文章编号:1000-2367(2020)05-0009-07 DOI:10.16366/j.cnki.1000-2367.2020.05.002

Simon 算法对 SIMON 密码的密钥恢复攻击

彭信行,孙兵,李超

(国防科技大学 文理学院,长沙 410073)

摘 要:近年来,随着量子技术被应用到密码算法的安全性分析中,经典密码算法的安全性受到了极大的威胁.将 Simon 量子算法应用到 SIMON 密码的分析之中,成功构造一个周期函数,将 3 轮 SIMON 密码与随机置换区分开.随后对该周期函数满足 Simon 问题条件的参数进行估计,找到且证明其存在一个上界,从而计算出 SIMON32/48/64 这 3 类密码对应参数的上界值.最后通过分别构造加密和解密过程相应的区分器,对 6 轮 SIMON 密码进行了密钥恢复攻击,得到了 4 个轮密钥,并给出了该攻击的时间复杂度.

关键词:Simon 算法;SIMON 密码;密钥恢复攻击

中图分类号:TP309.7 **文献标志码**:A

随着移动互联和物联网等信息技术的飞速发展,智能卡、移动支付、人脸识别等物联网技术得到了广泛的应用.物联网设备由于受到存储资源、计算资源和能耗资源等限制,物联网环境下的数据安全成为人们广泛关注的问题.针对这个问题,一些专家和学者提出了很多轻量级的密码算法和协议[1-6].轻量级密码算法既能保证设备安全,又能在资源受限的条件下高效工作,实现安全性和高效性的平衡.近年来国内外设计的轻量级密码算法主要有 GIFT[1],PRESENT[2],PRINCE[3],LED[4],LBLOCK[5],SIMON[6] 等.其中 SIMON 是美国国家安全局(NSA)在 2013 年提出的轻量级密码算法,其轮函数简单,包含容易实现的按位与,按位异或和循环移位操作,该算法占用的资源较少且效率很高.SIMON 密码一经提出便引起了密码学界的广泛关注,一些专家和学者对其进行了大量的经典密码分析.2013 年,文献[7]对 SIMON 密码进行差分分析和不可能差分分析,文献[8]在此基础上将差分分析和不可能差分分析的结果进行了改进,并首次给出了 SIMON 密码线性分析的结果.2014 年,文献[9]对 SIMON 密码进行了差分故障分析,文献[10]构造出 15 轮积分区分器,利用该区分器对 SIMON32 进行了 21 轮密钥区分攻击.

近年来,随着量子计算的不断进步,量子技术被应用到密码算法的安全性分析中,经典密码算法的安全性受到了极大的挑战.特别是 2017 年美国国家标准与技术研究院在征集轻量级密码算法标准时,提出了抵抗量子攻击的要求,使得使用量子技术分析密码算法成为一个热门的研究方向.由于量子计算机的并行特性,一些量子算法对经典密码算法安全性产生了严重的威胁,其中 Shor 算法和 Grover 算法是密码分析中著名的量子算法.文献[11]提出能够在多项式时间内对大整数进行质因子分解的 Shor 算法,这就对基于大整数分解构造的公钥密码算法如 RSA 算法构成了巨大的威胁.文献[12]提出量子搜索的 Grover 算法,该算法能够对经典的穷搜实现平方加速,以 $O(2^{n/2})$ 的时间复杂度从 $2n$ 个无序数据中找到目标数据,应用于密码算法的密钥穷搜中,相当于将密钥长度减半,攻击效率大大提高.本文涉及的 Simon 算法是文献[13]提出的量子算法,该算法能够在多项式时间内恢复出一个特殊布尔函数的周期,构造出三轮的 Feistel 结构和随机置换之间的区分器[14].

收稿日期:2020-03-21;**修回日期**:2020-06-08.

基金项目:国家自然科学基金(61672530;61772545)

作者简介:彭信行(1995—),男,河南信阳人,国防科技大学硕士研究生,研究方向为编码密码理论及其应用,E-mail:1576522387@qq.com.

通信作者:李超(1966—),男,湖南汨罗人,国防科技大学教授,博士生导师,主要从事编码密码理论及其应用研究,E-mail:lichao_nudt@sina.com.cn.

