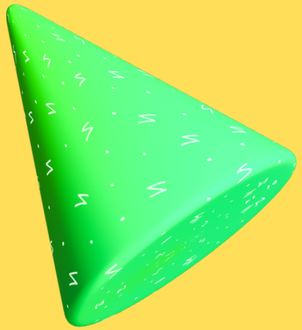
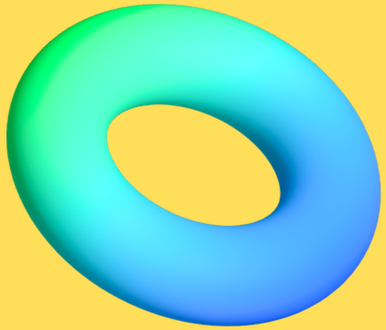
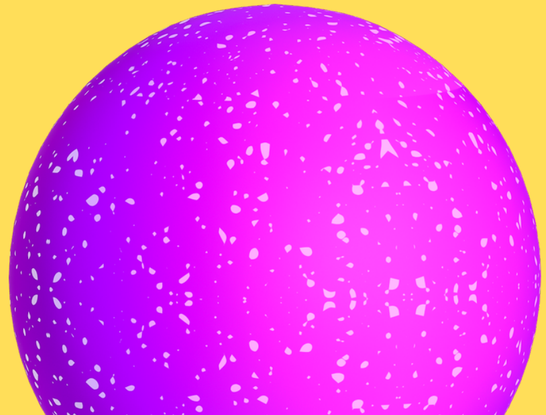
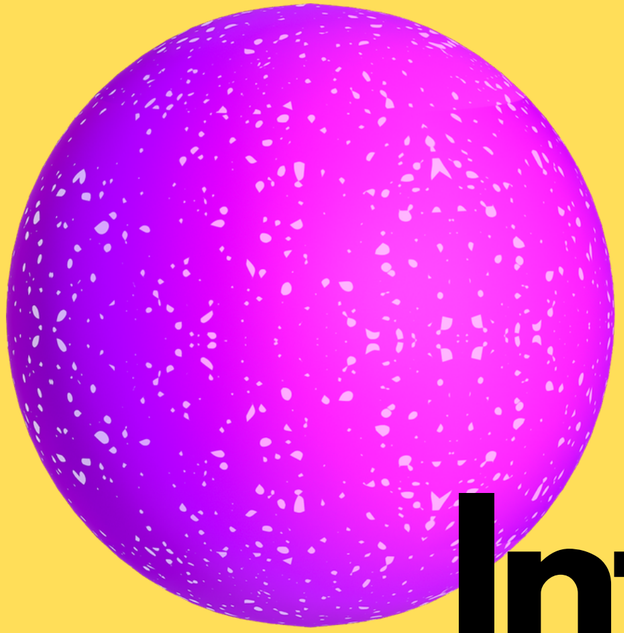
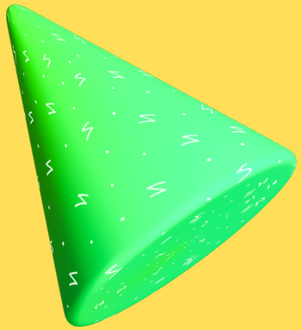
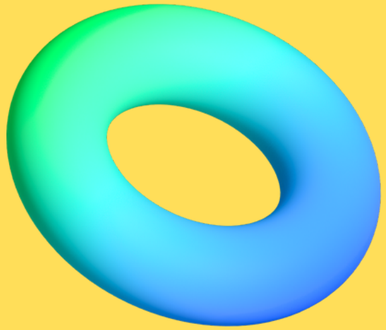
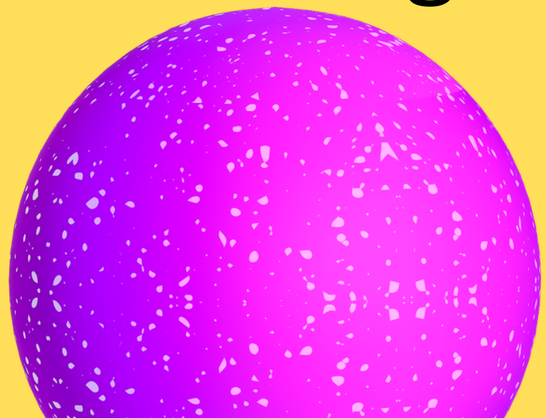





Implementation of Shor's Algorithm

Lai, Chia-Tso

What is Shor's Algorithm?

- Quantum algorithm that factorizes a large integer N into prime factors
- Extremely demaniding task for a classical computer (runtime O(N))
- Exponential speedup on a quantum computer: O(logN)
- Superposition enables parallel computation of multiple states

Introduction to Shor's Algorithm

From Factorizing to Period Finding

Factorization

TWO INTEGERS A&B COPRIME (NO COMMON FACTOR)

$$A^p = mB + 1$$

$$7^4 = 160 \cdot 15 + 1$$

$$42^3 = 5699 \cdot 13 + 1$$

SIMILARYLY, WE CAN TAKE A RANDOM GUESS AND RAISE IT TO A POWER P

$$g^p = mN + 1 \Rightarrow g^p - 1 = mN \Rightarrow (g^{p/2} + 1)(g^{p/2} - 1) = mN$$

BETTER GUESS!

EITHER A FACTOR OF N OR SHARES FACTORS WITH N

GREATEST COMMON DIVISOR

$$gcd(g^{p/2} + 1, N)$$

$$gcd(g^{p/2} - 1, N)$$

Factorization

A BETTER STRATEGY:

LOOK FOR POWER P!

$$g^p \mod N = 1$$

GOAL OF SHOR'S ALGORITHM!

Factorization

SOME PROBLEMS:

1

POWER P IS ODD → $g^{\frac{p}{2}}+1 \quad g^{\frac{p}{2}}-1$

2

$$\begin{aligned} g^{p/2}+1 &= aN \\ (g^{p/2}-1)a &= m \end{aligned}$$

→ **SHARE NO COMMON FACTOR WITH N**

EMPIRICALLY SPEAKING, 37.5% OF THE TIME THESE PROBLEMS DO NOT OCCUR

→ **SIMPLY TAKE ANOTHER GUESS**

Period Finding

$$g^p \mod N = 1$$

SHOR'S ALGORITHM TURNS THE PROBLEM OF FACTORIZATION INTO A PERIOD FINDING PROBLEM

$$\begin{cases} g^p = m_1 N + 1 \\ g^x = m_r N + r \end{cases}$$

TAKE X+P AS THE POWER

$$g^{x+p} = (m_r N + r)(m_1 N + 1) = MN + r$$

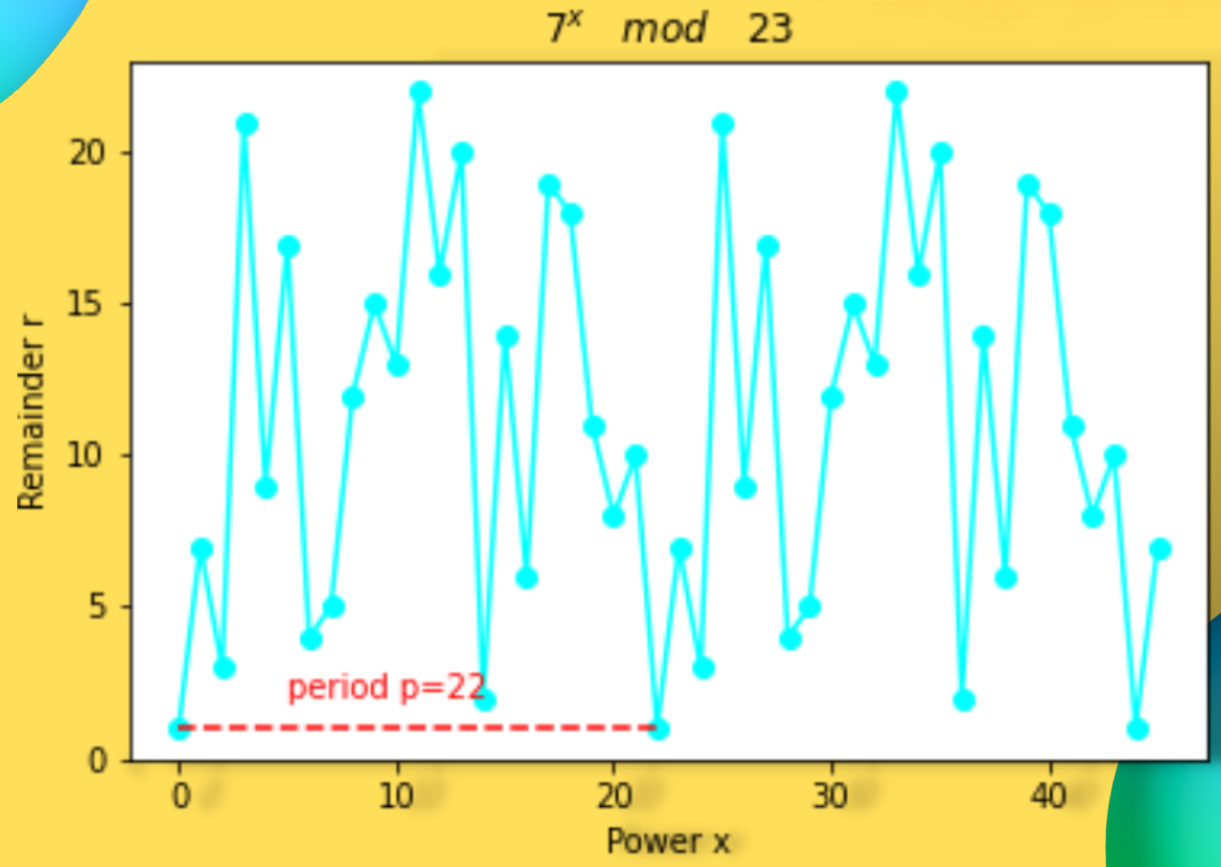
$$g^{x+p} \mod N = r$$

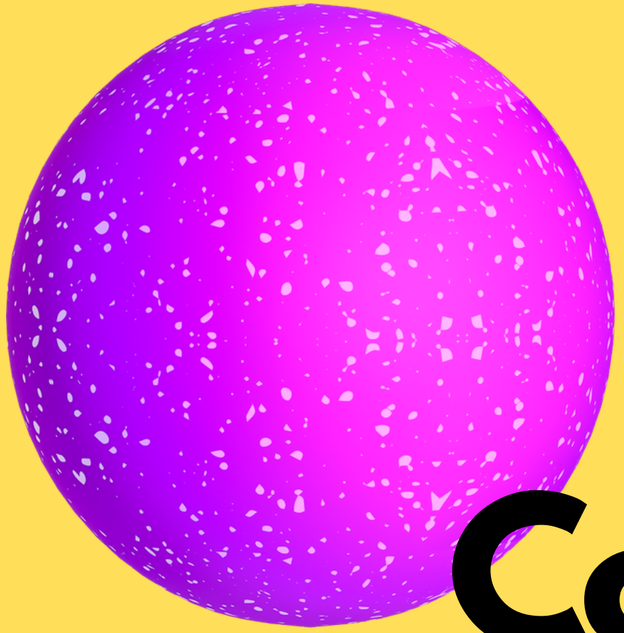
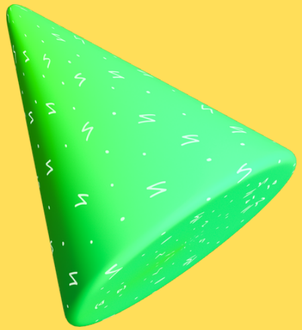
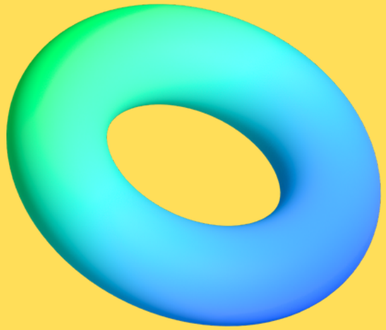
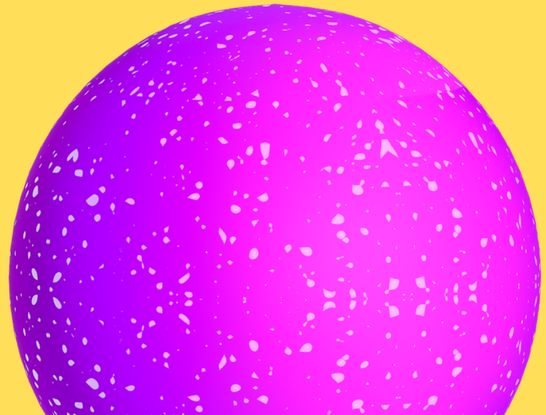
A SHIFT OF P IN POWER DOES NOT CHANGE THE VALUE OF THE MODULO OPERATION!

