Keamanan Kuantum

Hendrik Santoso Sugiarto

IBDA4221 – Selected Topic in Computer Technology

Quantum Computing

Capaian Pembelajaran

- Algoritma Shor
- Aplikasi Algoritma Shor
- Kriptografi Kuantum

Algoritma Shor

Prime Number Factorization

- Sistem kriptografi RSA menggunakan perkalian 2 bilangan prima untuk menjaga keamanan enkripsi-dekripsi mereka
- Faktorisasi bilangan prima adalah problem yang membutuhkan waktu miliaran tahun bagi algoritma klasik
- Faktorisasi dapat diubah menjadi period finding: jika kita dapat menghitung periode dari $a^x mod\ N$ secara efisien maka kita dapat menghitung faktorisasi secara efisien
- Algoritma Shor memanfaatkan QPE untuk menemukan periode ini

Aritmatika Modular

- Suatu bilangan bulat dibagi bilangan bulat lainnya akan menghasilkan sisa
- Secara umum $x \; mod \; N = y \rightarrow x = kN + y$
- Contoh: 5:3 = 1 sisa 2 →5 mod 3 = 2

Uji Pemahaman

- Berapakah 6 mod 3?

Faktorisasi

- Mekanisme:
  - Pilih a yang koprima dengan $N = pq$
    - Koprima $\rightarrow \gcd(a, N) = 1$
  - Temukan r dari fungsi $a^r (mod\ N) = 1 \rightarrow (a^r - 1) mod\ N = 0$
  - Dimana nilai N harus membagi $(a^r - 1) \rightarrow a^r - 1 = \left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right)$
  - $\{p, q\} = \{\gcd(a^{\frac{r}{2}} - 1, N), \gcd(a^{\frac{r}{2}} + 1, N)\}$
- Contoh: $N = 15$
  - Pilih $a = 7$ dimana $\gcd(7,15) = 1$
  - $7^r (mod\ 15) = 1 \rightarrow r = 4$
  - $\{p, q\} = \{4 - 1, 4 + 1\} = \{3,5\}$

Uji Pemahaman

- Faktorkan 15=3x5 dengan menggunakan $a = 13$

Period Finding

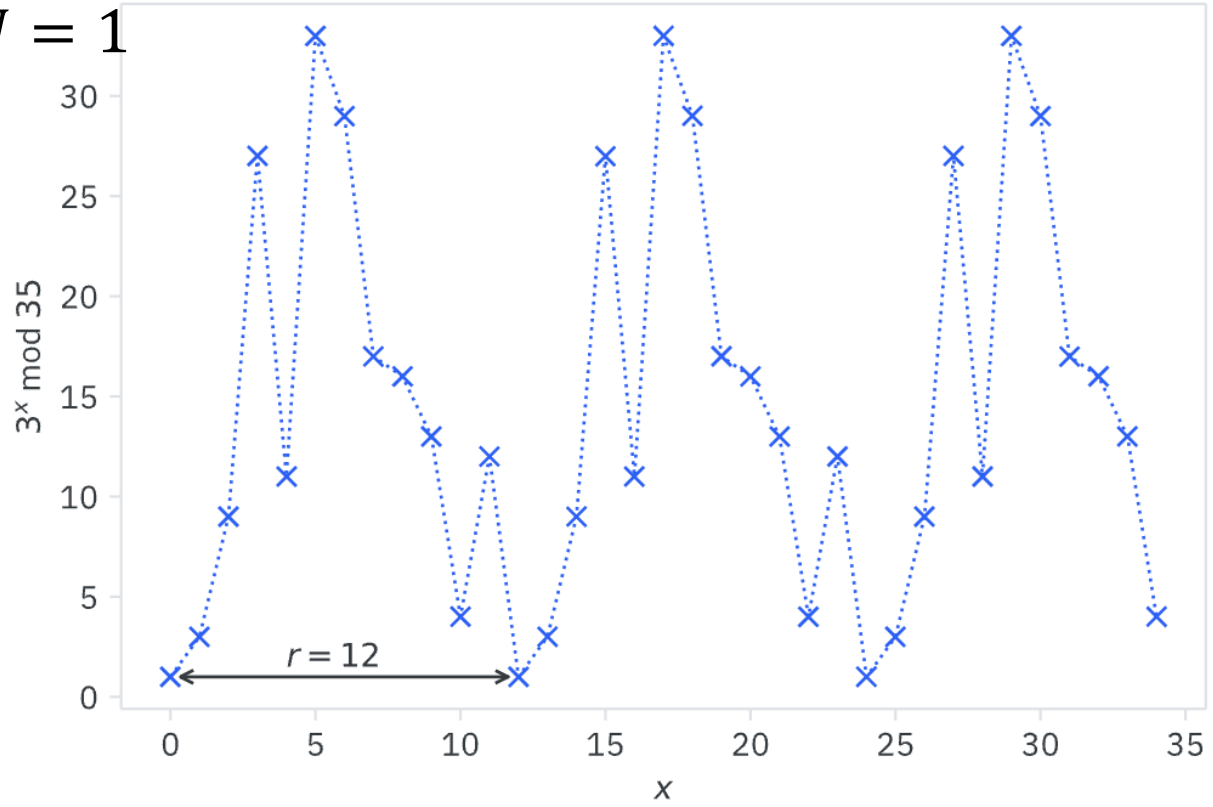
- Terdapat sebuah fungsi periodik:

$$f(x) = a^x mod\ N$$

- Dimana a dan N adalah bilangan bulat positif dan $a < N$. Periode r adalah bilangan bulat terkecil dimana:

$$a^r mod\ N = 1$$

- Contoh: $N = 35, a = 3$

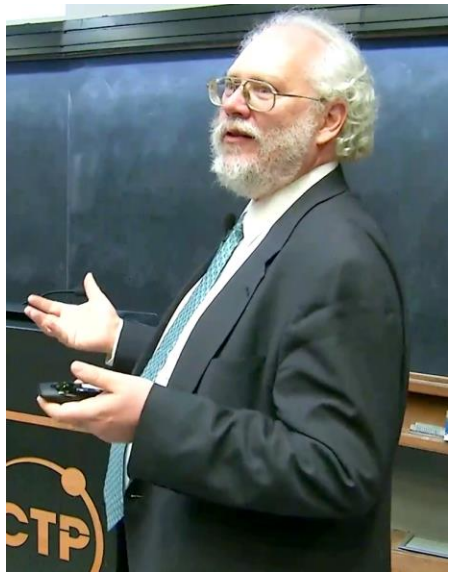


Solusi Kuantum

- Shor menggunakan sebuah unitary operator (yang aturannya mirip QPE):

$$U|y\rangle = |ay \; mod \; N\rangle$$

- Jika kita mulai dari $|1\rangle$, operasi beruntun operator U sebanyak r kali akan kembali ke state $|1\rangle$
- Contoh: $a = 3, N = 35$



$$U|1\rangle = |3 \times 1 \; mod \; 35\rangle = |3\rangle$$
$$U^2|1\rangle = U|3\rangle = |3 \times 3 \; mod \; 35\rangle = |9\rangle$$
$$U^3|1\rangle = U|9\rangle = |3 \times 9 \; mod \; 35\rangle = |27\rangle$$
$$U^4|1\rangle = U|27\rangle = |3 \times 27 \; mod \; 35\rangle = |11\rangle$$
$$U^5|1\rangle = U|11\rangle = |3 \times 11 \; mod \; 35\rangle = |33\rangle$$
$$U^6|1\rangle = U|33\rangle = |3 \times 33 \; mod \; 35\rangle = |29\rangle$$
$$U^7|1\rangle = U|29\rangle = |3 \times 29 \; mod \; 35\rangle = |17\rangle$$
$$U^8|1\rangle = U|17\rangle = |3 \times 17 \; mod \; 35\rangle = |16\rangle$$
$$U^9|1\rangle = U|16\rangle = |3 \times 16 \; mod \; 35\rangle = |13\rangle$$
$$U^{10}|1\rangle = U|13\rangle = |3 \times 13 \; mod \; 35\rangle = |4\rangle$$
$$U^{11}|1\rangle = U|4\rangle = |3 \times 4 \; mod \; 35\rangle = |12\rangle$$
$$U^{12}|1\rangle = U|12\rangle = |3 \times 12 \; mod \; 35\rangle = |1\rangle$$

