量子噪声对 Shor 算法的影响

黄天龙 吴永政† 倪明 汪士 叶永金

(中国电子科技集团公司第三十二研究所, 上海 201808)

(2023 年 9 月 3 日收到; 2023 年 12 月 10 日收到修改稿)

Shor 算法能够借助量子计算机以多项式级别复杂度解决大整数因式分解问题, 从而破解一系列安全性基于大整数因式分解的加密算法, 例如 Rivest-Shamir-Adleman 加密算法、Diffie-Hellman 密钥交换协议等. 由于量子测量结果是概率性的, 在运行量子线路时很容易受到噪声的干扰, 这将导致无法测量得到预期结果. 本文分别研究了不同通道的噪声对 Shor 算法的影响, 分别是去极化通道、状态制备与测量通道以及热退相干通道. 本文模拟在噪声环境中运行 Shor 算法并且给出了数值结果. 数值结果表明 Shor 算法成功分解整数的概率易受到噪声影响, 其中去极化通道中的噪声能够以指数形式影响 Shor 算法成功分解整数的概率, 其次是热退相干通道噪声, 最后是状态制备与测量通道噪声, 能够线性影响到 Shor 算法成功分解的概率. 本文能够为后续纠错、改进 Shor 算法以及确定工程实现 Shor 算法所需要的保真度等提供建设性意见.

关键词: 量子计算, 量子算法, 量子噪声, Shor 算法

PACS: 03.67.Ac, 03.67.Dd, 42.50.Lc **DOI:** 10.7498/aps.73.20231414

1 引 言

Shor[1] 于 1994 年提出用于解决大整数因式分解的量子算法, 该算法能够以多项式级的复杂度解决大整数因式分解及离散对数问题 [1,2]. 相较于经典因式分解算法, Shor 算法有指数级提升. 目前复杂度最低的传统大整数分解算法是数域筛法 [3–5], 它的复杂度为 $O\left\{\mathrm{e}^{[(\frac{64}{9})^{\frac{1}{3}}+O(1)](\log_2 n)^{\frac{1}{3}}(\log_2\log_2 n)^{\frac{2}{3}}}\right\}$. Kleinjung 等 [6] 借助上百台计算机花费两年时间使用数域筛法分解了一个 768 比特的 RSA (Rivest-Shamir-Adleman) 整数, 并且指出分解 2048 比特的 RSA 整数的开销是前者的百万倍. 而文献 [7] 指出理论上在一台拥有两千万个物理比特的量子计算机上运行 Shor 算法可以在 8 h 内完成 2048 比特的 RSA 整数的分解. 然而目前的量子计算机系统仍然处于萌芽状态, 我们处于带噪声的中等规模的量子计算机时代 (noise intermediate-scale quantum, NISQ)[8]. 中等规模指的是量子计算机所含有的量子比特个数范围为 50—100, 并且量子计算机运行量子算法时会受到噪声的影响. 噪声是搭建 NISQ 时代量子计算机的主要障碍 [9,10]. 噪声出现的主要原因在于硬件 (西门) 的失真以及量子计算机与环境之间会产生交互 (例如弛豫与退相位、电磁退相干、引力退相干等)[11–13], 这些噪声会对算法结果产生影响, 导致与预期结果产生偏差. 因此研究噪声对 Shor 算法的影响是十分重要的. 本文分别针对不同通道的噪声对 Shor 算法的影响进行深入研究, 通过数值分析任一通道中不同噪声大小与 Shor 算法分解整数成功率的关系 (Shor 算法成功率定义见 2.2 节).

Shor 算法中的量子线路十分复杂, 因此大量关于优化线路的文献被提出. Vedral 等 [14] 首先搭建了算术运算的量子线路, 其中包括加法门、乘法门以及模指数门等. 模指数门是构成 Shor 算法量子线路的重要组成部分. 使用 Vedral 等的方法搭

† 通信作者. E-mail: yzwu15@fudan.edu.cn

建 Shor 算法所需的量子线路需要 $7n$+2 个逻辑比特, 其中 n 是待分解整数 N 的二进制比特数. 在此基础上 Draper[15] 改进了加法门. 改进后的加法器需要两个输入 a, b. 与一般加法器不同的是, Draper 加法门首先计算 a 的量子傅里叶 (quatnum fourier transform, QFT) 结果, 记作 $F(a)$, 紧接着再计算 $F(a+b)$, 能够将 Shor 算法中需要的逻辑比特数量级降低至 $2n$. Beauregard[16] 使用量子 QFT 加法器以及半经典 QFT (semi-classical QFT) 构建 Shor 算法线路. 如果只使用一个量子比特循环控制受控模指数门, 分解大整数 N 只需要 $2n$+3 个逻辑比特.

由于真实量子计算机中噪声的存在, 在不纠错的情况下运行复杂量子线路很难得到正确结果. 关于在真实量子计算机上运行 Shor 算法 (使用纠错算法后) 的开销也被分析. Fowler 等[17] 指出, 以表面码为基础, 当量子门噪声大小为 10^{-3} 时, 需要在一台拥有 2.2×10^8 个物理比特的量子计算机上运行 26.7 h, 才能够分解一个 2000 比特的整数. 在 O'Gorman 和 Campbell[18] 的工作中, 使用了改进后的表面码, 每个逻辑比特需要的物理比特数目更少, 在量子门噪声大小为 10^{-4} 的情况下, 整个线路只需要 6.3×10^6 个物理比特. Hwang 等[19] 在使用 Steane 码以及表面码的基础上, 对 Shor 算法进行了分析, 相比于文献 [17, 18] 的工作, 他们对 Shor 算法的分析更加详细, 从而取得了更合理的结果, 他们指出在量子门噪声大小为 10^{-3} 的情况下使用 Shor 算法分解一个 512 比特的整数需要 9.5×10^{10} 个物理比特并且花费 8.78×10^5 h. Ha 等[20] 在使用旋转平面表面码[21] 的基础上给出了待分解整数的比特数与分解时间以及分解所需要的量子比特数目的具体关系, 他们指出, 在量子门噪声大小为 10^{-3} 的情况下分解 2048 比特的 RSA 整数需要 1.37×10^7 个物理比特, 并且要花费 1.89×10^7 h 完成. 在 Gidney[7] 的工作中, 他指出为了分解一个 2048 比特的整数, 在量子门噪声大小为 10^{-3} 的情况下需要在一台拥有 2×10^7 个物理比特的量子计算机上运行大约 8 h. 此外, Gidney[22] 将窗口法与量子线路融合, 进行量子运算的加窗操作, 能够降低模乘法门中的线路深度. Xiao 等[23] 提出以量子隐形传态为基础使用两台量子计算机实现分布式的 Shor 算法, 能够降低每台量子计算机运行所需要的量子比特数目以及线路深度. Rossi 等[24] 提出了 Shor 算法的简化版本, 并且在 IBM 的真实量子计算机上进行了验证, 结果表明在损失部分准确率的情况下仍能够得到正确的分解结果.

然而鲜有强调关于给噪声建模或者模拟噪声对算法影响的文献[9,25,26]. 文献 [10, 25] 提及了噪声建模的重要意义并且建立了对应的噪声模型. 文献 [27] 研究了特定噪声对量子近似优化算法[28] 的影响并且进行了数值分析. 大部分实验室并没有可以运行的量子计算机, 而一些公用量子计算机的比特数量以及相应参数不同, 因此很难准确地进行量子噪声建模[29]. 根据文献 [10], 本文将噪声分成 3 个通道分别进行研究, 分别是去极化通道 (depolarizing channel, DC)[30–32]; 状态制备与测量通道 (state preparation and measurement channel, SPAM)[33]; 热退相干通道 (thermal relaxation channel, TRC)[13,30].

目前 Shor 算法中的量子线路的复杂度仍然很高. 本文搭建的量子线路的深度达到了 $O(n^3)$, 线路宽度达到了 $4n$+2. 因此线路可能很容易受到噪声影响. 一方面, 明确量子计算机中噪声来源能够更有效地进行纠错[34,35]; 另一方面, 了解不同噪声对 Shor 算法的影响程度对于纠错也是十分重要的. 本文针对噪声对 Shor 算法的影响进行研究, 根据文献 [10] 将噪声分成 3 个通道, 通过一系列模拟得到了每个通道中不同大小的噪声与 Shor 算法成功率的数值关系, 对于后续对 Shor 算法进行纠错、改进等能够提供建设性的意见.

本文第 1 节介绍 Shor 算法以及量子噪声对 Shor 算法的影响, 分析本项研究的创新性以及意义; 第 2 节对 Shor 算法进行系统梳理, 定义了 Shor 算法整数分解的成功率和均方误差并且分析了量子线路的复杂度; 第 3 节讨论 3 个通道中噪声的模型以及作用过程; 第 4 节详述模拟噪声的实验过程并且对数值结果进行分析; 第 5 节总结数值模拟结果并且提出未来研究方向.

2 Shor 算法

Shor 算法将因数分解问题转换至一个求 a 在乘法群 Z_N^* 中的阶的问题[1]. a 的阶 $r=\mathrm{ord}(a,N)$ 的定义是能够使 $a^r\equiv1\ (\mathrm{mod}\ N)$ 成立的最小的正整数 r. 算法流程如表 1 所列.

表 1 Shor 算法流程

Table 1. Pseudo of Shor's algorithm.

算法 1 Shor算法

输入: 待分解的整数N

输出: N的非平凡素因子p, q

1: **if** N is even **then**

2: **return** $2, N/2$

3: **end if**

4: **if** $N=p^k$, where p is prime, $k>0$ **then**

5: **return** p

6: **end if**

7: select a random number a, where $1<a<N$

8: **if** $\gcd(a,N)>1$ **then**

9: **return** $\gcd(a,N)$, $N/\gcd(a,N)$

10: **end if**

11: excute quantum circuit, find minimal positive period of $f_a(x)=a^x \bmod N$, denoted as r

12: **if** r is odd **or** $a^{\frac{r}{2}}\equiv -1\ (\mathrm{mod}\ N)$ **then**

13: GOTO 7

14: **end if**

15: calculate $p=\gcd(a^{\frac{r}{2}}-1,N)$ and $q=\gcd(a^{\frac{r}{2}}+1,N)$

16: **return** p,q

Shor 分解算法包括经典部分与量子部分. 量子噪声会直接影响到其中的量子线路运行的结果. 本节对 Shor 算法量子部分进行系统梳理.

2.1 Shor 算法量子线路

Shor 算法的量子线路 (量子求阶程序) 如图 1 所示.

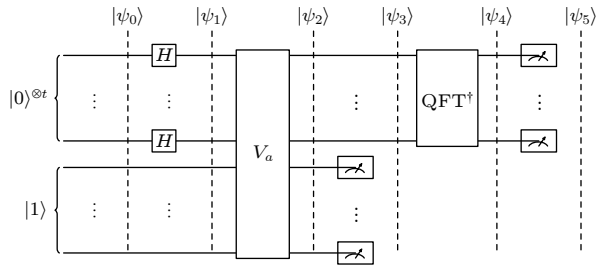

图 1 Shor 算法中的量子线路

Fig. 1. Quantum circuit of Shor's algorithm.