Period Finding

$$g^p \mod N = 1$$

THE POWER HAS A REPEATING PROPERTY → **P IS THE PERIOD!**



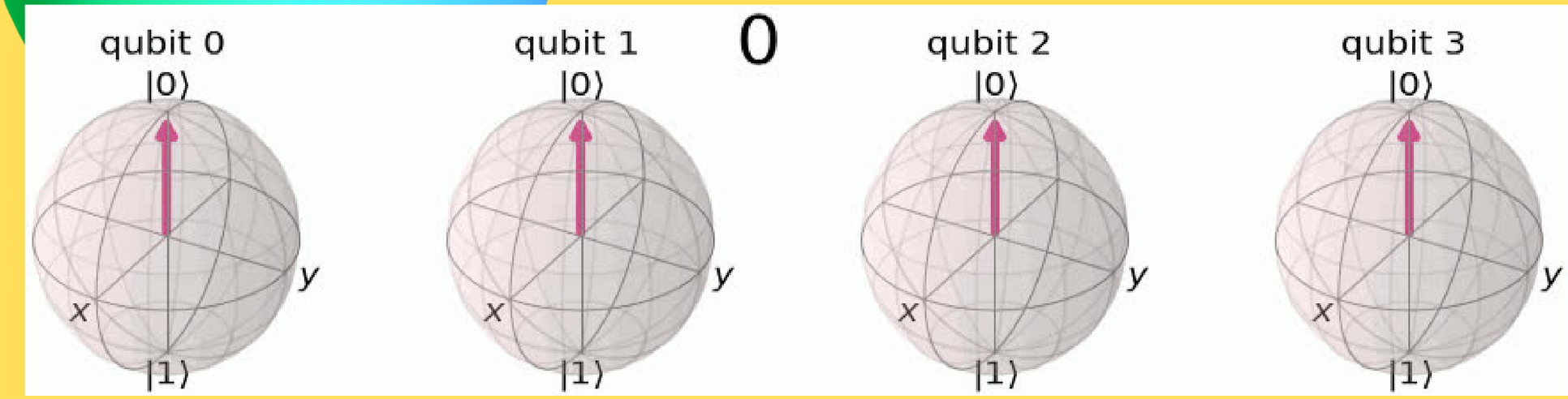





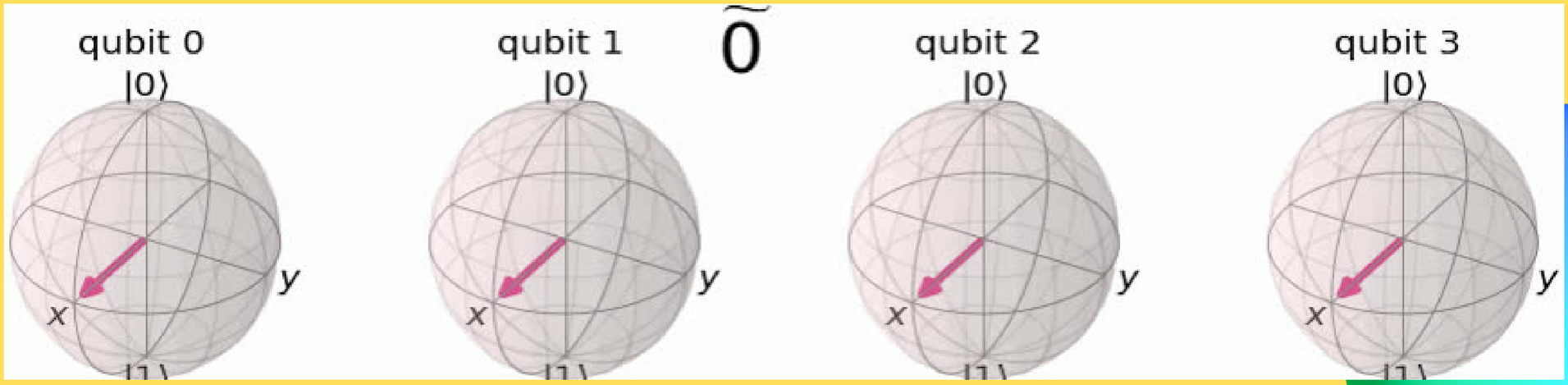
Components of Shor's Algorithm

QFT, QPE, Modular Exponentiation

Quantum Fourier Transform

MAPS THE QUBITS FROM COMPUTATIONAL BASIS TO FOURIER BASIS. **E.X. 1-QUBIT QFT:** $H|0\rangle = |+\rangle$





Quantum Fourier Transform

$$QFT : |x\rangle \rightarrow \ |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w_N^{xy} |y\rangle \ , \ w_N = e^{\frac{2\pi i}{N}}$$

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} (|0\rangle + e^{\frac{2\pi i x}{2^k}}|1\rangle)$$

$$|x\rangle = |x_1\rangle \otimes \ |x_2\rangle \ldots \otimes |x_n\rangle$$
$$x = 2^{n-1}x_1 + 2^{n-2}x_2 + \ldots + x_n$$

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w_N^{xy} |y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i (\sum_{k=1}^{n} \frac{y_k}{2^k}) x} |y_1 y_2 \ldots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y_k}{2^k}} |y_1 y_2 \ldots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} (\sum_{y_1=0}^{1} e^{\frac{2\pi i x y_1}{2}} |y_1\rangle) \otimes \ (\sum_{y_2=0}^{1} e^{\frac{2\pi i x y_2}{2^2}} |y_2\rangle) \otimes \ldots \otimes (\sum_{y_n=0}^{1} e^{\frac{2\pi i x y_n}{2^n}}) |y_n\rangle)$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} (|0\rangle + e^{\frac{2\pi i x}{2^k}}|1\rangle)$$

Quantum Fourier Transform

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} (|0\rangle + e^{\frac{2\pi i x}{2^k}}|1\rangle)$$

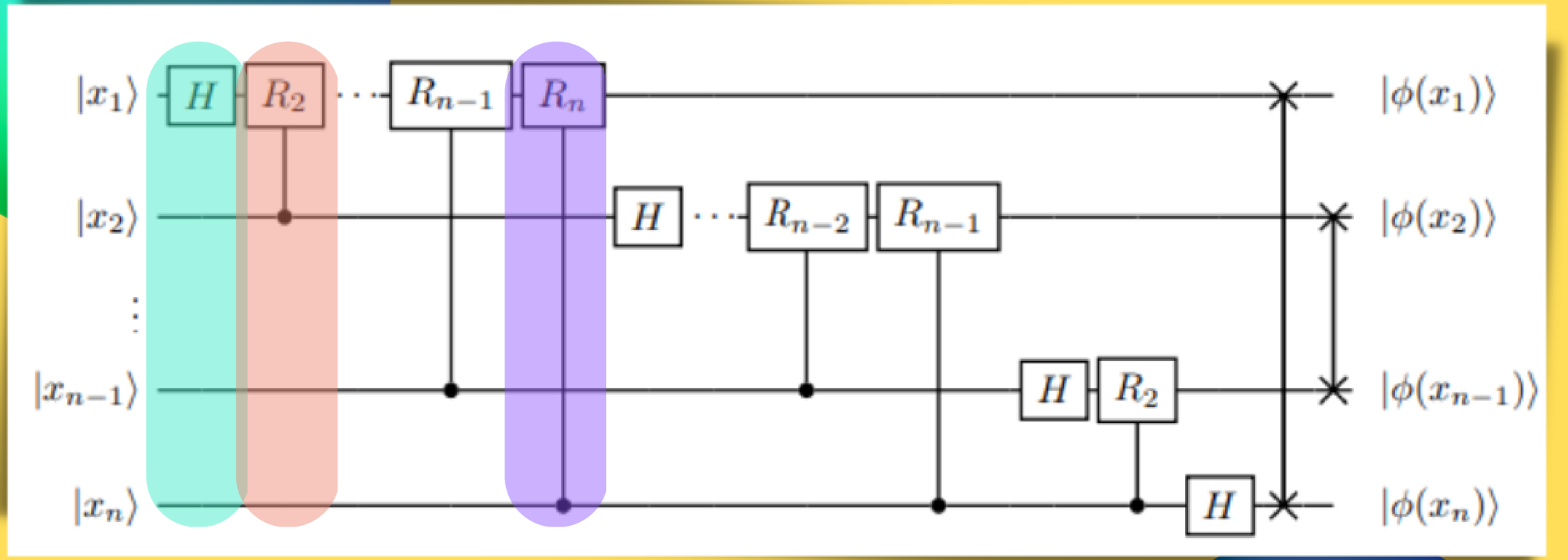
1. **HADAMARD GATES: FLIP THE QUBITS TO X-Y PLANE**
2. **PHASE GATES: ASSIGN A CERTAIN PHASE TO EACH QUBIT**

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

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

$$CR_k|x_1 x_2\rangle = |x_1\rangle \otimes e^{\frac{2\pi i x_1}{2^k}}|x_2\rangle$$

Quantum Fourier Transform



$$H|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi i x_1}{2}}|1\rangle)$$

$$CR_2H|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi i(2x_1+x_2)}{2^2}}|1\rangle)$$

$$CR_2 \ldots R_nH|x_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle) = |\tilde{x_n}\rangle$$