在量子计算机中可以实现量子选择明文攻击(qCPA)[15],指的是密码算法运行在量子计算机中,攻击者在选择明文的情况下,对密码算法的输入进行叠加状态查询.1988 年,文献[16]已经证明 3 轮 Feistel 结构是伪随机置换,是可证明安全的,但是 2010 年两位日本学者发现了 3 轮 Feistel 结构存在一个固定的周期,并且使用 Simon 算法在 $O(n)$时间复杂度内恢复出周期,这一结果比经典方法 $O(2^{n/2})$的时间复杂度有了很大的提高[17].紧接着在 2012 年,文献[18]将 Simon 算法应用在 Even-Mansour 结构上,在 $O(n)$时间复杂度内恢复出固定的周期刚好是密钥.证明了 3 轮 Feistel 结构和 Even-Mansour 结构在量子条件下是不安全的,攻击者可以在多项式时间内恢复出周期进而恢复密钥.在文献[18]工作的基础上,文献[19]在 CRYPTO2016 上使用概率方法进一步拓展了 Simon 算法的应用范围,给出了 LRW,XEX 和 XE 结构在多项式时间复杂度内恢复出固定周期的结果,以及对 CBC-MAC、PMAC 和 GMAC 等不同消息认证算法的多项式时间攻击结果.2017 年,LEANDER 等人[20]用 Simon 算法和 Grover 算法组合来攻击 FX 结构.国内的 DONG 等人分别对 Feistel 结构、广义 Feistel 结构构建了密钥恢复攻击,并结合 Simon 算法改进了经典的滑动攻击[21-22].

1 基础知识

1.1 符号说明

表 1 符号说明

Tab.1 Notations

符号	含义	符号	含义	符号	含义
SIMON	SIMON 密码算法	F	SIMON 密码轮函数	&	按位与
Simon	Simon 量子算法	$\oplus$	按位异或	S^j	左循环移 j 位

1.2 Simon 问题和 Simon 算法

Simon 问题[18]:给定一个向量值函数 $f:\{0,1\}^n \to \{0,1\}^n$,假设存在一个周期 $s \in \{0,1\}^n$ 使得对任意的 $x \in \{0,1\}^n$,都有 $f(x)=f(x+s)$, Simon 问题就是如何寻找周期 s.

解决 Simon 问题,根据生日悖论经典方法的计算复杂度是 $O(2^{n/2})$,当 n 的值特别大的时候,计算复杂度呈指数增长,无法计算.为了更好地解决 Simon 问题,1994 年 Simon 提出了 Simon 算法[13],使用 Simon 算法寻找周期 s 的计算复杂度是 $O(n)$.

Simon 算法的 5 个主要步骤如下[21]:

(i)初始化 2 个 n 个量子比特量子态 $|0\rangle^{\otimes n}|0\rangle^{\otimes n}$,将 Hadamard 变换应用到第 1 个寄存器得:

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

(ii)对第 2 个寄存器进行量子 Oracle 访问得:$\frac{1}{\sqrt{2^n}}\sum_{x\in[0,1)^n}|x\rangle|f(x)\rangle$;

(iii)当测量第 2 个寄存器的时候,第 1 个寄存器坍塌为:$\frac{1}{\sqrt{2}}(|z\rangle+|z\oplus s\rangle)$;

(iv)对第 1 个寄存器使用 Hadamard 变换,得到:$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{y\cdot z}(1+(-1)^{y\cdot s})|y\rangle$;

(v)满足 $y\cdot s=1$ 的向量 y 的幅度为 0,因此测量的向量 y 都满足 $y\cdot s=0$.

重复上面步骤 $O(n)$ 次,能以很大的概率得到$(n-1)$ 个不相关的与 s 正交的向量,s 可通过解线性方程组得到.这样就以 $O(n)$ 的计算复杂度得到了周期 s,与传统方法 $O(2^{n/2})$ 计算复杂度相比有了很大的提高.

Simon 问题条件要求向量值函数严格满足二对一的条件,即同一个函数值对应有两个原像,且两个原像之间相差一个固定的周期[18].在密码分析的过程中,严格满足 Simon 问题条件的向量值函数是很少见的.在实际应用中,很多向量值函数含有其他干扰性的碰撞 t,对于一个向量值函数 f,对任意的 x 满足 $f(x)=f(x\oplus s)$,但是对于部分 x,满足 $f(x)=f(x\oplus t)$,其中 $t\neq s$ 且 $t\neq 0$,则称 t 为布尔函数的碰撞. KAPLAN 等人[19]研究得出,当碰撞 t 所占的比例不是很大的时候,仍然可以通过 Simon 算法以一定的概率计算得出

向量值函数 f 的周期 s,如果碰撞 t 所占的比例很大的时候,就不能通过 Simon 算法得出周期 s.KAPLAN 等人[19]得出如下的定理.

