus F^2(y_1,y_2)\oplus F^2(\mathrm{rk}_8^1\oplus y_1\oplus F^1(\mathrm{rk}_{11}^1\oplus y_7\oplus F^1(y_5,y_6),\mathrm{rk}_{10}^2\oplus y_4\oplus F^2(y_1,y_2)),\ \mathrm{rk}_9^2\oplus y_2\oplus F^2(\mathrm{rk}_{10}^1\oplus y_3\oplus F^1(y_1,y_2),\ \mathrm{rk}_{11}^2\oplus y_8\oplus F^2(y_5,y_6)))$，其中，$z=b\|x_0^3$，长度为 9 bit；$\alpha_0,\alpha_1$ 为任意常数，且 $\alpha_0\neq\alpha_1$。给定量子黑盒 g 和加密函数 Enc，将需要 464 个量子比特和 2^{28} 次量子查询恢复出密钥 k^*。

证明 当密钥 k^* 猜测正确时，函数 g 为周期函数，即满足

$$g(k^*,z)=g(k^*,z\oplus s)$$

Piccolo 算法的 6 轮量子密钥恢复攻击的具体步骤如下。

1) 定义函数

$$\begin{aligned}&h:F_2^{56}\times F_2^{(8+1)^{24}}\to F_2^{(8)^{24}}\\&(k^*,z_1,\cdots,z_{24})\mapsto g(k^*,z_1)\|\cdots\|g(k^*,z_{24})\end{aligned}$$

设有映射 U_h 满足

$$\begin{aligned}&U_h:\left|k^*,z_1,\cdots,z_{24},0,\cdots,0\right\rangle\mapsto\\&\left|k^*,z_1,\cdots,z_{24},h(k^*,z_1,\cdots,z_{24})\right\rangle\end{aligned}$$

根据文献[14]，密钥恢复攻击所需要的量子比特数为

$$\mathrm{sum}=n_k+n_{\mathrm{in}}l+n_{\mathrm{out}}l,\ \ l=2(\tilde{n}+\sqrt{\tilde{n}})$$

其中，n_k 为密钥长度，n_{in} 为周期函数输入长度，n_{out} 为周期函数输出长度，$\tilde{n}$ 为周期长度，本文猜测密钥长度为 56 bit，周期长度 $\tilde{n}=8+1=9$，周期函数输入长度 $n_{\mathrm{in}}=8+1=9$，周期函数输出长度 $n_{\mathrm{out}}=8$，因此计算可得密钥恢复攻击所需量子比特数为 $\mathrm{sum}=56+9\times24+8\times24=464$。

2) 构造量子算法 A

① 准备一个 464 bit 的量子寄存器，并将其初始化为 $|0\rangle$。

② 对前 $56+9\times24$ 个量子比特进行 Hadamard 变换，得到均匀叠加态为

$$2^{-\frac{56+9\times24}{2}}\sum\left|k^*\right\rangle\left|z_1\right\rangle\cdots\left|z_{24}\right\rangle|0\rangle$$

③ 对②得到的叠加态应用 U_h 变换，得到

$$2^{-\frac{(56+9\times24)}{2}}\sum\left|k^*\right\rangle\left|z_1\right\rangle\cdots\left|z_{24}\right\rangle\left|h(k^*,z_1,\cdots,z_{24})\right\rangle$$

④ 对量子比特 $\left|z_1\right\rangle\cdots\left|z_{24}\right\rangle$ 进行 Hadamard 变换，得到叠加态 $|\varphi\rangle$ 为

$$\begin{aligned}|\varphi\rangle=&2^{-\frac{56+9\times24}{2}}\times2^{-\frac{9\times24}{2}}\sum\left|k^*\right\rangle(-1)^{\langle u_1,z_1\rangle}\left|u_1\right\rangle\cdots\\&(-1)^{\langle u_{24},z_{24}\rangle}\left|u_{24}\right\rangle\left|h(k^*,z_1,\cdots,z_{24})\right\rangle\end{aligned}$$

其中，$k^*=(\mathrm{rk}_7^2,\mathrm{rk}_8^1,\mathrm{rk}_9^2,\mathrm{rk}_{10}^1,\mathrm{rk}_{10}^2,\mathrm{rk}_{11}^1,\mathrm{rk}_{11}^2)\in F_2^{(8)^7}$，$z_1,\cdots,z_{24},u_1,\cdots,u_{24}\in F_2^{8+1}$。根据文献[14]的引理 4，取 $l=2\left(8+1+\sqrt{8+1}\right)=24$ 即可计算出唯一的周期 s。