线路需要两个量子寄存器, 分别含有 $t=2\lceil\log_2 N\rceil$ 和 $n=\lceil\log_2 N\rceil$ 个量子比特. 对第一个寄存器中的每个比特施加一个 H 门得到均匀叠加态. 并且第二个寄存器的初态为 $|1\rangle$. 那么 $|\psi_1\rangle=\dfrac{1}{\sqrt{j}}\sum_{l=0}^{j-1}|l\rangle\otimes|1\rangle$, 其中 $j=2^t$. V_a 量子门是通过量子线路实现的模指数运算, 本质上是一个受控酉门[30], 其定义为 $V_a(|i\rangle|k\rangle)=|i\rangle\left|(k+a^i)\mathrm{mod}N\right\rangle$. 根据相位反冲原理, $|\psi_2\rangle=V_a|\psi_1\rangle=\dfrac{1}{\sqrt{j}}\sum_{l=0}^{j-1}|l\rangle\otimes\left|a^l\mathrm{mod}N\right\rangle$. 如果对第二个寄存器进行测量, 将测量结果记作 a^b, 其中 $0\leqslant b<r$. $|\psi_2\rangle$ 将坍缩至所有 $|l\rangle$ 的叠加, l 满足 $a^l\equiv a^b \bmod N$, 即 a^l 与 a^b 同余, 并且 $l=kr+b$, 其中 $0\leqslant k<r$. 那么 $|\psi_3\rangle=\left(\dfrac{1}{\sqrt{c}}\sum_{k=0}^{c-1}|kr+b\rangle\right)\otimes\left|a^b\right\rangle$, 其中 $c=\lceil j/r\rceil$. 此时使用量子傅里叶逆变换[36–38] 提取隐藏在第一个寄存器中的周期信息. 根据量子傅里叶变换的定义可以得到:

$$|\psi_4\rangle=\frac{\sqrt{c}}{\sqrt{j}}\sum_{\substack{l=0\\ j\mid(lr)}}^{j-1}\omega^{-lb}|l\rangle+\frac{1}{\sqrt{jc}}\sum_{\substack{l=0\\ j\nmid(lr)}}^{j-1}\omega^{-lb}\frac{1-\omega^{-lcr}}{1-\omega^{-lr}}|l\rangle, \tag{1}$$

其中 $\omega=\exp(2\pi\mathrm{i}/j)$. 该态的含义是包含两种情况, 分别是 $j\mid lr$ 以及 $j\nmid lr$ 的不同情况的叠加态. 测量 $0\leqslant l<j$ 的概率大小是:

$$P(l)=\begin{cases}c/j, & j\mid(lr),\\ \dfrac{\sin^2(\pi lrc/j)}{jc\sin^2(\pi lr/j)}, & \text{otherwise.}\end{cases} \tag{2}$$

当 j 能够被 (lr) 整除时, 概率大小是 c/j, 此时对应的测量结果 l 满足 $l=kj$, 其中 k 是正整数. 当 j 不能被 (lr) 整除时, $P(l)$ 会在 l 满足 $\sin^2(\pi lr/j)\approx 0$ 的条件下产生极大值, 对应的测量结果 l 应该满足 $l\approx kj/r$. 因此对 $|\psi_4\rangle$ 进行测量时, 会有更高的概率使测量结果 l 满足 $l\approx kj/r$ (约等于符号是因为测量得到的 l 是整数, 是离散的)[39].

假设待分解的整数 $N=21$, 随机数选择 $a=2$, 那么 $r=\mathrm{ord}_{21}(2)=6$, $t=2\lceil\log_2 N\rceil=10$, $j=2^t=1024$, $c=\lceil j/r\rceil=171$, l 的范围是 $0\leqslant l<1024$, $l\in\mathbb{Z}$. l 的理论概率分布如图 2 所示.

当 $l=0$ 或者 $l=512$ 时满足 $l\mid(qr)$, 对应于图 2 中最高的两个峰, 其大小等于 $1/r\approx 0.167$. 其他情况 ($l\neq 0, l\neq 512$) 下, 当 $l\approx k(j/r)$, 即 $l=171$, 341, 683, 853 时, 在图像中对应第二高的峰, 大小约为 0.114. $|\psi_4\rangle$ 分布是有规律的. 选择不同的随机数分解同一个整数时, 分布会因随机数阶的不同发生差异. 并且随着待分解整数增大, 峰值概率也会降低. 对于不同大小噪声下的情况, 可以比较分布的差异从而判断出噪声对于线路影响程度的不同.

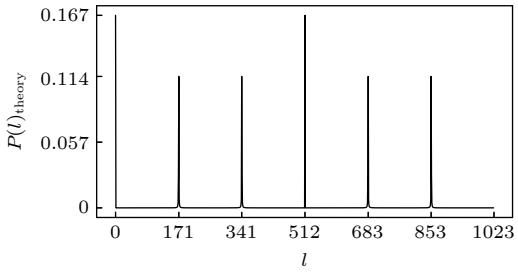

图 2 Shor 算法分解 ($N=21$, $a=2$) 实验中 $|\psi_4\rangle$ 的预期概率分布

Fig. 2. Expected probability distribution of $|\psi_4\rangle$ in factoring ($N=21$, $a=2$).

2.2 成功率的定义

在经典计算机上模拟时, 能够计算 $|\psi_4\rangle$ 的状态向量, 因此能够得到 l 的分布. 如果测量结果满足 $l=k(j/r)$, $1\leqslant k<r$, 则可以进一步求其连分数[1] (具体实现在附录 A 中) 最终完成对 N 的分解. 例如在分解 $N=21(a=2)$ 的实验中, $|\psi_4\rangle$ 的概率分布如图 2 所示, 除去 $l=0$, $l=512$, 该分布有 4 个峰值, 将该 4 个峰值的测量概率求和作为 Shor 算法整数分解的成功率, 即 $P_{\rm s}=P(171)+P(341)+P(683)+P(853)$. 对于一般情况, 成功率的定义则是:

$$P_{\rm s}=\sum_{L}P(l),\ l=\left\lceil k\frac{j}{r}\right\rfloor,\ k\frac{j}{r}\neq\left\lceil k\frac{j}{r}\right\rfloor,\ 1\leqslant k<r. \tag{3}$$

当 a 在 Z_N^* 的阶 r 满足 $r=2^k$ 时 (其中 $k\geqslant 1$), 此时天然满足 $r|j$. 在这种情况下有 $c=\left\lceil\dfrac{j}{r}\right\rfloor=\dfrac{j}{r}$. 那么在 (1) 式中只有 $j\mid(lr)$ 这一项, 此时 $|\psi_4\rangle=\dfrac{\sqrt{c}}{\sqrt{j}}\sum\limits_{\substack{l=0\\ j|(lr)}}^{j-1}\omega^{-lb}|l\rangle$. 当 $l=k\dfrac{j}{r}$ 时 (其中 $k\geqslant 0$, 是正整数), $P(l)$ 取得最大值, 大小为 $P(l)=\dfrac{c}{j}=\dfrac{1}{r}$, 其他情况下, $P(l)=0$. 此时成功率计算公式为

$$P_{\rm s}=\sum_{L}P(l)\ ,\ l=k\frac{j}{r},\ \ 1\leqslant k<r. \tag{4}$$

此外, 本文还将均方误差 (mean squared error, MSE) 这一指标用于实验结果的比较, 该指标定义式为

$$\text{MSE}=\frac{1}{k}\sum_{j=1}^{k}(P(l)_{\text{theory}}-P(l)_j)^2, \tag{5}$$

其中, $P(l)_{\text{theory}}$ 代表 l 的理论概率分布, $P(l)_j$ 代表某一噪声环境下第 j 次实验中 l 的概率分布, 一共重复实验 k 次. 而 $(P(l)_{\text{theory}}-P(l)_j)^2$ 的定义是所有可能测量得到的结果的理论概率与实际概率作差并求其平方和. 这一指标能够很好地反映 $|\psi_4\rangle$ 在不同噪声环境下的分布与理论分布的差异, 从而能够帮助我们判断分解是否成功.

2.3 量子线路复杂度分析

本文以 Draper[15] 提出的 QFT 加法器作为量子线路的算术基础, 并且按照 Beauregard[16] 的方法依次搭建了模 N 加法门、受控模 N 乘法门、受控模指数门. 与 Beauregard 的方法不同的是, 本文并没有使用半经典 QFT, 而是一般 QFT (normal QFT), 因此共需要 $4n+2$ 个量子比特.

QFT 加法门的深度为 1, 需要 $n+1$ 个量子比特, 其中 n 是待分解整数 N 的二进制比特数. 额外的一个量子比特用于防止溢出. 模 N 加法门的复杂度取决于 QFT 的精度. 如果使用精确 QFT, 那么量子门数量为 $O(n^2)$, 线路深度达到了 $O(n)$, 一共使用 $n+4$ 个量子比特, 其中 $n+1$ 个比特用于实现 QFT 加法门; 2 个用于控制比特; 1 个作为辅助比特. 受控模 N 乘法门需要 2 次 QFT 以及 n 个模 N 加法门, 线路深度达到了 $O(n^2)$, 共需要 $2n+3$ 个量子比特, 其中 $n+2$ 个量子比特用于模 N 加法, 另外 n 个比特用于存放 $|x\rangle$, 剩下一个量子比特用于控制比特. 受控模 N 指数门由一个受控模 N 加法门、受控交换门以及一个受控模 N 乘法门的逆门构成, 因此深度仍然是 $O(n^2)$, 并且所需要的量子比特数目和受控模 N 乘法门相同, 均为 $2n+3$ 个量子比特. 搭建图 1 中的 V_a 门需要 $2n$ 个 U_a 门, 每个 U_a 门由不同的量子比特控制. 最终的线路宽度为 $4n+2$, 线路的总深度达到了 $O(n^3)$.

Shor 算法中的量子线路首先对第一个寄存器的所有的比特施加 1 个 H 门, 并且在对第一个寄存器进行测量前进行 1 次 QFT 逆运算, 分别需要 $O(n)$ 个单比特门以及 $O(n^2)$ 个双比特门. 在 QFT 加法器中, 需要 1 次 QFT 以及 $n(n+1)/2$ 个双比特门, 那么单比特门的数量为 $O(n)$, 双比特门的数量为 $O(n^2)$. 在模 N 加法门中, 需要 3 个受控加法门、2 个加法门以及 4 次 QFT (其中 2 次是逆变换) 和 2 个 X 门以及 2 个 CX 门. 那么双比特门的数量仍是 $O(n^2)$, 单比特门的数量为 $O(n)$. 受控模 N 乘法门需要 n 个模 N 加法门以及 2 次 QFT (其

中 1 次是逆运算), 因此该门共需要 $O(n^3)$ 个双比特门以及 $O(n^2)$ 个单比特门. U_a 门包含一个受控模 N 乘法门、一个 CSWAP 门以及一个受控模 N 乘法门的逆, 不会改变所需量子门数目的量级. 整个 Shor 算法中共需要 $2n$ 个 U_a 门来完成模指数运算. 因此整个 Shor 量子线路中共使用了 $O(n^4)$ 个双比特门以及 $O(n^3)$ 个单比特门.

3 量子噪声

在量子计算机上运行量子算法的过程中噪声是不可避免的. 噪声是构建大型量子计算机的主要障碍[9,10]. 随着构成量子线路的门数量增多以及使用的量子比特数增多, 线路更容易受到噪声的影响, 从而导致最终结果与预期产生偏差. 根据 2.3 节中的分析, Shor 算法中量子线路的宽度达到了 $4n$+2, 量子门数量达到了 $O(n^4)$, 在量子计算机上运行时很容易受到噪声影响, 从而影响 Shor 算法的成功率. 因此模拟噪声环境中运行 Shor 算法能够研究得到哪种噪声对算法的影响最大, 能够使得纠错环节更加高效[34]. 本文根据文献 [10] 将噪声分为 3 个通道进行研究, 分别是去极化通道; 状态制备与测量通道; 热退相干通道. 这 3 个通道的噪声能够涵盖真实量子计算机环境中常见的噪声类别.

