

第一寄存器小 Qubit 量子计算攻击 RSA 研究

王宝楠¹, 陈宇航¹, 尹宝¹, 胡风¹, 张焕国², 王潮¹

(1. 上海大学通信与信息工程学院特种光纤与光接入网省部共建教育部重点实验室, 上海 200072;
2. 武汉大学空天信息安全与可信计算教育部重点实验室, 湖北 武汉 430072)

摘要: 提出了针对 RSA 的小 Qubit 量子攻击算法设计, 量子攻击的第一量子寄存器所需的 Qubit 数目由原先至少 $2L$ 降低到 $L1$, 总体空间复杂度记为 $(L1, L)$, 其中 $2L1 \geq r$, r 为分解所得周期。由于第一寄存器量子比特数的减少, 降低了算法复杂度和成功率, 且改进原算法中模幂计算, 提升运算速率。改进攻击算法的量子电路的时间复杂度为 $T=O(2L2)$ 。在时间复杂度和空间复杂度上都有明显的进步。改进算法的成功率降低了, 但实际成功求解时间, 即每次分解时间/成功率, 依然低于 Shor 算法目前的主要改进算法。完成了仿真模拟实验, 分别用 11、10、9 Qubit 成功分解 119 的量子电路。

关键词: Shor 算法; RSA 算法; 量子电路; 小比特; 攻击

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00206

Research of the small Qubit quantum computing attack to the RSA public key cryptography

WANG Bao-nan¹, CHEN Yu-hang¹, YIN Bao¹, HU Feng¹, ZHANG Huan-guo², WANG Chao¹

(1. Key Laboratory of Special Fiber Optics and Optical Access Networks, School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China;

2. Key Laboratory of Aerospace Information Security and Trusted Computing, Wuhan University, Wuhan 430072, China)

Abstract: The small Qubit quantum algorithm attack to RSA was proposed, the need Qubit of the first quantum register from $2L$ to $L1$, it can be reduced to 2 Qubit, the overall space complexity denoted $(L1, L)$, where $2L1 \geq r$, r is the period of decomposed. Because of the reduce of the first quantum register, it reduces the algorithm's complexity and success rates, and use the binary look-up table method to compute the modular exponentiation, it enhances the computing speed. The improved algorithm's quantum circuit complexity is $T=O(2L2)$. It have a significant improvement on the time complexity and space complexity. Although the success rate is reduced, the overall success solution time is still lower than the Shor algorithm and the current major improvements Shor algorithm. Completed a simulation experiment. Respectively use the 11、10、9 Qubit decomposing the quantum circuit 119. The new algorithm explore the reality of using a universal quantum computer device to decipher the public key cryptography.

Key words: Shor algorithm, RSA algorithm, quantum circuits, small qubits, attack

收稿日期: 2017-08-19; 修回日期: 2017-09-27。通信作者: 王潮, wangchao@staff.shu.edu.cn

基金项目: 国家自然科学基金重点资助项目 (No.61332019); 国家自然科学基金资助项目 (No.61572304, No.61272096, No.60970006)

Foundation Items: The Key Program of National Natural Science Foundation of China (No.61332019), The National Natural Science Foundation of China (No.61572304, No.61272096, No.60970006)

1 引言

《Nature》^[1]在调查欧洲、美国多个量子中心后,判断破译现有的 1 024 bit RSA 密码所需要的千位 Qubit 以上的通用量子计算机,在未来 5~10 年内仍难实现。

根据《Nature》^[1],Hanson 和 Vandersypen 等领导的荷兰量子研究中心 (QuTech Centre) 的目标是近期研究 17 Qubit。

瑞士苏黎世联邦技术研究所的 Matthias Troyer^[1]认为目前的通用量子计算机缺乏杀手级应用,已知的 2 个应用 (密码破译和数据库搜索) 都不成功。Matthias Troyer 还认为,百位 Qubit 不容易实现或者无法很经济地实现。Matthias Troyer 对目前量子计算机的情况非常熟悉,还参加了南加州大学的加拿大量子计算机测试。

事实上,根据《Nature》,目前已经实现的通用量子计算机最大规模为 9 Qubit,由加州大学圣巴巴拉分校 (UCSB) 的 John Martinis 团队实现,然而 John Martinis 认为通用量子计算机还在二战时期第一台电子计算机的程度。

尽管 John Martinis 团队已经在原理上验证了 Shor 计算攻击 RSA 的可行性,并在 2011 年成功用量子电路实现了量子傅里叶变换^[2],这是破译 RSA 的量子计算 Shor 算法的核心基础,2012 年,John Martinis 团队还成功完成攻击小规模 RSA 实验^[3],分解了 $15=3\times 5$ 。但是,John Martinis 团队不再继续从事通用量子计算机的研究,2014 年 9 月,John Martinis 整个团队全部搬入谷歌总部“建造能解决实际问题的量子计算机”——基于量子退火的专用量子计算机,其原理并不适合运用于公钥密码破译的 Shor 算法。

