计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS

基于 D-Wave Advantage 的量子计算实用化 SPN 结构对称密码攻击研究

裴植　洪春雷　王启迪　胡巧云　王潮

(上海大学 特种光纤与光接入网重点实验室 上海 200444)

摘　要　截至 2023 年，谷歌的量子霸权芯片 Sycamore 尚不能用于密码攻击. 量子计算在理论上对公钥密码有致命性威胁，但对对称密码影响甚微，目前业内已经从缩减版密码算法开始积极探索对称密码的量子攻击. SPN 结构是对称密码算法中的一种代表性结构，目前基于真实量子计算机的各类量子算法均未能对该结构未经缩减的全规模密码算法进行攻击. 基于量子退火算法独有的隧穿效应，使得该算法有利于科学问题的指数级解空间搜索，可将其视为一类具有全局寻优能力的人工智能算法. 受传统密码分析方法的影响，本文提出一种对称密码攻击架构：量子退火耦合传统数学方法密码攻击的新型计算架构—QuCMC. 基于该架构，首先利用可分性刻画 SPN 结构对称密码算法的线性层和非线性层传播规律，将区分器搜索问题转化为 MILP 模型求解问题. 进一步将 MILP 模型转化为 D-Wave CQM 模型，在求解该模型的过程利用量子波动产生的量子隧穿效应跳出传统智能算法极易陷入的局部亚优解，获得更优的解，即攻击目标对称密码算法的积分区分器. 本文使用 D-Wave Advantage 量子计算机攻击了 PRESENT、GIFT-64、RECTANGLE 三种 SPN 结构代表算法，均成功搜索到最长 9 轮的积分区分器. 并且实验结果表明，量子退火算法在跳出局部亚优解能力与求解时间两个方面，均优于经典启发式全局寻优算法模拟退火. 本研究首次成功利用真实量子计算机对多种全规模 SPN 结构对称密码算法完成了攻击，攻击效果与传统数学方法持平.

关键词　对称密码；量子计算；量子退火；D-Wave 量子计算机；量子隧穿效应

中图法分类号　TP309

Research on Quantum Computing for Practical SPN Structure Symmetric Ciphers Attacks Using the D-Wave Advantage

PEI Zhi　HONG Chun-Lei　WANG Qi-Di　HU Qiao-Yun　WANG Chao

(Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444)

Abstract The emergence of quantum computers brings new challenges and opportunities for the security analysis of modern cryptography. The nascent interdisciplinary realm of quantum computing and symmetric ciphers holds immense potential, with numerous unexplored problems awaiting comprehensive investigation. As of 2023, Google's quantum supremacy chip Sycamore is still not capable of performing cryptanalysis. Quantum computing is widely regarded as a significant threat to the security of public key cryptography, but it has little impact on symmetric ciphers. The prospect of quantum computing attacks on symmetric ciphers presents both an exhilarating and formidable challenge. Currently, the industry is starting to actively explore quantum computing attacks on symmetric ciphers, initially focusing on reduced-version algorithms. Substitution-Permutation Network (SPN) structure is a representative structure of symmetric cipher algorithms, and currently, various quantum algorithms have not been able to attack full-scale SPN structure symmetric cipher algorithms. The quantum annealing algorithm proposed in 1994 aims to solve the problem of finding the minimum value of a multivariate function. The quantum annealing algorithm can empower various fields with diverse applications,

本课题得到密码科学技术全国重点实验室开放课题基金资助. **裴植**，博士研究生，主要研究领域为网络空间安全、量子计算密码. **洪春雷**，博士研究生，主要研究领域为网络空间安全、量子计算密码. **王启迪**，硕士，主要研究领域为网络空间安全、量子计算密码. **胡巧云**，硕士，主要研究领域为网络空间安全、量子计算密码. **王潮**（**通信作者**），博士，教授，中国计算机学会(CCF)高级会员，中国人工智能学会理事，中国电子学会理事，主要研究领域为人工智能、网络空间安全、量子计算密码.

including but not limited to financial services, manufacturing logistics, deep neural networks, cryptanalysis and design, machine learning, and city brain. Thanks to the unique tunneling effect of quantum annealing algorithm, this algorithm is advantageous for exponential search space exploration of scientific problems. It can be regarded as a class of artificial intelligence algorithms with global optimization capabilities. Inspired by traditional cryptanalysis methods, we proposed a novel computational architecture for symmetric cryptanalysis: Quantum Annealing-Classical Mixed Cryptanalysis (QuCMC), which combines the quantum annealing algorithm with traditional mathematical methods. Utilizing this architecture, we initially applied the division property to describe the propagation rules of the linear and nonlinear layers in SPN structure symmetric cipher algorithms. Subsequently, the SPN structure distinguisher search problems were transformed into Mixed Integer Linear Programming (MILP) problems. These MILP models were further converted into D-Wave Constrained Quadratic Models (CQM), leveraging the quantum tunneling effect induced by quantum fluctuations to escape local minima solutions and achieve an optimal solution corresponding to the integral distinguisher for the cipher algorithms being attacked. Experiments conducted using the D-Wave Advantage quantum computer have successfully executed attacks on three representative SPN structure algorithms: PRESENT, GIFT-64, and RECTANGLE, and successfully searched integral distinguishers up to 9-round. Experimental results demonstrate that the quantum annealing algorithm surpasses traditional heuristic-based global optimization algorithms, such as simulated annealing, in its ability to escape local minima and in solution time. This marks the first practical attack on multiple full-scale SPN structure symmetric cipher algorithms using a real quantum computer. Additionally, this is the first instance where quantum computing attacks on multiple SPN structure symmetric cipher algorithms have achieved the performance of the traditional mathematical methods. Future work might consider extending the methodologies discussed here to other SPN structure symmetric cipher algorithms. As quantum computing technology further develops, this field is expected to achieve more breakthroughs. Through this exploration, it is expected to establish a computing architecture that combines artificial intelligence algorithms with quantum effects and mathematical methods in the future.

Key words: Symmetric cipher; Quantum computing; Quantum annealing; D-Wave quantum computer; Quantum tunneling effect

1 引言

目前，各类新型密码攻击方法正逐渐成为研究和关注的焦点[1]. 同时，多种量子计算技术百花齐放，发展迅速[2, 3]，为众多领域带来了新的发展契机. 量子计算的兴起也为现代密码学安全性分析带来了前所未有的挑战和机遇，各类成果不断涌现[4]. 量子计算和对称密码构成的交叉学科是一个新兴领域，存在许多尚待探索的问题. 置换代换网络(Substitution-Permutation Network, SPN)结构是对称密码结构中一种重要的迭代网络结构，比 Feistel 结构扩散速度更快[5]，其安全性分析一直是业界长期关注的研究.

在对称密码的量子攻击方面，Shor 算法[6]等量子算法对公钥密码具有致命性威胁，这是目前抗量子密码标准制定的一个主要原因，但 Shor 算法无法用于对称密码的攻击. 针对 Grover 算法[7]的对称密码攻击，仅需将密钥长度加倍，便可在量子环境下获得相同的安全强度[8]，对对称密码的安全性不构成颠覆性威胁. 另一类基于 Simon 算法[9]或组合算法展开的对称密码分析大都针对较简单的 Feistel 结构及其变体[10]. 上述研究都在理论描述的量子框架下进行对称密码的安全性评估，还停留在概念阶段.

基于嘈杂中型量子(Noisy Intermediate-Scale Quantum, NISQ)[11]设备对缩减版的对称密码算法实施量子攻击也是当前的一个研究热点. 清华大学团队[12]对缩减版的 S-DES(8 比特明文，10 比特密钥，8 比特密文)进行攻击探索，设计了 S-DES 的代价函数，根据已知明密文对，利用变分量子算法得到了密钥. 文[13]在文[12]的基础上减少了攻击 S-DES 所需的量子比特. L. Phab, S[14]等人使用 NISQ 设备运行量子近似优化算法(Quantum Approximate Optimization Algorithm, QAOA)[15]完成 HeysCipher 算法的两轮密钥恢复，但由于量子电路深度的限制，作者指出文中的攻击方法不确定是否能扩展至更大规模的实例上. 另外，变分量子算法的发展还需要克服贫瘠高原挑战[16].

量子比特之间状态信息的传递会受到纠错码

等技术限制，如何在真实的量子计算机设备上进行对称密码的量子攻击一直是悬而未决的难题. 2019 年推出的谷歌量子霸权芯片 Sycamore 尚不能用于密码破译[17]，2023 年谷歌提升了 Sycamore 芯片的容错率，但仍不能用于实际密码的破译[18]，最新的量子霸权里程碑[19]针对特殊问题验证了其计算能力，但是否可以用于密码攻击和分析有待考量. 由于可扩展量子比特数有限、相干时间较长等技术限制，《Nature》和《Science》[20, 21]均刊文表示通用量子计算机需要发展基础理论. 综上，将量子计算用于破译对称密码，需要寻找适合的量子算法，探索能在真实量子计算机上执行的新型技术路线.