3.1 去极化通道

由于量子门的保真度无法达到 100%, 因此量子比特在经过量子门时会有一定的概率产生相位翻转或者比特翻转或者同时发生[30,40]. 比特翻转相当于在原有量子门基础上添加了一个 X 门. 而相位翻转相当于在原有量子门基础上添加了一个 Z 门. 当相位翻转和比特翻转同时发生时, 相当于在原有量子门基础上添加了一个 Y 门. 3 种泡利噪声出现的可能性相等. 去极化通道作用于量子线路如下:

$$\boldsymbol{\rho} \to D(\rho) = \sum_{i=0}^{3} \boldsymbol{K}_{D_i} \boldsymbol{\rho} \boldsymbol{K}_{D_i}^{\dagger}, \tag{6}$$

其中 $\boldsymbol{K}_{D_0} = \sqrt{1-P}I, \boldsymbol{K}_{D_1} = \sqrt{\dfrac{P}{3}}X, \boldsymbol{K}_{D_2} = \sqrt{\dfrac{P}{3}}Z, \boldsymbol{K}_{D_3} = \sqrt{\dfrac{P}{3}}Y$, $\boldsymbol{\rho}$ 是一个比特的密度矩阵. 在量子线路中, 量子比特要么经过单比特门要么经过双比特门. 可以根据量子门的类型将其分为两类: 单比特门去极化噪声, 去极化噪声出现在单比特门后; 双比特门去极化噪声, 只有目标比特经过双比特门后会受到影响, 控制比特不会受到影响, 主要原因在于在此通道中, 只有当量子比特的态发生转变时才会受到去极化噪声影响, 而控制比特只是作为量子门的驱动器, 其态在经过双比特门前后不会发生改变, 因此不会受到去极化噪声的影响. 本文分别研究单比特门去极化噪声与双比特门去极化对 Shor 算法的影响, 将单比特门去极化噪声、双比特门去极化噪声大小分别记作 P_1 与 P_2.

3.2 状态制备与测量通道

SPAM 通道的噪声仅导致状态制备后以及测量前的比特翻转. 将 SPAM 通道与 DC 区别的原因在于, 状态制备会向量子寄存器中注入预期的初态, 会需要进行额外的操作, 后者主要是发生在量子线路的运行过程中[33]. 将此通道中发生比特翻转的大小记作 P_{spam}. 使用算符和表达则是:

$$\boldsymbol{\rho} \to S(\rho) = \boldsymbol{K}_{M_0} \boldsymbol{\rho} \boldsymbol{K}_{M_0}^{\dagger} + \boldsymbol{K}_{M_1} \boldsymbol{\rho} \boldsymbol{K}_{M_1}^{\dagger}, \tag{7}$$

其中 $\boldsymbol{K}_{M_0} = \sqrt{1-P_{\text{spam}}}I$, $\boldsymbol{K}_{M_1} = \sqrt{P_{\text{spam}}}X$. 在本文构建的 Shor 算法量子线路中, 一开始需要将第二个寄存器的初态制备成 $|1\rangle$, 第一个寄存器制备成 $|0\rangle^{\otimes t}$, 以及在线路最后需要对第一个寄存器进行测量. 因此 SPAM 通道的噪声一共只出现 $2t+n$ 次.

3.3 热退相干通道

退相干指的是量子比特与环境耦合过程中逐渐失去相干性的过程, 来源于噪声与量子比特的微弱耦合[30,41]. 实际的量子比特系统很难做到完全孤立, 除此之外, 还要对量子比特进行测量, 这就会使得量子比特总会与外部环境耦合. 按照对量子比特的影响不同可以分为退相位 (dephasing)[30]、弛豫 (relaxation)[42].

3.3.1 退相位

退相位描述了量子比特携带的信息损失[30]. 这里假定退相位噪声单独作用, 即纯退相位 (pure dephasing, PD). 假设初态是 $\boldsymbol{\rho}_{\text{in}} = \begin{bmatrix} a & b \\ b^* & 1-a \end{bmatrix}$. 使用 Kraus 算符描述退相位则是 $\boldsymbol{E}_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$,

$\boldsymbol{E}_1=\begin{bmatrix}0&0\\0&\sqrt{\gamma}\end{bmatrix}$. 密度矩阵的转化为 $\boldsymbol{\rho}_{\text{out}}=\boldsymbol{E}_0\boldsymbol{\rho}_{\text{in}}\boldsymbol{E}_0^{\dagger}+\boldsymbol{E}_1\boldsymbol{\rho}_{\text{in}}\boldsymbol{E}_1^{\dagger}=\begin{bmatrix}a&b\sqrt{1-\gamma}\\b^*\sqrt{1-\gamma}&1-a\end{bmatrix}$. 其中对角线元素没有发生变化, 非对角线元素会随时间呈指数发生纯退相位. 用参数 T_2^{pure} [25] 描述纯退相位时间, 则 $\sqrt{1-\gamma}=\exp\left(-t/T_2^{\text{pure}}\right),\gamma=1-\exp\left(-2t/T_2^{\text{pure}}\right)$. 最终能够得到纯退相位的过程:

$$\boldsymbol{\rho}_{\text{out}}=\begin{bmatrix}a&b\exp\left(-\dfrac{t}{T_2^{\text{pure}}}\right)\\b^*\exp\left(-\dfrac{t}{T_2^{\text{pure}}}\right)&1-a\end{bmatrix}. \tag{8}$$

3.3.2 弛豫

热力的弛豫过程也是非西并且不可逆的, 这一过程包括了量子比特与所处环境的能量交换 [30]. 假设初态为 $\boldsymbol{\rho}_{\text{in}}=\begin{bmatrix}a&b\\b^*&1-a\end{bmatrix}$. 以 Kraus 算符的形式描述弛豫退相干则是 $\boldsymbol{E}_0=\begin{bmatrix}1&0\\0&\sqrt{1-\gamma}\end{bmatrix}$, $\boldsymbol{E}_1=\begin{bmatrix}0&\sqrt{\gamma}\\0&0\end{bmatrix}$, 其中参数 γ 决定了弛豫的概率, 假设弛豫结束后的最终态是 $|0\rangle$, 那么 $\boldsymbol{\rho}_{\text{out}}=\begin{bmatrix}a+\gamma(1-a)&b\sqrt{1-\gamma}\\b^*\sqrt{1-\gamma}&(1-\gamma)(1-a)\end{bmatrix}$. 弛豫同时影响到了对角线与非对角线的元素. 一般使用 T_1 来描述弛豫与时间的关系, T_1 也被称为弛豫时间; 假设一个量子比特初态为 $|1\rangle$, T_1 描述了该态需要多久会坍缩到 $|0\rangle$ [43], 即 $\gamma=1-\exp(-t/T_1)$, $\sqrt{1-\gamma}=\exp(-t/(2T_1))$. 那么

$$\boldsymbol{\rho}_{\text{out}}=\begin{bmatrix}1-(1-a)\exp\left(-\dfrac{t}{T_1}\right)&b\exp\left(-\dfrac{t}{2T_1}\right)\\b^*\exp\left(-\dfrac{t}{2T_1}\right)&(1-a)\exp\left(-\dfrac{t}{T_1}\right)\end{bmatrix},$$

当 T_1 越大时, 该量子比特能够保持 $|1\rangle$ 状态的时间也越久. 将纯退相位的过程一起考虑进来. 根据 (8) 式, 当能量弛豫与纯退相位两种噪声同时作用时, 有

$$\boldsymbol{\rho}_{\text{out}}=\begin{bmatrix}1-(1-a)\exp\left(-\dfrac{t}{T_1}\right)&b\exp\left(-\dfrac{t}{T_2}\right)\\b^*\exp\left(-\dfrac{t}{T_2}\right)&(1-a)\exp\left(-\dfrac{t}{T_1}\right)\end{bmatrix}. \tag{9}$$

这里引入了参数 T_2 来描述弛豫与纯退相位共同作用的结果, T_2 也被称为退相位时间. 在实验中使用 T_1 与 T_2 来描述热退相干 [25] 噪声. T_2 与 T_1 的关系为 $1/T_2=1/T_2^{\text{pure}}+1/2T_1$. 在模拟时, T_2 最大能够取到 $2T_1$. 在量子线路运行时 (不包括测量与状态制备) 每个量子比特经过量子门 (单比特门、双比特门) 都会按照 (9) 式同时发生弛豫与纯退相位. 并且本文假定所有比特的热退相干模型相同, 即共享一组 T_1,T_2 参数.

4 数值模拟

本文以 Python 作为开发语言, 借助用于量子计算的 Qiskit 库 [44] 进行模拟实验, 在此基础上搭建了 Shor 算法的量子线路、设置了不同的噪声环境以及计算 $|\psi_4\rangle$ 的状态向量, 从而计算 $|\psi_4\rangle$ 的概率分布, 并且按照 2.2 节中的定义能够计算出成功率. 这样做的优点在于仅进行一次模拟就可以得到准确的概率分布以及成功率, 避免了通过重复测量得到分布的繁琐. 按照第 3 节将噪声分成 3 类进行单独模拟. 对于每一种噪声分别设置了不同参数区间, 在不同噪声大小的基础上模拟运行 Shor 算法量子线路, 并且记录 $|\psi_4\rangle$ 的分布. 对于每次模拟, 都至少重复 1000 次, 从而减弱随机误差的影响, 将每次计算得到的成功率进行平均, 作为最后的成功率, 并进行进一步的分析.

4.1 去极化通道

本文针对去极化通道分别研究了单比特门去极化噪声与双比特门去极化噪声对 Shor 算法的影响, 并且认为所有的单比特门 (X 门, H 门等) 所经历的噪声大小相同. 在运行量子线路过程中 (不包括状态制备以及测量) 当量子比特经过任意单比特门后, 可能会发生 X 门翻转或者 Y 门翻转或者 Z 门翻转, 概率均为 $P_1/3$. 本实验模拟了 $N=15$, $N=21$, $N=35$ 的分解, 对于每个整数使用不同的随机数进行分解, 具体组合如表 2 所列. 一次模拟整数分解实验所消耗的资源随着待分解整数比特增加而指数上升, 代码运行时间只与待分解大整数的比特数目与硬件配置有关. 平均 1 s 左右即可完成一次对 $N=15$ 的分解. 一次 $N=21$ 的分解实验需要消耗约 12 s. 而在对 $N=35$ 进行分解时, 每进行一次分解实验需要花费大约 2 min 的时间. 对于每一次模拟都重复 1000 次从而减弱随机误

差, 因此共需要花费约 1.4 d 的时间完成, 这导致无法对更大的整数进行模拟分解.

表 2 实验选择的待分解整数与随机数组合 (N, a)
Table 2. Combination of integer about to be factored and random number (N, a).

N	a
15	[2, 4, 7]
21	[2, 8, 11]
35	[2, 4, 9]

对于每一个 (N, a) 组合, 本文模拟了不同大小的单比特门去极化噪声作用于量子线路的实验. 单比特去极化噪声大小取值为 [0, 0.0005, 0.001, 0.0015, $\cdots$, 0.01]. 对于双比特门去极化噪声, 只有当目标比特经过任意双比特门 (如 CY 门, CZ 门, CX 门等) 后会发生 X 翻转或 Y 翻转或 Z 翻转, 3 种噪声发生的概率均为 $P_2/3$, 而控制比特不会受到影响. 本文选择表 2 的大整数、随机数组合进行模拟, 对于每一个组合都模拟了其在不同噪声大小下的实验. P_2 取值为 [0, 0.00015, 0.0003, 0.00045, $\cdots$, 0.003]. 在去极化通道的模拟实验中, 首先对比不同大小的单比特门去极化噪声对 $|\psi_4\rangle$ 的影响, 如图 3 所示.

