Simon 量子算法攻击下的可调加密方案研究

毛淑平[1,2], 王 鹏[1,2], 胡 磊[1,2]

[1] 信息安全国家重点实验室 中国科学院信息工程研究所 北京 中国 100085
[2] 中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 随着量子计算机和量子计算技术的迅速发展, 量子算法对密码系统安全性的威胁迫在眉睫。之前的研究表明, 许多经典安全的对称密码结构或方案在基于 Simon 算法的量子攻击下不安全, 例如 3 轮 Feistel 结构、Even-Mansour 结构、CBC-MAC、GCM 和 OCB 等方案。可调加密方案通常设计为分组密码工作模式, 用于磁盘扇区加密, 其结构可以分为 Encrypt-Mask-Encrypt(CMC、EME、EME*等)、Hash-CTR-Hash(XCB、HCTR、HCH 等)和 Hash-ECB-Hash(PEP、TET、HEH 等)三种类型。本文利用 Simon 算法, 对 HCTR、HCH、PEP 和 HEH 四种可调加密方案进行了分析, 研究结果表明这四种可调加密方案在选择明文量子攻击下是不安全的, 使用多项式次的量子问询即可得到与方案秘密值有关的周期函数的周期, 进而将其和可调随机置换区分开来。对于利用 Simon 算法对可调加密方案的攻击, 构造周期函数是关键。一般基于两种特殊形式的可调加密方案构造周期函数: 一种是固定调柄, 一种是变化调柄。本文用变化调柄的方法给出了对 CMC 和 TET 两种可调加密方案更简洁的量子攻击方法。通过对比分析, 固定调柄和变化调柄两种不同的 Simon 量子攻击方式得到的周期不同, 可结合得到进一步的结果。最后本文从固定调柄和变化调柄的角度对可调加密方案的一般量子攻击方法进行了总结, 并给出了对基于泛哈希函数可调加密方案(Hash-CTR-Hash 和 Hash-ECB-Hash)的通用攻击。

关键词 可调加密方案; HCTR; HCH; PEP; HEH; Simon 量子算法
中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.03.08

Study on Tweakable Enciphering Schemes Against Simon's Quantum Algorithm

MAO Shuping[1,2], WANG Peng[1,2], HU Lei[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract With the rapid development of quantum computers and quantum computing technology, the threat of quantum attack algorithms to the security of cryptosystems is imminent. Previous studies have shown that many classically secure symmetric cryptographic structures or schemes are not secure under quantum attacks based on Simon's algorithm, for example, 3 rounds Feistel structure, Even-Mansour structure, and schemes including CBC-MAC, GCM, OCB, etc. Usually designed as block cipher modes of operation, tweakable enciphering schemes can be used as disk sector encryption algorithm and its structures can be divided into three types: Encrypt-Mask-Encrypt (CMC, EME, EME*, etc.), Hash-CTR-Hash (XCB, HCTR, HCH, etc.) and Hash-ECB-Hash (PEP, TET, HEH, etc.). This paper uses Simon's algorithm to analyze four tweakable enciphering schemes including HCTR, HCH, PEP and HEH, showing that these four tweakable enciphering schemes are insecure under the quantum chosen-plaintext attacks. The period of the periodic function related to the secret value of the scheme can be obtained by using Simon's algorithm with polynomial quantum queries, and then can be used to distinguish the scheme from a tweakable random permutation. For attacks on tweakable enciphering schemes using Simon's algorithm, the construction of periodic functions is the key point. Generally, periodic functions are constructed based on two special forms of tweakable enciphering schemes: one is fixed tweaks, and the other is variable tweaks. More concise quantum attacks against two tweakable enciphering schemes CMC and TET are given by using the method of variable tweaks. It is shown that the two different quantum attacks with fixed tweaks and variable tweaks have different periods, which can be combined to obtain further results. Finally, we summarize general quantum attacking methods against tweakable enciphering schemes from the perspective of fixed tweaks and variable tweaks, and gives a general attack on tweakable enciphering schemes based on universal hash functions (Hash-CTR-Hash and Hash-ECB-Hash).

Key words tweakable enciphering scheme; HCTR; HCH; PEP; HEH; Simon's Algorithm

---

通讯作者: 王鹏, 博士, 副研究员, Email: wpeng@iie.ac.cn
本课题得到国家自然科学基金(No. 61732021)和国家重点研发计划(No. 2018YFB0803800, No. 2018YFA0704704)资助。
收稿日期: 2020-05-30; 修改日期: 2020-09-08; 定稿日期: 2022-12-07

1 引言

1.1 可调加密方案

2011 年, Liskov 等人[1]提出了可调分组密码(tweakable block ciphers, 简称 TBC)的概念，将“调柄”加入了分组密码之中。调柄的加入使得分组密码更易于使用, 基于其上的工作模式安全性更加容易证明。可调分组密码这一概念原本是为工作模式设计服务的, 随后人们发现这一概念同时适用于磁盘扇区加密。磁盘扇区进行加密时, 扇区地址对应调柄, 每个扇区的明文和密文等长。磁盘扇区长度大于一般分组密码分组长度, 一般需要再基于分组密码或者可调分组密码进行构造, 这种加密方案被称为可调加密方案(tweakable enciphering scheme, 简称 TES)。可调加密方案与可调分组加密的安全性定义一致, 区别在于可调分组密码的分组长度固定, 可调加密方案的分组长度一般是可变长的.可调加密方案应用广泛, 不仅可以直接用于磁盘扇区加密, 而且可以通过简单对明文加入冗余信息的方式, 成为认证加密方案, 例如 AEZ 等方案的设计, 其核心就是一个可调加密方案。

可调加密方案可以分为 Encrypt-Mask-Encrypt、Hash-CTR-Hash 和 Hash-ECB-Hash 三种类型。其中 Encrypt-Mask-Encrypt 类型的第一和三层都是加密模式(Encrypt), 第二层先生成一些非线性的值, 然后对其它对分组进行异或(Mask), 这一类型包括 CMC[2]、EME[3]、EME*[4]等; Hash-CTR-Hash 类型的第一和三层用到了泛哈希函数(universal hash function)处理数据, 第二层主要用 CTR 模式加密数据, 这一类型包括 XCB[5]、HCTR[6]、HCH[7]等; Hash-ECB-Hash 类型的第一和三层用到了泛哈希函数处理数据, 第二层用 ECB 模式加密数据, 这一类型包括 PEP[8]、TET[9]、HEH[10]等。

1.2 量子算法

近年来量子技术迅速发展, 量子算法在许多问题上可以达到经典算法的指数级加速。Shor[11]研究发现大数分解问题和离散对数问题都存在量子多项式时间算法, 比相应的经典算法具有指数级的加速。由于 Shor 算法, 量子计算对 RSA 等公钥密码构成了严重威胁。在对称密码领域, 一直以来都认为最大的威胁来自于 Grover 量子搜索算法[12], 此算法可以将 k 比特密钥的搜索复杂度降低为 $O\left(2^{\frac{k}{2}}\right)$。Simon[13]提出的量子算法可以用 $O(n)$次查询获取特殊函数 f 的周期, 远远优于经典算法 $O\left(2^{\frac{n}{2}}\right)$次的查询。我们将这一算法称为 Simon 算法。近些年来, Simon 量子算法在对称密码领域得到应用, 表明某些对称密码在量子攻击下的脆弱性。

1.3 基于 Simon 算法的量子攻击

利用 Simon 算法的量子攻击可分为以下几步:

(1) 利用原方案构造一个周期函数, 周期一般是一个和密钥等秘密信息相关的值;