定理 1[19]　对于一个向量值函数 $f:\{0,1\}^n \to \{0,1\}^n$,满足 $f(x)=f(x\oplus s)$ 对任意的 x 成立,考虑参数$\varepsilon(f,s)=\max\limits_{t\in\{0,1\}^n\setminus\{0,s\}} P[f(x)=f(x\oplus t)]$.这个参数衡量了向量值函数 f 满足 Simon 问题的程度.如果 $\varepsilon(f,s)\leq p_0<1$,则 Simon 算法在执行 cn 次之后得到 s 的概率至少为 $1-\left(2\left(\dfrac{1+p_0}{2}\right)^c\right)^n$.

当参数 ε 的值接近于 0 的时候,Simon 算法成功恢复出周期的概率会趋近于 1;当参数 ε 的值很大的时候,Simon 算法成功恢复出周期的概率会很小;当参数 ε 的值趋近于 1 的时候,会存在一个接近周期的值 t,使得对绝大多数 x,满足 $f(x)=f(x\oplus t)$,此时成功恢复出周期的概率趋近于 0.

1.3　Simon 算法攻击 3 轮 Feistel 结构

自从 SIMON 提出 Simon 算法[13],有关 Simon 算法的研究一直是研究的热点.本文主要是将 Simon 算法应用于 SIMON 密码结构,SIMON 密码结构采用的是 Fesitel 结构,下面介绍 KUWAKADO 等人[18]在 3 轮 Feistel 结构和随机置换之间构造的区分器.

Feistel 结构是一个经典的密码结构,对其安全性研究是对称密码研究中的重要问题.一个 3 轮 Feistel 结构如图 1 所示,输入为 (x_L,x_R),输出为$(y_L,y_R)=E(x_L,x_R)$,轮函数为 R_1,R_2,R_3,且满足:

$$(u_0,v_0)=(x_L,x_R),$$
$$(u_i,v_i)=(v_{i-1}\oplus R_i(u_{i-1}),u_{i-1}),$$
$$(u_3,v_3)=(y_L,y_R).$$

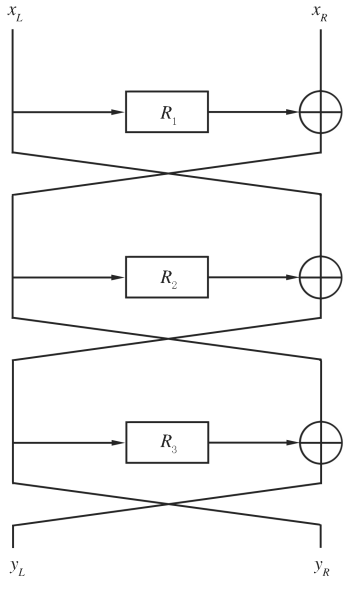

图1　三轮Feistel结构

Fig.1　Three rounds Feistel structure

构造一个向量值函数,任取两个非零常数 $\alpha_0,\alpha_1\in\{0,1\}^{n/2}$,构造如下:

$$f:\{0,1\}\times\{0,1\}^{n/2}\to\{0,1\}^{n/2},$$
$$b,x\to y_R\oplus\alpha_b,\text{其中}(y_R,y_L)=E(\alpha_b,x),f(b,x)=R_2(x\oplus R_1(\alpha_b)).$$

当 R_2 满足置换条件时,函数 f 就满足 Simon 问题的条件,于是可根据下式来计算函数 f 的周期.

$$f(b',x')=f(b,x)\Leftrightarrow R_2(x\oplus R_1(\alpha_b))=R_2(x'\oplus R_1(\alpha_{b'}))\Leftrightarrow x'\oplus R_1(\alpha_{b'})=x\oplus R_1(\alpha_b)\Leftrightarrow$$
$$\begin{cases}x'\oplus x=0, & b'=b,\\ x'\oplus x=R_1(\alpha_0)\oplus R_1(\alpha_1), & b'\neq b.\end{cases}$$

根据上面的计算过程可以得到函数 f 的周期为$s=1\parallel R_1(\alpha_0)\oplus R_1(\alpha_1)$.也就是说 $f(b,x)=f(b\oplus 1,x\oplus R_1(\alpha_0)\oplus R_1(\alpha_1))$.

1.4　SIMON 密码的介绍

SIMON 密码[6]是一类轻量级的分组密码,分组长度有 32,48,64,96 和 128 比特,密钥的长度为 64,72,96,128,144,192 和 256 比特,对应关系如表 2.