CALVIN INSTITUTE OF TECHNOLOGY

Eigenstate

- Superposisi semua states pada siklus ini menjadi eigenstate dari U dengan eigenvalue 1:

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

$$U|u_0\rangle = |u_0\rangle$$

- Contoh: $a = 3, N = 35$

$$|u_0\rangle = \frac{1}{\sqrt{12}}(|1\rangle + |3\rangle + |9\rangle + |27\rangle + |11\rangle + |33\rangle + |29\rangle + |17\rangle + |16\rangle + |13\rangle + |4\rangle + |12\rangle)$$

$$U|u_0\rangle = \frac{1}{\sqrt{12}} U(|1\rangle + |3\rangle + |9\rangle + |27\rangle + |11\rangle + |33\rangle + |29\rangle + |17\rangle + |16\rangle + |13\rangle + |4\rangle + |12\rangle)$$

$$U|u_0\rangle = \frac{1}{\sqrt{12}}(|3\rangle + |9\rangle + |27\rangle + |11\rangle + |33\rangle + |29\rangle + |17\rangle + |16\rangle + |13\rangle + |4\rangle + |12\rangle + |1\rangle)$$

$$U|u_0\rangle = |u_0\rangle$$

CALVIN INSTITUTE OF TECHNOLOGY

Eigenstate

- Superposisi semua states pada siklus ini dengan fase menjadi eigenstate dari U:

$$|u_1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}} |a^k mod\ N\rangle$$

$$U|u_1\rangle = e^{\frac{2\pi i}{r}} |u_1\rangle$$

- Contoh: $a = 3, N = 35$

$$U|u_1\rangle = \frac{1}{\sqrt{12}} U \left(|1\rangle + e^{-\frac{2\pi i}{12}} |3\rangle + e^{-\frac{4\pi i}{12}} |9\rangle + e^{-\frac{6\pi i}{12}} |27\rangle + e^{-\frac{8\pi i}{12}} |11\rangle + e^{-\frac{10\pi i}{12}} |33\rangle + e^{-\frac{12\pi i}{12}} |29\rangle + e^{-\frac{14\pi i}{12}} |17\rangle + e^{-\frac{16\pi i}{12}} |16\rangle + e^{-\frac{18\pi i}{12}} |13\rangle + e^{-\frac{20\pi i}{12}} |4\rangle + e^{-\frac{22\pi i}{12}} |12\rangle \right)$$

$$U|u_1\rangle = \frac{1}{\sqrt{12}} e^{\frac{2\pi i}{12}} \left(e^{-\frac{2\pi i}{12}} |3\rangle + e^{-\frac{4\pi i}{12}} |9\rangle + e^{-\frac{6\pi i}{12}} |27\rangle + e^{-\frac{8\pi i}{12}} |11\rangle + e^{-\frac{10\pi i}{12}} |33\rangle + e^{-\frac{12\pi i}{12}} |29\rangle + e^{-\frac{14\pi i}{12}} |17\rangle + e^{-\frac{16\pi i}{12}} |16\rangle + e^{-\frac{18\pi i}{12}} |13\rangle + e^{-\frac{20\pi i}{12}} |4\rangle + e^{-\frac{22\pi i}{12}} |12\rangle + e^{-\frac{24\pi i}{12}} |1\rangle \right)$$

$$U|u_1\rangle = e^{\frac{2\pi i}{12}} |u_1\rangle$$

CALVIN INSTITUTE OF TECHNOLOGY

Eigenstate

- Superposisi semua states pada siklus ini dengan fase kelipatan s menjadi eigenstate dari U:

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

$$U|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle$$

- Contoh: $a = 3, N = 35$

$$U|u_s\rangle$$
$$= \frac{1}{\sqrt{12}} U \left(|1\rangle + e^{-\frac{2\pi i s}{12}} |3\rangle + e^{-\frac{4\pi i s}{12}} |9\rangle + e^{-\frac{6\pi i s}{12}} |27\rangle + e^{-\frac{8\pi i s}{12}} |11\rangle + e^{-\frac{10\pi i s}{12}} |33\rangle + e^{-\frac{12\pi i s}{12}} |29\rangle \right.$$
$$\left. + e^{-\frac{14\pi i s}{12}} |17\rangle + e^{-\frac{16\pi i s}{12}} |16\rangle + e^{-\frac{18\pi i s}{12}} |13\rangle + e^{-\frac{20\pi i s}{12}} |4\rangle + e^{-\frac{22\pi i s}{12}} |12\rangle \right)$$