D-Wave 量子计算机发展迅速，目前已有 5000 个以上的量子比特. 第六代量子系统 Advantage2，将在 2023-2024 年扩展至 7000 个量子比特. D-Wave 的原理量子退火算法[22]具有量子加速效应[23]，并且收敛性理论完备[24]，算法在大规模优化问题求解方面具有优势[25]. 运用其独有的量子隧穿效应，量子退火算法的寻优过程可以跳出传统智能算法极易陷入的局部极值，擅长求解组合优化问题. 当科学问题缺乏传统数学多项式求解算法，并且存在指数级解空间搜索的情况时，可以利用量子退火快速逼近全局最优解[26].

基于量子退火算法独特的隧穿效应、求解组合优化问题时的优势、器件发展情况，2012 年我们[27]原创提出 D-Wave 量子计算机或可用于密码分析和密码设计. 受启发于演化密码的思想，我们认为可以使用人工智能算法来进行解空间的搜索[28]，并且提出量子人工智能密码这一量子计算环境下的密码理论研究及 D-Wave 密码分析和设计的新型技术路线：将密码算法的攻击或设计问题转化为组合优化问题，利用 D-Wave 量子退火的量子隧穿效应跳出局部极值，基于量子退火的指数级解空间搜索优势全局寻优，实现密码分析和设计. 2019 年和 2020 年的前期研究[29, 30]均验证了此技术路线的可行性，实验结果达到当年各类量子计算攻击 RSA 的最高实验指标.

2019 年起结合量子退火算法和密码攻击数学方法，形成一类量子攻击密码的新型技术路线，以期利用此技术路线攻击公钥密码和对称密码. 目前，基于此技术路线我们已经完成了 50 比特 RSA 攻击实验，实验结果是各类量子算法分解 RSA 整数的最高实验指标[31]，验证了技术路线的可行性. 因此，本文沿用此技术路线进一步探索对称密码的攻击，旨在与密码攻击数学方法持平.

根据 D-Wave 量子计算机的增长态势、量子退火算法的理论优势以及量子退火算法对公钥密码算法的实际攻击效果，本研究选用 D-Wave 量子退火作为 SPN 结构全规模对称密码量子计算攻击的探索量子算法. 本文提出一种通用的量子退火耦合传统数学方法密码攻击新型计算架构，将其命名为：QuCMC(Quantum Annealing-Classical Mixed Cryptanalysis). 具体思路是利用量子退火算法的优势求解数学难题，使用量子特性实现对现有密码分析方法的扩展. 本文选择三种 SPN 结构代表算法：PRESENT[32]、GIFT-64[33]、RECTANGLE[34]作为 QuCMC 计算架构的验证算法. 将密码算法中的线性层及非线性层密码性质的传播转化为组合优化问题，嵌入至 D-Wave Advantage 真实量子计算机中求解. 利用量子退火算法均寻优搜索到了这三种算法最长 9 轮的积分区分器. 这是首次使用量子算法在多种对称算法的攻击都达到与传统数学方法轮数持平的效果，计算架构具有普适性，提高了目前密码分析方法的多样性.

本文的实验结果表明，量子退火算法在区分器搜索问题的求解上展现出了优于模拟退火算法的效果. 通过此次探索，未来有望建立具有量子效应的人工智能算法与数学方法融合的计算架构.

2 量子退火算法

1994 年提出的量子退火算法[22]旨在解决多元函数最小值问题，在寻找全局最优解的过程中可以通过量子隧穿效应跳出局部亚优解，有望在多项式时间内求解 NP-Hard 问题[35]. D-Wave 各代量子系统均通过量子退火算法来寻找问题的解决方案. 基于 D-Wave 量子计算机强大机器背景，量子退火算法发展十分迅速，各代 D-Wave 量子计算机量子比特数量发展见表 1，基本呈隔年倍增的发展态势.

表 1　各代 D-Wave 量子计算机量子比特数量

	D-Wave One	D-Wave Two	D-Wave 2X	D-Wave 2000Q	Advantage	Advantage 2
发行时间	2011	2013	2015	2017	2020	2023-2024
量子比特数	128	215	1152	2048	5760	7000+

基于其硬件稳定的发展态势，量子退火算法可以以多样的应用赋能给各个领域，包括但不局限于：金融服务[36]、制造物流[37]、深度神经网络[38]、密码分析与设计[39, 40]、机器学习[41]、以及城市大脑[42]等领域.

量子退火的初始状态为包含整个搜索空间所有状态的叠加态，在该叠加态中每个状态的权重相同. 整个系统状态随系统的时变薛定谔方程演化：

$$i\frac{\partial\left|\psi(t)\right\rangle}{\partial t}=H(t)\left|\psi(t)\right\rangle, \tag{1}$$

其中 t 为演化时间，$H(t)$ 为时变哈密顿量，$\left|\psi(t)\right\rangle$ 为状态向量，表示系统在该时刻的状态.

随着演化过程的进行，系统利用量子隧穿效应跳出局部亚优解，各状态的概率发生变化，此过程

通过控制时变哈密顿量 $H(t)$ 实现，量子退火的时变哈密顿量可表示为式(2)：

$$H(t)=\Gamma(t)H_{init}+\Lambda(t)H_{final}, \tag{2}$$

其中 $H_{init}=\sum_i \Delta_i \sigma_i^x$ 是系统初始哈密顿量，也称为横向场，Δ_i 参数化 $|\uparrow\rangle$ 和 $|\downarrow\rangle$ 之间的量子隧穿效应. 终态哈密顿量可表示为：

$$H_{final}=\sum_i h_i(t)\sigma_i^z+\sum_{i,j} J_{ij}(t)\sigma_i^z\sigma_j^z, \tag{3}$$

其基态由优化问题的最优解编码决定，其中 h_i 代表第 i 个量子比特的权重，称为局部场系数. $J_{i,j}$ 表示第 i 和第 j 个量子比特的耦合强度，称为耦合项系数.

$$\sigma_i^z=I\otimes I\otimes\cdots\otimes\sigma^z\otimes\cdots\otimes I, \tag{4}$$

I 为二维单位矩. “⊗”为张量积，σ^z 和 σ^x 为泡利矩阵：

$$\sigma^z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\quad \sigma^x=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}. \tag{5}$$

Γ，Λ 是随时间演化而变化的非线性组合系数. 如图 1 所示，系统从初态演化到终态时，Γ 从 1 降低至 0，而 Λ 由初值 0 逐渐增加到 1.

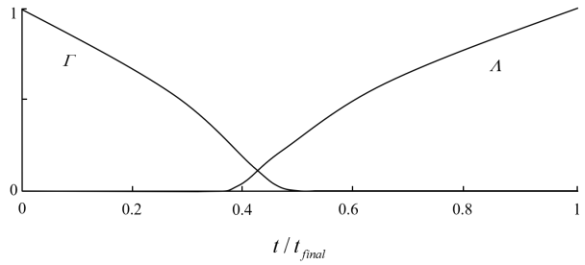

图 1 时变哈密顿量的系数变化[43]

t/t_{final} 表示量子退火的演化进度.

在使用量子退火解决优化问题时，要将优化问题的最优解和系统终态哈密顿量的基态匹配，演化完成后测量系统信息即可得到优化问题的解.

传统人工智能算法的运行时间长短很大程度上取决于组合优化问题的规模，而量子退火算法可以以高度并行的方式进行计算，在大规模实际问题解决方面具有很强的扩展性.

3 准备工作

本文使用量子退火算法基于真实量子计算机 D-Wave Advantage，刻画一类 SPN 对称密码算法的线性层及非线性层的可分性[44]传播路径，把传播路径转化为混合整数线性规划(Mixed-Integer Linear Programming, MILP)模型的约束条件，使用量子退火算法搜索寻优该数学问题，求解出满足所有约束的解，最终找到对应轮数的积分区分器. 本节将会对本研究使用的可分性、MILP 模型、MILP 模型约简算法相关的概念及符号进行介绍.

3.1 可分性

对称密码主流攻击方法包括：差分攻击、线性攻击、积分攻击以及最近兴起的量子攻击等[45]. 积分攻击于 2002 年首次提出[46]，已经成为评估分组密码安全性的基本方法之一. 积分攻击通常包括两个主要阶段：首先寻找积分区分器，随后利用这些区分器进行密钥恢复攻击. 积分区分器通过数据的平衡特性以不可忽略的概率区分算法 E 和随机置换 R. 具体来说，攻击者固定输入的部分比特，遍历剩余比特的可能取值，检查输出比特是否表现出积分特性中的平衡特性，即每个可能的取值发生的次数是否相同来区分算法和随机置换[47].

