基于D-Wave Advantage的量子退火公钥密码攻击算法研究

王 潮 王启迪 洪春雷 胡巧云 裴 植

(上海大学特种光纤与光接入网重点实验室 上海 200444)

摘 要 D-Wave专用量子计算机的原理量子退火凭借独特的量子隧穿效应可跳出传统智能算法极易陷入的局部极值,可视为一类具有全局寻优能力的人工智能算法.本文研究了两类基于量子退火的RSA公钥密码攻击算法(分解大整数$N=pq$):一是将密码攻击数学方法转为组合优化问题或指数级空间搜索问题,通过Ising模型或QUBO模型求解,提出了乘法表的高位优化模型,建立新的降维公式,使用D-Wave Advantage分解了200万整数2269753.大幅度超过普渡大学、Lockheed Martin和富士通等实验指标,且Ising模型系数h范围缩小了84%,系数J范围缩小了80%,极大地提高了分解成功率,这是一类完全基于D-Wave量子计算机的攻击算法;二是基于量子退火算法融合密码攻击数学方法优化密码部件的攻击,采用量子退火优化CVP问题求解,通过量子隧穿效应获得比Babai算法更近的向量,提高了CVP问题中光滑对的搜索效率,在D-Wave Advantage上实现首次50比特RSA整数分解.实验表明,在通用量子计算机器件进展缓慢情况下,D-Wave表现出更好的现实攻击能力,且量子退火不存在NISQ量子计算机VQA算法的致命缺陷贫瘠高原问题:算法会无法收敛且无法扩展到大规模攻击.

关键词 RSA;D-Wave;量子退火;CVP;量子隧穿;整数分解;量子计算

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2024.01030

Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage

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

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

Abstract Quantum computing presents an exciting yet formidable challenge to cryptographic security. The advancement of various quantum computers in their efforts to attack RSA has been notably sluggish. In contrast to the constraints imposed by key technologies such as error correction codes on universal quantum computers, the developments of critical theoretical and hardware developments of D-Wave special quantum computers show a stable growth trajectory. Quantum annealing is the fundamental principle behind D-Wave special quantum computing. It has a unique quantum tunneling effect that can jump out of the local extremes that traditional intelligent algorithms are prone to fall into. It can be considered a class of artificial intelligence algorithms with global optimization-seeking capability. This paper introduces two technical approaches grounded in the quantum annealing algorithm, using pure quantum algorithm and quantum annealing combined with classical algorithm to implement RSA public key cryptography attack (factorizing the large integer $N=pq$). One is to convert the mathematical method of cryptographic attack into a combinatorial optimization problem or exponential space search problem, which is solved by Ising model

收稿日期:2023-06-02;在线发布日期:2024-01-15.**王 潮**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为人工智能、网络空间安全、量子计算密码.E-mail:wangchao@shu.edu.cn.**王启迪**,硕士研究生,主要研究方向为网络空间安全、量子计算密码.**洪春雷**,博士研究生,主要研究方向为网络空间安全、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.**裴 植**(通信作者),博士研究生,主要研究方向为网络空间安全、量子计算密码.E-mail:peizhiiii@163.com.

or QUBO model. We propose a high level optimization model for multiplication tables and establish a new dimensionality reduction formula from the two aspects of saving qubit resources and improving the stability of Ising model, and decompose the two million level of integers 2 269 753 using D-Wave Advantage. Not only does it significantly exceed the experimental indexes of Purdue University, Lockheed Martin and Fujitsu, but the range of coefficient h of the Ising model is reduced by 84% and the range of coefficient J is reduced by 80%, which greatly improves the success rate of decomposition. This is a class of attack algorithms entirely based on D-Wave quantum computers. Secondly, based on quantum annealing algorithm fused with mathematical methods of cryptographic attacks to optimize the attacks on cryptographic components. The classical lattice reduction algorithm is synergistically integrated with the Schnorr algorithm. The quantum annealing algorithm is incorporated, and the Babai algorithm's rounding direction is adjusted leveraging the quantum tunneling effect for precise vector determination. Leveraging the exponential acceleration capabilities of quantum computing, we address the challenge by computing two rounded directions for solutions on each bit of an N-dimensional lattice. This enables the realization of an exponential solution space search, a capability beyond the reach of traditional computing methods. This approach enhances the search efficiency for close vectors in the CVP(Closest Vector Problem) by considering both the resource and time costs associated with qubits. And we implement the first 50-bit integer decomposition on D-Wave Advantage. Randomly selecting RSA integer decompositions within the range of 4—50 bits serves as a demonstration to validate the algorithm's universality and expansibility. The experiments indicate that, in the context of slow progress in universal quantum computing devices, D-Wave quantum annealing has shown better realistic attack capabilities. Quantum annealing does not suffer from the critical deficiency of the NISQ(Noisy Intermediate-Scale Quantum) quantum computing VQA(Variational Quantum Algorithms)—the barren plateaus problem, which can lead to algorithmic convergence issues, and it cannot be extended to large-scale attacks.

Keywords　RSA; D-Wave; quantum annealing; CVP; quantum tunneling; integer factorization; quantum computing

1　引　言

近年来量子信息技术不断地有突破性成果涌现，如南京大学尹华磊教授等人[1]构建了首个集信息安全通信、数字签名、秘密共享和会议密钥协议于一体的量子安全网络，谷歌于 2018 年推出 72 量子比特芯片狐尾松(Bristlecone)[2]，2019 年推出量子霸权芯片悬铃木(Sycamore)[3]，2023 年提高量子霸权芯片的容错率[4-5]. 谷歌已达到通往构建大型量子计算机道路上六个里程碑中的第二个[6].

但是，谷歌的量子霸权芯片至今依旧不能用于密码破译. 2023 年富士通的最新进展仅为分解 253＝11×23. 量子计算对密码的攻击是一个令人振奋又举步维艰的挑战难题.

公钥密码体制的安全性，一般是基于数学上的计算困难问题. 如 RSA 的安全性依赖于大整数因子分解的困难性. 这些数学问题在传统计算机上无法在多项式时间内解决，Farhi 等人[7-8]通过实验验证了量子退火对于部分数学问题求解有更大优势. 不同于通用量子计算机，由加拿大 D-Wave 量子计算公司开发的专用量子计算机 D-Wave 发展迅猛. 量子退火算法可发挥其量子隧穿效应，在指数级空间搜索问题中使量子直接穿过能量势垒，有望逼近甚至以较大概率获得全局最优解. 2011 年王潮和张焕国[9]认为这是 D-Wave 量子退火可以用于密码攻击和设计的重要理论基础，并在国际上首次提出 D-Wave 量子退火密码设计和密码攻击的研究. 在密码攻击和密码设计(如抗多种攻击指标密码设计)缺乏多种有效的数学方法时，其指数级解空间“解的结构”和“解的分布概率”均不明确时，可以把密码攻击和密码设计的问题转为指数级解空间求

解问题，借助 D-Wave 量子退火独特的量子隧穿效应跳出搜索的局部极值，快速逼近全局最优解. 由于量子退火算法没有量子近似优化算法(Quantum Approximate Optimization Algorithm, QAOA)等量子算法存在的贫瘠高原问题，为这类技术路线能够稳定、全局遍历的实施密码攻击提供算法理论支撑(QAOA 等算法的贫瘠高原问题会导致搜索过程不收敛，不能遍历性的攻击，有的整数分解不能实现). 2018 年，Jiang 等人[10]使用了一种改进乘法表的算法，将整数分解问题转化成优化问题并嵌入 Ising 模型中，使用 D-Wave2000Q 量子计算机成功分解 19 位比特整数 376289. 该算法在专用量子计算机上使用量子退火成功超越了通用量子算法. 2019 年，Peng 等人[11]将乘法表做出优化并添加约束，减少了量子比特的使用，成功分解 20 位比特整数 1005973. Lockheed Martin 公司的 Warren[12]通过遍历分解 10000 以内的整数来展示他们的算法. 2021 年，上海大学陈玺教授等人[13]使用数字化绝热量子分解算法分解了整数 2479. 近两年，Ji 等人[14-15]提出新型计算架构来验证 D-Wave 量子退火对密码学的扩展性.

D-Wave 量子计算机硬件平台发展迅猛而稳定，D-Wave 公司计划将在 2023 年或 2024 年发布下一代量子计算机 Advantage2. 全新的量子计算机具有 7000 多个量子比特，有新的拓扑结构 Zephyr 和更大的能量规模，这大大提高了量子比特资源的使用效率. 2022 年郭光灿院士[16]指导的本源量子撰文认为，D-Wave 专用量子计算机进行公钥密码攻击效果比通用量子计算机的技术路线更好.