表 2　Simon 算法参数表

Tab.2　Simon parameters

分组长度	32	48	64	96	128
密钥长度	64	72,96	96,128	96,144	128,192,256

SIMON 密码的轮函数简单,仅包含以下 3 种操作:

1)比特异或,⊕;

2)比特与,&;

3)左循环移 j 位,S^j.

轮变换为 R_k,如图 2 所示.

$GF(2)^n \times GF(2)^n \to GF(2)^n \times GF(2)^n$,

$R_k(x,y)=(y \oplus F(x) \oplus k, x)$,

其中 $F(x)=(Sx \& S^8 x) \oplus S^2 x$ 为轮函数,k 为轮密钥.

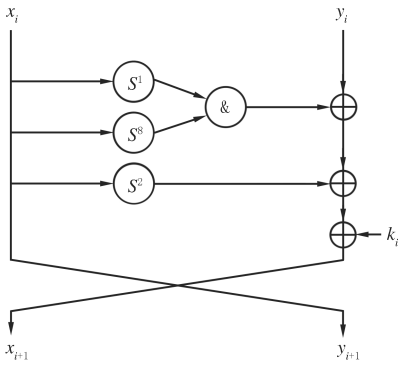

图2 SIMON密码轮函数

Fig.2 SIMON cipher's round function

2 Simon 算法应用于 3 轮 SIMON 密码

构造 SIMON 密码的向量值函数,任取两个非零常数 $\alpha_0,\alpha_1 \in \{0,1\}^{n/2}$, 构造如下:

$$f:\{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2},$$

$$b,x \to y_3 \oplus \alpha_b, \text{其中}(x_3,y_3)=E(\alpha_b,x), f(b,x)=F(F(\alpha_b) \oplus x \oplus k_0) \oplus k_1.$$

计算向量值函数的周期:

$$f(b',x')=f(b,x) \Leftrightarrow F(F(\alpha_{b'}) \oplus x' \oplus k_0) \oplus k_1 = F(F(\alpha_b) \oplus x \oplus k_0) \oplus k_1 \Leftrightarrow$$

$$F(F(\alpha_{b'}) \oplus x' \oplus k_0) = F(F(\alpha_b) \oplus x \oplus k_0) \Leftrightarrow F(\alpha_{b'}) \oplus x' \oplus k_0 = F(\alpha_b) \oplus x \oplus k_0 \Leftrightarrow$$

$$F(\alpha_{b'}) \oplus x' = F(\alpha_b) \oplus x \Leftrightarrow \begin{cases} x' \oplus x = 0, & b'=b, \\ x' \oplus x = F(\alpha_b) \oplus F(\alpha_{b'}), & b' \neq b. \end{cases}$$

当轮函数 F 是一个置换时,函数 f 就满足 Simon 问题的条件,于是可以根据 Simon 算法计算出函数 f 的周期为:$s=1 \| F(\alpha_b) \oplus F(\alpha_{b'})$,也就是对任意 x,均有 $f(b,x)=f(b \oplus 1, x \oplus F(\alpha_b) \oplus F(\alpha_{b'}))$.

遗憾的是,SIMON 密码的轮函数 F 不是置换,因此不能根据上面的公式来计算函数 f 的周期.注意到 F 不是双射时,根据 3 轮 Feistel 结构的特点,如下结果仍然成立:

$$f(b',x')=f(b,x) \Leftrightarrow F(F(\alpha_{b'}) \oplus x' \oplus k_0) \oplus k_1 = F(F(\alpha_b) \oplus x \oplus k_0) \oplus k_1 \Leftrightarrow$$

$$F(F(\alpha_{b'}) \oplus x' \oplus k_0) = F(F(\alpha_b) \oplus x \oplus k_0).$$

此时,由于 F 不是双射,则分为 2 种情况.

第 1 种情况是,对任意 $x \in \{0,1\}^{n/2}$,有

$$F(\alpha_{b'}) \oplus x' \oplus k_0 = F(\alpha_b) \oplus x \oplus k_0 \Leftrightarrow F(\alpha_{b'}) \oplus x' = F(\alpha_b) \oplus x \Leftrightarrow$$

$$\begin{cases} x' \oplus x = 0, & b'=b, \\ x' \oplus x = F(\alpha_b) \oplus F(\alpha_{b'}), & b' \neq b. \end{cases}$$

令 $s=1 \| F(\alpha_b) \oplus F(\alpha_{b'})$,则 f 是一个周期函数,$f(x)=f(x \oplus s)$ 对任意 x 成立.