因此需要考虑在通用量子计算机器件条件限制的情况下,研究公钥密码 RSA 的小 Qubit 量子计算攻击方法,降低对通用量子计算机的器件要求^[4]。

本文改进了原始 Shor 算法,提出新的量子电路设计,降低了量子器件要求,探究性地提出了小规模 Qubit 实现 Shor 算法对公钥密码的攻击,并进行了仿真模拟。

本文介绍了 Shor 算法攻击 RSA 的国内外研

究现状,引出改进 Shor 量子算法对公钥密码的攻击;给出 Shor 算法分解实验。另外,本文分别给出 Shor 算法攻击 RSA 的量子电路攻击实验和改进 Shor 量子攻击算法实验及运行结果;并进行了实验分析;比较了目前主要的 Shor 改进算法,并对改进的 Shor 算法进行分析。

2 Shor 算法攻击 RSA 国内外研究现状

Shor 算法对 RSA 的攻击体现在 Shor 算法对 RSA 安全基础的大数 N 的分解,关于 Shor 算法对 N 分解的研究一直是国内外专家学者的研究热点。

1996 年,美国科学家 Juan Pablo Paz 在一个有干扰和损耗的量子电路上展示分解了 15,理论上需要 27 Qubit 才能成功分解。同时他更是指出对于大数 N ,所需要的量子比特数是 $n=5L+7$ (其中 L 为不小于 $\log_2 N$ 的最小正整数)。这项工作的研究成果给实际操作中实现 Shor 量子算法提供了很好的借鉴。

2001 年,斯坦福大学和美国 IBM 公司合作,利用核磁共振技术演示了 Shor 算法对整数 15 进行分解的实验过程,但该实验不能显示其量子属性,也无法扩展到更多的比特情况,限制了进一步的研究。

2004 年,美国赫尔辛基理工大学的 Vartiainen^[5]利用约瑟夫森电荷构成的量子比特实现了 Shor 算法。他把 Shor 算法的量子电路分成了一系列 2 Qubit 和 3 Qubit 的量子门,不仅加速了 Shor 算法的实现,而且在此基础上通过数值优化的方法成功完成对 $N=21$ 分解的物理实现。但该实验要求很高的物理性,即必须在特定的物理条件下才能实现。

2007 年,法国理论物理研究实验室在研究 Shor 算法的缺陷^[8] (由量子比特间残余耦合所造成) 所产生的影响时,通过编写 Quantware 库并且调用该库,用 30 个量子比特模拟实现了 $N=943$ 的分解。该方法虽然很好理解,但是 Quantware 库所用的限制性很多。2007 年,中国科学院公布,中国科学技术大学潘建伟教授和杨涛教授等^[9]与英国牛津大学的研究人员合作,在国际上首次利用光量子计算机实现了 Shor 量子分解

算法, 研究发表在 2007 年 1 月的物理评论快报上, 并在该量子计算上成功操控 4 个光子量子比特构造一个简单的线性光网络, 实现 $N=15$ 的分解。

2010 年, 英国布里斯托大学电气和电子工程物理实验室和量子光学中心的 Thompson 等^[10]介绍了基本的 Shor 因式分解量子算法实现过程, 主要是在由 6 个 H 门和 2 个可控的相位门组成的波导电路中建立一个可以实现 Shor 量子分解算法的电路, 并且成功地用 Shor 算法分解 $N=15$ 。

2010 年, 解放军信息工程大学通过改进量子傅里叶变换加速实现 Shor 算法对 N 的分解^[11], 但该算法中改进的量子傅里叶变换是以串行代替并行加快速度的。该算法的空间复杂度记为 $(4, L)$, 时间复杂度 $T=O(L^3)$ 。

2012 年, 美国加州大学圣巴巴拉分校的 John Martinis^[3], 在实现量子傅里叶变换电路基础上, 完成了 $15=3 \times 5$ 的素数分解实验, 原理上验证了 Shor 计算攻击 RSA 的可行性。

上述研究和最近的一些研究^[12,13]都是 Shor 算法分解 N 研究的代表, 但基本上都需要在量子计算机器件^[6,7]很高的要求下, 包括需要千位量子比特的量子计算机和高精度的纠缠能力等。

3 改进 Shor 算法

3.1 改进 Shor 算法介绍

对大数 N ($N>0$) 的素因子分解, 也就是对大数 N 和整数 x ($x<N$) 求出满足同余式 $xr=1 \bmod N$ 的阶 r 。

改进 Shor 算法步骤如下。

Step1 准备具有 $L1$ 量子比特的第一寄存器和 L 量子比特的第二寄存器的态矢量 $|\varphi_1\rangle = |0\rangle^{\otimes L1} |1\rangle$ 。其中, $L=[\text{Log}[2,N]]$, $2^{L1} \geq r$, r 为周期。

Step2 对第一寄存器实行 $L1$ 次 Hadamard 变换得到 $|0\rangle$ 到 $|q-1\rangle$ 的 $q=2^{L1}-1$ 个态的叠加, 可给出 $|\varphi_2\rangle = \sum_{a=0}^{q-1} |a\rangle |1\rangle$ 。

Step3 将 $U_{x,a}$ 算符应用到寄存器, $|\varphi_3\rangle = U_{x,a} \sum_{a=0}^{q-1} |a\rangle |1\rangle = \sum_{a=0}^{q-1} |a\rangle |x^a \bmod N\rangle$ 。