在本文中，通过栏宽均为 2 的分栏方式从乘法表高栏位置分析了变量和进位之间的关系，减少了量子比特的使用. 针对降维公式的惩罚项做出改进，提出了新的优化模型，进一步降低局部场系数 h 和耦合项系数 J 的范围. 基于真实量子计算机 D-Wave Advantage 成功分解 22 位比特整数 2269753. 本文通过量子赋能经典算法，利用量子退火的量子隧穿优势优化 CVP 的解，提高了 CVP 问题中光滑对的搜索效率，加快了分解整数的速度. 首次实现 50 比特整数分解. 通过两个实验论证了量子退火在公钥密码攻击中的重要作用.

2 D-Wave 量子退火发展历程

2.1 符号说明

本文符号的含义见表 1.

表 1 符号含义

符号	含义
mK	毫开尔文，为热力学单位
Ising	用于描述自旋之间的作用
QUBO	用于解决组合优化问题的数学模型
$\boldsymbol{h}$	二维模型中一次项系数组成的矩阵
$\boldsymbol{J}$	二维模型中二次项系数组成的矩阵

2.2 量子退火算法

量子退火是一种基于绝热理论的启发式人工智能算法. 量子退火利用量子波动产生的量子隧穿效应，可以跳出局部亚优解. 算法的运行要在接近绝对零度的−273.145 度，只有 25 kW 的低功耗，远低于高性能计算机的损失. 若通过系统初态制备使其处于某一已知基态，同时将系统末态哈密顿量[17]的基态编码为组合优化问题的最优解，则可基于绝热演化理论处理相应的组合优化问题并得到最优解. 当一个量子系统在绝热条件下由哈密顿量初态缓慢演化到终态，假设初态处于哈密顿量的基态，则演化结束后哈密顿终态也处于基态. 该过程可由式(1)描述：

$$H(t)=\left(1-L\left(\frac{t}{T}\right)\right)H_{\text{init}}+L\left(\frac{t}{T}\right)H_{\text{final}} \quad (1)$$

其中 H_{init} 为哈密顿初态，H_{final} 为哈密顿终态，T 为总退火时间，$t\in[0,T]$，L 为单调递增函数，$L(0)=0$，$L(1)=1$.

基于量子隧穿效应和绝热理论，量子退火算法可以以更大的概率跳出局部亚优解，逼近甚至直接找到全局最优解. 在公钥密码攻击研究中，可以将数学问题转化成组合优化问题，映射为二次无约束二值优化(Quadratic Unconstrained Binary Optimization, QUBO)或者 Ising 形式[17]. 这样就将整数分解问题转化为最小值求解问题，然后利用量子退火算法求解系统最低能量下的最优解. 量子退火的适用范围包括：

(1)在小规模问题求解中由于不需要跳出局部亚优解，量子退火与经典方法都能达到全局最优.

(2)在指数级科学问题求解中，如果数学方法没有确定性数学公式，而解空间分布又没有规律的情况下，数学方法推导的数学公式只能相当于局部极值，量子退火有望通过量子隧穿效应跳出局部极值，逼近全局最优.

(3)当经典数学算法无法逼近全局最优，量子退火可以在经典算法基础之上进一步搜索，有望把经典方法继续向前推进.

2.3 D-Wave 量子计算机的硬件发展

如今很多复杂的计算问题无法用传统系统来解

决.数据的巨大增长促使人们寻求新工具.量子计算是下一个前沿领域,为解决困难问题提供了一种新方法.量子计算机主要分为两种架构:门模型量子计算机和绝热演化量子计算机.门模型使用量子门实现计算算法,类似于经典计算机中的布尔门.D-Wave使用的量子退火算法可以在低能状态下缓慢演化从而求得最优解.

D-Wave 成立于 1999 年,是量子计算系统、软件和服务领域的领导者,也是世界上第一家量子计算机商业供应商.该公司最初计划使用高温超导体"D 波超导体"材料制备量子比特.直到 2007 年该公司展示了第一台原型机 D-Wave Orion.Orion 拥有 16 个由约瑟夫森结构成的量子比特,是世界上首台量子退火计算机.2011 年,D-Wave 推出了 D-Wave One,声称是全球第一个商业量子计算机.同年 9 月,D-Wave 在《Nature》上刊登论文[17],证明了 D-Wave 芯片的量子特性.美国航天航空制造商 Lockheed Martin 公司购买 128 量子比特系统 D-Wave One.在他们的需求中,公司自己的系统解决问题需要耗费几个月时间,而 D-Wave 量子退火只需要几个星期.2013 年至 2015 年,D-Wave 分别发布了 D-Wave Two 和 D-Wave 2X,并先后被 NASA、谷歌和 Los Alamos 国家实验室购买,应用于各种复杂问题,如机器学习、规划和调度等.2017 年,D-Wave 推出了 D-Wave2000Q,具有全新的量子比特拓扑结构 Chimera.D-Wave2000Q 处理器具有较低的噪声,其性能是上一代的 25 倍.2020 年,D-Wave 推出 Advantage 量子计算机,并允许用户通过 Leap 云服务访问量子系统.该量子计算机具有 5000 多个量子比特和全新的拓扑结构 Pegasus.D-Wave 称预计在 2023～2024 年推出新一代量子计算机 Advantage2,该机器具有连通性更优的 Zephyr 拓扑结构和超过 7000 个量子比特.D-Wave 的发展迅猛,也是最适合商业化的量子计算机.D-Wave 量子计算机的发展历程见图 1,拓扑结构发展见表 2.

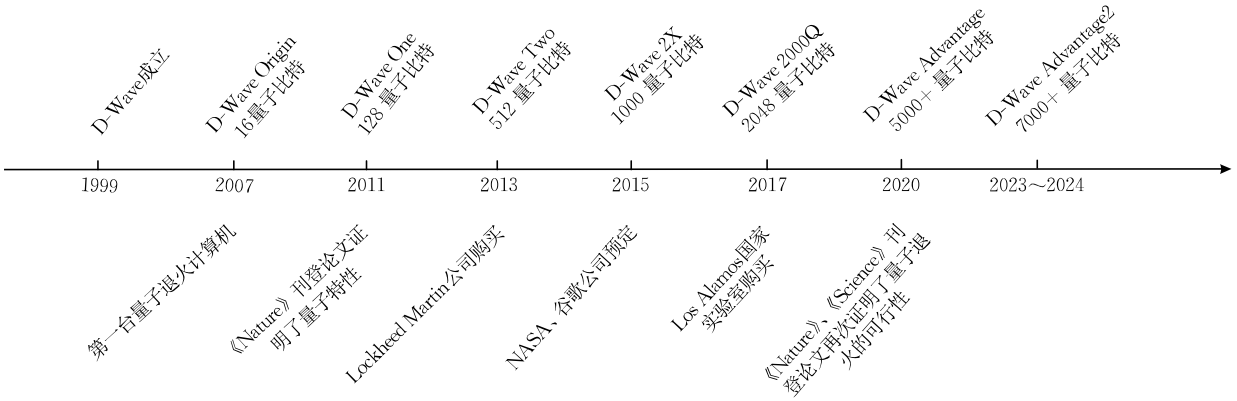

图 1　D-Wave 的发展历程

表 2　量子拓扑结构发展

	D-Wave 2000Q	D-Wave Advantage	D-Wave Advantage2
量子比特数量	2048	5000+	7000+
拓扑结构	Chimera	Pegasus	Zephyr
上市时间	2017 年	2021 年	2023～2024 年
量子比特连接数量	6	15	20

D-Wave 系统包含一个 QPU,必须将其保持在接近绝对零度的温度下,并与周围环境隔离,以便以量子力学方式表现.系统应满足以下要求:

(1)低温,使用闭环低温稀释冰箱系统实现.QPU 可在低于 15 mK 的温度下运行.

(2)屏蔽电磁干扰,使用功能射频屏蔽外壳和磁屏蔽系统实现.

D-Wave 的量子比特在冷却至绝对零度时,会实现两个状态的叠加.首先在彻底消除量子比特间相互作用的同时施加"横向磁场"的控制信号,目的是使量子比特更容易同时既向上又向下.然后在磁场不断减弱的同时,不断增强量子比特间的相互作用.量子比特会根据设定值变成两个状态的其中一个,所有量子比特会向最稳定、最低能量演化.对比通用量子计算机受纠错码等关键技术的制约,D-Wave 的关键理论和硬件发展呈现稳定的增长态势.