2015 年 Todo[48]在欧密会上提出了一种广义积分性质—可分性，该技术通过结合对称密码算法非线性组件的代数次数优化积分性质，从而更精确地搜索密码算法的积分特征. 本文使用不等式集合刻画 SPN 结构对称密码算法可分性传播规律，构建可分性传播的 MILP 模型，最终基于量子退火算法求得对应算法的积分区分器.

为方便理解，本节首先介绍文中使用的可分性相关的术语、记法、定义及概念. F_2 为只有两个元素的有限域，F_2^n 为 n 维二元域. $\forall \boldsymbol{u}\in F_2^n$，记 $\boldsymbol{u}$ 的第 i 个分量为 u_i，向量 $\boldsymbol{u}$ 的汉明重量可由式(6)计算得到：

$$wt(\boldsymbol{u})=\sum_{i=0}^{n-1} u_i. \tag{6}$$

比特乘积函数[48]：$\forall \boldsymbol{u},\boldsymbol{x}\in F_2^n$，比特乘积函数 $\pi_{\boldsymbol{u}}(\boldsymbol{x}):F_2^n\to F_2$ 定义如下：

$$\pi_{\boldsymbol{u}}(\boldsymbol{x})=\prod_{i=0}^{n-1} x_i^{u_i}. \tag{7}$$

偏序关系：对任意向量 $\boldsymbol{v},\boldsymbol{v}'\in F_2^n$，按如下定义两种偏序关系 $\preceq$ 和 $\succeq$：

$$\boldsymbol{v}\preceq\boldsymbol{v}' \Leftrightarrow v_i\le v_i', \tag{8}$$

$$\boldsymbol{v}\succeq\boldsymbol{v}' \Leftrightarrow v_i\ge v_i'. \tag{9}$$

代数正规型：对任意布尔函数 $f:F_2^n\to F_2$，其代数正规型可记为以下形式：

$$f(\boldsymbol{x})=f(x_0,\cdots,x_{n-1})=\bigoplus_{\boldsymbol{u}\in F_2^n} a_{\boldsymbol{u}}\prod_{i=0}^{n-1} x_i^{u_i}=\bigoplus_{\boldsymbol{u}\in F_2^n} a_{\boldsymbol{u}}\pi_{\boldsymbol{u}}(\boldsymbol{x}), \tag{10}$$

其中，$a_{\boldsymbol{u}}\in F_2$.

本文使用的可分性定义在比特之上，使用两子集合比特级别可分性来进行 SPN 结构算法积分区

分器搜索，下面介绍这种可分性：

定义 1：两子集比特级可分性[44]：令 X ,K 取值于多重集 F_2^n，$\boldsymbol{k}\in F_2^n$，若 X 满足式(11)：

$$\bigoplus_{x\in X}\pi_{\boldsymbol{u}}(x)=\begin{cases}unknown, & \text{若存在 } \boldsymbol{k}\in K \text{ 使得 } \boldsymbol{u}\succeq\boldsymbol{k}\\ 0, & \text{否则}\end{cases} \tag{11}$$

则称此多重集 X 具有二子集合比特级可分性 $D_{\mathrm{K}}^{1,n}$. 若无特别声明，下文中使用的可分性均为二子集合比特可分性.

假设多重集 X 中存在两个向量 $\boldsymbol{x}$ 与 $\boldsymbol{x}'$ 满足 $\boldsymbol{x}'\succeq\boldsymbol{x}$，则此时 $\boldsymbol{x}'$ 对描述可分性没有帮助，称 $\boldsymbol{x}'$ 为冗余向量. 为节约运算成本，可在后续运算中对其删除.

定义 2：可分迹[49]：设 f_r 为密码算法的轮函数，$K_0,\cdots,K_r$ 为目标算法明文、中间状态或密文的多重集. K_i 和 K_{i+1} 可以由 f_i 联通. 即对任意 $\boldsymbol{k}_i\in K_i$，在具有可分性的传播轨迹 $\{\boldsymbol{k}\}\overset{def}{=}K_0\xrightarrow{f_1}\cdots\xrightarrow{f_r}K_r$ 中，一定存在向量 $\boldsymbol{k}_{i-1}\in K_{i-1}$ 使得 $\boldsymbol{k}_{i-1}$ 能传播到 $\boldsymbol{k}_i$，则称 $(\boldsymbol{k}_0\to\cdots\to\boldsymbol{k}_r)$ 为一条 r 轮的可分迹.

3. 2 MILP模型

MILP 问题作为一类在一定约束下求解目标函数的最值优化问题，最早由 Mouha 等人引入密码分析中[50]，很多对称密码攻击问题都可以归约为 MILP 模型的求解问题. 因此，探索 MILP 量子求解的新方法十分重要. 本文将明密文的可分性传播规律转化为 MILP 模型求解问题，通过量子退火进行求解. MILP 模型可表述为以下的形式：

$$M:\begin{cases}M\ .obj\\ M\ .con\ 1\\ M\ .con\ 2\\ \quad\vdots\\ M\ .con\ n\\ M\ .var\end{cases}. \tag{12}$$

其中，$M\ .obj$ 为目标函数，$M\ .con\ i$（$1\le i\le n$）为约束条件，$M\ .var$ 为变量值域，可表示为最大化目标函数和最小化目标函数两种形式. 例如，式(13)为一个小规模的 MILP 模型：

$$M:\begin{cases}M\ .obj\leftarrow\min\{7x_1+5x_2+3x_3\}\\ M\ .con\ \leftarrow x_1+x_2\le 1\\ M\ .con\ \leftarrow 2x_1+2x_2+x_3\ge 3\\ M\ .var\leftarrow x_1,x_2,x_3\in\{0,1\}\end{cases}, \tag{13}$$

经计算该模型的解为 $x_1=0$，$x_2=1$，$x_3=1$.

MILP 模型在实际问题中应用广泛，本文将对称密码算法区分器搜索问题归约为寻找 MILP 问题的解，通过量子退火算法全局寻优，以期为后量子时代的密码攻击方法提供新的视角.

3. 3 MILP模型约简算法

本文使用一组不等式作为 MILP 模型的约束条件，刻画 SPN 结构密码算法各部件的可分性传播规律，并且将 MILP 模型转化为量子计算机能求解的形式. 由于量子计算机量子比特数量的限制，大规模的不等式组可能会导致后续模型过载，影响求解效率. 为了解决这一问题，引入约简算法显得尤为关键.

文献[49]使用的贪婪算法[51]广泛应用于不等式归约，但在不等式组的约简表达上有冗余. 因此，本文使用 Sasaki[52]提出的基于 MILP 模型约简算法，在不改变可行解的前提下，对 SPN 结构密码算法中非线性层 S 盒表达式进行优化，以实现理论上的全局最简式表达. 算法可被简单描述如下：

算法 1 MILP 模型约简算法

输入：离散点集 P；描述 P 的线性不等式集合 $L_{P'}$

输出：约简后的不等式集合 L_P

1. $P^c=F_2^n-P$
2. **FOR** p_j in P^c **DO**
3. **FOR** l_j in $L_{P'}$ **DO**
4. **IF** p_j 不满足不等式 l_j **THEN**
5. 标记 $s_{i,j}=1$
6. **ELSE**
7. 标记 $s_{i,j}=0$
8. **END IF**
9. **END FOR**
10. **END FOR**
11. 对 $L_{P'}$ 中的每一个不等式设置其标记变量 z_j
12. 构建 MILP 模型
13. $M\ .obj$： $\min\left\{\sum_j z_j\right\}$
14. $M\ .con$： $\sum_j s_{i,j}\times z_j\ge 1$
15. $M\ .var$： $z_j\in\{0,1\}$
16. 求解 MILP 模型
17. z_j 为 1 对应的所有不等式构成新的不等式集合 L_P

4 量子经典结合SPN结构密码攻击

4. 1 QuCMC计算架构

本文提出量子退火耦合传统数学方法对称密

码攻击计算架构(见图 2)，将其命名为 QuCMC，该架构具有极强的可扩展性. 总体思想是利用量子退火算法赋能传统数学方法，具体操作是将传统数学算法中一些难解的数学问题建模转化成为组合优化问题或者指数级解空间搜索问题，利用量子退火算法进行求解，此架构具有通用性可扩展至其它量子算法. 需要注意的是，在使用此架构进行对称密码真实量子计算机攻击探索时，量子算法选型需要注意以下三个要素：

1) 是否有真实的量子计算机支撑使算法和硬件做到耦合；

2) 算法是否存在收敛性的问题；

3) 算法是否有足够的理论优势.