每一列子图都代表一组 (N, a) 组合, 从左至右依次是 $N = 15$, $N = 21$, $N = 35$, 每一组都选择 $a = 2$ 作为随机数. 每条曲线的数据都是 1000 次模拟的平均并且归一化处理后的结果. $|\psi_4\rangle$ 的分布随着噪声大小增大而变得更混乱. 随着噪声逐渐增大, 峰值大小相比无噪声时下降了很多. 在 3 组整数分解中, 分解 $N = 35$ 的实验受噪声影响最大. 不同大小的双比特门去极化噪声对 $|\psi_4\rangle$ 的影响如图 4 所示.

类似于图 3, 随着双比特门去极化噪声增大, 每一组的分布更加混乱, 峰值大小逐渐降低, 分解 $N = 35$ 受到噪声影响最大. 按照 2.2 节中定义的 Shor 分解算法的成功率, 给出了 P_s 和 MSE 分别与两种去极化噪声的关系, 如图 5(a) 和图 5(b) 所示 (这里只给出部分结果, 所有结果见附录 B).

图 5(a) 和图 5(b) 中的每个点对应相应噪声大小下成功率的具体值, 曲线是对成功率与噪声大小关系的拟合, 每组实验都选择随机数 $a = 2$. 去极化噪声大小对成功率的影响呈指数形式, 2.3 节中

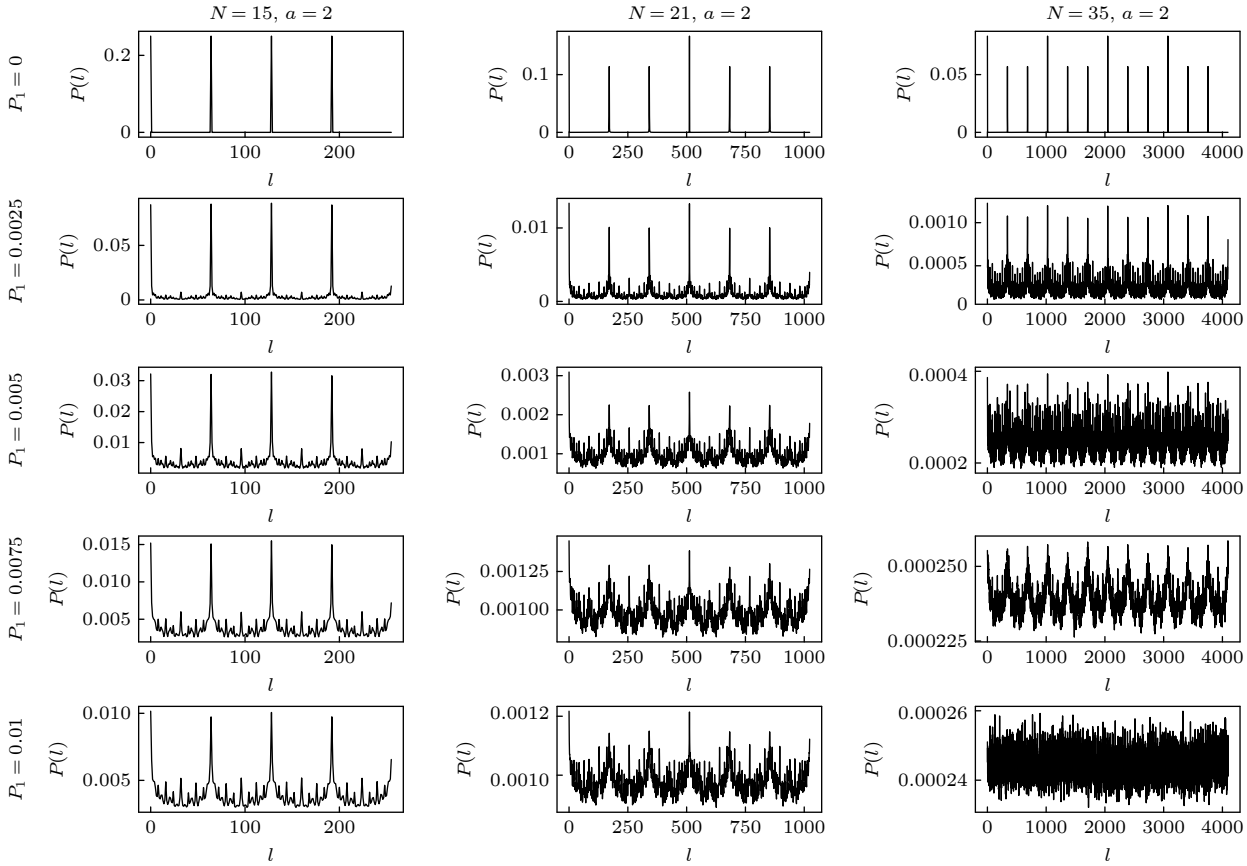

图 3 去极化通道中单比特门噪声对 ($N = 15$, $a = 2$), ($N = 21$, $a = 2$), ($N = 35$, $a = 2$) 中 $|\psi_4\rangle$ 概率分布的影响

Fig. 3. Effect of one-qubit gate noise in DC on probability distribution of $|\psi_4\rangle$ in ($N = 15$, $a = 2$), ($N = 21$, $a = 2$), ($N = 35$, $a = 2$).

分析了量子门数量与待分解整数的二进制比特数的关系. 随着待分解整数比特数目增多, 线路中的门数量更多, 导致成功率随着噪声增大而下降更快. 成功率随着双比特去极化噪声增大而降低的趋势快于单比特门, 原因在于线路中双比特门的数量多于单比特门数目. 图 6(a) 和图 6(b) 是 MSE 与两种去极化噪声的关系.

图 6(a) 和图 6(b) 中的每个点对应某一噪大小下 MSE 的值, 曲线则是对结果的拟合. 类似于图 5 中的结果, MSE 随着噪声增大而呈对数增长, 说明随着噪声增大, $|\psi_4\rangle$ 的分布与理论值的差异也越来越大, 分布逐渐失去规律从而无法得到正确的分解结果. 随着待分解整数比特数目增多, MSE 的变化趋势更加陡峭.

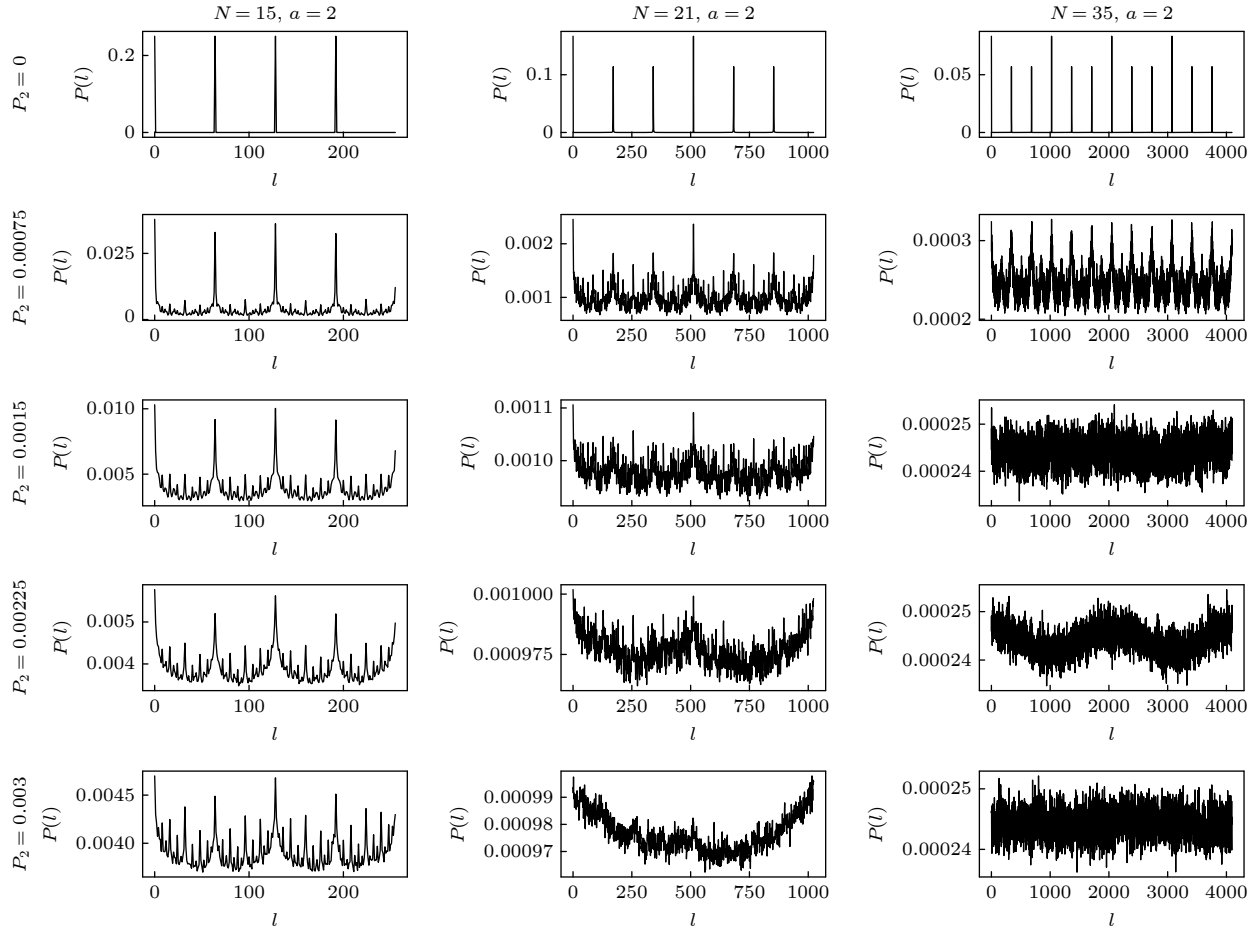

图 4 去极化通道中双比特门噪声对 ($N = 15$, $a = 2$), ($N = 21$, $a = 2$), ($N = 35$, $a = 2$) 中 $|\psi_4\rangle$ 概率分布的影响

Fig. 4. Effect of two-qubit gate noise in DC on probability distribution of $|\psi_4\rangle$ in ($N = 15$, $a = 2$), ($N = 21$, $a = 2$), ($N = 35$, $a = 2$).

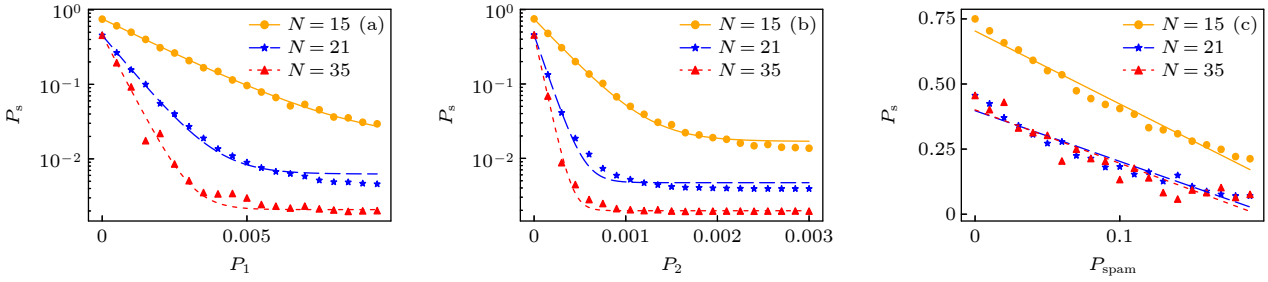

图 5 (a) P_s 与去极化通道中单比特门噪声的关系; (b) P_s 与去极化通道中双比特门噪声的关系; (c) P_s 与状态制备与测量通道中噪声的关系

Fig. 5. (a) Effect of one-qubit gate noise in DC on P_s; (b) effect of two-qubit gate noise in DC on P_s; (c) effect of noise in SPAM channel on P_s.