Step4 利用二进制查表法计算 $x^a \bmod N$ 的

值。如下^[14]。

① 计算和存储所有的 $x^{a_k a_{k-1} \dots a_2 a_1} \bmod N$, 其中 $a_k=1$, $a_i \in \{0,1\}, i=1,2,\dots,k-1$ 。

② 令 $i=t-k$, $m = x^{a_i a_{i-1} \dots a_{t-k+1}}$ 且该值已经存储。

③ 当 $i \geq 0$ 时, 执行④~⑩。

④ 如果 $a_i=1$, 则执行⑤~⑨。

⑤ 如果 $i \geq k$, 则执行⑥~⑧。

⑥ 把该位开始的 k 个二进制数作为一个整体进行计算, 进行连续 k 次平方。

⑦ 对⑥中的结果与已经记忆的对应的 $x^{a_k a_{k-1} \dots a_2 a_1} \bmod N$ 值相乘。

⑧ 令 $i=i-k$, 减少一个分组的长度。

⑨ 如果 $i < k$, 则把该位开始的 k 个二进制数作为一个整体, 即令 $m=m \times m \times x \bmod N$, 且 $i=i-1$ 。

⑩ 如果 $a_i=0$, 则直接计算该位开始的 k 个二进制的平方取模, 且 $i=i-1$, 最后返回 m 值。

Step5 进行 $x^a \bmod N$ 的阶数搜索过程。

Step6 对第一个量子寄存器进行 QFT 逆变换, 并观测概率。

Step7 由周期性求得阶数 r 。

Step8 由阶数 r 求得 2 个 N 的分解数。

3.1.1 原始 Shor 算法分解 $N=119$ 量子电路

图 1 是理论上 Shor 算法的完整实现, 第一量子寄存器需要的量子比特数 $n1 = 2 \lceil \lg N \rceil = 14$, 第二量子寄存器需要的量子比特数 $n2 = \lceil \lg N \rceil = 7$ 。

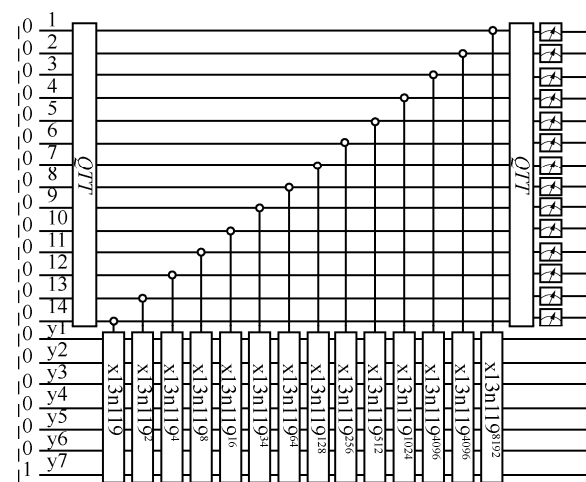


图 1 原始 Shor 算法分解 $N=119$ 的量子电路

3.1.2 改进 Shor 量子算法分解 $N=119$ 量子电路

基于改进 Shor 量子算法实现对 RSA 的攻击量子电路原理如图 2 所示。

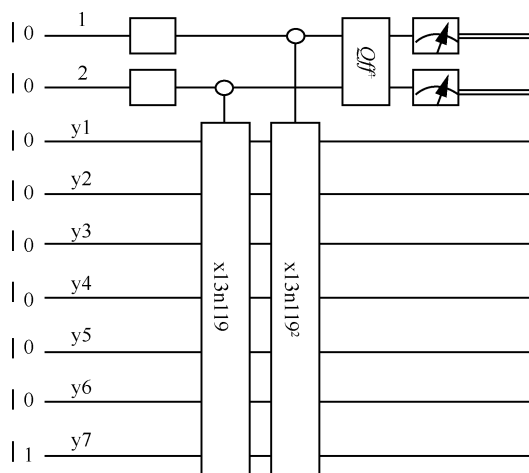


图2 改进的Shor小比特攻击算法分解 $N=119$ 的量子电路

对比图1和图2,改进的地方在于把第一量子寄存器的量子比特数1~14进行了减少,由原来的14 Qubit修改成了1~2的2个量子比特,与理论上相比少用了12个量子比特,这大大减少了对量子计算机的器件要求。

3.2 改进Shor量子算法分析

改进Shor算法相比原始Shor算法分析如下。

参考Shor算法及相关文献[15]对Shor算法分解大数的理论分析,本文设计的量子电路主要包括3个部分:一是用一系列的H变换替换傅里叶变换;二是控制模幂变换,并引入二进制查表法计算模幂算法;三是量子傅里叶变换。