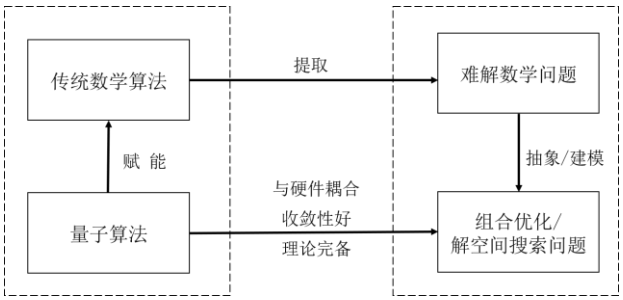

图 2 QuCMC

可分性技术较其它区分攻击方法可以更精确的刻画密码算法的积分性质[53]. 本节利用 QuCMC 架构，使用量子退火算法赋能传统数学方法；将量子退火算法与使用可分性的区分器搜索方法结合，形成量子退火与数学方法结合 SPN 结构对称密码算法的积分区分器搜索的通用型方法. 在密码攻击时发挥量子计算的加速效能，以突破现有量子计算对称密码攻击瓶颈. 本文选取对称密码算法中三种代表性算法：PRESENT、GIFT-64、RECTANGLE 进行探索研究，以验证量子退火算法攻击 SPN 结构对称密码的可行性和潜力.

4.2 量子退火SPN结构对称密码算法区分器搜索方法概述

在本节中，我们将介绍如何根据 SPN 结构密码算法的可分性传播规律构建模型，并利用 D-Wave 求解该模型. 基于 QuCMC 架构，本研究首先使用文献[49]中首次提出的方法计算对称密码算法中非线性层的可分迹. 通过不等式描述非线性层的可分迹，并结合初始可分性以及密码算法线性层的传播规律，构建了描述 SPN 结构密码算法可分性传播规律的 MILP 模型. 随后，将此 MILP 模型转化为 CQM 模型. 最终，我们应用量子退火算法对该 CQM 模型进行全局搜索. 具体步骤可参见算法 2：

算法 2 量子退火对称密码积分区分器搜索算法

输入: 对称密码算法 S 盒输入可分特性 $D_k^{1,n}$，轮数 r，初始可分性

输出: 对称密码算法的积分区分器

1. $\overline{\mathrm{S}}=\{\overline{\boldsymbol{k}}\,|\,\overline{\boldsymbol{k}}\succeq\boldsymbol{k}\}$
2. $F(X)=\{\pi_{\overline{k}}(\boldsymbol{x})\,|\,\overline{\boldsymbol{k}}\in\overline{\mathrm{S}}\}$
3. $\overline{\mathrm{K}}\leftarrow\varnothing$
4. **FOR** $\boldsymbol{u}$ in F_2^n **DO**
5. **IF** $\pi_u(\boldsymbol{y})$ 包含 $F(X)$ 中任意单项式 **THEN**
6. $\overline{\mathrm{K}}\leftarrow\overline{\mathrm{K}}\cup\{\boldsymbol{u}\}$
7. **End IF**
8. **END FOR**
9. $\mathrm{K}=\boldsymbol{SizeReduce}(\overline{\mathrm{K}})$
10. 将 $D_k^{1,n}$ 和 $D_{\mathrm{K}}^{1,n}$ 视为一个点集 P
11. 使用 SageMath:inequality_generator( ) 得到点集 P 的不等式集合 $L_{P'}$
12. 使用算法 1 对上一步得到的不等式进一步约简得到新的不等式集合 L_P
13. 提取 L_P 的系数得到系数矩阵 S_T
14. **FOR** i in r **DO**
15. S_T 作为第 i 轮不等式变量的系数，构建第 i 轮可分性传递的不等式组
16. **END FOR**
17. 构建 MILP 模型
18. 根据 MILP 模型构建 D-Wave CQM 模型
19. 目标函数：第 r 轮输出变量汉明重量的最小值
20. 约束条件：r 轮攻击目标算法可分性传播不等式组、
    初始可分性等式表示
21. 使用量子退火搜索第 r 轮 CQM 模型的解
22. **IF 不满足终止条件 THEN**
23. **RETURN** “第 r 轮存在积分区分器”，输出区分器
24. **ELSE**
25. **RETURN** “第 r 轮不存在积分区分器”

注释 1. ***SizeReduce***（）函数是去除冗余向量的操作；

注释 2. 算法搜索的终止条件为第 r 轮的所有输出为均为不确定比特，即第 r 轮的输出多重集第一次包含 n 个单位向量，并且第 r-1 轮不包含全部的 n 个单位向量，n 为 SPN 结构密码算法的分组长度；

注释 3. 对于初始可分性，当选取的比特为活跃的则取该比特值为 1，否则取 0.

接下来以 PRESENT 算法为例，详细描述利用量子退火算法搜索 SPN 结构对称密码算法积分区分器的具体步骤，GIFT-64 与 RECTANGLE 算法的区分器可类似搜索.

1) 根据 S 盒的输入和输出计算其代数正规型；

PRESENT 算法的非线性层由 16 个相同的代数次数为 3 的 S 盒构成，可通过其输入和输出构建代数正规型. 假定 S 盒输入为 $\boldsymbol{x}=(x_3,x_2,x_1,x_0)$，对应的输出为 $\boldsymbol{y}=(y_3,y_2,y_1,y_0)$. 经计算我们得到与文献[49]相同的 PRESENT 算法 S 盒的代数正规型：

$$\begin{cases} y_3 = 1 \oplus x_0 \oplus x_1 \oplus x_3 \oplus x_1x_2 \oplus x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \\ y_2 = 1 \oplus x_2 \oplus x_3 \oplus x_0x_1 \oplus x_0x_3 \oplus x_1x_3 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \\ y_1 = x_1 \oplus x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_2x_3 \\ y_0 = x_0 \oplus x_2 \oplus x_3 \oplus x_1x_2 \end{cases} \tag{14}$$

2) 根据可分性传播规则求得 S 盒的可分迹；

以输入可分性为$D^{1,4}_{(1,0,0,1)}$为例，应用式(14)，遍历 2^4 种输出可分性的组合，如

$$\oplus \boldsymbol{\pi}_{(0,0,0,1)}\left((y_3,y_2,y_2,y_1)\right) = y_0, \tag{15}$$

即

$$\begin{aligned} &\bigoplus_{x\in X} \boldsymbol{\pi}_{(0,0,0,1)}\left((y_3,y_2,y_2,y_1)\right) \\ &= \bigoplus_{x\in X} y_0 \\ &= \bigoplus_{x\in X} \left(x_0 \oplus x_2 \oplus x_3 \oplus x_1x_2\right) \\ &= \bigoplus_{x\in X} \boldsymbol{\pi}_{(0,0,0,1)}(\boldsymbol{x}) \bigoplus_{x\in X} \boldsymbol{\pi}_{(0,1,0,0)}(\boldsymbol{x}) \bigoplus_{x\in X} \boldsymbol{\pi}_{(1,0,0,0)}(\boldsymbol{x}) \bigoplus_{x\in X} \boldsymbol{\pi}_{(0,1,1,0)}(\boldsymbol{x}) \\ &= 0 \end{aligned} \tag{16}$$

如上所示，可以得到 $\boldsymbol{y}$ 的最低输出位 y_0 为平衡的，类似可以得到其它输出位的情况. 经计算可得到输出多重集Y 的可分性为$D^{1,4}_{(0,0,1,0)\ (0,1,0,0)\ (1,0,0,0)}$，从而得到 S 盒的 3 条可分迹：

$$(1,0,0,1) \xrightarrow{sbox} (0,0,1,0),\ (1,0,0,1) \xrightarrow{sbox} (0,1,0,0),$$

$$(1,0,0,1) \xrightarrow{sbox} (1,0,0,0).$$

根据上述计算过程，通过 ***SizeReduce***（）操作删除冗余向量，采用文献[49]的方法经计算得到得到该文献中 PRESENT 算法 S 盒的 47 条可分迹(见表 2).

表 2　PRESENT 算法 S 盒的可分迹[49]

输入$D^{1,4}_{\boldsymbol{k}}$	输出$D^{1,4}_{K}$
(0,0,0,0)	(0,0,0,0)
(0,0,0,1)	(0,0,0,1) (0,0,1,0) (0,1,0,0) (1,0,0,0)
(0,0,1,0)	(0,0,0,1) (0,0,1,0) (0,1,0,0) (1,0,0,0)
(0,0,1,1)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(0,1,0,0)	(0,0,0,1) (0,0,1,0) (0,1,0,0) (1,0,0,0)
(0,1,0,1)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(0,1,1,0)	(0,0,0,1) (0,0,1,0) (1,0,0,0)
(0,1,1,1)	(0,0,1,0) (1,0,0,0)
(1,0,0,0)	(0,0,0,1) (0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,0,0,1)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,0,1,0)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,0,1,1)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,1,0,0)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,1,0,1)	(0,0,1,0) (0,1,0,0) (1,0,0,0)
(1,1,1,0)	(0,1,0,1) (1,0,1,1) (1,1,1,0)
(1,1,1,1)	(1,1,1,1)

3) 使用不等式刻画 S 盒的可分迹，并对这些不等式进行约简，以提高后续嵌入量子计算机搜索求解时的效率.