(2) 利用 Simon 量子算法求出周期;

(3) 利用得到的周期, 对原方案进行区分、伪造等攻击。

2010 年, Kuwakado 和 Morii[14]利用 Simon 算法给出了 3 轮 Feistel 结构的量子选择明文攻击, 该攻击可在多项式时间内将轮函数为随机置换的 3 轮 Feistel 结构与随机置换区分开来。2012 年, 他们利用 Simon 算法对 Even-Mansour 结构的分组密码进行了攻击[15], 表明 Even-Mansour 结构在量子环境下不安全。2016 年, Kaplan 等人[16]针对 Simon 承诺条件弱化的情况作了分析, 表明在轮函数为随机函数的情况下 Simon 算法仍有极大的概率成功, 并对 CBC-MAC、GCM、OCB 等分组密码工作模式进行了量子攻击。2017 年 Leander 和 May[17]将 Simon 算法与 Grover 算法结合起来, 用 Grover 算法搜索的同时, 用 Simon 算法求周期, 表明分组密码前后异或独立密钥并不能在量子环境下提高安全性。2019 年, 罗宜元等人[18]利用 Simon 算法对三轮 MISTY-L 结构与 3 轮 MISTY-R 结构进行了区分攻击。

2019 年 Ghosh 和 Sarkar[19]利用 Simon 算法分析了 6 种可调加密方案, 包括 CMC、EME、XCB、TET、AEZ 和 FAST, 这些方案在经典计算环境下都被证明是安全的, 但是在量子环境下只需要 $O(n)$次查询就可以将其和随机置换区分开来。

1.4 本文贡献

本文的贡献分为以下 3 个方面:

(1) 首次给出了对 4 种可调加密方案的量子攻击方法, 包括 HCTR、HCH、PEP 和 HEH。在经典环境中, 这些方案都是可证明安全的。而在量子环境中, 使用 Simon 量子算法可在多项式时间内将 HCTR、HCH、PEP 和 HEH 方案与可调随机置换区分开来, 因此上述 4 种可调加密方案在量子环境下是不安全的。

(2) 我们具体使用了固定调柄和变化调柄两种不同攻击方法。用变化调柄法给出了 CMC 和 TET

更简洁的攻击。某些可调加密方案同时可以用两种攻击, 所得周期涉及变量也不同, 可根据攻击需要选择或结合两种攻击方式分析。

(3) 给出了利用 Simon 算法攻击 Hash-CTR-Hash 和 Hash-ECB-Hash 两类可调加密方案的统一方法。

2 基础知识

2.1 基本定义

分组密码是一个函数 E: $\mathcal{K}\times\mathcal{M}\rightarrow\mathcal{M}$, 其中 $\mathcal{K}\neq\phi$ 是密钥空间, $\mathcal{M}\neq\phi$ 是消息空间, $E_K(\cdot)=E(K,\cdot)$ 是所有 $K\in\mathcal{K}$ 的保长置换。可调分组密码是函数 E: $\mathcal{K}\times\mathcal{T}\times\mathcal{M}\rightarrow\mathcal{M}$ 其中 $\mathcal{T}$ 是调柄空间, $\widetilde{E}_K^T(\cdot)=\widetilde{E}_K(T,\cdot)=\widetilde{E}(K,T,\cdot)$ 是所有 $K\in\mathcal{K}$ 和 $T\in\mathcal{T}$ 的保长置换。

我们令 $s\overset{R}{\leftarrow}S$ 表示通过均匀分布从集合 S 中选择一个随机元素 s。令 $Perm(\mathcal{M})$ 为 $\mathcal{M}$ 上所有保长置换的集合。当 $\mathcal{M}=\{0,1\}^n$ 时, 将其表示为 $Perm(n)$。同时令 $Perm^{\mathcal{T}}(\mathcal{M})$ 为从 $\mathcal{T}$ 到 $Perm(\mathcal{M})$ 的所有映射的集合。$Perm^{\mathcal{T}}(\mathcal{M})$ 也可以看作是所有分组密码 E: $\mathcal{T}\times\mathcal{M}\rightarrow\mathcal{M}$ 的集合。如果 $\widetilde{\pi}\overset{R}{\leftarrow}Perm^{\mathcal{T}}(\mathcal{M})$, 则对于每一个 $T\in\mathcal{T}$, $\widetilde{\pi}^T(\cdot)=\widetilde{\pi}(T,\cdot)$ 是一个随机置换。当 $\mathcal{M}=\{0,1\}^n$ 时, 我们表示为 $Perm^{\mathcal{T}}(\mathcal{M})$。

敌手 A 是一种可以访问一个或多个查询对象的算法, 查询对象一般写在敌手 A 的上标位置。令 $A^{\rho}\Rightarrow 1$ 是带有查询对象 ρ 的敌手 A 输出比特 1 的事件。

如果可调分组密码 E: $\mathcal{K}\times\mathcal{T}\times\mathcal{M}\rightarrow\mathcal{M}$ 无法与可调随机置换 $\widetilde{\pi}\overset{R}{\leftarrow}Perm^{\mathcal{T}}(\mathcal{M})$ 区分开, 则称可调分组密码是一个可调(强)伪随机置换($\widetilde{prp}$ 或 $\widetilde{sprp}$)。具体来说:

$$\begin{aligned}\mathrm{Adv}_{\widetilde{E}}^{\widetilde{prp}}(A) &= \Pr\left[K\overset{R}{\leftarrow}\mathcal{K}: A^{\widetilde{E}_K(\cdot,\cdot)}\Rightarrow 1\right]- \\ &\quad \Pr\left[\widetilde{\pi}\overset{R}{\leftarrow}\mathrm{Perm}^{\mathcal{T}}(\mathcal{M}): A^{\widetilde{\pi}(\cdot,\cdot)}\Rightarrow 1\right] \\ \mathrm{Adv}_{\widetilde{E}}^{\widetilde{sprp}}(A) &= \Pr\left[K\overset{R}{\leftarrow}\mathcal{K}: A^{\widetilde{E}_K(\cdot,\cdot),\widetilde{E}_K^{-1}(\cdot,\cdot)}\Rightarrow 1\right]- \\ &\quad \Pr\left[\widetilde{\pi}\overset{R}{\leftarrow}\mathrm{Perm}^{\mathcal{T}}(\mathcal{M}): A^{\widetilde{\pi}(\cdot,\cdot),\widetilde{\pi}^{-1}(\cdot,\cdot)}\Rightarrow 1\right]\end{aligned}$$

若对于任意满足一定资源限制的敌手 A 来说, $\mathrm{Adv}_{\widetilde{E}}^{\widetilde{prp}}(A)$ 是可忽略的, 则称 $\widetilde{E}$ 为可调伪随机置换($\widetilde{prp}$), 即选择明文攻击安全的; 若 $\mathrm{Adv}_{\widetilde{E}}^{\widetilde{sprp}}(A)$ 是可忽略的, 则称 $\widetilde{E}$ 是可调强伪随机置换($\widetilde{sprp}$), 即选择密文攻击安全的。

2.2 Simon 算法及扩展

1997 年, Simon [13]提出了 Simon 问题和 Simon 量子算法, 该算法对经典算法作出了指数级加速。Simon 问题可以叙述如下:

Simon 问题: 给定一个布尔函数 f:$\{0,1\}^n\rightarrow\{0,1\}^n$, 对 $x,y\in\{0,1\}^n$, 满足条件 $[f(x)=f(y)]\Leftrightarrow[x\oplus y\in\{0^n,s\}]$, s 非零且 $s\in\{0,1\}^n$, 目标是求出 s 的值。