该改进Shor量子算法主要是量子比特数的减少,一般情况下空间复杂度和时间复杂度与成功率呈相反的关系,即成功率的提升是以复杂度的提升为代价的。由于第一量子寄存器比特数的减少,所需通过H变换的次数也相应地减少,引起了模幂中模乘次数的减少,促进了整个算法运行时间的减少,且并不影响后续的操作。第一量子寄存器执行的是模幂操作的控制,是用于控制模幂运算的模乘次数和量子傅里叶变换,缩小了量子比特数,使所能进行的模幂运算次数也变少,并引发了后面操作次数的减少,在一定程度上降低了该Shor算法攻击的成功率,但提高了成功求解速度。而引入二进制查表法的目的是进一步减少模乘的次数,该算法虽然增加了一点空间,但并不影响整体算法的空间复杂度,且引入该算法的主要目的是该算法能大幅度减少模幂中乘法的次数,使模幂的计算速度进一步提高。

Shor原始算法量子电路空间复杂度需要至少 $S=(2L, L)$, $L=\log_2 N$ Qubit(第一量子寄存器需要 $2L$ Qubit,第二量子寄存器需要 L Qubit, S 表示空间复杂度)。改进Shor算法量子电路空间复杂度需要 $S=(L1, L)$ (第一量子寄存器需要 $L1$ Qubit,第二量子寄存器需要 L Qubit)。其中, L Qubit即进行模幂运算至少要有量子比特数(保存模幂运算预运算的值)。 $L1$ Qubit即量子傅里叶变换需要的量子比特数。例如,基于改进Shor算法分解 N 的步骤分析,设计的量子电路的量子比特数对于分解119的量子电路而言,从原来至少需要(14, 7)量子比特降为仅用(2, 7)量子比特。Shor原始算法量子电路计算复杂度,即时间复杂度为 $T=O(L3)$,改进Shor算法量子电路复杂度为 $T=O(L2)$ 。

与Shor算法相比,降低了至少 L 规模的比特数,即空间复杂度降低了 $O(L)$ 规模。与目前主要的Shor改进算法相比,改进Shor算法的比特数基本上与其他相近或更少,但是在成功求解时间上更小,且做法上更简单,更易于理解。

由于现阶段的通用量子计算机难以满足破译RSA公钥密码的实际需求,所以降低了成功率而使所需空间复杂度变低,能在一定程度内解决量子计算机器件的难题,这样做对目前更好地解决更大数的RSA破译有深远的影响,所以值得推广。正是应用这一特点,提出了改进Shor量子攻击方法。

3.3 改进Shor算法分解 $N=119$ 量子电路的实验

本实验在配置为Intel Core2 Duo CPU T6670 2.20 GHz、内存2 G的联想笔记本上,在数学工具Mathematics9.0软件下调用José Luis Gómez-Muñoz和Francisco Delgado编写的量子程序包进行的量子电路上进行仿真。基于Shor算法实现步骤的分析,实验成功分解了15、21、35、65、119、123、205等数,下面讨论Shor算法量子电路^[15]实现分解 $N=119$ 的实验。

将改进Shor量子攻击算法与原Shor算法进行对比实验,比较其攻击结果。选用Shor算法分解 $N=119$ 的实验,选择的随机数 $x=13$,在Mathematics 9.0软件下进行仿真实验。

运行如图2所示的量子电路,求解所得周期,结果如图3所示。

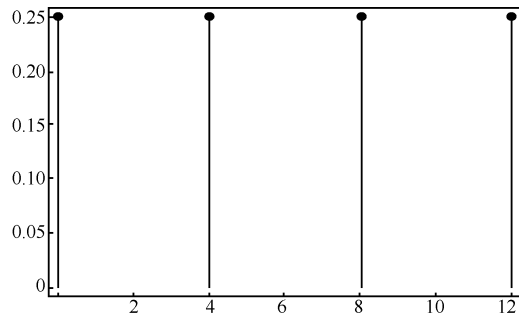


图 3 量子傅里叶变换后第一寄存器 $|c\rangle$ 的概率
(第二寄存器的 $s=0,1,\cdots,r-1$)

从图 3 可以看出, 对每个 s 值, 概率接近于 $P \sim \frac{1}{r}$ 的满足 C 的 K 值为 $k=0,1,2,3,\cdots,15$ 。如果取 $k=1$ 或 $k=3$, 则从 $\frac{k}{q}$ 的连分数展开均搜索到阶 $r=4$ 。

由 $x^{\frac{r}{2}} \pm 1 = 13^2 \pm 1 = 170, 168$ 得

$$\gcd(x^{\frac{r}{2}} + 1, 119) = \gcd(170, 119) = 17$$

$$\gcd(x^{\frac{r}{2}} - 1, 119) = \gcd(168, 119) = 7$$

由此得到 $N=119$, 可以分解为 $119=17 \times 7$ 。

这里要说明的是, 在判断周期 r 的时候, 其实只要观察图 3 的波峰即可确定。在判断时, 直接观察波峰数就是周期数的依据是: 结合最后测量的概率公式, 在观察 $\frac{s}{r} = \frac{c}{q}$ 的概率分布时, $s=1,\cdots,r-1, c$ 的取值为 k , 当出现一个 k 满足 $\frac{s}{r} = \frac{c}{q}$ 时, 离散概率就出现一个波峰。

$$P_c = \frac{1}{r} \frac{1}{q^2} \left| \sum_{a=0}^{2^n-1} \exp \exp \left(2\pi i \left(\phi_s - \frac{c}{q} \right) a \right) \right|^2 \quad (1)$$