3) 在未对叠加态 $|\varphi\rangle$ 进行测量时，本文定义 Classifier B 以恢复密钥 k^*。

Classifier B：定义布尔函数

$$\begin{aligned}&B:F_2^{56+(8+1)\times24}\to\{0,1\}\\&(k^*,u_1,\cdots,u_{24})\mapsto\{0,1\}\end{aligned}$$

① 令 $\bar{U}=\langle u_1,u_2,\cdots,u_{24}\rangle$ 是由所有 $u_i(i=1,2,\cdots,24)$ 构成的线性空间，若 $\dim(\bar{U})\neq8$，则输出为 0；否则输出为 1，根据 $\langle u_i,s\rangle=0$ 可求出唯一的周期 s。

② 对给定的 $z_i(i=1,2,\cdots,24)$，检验 $g(k^*,z)=g(k^*,z\oplus s)$ 是否成立，若成立则输出为 1；否则输出为 0。

为了便于理解，本文忽略了相位等技术细节，将有限维的希尔伯特空间（球状体）简化为一个圆，振幅放大过程是在有限维希尔伯特空间内实现的，如图 8 所示。叠加态 $|\varphi\rangle$ 可以表示为希尔伯特空间中 2 个子空间 $|\varphi_1\rangle$、$|\varphi_0\rangle$ 的直和，即 $|\varphi\rangle=|\varphi_1\rangle+|\varphi_0\rangle$，其中，$|\varphi_1\rangle$、$|\varphi_0\rangle$ 分别代表密钥 k^* 猜测正确、错误时所有基态的总和。实际上，Classifier B 定义了一个酉算子 S_B，以有条件地改变量子状态的符号，即

$$\left|k^*\right\rangle\left|u_1\right\rangle\left|u_2\right\rangle\cdots\left|u_{24}\right\rangle\mapsto$$
$$\begin{cases}-\left|k^*\right\rangle\left|u_1\right\rangle\left|u_2\right\rangle\cdots\left|u_{24}\right\rangle, & B(k^*,u_1,u_2,\cdots,u_{24})=1\\ \left|k^*\right\rangle\left|u_1\right\rangle\left|u_2\right\rangle\cdots\left|u_{24}\right\rangle, & B(k^*,u_1,u_2,\cdots,u_{24})=0\end{cases}$$

当 $B(k^*,u_1,\cdots,u_{24})=1$ 时，对叠加态 $\left|\varphi\right\rangle$ 直接测量得到正确密钥 k^* 的概率为 $p\approx 2^{-n}$。

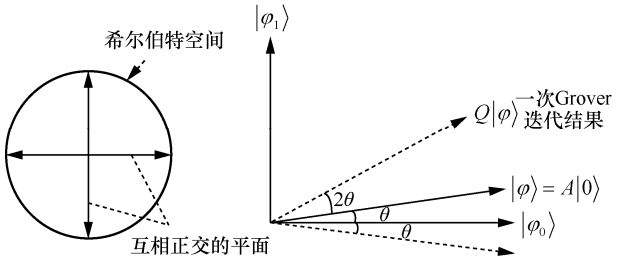


图 8　振幅放大过程示意

由文献[15]可知，完整的振幅放大过程是指对叠加态 $\left|\varphi\right\rangle=A\left|0\right\rangle$ 重复应用 t 次酉变换 $Q=-AS_0A^{-1}S_B$，从而增大获得正确密钥 k^* 的概率，即 $Q^t\left|\varphi\right\rangle=Q^tA\left|0\right\rangle$。若设 $\left|\varphi\right\rangle=A\left|0\right\rangle$ 与 $\left|\varphi_0\right\rangle$ 的初始夹角为 θ，每经过一次 Grover 迭代，该夹角将增大 2θ，其中，θ 满足 $\sin^2(\theta)=p=\left\langle\varphi_1\right|\left.\varphi_1\right\rangle$，当 p 足够小时，$\theta\approx\arcsin(\sqrt{p})\approx 2^{-28}$。在迭代大约 $t=\left\lceil\dfrac{\pi}{4\theta}\right\rceil=2^{28}$ 次之后，该夹角增大到约 $\dfrac{\pi}{2}$，此时 $Q^t\left|\varphi\right\rangle$ 与子空间 $\left|\varphi_0\right\rangle$ 几乎正交（与子空间 $\left|\varphi_1\right\rangle$ 几乎重合）。最终测量叠加态 $Q^t\left|\varphi\right\rangle$ 之后将大概率地（概率几乎为 1）得到正确密钥 k^*。

