

Criptografía post-cuántica basada en retículos

Lección 3: Minicurso Mar del Plata, Noviembre 2025

Syllabus

- Criptografía post-cuántica (PQC)
- Ordenador cuantico: Qubits y registro
- Algoritmo de Shor
- Logaritmo discreto



Índice

3.5 Criptografia post-cuantica	3
3.5.1 Ordenador Cuantico	4
3.5.1.1 Registro de n Qubit: Notación de Dirac, Bra-Ket, de la mecanica cuantica	7
3.5.1.2 Operaciones y programas cuanticos	8
3.6 Algoritmo de Shor : funciones periodicas y transformada de Fourier	9
3.6.0.1 Transformada de Fourier	9
3.6.1 Como utilizarlo para resolver el Logaritmo Discreto	11
Referencias	12

3.5 Criptografia post-cuantica

Se trata de algoritmos ejecutables en computadoras clasicas que logran desbalancear la complejidad incluso asumiendo que el atacante poseea una computadora cuantica.

Es decir, esquemas criptograficos ejecutables en maquinas clasicas resistentes al ataque de un enemigo que poseea un maquina cuantica (y maquinas clasicas tambien).

3.5.1 Ordenador Cuantico

Similarmente a un ordenador clasico el ordenador cuantico posee una memoria (registros), operaciones que permiten cambiar el estado de los registros y programas compuestos de dichas operaciones.

La diferencia esencial, o quizas el cambio de paradigma, con el ordenador clasico consiste en:

- el registro, o los registros, contiene una distribucion de probabilidad,
- las operaciones cambian dichas distribuciones de probabilidad,
- el resultado de la lectura del registro sigue la distribucion de probabilidad contenida en el registro,
- despues de la lectura del registro, la distribucion en el registro cambia y se concentra en el estado del resultado de la lectura

De modo analogo a un registro clásico formado de Flip-Flops el registro cuántico está formado de Qubits.

3.5.1.1 Registro de un solo qubit

El registro contiene vectores unitarios (versores) \mathbf{v} de un espacio vectorial complejo V de dimensión dos.

Dos versores (perpendiculares) de una base de V , **cero** y **uno**, representan las dos posibles lecturas del registro,

Si leo el registro que contiene $\mathbf{v} \in V$ entonces el resultado de la lectura es :

cero con probabilidad p^2

uno con probabilidad q^2

donde p, q son las coordenadas de \mathbf{v} respecto a la base **cero**, **uno**, i.e.

$$\mathbf{v} = p \cdot \mathbf{cero} + q \cdot \mathbf{uno}$$

Si el resultado de la lectura es **cero** el nuevo contenido del registro es una distribución concentrada en **cero** en caso contrario leo **uno** y el estado del registro pasa a ser la distribución concentrada en **uno**.

NOTE 3.5.1.2

Si el registro contiene el vector

$$\mathbf{v} = p \cdot \mathbf{cero} + q \cdot \mathbf{uno}$$

se dice que describe la física de la **superposición** (superposition) de los dos estados **cero** y **uno**.

3.5.1.3 Registro de dos qubits

El registro contiene vectores unitarios (versores) \mathbf{v} del producto tensorial $V \otimes V$ de dimension cuatro.

Los dos vectores **cero** y **uno** de V crean los cuatro posibles lecturas del registro:

$$\mathbf{cero} \otimes \mathbf{cero}, \mathbf{cero} \otimes \mathbf{uno}, \mathbf{uno} \otimes \mathbf{cero}, \mathbf{uno} \otimes \mathbf{uno}$$

Si leo el registro que contiene $\mathbf{v} \in V$ entonces el resultado de la lectura es :

$$\mathbf{cero} \otimes \mathbf{cero} \text{ con probabilidad } p_1^2$$

$$\mathbf{cero} \otimes \mathbf{uno} \text{ con probabilidad } p_2^2$$

$$\mathbf{uno} \otimes \mathbf{cero} \text{ con probabilidad } p_3^2$$

$$\mathbf{uno} \otimes \mathbf{uno} \text{ con probabilidad } p_4^2$$

donde p_1, p_2, p_3, p_4 son las coordenadas de \mathbf{v} respecto a la base de productos tensoriales, i.e.

$$\mathbf{v} = p_1 \cdot \mathbf{cero} \otimes \mathbf{cero} + p_2 \cdot \mathbf{cero} \otimes \mathbf{uno} + p_3 \cdot \mathbf{uno} \otimes \mathbf{cero} + p_4 \cdot \mathbf{uno} \otimes \mathbf{uno}$$

Si el resultado de la lectura es **cero** \otimes **cero** el nuevo contenido del registro es la distribucion concentrada en **cero** \otimes **cero** y analogamente en el caso de las otras posibles lecturas.