D-Wave 的量子比特数量远高于通用量子计算机,增长速度也优于通用量子计算机.D-Wave 每一代都优化了量子的拓扑结构,更新的拓扑结构具有更好的连通性,可以提高量子比特使用率,提高量子计算机性能.

2.4　量子退火应用于密码学的两类技术路线起源

量子计算攻击公钥密码的技术路线可划分为三大类.第一类是基于通用量子计算机来完成攻击,如

著名的 Shor 算法，利用量子的并行性，把整数分解问题转化为寻找函数的周期问题，从而利用量子加速来求解此类问题. Shor 算法对 RSA 的攻击也一直受到各方关注. 但受到通用量子计算机硬件发展的限制. 谷歌的量子霸权芯片尚没有实现 Shor 算法.

第二类和第三类是王潮、张焕国[9]提出的基于专用量子计算机 D-Wave 的量子退火算法，其独特的量子隧穿效应可以跳出传统智能算法的局部亚优解，可以视为一类基于量子效应的智能算法. 利用人工智能设计出高强度的密码和密码设计自动化是密码学界的研究焦点. 2011 年左右首次提出[9] D-Wave 量子计算机或可用于密码攻击和密码设计，将密码攻击和设计问题转为 D-Wave 量子计算机擅长求解的组合优化问题或指数级解空间搜索问题，基于 Ising 模型或 QUBO 模型求解. 这是不同于通用 Shor 算法的一类新的量子计算攻击公钥密码的技术路线[18-19].

2012 年以后进一步提出[9,20-21]第三类技术路线：可以把密码函数设计和密码部件攻击所涉及的困难数学问题求解，转为组合优化问题或指数级解空间搜索问题，这恰是量子退火的优点. 基于这类技术路线是量子计算与传统数学方法的结合，并对其中的某个部件的数学问题求解进行量子加速. 2017 年，使用量子算法结合侧信道攻击的思想完成了 ECC 密码攻击[22]，实现量子算法结合经典数学算法的技术路线. 针对抗多种密码攻击的布尔函数设计，基于 D-Wave 2000Q 真实量子计算机完成了国际上首次量子计算机密码设计实验[23]，这是量子退火与经典数学算法结合用于密码设计的一个概念性验证实验.

第二类和第三类技术路线也是本文涉及的两类技术路线.

3 D-Wave 对公钥密码攻击的两种技术路线研究

3.1 量子退火算法分解 RSA-22 的算法设计——第一类技术路线

3.1.1 分栏二进制乘法表算法

RSA 密码的攻击问题主要困难在于大整数分解的困难性. 下面方法使用乘法表分栏操作将整数分解问题转化为组合优化问题. 定义 $N=pq$，N 为待分解的整数，p、q 为两个素数.

$$p=(1,p_{l_1-1},p_{l_1-2},\cdots,p_1,1),$$

$$q=(1,q_{l_2-1},q_{l_2-2},\cdots,q_1,1).$$

l_1 和 l_2 为 p、q 的二进制比特数量，$l_1=\lfloor\log_2 p\rfloor$，$l_2=\lfloor\log_2 q\rfloor$.

考虑到穷举法的威胁，两素数不应该相差太大，这里令 $l_1=l_2$. 所以通常认为两个素数的二进制长度相等. 以 $143=11\times13$ 为例，乘法表见表 3. 将该乘法表划分为 3 栏，栏宽分别为 2、2、2. 该思想由 Jiang 等人[10]提出. 进位也根据划分的栏考虑. 根据每一栏的变量关系列出式(2). 通过 $x_i=(1-s_i)/2$ 将变量的取值范围从[0,1] 映射到 [+1,−1]，然后嵌入 Ising 模型中使用量子退火求解.

表 3 $N=pq$ 的二进制乘法表

$143=11\times13$								
p					1	p_2	p_1	1
q					1	q_2	q_1	1
					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
进位		c_4	c_3	c_2	c_1			
N	1	0	0	0	1	1	1	1

$$f=(p_1+q_1+2p_2+2p_1q_1+2q_2-4c_1-8c_2-3)^2+(p_2q_1+p_1q_2+2q_1+2p_2q_2+2p_1+c_1+2c_2-4c_3-8c_4+1)^2+(q_2+p_2+c_3+2c_4-2)^2 \quad (2)$$

3.1.2 高位优化模型

在二进制乘法表分栏算法中，栏宽的取值也会影响退火的效果. 栏宽越宽时，单栏列出的表达式变量数将相应增加，系数范围也会变大. 这不利于量子退火算法优势的发挥. 因此，本文将栏宽全部限制在 2. 此时，乘法表的最高位置的栏就会出现以下两种情况：

	q_{l_2-1}	
1	p_{l_1-1}	
c_M	c_{M-1}	
1	n_{l-1}	

(1)

		q_{l_2-1}	
	1	p_{l_1-1}	
c_M	c_{M-1}	c_{M-2}	
1	n_{l-1}	n_{l-2}	

(2)

其中，p_{l_1-1} 和 q_{l_2-1} 为素数 p 和 q 中的变量，n_{l-1} 和 n_{l-2} 为整数 N 的变量，c 为进位. 在单栏中，假设最右列为第一列，基于二进制乘法表，如果第一列的权重为 1，那么第二列的权重为 2. 根据此计算方法结合乘法表的结构，上一栏包含权重为 1 的变量 4

个和进位 1 个，权重为 2 的变量 3 个和进位 1 个. 因此，上一栏最大值为 13，往最高栏的进位个数最多为两个. 因此第二种情况 c_M 恒为 0.

根据 N 的最高两位为 10 和 11 两种取值分别对以上两种情况讨论，总共分为 4 种情况.

(1) (1.1)10：$c_M=c_{M-1}=p_{l_1-1}=q_{l_2-1}=0$，

(1.2)11：$c_M=0$，$c_{M-1}=1-p_{l_1-1}-q_{l_2-1}$；

(2) (2.1)10：$c_M=0$，$c_{M-2}=2(1-c_{M-1})+n_{l-2}-p_{l_1-1}-q_{l_2-1}$，

(2.2)11：$c_M=0$，$c_{M-1}=1$，$c_{M-2}=2+n_{l-2}-p_{l_1-1}-q_{l_2-1}$.

根据以上 4 种情况，最终在 1 种情况下可以减少 4 个量子比特资源，1 种情况下可以减少 3 个量子比特资源，2 种情况可以减少 2 个量子比特资源. 其中在(1)的(1.1)情况下，可以将 p_{l_1-1} 和 q_{l_2-1} 置 0. 在乘法表中，这两个变量使用非常频繁，将它们置 0 可以减少方程的多项式数量，大大减少模型系数范围. 在量子计算机发展还不完善的大环境下，量子比特资源的节约非常重要. 减少量子比特的使用有利于量子退火的成功率.

3.1.3　新型降维公式

由于 Ising 模型只接受一维或二维多项式，而优化问题中往往会出现更高维多项式. 普渡大学的 Jiang 等人[10]在将优化问题映射到 Ising 模型时，采用降维式(3). 据 Jiang 等人的描述，以正项为例，公式的正确性来自式(4).

$$\begin{cases}\min(x_1x_2x_3)=\min(x_4x_3)+2(x_1x_2-2x_1x_4-2x_2x_4+3x_4)\\ \min(-x_1x_2x_3)=\min(-x_4x_3)+2(x_1x_2-2x_1x_4-2x_2x_4+3x_4)\end{cases}\tag{3}$$

$$\begin{cases}x_1x_2x_3=x_4x_3+2(x_1x_2-2x_1x_4-2x_2x_4+3x_4)\ \text{if}\ x_4=x_1x_2\\ x_1x_2x_3<x_4x_3+2(x_1x_2-2x_1x_4-2x_2x_4+3x_4)\ \text{if}\ x_4\neq x_1x_2\end{cases}\tag{4}$$

当 $x_4=x_1x_2$ 时，原式最低能量下等式左边的值等于等式右边的值. 该方法通过使用新变量替换旧变量并且加入惩罚项作为约束条件将 3 次项转换为 2 次项. 惩罚项符合如式(5)：

$$\begin{cases}x_1x_2-2x_1x_4-2x_2x_4+3x_4=0\ \text{if}\ x_4=x_1x_2\\ x_1x_2-2x_1x_4-2x_2x_4+3x_4>0\ \text{if}\ x_4\neq x_1x_2\end{cases}\tag{5}$$

这里存在一种特殊情况，当 $x_1=x_2=x_3=1$ 时，若 $x_4=1$，则 $x_4x_3=1$，$x_1x_2-2x_1x_4-2x_2x_4+3x_4=0$，若 $x_4=0$，则 $x_4x_3=0$，$x_1x_2-2x_1x_4-2x_2x_4+3x_4=1$. 两项和相同，这样不能保证 $x_4=x_1x_2$. 因此，Jiang 在文章里给惩罚项加上系数 2，以保证 $x_4\neq x_1x_2$ 时的表达式取值始终大于 $x_4=x_1x_2$ 时表达式的取值.