其中条件 $[f(x)=f(y)]\Leftrightarrow[x\oplus y\in\{0^n,s\}]$ 称为 Simon 承诺, 表明 s 是函数 f 唯一的周期。用“$\oplus$”表示二进制异或操作, 查询函数 f 满足 $|x\rangle|y\rangle\mapsto|x\rangle|y\oplus f(x)\rangle$。Simon 算法用量子复杂度 $O(n)$ 来计算 s, 远远优于经典算法的 $O\left(2^{\frac{n}{2}}\right)$ 次的查询。对于 Simon 问题, $x\in\{0,1\}^n$, 在 n 量子比特状态 $|x\rangle$ 的 Hadamard 变换 $H^{\otimes n}$ 有 $H^{\otimes n}|x\rangle=\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$,其中有 $x\cdot y:=x_1y_1\oplus\cdots\oplus x_ny_n$。

Simon 算法的步骤如下:

(1) 初始化 $2n$ 个量子比特状态为 $|0\rangle^{\otimes n}|0\rangle^{\otimes n}$;

(2) 将 Hadamard 变换 $H^{\otimes n}$ 应用于前 n 个量子比特获得量子叠加 $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle$;

(3) 对函数 f 的量子查询将其映射到状态 $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$;

(4) 对后 n 个量子比特测量, 得到 $f(x)$ 的输出 y, 同时前 n 个量子比特坍缩为 $\frac{1}{\sqrt{2}}(|z\rangle+|z\oplus s\rangle)$;

(5) 对前 n 个量子再次应用 Hadamard 变换 $H^{\otimes n}$ 得到 $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{y\cdot z}(1+(-1)^{y\cdot s})|y\rangle$, 此时若 $y\cdot s=1$ 则 $|y\rangle$ 幅度为 0 测量不到, 因此若测量得到 $|y\rangle$ 必有 $y\cdot s=0$, 即测量得到的 $|y\rangle$ 必与 s 正交。

通过重复该步骤 $n-1$ 次, 可以获得 $n-1$ 个与 s 正交的独立向量 $\boldsymbol{y}$, 因此可以使用线性代数来恢复 s.

引理 1.[17] 令 $U\subset\mathbb{F}_2^n$ 为 $n-1$ 维子空间。若获得 $n-1$ 个正交独立向量 $u_1,\ldots,u_{n-1}\in U$, 则 $u_1,\ldots,u_{n-1}$ 线性独立且形成 U 的基的概率大于 $\frac{1}{4}$。

实际上对于引理 1, 至少可以以 0.288 的概率得到 $n-1$ 个独立向量, 文献[18]指出当 $m=20$ 时算法成功率大于 0.99。

2016 年, Kaplan 等人[16]针对 Simon 承诺条件弱化的情况作了分析, 并表明在轮函数为随机函数的情况下 Simon 算法仍有极大的概率成功。他们定义了一个衡量 Simon 承诺满足情况的指标并分析了在 Simon 承诺弱化的情况下 Simon 算法成功的概率:

定义 1. [16] 对于 f:$\{0,1\}^n\rightarrow\{0,1\}^n$, 且对任意 x 有 $f(x\oplus s)=f(x)$, 定义

$$\varepsilon(f,s)=\max_{t\in\{0,1\}^n\setminus\{0,s\}}\Pr_x[f(x)=f(x\oplus t)]。$$

定理 1.[16](具有近似承诺的 Simon 算法) 如果

$\varepsilon(f,s)\leqslant p_0<1$, 则Simon算法经过 cn 次查询后, 得到正确 s 的概率至少为 $1-\left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$。

定理 2.[16] 在Simon算法的 cn 次查询之后, 如果 t 与算法的每个步骤返回的所有向量 $\boldsymbol{u}_i$ 正交, 则 $\Pr_x[f(x\oplus t)=f(t)]\geqslant p_0$概率至少为 $1-\left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$。

2019 年, 罗宜元等人[18]证明了即使 Simon 承诺不完全满足, 若函数 f 存在周期, 则其只存在唯一周期的概率接近 1, 并计算表明当 $n\geqslant4$ 即 $N\geqslant2^4$时 $P(n)>0.99$, 即当周期函数 f 的输入输出长度≥4时, 其存在唯一周期的概率大于 0.99。

3 常见可调加密方案的 Simon 量子算法攻击

对于利用 Simon 算法对可调加密方案的攻击, 构造周期函数是关键。一般基于两种特殊形式的可调加密方案构造周期函数: 一种是固定调柄, 考虑两到三个分组输入的情况; 另一种将调柄当成变量, 考虑一个明文分组输入的情况。在之前利用 Simon 算法对分组密码工作模式的攻击, 由于不涉及调柄, 多采用第一种形式。文献[19]对 CMC、XCB、TET 等可调加密方案的攻击亦延续了这种攻击方式。事实上, 由于调柄的加入, 使得对可调加密方案的攻击更加简洁, 两种攻击方式得到的周期也不尽相同。

下文我们首先使用第一种攻击和第二种攻击形式对 HCTR、HCH、HEH (3.1-3.3) 进行区分攻击, 随后使用第二种攻击形式对 PEP (3.4) 以及文献[19]中攻击过的 CMC (3.5) 、TET (3.6) 进行攻击。可以看出如果第二种攻击形式可以攻击成功, 得出的周期多比第一种攻击形式得出的周期形式简单, 涉及变量少。可以通过对两种攻击形式的结合进行进一步分析。表 1 给出了我们对可调加密方案的攻击汇总。

表 1 可调分组密码两种攻击周期汇总

Table 1 Summary of periods in two attacks

周期	固定调柄		变化调柄		备注
CMC	$E_K(E_K(m\oplus E_{K'}(\mathrm{T}))\oplus\alpha_0)\oplus E_K(E_K(m\oplus E_{K'}(\mathrm{T}))\oplus\alpha_1)$	文献[19]	$E_{K'}(t_0)\oplus E_{K'}(t_1)$	3.5	Hash-CTR-Hash 类型与 Hash-ECB-Hash 类型的一般攻击方法 (本文 4.2)
HCTR	$1\|\|\alpha_0H^3\oplus\alpha_1H^3$	3.1	$1\|\|\alpha_0H^2\oplus\alpha_1H^2$	3.1	
HCH	$1\|\|\alpha_0R^2\oplus\alpha_1R^2$	3.2	输入长度不可为 1 个分组[7]		
PEP			$EN\oplus EN'$	3.4	
TET	$\alpha^2\beta\oplus\beta\|\|\frac{(\alpha^2\beta\oplus\beta)(\tau\oplus\tau^3)}{\tau^2}\|\|\alpha^2\beta\oplus\beta$	文献[19]	$\frac{\beta\oplus\beta'}{1\oplus\tau}$	3.6	
HEH	$s\|\|s\|\|0^n, s=xEN\oplus x^2EN$	3.3	$EN(t_0)\oplus EN(t_1)$	3.3	

3.1 对 HCTR 的攻击

HCTR 是 2005 年由 Wang, Feng 和 Wu [6]提出的可调加密方案, 被证明是一种可调强伪随机置换。2008 年 Chakraborty 和 Nandi[20]对 HCTR 的安全性界进行了改进。