Quantum Phase Estimation

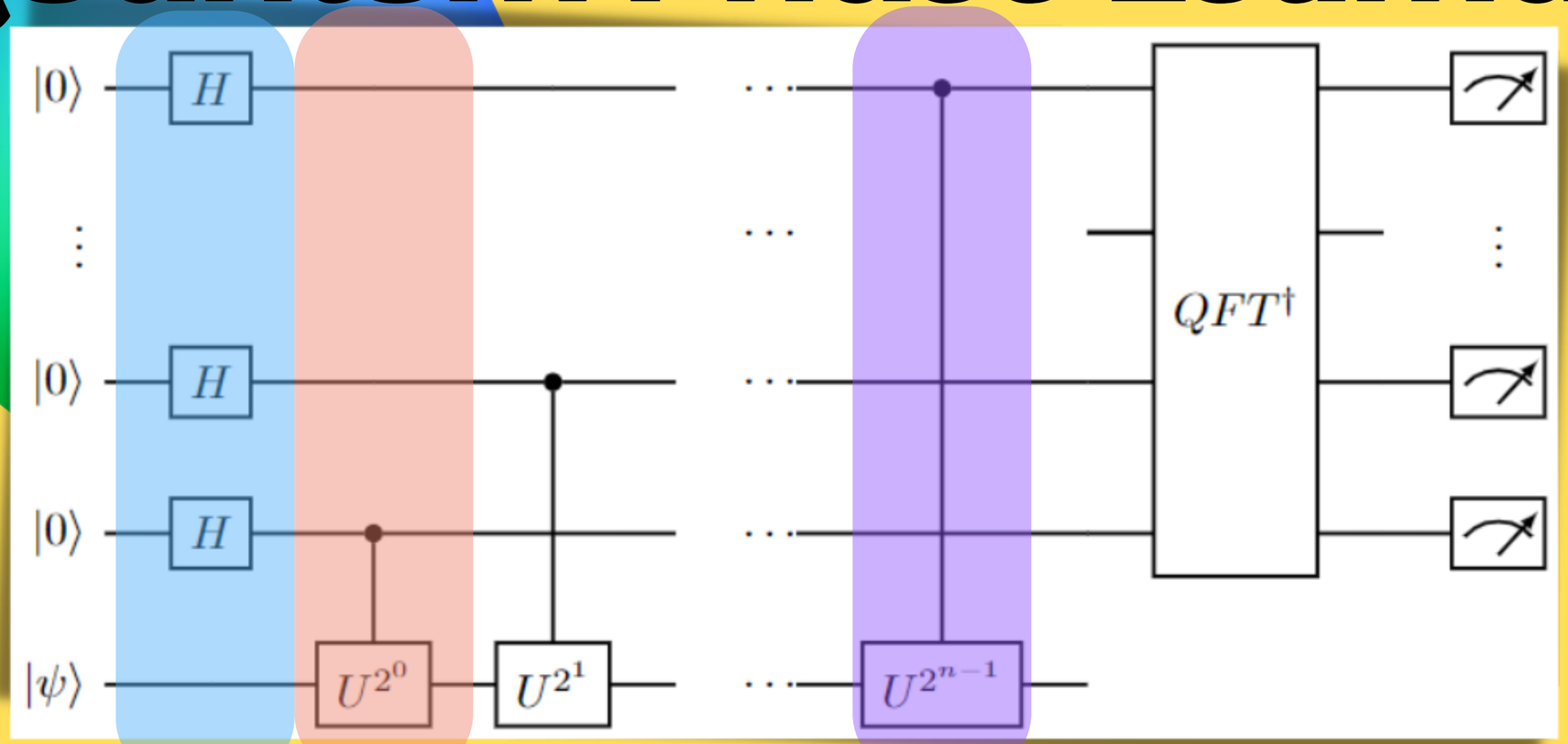
*COMPUTES THE PHASE OF THE EIGENVALUE OF A GIVEN UNITARY OPERATOR AND ITS EIGENVECTOR.

*THE PERIOD OF POWER P IS ENCODED IN THE PHASE OF A SPECIFIC UNITARY OPERATOR.

*THE CONSTRUCTION OF QPE EXPLOITS ITS RESEMBLANCE TO QFT.

$$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$$

Quantum Phase Estimation



$$|x\rangle \equiv |2^n\theta\rangle$$

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} (|0\rangle + e^{\frac{2\pi i x}{2^k}}|1\rangle)$$

$$(\frac{1}{\sqrt{2}})^n (|0\rangle + |1\rangle)^{\otimes n} |\psi\rangle$$

$$(\frac{1}{\sqrt{2}})^n (|0\rangle + e^{2\pi i\theta \cdot 2^{n-1}}|1\rangle) \otimes (|0\rangle + e^{2\pi i\theta \cdot 2^{n-2}}|1\rangle) \otimes \ldots (|0\rangle + e^{2\pi i\theta \cdot 2^0}|1\rangle)|\psi\rangle$$

$$(\frac{1}{\sqrt{2}})^n (|0\rangle + |1\rangle)^{\otimes n-1} \otimes (|0\rangle|\psi\rangle + |1\rangle e^{2\pi i\theta \cdot 2^0}|\psi\rangle)$$

Modular Exponentiation

$$a^k \mod N$$

*THE GREATEST CHALLENGE IN BUILDING THE CIRCUIT OF SHOR'S ALGORITHM.

*TAKES MANY QUBITS AND GATES TO OPERATE ONE COMPUTATION

*CONSIDER THE UNITARY TRANSFORMATION:

$$U|x\rangle = |ax \ mod \ N\rangle$$

*TAKE THE INITIAL STATE |X> TO BE |1> AND APPLY U FOR MULTIPLE TIMES:

$$U^r|1\rangle = |a^r \ mod \ N\rangle = |1\rangle$$

Modular Exponentiation

$$a^k \mod N$$

***A SUPERPOSITION OF ALL THE BASIS STATES WITHIN ONE CYCLE WOULD BE AN EIGENSTATE OF U**

$$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \ mod \ N\rangle$$

***TO GENERALIZE, ADDITIONAL PHASES CAN BE INTRODUCED TO EACH BASIS STATE:**

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi iks}{r}} |a^k \ mod \ N\rangle \qquad s \in \mathbb{Z} \ , \ 0 \leq s \leq r-1$$

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{2\pi is}{r}} e^{\frac{-2\pi i(k+1)s}{r}} |a^{k+1} \ mod \ N\rangle = e^{\frac{2\pi is}{r}} |u_s\rangle$$

Modular Exponentiation

$$a^k \mod N$$

***IF WE SUM UP ALL THE POSSIBLE EIGENSTATES, ALL TERMS CANCEL OUT EXCEPT FOR |1> (K=0)**

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i k s}{r}} |a^k \ mod \ N\rangle$$

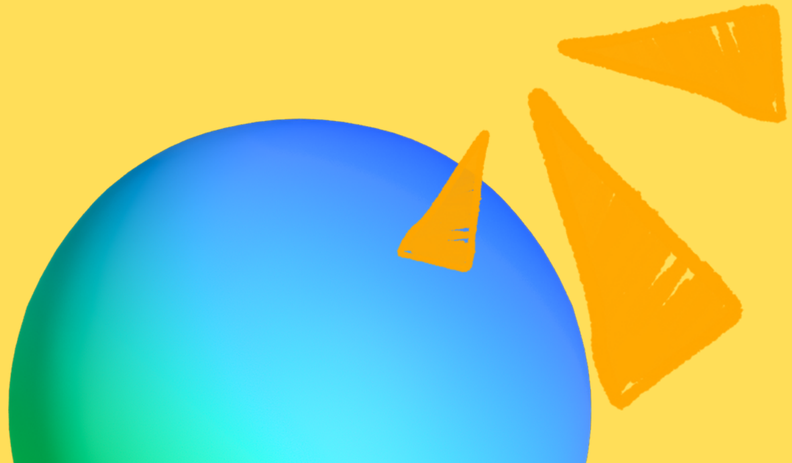
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$$

$$U|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{\frac{2\pi i s}{r}} |u_s\rangle$$

***IF QPE IS APPLIED TO U & |1>:**

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |2^n \frac{s}{r}\rangle$$

SHOR'S ALGORITHM IS NOTHING BUT QPE OF MODULAR EXPONENTIATION IN DISGUISE!