由式(1)可以看出, 只有当 $\frac{s}{r} = \frac{c}{q}$ 时, 才会有

接近于 $\frac{1}{r}$ 的概率, 即 C 的概率分布出现波峰值。

当不满足上述条件时, q 越大越精确, 直至找出所有的 k , 刚好满足 $\frac{s}{r} = \frac{c}{q}$ 。因为 s 共有 r 个取值, 所以一定存在 r 个波峰, 这样可以判断波峰数一定就是周期数。

本次实验的其他结果统计如表 1~表 4 所示。

表 1 分解相同数、相同比特数, 不同随机数下的实验结果

实验次数	分解数	需要的量子比特		随机数 x	周期	总运行时间/s	分解周期时间/s	是否成功
		第一个量子寄存器	第二个量子寄存器					
10	119	4	7	7	16	1 821	1 442	失败
10	119	4	7	11	16	1 670	1 350	失败
10	119	4	7	13	4	395	153	成功
10	119	4	7	53	16	1 790	1 413	失败
10	119	4	7	83	8	614	381	成功
10	119	4	7	97	16	1 881	1 451	成功
10	119	4	7	113	16	1 886	1 458	成功

表 2 分解相同数、相同随机数 13, 不同比特数下的实验结果

实验次数	分解数	需要的量子比特		随机数 x	周期	总运行时间/s	分解周期时间/s	是否成功
		第一个量子寄存器	第二个量子寄存器					
5	119	5	7	13	未知	未知	未知	失败
10	119	4	7	13	4	395	153	成功
10	119	3	7	13	4	253	24	成功
10	119	2	7	13	4	250	7	成功
10	119	1	7	13	2	235	0.6	失败

表 3 分解相同数，相同随机数 83，不同比特数下的实验结果

实验次数	分解数	需要的量子比特		随机数 x	周期	总运行时间/s	分解周期时间/s	是否成功
		第一个量子寄存器	第二个量子寄存器					
5	119	5	7	83	未知	未知	未知	失败
10	119	4	7	83	8	614	381	成功
10	119	3	7	83	8	324	114	成功
10	119	2	7	83	4	252	13	失败
10	119	1	7	83	2	231	0.65	失败

表 4 分解相同数、相同随机数 97，不同比特数下的实验结果

实验次数	分解数	需要的量子比特		随机数 x	周期	总运行时间/s	分解周期时间/s	是否成功
		第一个量子寄存器	第二个量子寄存器					
5	119	5	7	97	未知	未知	未知	失败
10	119	4	7	97	16	1 881	1 451	成功
10	119	3	7	97	8	325	98	失败
10	119	2	7	97	4	248	11	失败
10	119	1	7	97	2	240	0.67	失败

观察表 1 可发现，不同随机数会影响分解运行时间。

由表 2~表 4 可以发现，量子比特数的多少对运行时间是有影响的，且随机数的选择对量子比特数的多少也是有影响的。

4 实验分析

4.1 成功率分析

分解 119，在设置不同量子比特数、不同随机数下，实验成功次数的统计如表 5 所示。

观察表 5 可以发现，当量子比特数减少时，

对于分解的成功率是有影响的，且可以定性地反映出当量子比特数减少时，成功率是下降的。

Shor 原始算法给出，选定一个随机数求得周期 r 的成功率为 $\frac{\phi(r)}{3r}$ ，其中 r 是阶也可以说是周期，欧拉函数 $\phi(N) = (p-1)(q-1)$ ， p 和 q 是 N 的 2 个因子。因为数论上有 $\frac{\phi(r)}{3r} > \frac{k}{\log \log r}$ ， k 是一个小于 1 的常数。所以，Shor 认为如果重复做 $O(\log \log r)$ 规模次，其成功率一定可以增加。由

表 5 分解 119，第一量子寄存器量子比特数、随机数不同情况下的周期

第一个量子寄存器的数量	13	29	41	43	47	83	97	113	总成功数目
	周期								
$L=4$	4	16	16	8	16	8	16	16	8 次
	成功	成功	成功	成功	成功	成功	成功	成功	
$L=3$	4	8	8	8	8	8	8	8	3 次
	成功	失败	失败	成功	失败	成功	失败	失败	
$L=2$	4	4	4	4	4	8	4	4	1 次
	成功	失败	失败	失败	失败	失败	失败	失败	

于本文的改进 Shor 算法与 Shor 算法本质上是一样的，所以成功求得周期 r 的概率也是 $\frac{\phi(r)}{3r}$ 。如果知道周期 r ，则可成功分解的概率至少是 $\frac{3}{4}$ ，即 Shor 算法成功分解的概率至少是 $\frac{\phi(r)}{3r} \frac{3}{4}$ 。结合实验数据，给出成功率公式为

$$p = \begin{cases} 0, & 2^L < r \\ \frac{1}{\phi(N)} \frac{\phi(r)}{3r} \frac{3}{4}, & 2^L \geq r \end{cases} \quad (2)$$