3.1.1 固定调柄的攻击

固定一个分组的调柄, 当输入是两个分组数据时, HCTR 的加密算法如下。其中输入为(T,P_1,P_2), 输出为(C_1,C_2), 其中$P_1,P_2,C_1,C_2\in\{0,1\}^n$, $H\in\{0,1\}^n$, $K\in\{0,1\}^k$, $T\in\{0,1\}^n$。对于 $0\leqslant i\leqslant2^n-1$, 用 $bin_n(i)$ 表示整数 i 的 n 位二进制表示。$2n$ 表示输入长度的二进制表示, 乘法为有限域 $GF(2^n)$中的乘法。

HCTR $_{K,H}^{T}(P_1,P_2)$:

$M_1\leftarrow P_1\oplus P_2H^3\oplus TH^2\oplus bin_n(2n)H$

$CC\leftarrow E_K(M_1)$

$S\leftarrow M_1\oplus CC$

$C_2\leftarrow P_2\oplus E_K(S\oplus1)$

$C_1\leftarrow CC\oplus C_2H^3\oplus TH^2\oplus bin_n(2n)H$

$return(C_1,C_2)$

在下文中, 我们从 HCTR 定义了周期函数 f, 并利用 Simon 算法求出周期, 从而将 HCTR 与可调随机置换区分开来。令 $x\in\{0,1\}^n$;$\alpha_0,\alpha_1\in\{0,1\}^n$且$\alpha_0\neq\alpha_1$, b 是一个比特, $T\in\{0,1\}^n$取常数。定义函数 f 如下:

$$\begin{aligned} f:\{0,1\}\times\{0,1\}^n &\to\{0,1\}^n\\ (b,x) &\mapsto C_2\oplus\alpha_b,(C_1,C_2)\leftarrow\mathbf{HCTR}_{K,H}^{T}(x,\alpha_b)\end{aligned}$$

则有:

$b\oplus b'=1,x\oplus x'=\alpha_0h^3\oplus\alpha_1h^3\Rightarrow f(b,x)=f(b',x')$当输入是$(0,x)$时, 我们有:

$$M_1 = x \oplus \alpha_0 H^3 \oplus TH^2 \oplus bin_n(2n)H$$
$$C_2 = \alpha_0 \oplus E_K(M_1 \oplus E_K(M_1) \oplus 1)$$
$$C_2 \oplus \alpha_0 = E_K(M_1 \oplus E_K(M_1) \oplus 1)$$

当输入是$(1,x \oplus s),s = \alpha_0 H^3 \oplus \alpha_1 H^3$时, 我们有:

$$\begin{aligned} M_1 &= x \oplus s \oplus \alpha_1 H^3 \oplus TH^2 \oplus bin_n(2n)H \\ &= x \oplus \alpha_0 H^3 \oplus TH^2 \oplus bin_n(2n)H \\ C_2 &= \alpha_1 \oplus E_K(M_1 \oplus E_K(M_1) \oplus 1) \\ C_2 \oplus \alpha_1 &= E_K(M_1 \oplus E_K(M_1) \oplus 1) \end{aligned}$$

输入$(0,x)$及输入$(1,x \oplus s)$, $s = \alpha_0 H^3 \oplus \alpha_1 H^3$时, 两个$M_1$相等, 故后边两个$C_2 \oplus \alpha_b$相等, 确定$1||s,s = \alpha_0 H^3 \oplus \alpha_1 H^3$为函数$f$的周期.文献[18]中指出, 在 Simon 算法中, 当运行全算法 20 次及以上的时候, 找到正确周期值的概率大于 0.99。同时指出当周期函数f的输入输出长度$n \geqslant 4$时, 函数f存在唯一周期的概率大于 0.99。

而当周期不唯一时, 即 Simon 算法满足近似承诺, 有$\varepsilon(f,1||s) < \frac{1}{2}$, 进而由定理 1 可知则 Simon 的算法经过cn次查询后, 得到正确$1||s$的概率至少为$1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$。下证$\varepsilon(f,1||s) < \frac{1}{2}$。

假设$\varepsilon(f,1||s) \geqslant \frac{1}{2}$, 则存在$(\tau,t) \notin \{(0,0),(1,s)\}$使得$\Pr[f(b,x) = f(b \oplus \tau,x \oplus t)] \geqslant \frac{1}{2}$。

若$\tau = 0$, 则有$\Pr[f(0,x) = f(0,x \oplus t)] \geqslant \frac{1}{2}$或$\Pr[f(1,x) = f(1,x \oplus t)] \geqslant \frac{1}{2}$, 即对$b$有:

$$\begin{aligned} \Pr\ &[E_K(x \oplus \alpha_b H^3 \oplus TH^2 \oplus bin_n(2n)H \oplus \\ &E_K(x \oplus \alpha_b H^3 \oplus TH^2 \oplus bin_n(2n)H) \oplus 1) \\ &= E_K(x \oplus t \oplus \alpha_b H^3 \oplus TH^2 \oplus bin_n(2n)H \oplus \\ &E_K(x \oplus t \oplus \alpha_b H^3 \oplus TH^2 \oplus bin_n(2n)H) \oplus 1)] \\ \geqslant\ &\frac{1}{2} \end{aligned}$$

即有:

$$\Pr\ [E_K(x \oplus E_K(x) \oplus 1) = E_K(x \oplus t \oplus E_K(x \oplus t) \oplus 1)] \geqslant \frac{1}{2}$$

若$\tau = 1$, 则有:

$$\begin{aligned} \Pr\ &[E_K(x \oplus \alpha_0 H^3 \oplus TH^2 \oplus bin_n(2n)H \oplus \\ &E_K(x \oplus \alpha_0 H^3 \oplus TH^2 \oplus bin_n(2n)H) \oplus 1) \\ &= E_K(x \oplus t \oplus \alpha_1 H^3 \oplus TH^2 \oplus bin_n(2n)H \oplus \\ &E_K(x \oplus t \oplus \alpha_1 H^3 \oplus TH^2 \oplus bin_n(2n)H) \oplus 1)] \\ \geqslant\ &\frac{1}{2} \end{aligned}$$

即有:

$$\begin{aligned} \Pr\ &[E_K(x \oplus E_K(x) \oplus 1) \\ &= E_K(x \oplus t \oplus \alpha_0 H^3 \oplus \alpha_1 H^3 \oplus \\ &E_K(x \oplus t \oplus \alpha_0 H^3 \oplus \alpha_1 H^3) \oplus 1)] \\ \geqslant\ &\frac{1}{2} \end{aligned}$$

即若$\varepsilon(f,1||s) \geqslant \frac{1}{2}$, 则存在一个$u$使得

$$\Pr\ [E_K(x \oplus E_K(x) \oplus 1) = E_K(x \oplus u \oplus E_K(x \oplus u) \oplus 1)] \geqslant \frac{1}{2}$$

即若$\varepsilon(f,1||s) \geqslant \frac{1}{2}$, 则函数$E_K(x \oplus E_K(x) \oplus 1)$存在碰撞的概率大于等于$\frac{1}{2}$。假设$E_K$为一个随机置换, 对于不同的$x_1,x_2$, 则有:

$$\Pr\ [E_K(x_1 \oplus E_K(x_1) \oplus 1) = E_K(x_2 \oplus E_K(x_2) \oplus 1)] \geqslant \frac{1}{2}$$

即有:

$$\Pr\ [E_K(x_1) = x_1 \oplus x_2 \oplus E_K(x_2)] \geqslant \frac{1}{2}$$

当x_1,x_2取固定值时, $x_1 \oplus x_2 \oplus E_K(x_2)$为一个固定值, 而$E_K$为一个随机置换, 因此:

$$\Pr\ [E_K(x_1) = x_1 \oplus x_2 \oplus E_K(x_2)] = \frac{1}{2^n}$$

当$n > 1$时, 存在碰撞的概率小于$\frac{1}{2}$, 矛盾。故$\varepsilon(f,1||s) < \frac{1}{2}$, 由定理 1 可知 Simon 的算法经过$cn$次查询后, 得到正确$1||s$的概率至少为$1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$。