NOTE 3.5.1.4

El producto tensorial $V \otimes V$ captura la fisica del **entrelazamiento** (entanglement) fisico de dos qubits. El estado \mathbf{v} del registro representa un entrelazamiento de los dos qubits cuando no se puede factorizar $\mathbf{v} = \mathbf{a} \otimes \mathbf{b}$ en dos estados $\mathbf{a}, \mathbf{b} \in V$.

3.5.1.1 Registro de n Qubit: Notación de Dirac, Bra-Ket, de la mecanica cuantica

Para simplificar la generalización a un registro con n qubits en la literatura se utiliza la notación de Dirac:

- **un Ket es un vector:** e.g. $|\mathbf{v}\rangle = \mathbf{v}$ o

$$|0\rangle = \text{cero}, |1\rangle = \text{uno}$$

para los dos estados de la base de V .

- **Producto tensorial:**

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle$$

o en el caso de $V \otimes V$:

$$|00\rangle = \text{cero} \otimes \text{cero}$$

$$|01\rangle = \text{cero} \otimes \text{uno}$$

$$|10\rangle = \text{uno} \otimes \text{cero}$$

$$|11\rangle = \text{uno} \otimes \text{uno}$$

El estado de un registro de n qubits es un vector $|\mathbf{v}\rangle$ del producto tensorial

$$V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n \text{ veces}}.$$

El resultado de la lectura del registro sera entonces uno de los 2^n vectores de la base:

$$|00\cdots 00\rangle, |00\cdots 00\rangle, \dots, |11\cdots 10\rangle, |11\cdots 11\rangle$$

NOTE 3.5.1.5

Un estado del registro es entonces una combinación lineal de los vectores de esta base.

3.5.1.2 Operaciones y programas cuanticos

Una operación, tambien conocida como *gate* o *puerta cuantica* que cambia el estado del registro, es un operador lineal unitario \mathbf{U} del espacio $V^{\otimes n}$. Es decir, una matriz \mathbf{U} unitaria.

Un programa es un secuencia de operaciones i.e. $\mathbf{U}_1 \mathbf{U}_2 \cdots \mathbf{U}_k$ aplicadas a un estado inicial del registro, combinadas con lecturas.

3.5.1.6 Operador de Hadamard

El operador de Hadamard (H) en forma matricial se define como:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Aplicando el operador de Hadamard al estado inicial $|v\rangle = |0\rangle$ se logra poner en el registro el estado en superposicion:

$$\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$$

La importancia del operador de Hadamard es que permite poner el registro en un estado de superposicion donde todas las lecturas son equiprobables.

NOTE 3.5.1.7

Tensorizando $H^{\otimes n} := H \otimes H \otimes \cdots \otimes H$ se obtiene un operador de Hadamard de $V^{\otimes n}$ que permite poner el registro en un estado de superposicion y entrelazamiento donde todas las lecturas son equiprobables.

3.6 Algoritmo de Shor : funciones periodicas y transformada de Fourier

3.6.0.1 Transformada de Fourier

Un periodo p de una función $f : G \rightarrow A$, por definición, satisface

$$f(x + p) = f(x)$$

para todos los valores de x .

El algoritmo de Shor [Sho94] implementa una versión de transformada de Fourier \hat{f} debido a una propiedad fundamental de \hat{f} que relaciona su soporte con los períodos de f .

Gracias a esta relación *periodos de f -soporte de \hat{f}* el cálculo de los períodos de f será eficientemente.

El registro cuántico contendrá el gráfico $(x, f(x))$ de la función f del siguiente modo:

En el producto tensorial $V^{\otimes n} \otimes V^{\otimes n}$ los argumentos x van a estar en el primer factor $V^{\otimes n}$ y los valores $f(x)$ en el segundo $V^{\otimes n}$.

Utilizando las operaciones cuánticas transformaremos el gráfico $(x, f(x))$ en el gráfico de su transformada $(x, \hat{f}(x))$ y al final se efectuará la lectura del primer registro.

Aquí el pseudocódigo :

3.6.0.1 Shor's Algorithm

$ v\rangle \leftarrow 00\cdots 00\rangle \otimes 00\cdots 00\rangle$	\triangleright (estado inicial del registro cuántico)
$ v\rangle \leftarrow \sum_{x \in G} \frac{1}{\sqrt{ G }} \cdot x \otimes 00\cdots 00\rangle$	\triangleright (Operador de Hadamard)
$ v\rangle \leftarrow \sum_{x \in G} \frac{1}{\sqrt{ G }} \cdot x \otimes f(x)$	\triangleright (Operador adecuado)
$ v\rangle \leftarrow \sum_{x \in G} \frac{1}{\sqrt{ G }} \cdot x \otimes \hat{f}(x)$	\triangleright (Operador transformada-Fourier)
$ v\rangle \leftarrow x_0$	\triangleright (lectura del primer factor del registro)

La probabilidad de leer x_0 , antes de la lectura en el último paso, era

dada

$$\frac{|\widehat{f}(x_0)|}{\sqrt{|G|}}$$

y es distinta de cero solo si x_0 pertenece al soporte de \widehat{f} .