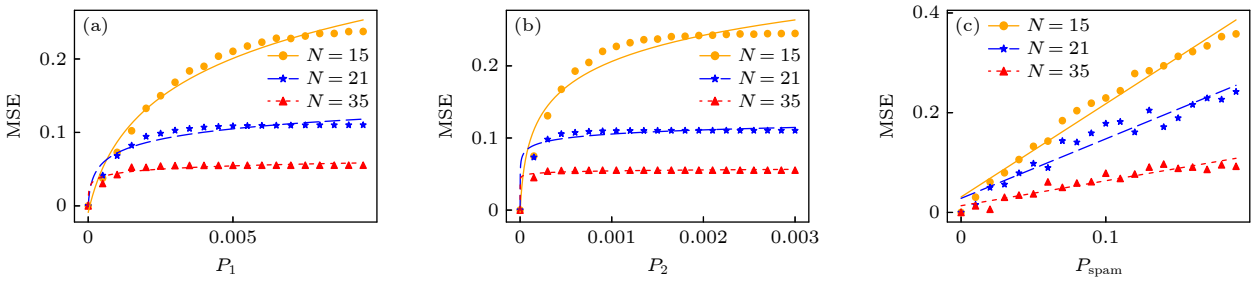

图 6 (a) MSE 与去极化通道中单比特门噪声的关系; (b) MSE 与去极化通道中双比特门噪声的关系; (c) MSE 与状态制备与测量通道中噪声的关系

Fig. 6. (a) Effect of one-qubit gate noise in DC on MSE; (b) effect of two-qubit gate noise in DC on MSE; (c) effect of noise in SPAM channel on MSE.

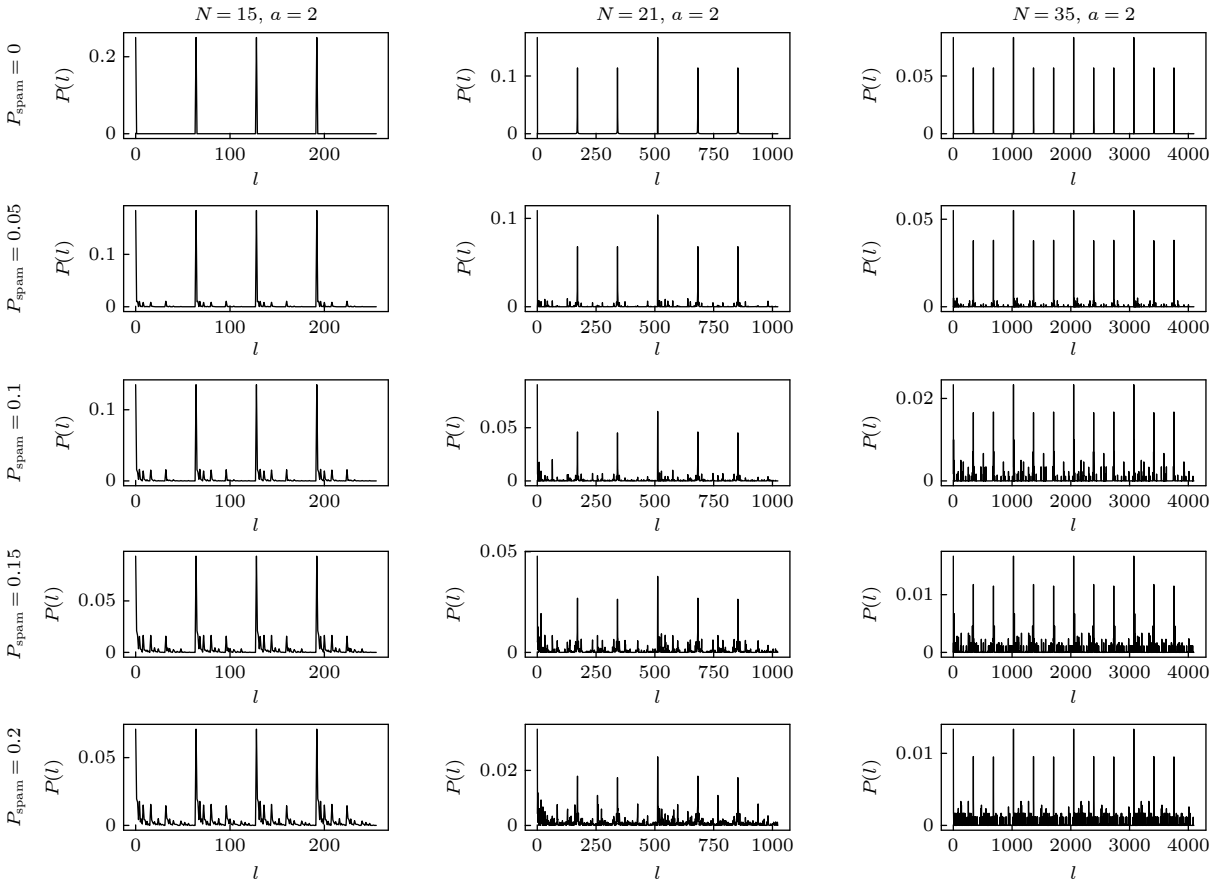

图 7 状态制备与测量通道中噪声对 $(N = 15,\ a = 2)$, $(N = 21,\ a = 2)$, $(N = 35,\ a = 2)$ 中 $|\psi_4\rangle$ 概率分布的影响

Fig. 7. Effect of noise in SPAM channel on probability distribution of $|\psi_4\rangle$ in $(N = 15\ a = 2)$, $(N = 21,\ a = 2)$ and $(N = 35,\ a = 2)$.

4.2 状态制备与测量通道

在状态制备与测量过程中, 本文假定所有制备状态或者测量的量子比特都会按照 P_{spam} 的概率发生比特翻转, 选择表 2 中的大整数、随机数的组合进行模拟. P_{spam} 的范围是 $[0.01,\ 0.02,\ 0.03,\ \cdots, 0.2]$. 类似于去极化通道, 对于每一次模拟都重复 1000 次. 首先对比不同大小的 SPAM噪声对 $|\psi_4\rangle$ 的影响, 如图 7 所示.

在分解 $N = 15$ 中, 随着噪声增大, 概率分布的峰值降低. $|\psi_4\rangle$ 的分布相较无噪声情况更混乱. 本文使用 P_{s} 与 MSE 来量化 SPAM 噪声对 Shor 算法的影响程度, 分别如图 5(c) 和图 6(c) 所示. 曲线中的每个点是实际计算的成功率大小, 曲线则是对结果的拟合. 通过曲线可以看出 SPAM 噪声的影响是线性的. 因为在线路中一共只会受到 $2t+n$ 次 SPAM 噪声的影响. 理论上随着待分解整

数比特数目增加, 线路会更容易受到噪声影响, 反映在图 5(c) 中是斜率的绝对值更大. 然而模拟结果这种特征并不明显, 主要原因在于分解的整数相差不大, 相邻两个整数只相差了一位. 并且由于测量次数与带分解整数二进制位数呈线性关系, 导致图中拟合曲线斜率变化不明显.

4.3 热退相干通道

本文假定所有量子比特共享一组 T_1, T_2, 并且选择表 2 中的大整数、随机数的组合进行模拟, 对于每一个组合都模拟了在不同 T_1, T_2 组合下的算法运行. T_1, T_2 参数选择如表 3 所列, 共 100 组. 在模拟中量子门的时间均设置为 50 ns. 并且分别针对退相干通道中 $N=15$, $N=21$, $N=35$ 的分解实验重复了 2000 次、4000 次以及 8000 次.

对比不同 T_1, T_2 对于分解 $N=15$, $N=21$, $N=35$ 的 $|\psi_4\rangle$ 分布的影响, 如图 8 所示.

随着退相干时间降低, 每一组 $|\psi_4\rangle$ 的峰值大小降低, 分布也更混乱. 待分解的整数越大, 对应的 $|\psi_4\rangle$ 分布的峰值下降得越明显. 与去极化通道的噪声类似, 在模拟中每当量子比特经过一个量子门时都会按照 (9) 式发生热退相干. 通过 $P_{\rm s}$ 以及 MSE 与退相干时间的关系可以更好地分析该类噪声对 Shor 算法的影响, 如图 9 和图 10 所示.

图 9 中白色区域是没有数据的点. 其他区域里颜色越深代表该 T_1, T_2 条件下的成功率越高. 随着 T_1, T_2 增大, 成功率逐渐增大, 并且随着待分解整数比特数目增多, 更容易受到退相干噪声的影响, 其成功率随着 T_1, T_2 变化而波动的幅度相对更大. 图 10 则是 MSE 与 T_1, T_2 的关系.

图 10 中白色区域是没有数据的点. 其他区域里颜色越深代表该 T_1, T_2 条件下的 MSE 越高. 随着 T_1, T_2 增大, 成功率也逐渐增大, 对应的 MSE 逐渐降低.

表 3 退相干通道中 T_1, T_2 的取值

Table 3. Choice of T_1, T_2 in TRC.

T_1/μs	T_2/μs
$[20, 30, \cdots, 90, 110]$	30
$[30, 40, \cdots, 100, 120]$	50
$[40, 50, \cdots, 110, 130]$	70
$[50, 60, \cdots, 120, 140]$	90
$[60, 70, \cdots, 130, 150]$	110
$[70, 80, \cdots, 140, 160]$	130
$[80, 90, \cdots, 150, 170]$	150
$[90, 100, \cdots, 160, 180]$	170
$[100, 110, \cdots, 170, 190]$	190

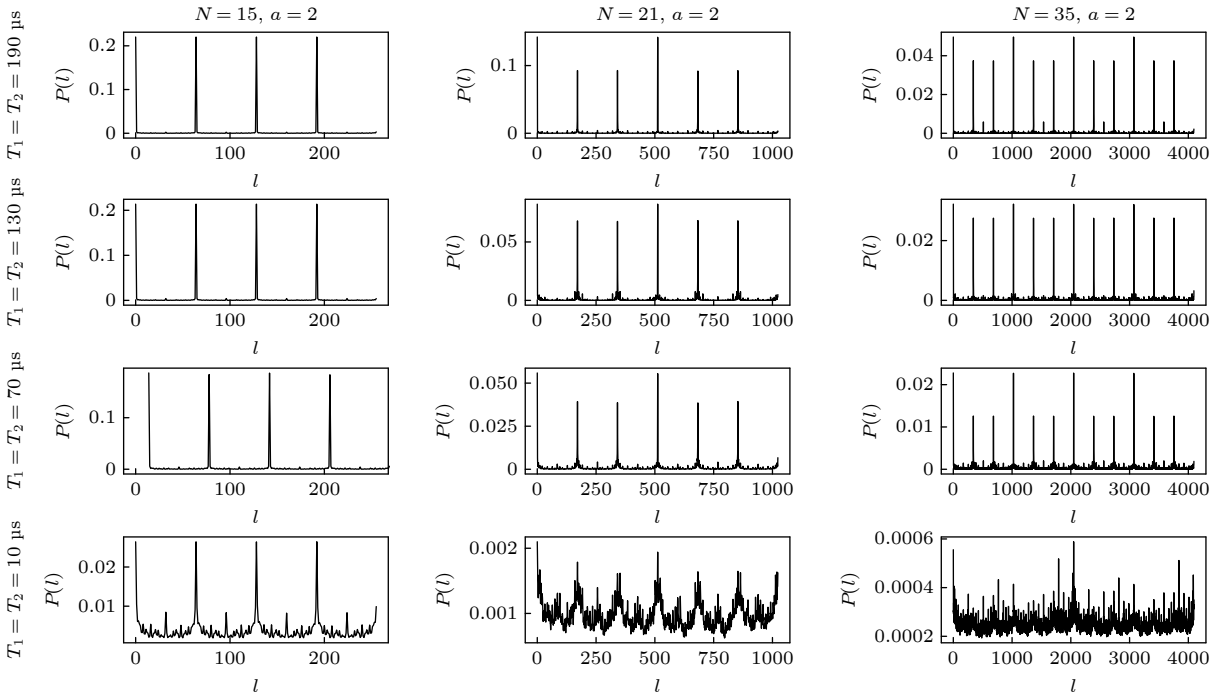

图 8 热退相干通道中不同 T_1, T_2 对 ($N=15$, $a=2$), ($N=21$, $a=2$), ($N=35$, $a=2$) 中的 $|\psi_4\rangle$ 概率分布的影响

Fig. 8. Different T_1, T_2 of TRC on probability distribution of $|\psi_4\rangle$ in ($N=15$, $a=2$), ($N=21$, $a=2$) and ($N=35$, $a=2$).

