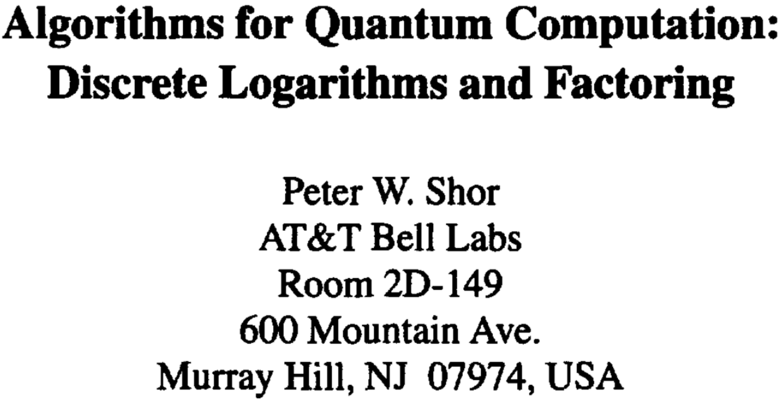
Projeto de Pesquisa
Linguagem de programação quântica

Evandro Chagas Ribeiro da Rosa
Orientador: Rafael de Santiago

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Outubro de 2019



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Qubit

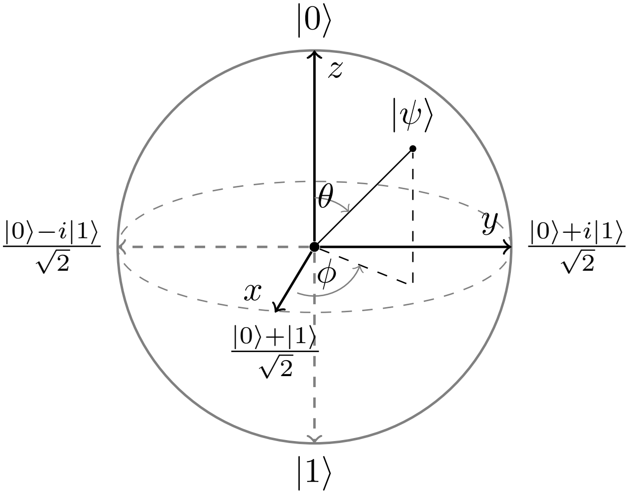


Figura: Esfera de Bloch.

RSA

- Geração das chaves privada (p, q, d) e publica (n, e):
  1. Selecione doi numero primos p e q
  2. $n = pq$
  3. $\phi(n) = \gcd(p-1, q-1)$
  4. Escolha $1 < e < \phi(n)$, onde $\gcd(e, \phi(n)) = 1$
  5. $d \equiv e^{-1} \mod \phi(n)$
- Cifragem: $m^e \equiv c \mod n$.
- Decifragem: $c^d \equiv m \mod n$.

Fatoração

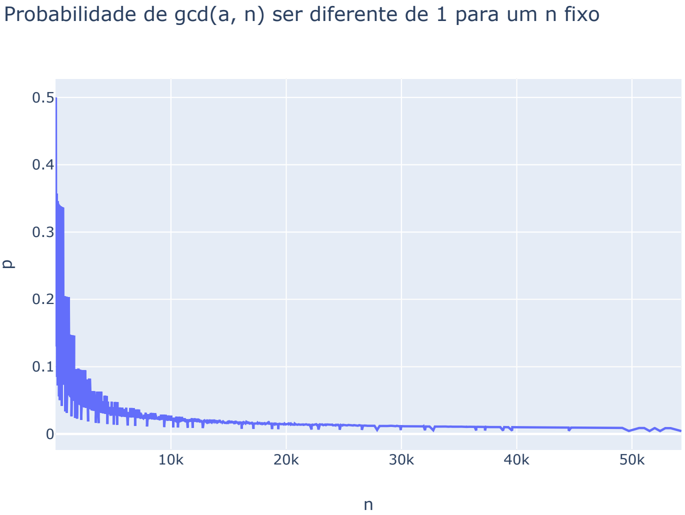
Algoritmo de Shor

$n = p \times q$

1. Seleciona aleatoriamente um $x < n$
2. Se $\gcd(x, n) \neq 1$, então
    - 2.1 $p = \gcd(x, n)$
    - 2.2 $q = \frac{n}{\gcd(x,n)}$
3. Se não, ache r tal que $x^r \equiv 1 \mod n$, então
    - 3.1 Se r for par e $x^{r/2} \not\equiv -1 \mod n$, então
        - 3.1.1 $p = \gcd(x^{r/2} + 1, n)$
        - 3.1.1 $q = \gcd(x^{r/2} - 1, n)$
    - 3.2 Se não, selecione outro x