这种使用惩罚项的方式使得降维公式的系数偏大，最大为 6. 该系数会被代入到优化问题表达式中，影响量子退火的效果. 因此，缩小系数范围非常有必要.

本文摒弃这种方法，将惩罚项混合到替换后的新变量表达式中，然后对整个表达式的系数进行调整. 在满足条件的情况下，将系数降低到最低.

为了找到系数最低的公式，首先定义新的降维表达式：

$$f=Ax_1+Bx_2+Cx_3+Dx_4+Ex_1x_2+Fx_1x_3+Gx_1x_4+Hx_2x_3+Ix_2x_4+Jx_3x_4,$$

表达式中 x_1、x_2、x_3 均为目标变量，x_4 为附加变量，添加附加变量是为了缩小公式维度. 为了将三维降到二维，需要将 $x_1x_2x_3$ 替换为 x_4x_3，其中 $x_4=x_1x_2$. 为了保证 $x_4=x_1x_2$，需要令同一情况下 $x_4\neq x_1x_2$ 的 f 值大于 $x_4=x_1x_2$ 的 f 值. 例如在表 4 中 x_1、x_2、x_3 的取值分别为 0、0、0 时，$x_4=x_1x_2=0$ 的 f 值为 0，则 $x_4=1$ 的 f 值为 D，应大于 0；当 x_1、x_2、x_3 的取值分别为 1、1、1 时，$x_4=x_1x_2=1$ 的 f 值为 $A+B+C+D+E+F+G+H+I+J=x_1x_2x_3=1$，则 $x_4=0$ 的 f 值为 $A+B+C+E+F+H$，应大于 1，即满足式(6).

$$\begin{cases}f=x_1x_2x_3\ \text{if}\ x_4=x_1x_2\\ f>x_1x_2x_3\ \text{if}\ x_4\neq x_1x_2\end{cases}\tag{6}$$

表 4　优化后的降维公式 f 真值表

正项($x_1x_2x_3$)						负项($-x_1x_2x_3$)					
x_1	x_2	x_3	x_4	$x_1x_2x_3$	值	x_1	x_2	x_3	x_4	$-x_1x_2x_3$	值
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0	0	1	0	2
0	0	1	0	0	0	0	0	1	0	0	0
0	0	1	1	0	2	0	0	1	1	0	1
0	1	0	0	0	0	0	1	0	0	0	0
0	1	0	1	0	0	0	1	0	1	0	1
0	1	1	0	0	0	0	1	1	0	0	0
0	1	1	1	0	1	0	1	1	1	0	0
1	0	0	0	0	0	1	0	0	0	0	0
1	0	0	1	0	0	1	0	0	1	0	1
1	0	1	0	0	0	1	0	1	0	0	0
1	0	1	1	0	1	1	0	1	1	0	0
1	1	0	1	0	0	1	1	0	1	0	0
1	1	0	0	0	1	1	1	0	0	0	0
1	1	1	1	1	1	1	1	1	1	−1	−1
1	1	1	0	1	1	1	1	1	0	−1	0

将新的降维表达式替换原来的三维表达式 $x_1x_2x_3$ 后，在表达式最小值下 x_4 始终等于 x_1x_2，保证了降维公式的正确性. 量子退火原理为求解哈密顿量的最低能量，在问题中体现为求解表达式的最小值，也即问题的正确解. 按照上述举例，将表 4 中 x_1、x_2、x_3 的 8 种情况下 16 个约束条件全部列出，计算出 f 的所有最低系数.

$$\begin{cases}0=0\\D>0\\C=0\\C+D+J>0\\B=0\\B+D+I>0\\B+C+H=0\\B+C+D+H+I+J>0\\A=0\\A+D+G>0\\A+C+F=0\\A+C+D+F+G+J>0\\A+B+D+E+G+I=0\\A+B+E>0\\A+B+C+D+E+F+G+H+I+J=1\\A+B+C+E+F+H>1\end{cases}.$$

以上为正项取值的 16 个约束条件，负项可同理得到. 在满足所有约束条件下找到表达式 f 所有系数最小的式(7). 在式(7)中，所有 x_1、x_2、x_3 的 8 种取值情况下 $x_4\neq x_1x_2$ 的能量均高于 $x_4=x_1x_2$ 的能量. 正项公式的系数最大为 4，负项公式的系数最大为 5，均低于式(3).

$$\begin{cases}\min(x_1x_2x_3)=\min(x_4x_3+2x_1x_2-3x_1x_4-3x_2x_4+4x_4)\\\min(-x_1x_2x_3)=\min(-x_4x_3+x_1x_2-3x_1x_4-3x_2x_4+5x_4)\end{cases}\tag{7}$$

考虑到算法需要计算的是 x_1、x_2、x_3 的值，x_4 为中间变量. x_4 取值的正确性并不影响结果需要的正确解. 例如，在表 4 中 x_1、x_2、x_3 的取值分别为 0、0、0 时，$x_4=x_1x_2=0$ 的 f 值为 0，则 $x_4=1$ 的 f 值为 D，为大于等于 0，与之前相比区别为 $x_4=1$ 时 f 值可以等于 0，即满足式(8). 因为在该情况下，虽然 $x_4\neq x_1x_2$，但 x_1、x_2、x_3 的结果是正确的，我们最终只需要提取 x_1、x_2、x_3 的结果. 因此 $x_4=x_1x_2$ 与 $x_4\neq x_1x_2$ 的能量相等时，加上这个条件后重新对降维公式的系数调整.

$$\begin{cases}f=x_1x_2x_3 \text{ if } x_4=x_1x_2\\f\geq x_1x_2x_3 \text{ if } x_4\neq x_1x_2\end{cases}\tag{8}$$

根据式(8)，以正项为例使用同样的方法列出所有约束条件.

$$\begin{cases}0=0\\D\geq 0\\C=0\\C+D+J\geq 0\\B=0\\B+D+I\geq 0\\B+C+H=0\\B+C+D+H+I+J\geq 0\\A=0\\A+D+G\geq 0\\A+C+F=0\\A+C+D+F+G+J\geq 0\\A+B+D+E+G+I=0\\A+B+E\geq 0\\A+B+C+D+E+F+G+H+I+J=1\\A+B+C+E+F+H\geq 1\end{cases}.$$

在满足以上所有条件的情况下，将系数降到最低，找到表达式 f 系数最低的式(9).

$$\begin{cases}\min(x_1x_2x_3)=\min(x_4x_3+x_1x_2-x_1x_4-x_2x_4+x_4)\\\min(-x_1x_2x_3)=\min(-x_4x_3-x_1x_4-x_2x_4+2x_4)\end{cases}\tag{9}$$

其真值表为表 4. 其中正项公式与 Wang 等人[18]的公式一致，系数最大为 1，相比式(3)和式(6)有大幅度减小. 而负项为新公式，系数最大为 2. 虽然系数没有降到 1，但是相比式(3)和式(7)也有大幅度减小，并且多项式长度也缩短了. 负项公式在实际计算中效果非常明显.

优化后的降维模型对局部场系数 h 和耦合项系数 J 的取值范围影响非常大. 替换优化后的新公式后，两项系数将会大幅度缩小，这对 D-Wave 的退火效果将有明显提高.

3.1.4 实验结果

本文将优化变量和降维公式后得到的 Ising 模型提交给 D-Wave 真实量子计算机中成功分解了 22 位整数 2269753.

首先在分解 7781 的实验时，在同样的分栏方式下分析了 Warren 等人[12]、Jiang 等人[10]和 Wang 等人[19]与本文的算法在 h 和 J 范围的对比，见表 5. Lockheed Martin 公司的 Warren 通过遍历分解10000以内的整数来展示他们的算法. 因此，本文用分解 7781 的结果将本文的算法与 Warren 和其他人之前的工作，在 h 和 J 范围上做对比. 实验结果表明，本文算法的量子比特数量具有很大优势，特别是在降

低局部场系数 h 和耦合项系数 J 的范围方面. 与 Wang 等人的实验相比，局部场系数 h 的范围缩小了 79%，耦合项系数 J 的范围缩小了 87%，系数范围缩小明显. 系数范围的缩小可以降低量子比特间的耦合强度，使各量子比特翻转统一，增强量子间的耦合稳定性，对本文算法相比 Wang 等人的方法可能在量子比特上没有优势，但目前 D-Wave 量子退火算法的瓶颈在于 h 和 J 的数量和范围太多，实验结果表明减小系数范围比减少量子比特在分解时所带来的优势更明显.