证毕。

由定理 1 可知，在经过大约 $t=2^{28}$ 次 Grover 迭代后，可以恢复出 56 bit 密钥 $\mathrm{rk}_7^2,\mathrm{rk}_8^1,\mathrm{rk}_9^2,\mathrm{rk}_{10}^1$，$\mathrm{rk}_{10}^2,\mathrm{rk}_{11}^1,\mathrm{rk}_{11}^2$，攻击所需量子比特数为 464，量子查询次数为 2^{28}。当攻击轮数 $r>6$ 轮时，需要猜测 $56+32\ (r-6)$ bit 密钥，时间复杂度为 $2^{28+16(r-6)}$。

4　结束语

本文在 Q2 模型下提出了对轻量级分组密码 Piccolo 算法的量子密码分析，找到了该算法的 3 轮量子区分器，用 Grover meets Simon 算法对其进行 6 轮量子密钥恢复攻击，恢复密钥比特数为 56 bit，所需量子比特数为 464，时间复杂度为 2^{28}；当攻击轮数大于 6 轮时，时间复杂度将以每轮 2^{16} 进行递增，即当攻击轮数 $r>6$ 时，时间复杂度为 $2^{28+16(r-6)}$，降至 Grover 量子暴力搜索的 $\dfrac{1}{2^{68}}$。经研究表明，该算法具有足够的安全性以抵抗量子攻击。本文对该算法进行量子密码分析，其时间复杂度相较于 Grover 暴力搜索有显著降低，为后续轻量级分组密码量子攻击的研究提供了新的思路。

下一步工作将继续探讨在 Q2 模型下针对其他密码算法的量子密码分析；探究在 qCPA 条件下和 qCCA 条件下针对不同 Feistel 结构密码算法的量子区分器的构造方法，以减少时间复杂度或增加量子密钥恢复攻击的轮数。

参考文献：

[1] SHIBUTANI K, ISOBE T, HIWATARI H, et al. Piccolo: an ultra-lightweight blockcipher[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 342-357.

[2] ISOBE T, SHIBUTANI K. Security analysis of the lightweight block ciphers XTEA, LED and Piccolo[C]//Proceedings of Australasian Conference on Information Security and Privacy. Berlin: Springer, 2012: 71-86.

[3] AZIMI S A, AHMADIAN Z, MOHAJERI J, et al. Impossible differential cryptanalysis of Piccolo lightweight block cipher[C]//Proceedings of 2014 11th International ISC Conference on Information Security and Cryptology. Piscataway: IEEE Press, 2014: 89-94.

[4] FU L S, JIN C H, LI X R. Multidimensional zero-correlation linear cryptanalysis of lightweight block cipher Piccolo-128[J]. Security and Communication Networks, 2016, 9(17): 4520-4535.

[5] TOLBA M, ABDELKHALEK A, YOUSSEF A M. Meet-in-the-middle attacks on reduced round piccolo[C]//Proceedings of Lightweight Cryptography for Security and Privacy. Berlin: Springer, 2016: 3-20.

[6] LIU Y, CHENG L, LIU Z Q, et al. Improved meet-in-the-middle attacks on reduced-round Piccolo[J].Science China Information Sciences, 2017, 61(3): 1-13.

[7] ASHUR T, DUNKELMAN O, MASALHA N. Linear cryptanalysis reduced round of piccolo-80[C]//Proceedings of Cyber Security Cryptography and Machine Learning. Berlin: Springer, 2019: 16-32.

[8] LIU Y, CHENG L, ZHAO F Y, et al. New analysis of reduced-version of piccolo in the single-key scenario[J]. KSII Transactions on Internet and Information Systems, 2019, 13(9): 4727-4741.

[9] GROVER L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 212-219.