Fatoração

Algoritmo de Shor



Fatoração

Ideia por traz da redução

$$x^r \equiv 1 \mod n \tag{1}$$

$$x^r - 1 \equiv 0 \mod n \tag{2}$$

$$(x^{r/2}+1)(x^{r/2}-1) \equiv 0 \mod n \tag{3}$$

$$\underbrace{(x^{r/2}+1)}_{p \times a}\underbrace{(x^{r/2}-1)}_{q \times b} = n \times k \tag{4}$$

$$\gcd(p \times a, p \times q) = p \tag{5}$$

$$\gcd(q \times b, p \times q) = q \tag{6}$$

Fatoração

Parte quântica

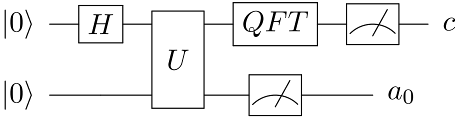


Figura: $U : |a\rangle |0\rangle \to |a\rangle |x^a \mod n\rangle$

Fatoração

Parte quântica

$$s = 2^{\lceil \log_2 n \rceil} \tag{7}$$

$$|0\rangle\,|0\rangle \qquad \xrightarrow{H^{\otimes \lceil \log_2 n \rceil}} \tag{8}$$

$$\frac{1}{\sqrt{s}} \sum_{a=0}^{s-1} |a\rangle\,|0\rangle \qquad \xrightarrow{U} \tag{9}$$

$$\frac{1}{\sqrt{s}} \sum_{a=0}^{s-1} |a\rangle\,|x^a \mod n\rangle \qquad \xrightarrow{\text{mede } 2^{\text{o}} \text{ registrador}} \tag{10}$$

$$\sqrt{\frac{r}{s}} \sum_{k=0}^{s/r-1} |kr + a_0\rangle\,|x^{a_0} \mod n\rangle \qquad \xrightarrow{QFT_{\lceil \log_2 n \rceil}} \tag{11}$$

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{i\theta_{a_0,k}} \left|k\frac{s}{r}\right\rangle \tag{12}$$

Logaritmo discreto

$g^{?} \equiv x \mod p$

- ElGamal encryption.
- Diffie–Hellman key exchange.
- Digital Signature Algorithm (DSA).
- Elliptic curve cryptography.

Logaritmo discreto

Algoritmo de Shor

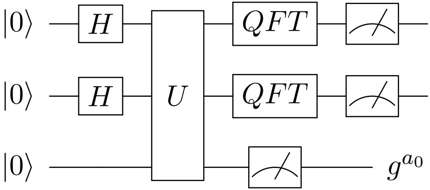


Figura: $U : |a\rangle\,|b\rangle\,|0\rangle \to |a\rangle\,|b\rangle\,|g^a x^b \mod n\rangle$

Logaritmo discreto

$g^r \equiv x \mod p$

$$|0\rangle\,|0\rangle\,|0\rangle \xrightarrow{H^{\otimes 2\lceil \log_2 p\rceil}} \quad (13)$$

$$\frac{1}{p}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}|a\rangle\,|b\rangle\,|0\rangle \xrightarrow{U} \quad (14)$$

$$\frac{1}{p}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}|a\rangle\,|b\rangle\,|g^a x^b \mod n\rangle \xrightarrow{\text{mede ultimo registrador}} \quad (15)$$

$$g^a x^b = g^a (g^r)^b = g^{a_0} \quad (16)$$

$$a + rb \equiv a_0 \mod p \quad (17)$$

$$a \equiv a_0 - rb \mod p \quad (18)$$

Logaritmo discreto

$g^r \equiv x \mod p$

$$\frac{1}{\sqrt{p}}\sum_{b=0}^{p-1}|a_0 - rb\rangle\,|b\rangle \qquad \xrightarrow{QFT^{\otimes 2}_{\lceil \log_2 p\rceil}} \tag{19}$$

$$\frac{1}{\sqrt{p}}\sum_{c=0}^{p-1} e^{i\theta_{a_0,c}}\,|c\rangle\,|d \equiv rc \mod p\rangle \tag{20}$$

$$c \neq 0 \Rightarrow r \equiv dc^{-1} \mod p \tag{21}$$

Fatorando RSA de 2048 bit

Premissas

- Qubits em uma grade, comunicando apenas com os vizinhos.
- Porta quântica com erro de 10^{-3}.
- Código de superfície com atualização de 1 μs