攻击者 A 分别用(b,x)和$(b \oplus 1,x \oplus s)$对$\mathcal{O}$进行询问, 得到(C_1,C_2), 计算$C_2 \oplus \alpha_b$, 如果结果相等就输出 1, 否则输出 0。那么$\Pr[A^{\tilde{\pi}(b,x)} \Rightarrow 1] = \frac{1}{2^n}$, $\Pr[A^{\mathrm{HCTR}} \Rightarrow 1] = 1$, 因此$\mathrm{Adv}_{\mathrm{HCTR}}^{\widetilde{prp}}(A) = 1 - \frac{1}{2^n}$, 可以将 HCTR 与可调随机置换区分开来, 因此 HCTR 在量子选择明文攻击环境中是不安全的。

以下分析中, 对于获得周期的概率以及利用周期做区分攻击都是类似的, 因此都省略, 只保留了关键的构造周期函数和利用 Simon 算法求周期的方法。

3.1.2 变化调柄的攻击

当输入为 1 个分组时, HCTR 加密算法如下。其中输入为P_1, 输出为C_1, $P_1,C_1 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$.

$$\begin{aligned} &\mathbf{HCTR}_{K,H}^{T}(P_1): \\ &\quad M_1 \leftarrow P_1 \oplus TH^2 \oplus bin_n(n)H \\ &\quad C_1 \leftarrow E_K(M_1) \oplus TH^2 \oplus bin_n(n)H \\ &return\ \ (C_1,C_2) \end{aligned}$$

令$y \in \{0,1\}^n;t_0,t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f:\{0,1\}^n &\to \{0,1\}^n \\ y &\mapsto C_1 \oplus C'_1 \\ &\quad C_1 \leftarrow \mathbf{HCTR}_{K,H}^{t_0}(y), C'_1 \leftarrow \mathbf{HCTR}_{K,H}^{t_1}(y) \\ f(y) &\mapsto E_K(y \oplus t_0 H^2 \oplus bin_n(n)H) \oplus t_0 H^2 \oplus \\ &\quad E_K(y \oplus t_1 H^2 \oplus bin_n(n)H) \oplus t_1 H^2 \end{aligned}$$

则有 $s = t_0H^2 \oplus t_1H^2 \Rightarrow f(y) = f(y \oplus s)$。可以确定 $s = t_0H^2 \oplus t_1H^2$为函数 $f(y)$周期。HCTR 在量子环境中选择明文攻击不安全。

3.2 对 HCH 的攻击

HCH 由 Chakraborty 和 Sarkar[7]构造, 固定一个分组的调柄, 当输入为 3 个分组时, 加密算法如下。其中输入为 (T,P_1,P_2,P_3), 输出为 (C_1,C_2,C_3), 其中 $P_1,P_2,P_3,C_1,C_2,C_3 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$。对于 $0 \leqslant i \leqslant 2^n - 1$, 用 $bin_n(i)$表示整数 i 的 n 位二进制表示。

$$
\begin{aligned}
&\textbf{HCH}\quad {}_K^T(P_1,P_2,P_3):\\
&\qquad R = E_K(T); Q = E_K(R \oplus bin_n(3n));\\
&\qquad M_1 = Q \oplus P_1 \oplus P_2R \oplus P_3R^2;\\
&\qquad S = E_K(M_1 \oplus E_K(M_1));\\
&\qquad C_2 = P_2 \oplus E_K(S \oplus bin_n(1))\\
&\qquad C_3 = P_3 \oplus E_K(S \oplus bin_n(2))\\
&\qquad C_1 = xQ \oplus E_K(M_1) \oplus C_2R \oplus C_3R^2;\\
&return\quad (C_1,C_2,C_3)
\end{aligned}
$$

在下文中, 我们从 HCH 定义了周期函数 f, 并利用 Simon 算法求出周期, 从而将 HCH 与可调随机置换区分开来。令 $y \in \{0,1\}^n; \alpha_0,\alpha_1 \in \{0,1\}^n$且$\alpha_0 \neq \alpha_1$, b 是一个比特, $T \in \{0,1\}^n$取常数。定义以下函数:

$$
\begin{aligned}
f: \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n\\
(b,y) &\mapsto C_2, (C_1,C_2,C_3) \leftarrow \textbf{HCH}_K^T(y,0^n,\alpha_b)
\end{aligned}
$$

则有:

$$
b \oplus b' = 1, y \oplus y' = \alpha_0R^2 \oplus \alpha_1R^2 \Rightarrow f(b,y) = f(b',y')
$$

当输入是$(0,y)$时, 我们有:

$$
\begin{aligned}
R &= E_K(T); Q = E_K(R \oplus bin_n(3n))\\
M_1 &= Q \oplus y \oplus \alpha_0R^2\\
S &= E_K(M_1 \oplus E_K(M_1))\\
C_2 &= E_K(S \oplus bin_n(1))\\
&= E_K(E_K(Q \oplus y \oplus \alpha_0R^2 \oplus E_K(Q \oplus y \oplus \alpha_0R^2)) \oplus bin_n(1))
\end{aligned}
$$

当输入是$(1,y \oplus s), s = \alpha_0R^2 \oplus \alpha_1R^2$时, 有:

$$
\begin{aligned}
R &= E_K(T); Q = E_K(R \oplus bin_n(3n))\\
M_1 &= Q \oplus y \oplus s \oplus \alpha_1R^2 = Q \oplus y \oplus \alpha_0R^2\\
S &= E_K(M_1 \oplus E_K(M_1))\\
C_2 &= E_K(S \oplus bin_n(1))\\
&= E_K(E_K(Q \oplus y \oplus \alpha_0R^2 \oplus E_K(Q \oplus y \oplus \alpha_0R^2)) \oplus bin_n(1))
\end{aligned}
$$

由上式可以看出当输入为$(0,y)$以及输入为$(1,y \oplus s), s = \alpha_0R^2 \oplus \alpha_1R^2$时, 两个$M_1$相等, 故后边两个$C_2$相等, 确定 $1||\alpha_0R^2 \oplus \alpha_1R^2$为函数 f 的周期, 可知当运行 Simon 算法 20 次及以上时, 可以找到正确的周期 $1||\alpha_0R^2 \oplus \alpha_1R^2$的值。当 $n \geqslant 4$ 时, Simon 函数以大于 0.99 的概率只具有唯一周期, 而当周期不唯一时, 即 Simon 算法满足近似承诺, 有 $\varepsilon(f,1||s) < \frac{1}{2}$, 进而由定理 1 可知则 Simon 的算法经过 cn 次查询后, 得到正确 $1||s$ 的概率至少为 $1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$。同理有即$\mathrm{Adv}_f(A)$不可忽略, 因此可以通过输出值在多项式时间内区分 HCH 与可调随机置换, 因此 HCH 在量子环境中选择明文攻击不安全。