其中， $\phi(N)$ 、 $\phi(r)$ 都是关于 N 和 r 的欧拉函数， N 是要分解的数， r 是求的阶，即周期。所以在分解 119 的时候，当 $L=2$ ， $r=4$ 时，成功率为

$$p = \frac{1}{96} \frac{1}{6} \frac{3}{4} = 1.3\% \quad (3)$$

1997 年，Eicher J 和 Opoku Y 的研究给出了一个在多项式时间内以 $1/480 \approx 0.002$ 的成功率攻击椭圆曲线离散对数问题的量子计算算法，证明低成功率也可以成功攻击。而这里分解 119，成功率为 0.001 3，所以也满足条件。

4.2 复杂度分析

一个量子电路的复杂度分为空间复杂度和时间复杂度，具体反映在 3 个方面：量子电路比特数^[16]、量子电路需要的基本量子门规模（也称量子电路尺寸）和量子电路深度。量子电路尺寸和量子电路深度对应量子电路所需要的时间规模，即时间复杂度，量子比特数目即空间复杂度。电路尺寸是指一个量子电路中所有基本量子门电路的总数，基本量子门指的是 H 门、CNOT 门、控制-旋转门、Toffli 门等。一个量子电路的深度是指该量子电路所有量子门的深度之和，直观上讲就是这个量子电路有几层，类似于程序的循环。总之，在计算量子电路复杂度时，一要计算该量子电路需要的量子比特数，即空间复杂度；二是

计算量子电路所需要的基本量子门规模和量子电路的深度，即量子电路的时间复杂度。

由于算法本质上还是 Shor 算法的原型，下面给出改进 Shor 算法的复杂度。因为 Shor 算法主要由量子傅里叶变换和模幂运算组成，故 Shor 算法的复杂度也是指这两部分的复杂度，如表 6 所示。

表 6 Shor 算法复杂度		
操作	时间复杂度	空间复杂度
模幂	$O(L^3)$	$O(L)$
量子傅里叶变换	$O(L^2)$	$O(L+2)$

表 6 中的 $L=\log 2N$ ， N 为要分解的数。

引入二进制查表法加快了模幂算法的运算速度。在改进的 Shor 算法引入该算法后，其空间复杂度和时间复杂度依然为 $(L1, L)$ 和 $T=O(2L2)$ 。

4.3 算法比较

4.3.1 与原始 Shor 攻击算法比较

通过分解 119 实验，总结改进 Shor 量子算法属性，并与原始 Shor 算法进行比较，如表 7 所示。其中， $L1$ 为第一量子寄存器量子比特数， $L=\log 2N$ 。

可以知道，改进 Shor 算法成功求解时间相对于 Shor 原始算法成功求解时间可简化为 $\phi(N)O(L^2)$ ，Shor 原始算法成功求解时间可简化为 $O(L^3)$ ， $\phi(N)O(L^2) < O(L^3)$ ，所以，改进 Shor 算法成功求解时间小于原始算法，得到了一定的提升。

虽然降低了成功率，但也成功降低了复杂度，在分解 119 的时候，成功地将所需空间复杂度从 $S=(2L, L)$ 降低为 $S=(2, L)$ 。这对于现阶段还没有通用的大量量子比特计算机来说具有深刻的意义，复杂度降低，让其可以在更少量子比特数的量子计算机上运行，能很好地解决现阶段量子计算机

表 7 改进 Shor 量子算法与原始 Shor 算法的比较

攻击方法	时间复杂度	第一个寄存器的比特	第二个寄存器的比特	成功率	成功解决时间
Shor 算法	$O(L^3)$	$2L$	L	$\frac{\phi(r)}{3r} \frac{3}{4}$	$\frac{O(L^3)}{\frac{\phi(r)}{4r}}$
改进的 Shor 算法	$O(L^2)$	$L1$	L	$p = \begin{cases} 0, & 2^L < r \\ \frac{1}{\phi(N)} \frac{\phi(r)}{3r} \frac{3}{4}, & 2^L \geq r \end{cases}$	$\frac{O(N)O(L^2)}{\frac{\phi(r)}{4r}}$

器件要求高的难题。

4.3.2 与目前主要改进 Shor 算法比较

2008 年,英国伦敦帝国学院布莱克特实验室的 Parker S 等^[17]给出了一个单一的纯量子比特与 $\log 2N$ 量子比特在任意混合态下的集合来有效实现 Shor 因式分解的算法。该算法大大减少了所需的量子比特数。

2010 年,解放军信息工程大学^[11]提出了 2 个新的改进 Shor 算法:具有高概率的整数分解量子计算算法和 Shor 整数分解量子算法的加速实现算法。

具有高概率的整数分解量子计算算法指出需要 3 个 L bit 的量子寄存器实现(该量子电路需要 4 次量子傅里叶变换和 1 次模幂运算)。

Shor 整数分解量子算法的加速实现算法指出需要 $S=(4, L)$ 量子比特(每个量子傅里叶变换需要 2 个量子比特,第一量子寄存器对应量子傅里叶变换需要 4 个量子比特,第二个量子寄存器需要 L Qubit)。