第 2 种情况是,对部分 $x \in \{0,1\}^{n/2}$,存在一个常数 $\beta(\beta \neq 0)$,有

$$F(\alpha_{b'}) \oplus x' \oplus k_0 = F(\alpha_b) \oplus x \oplus k_0 \oplus \beta \Leftrightarrow F(\alpha_{b'}) \oplus x' = F(\alpha_b) \oplus x \oplus \beta \Leftrightarrow$$

$$\begin{cases} x' \oplus x = \beta, & b'=b, \\ x' \oplus x = F(\alpha_b) \oplus F(\alpha_{b'}) \oplus \beta, & b' \neq b. \end{cases}$$

令 $t=0 \| \beta$ 或 $t=1 \| F(\alpha_b) \oplus F(\alpha_{b'}) \oplus \beta$,则 $f(x)=f(x \oplus t)$ 对部分 x 成立,这就对求解 $f(x)=f(x \oplus s)$ 中的周期 s 造成干扰.

为了能够以很大的概率得到 s,需要考虑干扰 t 的大小,即 f 满足 Simon 问题的程度,也就是上文提到的定理 1,当参数 ε 的值趋近于 0 的时候,Simon 算法成功恢复出周期的概率会趋近于 1[19].其中 $\varepsilon(f,s)=\max_{t \in \{0,1\}^{n+1} \setminus \{0,s\}} P[f(x)=f(x \oplus t)]$, 在 SIMON 密码中,直接求解 $\varepsilon(f,s)$很困难,由于轮函数 F 已知,可以转化为求解 $\varepsilon(f,s)$的一个上界.

定理 2 在 SIMON 密码中,F 函数为轮函数,定义参数 $\varepsilon'(F)=\max\limits_{\beta \in \{0,1\}^n, \beta \neq 0} P_x[F(x)=F(x \oplus \beta)]$.则下式成立:$\varepsilon(f,s) \leq 2\varepsilon'(F)$.

证明 当 $t=0 \| \beta$ 或 $t=1 \| F(\alpha_b) \oplus F(\alpha_{b'}) \oplus \beta$ 时,$f(x)=f(x \oplus t)$ 对部分 x 成立.t 与 β 存在对

应关系,一个 t 对应两个 β,取 $t=t_0$,则 $\exists\beta=\beta_0,\beta_1$ 与之对应,其中 $t_0=0\,||\,\beta_0, t_0=1\,||\,F(\alpha_b)\oplus F(\alpha_{b'})\oplus\beta_0$. 则有

$$P_x[f(x)=f(x\oplus t_0)]=P_x[F(x)=F(x\oplus\beta_0)]+P_x[F(x)=F(x\oplus\beta_1)]-$$
$$P_x[F(x)=F(x\oplus\beta_0)\cap F(x)=F(x\oplus\beta_1)]\leq P_x[F(x)=F(x\oplus\beta_0)]+$$
$$P_x[F(x)=F(x\oplus\beta_1)]\leq 2\max_{\beta\in\{0,1\}^n,\beta\neq 0}P_x[F(x)=F(x\oplus\beta)],$$

故 $\max\limits_{t\in\{0,1\}^{n+1}\setminus\{0,s\}}P_x[f(x)=f(x\oplus t)]\leq 2\max\limits_{\beta\in\{0,1\}^n,\beta\neq 0}P_x[F(x)=F(x\oplus\beta)]$,即 $\varepsilon(f,s)\leq 2\varepsilon'(F)$.

根据定理 2 只需要求出 $\varepsilon'(F)$的值即可估计 $\varepsilon(f,s)$的上界,SIMON 密码中轮函数 F 是已知的,根据算法 1,以 SIMON32/64、SIMON48/72(96)和 SIMON64/96(128)为例计算 $2\varepsilon'(F)$的值.

算法 1　计算上界 $2\varepsilon'(F)$

Input　分支长度 N,计数数组 $Arr[2^N]$,最大计数 max

Output　上界 $2\varepsilon'(F)$

```
初始化轮函数 F, Arr[2^N] ← 0, max ← 0, i ← 0
for i < 2^N do
    Arr[F(i)] = Arr[F(i)] + 1
    if Arr[F(i)] > max then
        max = Arr[F(i)]
    end
end
计算 2ε'(F) = max / 2^(N-1)
```

计算结果如表 3 所示.由表 3 可以看出 $\varepsilon(f,s)$的上界很小趋近于 0,根据定理 1,此时使用 Simon 算法能够以很大的概率恢复出向量值函数 f 的周期 s.