3.3 对 HEH 的攻击

3.3.1 固定调柄的攻击

HEH 由 Sarkar[10]在 2007 年构造, 固定一个分组的调柄, 我们以 3 个输入分组$(m = 3)$为例, 加密算法如下。其中输入为(T,P_1,P_2,P_3), 输出为(C_1,C_2,C_3), $P_1,P_2,P_3,C_1,C_2,C_3 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$。x 代表有限域 $GF(2^n)$中的常数 2, α为常数值初始元素。

$$
\begin{aligned}
&\textbf{HEH}\quad {}_K^T(P_1,P_2,P_3):\\
&\qquad R = E_K(T); EN = E_K(R \oplus \mathrm{bin}_n(3));\\
&\qquad EN' = xEN; U = U_R \oplus P_3\\
&\qquad PPP_1 = P_1 \oplus U \oplus xEN\\
&\qquad PPP_2 = P_2 \oplus U \oplus x^2EN\\
&\qquad PPP_3 = U \oplus EN\\
&\qquad CCC_1 = E_K(PPP_1); CCC_2 = E_K(PPP_2);\\
&\qquad CCC_3 = E_K(PPP_3)\\
&\qquad V = CCC_3 \oplus EN'\\
&\qquad C_1 = CCC_1 \oplus \alpha EN' \oplus V\\
&\qquad C_2 = CCC_2 \oplus \alpha^2EN' \oplus V\\
&\qquad C_3 = V \oplus W_R\\
&return\quad (C_1,C_2,C_3)
\end{aligned}
$$

在下文中, 我们从 HEH 定义了周期函数 f, 并利用 Simon 算法求出周期, 从而将 HEH 与可调随机置换区分开来。令 $y \in \{0,1\}^n; T \in \{0,1\}^n$, m'是一个常数。定义以下函数:

$$
\begin{aligned}
f: \{0,1\}^n &\to \{0,1\}^n\\
y &\mapsto C_1 \oplus C_2, (C_1,C_2,C_3) \leftarrow \textbf{HEH}_K^T(y,y,m')
\end{aligned}
$$

则有:

$f(y||y||m') = f(y \oplus xEN \oplus x^2EN||y \oplus xEN \oplus x^2EN||m')$当输入是 y 时, 我们有:

$$
\begin{aligned}
R &= E_K(T); EN = E_K(R \oplus \mathrm{bin}_n(3));\\
EN' &= xEN;\\
U &= U_R \oplus P_3\\
PPP_1 &= y \oplus m' \oplus U_R \oplus xEN\\
PPP_2 &= y \oplus m' \oplus U_R \oplus x^2EN\\
PPP_3 &= m' \oplus U_R \oplus EN\\
C_1 &= E_K(PPP_1) \oplus E_K(PPP_3) \oplus EN' \oplus \alpha EN'\\
C_2 &= E_K(PPP_2) \oplus E_K(PPP_3)\\
&\quad \oplus EN' \oplus \alpha^2EN'
\end{aligned}
$$

$$\begin{aligned} C_1 \oplus C_2 &= E_K(PPP_1) \oplus E_K(PPP_2) \\ &\quad \oplus \alpha EN' \oplus \alpha^2 EN' \\ &= E_K\big(y \oplus m' \oplus U_R \oplus xEN\big) \oplus \\ &\quad E_K\big(y \oplus m' \oplus U_R \oplus x^2 EN\big) \oplus \\ &\quad \alpha EN' \oplus \alpha^2 EN' \end{aligned}$$

由上式可以看出当输入为 $y||y||m'$以及输入为 $y \oplus s||y \oplus s||m'$,$s = xEN \oplus x^2 EN$ 时, $C_1 \oplus C_2$相同, 确定 $s||s||0^n$,$s = xEN \oplus x^2 EN$ 为函数 f 的周期, 因此 HEH 在量子环境中选择明文攻击不安全。

3.3.2 变化调柄的攻击

当输入为 1 个分组时, HEH 加密算法如下。其中输入为P_1, 输出为C_1, P_1,$C_1 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$。

$$\begin{aligned} &\mathbf{HEH}{}^{T}_{K}(P_1): \\ &\quad R = E_K(T); EN = E_K(R \oplus \mathrm{bin}_n(1)) \\ &\quad PPP_1 = P_1 \oplus EN \\ &\quad CCC_1 = E_K(PPP_1) \\ &\quad C_1 = CCC_1 \oplus EN \oplus W_\tau \\ &return \quad (C_1) \end{aligned}$$

令 $y \in \{0,1\}^n$;t_0,$t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f: \{0,1\}^n &\to \{0,1\}^n \\ y &\mapsto C_1 \oplus C'_1 \\ &\quad C_1 \leftarrow \mathbf{HEH}^{t_0}_K(y), C'_1 \leftarrow \mathbf{HEH}^{t_1}_K(y) \\ f(y) &\mapsto E_K(y \oplus E_K(E_K(t_0) \oplus \mathrm{bin}_n(1))) \oplus \\ &\quad E_K(y \oplus E_K(E_K(t_1) \oplus \mathrm{bin}_n(1))) \oplus \\ &\quad E_K(E_K(t_0) \oplus \mathrm{bin}_n(1)) \oplus \\ &\quad E_K(E_K(t_1) \oplus \mathrm{bin}_n(1)) \end{aligned}$$

记 $EN(t_b) = E_K(E_K(t_b) \oplus \mathrm{bin}_n(1))$, 则有 $s = EN(t_0) \oplus EN(t_1) \Rightarrow f(y) = f(y \oplus s)$。可以确定 $s = EN(t_0) \oplus EN(t_1)$为函数 $f(y)$周期。HEH 在量子环境中选择明文攻击不安全。

3.4 对 PEP 的攻击

PEP 是 2006 年 Chakraborty 和 Sarkar [8]提出的方案, 我们以 1 个输入分组为例, 加密算法如下。其中输入为(T,P_1), 输出为C_1, P_1,$C_1 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$, x 代表有限域 $GF(2^n)$中的常数 2。

$$\begin{aligned} &\mathbf{PEP}{}^{T}_{K}(P_1): \\ &\quad R = E_K(T); EN = E_K(R \oplus bin_n(1)); \\ &\quad EEN = E_K(xEN) \\ &\quad PPP_1 = P_1 \oplus EN \\ &\quad CCC_1 = E_K(PPP_1) \\ &\quad C_1 = CCC_1 \oplus xEEN \\ &return \quad C_1 \end{aligned}$$

令 $y \in \{0,1\}^n$;t_0,$t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f: \{0,1\}^n &\to \{0,1\}^n \\ y &\mapsto C_1 \oplus C'_1, \\ &\quad C_1 \leftarrow PEP^{t_0}_K(y), C'_1 \leftarrow PEP^{t_1}_K(y) \\ f(y) &\mapsto E_K(y \oplus EN) \oplus xEEN \oplus \\ &\quad E_K\big(y \oplus EN'\big) \oplus xEEN' \end{aligned}$$

其中:

$$\begin{aligned} &EN = E_K(E_K(t_0) \oplus \mathrm{bin}_n(1)) \\ &EEN = E_K(xEN) \\ &EN' = E_K(E_K(t_1) \oplus \mathrm{bin}_n(1)) \\ &EEN' = E_K EEN' \end{aligned}$$

则有 $f(y) = f(y \oplus s) \Rightarrow s = EN \oplus EN'$。可以确定 $s = EN \oplus EN'$为函数 $f(y)$周期, 因此 PEP 在量子环境中选择明文攻击不安全。

3.5 对 CMC 的攻击

CMC 是 2003 年 Halevi 和 Rogaway [2]提出的方案, 在文献[19]中 Ghosh 和 Sarkar 两人使用固定调柄T', 对 3 个输入分组$(m||\alpha_b||x)$的 CMC 加密方案进行了攻击, 找到周期为:

$$E_K\big(E_K\big(m \oplus T'\big) \oplus \alpha_0\big) \oplus E_K\big(E_K\big(m \oplus T'\big) \oplus \alpha_1\big),$$