Complete Layout of Shor's Algorithm

***THE PERIOD FOR FACTORIZATION CAN BE DERIVED FROM EXECUTING QPE ON A SPECIFIC U:**

$$U^k|1\rangle = |a^k \mod N\rangle$$

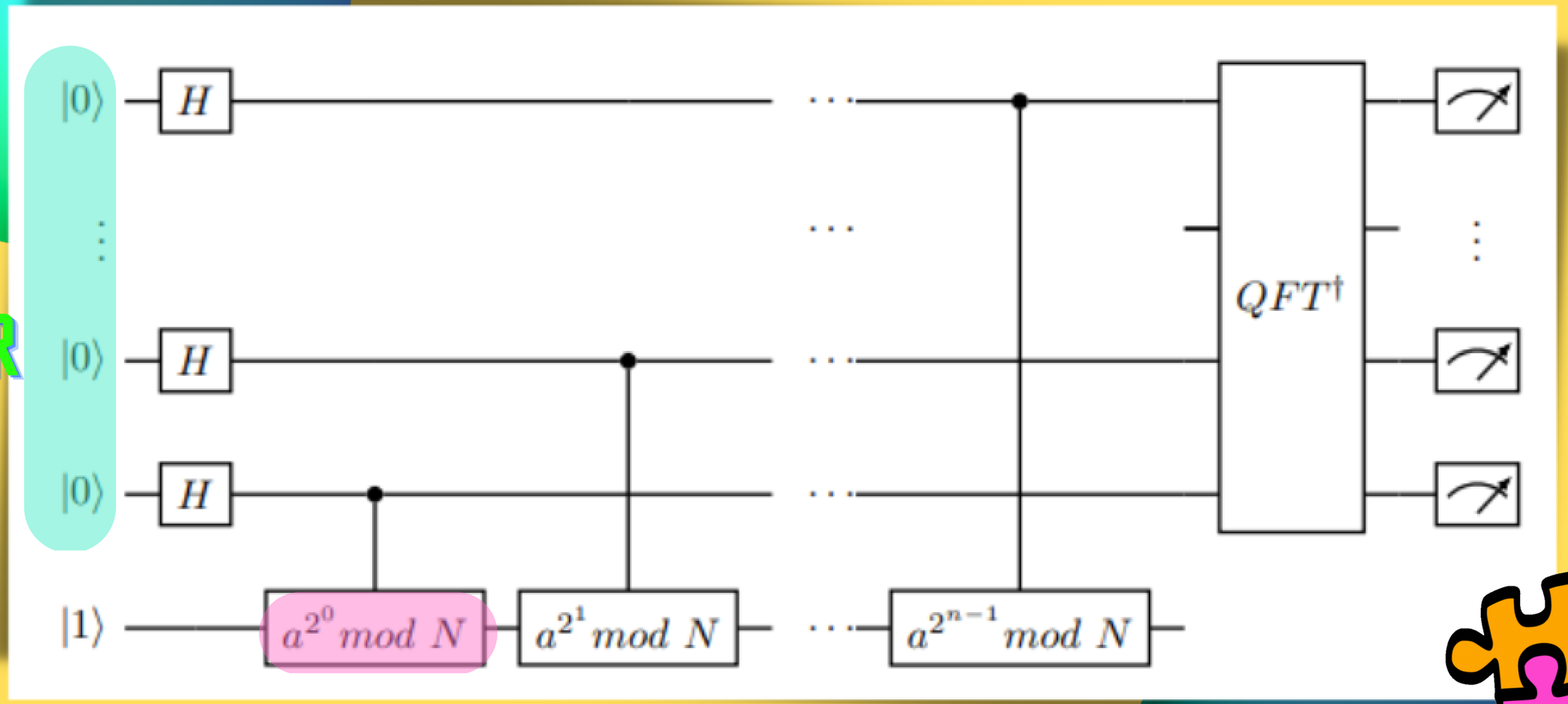
$$U^k \equiv a^k \mod N$$

***MODULAR EXPONENTIATION CAN BE REALIZED AS A SERIES OF CONTROLLED GATES:**

$$U^k = U^{2^0 k_n} U^{2^1 k_{n-1}} \ldots U^{2^{n-1} k_1}$$

CONTROLLED QUBITS

Complete Layout of Shor's Algorithm

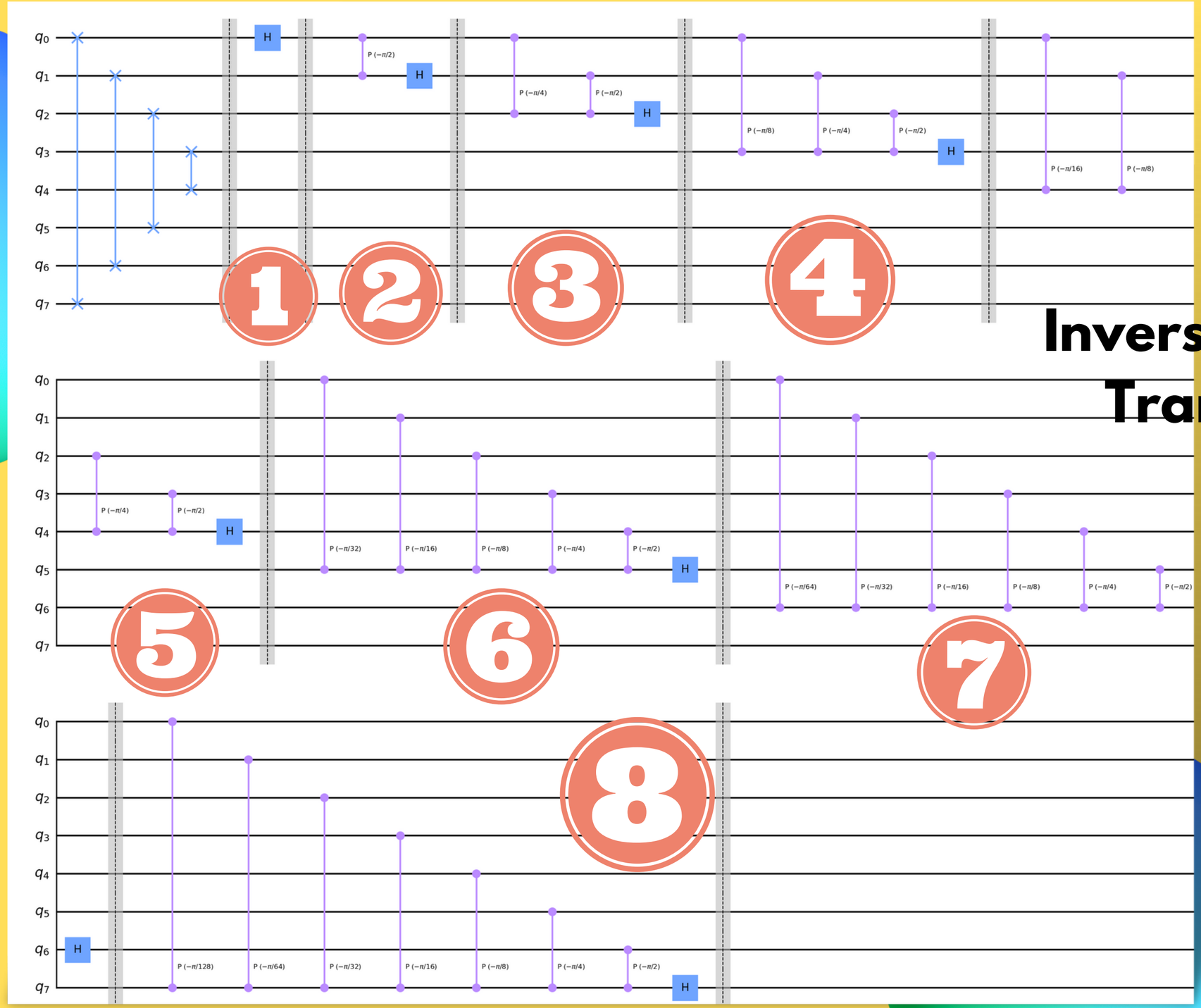


POWER

U

Implementation with Qiskit