S 盒变换为非线性变换，要根据其输入和输出构建模型，PRESENT 算法输入输出均为 4 比特，我们把每条可分迹视为一个 8 维的点，所有可分迹构成 8 维空间上的点集 P. 使用求解软件 SageMath 可以得到点集 P 的不等式集合，此集合由 122 个不等式构成，规模较大. 由于量子计算机量子比特的限制，大规模的不等式约束条件会导致后续 CQM 模型过载而无法求解，因此约简算法十分必要. 这里我们利用算法 1 进行约简，在不改变不等式组可行域的前提下，降低计算复杂度. 化简后 PRESENT 算法 S 盒的可分性传播路径的不等式表示见式(17)：

$$\begin{cases} x_1 - x_2 - x_3 + 0x_4 + 0y_1 - y_2 + 0y_3 + 0y_4 \geq -2 \\ -2x_1 - x_2 - x_3 - 2x_4 + 5y_1 + 5y_2 + 5y_3 + 2y_4 \geq 0 \\ -5x_1 - 5x_2 - 5x_3 - 2x_4 + y_1 + 2y_2 + y_3 + 2y_4 \geq -11 \\ x_1 + x_2 + x_3 + 2x_4 - 2y_1 - 2y_2 + 0y_3 - 2y_4 \geq -1 \\ 0x_1 + 3x_2 + 0x_3 + 0x_4 - y_1 - y_2 - y_3 - y_4 \geq -1 \\ x_1 + x_2 + x_3 + x_4 + y_1 - 2y_2 - 2y_3 - 2y_4 \geq -1 \\ 3x_1 + 0x_2 + 0x_3 + 0x_4 - y_1 - y_2 - y_3 - y_4 \geq -1 \\ 0x_1 + 0x_2 + 3x_3 + 0x_4 - y_1 - y_2 - y_3 - y_4 \geq -1 \end{cases} \tag{17}$$

由于比特置换仅改变变量的位置，不改变可分性，为减少约束规模，我们在第二轮迭代时根据算法比特置换规律改变对应变量的标号，实现比特置换操作. 联立 r 轮各不等式，将该不等式组以及初始可分性等式表示作为 PRESENT 算法 MILP 模型的约束条件，最小化第 r 轮输出变量汉明重量作为目标函数.

4) 构建 D-Wave CQM 模型，并使用 D-Wave Advantage 求解此模型；

设置可分性传播的终止条件，联立各不等式，即可得到一组可表示经过置换层的输入到输出可分性的传递不等式. 将 MILP 模型转化为如下量子退火 CQM 模型：

此模型中目标函数为：

$$E(x)=\sum_i a_i x_i+\sum_{i,j} b_{i,j} x_i x_j+c\,, \tag{18}$$

约束为：

$$\sum_i a_i^{(m)} x_i+\sum_{i\le j} b_{i,j}^{(m)} x_i x_j+c^{(m)}\circ 0\,. \tag{19}$$

其中 $i=1,...,N$ ，$m=1,...,M$ ，M 为约束的总数. x_i 取二进制. $a_i,b_{i,j},c\in R$ ，$\circ$ 为运算符，$\circ\in\{\ge,=,\le\}$.

至此可得到 PRESENT 算法经过 r 轮加密后的具有可分性传递规律的 CQM 模型，将其命名为 PRESENT-Q.

设定初始可分性为：
(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaacccc)
则 PRESENT-Q 9 轮积分区分器搜索模型如下：
目标函数：

$$E(x)=\min\sum_{i=577}^{640} x_i\,, \tag{20}$$

约束为：

$$\begin{cases} x_1=1\\ x_2=1\\ \vdots\\ x_{61}=0\\ x_{62}=0\\ x_{63}=0\\ x_{64}=0\\ x_1-x_2-x_3+0x_4+0x_{65}-x_{66}+0x_{67}+0x_{68}\ge -2\\ -2x_1-x_2-x_3-2x_4+5x_{65}+5x_{66}+5x_{67}+2x_{68}\ge 0\\ -5x_1-5x_2-5x_3-2x_4+x_{65}+2x_{66}+x_{67}+2x_{68}\ge -11\\ x_1+x_2+x_3+2x_4-2x_{65}-2x_{66}+0x_{67}-2x_{68}\ge -1\\ 0x_1+3x_2+0x_3+0x_4-x_{65}-x_{66}-x_{67}-x_{68}\ge -1\\ x_1+x_2+x_3+x_4+x_{65}-2x_{66}-2x_{67}-2x_{68}\ge -1\\ 3x_1+0x_2+0x_3+0x_4-x_{65}-x_{66}-x_{67}-x_{68}\ge -1\\ 0x_1+0x_2+3x_3+0x_4-x_{65}-x_{66}-x_{67}-x_{68}\ge -1\\ \vdots \end{cases}. \tag{21}$$

使用 D-Wave min_time_limit 函数，我们得到该问题最少 D-Wave 计费时间 T. 此时间包括问题加载值 QPU 上的时间、从 QPU 上获取结果的时间以及保证 QPU 在适当状态的校准操作等待时间等. 使用基于真实量子计算机 D-Wave Advantage 量子计算机的 LeapHybridCQMSample 求解器求解该模型，求解步骤如下：

1) 将 PRESENT-Q 以及经计算获得的时间 T 输入至求解器；

2) 调用 CPU 及 GPU 上运行的启发式求解器搜索 PRESENT-Q 问题的解决方案;

3) 给每个启发式求解器配备一个量子模块，制定量子查询并将其发送至 D-Wave Advantage QPU，嵌入至 Pegasus 拓扑结构中以进行后续求解；

4) QPU 对查询响应，发挥量子波动产生的量子隧穿效应，跳出局部亚优解，量子加速在计算时间内引导启发式搜索或提高当前解集的质量，以较大概率获得全局最优解；

5) 在时间 T 之前，启发式求解器将 PRESENT-Q 的求解结果发送至前端；

6) 根据目标函数值求解值是否满足终止条件来判断是否存在积分区分器.

在进行对称密码算法的量子安全强度评估时，目前主流研究大多采用理想化的量子模型，忽略了量子计算机的硬件发展情况. 本文首次使用真实量子计算机 D-Wave Advantage 对 SPN 结构对称密码进行探索. 利用量子退火算法其量子隧穿独特的全局寻优特性，使用本文提出的 QuCMC 架构将对称密码算法的攻击转化为难解数学问题的求解，采用量子退火与数学方法结合的对称密码算法攻击的新型技术路线. 利用可分性，我们构建了对称密码算法的 CQM 模型，将该模型嵌入至真实的量子计算机并使用量子退火算法量子加速求解. 通过以上实验，最终搜索到 PRESENT、GITF-64、RECTANGLE 三种算法的积分区分器，验证了量子退火算法攻击对称密码算法的可能性.

未来可通过本实验搜索得到的积分区分器，结合 Grover 算法利用相关密钥恢复方法进行密钥恢复攻击，更大规模发挥量子效能.

5 量子退火对称密码区分器搜索结果

本文探索了量子退火耦合传统数学方法的对称密码算法攻击新型计算架构 QuCMC. 结合积分攻击密码分析方法，精确刻画对称密码算法可分性的传播，构建待攻击算法的 MILP 模型. 将 MILP 模型转化为量子退火 CQM 模型，发挥量子隧穿优势，求解密码算法的 CQM 模型，搜索积分区分器，并将这一方法应用到 SPN 结构代表性算法 PRESENT、GIFT-64、RECTANGLE 上.

根据文献[54]的方法，我们先判断初始可分性有一比特常数时积分区分器的存在性，再降低活跃比特数，以找到更优的区分器（输入活跃比特相同的情况下，平衡比特数量更多）. 利用量子退火算法全局寻优，我们搜索到 PRESENT 算法经 8、9 轮的可分性传播的积分区分器，同时也搜索到了 GIFT-64 算法及 RECTANGLE 算法分别经 9 轮可分性传播的积分区分器：

■PRESENT 算法 8 轮的积分区分器：
Input:(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaccccc)
Output:(????????????bbbb????????????bbbb????????????bbbbbbbbbbbbbbbbbbbb)

■PRESENT 算法 9 轮的积分区分器：
Input:(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaacccc)
Output:(??? ??????????????????????b)

■GIFT-64 算法 9 轮的积分区分器
Input:(aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaaacaa)
Output:(??bb??bb??bb?? bb?? bb??bb??bb??bb??bb?? bb?? bb?? bb?? bb?? bb?? bb?? bb)

■RECTANGLE 算法 9 轮的积分区分器

$$\text{Input:}\begin{pmatrix}\text{aaaaaaaaaaaaaaaa}\\ \text{aaaaaaaaaaaaaaaa}\\ \text{aaaaaaaaaaaaaaaa}\\ \text{aaaaaaaaaaaacccc}\end{pmatrix}$$

$$\text{Output:}\begin{pmatrix}\text{???b???b???????b}\\ \text{???????b???b??bb}\\ \text{???b??bb???b???b}\\ \text{???b???b???b???b}\end{pmatrix}$$

其中 c 表示常数比特，a 表示活跃比特，?表示不确定比特，b 代表平衡比特.