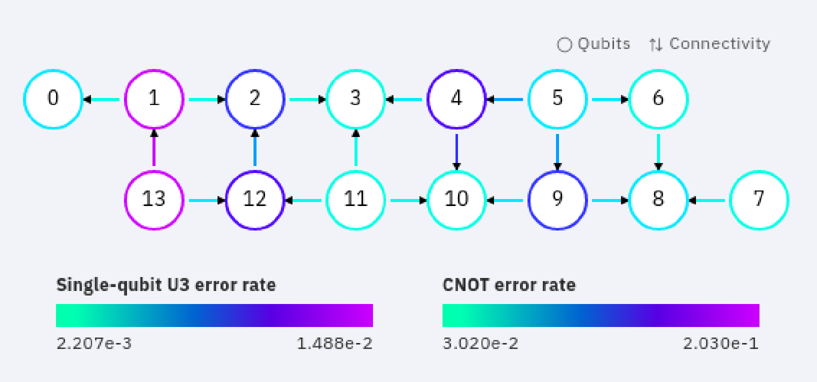


Figura: ibmq_16_melbourne

Fatorando RSA de 2048 bit

Algoritmo

- Reduzir o problema da fatoração para o logaritmo discreto.
  - Diminui o numero de multiplicações.
  - Maior probabilidade (99%) de obter o valor desejado.
- Exponenciação modular.
  - Multiplicação modular controlada.
  - Adição modular.
- Número de qubits lógicos: $3n + 0,002n \log_2 n$.
  - 6.190 qubits.
- Número de portas Toffoli: $0,3n^3 + 0,0005n^3 \log_2 n$.
  - 2.624.225.018 portas Toffoli.
- Número de portas CNOT: $1,78n^3 + 0,003n^3 \log_2 n$.
  - 15.745.350.108 portas CNOT.

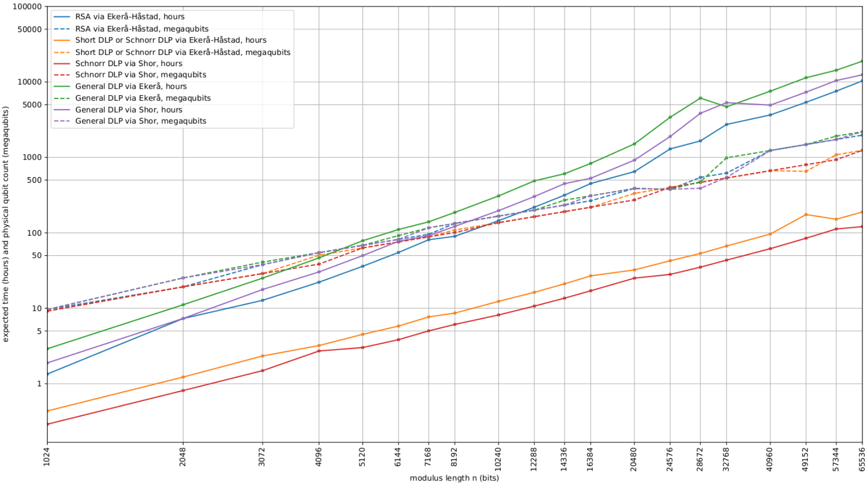
Fatorando RSA de 2048 bit

Correção de erro

- Grade de qubits lógicos: $\frac{113n}{1024} \times 63$.
    - $226 \times 63 = 8.136$ qubits lógicos.
- Tempo de execução aproximado: $0.15n^2 \cdot 37$ms
    - $\approx$ 7h
- Código superfície com $d = 27$
    - $30\% \sim 50\%$ erro.
- Número de qubits físicos: n. qubits lógicos $\times 2(d+1)^2$.
    - $226 \times 63 \times 1568 = 22.325.184$ qubits.

Fatorando RSA de 2048 bit

Escalabilidade



Onde estamos

Onde estamos

Número de qubits

Companhia	Atual	Proximo objetivo
Intel	49	TBD
Google	72	TBD
IBM	43	TBD
Rigetti	16	128
USTC	10	20
IonQ	11	79

Fonte: Quantum Computing Report (18/09/2019).

Referencias

- P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, in Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, p. 124–134.
- P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing, vol. 26, nº 5, p. 1484–1509, 1997.
- Proos e C. Zalka, “Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves”, Quantum Info. Comput., vol. 3, nº 4, p. 317–344, jul. 2003.
- C. Gidney e M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, arXiv:1905.09749 [quant-ph], maio 2019.