表明 CMC 在量子环境中选择明文攻击不安全。在这里我们以 1 个输入分组为例, 给出另一种攻击, CMC 加密算法如下。其中输入为P_1, 输出为C_1, P_1,$C_1 \in \{0,1\}^n$, K,$K' \in \{0,1\}^k$, $T \in \{0,1\}^n$。

$$\begin{aligned} &\mathbf{CMC}{}^{T}_{K,K'}(P_1): \\ &\quad PP_1 = P_1 \oplus E_{K'}(T) \\ &\quad PPP_1 = E_K\big(P_1 \oplus E_{K'}(T)\big) \\ &\quad CCC_1 = E_K\big(P_1 \oplus E_{K'}(T)\big) \\ &\quad CC_1 = E_K\big[E_K\big(P_1 \oplus E_{K'}(T)\big)\big] \\ &\quad C_1 = E_K\big[E_K\big(P_1 \oplus E_{K'}(T)\big)\big] \oplus E_{K'}(T) \\ &return \quad C_1 \end{aligned}$$

令 $y \in \{0,1\}^n$;t_0,$t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f: \{0,1\}^n &\to \{0,1\}^n \\ y &\mapsto C_1 \oplus C'_1, \\ &\quad C_1 \leftarrow \mathbf{CMC}^{t_0}_{K,K'}(y), C'_1 \leftarrow \mathbf{CMC}^{t_1}_{K,K'}(y) \\ f(y) &\mapsto E_K\big[E_K\big(y \oplus E_{K'}(t_0)\big)\big] \oplus E_{K'}(t_0) \oplus \\ &\quad E_K\big[E_K\big(y \oplus E_{K'}(t_1)\big)\big] \oplus E_{K'}(t_1) \end{aligned}$$

则有 $s = E_{K'}(t_0) \oplus E_{K'}(t_1) \Rightarrow f(y) = f(y \oplus s)$。可以确定 $s = E_{K'}(t_0) \oplus E_{K'}(t_1)$为函数 $f(y)$周期。

文献[19]对 CMC 的攻击所得的周期(其中$T' = E_{K'}(T)$):

$$E_K\big(E_K\big(m \oplus T'\big) \oplus \alpha_0\big) \oplus E_K\big(E_K\big(m \oplus T'\big) \oplus \alpha_1\big)$$

包含密钥 K,K'的多重加密, 较为复杂。我们用第二种攻击方式得到的周期$E_{K'}(t_0) \oplus E_{K'}(t_1)$更加简单, 只涉及一重加密且只包含一个密钥$K'$。对于密钥 K 的分析可以讲两种攻击方式结合得到进一步结果。

3.6 对 TET 的攻击

TET 是 2007 年 Halevi [9]提出的方案, 在文献[19]中 Ghosh 和 Sarkar 使用固定调柄, 对 3 个输入分组 $(x||x^{'}||x)$的 TET 加密方案进行了攻击, 找到周期为 $\alpha^2\beta \oplus \beta||\frac{(\alpha^2\beta\oplus\beta)(\tau\oplus\tau^3)}{\tau^2}||\alpha^2\beta \oplus \beta$, 表明 TET 在量子环境中选择明文攻击不安全。在这里我们以 1 个输入分组为例, 给出另一种攻击, TET 加密算法如下。其中输入为P_1, 输出为C_1, P_1,$C_1 \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$。

$$\mathbf{TET}\ {}_K^T(P_1):$$

$$PPP_1 = P_1 \oplus \frac{P_1\tau}{\sigma} \oplus \beta, \sigma = 1 \oplus \tau$$

$$CC_1 = E_{K_2}\left(\frac{P_1}{1 \oplus \tau} \oplus \beta\right) \oplus \beta,$$

$$\beta = PRF_{K_1}(L,T)$$

$$C_1 = \frac{CC_1}{1 \oplus \tau} = \frac{1}{1 \oplus \tau}\left(E_{K_2}\left(\frac{P_1}{1 \oplus \tau} \oplus \beta\right) \oplus \beta\right)$$

$$return \quad C_1$$

令 $y \in \{0,1\}^n$;t_0,$t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f:\{0,1\}^n &\to \{0,1\}^n \\ y &\mapsto C_1 \oplus C'_1, \\ & C_1 \leftarrow \mathbf{TET}_K^{t_0}(y), C'_1 \leftarrow \mathbf{TET}_K^{t_1}(y) \\ f(y) &\mapsto \frac{1}{1 \oplus \tau}(E_{K_2}\left(\frac{y}{1 \oplus \tau} \oplus \beta\right) \oplus \beta \\ & \oplus E_{K_2}\left(\frac{y}{1 \oplus \tau} \oplus \beta^{'}\right) \oplus \beta^{'}) \end{aligned}$$

其中, $\beta = PRF_{K_1}(L,t_0)$;$\beta^{'} = PRF_{K_1}(L,t_1)$。则有 $s = \frac{\beta\oplus\beta^{'}}{1\oplus\tau} \Rightarrow f(y) = f(y \oplus s)$。可以确定 $s = \frac{\beta\oplus\beta^{'}}{1\oplus\tau}$为函数$f(y)$周期, TET 在量子环境中选择明文攻击不安全。

相对于 $\alpha^2\beta \oplus \beta||\frac{(\alpha^2\beta\oplus\beta)(\tau\oplus\tau^3)}{\tau^2}||\alpha^2\beta \oplus \beta$, 我们用第二种攻击方式得到的周期$\frac{\beta\oplus\beta^{'}}{1\oplus\tau}$更加简练, 涉及相关变量系数更低。当然也可根据攻击需求结合两种攻击方式所得周期进行进一步分析。

4 一般攻击方法总结

4.1 固定调柄和变化调柄攻击方法

对于利用 Simon 算法对可调加密方案的攻击, 一般来说有两种形式:

(1) 固定调柄 T, 输入多个分组数据, 且变量 x 以及α_b(如果有的话)作为输入项, 得到的周期多为与α_b有关的多项式(例如 3.1, 3.2)或为与可调加密方案内部某些固定值有关的多项式(例如文献[19]中对 EME 的攻击、文献[19]对 TET 的攻击以及本文的 3.3), 这种攻击形式也主要应用于非可调的加密方案中;

(2) 变化调柄, 这种攻击多用在一个输入分组情况, 得到的周期多为与α_b有关的多项式(例如 3.4, 3.5, 3.6)。

对于这两种形式的攻击, 得到的周期本质上差别不大, 但第二种攻击相对来说得到的周期更加简单, 可以将两种攻击方式相结合或根据需求选择进行进一步分析。

4.2 对基于泛哈希函数可调加密方案的攻击

在可调加密方案的构造中, 有两类用到了泛哈希函数: Hash-CTR-Hash 和 Hash-ECB-Hash。泛哈希函数是具有一定组合性质的函数, 和伪随机函数等密码学强度的部件相比, 效率上有一定的优势。但是泛哈希函数是可调加密方案的薄弱环节, 只要得到泛哈希函数的方程, 一般就能将其密钥恢复出来, 进而给出对可调加密方案的有效攻击。

Hash-CTR-Hash 类型主要有 XCB、HCTR 和 HCH 等方案。文献[19]中对 XCB 模式进行了量子攻击, 本文对于 HCTR 和 HCH 模式进行了量子攻击, 表明 XCB、HCTR 和 HCH 模式在量子环境中选择明文攻击不安全。