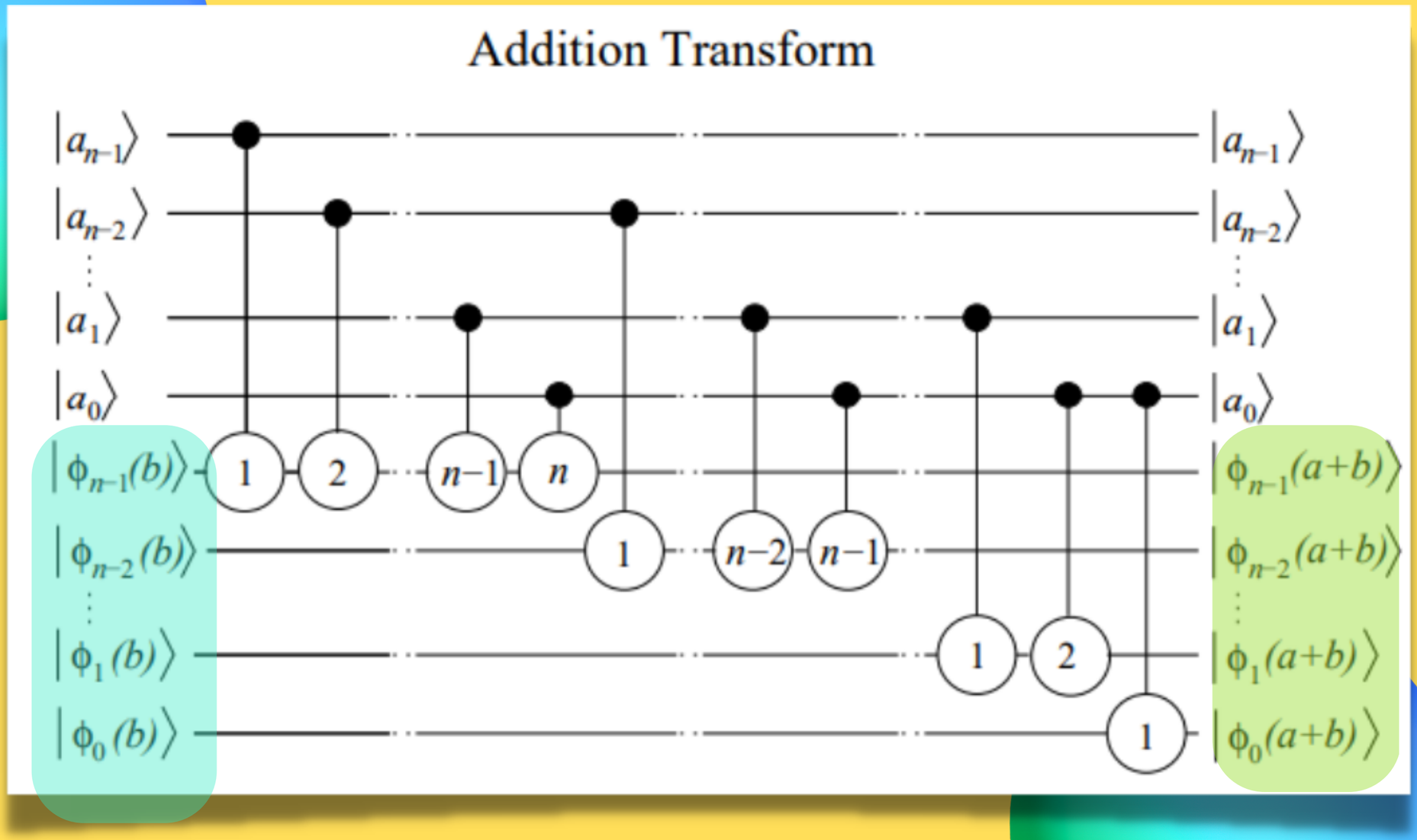
Simple Case Study N=15 a=7



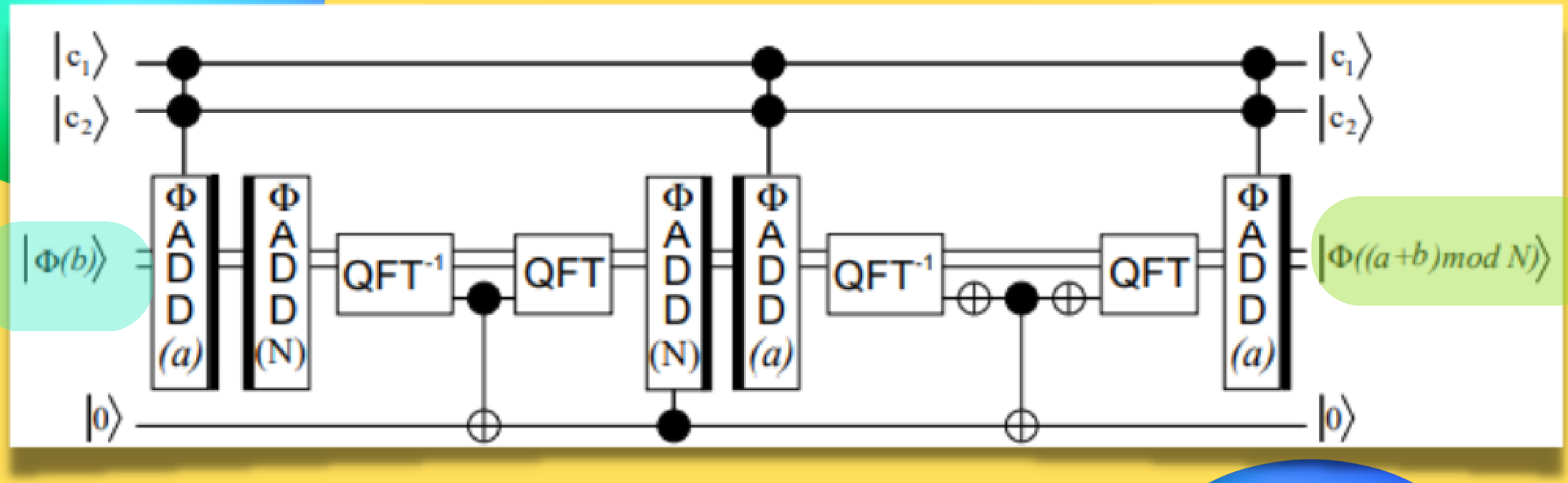
Inverse Fourier Transform

Modular Exponentiation

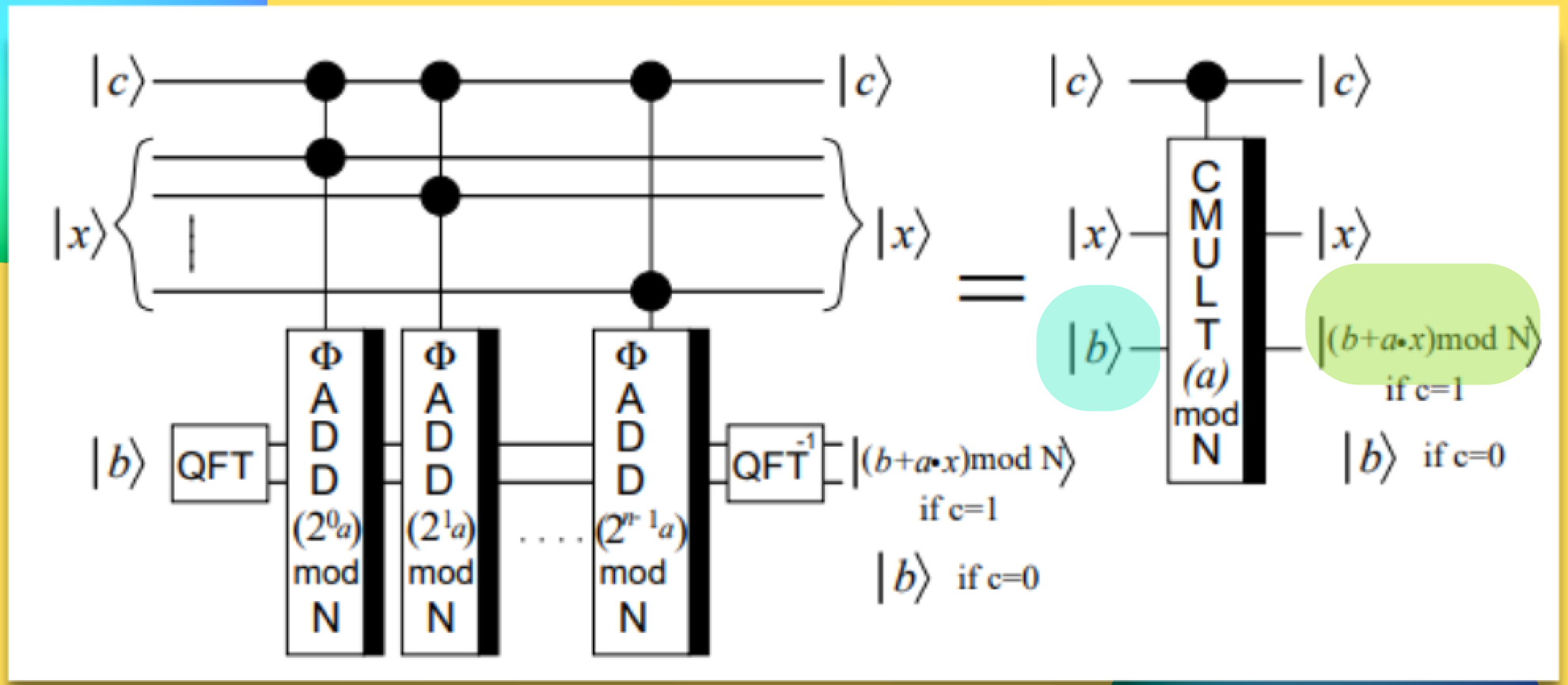
Draper QFT Adder



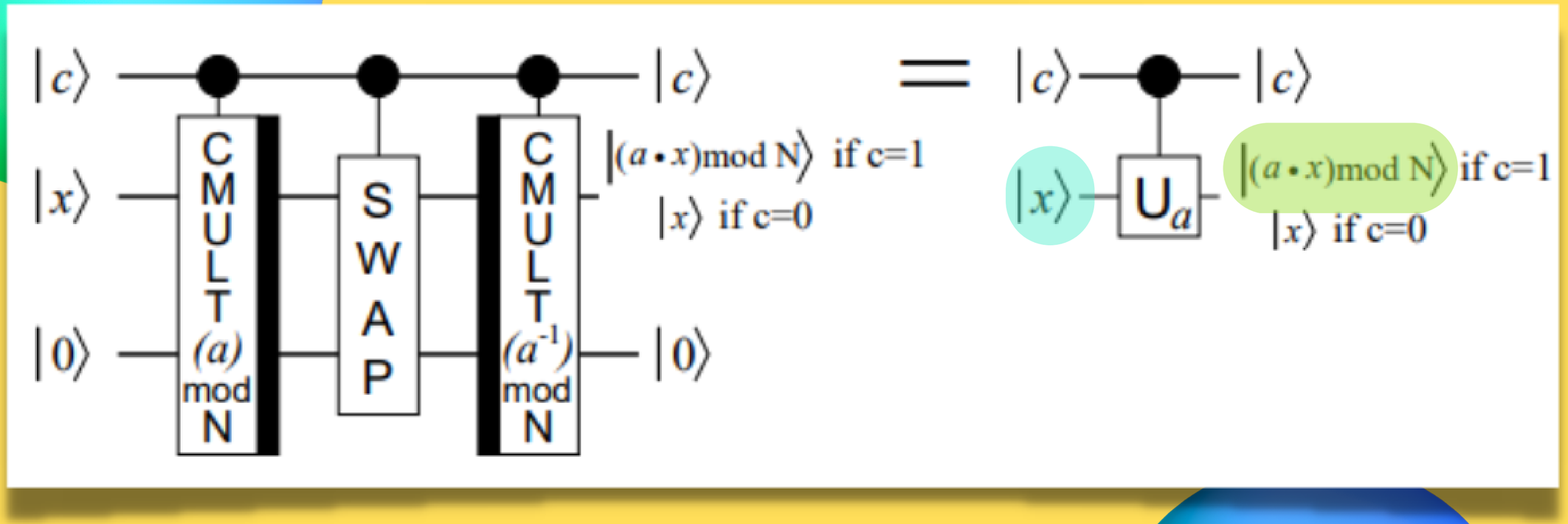
Modular Adder Gate



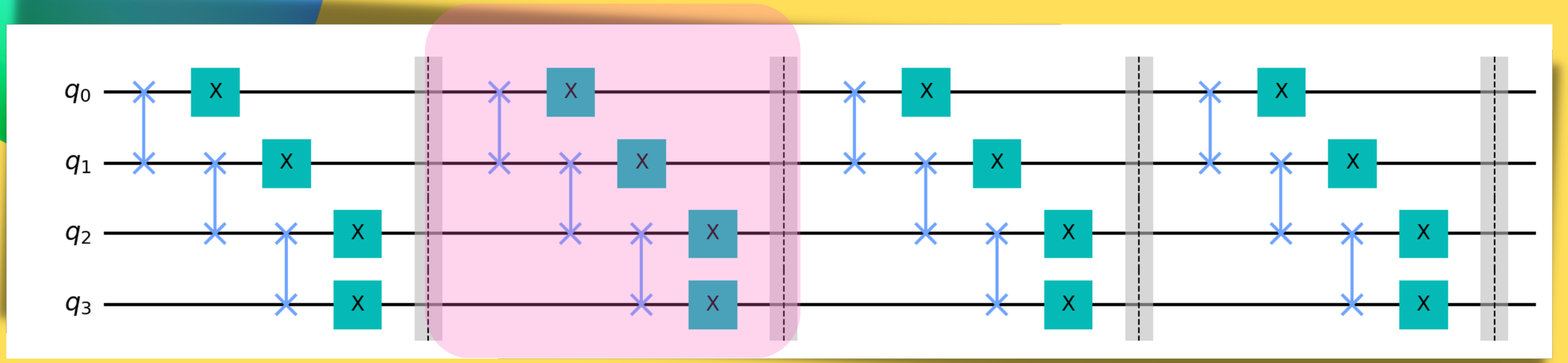
Controlled Multiplier Gate



Controlled-Ua Gate



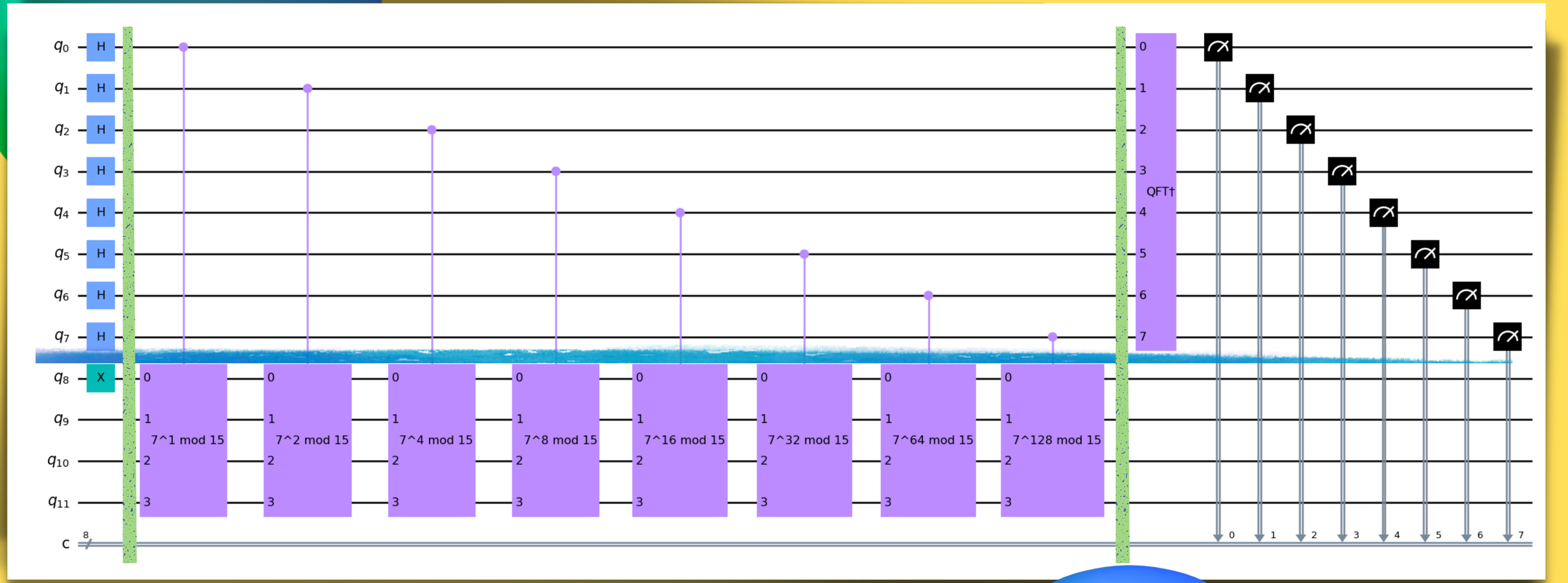
Simplified Circuit for 7x mod 15



$$U|x\rangle = |7x \mod 15\rangle$$