以 9 轮 PRESENT 算法积分区分器为例解释求得的积分区分器，我们将最左边的 60 位固定为活跃比特，改变最右边的 4 位为常量输入，算法经过 9 轮加密后最右边的 1 位变为平衡的，而其它位为不确定比特. 本文中其它积分区分器可类似解释，在此不再赘述.

这是首次使用真实量子计算机对正在使用的多种全规模 SPN 结构算法构成实质性威胁，也是首次使用量子攻击在多种对称密码算法均达到和传统积分攻击二子集比特可分性最好结果[55] 一致的轮数.

不同的对称密码算法结构有一定的区别，其对应的建模方式以及最后得到的模型及所需变量及约束条件个数也有所区别，需要具体问题具体分析. PRESENT、GIFT-64、RECTANGLE 算法攻击实验所需的变量数和约束条件见表 3 所示. 以 9 轮 PRESENT 算法量子退火求解为例分析，目前使用的变量数为 640，在 CQM 模型构建时，9 轮的可分性传播刻画为 1280 个约束条件.

表 3 刻画三种算法所需资源

算法	轮数	变量	约束
PRESENT	8	576	1152
	9	640	1280
GIFT-64	9	640	1856
RECTANGLE	9	640	1856

使用本文算法，较经典文献中常使用的贪婪算法，刻画三种对称密码算法 *S* 盒不等式规模见表 4. 分别将 PRESENT、GIFT-64 和 RECTANGLE 三种算法的 S 盒不等式规模较贪婪算法分别了减少 27.27%、20%和 29.41%. 以 PRESENT 算法为例，该算法单轮加密由 16 个相同的 *S* 盒构成，因此刻画一轮 PRESENT 算法的 *S* 盒贪婪算法需要 176 个不等式，而本文仅需 128 个不等式，而此差距在轮数增大时将更大. 无论是使用经典算法求解还是使用量子算法求解，本文引入的方法均能减少计算资源，提高计算效率.

表 4 本文使用的约简算法较贪婪算法 *S* 盒刻画不等式规模

算法	本文	贪婪算法
PRESENT	8	11[49]
GIFT-64	12	15 [33]
RECTANGLE	12	17[49]

在文中我们成功确定了 SPN 结构三种密码的积分区分器. 在此基础上密钥恢复攻击的步骤开始于通过区分器选择相应的明文集合对其加密. 然后，猜测第 *r* 轮的密钥并对密文进行解密，验证得到的中间值是否符合第 *r*-1 轮的积分特性. 以上过程需要反复进行，直至密钥唯一确定. 感兴趣的读者可以参照文献[56]中的方法，使用本研究结果开展进一步的密钥恢复尝试.

同时，为对比量子退火算法与经典全局寻优算法的效率，针对本文中三种算法积分区分器搜索的 MILP 模型，我们在跳出局部亚优解能力与求解时间两个方面与模拟退火算法进行了对比，具体结果见表 5.

表 5 模拟退火与量子退火算法积分区分器搜索对比

密码算法	轮数	求解算法	求解时间/s	最小值
PRESENT	9	模拟退火	599.261	15
		量子退火	2.048	1
GIFT-64	9	模拟退火	666.450	16
		量子退火	2.048	1
RECTANGLE	9	模拟退火	629.057	15
		量子退火	2.048	1

从表 5 的实验结果可知，模拟退火算法以表 6 的参数在百倍超过量子退火求解时间的情况下，求解三种算法积分区分器搜索的 MILP 模型时均陷入了局部亚优解. 以 9 轮 PRESENT 算法积分区分器搜索为例说明，模拟退火算法在迭代 2500 次求解耗时 599.261 秒的情况下陷入局部亚优解，解的最小值为 15. 而本文使用量子退火算法在 2.048s 的切片时间内达到了比模拟退火算法更优的解，解的最小值为 1.

表 6 模拟退火求解 MILP 问题时参数设置情况

参数	最大迭代次数	退火初始温度	降温速度	局部搜索迭代次数
参数情况	5000	4000	0.999	400

注释：温度下降速度参数值越接近 1 表示缓慢降温，允许更

充分的探索.

通过本文实验证明，量子退火算法在大规模问题的求解时展示出了超过模拟退火算法的优势. 如同模拟退火算法会受到初始点选择、降温速度、局部搜索策略的影响，量子退火 Schedule 方案也会对退火结束时的叠加态产生影响，从而影响到退火的成功率. 如何设计合理的退火 Schedule 也是目前使用量子退火算法密码攻击的挑战之一.

通过以上实验，我们验证了 QuCMC 架构的可行性，同时为考虑对称密码抵御量子攻击提供了新思路. 未来通过对模型进一步的优化有望找到更高轮数的积分区分器，对 Lai-Massey 等其它结构的对称密码算法进行进一步的探索. 除可将密码组件刻画为 MILP 模型外，也可将其刻画为 NPC 问题 SAT，以攻击其它结构对称密码算法. 后期还可以考虑使用此架构，结合差分分析或线性分析进行对称密码算法攻击.

6 总结

量子计算已应用于多种密码算法的攻击和设计. QuCMC 计算架构结合了量子退火算法与传统算法的优势，利用量子退火算法赋能传统数学算法.

本文首次使用真实的量子计算机 D-Wave Advantage 完成多种全规模的 SPN 结构对称密码算法的区分器搜索，刻画一类具有代表性的 SPN 结构密码算法 PRESENT、GIFT-64、RECTANGLE 的可分性质的传播规律. 根据此传播规律，最终我们搜索到了三种算法最长 9 轮的积分区分器，并且将上述三种算法的 S 盒不等式规模较贪婪算法分别减少了 27.27%、20%和 29.41%. 本文实验验证了在真实量子计算机上运行量子退火算法攻击对称密码的可能性，打破了目前量子计算方法距数学方法攻击指标相距甚远的现状.

本文通过实验对比模拟退火算法，展示了 D-Wave 量子退火凭借独特的量子隧穿效应跳出局部亚优解的算法优势，这是拓展量子退火应用的关键.

基于 D-Wave 量子计算机迅猛且稳定的发展，本文的可行性验证，形成的一类通用型架构未来有望探索非 SPN 结构（如 Lai-Massey 结构）的对称密码攻击. 未来可以考虑在此架构的基础上，进一步研究量子退火算法对其它新型密码及抗量子密码算法的攻击.

目前各类量子计算就像初生的婴儿，与经典计算相比还有很大的差距. 量子化当前传统密码攻击时，面临以下难点：

1) 量子比特的稳定性维持

在执行量子算法过程中必须维持量子比特的量子相干性. 这一状态是量子计算能力的核心，它使量子叠加和量子纠缠等量子特性得以实现，这些现象是量子算法运行的基础. 然而，量子比特在实际操作中非常容易受到周围环境的干扰，导致退相干现象的发生. 如何保持量子比特的相干性，即延长其相干时间是量子计算面临的一项主要技术挑战，这也关乎量子计算密码攻击是否能成功.

2) 算法和硬件同步发展

理论上有效的量子算法需要与实际可用的量子硬件相匹配. 目前量子硬件的发展尚未达到理论模型中假定的性能标准，这也限制了理论算法的实际应用.

3) 量子算法选择

在量子化当前传统密码攻击过程中，选择适合的量子算法是实现有效攻击的核心. 不同的量子算法对各种密码体系的效果和适应性各异. 因此，在选择用于密码攻击的量子算法时，必须针对待攻击加密算法的结构特征选择合适的量子算法，确保选用的量子算法能够针对性地解决具体问题.

通过本文工作我们概念性验证了 QuCMC 计算架构的可行性. 随着量子计算的不断发展，利用量子计算赋能传统密码攻击数学方法可以使两种方法相辅相成，扩展量子计算的应用领域，有望进一步助力经典方法效能的提升.