Hash-ECB-Hash 类型主要有 PEP、TET 和 HEH 等方案。文献[19]中对 TET 模式进行了量子攻击, 本文对于 PEP、HEH 模式进行了量子攻击, 表明 TET、PEP 和 HEH 模式在量子环境中选择明文攻击不安全。

对于 1 个输入分组的情况, Hash-CTR-Hash 类型和 Hash-ECB-Hash 类型的可调加密方案都可以简化为图 1 的形式, 其中h_1和h_2是两个泛哈希函数。

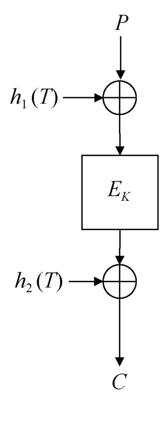

图 1 简化形式

Figure 1 Simplified form

对于这种简化形式, 令输入为项 P, 输出项为 C,

调柄 T, $P,C \in \{0,1\}^n$, $K \in \{0,1\}^k$, $T \in \{0,1\}^n$。令 $x \in \{0,1\}^n$;$t_0,t_1 \in \{0,1\}^n$且$t_0 \neq t_1$。定义以下函数:

$$\begin{aligned} f:\{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto C(t_0) \oplus C(t_1) \\ f(x) &= E_K(x \oplus h_1(t_0)) \oplus h_2(t_0) \oplus \\ &\quad E_K(x \oplus h_1(t_1)) \oplus h_2(t_1) \end{aligned}$$

可以看出, 当 $s = h_1(t_0) \oplus h_1(t_1)$时有 $f(x) = f(x \oplus s)$, 即$s = h_1(t_0) \oplus h_1(t_1)$为函数$f(x)$的周期, 可以利用 Simon 算法求出 s 的值。然后, 我们可以利用 s 给出区分攻击, 甚至可以恢复出h_1的密钥。之前我们对 HCTR、PEP、TET 和 HEH 的变换调柄攻击, 都用到了这种一般的攻击方法。

5 结论

本文主要利用量子 Simon 算法对 HCTR、HCH、PEP 和 HEH 四种可调加密方案进行了区分攻击, 表明上述四种可调加密方案在量子环境下选择明文攻击不安全。同时本文总结了固定调柄和变化调柄两种量子攻击方式, 并对 CMC、TET 等利用变化调柄的方式重新进行了攻击, 可以看出两种攻击方式得到的周期以及涉及到的变量不尽相同, 因此可以结合两种攻击形式一起分析或根据攻击需要选择。例如, 我们没有找到在固定调柄下对PEP的攻击, 但在变化调柄的情况下可以找到其周期 $s = EN \oplus EN'$。而变化调柄的攻击方式虽然多数情况下得到的周期简单, 但并不是所有可调加密方案都适用。例如无法用这种方法攻击 EME, 而使用固定调柄可简单有效的得到其周期 $6L, L = 2E_K(0^n)$[19]。最后我们给出了利用 Simon 算法攻击 Hash-CTR-Hash 和 Hash-ECB-Hash 两类可调加密方案的统一方法。

当前结果表明, 现有可调加密方案在量子环境下不安全。而如何根据区分攻击给出密钥恢复攻击以及如何构造抗量子攻击的可调加密方案值得我们进一步研究。

参考文献

[1] Liskov M, Rivest R L, Wagner D. Tweakable Block Ciphers[J]. *Journal of Cryptology*, 2011, 24(3): 588-613.

[2] Halevi S, Rogaway P. A Tweakable Enciphering Mode[M]. Advances in Cryptology - CRYPTO 2003. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 482-499.

[3] Halevi S, Rogaway P. A Tweakable Enciphering Mode[M]. Advances in Cryptology - CRYPTO 2003. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 482-499.

[4] Halevi S. EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data[M]. Progress in Cryptology - INDOCRYPT 2004. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 315-327.

[5] The Extended Codebook (XCB) Mode of Operation. Mcgrew D, Fluhrer S R. https://eprint.iacr.org/2004/278. Oct. 2004.

[6] Wang P, Feng D G, Wu W L. HCTR: A Variable-Input-Length Enciphering Mode[C]. *The First SKLOIS conference on Information Security and Cryptology*, 2005: 175-188.

[7] Chakraborty D, Sarkar P. HCH: A New Tweakable Enciphering Scheme Using the Hash-Counter-Hash Approach[J]. *IEEE Transactions on Information Theory*, 2008, 54(4): 1683-1699.

[8] Chakraborty D, Sarkar P. A New Mode of Encryption Providing a Tweakable Strong Pseudo-Random Permutation[C]. *The 13th international conference on Fast Software Encryption*, 2006: 293-309.

[9] Halevi S. Invertible Universal Hashing and the TET Encryption Mode[C]. *The 27th annual international cryptology conference on Advances in cryptology*, 2007: 412-429.

[10] Sarkar P. Improving Upon the TET Mode of Operation[C]. *The 10th international conference on Information security and cryptology*, 2007: 180-192.

[11] Shor P W, Processing C A. Algorithms for quantum computation: Discrete logarithms and factoring[C]. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 2002: 124-134.

[12] Grover L K. A Fast Quantum Mechanical Algorithm for Database Search[C]. *The twenty-eighth annual ACM symposium on Theory of Computing*, 1996: 212-219.

[13] Simon D R, Processing C A. On the power of quantum computation[C]. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 2002: 116-123.

[14] Kuwakado H, Morii M, Processing C A, et al. Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C]. *2010 IEEE International Symposium on Information Theory*, 2010: 2682-2685.

[15] Kuwakado H, Morii M, Processing C A. Security on the quantum-type Even-Mansour cipher[C]. *2012 International Symposium on Information Theory and its Applications*, 2013: 312-316.

[16] Kaplan M, Leurent G, Leverrier A, et al. Breaking Symmetric Cryptosystems Using Quantum Period Finding[M]. Advances in Cryptology - CRYPTO 2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016: 207-237.

[17] Leander G, May A. Grover Meets Simon - Quantumly Attacking the FX-Construction[M]. Advances in Cryptology - ASIACRYPT 2017. Cham: Springer International Publishing, 2017: 161-178.

[18] Luo Y Y, Yan H L, Wang L, et al. Study on Block Cipher Structures Against Simon's Quantum Algorithm[J]. *Journal of Cryptologic Research*, 2019, 6(5): 561-573.
(罗宜元, 闫海伦, 王磊, 等. 分组密码结构抗 Simon 量子算法攻击研究[J]. *密码学报*, 2019, 6(5): 561-573.)

[19] Breaking Tweakable Enciphering Schemes using Simon's Algorithm. Ghosh S, Sarkar P. https://eprint.iacr.org/2019/724. Jun. 2019.

[20] Chakraborty D, Nandi M. An Improved Security Bound for HCTR[M]. Fast Software Encryption. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 289-302.

毛淑平 于 2019 年在中国矿业大学(北京)信息与计算科学专业获得学士学位。现在中国科学院信息工程研究所网络空间安全专业攻读博士学位。研究领域为对称密码方案的设计与分析。Email: maoshuping@ iie.ac.cn

王鹏 于 2006 年在中国科院大学通信与系统专业获得博士学位。现在中国科学院信息工程研究所, 副研究员。研究领域为对称密码方案的设计与分析。Email: wpeng@iie.ac.cn

胡磊 于 1994 年在中国科学院系统科学研究所应用数学专业获得博士学位。现在中国科学院信息工程研究所, 研究员。研究领域为对称密码设计与分析、公钥密码设计与分析。Email: hulei@iie.ac.cn