表 5　分解 7781 对比实验

算法	量子比特使用数量	h 范围	J 范围
Warren 等人的方法	419	10^6	10^6
Jiang 等人的方法	40	777.50	344
Wang 等人的方法	29	613.25	554
Ours	40	126.75	68

3.2　量子退火融合经典算法分解 RSA-50——第二种技术路线

3.2.1　基础概念

格：格是 R^m 中一类具有周期性结构的离散点的集合. 也即格是 m 维欧式空间 R^m 的 $n(m\geq n)$ 个线性无关向量组 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n$ 的所有整系数线性组合. 即

$$L(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n)=\left\{\sum_{i=1}^{n}x_i\boldsymbol{b}_i : x_i\in\mathbb{Z},\ i=1,2,\cdots,n\right\}.$$

最近向量问题[24](Close Vector Problem，CVP)：给定格 L 和在 n 维欧式空间上的目标向量 $\boldsymbol{t}$，找一个非零格向量 $\boldsymbol{v}$，满足对格 L 上任意非零向量 $\boldsymbol{u}$，有 $\|\boldsymbol{v}-\boldsymbol{t}\|\leq\|\boldsymbol{u}-\boldsymbol{t}\|$.

LLL 算法[25]：LLL 算法是一种著名的格约简算法. 由 Lenstra、Lenstra 和 Lovász 在 1982 年提出. LLL 算法主要包括施密特正交化、约简和交换三个步骤. 可以在多项式时间内求解 n 维格问题.

Babai's 最近平面算法[26]：Babai 算法是一种可用于求解 CVP 问题的最近平面算法. 主要分为两个步骤：(1) 使用 LLL 算法优化输入格基；(2) 搜寻在 LLL 基下与目标向量 $\boldsymbol{t}$ 最接近的整数系数组合.

光滑对[24]：设 $\{p_i\}_{i=0,1,\cdots,n}$ 是一组质数基，如果待分解整数的所有质因数都小于 p_n，则称这个整数为 p_n 光滑. 如果 x_j 和 y_j 都为 p_n 光滑，且满足下式，则 (x_j,y_j) 是一组光滑对.

$$x=\prod_{i=1}^{n}p_i^{e_i},\ x-yN=\prod_{i=0}^{n}p_i^{e_i'}(e_i,e_i'\in\mathbb{N}).$$

3.2.2　算法步骤

利用量子退火融合经典方法，将整数分解问题转换为求解格上的最近向量问题(CVP)[24,27]. 使用 LLL 算法和 Babai 算法计算得到一组近似解. 将格、目标向量和近似解转化为哈密顿量，使用量子退火算法求解最低能量下更优解中存在的光滑对. 处理量子退火后的解得到整数 N 的质因数. 随机生成 50 比特以内的可分解整数进行分解，选定数据后实验可分为以下几个步骤：

(1) 首先选择一组质数基，并根据待分解整数构造格和目标向量.

(2) 使用 LLL 算法对上一步构造的格和目标向量进行约简处理，使用 Babai 算法计算 CVP 解.

(3) 将量子退火算法作为量子优化器对 Babai 算法的经典向量进行优化，在 Babai 算法解的基础上寻找更高质量的 CVP 解.

(4) 利用量子退火找到的距离目标向量更近的向量，求得足够多的光滑对.

(5) 利用求得的光滑对构建线性方程组并求解，分解得到 N 的两个质因数 p 和 q.

3.2.3　分解 50 比特整数

基于最近向量问题(CVP)，本文使用对文献[24,27]修改后的格基和目标向量构造式(10)和(11)，计算出格基 $\boldsymbol{B}=[\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_n]$ 和目标向量 $\boldsymbol{t}$.

$$\boldsymbol{B}=\begin{pmatrix} f(1) & 0 & \cdots & 0 \\ 0 & f(2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(n) \\ \lceil 10^c\ln p_1\rfloor & \lceil 10^c\ln p_2\rfloor & \cdots & \lceil 10^c\ln p_n\rfloor \end{pmatrix} \tag{10}$$

$$\boldsymbol{t}=(0\quad\cdots\quad 0\quad\lceil 10^c\ln N\rfloor) \tag{11}$$

其中，N 为待分解整数，n 为格的维度，$f(x)=x$，$x=1,2,\cdots,n$，$p_i\in[2,3,5,7,\cdots](i=1,2,\cdots,n)$ 为前 n 个质数构成的质数基. 为获得更多的光滑对，矩阵 $\boldsymbol{B}$ 的对角线为前 n 个整数随机排列的无重复组合. 通过生成更多的格基增加最近向量的搜索空间，避免出现在维度 n 下无法找到足够光滑对的情况. 格中向量的权重为 c，如果 c 是整数，更容易将格参数变为整数，提高一定的精度. 格的维度 n 通过式 $n=\log N/\log\log N$ 计算.

本文使用 Babai 算法对构造后的格基求解. Babai 算法可以在多项式时间内给出一个近似解. 使用 LLL 算法得到有利后续 Babai 算法求解的一组好基 $\boldsymbol{D}=[\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots\boldsymbol{d}_n]$，其向量之间两两正交. 对格基作正交化和约简有利于 Babai 算法给出高质量近似解 $\boldsymbol{t}_B$，也有利于提高后续量子部分的运算效能.

使用 Babai 算法求 CVP 解时会计算向量的正交系数，在计算这一参数时需要包含取整运算操作，而这一步骤会丢失一定的精度，影响 CVP 解的质量. 本文使用了量子退火算法，优化了求解 CVP 问题时的取整方向选择，从而找到更优解.

使用 n 个量子位来定义 n 个向量基系数的偏移. Ising 变量 σ_Z 的两个状态分别表示对应向量基正交系数的两个取整方向. 在表 6 中展示了 Babai 算法正交系数两个取整方向上对应的浮动变量和 Ising 模型变量之间的关系.

表 6 浮动变量和 Ising 变量的编码情况

正交系数取整方向	浮动变量 s	Ising 变量 σ_Z	变量映射关系
向上取整	0	1	$s=\frac{\sigma_Z-1}{2}$
	−1	−1	
向下取整	0	1	$s=\frac{1-\sigma_Z}{2}$
	1	−1	

如表 6 中所示，浮动变量取值 0 表示不在该向量基上作修正，即按照 Babai 算法正交系数的取整方向搜索. 浮动变量取值 ±1 表示在 Babai 算法正交系数取整的两个方向作修正处理，以此来寻找离目标向量更近的向量. 距离越近，解的质量越高，找到光滑对的概率也越大. 量子退火将搜索范围缩小至最低能量附近，以此来提高寻找光滑对的效率.

在 Babai 算法找到了 n 个向量基组合下的解后，使用量子退火算法寻找这 n 个向量基在两个取整方向下的更优解. 随着维度 n 的增长，搜索空间的范围将是指数级的增长，传统计算机将无法在非多项式时间内完成. 量子退火算法是一种启发式的人工智能算法，在大规模组合优化问题以及指数级解空间搜索问题上有独特的求解方式. 因此，本文将搜索更优解问题转化成组合优化问题并嵌入到 Ising 模型中，使用量子退火算法求解.

$\boldsymbol{t}'=\sum_{i=1}^{n}s_i\boldsymbol{d}_i$ 为 n 个向量基的修正处理部分，s_i 为第 i 个浮动变量. 量子算法优化后的更近向量为 $\boldsymbol{t}_{QA}=\boldsymbol{t}_B+\boldsymbol{t}'$. 由优化后的 $\boldsymbol{t}_{QA}$ 和目标向量 $\boldsymbol{t}$ 的欧氏距离构建出哈密顿量式(12).

$$H=\|\boldsymbol{t}-(\boldsymbol{t}'+\boldsymbol{t}_B)\|^2=\sum_{i=1}^{n+1}|\boldsymbol{t}_i-(\boldsymbol{t}'_i+t_{B_i})|^2 \tag{12}$$

其中 $\boldsymbol{t}=(t_1,t_2,\cdots,t_{n+1})$，$\boldsymbol{t}'=(t'_1,t'_2,\cdots,t'_{n+1})$，$\boldsymbol{t}_B=(t_{B_1},t_{B_2},\cdots,t_{B_{n+1}})$.

将哈密顿量中的一次项系数和二次项系数分别映射到 Ising 模型的局部场系数矩阵 $\boldsymbol{h}$ 和耦合项系数矩阵 $\boldsymbol{J}$ 中. 两个矩阵中的参数取值范围直接影响到量子退火的最低能量求解概率. LLL 算法的约简操作可以缩小这两个系数矩阵的参数范围.