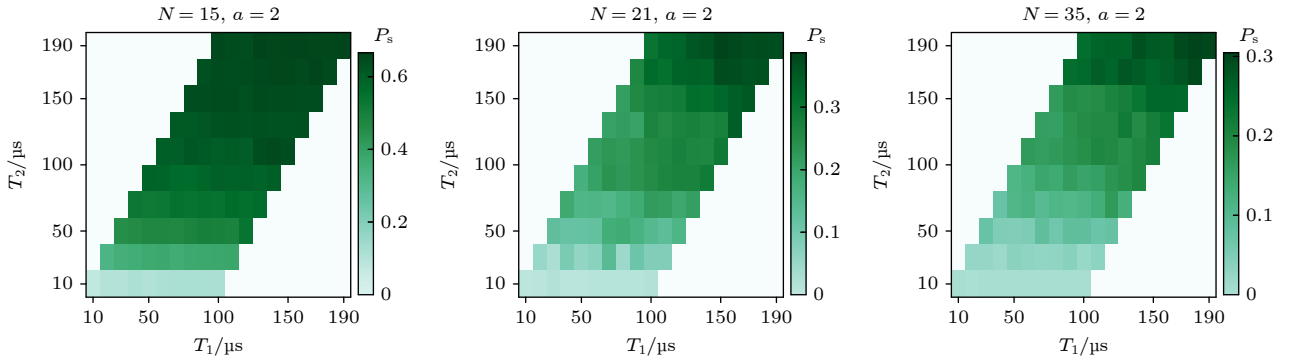

图 9 P_s 与热退相干通道的噪声的关系

Fig. 9. Effect of noise in TRC on P_s.

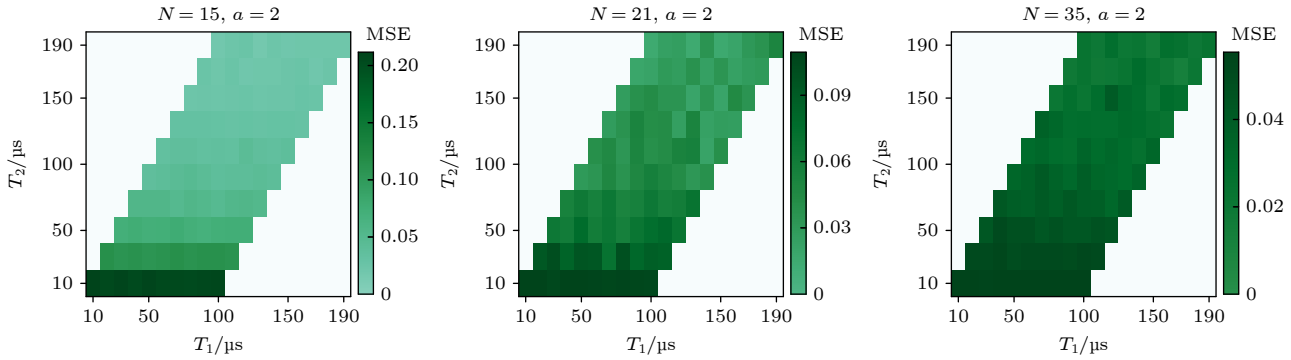

图 10 MSE 与热退相干通道的噪声的关系

Fig. 10. Effect of noise in TRC on MSE.

5 总结与展望

本文将 Shor 算法测量得到预期结果的概率之和作为 Shor 算法整数分解的成功率, 发现概率之和与均方误差的高低能够准确评估 Shor 算法中量子线路的运行结果的优劣, 在此基础上开展了一系列针对不同类型的噪声与成功率关系的研究. 分别研究了去极化通道、状态制备与测量通道、热退相干通道的噪声对 Shor 算法的影响, 并且在经典计算机上开展模拟 Shor 算法分解整数的实验. 对于任一通道, 设置了不同噪声大小, 得到了不同噪声大小与算法成功率的数值关系. 模拟结果表明, 在去极化通道中成功率随着噪声增大呈指数降低. 受量子线路搭建方式的影响, 成功率随双比特门去极化噪声增大而降低的趋势快于单比特门去极化噪声. 而状态制备与测量通道中的噪声对于成功率的影响是线性的. 相同噪声大小情况下, 随着待分解的整数比特位数增多, 需要的量子线路更加复杂, 线路深度以及宽度都将增加, 导致成功率随噪声增大而下降得更快. 在真实量子计算机中运行 Shor 算法时, 必须使用一系列的纠错手段进行纠错, 并且需要将纠错重点放在去极化噪声中. 此外, 对于 Shor 算法的量子线路进行优化与改进能够有效地降低线路复杂度, 并且有助于减弱算法运行时各类噪声对量子线路的影响, 如使用近似 QFT 代替精确 QFT 或者使用加窗以及陪集表示等方式都能够降低线路复杂度, 从而减弱因噪声引起的误差. 未来我们将针对优化后的线路进行纠错, 探究在使用纠错算法的基础上量子线路的复杂度以及噪声对线路的影响.

感谢中国电子科技集团公司第三十二研究所量子创新中心的陈鑫淼与高薪凯对搭建 Shor 算法量子线路的讨论, 同时感谢邢耀文以及姚晓梅对量子噪声建模提供的思考以及对论文撰写提供的指导.

参考文献

[1] Shor P W 1994 *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* Washington DC, USA, November 20–22, 1994 p124

[2] Shor P W 1999 *SIAM Rev. Soc. Ind. Appl. Math* **41** 303

[3] Lenstra A K, Hendrik Jr W 1993 *The Development of the Number Field Sieve*(Vol. 1554) (Heidelberg : Springer Science

& Business Media) p5
[4] Lenstra A K, Lenstra Jr H W, Manasse M S, Pollard J M 1990 *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing* Baltimore Maryland, USA, May 13–17, 1990 p564
[5] Buhler J P, Lenstra H W, Pomerance C 1993 *The Development of the Number Field Sieve* (Berlin Heidelberg: Springer) pp50–94
[6] Kleinjung T, Aoki K, Franke J, Lenstra A K, Thomé E, Bos J W, Gaudry P, Kruppa A, Montgomery P L, Osvik D A, Riele H T, Timofeev A, Zimmermann P 2010 *Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference* Santa Barbara, CA, USA, August 15–19, 2010 p333
[7] Gidney C, Ekerå M 2021 *Quantum* **5** 433
[8] Preskill J 2018 *Quantum* **2** 79
[9] Harper R, Flammia S T, Wallman J J 2020 *Nat. Phys.* **16** 1184
[10] Georgopoulos K, Emary C, Zuliani P 2021 *Phys. Rev. A* **104** 062432
[11] Brown K R, Harrow A W, Chuang I L 2004 *Phys. Rev. A* **70** 052318
[12] Bassi A, Großardt A, Ulbricht H 2017 *Classical Quantum Gravity* **34** 193002
[13] Viola L, Knill E, Lloyd S 1999 *Phys. Rev. Lett.* **82** 2417
[14] Vedral V, Barenco A, Ekert A 1996 *Phys. Rev. A* **54** 147
[15] Draper T G 2000 arXiv: 0008033 v1[quant-ph]
[16] Beauregard S 2002 arXiv: 0205095 v3[quant-ph]
[17] Fowler A G, Mariantoni M, Martinis J M, Cleland A N 2012 *Phys. Rev. A* **86** 032324
[18] O'Gorman J, Campbell E T 2017 *Phys. Rev. A* **95** 032338
[19] Hwang Y, Kim T, Baek C, Choi B S 2020 *Phys. Rev. Appl.* **13** 054033
[20] Ha J, Lee J, Heo J 2022 *Quantum Inf. Process.* **21** 60
[21] Horsman D, Fowler A G, Devitt S, Van M R 2012 *New J. Phys.* **14** 123011
[22] Gidney C 2019 arXiv: 1905.07682 v1[quant-ph]
[23] Xiao L, Qiu D, Luo L, Mateus P 2022 arXiv: 2207.05976 v1[quant-ph]
[24] Rossi M, Asproni L, Caputo D, Rossi S, Cusinato A, Marini R, Agosti A, Magagnini M 2022 *Quant. Mach. Intell.* **4** 18
[25] Bogdanov Y I, Chernyavskiy A Y, Holevo A, Lukichev V F, Orlikovsky A A 2013 *International Conference Micro-and Nano-Electronics* Zvenigorod, Russian Federation, October 1–5, 2012 p404
[26] Nachman B, Urbanek M, de Jong W A, Bauer C W 2020 *NPJ Quantum Inf.* **6** 84
[27] Xue C, Chen Z Y, Wu Y C, Guo G P 2021 *Chin. Phys. Lett.* **38** 030302
[28] Farhi E, Goldstone J, Gutmann S 2014 arXiv: 1411.4028 v1[quant-ph]
[29] Wallman J J, Emerson J 2016 *Phys. Rev. A* **94** 052325
[30] Nielsen M A, Chuang I L 2010 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) pp226–386
[31] Wilde M M 2013 *Quantum Information Theory* (Cambridge: Cambridge University Press) pp175–176
[32] Ji Z, Wang G, Duan R, Feng Y, Ying M 2008 *IEEE Trans. Inf. Theory* **54** 5172
[33] Ryan-Anderson C, Bohnet J G, Lee K, Gresh D, Hankin A, Gaebler J P, Stutz R P 2021 *Phys. Rev. X* **11** 041058
[34] Aliferis P, Preskill J 2008 *Phys. Rev. A* **78** 052331
[35] Tuckett D K, Bartlett S D, Flammia S T 2018 *Phys. Rev. Lett.* **120** 050505
[36] Coppersmith D 2002 arXiv: 0201067 v1[quant-ph]
[37] Ekert A, Jozsa R 1996 *Rev. Mod. Phys.* **68** 733
[38] Jozsa R 1998 *Proc. R. Soc. London, Ser. A* **454** 323
[39] Portugal R 2022 arXiv: 2201.10574 v5[quant-ph]
[40] King C 2003 *IEEE Trans. Inf. Theory* **49** 221
[41] Resch S, Karpuzcu U R 2021 *ACM Comput. Surv.* **54** 1
[42] Gottesman D 2009 arXiv: 0904.2557 v1[quant-ph]
[43] Tomita Y, Svore K M 2014 *Phys. Rev. A* **90** 062320
[44] McKay D C, Alexander T, Bello L, et al. 2018 arXiv: 1809.03452 v1[quant-ph]

附录 A

附录 A 详述了连分数 (continuous fraction) 的原理, 记作 Fraction() . 在测量得到 l 后, 需要计算 Fraction(l/j) , 结果记作 k/r , 其中 k 是正整数, r 是 a 的阶. 有限项的常规连分数 (简称连分数) 满足以下的约束条件: $\exists N \in \mathbf{N}$, $\forall k \in \mathbf{N}: a_{N+k} = 0$, 因此也可以写成如下形式:

$$[a_0; a_1, a_2, \cdots, a_N] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{N-1} + 1/a_N}}}. \tag{A1}$$

在 Shor 算法中, 将 l/j 记作 g, 根据 (A1) 式可以将任意一个小于 1 的正有理数其写成如下形式:

$$g = [g_1, \cdots, g_M] = \cfrac{1}{g_1 + \cfrac{1}{g_2 + \cfrac{1}{\cdots + 1/g_M}}}, \tag{A2}$$

其中 $g_1, g_2, \cdots, g_M$ 是正整数, 如果在某一个 g_i 将其截断, 舍弃掉一些小数, 便可以得到该数的一个收敛, 如

$$\frac{1}{g_1}, \frac{1}{g_1 + 1/g_2}, \frac{1}{g_1 + \cfrac{1}{g_2 + 1/g_3}}, \cdots. \tag{A3}$$

随着 g_i 的增加, 被舍弃的部分越来越小, 这些收敛值也越来越近 g. 在 Shor 算法中, 需要找到一组收敛 $[g_1, g_2, g_3, \cdots, g_i]$, 使得 i 足够大的同时满足有理数的分母 g_i 也要小于 N. 最后得到的分母可能就是 Shor 算法量子部分的最后结果 r, 即 $1/[g_1 + 1/(\cdots + 1/g_i)] = k/r$.