表 3　3 种 SIMON 密码对应的上界

Tab.3　Upper bound corresponding to three SIMON ciphers

分组长度	SIMON32/64	SIMON48/72(96)	SIMON64/96(128)
$2\varepsilon'(F)$	2^{-13}	2^{-20}	5×2^{-31}

3　对 6 轮 SIMON 密码进行密钥恢复攻击

在文献[21]中,DONG 等人在量子条件下结合 Simon 算法和 Grover 算法,给出了 5 轮 Feistel 结构密钥恢复攻击.本文以 Simon 算法为例,给出了 6 轮 Feistel 结构密钥恢复攻击,如图 3 所示.

上文对 3 轮 SIMON 密码构造了周期函数,这里在 3 轮的基础上对 6 轮 SIMON 密码进行密钥恢复攻击.其中,x_i, y_i 为每一轮输入,F 为轮函数,k_i 为轮密钥.对第 2 轮到第 4 轮构造周期函数,任取 3 个非零常数 $\alpha_0,\alpha_1,y_0\in\{0,1\}^{n/2}$,$(\alpha_0,y_0)$ 和(α_1,y_0) 作为输入,$f(b,y_1)=\beta_b\oplus y_4$,其中 $\beta_b=y_0\oplus F(\alpha_b)\oplus k_0$,$y_4=F(F(y_6)\oplus k_5\oplus x_6)\oplus k_4\oplus y_6$,则 $f(b,y_1)=y_0\oplus f(\alpha_b)\oplus k_0\oplus F(F(y_6)\oplus k_5\oplus x_6)\oplus k_4\oplus y_6$.

观察上式,可以对 $k_0\oplus k_4$ 和 k_5 进行密钥恢复攻击.若猜测 $k_0\oplus k_4$ 和 k_5 均正确,则 $f(b,y_1)$ 为周期函数,周期为 $s=1\,||\,F(\beta_0)\oplus F(\beta_1)$.若猜测不是全部正确,则 $f(b,y_1)$ 为随机函数具有周期的概率非常小.

同样,对上述 6 轮 SIMON 密码进行解密操作.如图 4 所示,x_i 为每一轮输入的右支,y_i 为每一轮输入的左支,F 为轮函数,k_i 为轮密钥,对于第一轮输入为(y_6,x_6),密钥为 k_5,后面的每轮依次类推.同样对第 2 轮到第 4 轮构造周期函数,任取 3 个非零常数 $\eta_0,\eta_1,x_6\in\{0,1\}^{n/2}$,$(\eta_0,x_6)$ 和(η_1,x_6) 作为输入,

$f(b,x_6)=\gamma_b\oplus x_2$,其中 $\gamma_b=x_6\oplus F(\eta_b)\oplus k_5$,$x_2=F(F(x_0)\oplus k_0\oplus y_0)\oplus k_1\oplus y_1$,则 $f(b,x_5)=x_6\oplus F(\eta_b)\oplus k_5\oplus F(F(x_0)\oplus k_0\oplus y_0)\oplus k_1\oplus y_1$.

观察上式,可对 $k_1\oplus k_5$ 和 k_0 进行密钥恢复攻击,若猜测 $k_1\oplus k_5$ 和 k_0 均正确,则 $f(b,x_5)$ 为周期函数,周期为 $s=1\,||\,F(\gamma_0)\oplus F(\gamma_1)$,若猜测不是全部正确,则 $f(b,x_5)$ 为随机函数具有周期的概率非常小.