$$U|u_s\rangle$$
$$= \frac{1}{\sqrt{12}} e^{\frac{2\pi i s}{12}} \left(e^{-\frac{2\pi i s}{12}} |3\rangle + e^{-\frac{4\pi i s}{12}} |9\rangle + e^{-\frac{6\pi i s}{12}} |27\rangle + e^{-\frac{8\pi i s}{12}} |11\rangle + e^{-\frac{10\pi i s}{12}} |33\rangle + e^{-\frac{12\pi i s}{12}} |29\rangle \right.$$
$$\left. + e^{-\frac{14\pi i s}{12}} |17\rangle + e^{-\frac{16\pi i s}{12}} |16\rangle + e^{-\frac{18\pi i s}{12}} |13\rangle + e^{-\frac{20\pi i s}{12}} |4\rangle + e^{-\frac{22\pi i s}{12}} |12\rangle + e^{-\frac{24\pi i s}{12}} |1\rangle \right)$$

$$U|u_s\rangle = e^{\frac{2\pi i s}{12}} |u_s\rangle$$

CALVIN INSTITUTE OF TECHNOLOGY

Superposisi eigenstate

- Interferensi terjadi pada superposisi semua eigenstates $|u_s\rangle$ dimana $0 \leq s \leq r-1$, sehingga hanya tersisa $|1\rangle$:

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

- Karena basis komputasi $|1\rangle$ adalah superposisi semua eigenstates $|u_s\rangle$, maka Ketika kita melakukan QPE terhadap U dengan state $|1\rangle$, kita akan mengukur fase:

$$\phi = \frac{s}{r}$$

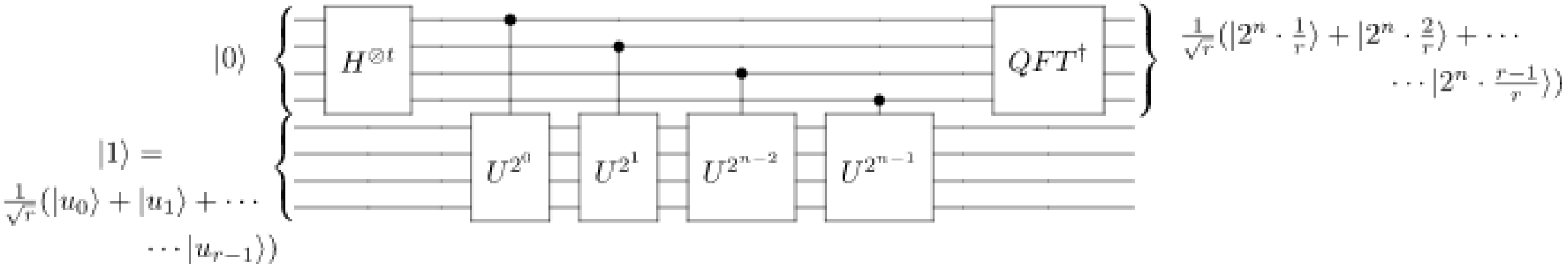
- Dimana s adalah bilangan bulan diantara 0 dan $r-1$
- Maka nilai r bisa didapatkan dengan menggunakan fraksi kontinu terhadap ϕ

Uji Pemahaman

- Coba hitung $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$ untuk:
  - $a = 7, N = 15$
  - $a = 3, N = 35$