附录 B

图 B1 和图 B2 给出了分解 $N = 15$, $N = 21$, $N = 35$ 的实验中 P_s 和 MSE 与去极化通道中单比特门噪声的关系.

图 B3 和图 B4 给出了分解 $N = 15$, $N = 21$, $N = 35$ 的实验中 P_s 和 MSE 与去极化通道中双比特门噪声的关系.

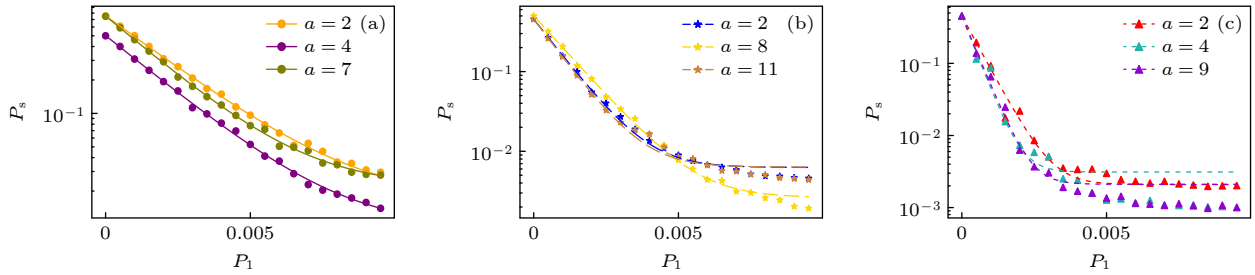

图 B1 分解实验中 P_s 与去极化通道中单比特门噪声的关系 (a) $N = 15$; (b) $N = 21$; (c) $N = 35$

Fig. B1. Effect of noise of one-qubit gate in DC on P_s of factoring: (a) $N = 15$; (b) $N = 21$; (c) $N = 35$.

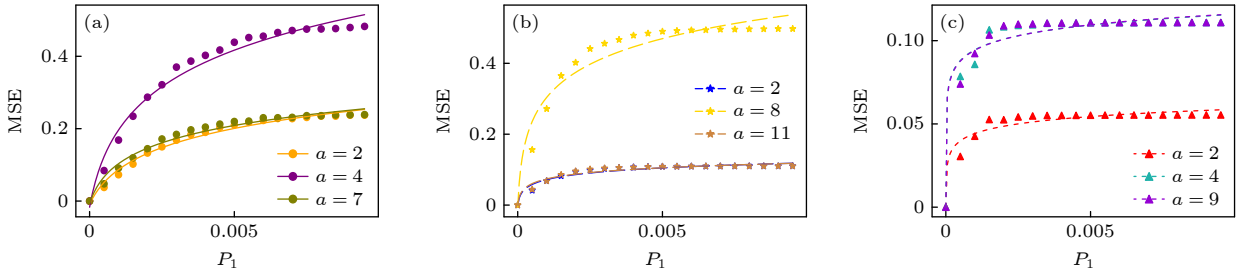

图 B2 分解实验中 MSE 与去极化通道中单比特门噪声的关系 (a) $N = 15$; (b) $N = 21$; (c) $N = 35$

Fig. B2. Effect of noise of one-qubit gate in DC on MSE of factoring: (a) $N = 15$; (b) $N = 21$; (c) $N = 35$.

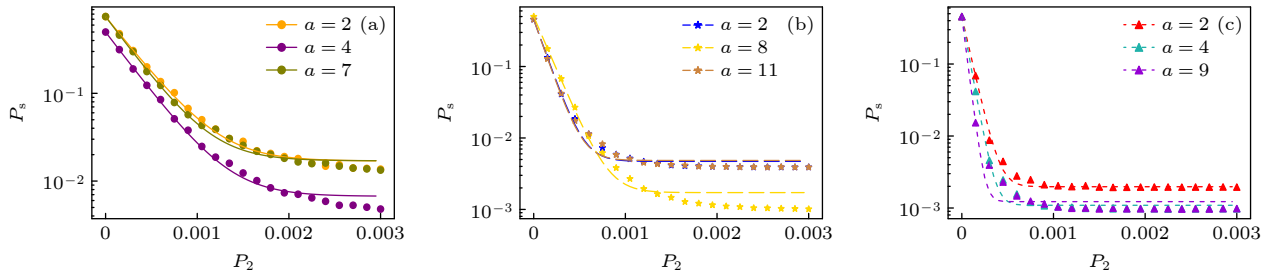

图 B3 分解实验中 P_s 与去极化通道中双比特门噪声的关系 (a) $N = 15$; (b) $N = 21$; (c) $N = 35$

Fig. B3. Effect of noise of two-qubit gate in DC on P_s of factoring: (a) $N = 15$; (b) $N = 21$; (c) $N = 35$.

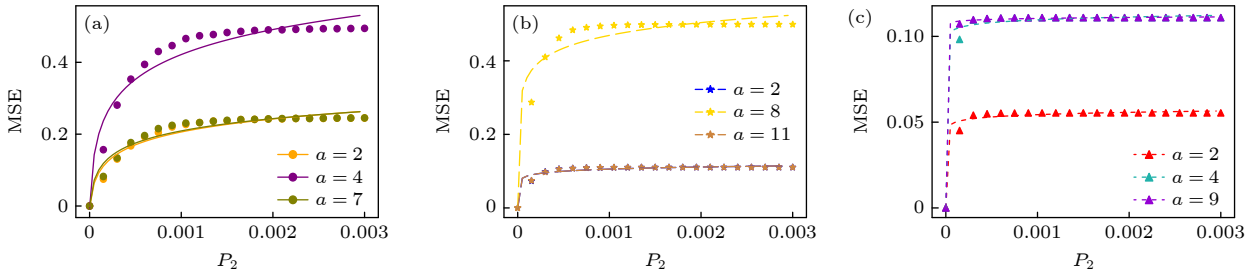

图 B4 分解实验中 MSE 与去极化通道中双比特门噪声的关系 (a) $N = 15$; (b) $N = 21$; (c) $N = 35$

Fig. B4. Effect of noise of two-qubit gate in DC on MSE of factoring: (a) $N = 15$; (b) $N = 21$; (c) $N = 35$.

图 B5 和图 B6 给出了分解 $N=15$, $N=21$, $N=35$ 的实验中 $P_{\rm s}$ 和 MSE 与状态制备与测量通道中噪声的关系.

图 B7 和图 B8 给出了分解 $N=15$, $N=21$, $N=35$ 的实验中成功率和 MSE 与退相干通道中噪声的关系.

表 B1 给出了分解所有 (N, a) 组合的线路参数以及在不同噪声的环境下的成功率.

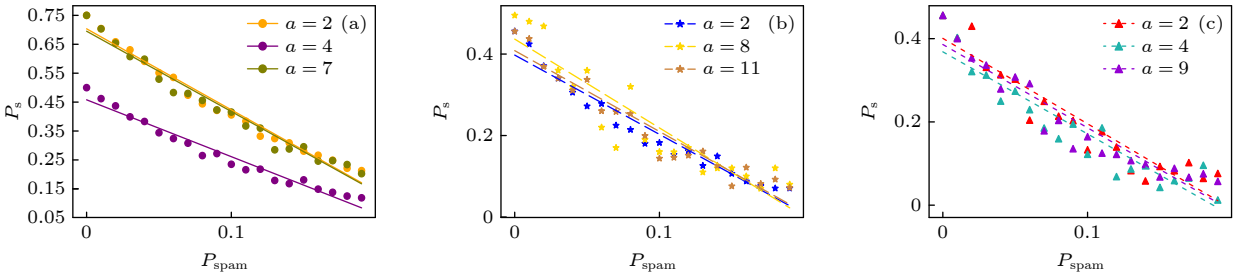

图 B5 分解实验中 $P_{\rm s}$ 与状态制备与测量通道中噪声的关系 (a) $N=15$; (b) $N=21$; (c) $N=35$

Fig. B5. Effect of noise in SPAM channel on $P_{\rm s}$ of factoring: (a) $N=15$; (b) $N=21$; (c) $N=35$.

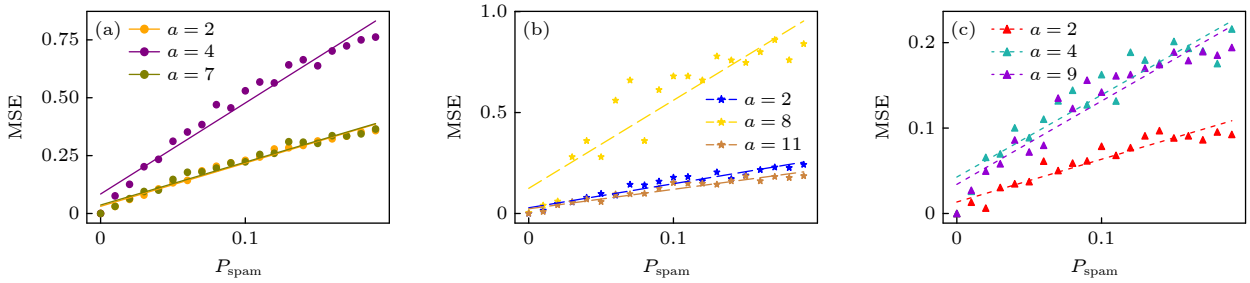

图 B6 分解实验中 MSE 与状态制备与测量通道中噪声的关系 (a) $N=15$; (b) $N=21$; (c) $N=35$

Fig. B6. Effect of noise in SPAM channel on MSE of factoring: (a) $N=15$; (b) $N=21$; (c) $N=35$.