Babai 算法和量子退火算法得到的解与初始格中的向量基之间的关系为 $\boldsymbol{t}_{QA}\approx\sum_{i=1}^{n}e_i\boldsymbol{b}_i$（$e_i$ 为线性组合系数）. 由格基 $\boldsymbol{B}$ 的第 $n+1$ 行可得到如下关系式：

$$p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}\approx N,$$

其中 $u=\prod p^{e_i}$，$e_i>0$，$v=1/\prod p^{e_i}$，$e_i<0$，易得关系式 $|u-vN|\approx 0$. CVP 解的质量越高，$|u-vN|$ 值越接近于 0. 为了更高效地找到足够多的光滑对，$|u-vN|$ 的质因数边界应适当放大. 经过 50 比特以下的实验结果，在权衡后选取边界为 $2n^2$，该范围方程组求解效率会更高一些，如果边界过大会影响方程组求解效率. 如果 u 的最大质因子小于等于第 n 个质数，$|u-vN|$ 的最大质因子不大于第 $2n^2$ 个质数，那么 u 和 $|u-vN|$ 为一组光滑对. 为了确保可得到足够的线性方程组用于分解整数，一般需要光滑对数量略大于 $|u-vN|$ 的边界 $2n^2$.

在找到足够多的光滑对后，需要将光滑对转换成线性方程组. 然后求解方程组得到呈线性相关关系的向量来分解整数. 基于筛法的原理，接下来需要找到两个二次指数的整数构成模 N 同余式. 首先，根据同一质数的指数 e_i 组合构建线性方程组，将 e_i 的奇偶性编码为二进制（1 代表 e_i 为奇数，0 代表 e_i 为偶数）. 将这样的线性方程组转化为一个二进制矩阵，然后寻找矩阵中线性相关的行向量组. 将向量组中对应的 u 和 $|u-vN|$ 分别连乘就能得到两个二次指数的整数. 这两个整数为模 N 同余关系：

$$\prod_{i=1}^{k}|u_i-v_iN|=\prod_{i=1}^{k}u_i-wN\equiv\prod_{i=1}^{k}u_i \bmod N,$$

$$\prod_{i=1}^{n}u_i-\prod_{i=1}^{n}|u_i-v_iN|\equiv 0 \bmod N.$$

k 为线性相关的行向量组维数，$w\in\mathbb{Z}$ 为化简后 N 的系数.

由光滑对组求解线性方程组可以在多项式时间内完成. 在本文中，首先使用高斯消元法将光滑对化简为行最简形，得到一组极大线性无关向量组. 其它的行向量均可由线性无关向量组线性表出，它们均可构成线性相关的行向量组. 这个步骤的复杂度为 $O(n^3)$.

使用线性相关的行向量组构成平方同余式，结合平方差公式，找到两个大整数 $X+Y$ 和 $X-Y$.

$$(X+Y)(X-Y)\equiv 0 \bmod N.$$

使用辗转相除法寻找 N 的两个质因子：

$$\begin{cases} p=\gcd(X+Y,N) \\ q=\gcd(X-Y,N) \end{cases}.$$

下面以 50 比特 $845\,546\,611\,823\,483=40\,052\,303\times 21\,111\,061$ 为例，介绍量子退火在该技术路线中的加速效果.

本文选用的例子格基和目标向量为 $\boldsymbol{B}$ 和 $\boldsymbol{t}$.

$$\boldsymbol{B}=\begin{pmatrix} 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8 \\ 69\,315 & 109\,861 & 160\,944 & 194\,591 & 239\,790 & 256\,495 & 283\,321 & 294\,444 & 313\,549 & 336\,730 \end{pmatrix},$$

$$\boldsymbol{t}=(0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 0\quad 3\,437\,100)^{\mathrm{T}}.$$

Babai 算法求解的向量 $\boldsymbol{t}_B$ 为

$$\boldsymbol{t}_B=(9\quad 4\quad 0\quad -6\quad 0\quad 5\quad 3\quad 7\quad 8\quad 0\quad 3\,437\,098),$$

与目标向量 $\boldsymbol{t}$ 的欧式距离为 $\|\boldsymbol{t}_B-\boldsymbol{t}\|=284$.

在 Babai 算法计算 CVP 解时使用正交系数进行就近取整运算，在一定程度上影响 CVP 解的质量. 因此，本文使用量子退火算法在求解 CVP 问题的取整方向上寻找更优解.

通过式(12)计算得到哈密顿量式(13). 提取式(13)的一次项系数组成局部场系数矩阵 $\boldsymbol{h}$，提取二次项系数组成耦合项系数矩阵 $\boldsymbol{J}$.

$$\begin{aligned} H_{10}=&2952I-498\sigma_Z^1-536\sigma_Z^2-358.5\sigma_Z^3-467\sigma_Z^4-83.5\sigma_Z^5-333.5\sigma_Z^6-562\sigma_Z^7-219\sigma_Z^8-679\sigma_Z^9-413\sigma_Z^{10}+\\ &17.5\sigma_Z^1\sigma_Z^2-42\sigma_Z^1\sigma_Z^3+85\sigma_Z^1\sigma_Z^4+88\sigma_Z^1\sigma_Z^5-28\sigma_Z^1\sigma_Z^6+64\sigma_Z^1\sigma_Z^7+43\sigma_Z^1\sigma_Z^8+85\sigma_Z^1\sigma_Z^9+43.5\sigma_Z^1\sigma_Z^{10}+77\sigma_Z^2\sigma_Z^3+\\ &84\sigma_Z^2\sigma_Z^4+13\sigma_Z^2\sigma_Z^5+72.5\sigma_Z^2\sigma_Z^6+66\sigma_Z^2\sigma_Z^7+7.5\sigma_Z^2\sigma_Z^8+73\sigma_Z^2\sigma_Z^9+26\sigma_Z^2\sigma_Z^{10}+20\sigma_Z^3\sigma_Z^4-39\sigma_Z^3\sigma_Z^5+68\sigma_Z^3\sigma_Z^6+\\ &56.5\sigma_Z^3\sigma_Z^7+18.5\sigma_Z^3\sigma_Z^8+53\sigma_Z^3\sigma_Z^9+19\sigma_Z^3\sigma_Z^{10}+78\sigma_Z^4\sigma_Z^5+33\sigma_Z^4\sigma_Z^6+21\sigma_Z^4\sigma_Z^7-\sigma_Z^4\sigma_Z^8+55\sigma_Z^4\sigma_Z^9+14\sigma_Z^4\sigma_Z^{10}-\\ &71.5\sigma_Z^5\sigma_Z^6-65\sigma_Z^5\sigma_Z^7+29.5\sigma_Z^5\sigma_Z^8-48\sigma_Z^5\sigma_Z^9-57\sigma_Z^5\sigma_Z^{10}+119\sigma_Z^6\sigma_Z^7+53.5\sigma_Z^6\sigma_Z^8-3\sigma_Z^6\sigma_Z^9+42.5\sigma_Z^6\sigma_Z^{10}+\\ &44.5\sigma_Z^7\sigma_Z^8+51\sigma_Z^7\sigma_Z^9+85\sigma_Z^7\sigma_Z^{10}+50\sigma_Z^8\sigma_Z^9-21.5\sigma_Z^8\sigma_Z^{10}+101.5\sigma_Z^9\sigma_Z^{10} \end{aligned} \tag{13}$$

$$\boldsymbol{h}^{\mathrm{T}}=\begin{pmatrix} \sigma_Z^1 & \sigma_Z^2 & \sigma_Z^3 & \sigma_Z^4 & \sigma_Z^5 & \sigma_Z^6 & \sigma_Z^7 & \sigma_Z^8 & \sigma_Z^9 & \sigma_Z^{10} \\ -498 & -536 & -358.5 & -467 & -83.5 & -333.5 & -562 & -219 & -679 & -413 \end{pmatrix},$$

$$\boldsymbol{J}=\begin{pmatrix} & \sigma_Z^1 & \sigma_Z^2 & \sigma_Z^3 & \sigma_Z^4 & \sigma_Z^5 & \sigma_Z^6 & \sigma_Z^7 & \sigma_Z^8 & \sigma_Z^9 & \sigma_Z^{10} \\ \sigma_Z^1 & & 17.5 & -42 & 85 & 88 & -28 & 64 & 43 & 85 & 43.5 \\ \sigma_Z^2 & & & 77 & 84 & 13 & 72.5 & 66 & 7.5 & 73 & 26 \\ \sigma_Z^3 & & & & 20 & -39 & 68 & 56.5 & 18.5 & 53 & 19 \\ \sigma_Z^4 & & & & & 78 & 33 & 21 & -1 & 55 & 14 \\ \sigma_Z^5 & & & & & & -71.5 & -65 & 29.5 & -48 & -57 \\ \sigma_Z^6 & & & & & & & 119 & 53.5 & -3 & 42.5 \\ \sigma_Z^7 & & & & & & & & 44.5 & 51 & 85 \\ \sigma_Z^8 & & & & & & & & & 50 & -21.5 \\ \sigma_Z^9 & & & & & & & & & & 101.5 \\ \sigma_Z^{10} & & & & & & & & & & \end{pmatrix}.$$

真实 D-Wave Advantage 的拓扑结构需要使用多个物理量子比特来表示一个逻辑量子比特，以达到全联通的物理结构. 故在真实量子计算机求解该 10 哈密顿问题时使用了 16 个 D-Wave Advantage 物理量子比特.