参 考 文 献

[1] Wang D, Shan X, Dong Q, et al. No single silver bullet: Measuring the accuracy of password strength meters: //Proceedings of the USENIX Security Symposium 2023. Anaheim, USA, 2023: 947-964

[2] Li H, Qiu D, Luo L, et al., Exact distributed quantum algorithm for generalized Simon’s problem. Acta Informatica, 2024, 61(2): 131-159

[3] Su Z. Local information as an essential factor for quantum entanglement. Entropy, 2021, 23(6): 728

[4] Yin H, Fu Y, Li ChenL, et al. Experimental quantum secure network with digital signatures and encryption. National Science Review, 2022, 10(4): 228

[5] Wu Wen-Ling, Sui Han, Zhang Bin. Lightweight cryptography. Beijing: Tsinghua University Press, 2022(in Chinese)
(吴文玲，眭晗，张斌. 轻量级密码学. 北京: 清华大学出版社, 2022)

[6] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring //Proceedings of the 35th Annual Symposium on Foundations of Computer Science. Santa Fe, USA, 1994 : 124-134

[7] Grover L K. A fast quantum mechanical algorithm for database search //Proceedings of the 28th annual ACM symposium on Theory of computing. Philadelphia, USA, 1996 : 212-219

[8] Dong Xiao-Yang. A survey of quantum cryptanalysis of symmetric cryptography. Journal of Cryptologic Research, 2024,11(01): 159-173(in Chinese)
(董晓阳. 对称密码的量子分析法综述. 密码学报(中英文), 2024,11(01):159-173)

[9] Simon D R. On the power of quantum computation. SIAM journal on computing, 1997, 26(5): 1474-1483

[10] [10] Luo Yi-Yuan, Yan Hai-Lun, Wang Lei, et al. Study on block cipher structures against simon's quantum algorithm. Journal of Cryptologic Research, 2019, 6(5): 561-573(in Chinese)
(罗宜元, 闫海伦, 王磊, et al. 分组密码结构抗 Simon 量子算法攻击研究. 密码学报, 2019, 6(05): 561-573)

[11] Preskill J. Quantum computing in the NISQ era and beyond. Quantum, 2018, 2: 79

[12] Wang Z, Wei S, Long G, et al. Variational quantum attacks threaten advanced encryption standard based symmetric cryptography. Science China Information Sciences, 2022, 65(10): 200503

[13] Aizpurua B, Bermejo P, Martinez J, et al. Hacking cryptographic protocols with advanced variational quantum attacks. arXiv preprint arXiv:2311.02986, 2023

[14] Phab L, Louise S, Sirdey R. A first attempt at cryptanalyzing a (toy) block cipher by means of QAOA://Proceedings of the International Conference on Computational Science. London, UK, 2022: 218-232

[15] Farhi E, Goldstone J, Gutmann S. A quantum approximate optimization algorithm. arXiv preprint arXiv:1411.4028, 2014

[16] Kulshrestha A, Safro I. Beinit: Avoiding barren plateaus in variational quantum algorithms://Proceedings of the 2022 IEEE International Conference on Quantum Computing and Engineering. Broomfield. USA, 2022: 197-203

[17] Arute F, Arya K, Babbush R, et al. Quantum supremacy using a programmable superconducting processor. Nature, 2019, 574(7779): 505-510

[18] Acharya R, Aleiner L, Allen R, et al. Suppressing quantum errors by scaling a surface code logical qubit. Nature, 2023, 614(7949): 676-681

[19] Morvan A, Villalonga B, Mi X, et al. Phase transition in random circuit sampling. arXiv preprint arXiv:2304. 11119, 2023

[20] Brainard J. What's coming up in 2018. Science, 2018, 359(6371): 10-12

[21] Gibney E. Physics: Quantum computer quest. Nature, 2014, 516(7529): 24-26

[22] Finnila A, Gomez M, Sebenik C, et al. Quantum annealing: A new method for minimizing multidimensional functions. Chemical physics letters, 1994, 219(5-6): 343-348

[23] Somma R, Nagaj D, Kieferová M. Quantum speedup by quantum annealing. Physical review letters, 2012, 109(5): 050501

[24] Morita S, Nishimori H. Convergence theorems for quantum annealing. Journal of Physics A: Mathematical and General, 2006, 39(45): 13903

[25] King A, Raymond J, Lanting T, et al. Quantum critical dynamics in a 5,000-qubit programmable spin glass. Nature, 2023, 617(7959): 61-66

[26] Wang Chao, Yao Hao-Nan, Wang Bao-Nan et al. Progress in quantum computing cryptography attacks. Chinese Journal of Computers, 2020,43(09): 1691-1707(in Chinese)
(王潮, 姚皓南, 王宝楠, et al. 量子计算密码攻击进展. 计算机学报, 2020,43(09): 1691-1707)

[27] Wang Chao, Zhang Huan-Guo. The influence of Canadian commercial quantum computer in cryptography. Information Security and Communications Privacy, 2012, 35(2): 31-32+35(in Chinese)
(王潮, 张焕国. 加拿大商用量子计算机对密码学影响. 信息安全与通信保密, 2012, 35(2): 31-32+35)

[28] Wang Bao-Nan, Hu Feng, Zhang Huan-Guo, et al. From evolutionary cryptography to quantum artificial intelligent cryptography. Journal of Computer Research and Development, 2019，56(10): 2112-2134 (in Chinese)
(王宝楠, 胡风, 张焕国等. 从演化密码到量子人工智能密码综述. 计算机研究与发展, 2019, 56(10): 2112-2134)

[29] Peng W, Wang B, Hu F, et al. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. Science China: Physics,Mechanics & Astronomy, 2019, 62(6): 60311

[30] Wang B, Hu F, Yao H, et al. Prime factorization algorithm based on parameter optimization of Ising model. Scientific reports, 2020, 10(1): 7106

[31] Wang Chao, Wang Qi-Di, Hong Chun-Lei, et al. Quantum annealing public key cryptographic attack algorithm based on D-Wave advantage. Chinese Journal of Computers, 2024, 47(5): 1030-1044(in Chinese)
(王潮，王启迪，洪春雷等. 基于 D-Wave Advantage 的量子退火公钥密码攻击算法研究. 计算机学报, 2024, 47(5): 1030-1044)

[32] Bogdanov A, Knudsen L, Leander G, et al. PRESENT: An ultra-lightweight block cipher://Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop. Vienna, Austria, 2007: 450-466

[33] Banik S, Pandey S K, Peyrin T, et al. GIFT: A small present: Towards reaching the limit of lightweight encryption://Proceedings of the Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, China, 2017: 321-345

[34] Zhang W, Bao Z, Lin D, et al. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms, Cryptology ePrint Archive, 2014,

[35] Farhi E, Goldstone J, Gutmann, et al. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem. Science, 2001, 292(5516): 472-475

[36] Orús R, Mugel S, Lizaso E. Quantum computing for finance: Overview and prospects. Reviews in Physics, 2019, 4: 100028

[37] Ding Y, Chen X, Lamata L, et al. Implementation of a hybrid classical-quantum annealing algorithm for logistic network design. SN Computer Science, 2021, 2: 1-9

[38] Adachi S, Henderson M. Application of quantum annealing to training of deep neural networks. arXiv preprint arXiv:1510.06356, 2015

[39] Wang Bao-Nan, Yao Hao-Nan, Hu Feng, et al. Quantum annealing

distributed integer decomposition study of local field coefficient h and coupling coefficient J with stability Ising model. Scientia Sinica: Physica, Mechanica & Astronomica, 2020, 50(3): 131-141(in Chinese)
(王宝楠, 姚皓南, 胡风等. 具有稳定性 Ising 模型局部场系数 h 和耦合项系数 J 的量子退火分布式整数分解研究. 中国科学: 物理学, 力学, 天文学. 2020, 50(3): 131-141)

[40] Hu F, Lamata L, Sanz M, et al. Quantum computing cryptography: Finding cryptographic boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer. Physics Letters A, 2020, 384(10): 126214

[41] Mott A, Job J, Vlimant J, et al. Solving a higgs optimization problem with quantum annealing for machine learning. Nature, 2017, 550(7676): 375-379

[42] Neukart F, Compostella G, Seidel C, et al. Traffic flow optimization using a quantum annealer. Frontiers in ICT, 2017, 4: 29

[43] Johnson M, Amin M, Gildert S, et al. Quantum annealing with manufactured spins. Nature, 2011, 473(7346): 194-198

[44] Todo Y, Morii M. Bit-based division property and application to Simon family: //Proceedings of the Fast Software Encryption: 23rd International Conferenc. Bochum, Germany, 2016: 357-377

[45] Liang Min, Luo Yi-Yuan, Liu Feng-Mei. A Survey on quantum-secure symmetric cryptography. Journal of Cryptologic Research, 2021,8(06): 925-947(in Chinese)
(梁敏, 罗宜元, 刘凤梅. 抗量子计算对称密码研究进展概述. 密码学报, 2021,8(06): 925-947)