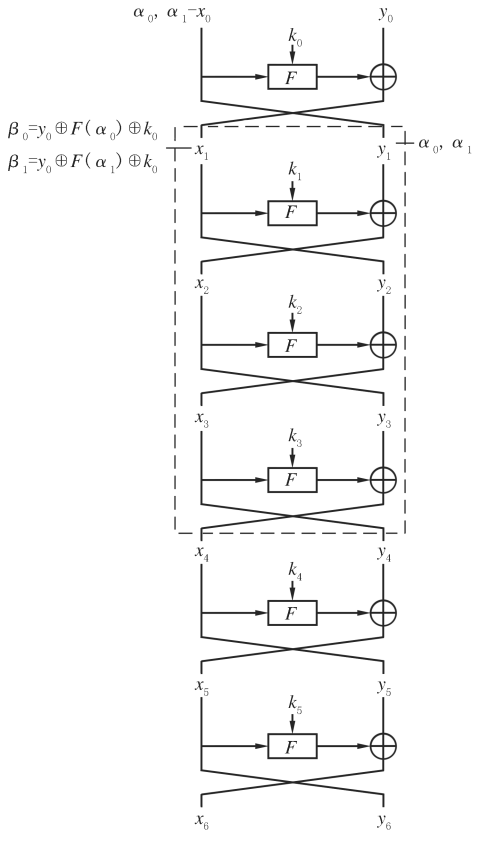

图3 6轮SIMON密码密钥恢复攻击

Fig.3 6 rounds key-recovery attack on SIMON

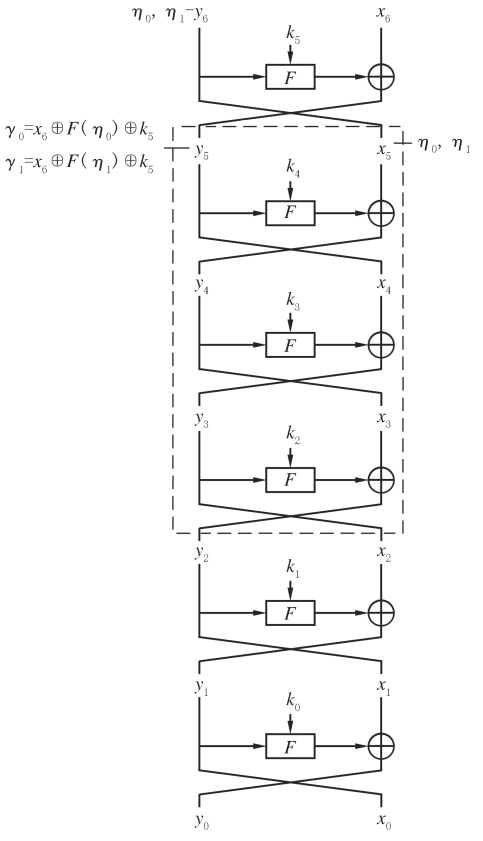

图4 6轮SIMON密码逆向密钥恢复攻击

Fig.4 6 rounds reverse key-recovery attack on SIMON

综上,可以恢复出 k_0,k_5,$k_0\oplus k_4$,$k_1\oplus k_5$,根据 k_0 和 $k_0\oplus k_4$ 可以得到 k_4,再根据 k_5 和 $k_1\oplus k_5$ 可以得到 k_5,则 k_0,k_1,k_4 和 k_5 都能够恢复出来.

文献[23]在传统条件下给出了 Feistel 结构密钥恢复攻击的时间复杂度.在文献[21]中,DONG 等人在量子条件下结合 Simon 算法和 Grover 算法,给出了 Feistel 结构 5 轮和 7 轮密钥恢复攻击的时间复杂度.本文以 Simon 算法为例,给出了 Feistel 结构 6 轮密钥恢复攻击的时间复杂度.三者的对比如表 4.

表 4 三者的时间复杂度比较

Tab.4 Comparison of time complexity of the three

轮数	文献 1	文献 2	本文
5 轮	2^n	$2^{0.5n}$	——
6 轮	——	——	$2^{0.5n}$
7 轮	$2^{1.5n}$	2^n	——

4 总 结

本文将 Simon 量子算法应用到 SIMON 密码中,对 3 轮的 SIMON 密码构造了一个周期函数,将 3 轮 SIMON 密码跟随机置换区分开.随后对构造的函数进行满足 Simon 问题条件的参数进行估计.由于 SIMON 密码的轮函数已知,因此可以找到参数的一个上界,并且给出严格的证明.之后编程计算出 SIMON 密码分组长度分别为 32,48 和 64 时,对应参数的上界值.最后对 6 轮的 SIMON 密码进行密钥恢复攻击,分别对加密和解密过程中第 2 轮到第 4 轮构造区分器,恢复出 4 个轮密钥.

参 考 文 献

[1] BANIK S,PANDEY S K,PEYRIN T,et al.GIFT:A small present[C]//Cryptographic Hardware and Embedded Systems-CHES 2017.Berlin:Springer,2017:321-345.

[2] BOGDANOV A,KNUDSEN L R,LEANDER G,et al.PRESENT:An ultra-lightweight block cipher[C]//Cryptographic Hardwareand Embedded Systems-CHES 2007.Berlin:Springer,2007:450-466.

[3] BORGHOFF J，CANTEAUT A，GüNEYSU T，et al.PRINCE-A low-latency block cipher for pervasive computing applications[C]//Advances in Cryptology-ASIACRYPT 2012.Berlin：Springer，2012：208-225.

[4] GUO J，PEYRIN T，POSCHMANN A，et al.The LED block cipher[C]//Cryptographic Hardware and Embedded Systems-CHES 2011.Berlin：Springer，2011：326-341.

[5] WU W，ZHANG L.LBLOCK：A lightweight block cipher[C]//Applied Cryptography and Network Security-ACNS 2011.Berlin：Springer，2011：327-344.