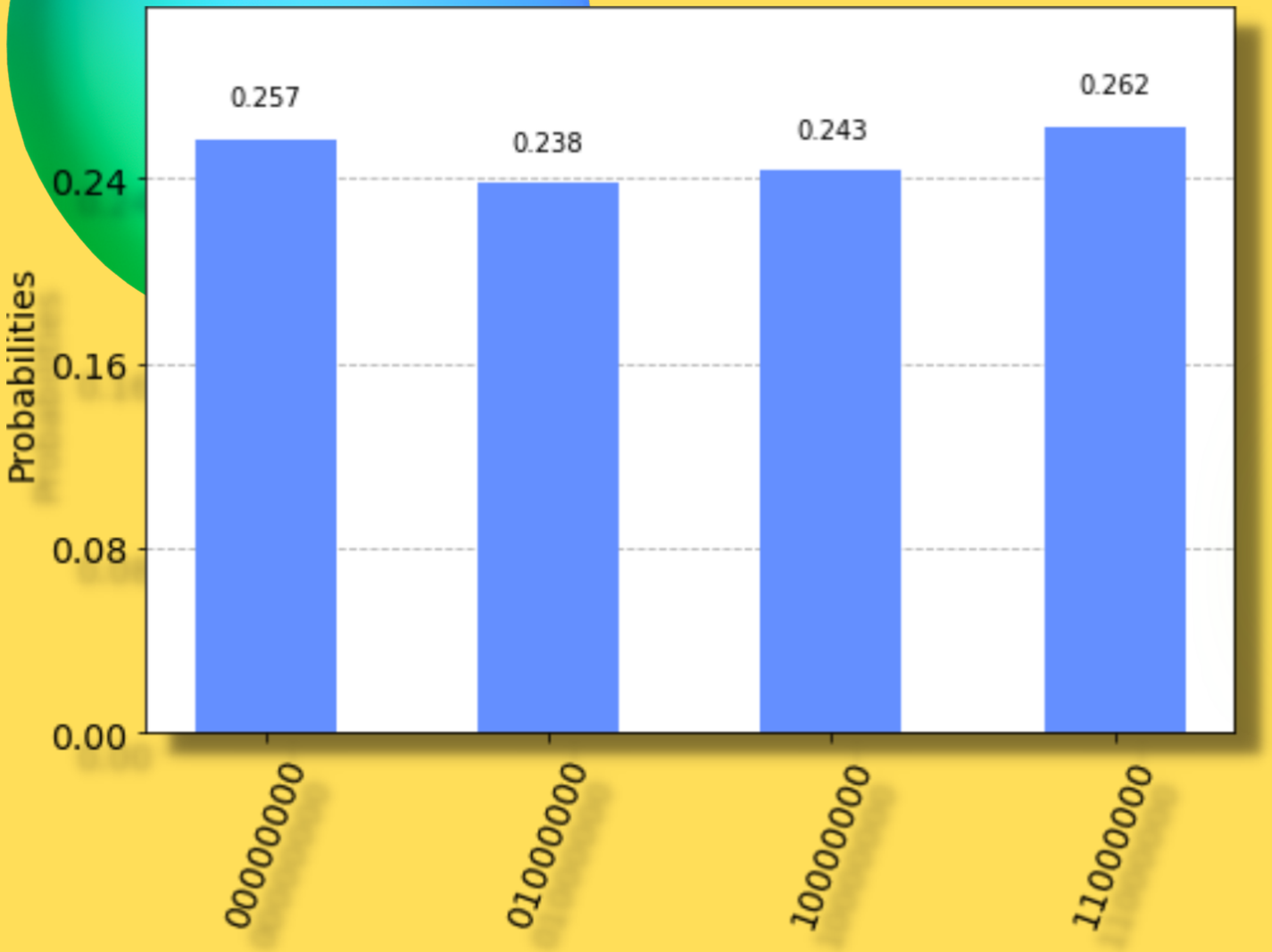
$$U^4|1\rangle = |7^4 \mod 15\rangle$$

Final Layout



N=15 a=7

Measurement



$$|2^n \frac{s}{r}\rangle = 0, 64, 128, 192$$

$$\frac{s}{r} = 0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}$$

PERIOD=4

References

(1)
BEAUREGARD, S. (2003). CIRCUIT FOR SHOR'S ALGORITHM USING 2N+3 QUBITS. QUANTUM INFORMATION AND COMPUTATION, 3(2), 175–185. HTTPS://DOI.ORG/10.26421/QIC3.2-8

(2)
MARKOV, I. L., & SAEEDI, M. (2012). CONSTANT-OPTIMIZED QUANTUM CIRCUITS FOR MODULAR MULTIPLICATION AND EXPONENTIATION. QUANTUM INFORMATION & COMPUTATION, 12(5), 361–394. HTTPS://DOI.ORG/10.5555/2230996.2230997

(3)
TEAM, T. Q. (2022A, NOVEMBER 29). QUANTUM FOURIER TRANSFORM. HTTPS://QISKIT.ORG/TEXTBOOK/CH-ALGORITHMS/QUANTUM-FOURIER-TRANSFORM.HTML

(4)
TEAM, T. Q. (2022B, NOVEMBER 29). QUANTUM PHASE ESTIMATION. HTTPS://QISKIT.ORG/TEXTBOOK/CH-ALGORITHMS/QUANTUM-PHASE-ESTIMATION.HTL

(5)
TEAM, T. Q. (2022C, NOVEMBER 29). SHOR'S ALGORITHM. HTTPS://QISKIT.ORG/TEXTBOOK/CH-ALGORITHMS/SHOR.HTML