2013 年,美国的佐治亚大学^[18]用 8 Qubit 实现了 Shor 算法分解 51 和 85 的实验,它是对量子输入态的改进,该算法指出第一量子寄存器和第二量子寄存器都只需要 $S=(L_{\max}, L_{\max})$ Qubit,其中, $L_{\max}$ 接近为 $L=\lceil \lg N \rceil$ 。

由表 8 可知,改进 Shor 算法的复杂度比文

献[11]的 2 个改进 Shor 整数分解算法要小。Shor 整数分解量子算法的加速实现算法的第一量子寄存器量子比特数虽然比较小,但所需的时间复杂度还是 $O(L^3)$,相对于改进 Shor 算法,虽然减少了量子比特数,但是时间复杂度多了 L 倍,所以第一量子比特数降低为 4 没有很大的意义。而具有高概率的整数分解量子计算算法增加了量子比特数,且时间复杂度还是 $O(L^3)$ 。这里定义一个新的时间——成功求解时间,即每次求解时间与成功率之间的比值。可知,改进 Shor 算法成功求解时间相对于文献[11]的 2 个改进 Shor 整数分解算法的成功求解时间可简化为 $\phi(N)O(L^2)4$,文献[11]的 Shor 整数分解算法成功求解时间可简化为 $O(L^3)4$,文献[11]的具有高概率的 Shor 分解算法成功求解时间简化为 $O(L^3)\frac{\pi^2}{4}$ 。 L 越大,复杂度一个级别的差距不是与几个简单的自然数相乘就可以达到的,因此可知改进 Shor 算法的成功求解时间小于文献[11]的 2 个改进 Shor 整数分解算法的成功求解时间。

对比 Michael^[18]的改进 Shor 算法,改进 Shor 算法的复杂度比 Michael 的复杂度要小,且成功求解时间比改进 Shor 算法的成功求解时间大。对比 Parker 的改进 Shor 算法,改进 Shor 算法的时间复杂度较小,空间复杂度相近,最主要的是,

表 8 改进 Shor 量子算法与目前主要的改进 Shor 算法的比较

攻击方法	时间复杂度	第一个寄存器的比特	第二个寄存器的比特	成功率	成功解决时间
改进的 Shor 算法	$O(L^2)$	$L1$	L	$p = \begin{cases} 0, & 2^L < r \\ \frac{1}{\phi(N)} \frac{\phi(r)}{3r} \frac{3}{4}, & 2^L \geq r \end{cases}$	$\frac{O(N)O(L^2)}{\frac{\phi(r)}{4r}}$
整数分解算法	$O(L^3)$	4	L	$\frac{3\phi(r)}{\pi^2 r}$	$\frac{O(L^3)}{\frac{\phi(r)}{4r}}$
高概率的整数分解算法	$O(L^3)$	第一寄存器 L	第二寄存器 L	第三寄存器 L	$\frac{3\phi(r)}{\pi^2 r} < p < \frac{4\phi(r)}{\pi^2 r}$ $\frac{O(L^3)}{\frac{4\phi(r)}{\pi^2 r}}$
Michael 的改进 Shor 算法	$O(L^3)$	$L_{\max} \leq L$	$L_{\max} \leq L$	$\frac{x}{4^{2L_{\max}}}$	$\frac{O(L^3)}{\frac{x}{4^{2L_{\max}}}}$
Parker 的改进 Shor 算法	$O(L^3)$	1	L	$\frac{3(p-1)(q-1)}{N\pi^2 r}$	$\frac{O(L^3)}{\frac{3(p-1)(q-1)}{N\pi^2 r}}$

成功求解时间比 Parker 改进 Shor 算法的成功求解时间小。

5 结束语

本文的主要内容在于牺牲成功率来换取空间复杂性的降低,并在一定范围内提高了算法的运算速度,目的是为了在现有量子计算机器件允许的条件下开展研究,事实上并没有降低实际上的成功求解时间。

虽然牺牲了成功率,需要数百次运行才能得到成功的破译结果,但降低了对通用量子计算机的器件要求,提高了通用量子计算机破译公钥密码的现实性。改进的模幂计算也提高了 Shor 算法的运算速度。

由于实际成功求解时间等于每次分解时间除以成功率。本文提出的小 Qubit 改进 Shor 算法,实际成功求解时间还是低于 Shor 算法和目前主要的改进 Shor 算法。

就算法本身而言,虽然 Shor 算法能够实现把指数级的运算降为多项式时间内来完成^[19],但其需要的资源却随着量子比特数指数级增长。理论上讲,当量子比特数增加时,量子算法的能力应该是更强的,因为量子比特数增加了,并行计算的资源增加了,那么利用并行计算的量子算法自然增强了。但事实上,当量子比特数增加时,消耗资源的增长反而限制了量子算法的实现,使量子算法陷入一个无法挣脱最开始并行的境地。由此,本文也验证了在通用量子计算机还没有达到千位量子比特之前,想要利用更多量子比特并行能力的想法目前还不能实现。

这就是说,尽管大家都认为多量子比特可能比小量子比特实现量子算法解决实际问题更好,但是当器件进展尚无法控制千位量子比特时,不能达到预期的效果。所以本文改进算法的研究有助于充分提高现有小通用量子计算机破译公钥密码的可行性。

参考文献:

- [1] GIBNEY E. Physics: quantum computer quest: after a 30-years struggle to harness quantum weirdness for computing, physicists finally have their goal reach[J]. Nature News Feature, 2014:24-26.
- [2] MARIANTONI M, WANG H, YAMAMOTO T et al. Implementing the quantum von neumann architecture with superconducting circuits[J]. Science, 2011, 334(6052):61-5.