[6] BEAULIEU R，SHORS D，SMITH J，et al.The SIMON and SPECK lightweight block ciphers[J].IACR Cryptology ePrint Archive，2013，2013：404.

[7] ALKHZAIMI H，LAURIDSER M M.Cryptanalysis of the SIMON family of block ciphers[J].IACR Cryptology ePrint Archive，2013，2013：543.

[8] ABED F，LIST E，LUCKS S，et al.Differential and linear cryptanalysis of reduced-round SIMON[R].[s.l.：s.n.]，2013.

[9] TUPSAMUDRE H，BISHT S，MUKHOPADHYAY D.Differential fault analysis on the families of SIMON and SPECK ciphers[C]//2014 Workshop on Fault Diagnosis and Tolerance in Cryptography-FDTC.Piscataway：IEEE，2014：40-48.

[10] WANG Q，LIU Z，VARC K，et al.Cryptanalysis of Reduced-Round SIMON32 and SIMON48[J].IACR Cryptology ePrint Archive，2014，2014：761.

[11] SHO R，PETER W.Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J].Siam Journal on Computing，1997，26(5)：1484-1509.

[12] GROVER L K.A fast quantum mechanical algorithm for database search[J].Phys Rev Lett，1997，79：212-219.

[13] SIMON，DANIEL R.On the Power of Quantum Computation[J].Siam J Comput，1997：1474-1483.

[14] KUWAKADO H，MORII M.Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C]//2010 IEEE International Symposium on Information Theory Proceedings (ISIT).[s.l.：s.n.]，2010：2682-2685.

[15] BONEH D，ZHANDRY M. Secure signatures and chosen ciphertext security in a quantum computing world[C]//Advances in Cryptology-CRYPTO 2013.Berlin：Springer-Verlag，2013：361-379.

[16] LUBY M G，RACKOFF C. How to construct pseudorandom permutations from pseudorandom functions[J].SIAM Journalon Computing，1988，17(2)：373-386.

[17] KUWAKADO H，MORII M. Quantum distinguisher between the 3-round feistel cipher and the random permutation[C]//International symposium on information theory.Piscataway：IEEE Press，2010：2682-2685.

[18] KUWAKADO H，MORII M.Security on the quantum-type even-mansour cipher[C]//International symposium on informa-tion theory and its applications ISITA 2012.Piscataway：IEEE Press，2012：312-316.

[19] KAPLAN M，LEURENT G，LEVERRIER A，et al.Breaking symmetric cryptosystems using quantum period finding[C]//Robshaw M，Katz J，eds.Advances in Cryptology-CRYPTO 2016.Berlin： Springer-Verlag，2016：207-237.

[20] LEANDER G，MAY A.Grover meets simon-quantumly attacking the FX-construction[C]//Takagi T，Peyrin T，eds.Advances in Cryptology - ASIACRYPT 2017 Part II.Berlin：Springer，2017：161-178.

[21] DONG X，WANG X.Quantum key-recovery attack on Feistel structures[J].Science China(Information Sciences)，2018，61(10)：240-246.

[22] DONG X Y，LI Z，WANG X Y.Quantum cryptanalysis on some generalized Feistel schemes[J].Science China(Information Sciences)，2019，62(2)：22501：1-22501：12.

[23] DINUR I，DUNKELMAN O，KELLER N，et al.New attacks on Feistel structures with improved memory complexities[C]//Advances in Cryptology-CRYPTO 2015.Berlin： Springer-Verlag，2015：433-454.

Simon algorithm key-recovery attack on SIMON

Peng Xinhang，Sun Bing，Li Chao

(College of Liberal Arts and Sciences，National University of Defense Technology，Changsha 410073，China)

Abstract：In recent years，with the application of quantum technology to the security analysis of cryptographic algorithms，the security of classical cryptographic algorithms has been greatly threatened.In this paper，the Simon quantum algorithm is applied to the analysis of SIMON cipher，and a periodic function is successfully constructed to distinguish the three rounds of SIMON cipher from random permutations.The parameters of the periodic function satisfying the conditions of the Simon problem are estimated，and an upper bound is found and proved，so that the upper bound values of the corresponding parameters of the three types of SIMON32/48/64 are calculated.Finally，by constructing corresponding discriminators for the encryption and decryption processes，six rounds of SIMON ciphers were subjected to key recovery attacks，four rounds of keys were obtained，and time complexity was given.

Keywords：Simon algorithm；SIMON cryptography；key recovery attacks

[责任编校　陈留院　赵晓华]