NOTE 3.6.0.2

Es un hecho del análisis armónico commutativo que la transformada de Fourier $\widehat{f}(x)$ es cero en x si x no es un múltiplo entero de la frecuencia $\frac{1}{p}$ de f . Aquí doy unos detalles de este cálculo:

$$\begin{aligned}\widehat{f}(x) &= \int_{g \in G} e^{i2\pi \cdot x \cdot g} \cdot f(g) \, dg = \\ &= \int_{\tilde{g} \in G} e^{i2\pi \cdot x \cdot (\tilde{g} + p)} \cdot f(\tilde{g} + p) \, d\tilde{g} = && \text{(cambio de variable } g = \tilde{g} + p\text{)} \\ &= \int_{\tilde{g} \in G} e^{i2\pi \cdot x \cdot \tilde{g}} \cdot e^{i2\pi \cdot x \cdot p} \cdot f(\tilde{g}) \, d\tilde{g} = \\ &= e^{i2\pi \cdot x \cdot p} \cdot \widehat{f}(x)\end{aligned}$$

de donde se concluye que si x no es un múltiplo entero de la frecuencia $\frac{1}{p}$ de f entonces

$$\widehat{f}(x) = 0 .$$

Es decir, la lectura x_0 permitirá calcular la frecuencia $\frac{1}{p}$ y por lo tanto el periodo p de f .

3.6.1 Como utilizarlo para resolver el Logaritmo Discreto

En esta sección explico como utilizar el cálculo eficiente de períodos para factorizar un número N . Antes de empezar subrayo que esto era conocido por Gauss quien dedicó el famoso trabajo, *Disquisitiones Arithmeticae*, a la aritmética definiendo los anillos modulares \mathbb{Z}_N y demostrando varios teoremas fundamentales.

La observación clave para factorizar N es obtener una solución w no trivial de la ecuación :

$$x^2 = 1 \pmod{N}$$

no trivial significa que $w \neq 1, -1 \pmod{N}$.

Dada una w , no trivial, para calcular un factor de N basta calcular el $d = \text{m.c.d}(w - 1, N)$.

Efectivamente si $d = 1$ entonces N tendría que dividir a $w + 1$ lo que implicaría que

$$w = -1 \pmod{N}$$

y w sería trivial. De modo similar si $d = N$ entonces $w = 1 \pmod{N}$ y de nuevo w sería trivial.

Suponemos entonces que tenemos una computadora cuántica que calcula rápidamente el período r de una función $f(x)$. Para factorizar N vamos a considerar la función periódica $f : \mathbb{Z} \rightarrow \mathbb{Z}_N$ definida como

$$f(x) := a^x \pmod{N}$$

Usando r calcularemos una solución no trivial w de $x^2 = 1 \pmod{N}$.

Tener presente que si r es el período de f entonces $a^r = 1 \pmod{N}$.

3.6.1.1 Factorizando N

$$a \xleftarrow{\$} \mathbb{Z}_N$$

$$r \leftarrow \text{QuaComPeriodo}(a, N)$$

\triangleright Calcula el período de $f(x) = a^x$

Si r es par continuar sino repetir

\triangleright busca una $f(x) = a^x$ cuyo período sea par

$$k \leftarrow \frac{r}{2}$$

$$w \leftarrow a^k \pmod{N}$$

\triangleright w resto de a^k dividido N

$$d \leftarrow \text{m.c.d}(w - 1, N)$$

return d

\triangleright Con alta probabilidad un factor no trivial de N

Referencias

- [FS21] Francesco Stocco, *A theoretical approach to Shor's Algorithm and Quantum Bits* <https://www.youtube.com/watch?v=-k5B0QPsFdA>
- [Di23] Antonio J. Di Scala, *Quantum Computers' Role in Shor's Algorithm* <https://qubip.eu/the-role-of-quantum-computers-in-shors-algorithm/>
- [Sho94] P.W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*. In Proceedings 35th Annual Symposium on Foundations of Computer Science, pages 124–134, 1994.
- [QUBIP23] QUBIP: *Transition to Post-Quantum Cryptography*
QUBIP project is co-funded by the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].
<https://qubip.eu/>
<https://github.com/QUBIP>
http://www.youtube.com/@qubip_eu