[46] Daemen J, Rijmen V, Fast Software Encryption: 9th International Workshop. Belgium: Springer, 2002

[47] Cui Ting-Ting. Security Analysis of block ciphers and stream ciphers [Ph.D. Dissertation]; Shandong University, Shandong, 2018
(崔婷婷. 分组密码算法和流密码算法的安全性分析 [博士学位论文]; 山东大学, 山东, 2018)

[48] Todo Y. Structural evaluation by generalized integral property: //Proceedings of the Advances in Cryptology--EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria, 2015: 287-314

[49] Xiang Z, Zhang W, Bao Z, et al. Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers://Proceedings of the Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security. Hanoi, Vietnam, 2016: 648-678

[50] Mouha N, Wang Q, Gu D, et al. Differential and linear cryptanalysis using mixed-integer linear programming: //Proceedings of the Information Security and Cryptology: 7th International Conference. Beijing, China, 2012: 57-76

[51] Sun S, Hu L, Wang P, et al., Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES (L) and other bit-oriented block ciphers, ://Proceedings of the Advances in Cryptology–ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, China, 2014: 158-178

[52] Sasaki Yu, Todo Yosuke. New algorithm for modeling S-box in MILP based differential and division trail search: //Proceedings of the Innovative Security Solutions for Information Technology and Communications: 10th International Conference. Bucharest, Romania, 2017: 150-165

[53] Huang Ming, Zhang Sha-Sha, Hong Chun-Lei, et al. MILP modeling of division property propagation for block ciphers with complex linear layers. Journal of Software, 2024,35(04): 1980-1992(in Chinese)
(黄明, 张莎莎, 洪春雷等. 分组密码复杂线性层可分性传播的 MILP 刻画方法. 软件学报, 2024,35(04): 1980-1992)

[54] Tian W, Hu B, Integral cryptanalysis on two block ciphers Pyjamask and uBlock. IET Information Security, 2020, 14(5): 572-579

[55] Ghosh S, Dunkelman O. Automatic search for bit-based division property: //Proceedings of the Progress in Cryptology–LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security. Bogotá, Colombia, 2021: 254-274

[56] Shang F, Shen X, Liu G, et al., Integral cryptanalysis on PUFFIN based on MILP. Journal of Cryptologic Research, 2019, 6(5): 627-638
(尚方舟, 沈璇, 刘国强等. 基于 MILP 搜索的 PUFFIN 算法积分分析, 密码学报. 2019, 6(5): 627-638

附录：待攻击对称密码算法简介

传统通信技术的数据安全保护技术不适用于发展极快的物联网环境，在此背景下轻量级密码算法应运而生. 由于实现高效及低功耗等特点，轻量级密码应用场景广泛，包括 RFID、物联网、智慧农业、智慧家电等领域[5].

利用 QuCMC 架构，我们搜索了 SPN 结构三种轻量级对称算法的积分区分器，三种算法结构相同，但每种算法的加密时密码部件又有所不同. SPN 结构中 S 指混淆层，P 为扩散层，可表示为图 S1 的形式. 该结构基于 Shannon 的混淆扩散原理实现其整体结构，相较 Feistel 结构具有扩散速度快的特点.

为了使读者能够充分理解文中的攻击，本节将简单介绍实验攻击的三种具有代表性的 SPN 结构对称密码算法. 以 PRESENT 算法为例，我们将阐述各个组件的操作过程. 另外两种算法由于篇幅限制，将仅进行简要说明，感兴趣的读者可阅读文中对应的参考文献进行详细了解.

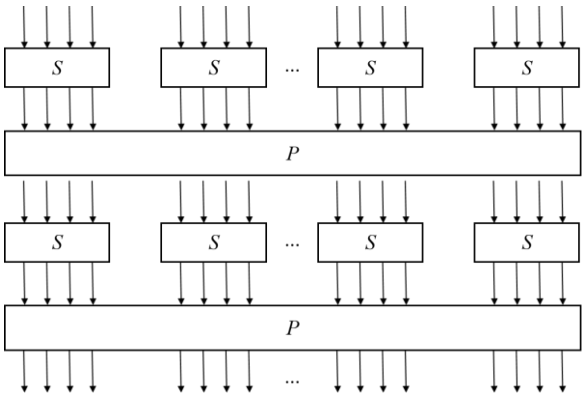

图 S1　SPN 结构示意图

■PRESENT 算法[32]

Bogdanov 等人在 CHES2007 提出的 PRESENT 算法有很强的代表性，2012 年被纳入 ISO/IEC 轻量级密码分组标准. 吴文玲在其《轻量级密码》[5]书中评价到：“PRESENT 在轻量级密码算法中占据了重要的地位，在设计之初，它一度曾被认为是最杰出的超轻量级密码算法. ”PRESENT 算法分组长度为 64 比特，加密算法的迭代轮数为 31，密钥长度为 80 或 128 比特. 算法的加密输入可分为两个部分：64 比特明文以及 80 或 128 比特密钥. 每一轮的基本操作可分为三步：

1) 轮密钥加；
2) *S* 盒代换；
3) *P* 置换.

其加密过程如图 S2 所示.

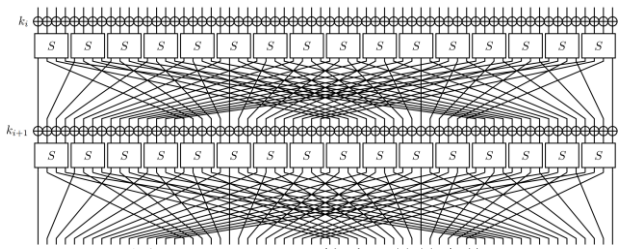

图 S2　PRESENT 算法两轮轮变换

PRESENT 算法的 *S* 盒起到混淆的作用，使明密文关系对关系尽量复杂，是 4 进 4 出的 *S* 盒， *S* 盒具体变换如表 S1 所示.

表 S1 PRESENT 算法的 *S* 盒

a	0	1	2	3	4	5	6	7
S(a)	*C*	5	6	*B*	9	0	*A*	*D*
a	8	9	*A*	*B*	*C*	*D*	*E*	*F*
S(a)	3	*E*	*F*	8	4	7	1	2

PRESENT 算法的 *P* 置换起到扩散的作用，相当于对 *S* 盒输出的状态位进行移位操作，可以使用以下公式表示置换的过程，其中 *b* 为第 *i* 轮输出的状态位.

$$P_i(b)=\begin{cases}16\cdot b \bmod 63 & 0\le b\le 62\\ 63 & b=63\end{cases}. \qquad \text{(S1)}$$

本实验利用加密算法中的初始可分性在 *S* 盒和 *P* 置换中的传播规律搜索区分器，而异或操作不改变可分性，所以本节仅对 *S* 盒和 *P* 置换两部分操作进行详细解释，不再赘述 PRESENT 算法的密钥扩展操作部分，感兴趣的读者可阅读文[32]详细了解.

■GIFT 算法[33]

GIFT 算法借鉴了 PRESENT 算法的设计原则，并在线性壳安全性方面进行了改进，同时优化了硬件实现的速度.

GIFT 算法分为两个版本，根据分组长度不同，分别为 GIFT-64 和 GIFT-128. 其中，GIFT-64 的分组长度为 64 比特，迭代轮数为 28；GIFT-128 的分组长度为 128 比特，迭代轮数为 40. 两个版本的密钥长度均为 128 比特. 算法轮变换基本操作可分为以下三步：

1) *S* 盒代换；
2) *P* 置换；
3) 轮密钥加.

GIFT 算法每个组件的具体操作可参见文[33]，这里不再展开描述.

■ RECTANGLE 算法[34]

RECTANGLE 是采用比特切片技术，兼顾软硬件性能的一种密码算法，其分组长度为 64 比特，密钥长度为 80 比特和 128 比特，加密算法迭代轮数为 25. 与以上两种算法不同的是 RECTANGLE 算法使用 4 行 16 列的矩阵表示密码状态. 前 16 比特为矩阵的第一行，以此类推. 算法轮变换基本操作可分为以下三步：

1) 轮密钥加；
2) 列替换，每一列 4 比特为一组做 *S* 盒变换；
3) 行移位，对每一行的 16 比特做左循环移位操作.

该算法每个组件的基本模块定义见文[34]，此处不再赘述.

PEI Zhi, Ph. D. candidate. Her main research interests include cyberspace security and quantum computing cryptography.

HONG Chun-Lei, Ph. D. candidate. His main research interests include cyberspace security and quantum computing cryptography.

WANG Qi-Di, M. S. His main research interests include cyberspace security and quantum computing cryptography.

HU Qiao-Yun, M. S. Her main research interests include cyberspace security and quantum computing cryptography.

WANG Chao, Ph. D., professor. His main research interests include artificial intelligence, cyberspace security and quantum computing cryptography.