- [3] ERIK L, BAREDNS R., CHEN Y, et al. Computing prime factors with a josephson phase Qubit quantum processor[J]. Nature Physical, 2012, 8: 719-723
- [4] 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[J]. 网络与信息安全学报, 2016, 2(3):17-27.
WANG C, WANG Y J, HU F. Shaping the future of commercial quantum computer and the challenge for information security[J]. Chinese Journal of Network and Information Security, 2016, 2(3):17-27.
- [5] VARTIAINEN J J, NISKANEN A O, NAKAHARA M, et al. Implementing Shor's algorithm on Josephson charge Qubits[J]. Physical Review A, 2004, 70(1).
- [6] GLENDINNING I, ÖMER B. Parallelization of the QC-Lib quantum computer simulator library[J]. Lecture Notes in Computer Science, 2003, (3019):461-468.
- [7] DE-RAEDT K, MICHELSEN K, DE-RAEDT H ET AL. Massively parallel quantum computer simulator[J]. Computerphysicscommunications,2007,176:121-136.
- [8] GARCÍA-MATA I, FRAHM K M, SHEPELYANSKY D L. Effects of imperfections for Shor's factorization algorithm[J]. Physical Review A, 2007,(75).
- [9] YANG C, DANIEL L, BROWNE E, YANG T, et al. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic Qubits[J]. Physical Review Letter, 2007, (99).
- [10] THOMPSON M G, POLITI A, MATTHEWS J C F, et al. Integrated waveguide circuits for optical quantum computing[J]. Institution of Engineering and Technology, 2011, 5: 94-102
- [11] 付向群, 鲍皖苏. 具有高概率的量子计算算法研究[D]. 郑州: 解放军信息工程大学. 2011
FU X Q, BAO W S. Research on the quantum algorithm with high probability[D]. Zhengzhou: PLA Information Engineering University. 2011
- [12] NAGAICH S, GOSWAMI Y C. Shor's algorithm for quantum numbers using MATLAB simulator [C]//The fifth International Conference on Advanced Computing & Communication Technologies. 2015:165-168.
- [13] DAVID S W, CHARIES D H, LLOYD C L, et al. Simulations of shor's algorithm using matrix product states[J]. 2015.
- [14] 董付国, 厉玉蓉, 杜萍. 方幂模快速计算的二进制分组查表法[J]. 计算机工程与应用, 2009, 45(22): 71-73.
DONG F G, LI Y R, DU P. Fast calculation of modular exponentiation binary group look-up table method[J]. Computer Engineering and Applications, 2009, 45(22): 71-73.
- [15] 佐川弘幸, 吉田宣章, 著. 宋鹤山 译. 量子信息论[M]. 大连: 大连理工大学出版社, 2007.
SONG H S. Quantum information theory[M]. Dalian: Dalian University of Technology Press, 2007.
- [16] CHOI B S, METER R V. On the effect of quantum interaction distance on quantum addition circuits[J]. ACM Journal on Emerging Technologies in Computing Systems. 2010.
- [17] PARKER S, PLENIO M B. Efficient factorization with a single pure Qubit and log N mixed qubits[J]. Physical Review Letter, 2000, (85): 3048-3052
- [18] MICHAEL R.G, ZHOU Z Y. Factoring 51 and 85 with 8 Qubits[R]. Scientific Reports, 2013.
- [19] 孙国栋, 苏盛辉, 徐茂智. 求根问题的量子计算算法[J]. 北京工业大学学报, 2015, (41): 366-371.
SUN G D, SU S H, XU M Z. Quantum computing algorithms of find roots problems[J]. Journal of Beijing University of Technology, 2015, (41): 366-371.

作者简介:



王宝楠 (1989-), 女, 江苏淮安人, 上海大学博士生, 主要研究方向为信息安全、量子计算密码、社会网络。



胡风 (1991-), 男, 浙江温州人, 上海大学博士生, 主要研究方向为信息安全、量子计算密码、社会网络。



陈宇航 (1991-), 男, 浙江杭州人, 上海大学硕士生, 主要研究方向为量子计算与量子攻击密码分析。



张焕国 (1945-), 男, 河北元氏人, 武汉大学教授、博士生导师, 主要研究方向为信息安全、密码学和可信计算。



尹宝 (1991-), 男, 河南信阳人, 上海大学硕士生, 主要研究方向为量子计算与量子攻击密码分析。



王潮 (1971-), 男, 江苏镇江人, 博士, 上海大学教授, 主要研究方向为无线传感器网络、网络信息安全与椭圆曲线密码学、量子计算与量子攻击密码分析。