将局部场系数矩阵 $\boldsymbol{h}$ 和耦合项系数矩阵 $\boldsymbol{J}$ 嵌入

量子计算机的 Ising 模型中得到最低能量对应的解. 表 7 展示了使用 D-Wave Advantage 求解得到的 10 个最低能量对应解集,求解次数代表在 1000 次退火中,对应解集出现次数.

Babai 算法求解的 CVP 解与目标向量的欧氏距离为 284,量子退火算法求解的最近距离为 274. 量子退火可以得到优于 Babai 算法的解,该解有更高的概率获得光滑对. 通过该解的格基线性组合获得 u,v 以及 $|u-vN|$ 的值,见表 8. 在小规模问题求解时,Babai 算法就已经陷入了局部极值,D-Wave 量子退火算法的优势为其可以跳出局部极值,以较大概率达到全局最优解. 未来在大规模求解时其优势将更加明显.

表 7 使用 D-Wave Advantage 得到 10 组解集

序号	能量	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	解出现次数
1	274	+1	+1	+1	+1	+1	+1	+1	−1	+1	+1	552
2	284	+1	+1	+1	+1	+1	+1	+1	+1	+1	+1	280
3	379	+1	+1	+1	+1	+1	−1	+1	+1	+1	+1	32
4	404	+1	+1	+1	+1	−1	−1	+1	+1	+1	+1	28
5	426	+1	+1	+1	−1	+1	+1	+1	−1	+1	+1	13
6	440	+1	+1	+1	−1	+1	+1	+1	+1	+1	+1	15
7	483	+1	−1	+1	+1	+1	+1	+1	+1	+1	+1	7
8	503	+1	−1	+1	+1	+1	+1	+1	−1	+1	+1	8
9	508	+1	+1	+1	+1	+1	+1	+1	−1	+1	−1	6
10	524	+1	+1	+1	+1	+1	+1	−1	+1	+1	+1	12

表 8 量子退火求解更低能量对应的光滑对

能量	量子比特状态位	u	v	$\lvert u-vN\rvert$
274	0000000100	$11^2*13*17^4*23^5$	1	$2^3*3^2*7*359*433*647$

由搜索到的光滑对求解线性方程组,将线性方程组中的 u 和 $|u-vN|$ 分别累乘得到 X 和 Y:

$X=$
9727024140598355259821831651790451719883194683554487089075517280072264866872695476773824341280273304665677436723472999905540983335744987697464378544097696504581071333766983138358252577449169056632033231404691787590312670780218403548521691252998461186460858387942767975300033637452476569174783574752020767831190684460600353125599714800195355573768210366552484159978666660834503369718412204951509598616868284638769845845489521825313568115234375000000000000000000000000000,

$Y=$
1281527508733708112191819725353664613698391043433945322801722445714993112052882565458389957141448455060718275496551494024798658161553754407371710573557067939557897612217649553100830256609840672343583780281364854203488667727538910258023077363622317056449210235079660106689833375147119606710660474265789957275787525022315808318147266301069814971290891098304753434380823843380141982027123525874117708087330947144199060313659499.

由于光滑对边界为 200,为了保证得到线性相关的向量组,总共搜索了 230 个光滑对. 从 230 个光滑对中的找到了 67 个呈线性相关关系的行向量组. 由这 67 个向量得到 X 和 Y. 最后使用辗转相除法求解式(14),

$$\begin{cases} p=\gcd(X+Y,N) \\ q=\gcd(X-Y,N) \end{cases} \tag{14}$$

得到 $845546611823483=40052303\times21111061$,即最终的整数分解的两个素因子.

近似最近向量的质量和光滑对数量成正比,光滑对数量会影响线性方程组求解的成功率,进而决定能否成功分解整数.

3.2.4 结果分析

Farhi 等人[7-8]通过实验验证了量子退火对于部分数学问题求解有更大优势. 量子退火的量子加速效应在 2012 年已经被 Los Alamos 国家实验室认证[28]. D-Wave 量子退火的优势体现在小规模问题求解时可与经典数学方法一样达到全局最优解,但指数级大规模问题求解时有更大概率跳出局部极值. 本文在进行整数分解实验时,在 Babai 算法解的基础上发挥量子隧穿效应找到更优的 CVP 解,表现出了一定的量子加速效能,对 4～50 比特内的整数做分解实验,每一位比特中随机选取一个整数,结果见附录.

第一类技术路线 RSA-22 整数分解全部依赖于 D-Wave 量子退火算法. 第二类技术路线 RSA-50 整数分解是量子退火融合密码攻击数学方法. 从人

工智能类脑认知的角度，量子退火与密码攻击数学方法的结合，相当于把人类已有经验和认知融入量子退火的密码攻击中，会更加提升量子计算的攻击效果. 例如，一些密码攻击和设计问题的求解，相当于多目标约束问题优化求解，数学方法推导的数学公式在一些情况下相当于得到局部极值. 事实上，这个局部极值附近可能还有一些更好的解. 量子退火独特的隧穿效应可跳出局部极值，逼近全局最优解. 因此从类脑认知的角度利用数学家已经得到的攻击结果，利用量子隧穿效应有望得到进一步的更优的解. 在解决抗多种攻击布尔函数设计[14]的时候，将其看作一个多目标函数的组合优化问题，以数学方法为起始点，利用量子隧穿效应对 IEEE IT[29]上的工作做了一定的推进. D-Wave 的硬件发展迅速而稳定，且没有 QAOA 等算法存在的贫瘠高原问题. 这两类技术路线都有很好的量子计算机的硬件支撑以及稳定的算法理论.

量子退火的优势很明显，利用量子隧穿优势跳出局部亚优解，处理大规模问题. 如同各类智能算法一样，量子退火也存在一些局限性，在算法的参数设置方面也需要做优化考虑：

(1) 如同模拟退火会受到初始点选择、温度降低模型、马氏链设计的影响，量子退火 Schedule 对退火结束时的基态重叠状态也会产生重大影响，会影响求解的效率.

(2) 操控量子对温度要求非常严格. 在常温环境下，量子退火并不能高效地演化到最低能量，尤其是随着规模增大，量子退火的成功率逐渐减小. 在 80 mK 时进入模拟退火状态，20 mK 时进入量子退火状态，量子退火的合理环境温度应控制在接近绝对零度，尽量在 5 mK 以下.

(3) Ising 模型的参数设置也会影响退火的成功率. 当模型的局部场系数 h 和耦合项系数 J 范围过大时，退火的成功率会受到很大影响.

通用量子计算机的硬件发展缓慢，且与量子算法适配度不高. D-Wave 量子计算机与量子退火算法紧密耦合，不存在线路深度、纠错码和收敛性不明确等问题[30]，理论优势明显. 随着 D-Wave 量子比特规模在稳步发展，通过 50 比特 RSA 整数分解的探索，期待量子退火的整数分解实验可以扩展至 64 比特以上. 本文分解 50 比特整数使用了 10 变量，嵌入到量子计算机后使用 16 个物理量子比特. D-Wave Advantage 拥有超过 5000 个物理量子比特，在量子比特数量上有极大富余. 因此，在未来更大规模问题时，D-Wave 有望发挥量子隧穿优势对更大规模 RSA 做出进一步探索攻击.

4　总结与展望

本文使用分栏二进制乘法表算法建立素数分解的目标函数，通过乘法表的高位优化减少了量子比特数量，使用新的降维模型缩小了局部场系数 h 和耦合项系数 J 的范围，极大提高退火成功率. 使用 D-Wave Advantage 量子计算机成功分解了 22 位比特整数 2269753. 与 Lockheed Martin 公司和普渡大学相比，分解的整数范围极大提升，局部场系数 h 和耦合项系数 J 的范围明显缩小. 系数范围的缩小可以使量子比特间的耦合强度降低，量子翻转更统一，可以显著提高退火成功率.