[10] SIMON D. On the power of quantum computation[J]. SIAM Journal on Computing, 1997, 26(5): 1474-1483.

[11] ZHANDRY M. How to construct quantum random functions[C]//Proceedings of 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2012: 679-687.

[12] KAPLAN M, LEURENT G, LEVERRIER A, et al. Quantum differential and linear cryptanalysis[J]. IACR Transactions on Symmetric

Cryptology, 2016, 1: 71-94.

[13] KUWAKADO H, MORII M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C]//Proceedings of 2010 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2010: 2682-2685.

[14] LEANDER G, MAY A. Grover meets Simon-quantumly attacking the FX-construction[C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2017: 161-178.

[15] DONG X Y, WANG X Y. Quantum key-recovery attack on Feistel structures[J]. Science China Information Sciences, 2018, 61(10): 1-7.

[16] DONG X Y, LI Z, WANG X Y. Quantum cryptanalysis on some generalized Feistel schemes[J]. Science China Information Sciences, 2019, 62(2): 1-12.

[17] DONG X Y, DONG B Y, WANG X Y. Quantum attacks on some Feistel block ciphers[J]. Designs, Codes and Cryptography, 2020, 88(6): 1179-1203.

[18] 倪博煜, 董晓阳. 改进的 Type-1 型广义 Feistel 结构的量子攻击及其在分组密码 CAST-256 上的应用[J]. 电子与信息学报, 2020, 42(2): 295-306.
NI B Y, DONG X Y. Improved quantum attack on type-1 generalized feistel schemes and its application to CAST-256[J]. Journal of Electronics & Information Technology, 2020, 42(2): 295-306.

[19] 尤启迪, 钱新, 周旋, 等. SMS4-like 结构以及 NBC 算法的量子算法攻击研究[J]. 密码学报, 2020, 7(6): 864-874.
YOU Q D, QIAN X, ZHOU X, et al. Research on quantum cryptanalysis on SMS4-like structure and NBC algorithm[J]. Journal of Cryptologic Research, 2020, 7(6): 864-874.

[20] 于博, 孙兵, 刘国强, 等. 若干广义非平衡 Feistel 结构的量子分析研究[J]. 密码学报, 2021, 8(6): 960-973.
YU B, SUN B, LIU G Q, et al. Quantum cryptanalysis on some generalized unbalanced feistel networks[J]. Journal of Cryptologic Research, 2021, 8(6): 960-973.

[21] 钱新, 尤启迪, 周旋, 等. MARS-like Feistel 结构的量子攻击[J]. 密码学报, 2021, 8(3): 417-431.
QIAN X, YOU Q D, ZHOU X, et al. Quantum attack on MARS-like feistel schemes[J]. Journal of Cryptologic Research, 2021, 8(3): 417-431.

[22] 李艳俊, 林昊, 易子晗, 等. MIBS 算法量子密码分析[J]. 密码学报, 2021, 8(6): 989-998.
LI Y J, LIN H, YI Z H, et al. Quantum cryptanalysis of MIBS[J]. Journal of Cryptologic Research, 2021, 8(6): 989-998.

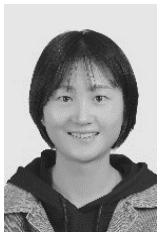
[23] LI Y J, LIN H, LIANG M, et al. A new quantum cryptanalysis method on block cipher Camellia[J]. IET Information Security, 2021, 15(6): 487-495.

[24] 李艳俊, 易子晗, 汪振, 等. 轻量级密码 TWINE-128 的量子密码分析[J]. 密码学报, 2022, 9(4): 633-643.
LI Y J, YI Z H, WANG Z, et al. Quantum cryptanalysis of lightweight cipher TWINE-128[J]. Journal of Cryptologic Research, 2022, 9(4): 633-643.

[作者简介]

杜小妮（1972− ），女，甘肃庆阳人，博士，西北师范大学教授、博士生导师，主要研究方向为密码学与信息安全等。

王香玉（1997− ），女，河南开封人，西北师范大学硕士生，主要研究方向为密码学与信息安全等。



梁丽芳（1995− ），女，甘肃定西人，西北师范大学硕士生，主要研究方向为密码学与信息安全等。

李锴彬（1997− ），男，甘肃天水人，西北师范大学硕士生，主要研究方向为密码学与信息安全等。