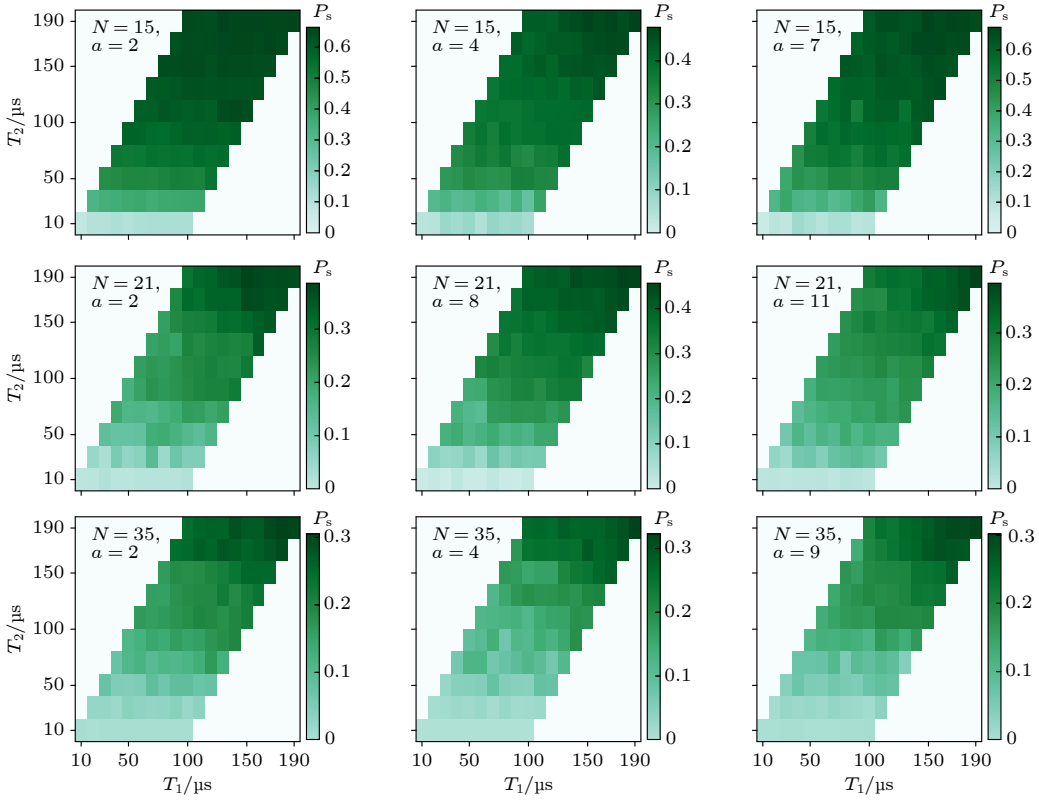

图 B7 分解 $N=15$, $N=21$, $N=35$ 实验中退相干噪声与 $P_{\rm s}$ 的关系

Fig. B7. Effect of noise in TRC on $P_{\rm s}$ of factoring $N=15$, $N=21$, $N=35$.

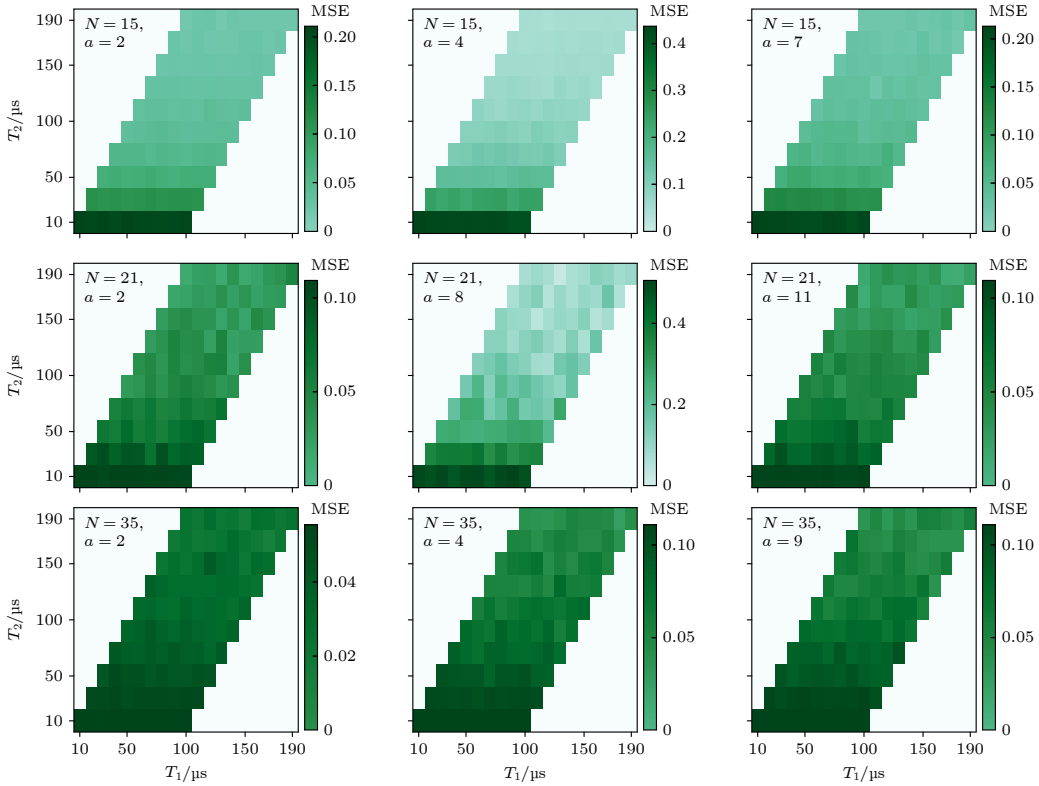

图 B8 分解 $N = 15$, $N = 21$, $N = 35$ 实验中退相干噪声与 MSE 的关系

Fig. B8. Effect of noise in TRC on MSE of factoring $N = 15$, $N = 21$, $N = 35$.

表 B1 所有整数与随机数组合 (N, a) 在不同噪声的环境下的成功率

Table B1. Effect of different levels of noise in 3 channels on success rates of all (N, a) pairs.

N		15			21			35		
a		2	4	7	2	8	11	2	4	9
单比特门数量			1584			2860			4680	
双比特门数量			8476			17045			30594	
线路深度			6432			12059			20565	
线路宽度(量子比特数)			18			22			26	
平均运行一次所需时间/s			1.15			11.89			142.34	
理论成功率(无噪声)		0.75	0.5	0.75	0.4559	0.5	0.4559	0.4559	0.4559	0.4559
噪声环境中的成功率	$P_1 = 0.0025$	0.2635	0.1593	0.2125	0.0408	0.0482	0.0327	0.0085	0.0058	0.0037
	$P_1 = 0.005$	0.0964	0.0526	0.0776	0.0089	0.0078	0.0085	0.0029	0.0013	0.0014
	$P_1 = 0.0075$	0.0455	0.0204	0.0358	0.0052	0.0031	0.0051	0.0021	0.0011	0.0011
	$P_1 = 0.01$	0.0295	0.0142	0.0278	0.0046	0.0019	0.0044	0.0020	0.0010	0.0010
	$P_2 = 0.00075$	0.1017	0.0512	0.0787	0.0073	0.0062	0.0082	0.0025	0.0012	0.0012
	$P_2 = 0.0015$	0.0284	0.0124	0.0255	0.0042	0.0015	0.0042	0.0019	0.0009	0.0010
	$P_2 = 0.00225$	0.0161	0.0064	0.0158	0.0039	0.0011	0.0039	0.0019	0.0008	0.0009
	$P_2 = 0.003$	0.0137	0.0048	0.0138	0.0038	0.0010	0.0038	0.0018	0.0008	0.0009
	$P_{\text{spam}} = 0.05$	0.5513	0.3441	0.5295	0.2721	0.3596	0.3373	0.3029	0.2739	0.3079
	$P_{\text{spam}} = 0.1$	0.4058	0.2354	0.4155	0.1823	0.1603	0.1438	0.1335	0.1223	0.1645
	$P_{\text{spam}} = 0.15$	0.2805	0.1812	0.2955	0.1066	0.1226	0.0758	0.0937	0.0427	0.0680
	$P_{\text{spam}} = 0.2$	0.2131	0.1193	0.2025	0.0705	0.0816	0.0721	0.0763	0.0125	0.0572
	$T_1 = T_2 = 10$ μs	0.0792	0.0386	0.0646	0.0067	0.0041	0.0083	0.0029	0.0014	0.0016
	$T_1 = T_2 = 70$ μs	0.5455	0.3444	0.5497	0.1556	0.2740	0.1963	0.1004	0.0722	0.1019
	$T_1 = T_2 = 130$ μs	0.6314	0.3992	0.6238	0.2714	0.3579	0.2811	0.2202	0.1972	0.2007
	$T_1 = T_2 = 190$μs	0.6603	0.4770	0.6513	0.3690	0.4521	0.3960	0.2998	0.3226	0.3014

Effects of quantum noise on Shor's algorithm

Huang Tian-Long Wu Yong-Zheng † Ni Ming
Wang Shi Ye Yong-Jin

(*The 32nd Research Institute of China Electronics Technology Group Corporation, Shanghai* 201808, *China*)

(Received 3 September 2023; revised manuscript received 10 December 2023)

Abstract

Shor's quantum factoring algorithm (Shor's algorithm) can solve factorization problem of large integers by using a fully-operational quantum computer with the complexity of polynomial-time level, thereby cracking a series of encryption algorithms (such as Rivest-Shamir-Adleman encryption algorithm, and Diffie-Hellman key exchange protocol) whose security is guaranteed by factorizing large integers, which is a difficult problem. We are currently in a noisy intermediate-scale quantum era, which means that we can only operate on quantum computers with a limited number of qubits and we have to take care of the effects of quantum noise. Quantum states on a quantum computer are prone to quantum noise caused by low-fidelity gates or interactions between qubits and the environment, which results in inaccurate measurements. We study the influence of quantum noise on Shor's algorithm through 3 typical quantum noise channels: the depolarizing channel, the state preparation and measurement channel, and the thermal relaxation channel. We successfully simulate the factorization of the numbers 15, 21, and 35 into their corresponding prime factors by using the quantum circuit we have constructed on a classical computer. Then we simulate a running quantum circuit of Shor's algorithm in a noisy environment with different level of noise for a certain type of noise channel and present numerical results. We can obtain precise measurements by calculating the state vector prior to measurement, instead of simulating and measuring expending much time, which contributes to higher efficiency. Each experiment is repeated 1000 times to reduce discrepancy. Our research indicates that Shor's algorithm is easily affected by quantum noise. Successful rate of Shor's algorithm decreases exponentially with the increase of noise level in the depolarizing channel, where the successful rate is an indicator we propose in this research to quantify the influence of noise on Shor's algorithm, meanwhile the noise in the state preparation and measurement channel and the thermal relaxation channel can linearly affect the successful rate of Shor's algorithm. There are $O(n^4)$ quantum gates in the circuit, each of which is disrupted by noise in depolarizing channel during running the circuit, meanwhile there are only $O(n)$ interruptions caused by noise in state preparation and measurement channel since we repeat the measurements only $O(n)$ times in the circuit where n is the number of bits of the integer about to be factored. Linear relationship in thermal relaxation channel is mainly due to the large gap between quantum gate time and relaxation time even if each gate in the circuit is disrupted by noise in thermal relaxation channel such as depolarizing channel. The present research results can be used for correcting the subsequent errors, improving Shor's algorithm, and providing guidance for the fidelity required in engineering implementation of Shor's algorithm.

Keywords: quantum computing, quantum algorithm, quantum noise, Shor's algorithm

PACS: 03.67.Ac, 03.67.Dd, 42.50.Lc **DOI:** 10.7498/aps.73.20231414

† Corresponding author. E-mail: yzwu15@fudan.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

量子噪声对Shor算法的影响

黄天龙 吴永政 倪明 汪士 叶永金

Effects of quantum noise on Shor’s algorithm

Huang Tian-Long Wu Yong-Zheng Ni Ming Wang Shi Ye Yong-Jin

引用信息 Citation: Acta Physica Sinica, 73, 050301 (2024) DOI: 10.7498/aps.73.20231414
在线阅读 View online: https://doi.org/10.7498/aps.73.20231414
当期内容 View table of contents: http://wulixb.iphy.ac.cn