本文使用量子算法融合经典算法的技术路线，发挥量子隧穿效应获得了比 Babai 算法更优的 CVP 解. 将光滑对的搜索范围缩小到目标向量附近，提升搜索效率，表现出了量子加速效能. D-Wave 量子退火的优势体现在指数级大规模问题求解时能跳出局部亚优解.

目前使用真实量子计算机的量子攻击方法不多，并且量子退火是一种极其稳定的无监督机器学习算法，在 RSA 密码攻击方面优于目前各类量子算法，具备 D-Wave 量子计算机硬件发展迅速的优势，也不存在 NISQ 量子计算机 VQA 算法的致命缺陷贫瘠高原问题(导致算法不收敛，有些整数不能分解，不能扩展到大规模攻击). 在使用量子退火融合经典方法技术路线进行攻击时，需要关注量子算法是否具备以下三个要点：算法与量子计算机硬件适配度、收敛性、理论优势是否丰富. 由于量子退火算法不受通用量子计算机的量子门电路等限制，量子加速效果明确[28]，收敛性明确[30].

通过两类技术路线，我们验证了 D-Wave 量子退火对 RSA 的现实攻击能力. 从目前 RSA 的实际攻击效果来看，量子退火大幅度超过其它各类量子计算. 2022 年郭光灿院士[16]指导的本源量子撰文认为，退火机能够分解的数字比通用机大几十个量级. 与一些量子算法比，量子退火没有其他像 QAOA 等算法会出现的贫瘠高原问题，有相当高的稳定性. 量子退火尤其擅长解决组合优化问题和指数级解空间问题. 很多密码问题都可以转化为组合优化问题或指数级解空间求解问题并使用量子退火求解. 因此量子退火可以推广到其他公钥密码以及对称密码的安全性评估.

致 谢 感谢郑建华院士、罗兰老师、靖青老师对本文算法设计及实验分析的指导!

参 考 文 献

[1] Yin H, Fu Y, Li C, et al. Experimental quantum secure network with digital signatures and encryption. National Science Review, 2022, 10(4): 1-11

[2] A Preview of Bristlecone, Google's New Quantum Processor. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html, 2018, 3, 5

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

[4] 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

[5] Morvan A, Villalonga B, Mi X, et al. Phase transition in random circuit sampling. arXiv preprint arXiv:2304.11119, 2023

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

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

[8] Boixo S, Rønnow T, Isakov S, et al. Evidence for quantum annealing with more than one hundred qubits. Nature Physics, 2014, 10(3): 218-224

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

[10] Jiang S, Britt K, McCaskey A, et al. Quantum annealing for prime factorization. Scientific Reports, 2018, 8(1): 17667-1-9

[11] 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): 5-12

[12] Warren R. Factoring on a quantum annealing computer. Quantum Information & Computation, 2019, 19(3&4): 252-261

[13] Hegade N, Paul K, Albarrán-Arriagada F, et al. Digitized adiabatic quantum factorization. Physical Review A, 2021, 104(5): L050403

[14] Ji X, Wang B, Hu F, et al. New advanced computing architecture for cryptography design and analysis by D-Wave quantum annealer. Tsinghua Science and Technology, 2022, 27(4): 751-759

[15] Wang C, Hu Q, Yao H, et al. Deciphering a million-plus RSA integer with ultralow local field coefficient h and coupling coefficient J of the Ising model by D-Wave 2000Q. Tsinghua Science and Technology, 2023, 29(3): 874-882

[16] Cui Fu-Xin, Wang Bei, Liu Yan, et al. Research status and prospect of quantum attacks in public-key cryptography. Cyber Security and Data Governance, 2022, 41(3): 3-12(in Chinese)
(崔富鑫, 王辈, 刘焱等. 公钥密码的量子攻击研究现状与展望. 网络安全与数据治理, 2022, 41(3): 3-12)

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

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

[19] 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): 030301(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): 030301)

[20] Wang Chao, Wang Yun-Jiang, Hu Feng. Shaping the future of commercial quantum computer and the challenge for information security. Chinese Journal of Network and Information Security, 2016, 2(3): 17-27(in Chinese)
(王潮, 王云江, 胡风. 量子计算机的商业化进展及对信息安全的挑战. 网络与信息安全学报, 2016, 2(3): 17-27)

[21] 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)

[22] Wang Chao, Cao Lin, Jia Hui-Hui, et al. ECC fault attack algorithm based on Grover's quantum search algorithm with 0.1π phase rotation. Journal on Communications, 2017, 38(8): 1-8(in Chinese)
(王潮, 曹琳, 贾徽徽等. 基于 0.1π 旋转相位 Grover 算法的 ECC 电压毛刺攻击算法. 通信学报, 2017, 38(8): 1-8)

[23] 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

[24] Schnorr C. Factoring integers by CVP algorithms. Number Theory and Cryptography, 2013, 8260: 73-93

[25] Lenstra A, Lenstra H, Lovász L. Factoring polynomiais with rational coefficients. Mathematische Annalen, 1982, 261: 515-534

[26] Babai L. On Lovasz' lattice reduction and the nearest lattice point problem. Combinatorica, 1986, 6: 1-13

[27] Schnorr C. Fast Factoring Integers by SVP Algorithms, corrected. Cryptology ePrint Archive, 2021

[28] Somma R, Nagaj D, Kieferová M. Quantum speedup by quantum annealing. Physical Review Letters, 2013, 109(5): 050501

[29] Zhang W, Pasalic E. Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties. IEEE Transactions on Information Theory, 2014, 60(10): 6681-6695

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

附　录.

比特数	分解数	逻辑量子比特	物理量子比特
4	15=3×5	2	2
5	21=3×7	2	2
6	35=5×7	2	2
7	65=5×13	2	2
8	143=11×13	3	3
9	403=13×31	3	3
10	899=29×31	3	3
11	1711=29×59	3	3
12	2623=43×61	3	3
13	4387=41×107	4	4
14	8881=83×107	4	4
15	19303=97×199	4	4
16	34427=173×199	4	4
17	67297=173×389	4	4
18	155989=389×401	4	4
19	331327=421×787	4	4
20	758603=743×1021	5	6
21	1568491=787×1993	5	6
22	2515171=1601×1571	5	6
23	5200733=1733×3001	5	6
24	10226243=3167×3229	5	6
25	17178901=2129×8069	6	8
26	36857467=5189×7103	6	8
27	81206053=5471×14843	6	8
28	170173931=10513×16187	6	8
29	326365969=15313×21313	6	8
30	815870819=26573×30703	6	8
31	1137188849=19207×59207	7	10
32	3508134653=56167×62459	7	10
33	4870201901=47143×103307	7	10
34	14230331263=117071×121553	7	10
35	22142487581=110273×200797	7	10
36	22142487581=110273×200797	7	10
37	75377310251=163981×459671	8	12
38	189458359247=378137×501031	8	12
39	398801616181=495527×804803	8	12
40	1074761139337=1028329×1045153	8	12
41	1184058275783=627017×1888399	8	12
42	3874666963561=1944457×1992673	8	12
43	5679969913721=1449379×3918899	8	12
44	12452672374231=3284999×3790769	9	14
45	20126970492877=4101011×4907807	9	14
46	43692318951517=5659651×7719967	9	14
47	87507538852607=5619937×15570911	9	14
48	195920816978287=13631221×1437294	9	14
49	289931961697979=16180159×17918981	10	16
50	845546611823483=40052303×21111061	10	16

WANG Chao, Ph. D., professor. His research interests include AI, cyberspace security, quantum computing cryptography.

WANG Qi-Di, M. S. candidate. His 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.

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

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

Background

This topic is a study of cryptographic attacks on quantum computing. Many scholars have studied various aspects of traditional cryptography and quantum cryptography. There are also many established research methods. However, quantum computers are still in their infancy, and many quantum algorithms still have some problems. This topic aims to find a robust quantum algorithm. To make some contributions to future cryptography research.

In this paper, a brief introduction and comparison of various types of quantum algorithms are made. Two technical routes of quantum algorithms to attack public key ciphers are proposed, and the largest scale RSA public key cipher attack by quantum algorithms has been implemented so far. The idea of this paper is to optimize the mathematical problems in the design of cryptographic functions and cryptographic component attacks by using the quantum tunneling effect of quantum annealing and to transform such mathematical problems into combinatorial optimization problems and exponential solution space search problems. The idea can be extended to other public key ciphers and symmetric ciphers.