Algoritma Shor

- Algoritma Shor adalah sebuah QPE



Uji Pemahaman

- Hitung QPE untuk:
  - $a = 7$ dan $N = 15$

Faktorisasi menggunakan period finding

- Fase yang diukur algoritma shor adalah $\phi = \frac{s}{r}$
- Dimana periode r mengikuti aturan $a^r mod\ N = 1$ dan s adalah bilangan bulat antara 0 dan $r - 1$
- Nilai periode r yang ditemukan dapat digunakan untuk memfaktorisasi N:

$$(a^r - 1) mod\ N = 0$$

- Dimana nilai N harus membagi $a^r - 1$:

$$a^r - 1 = \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)$$

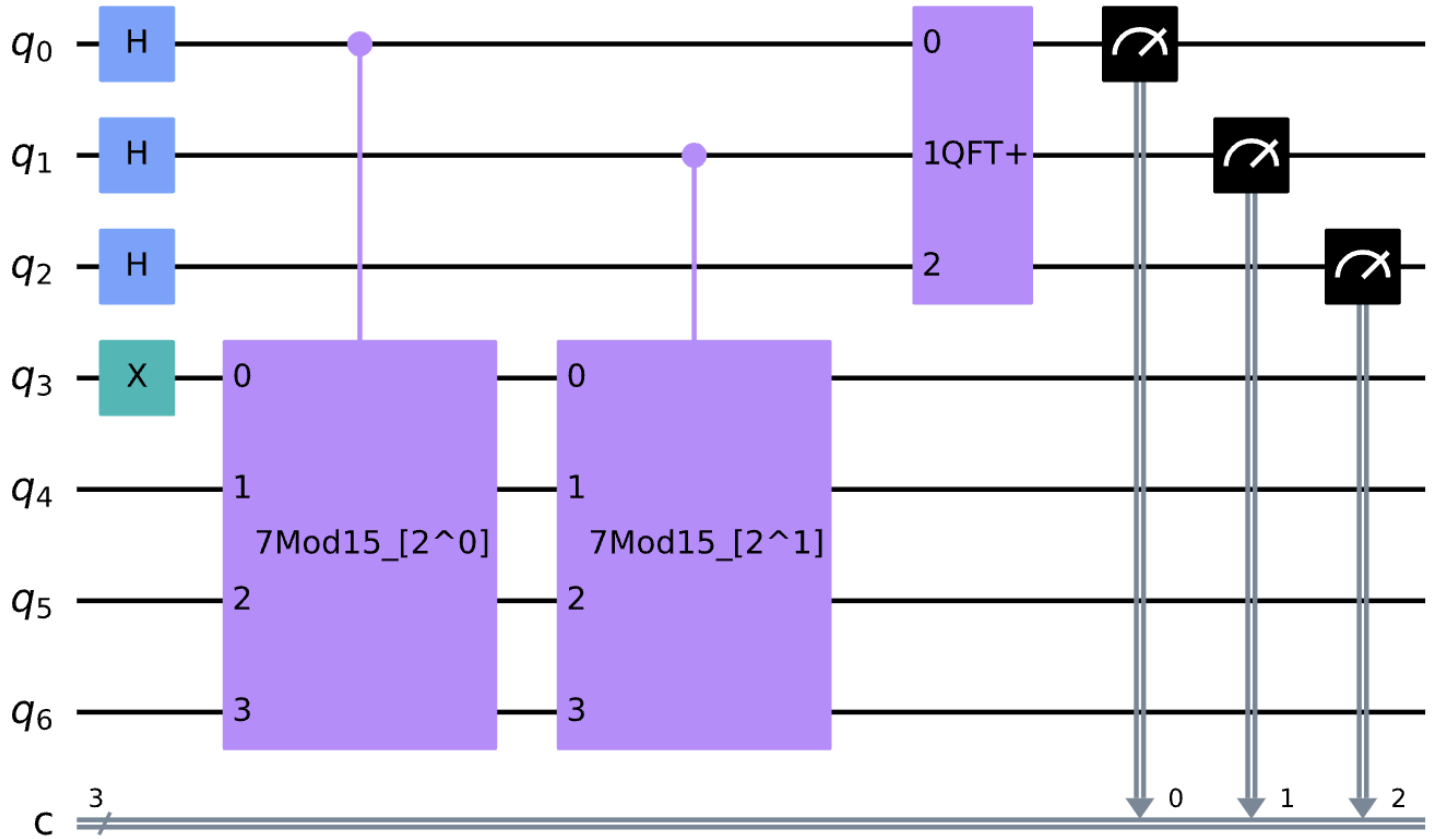
CALVIN INSTITUTE OF TECHNOLOGY

Aktivitas

- Algoritma Shor untuk $a = 7$ dan $N = 15$

Scalable Shor

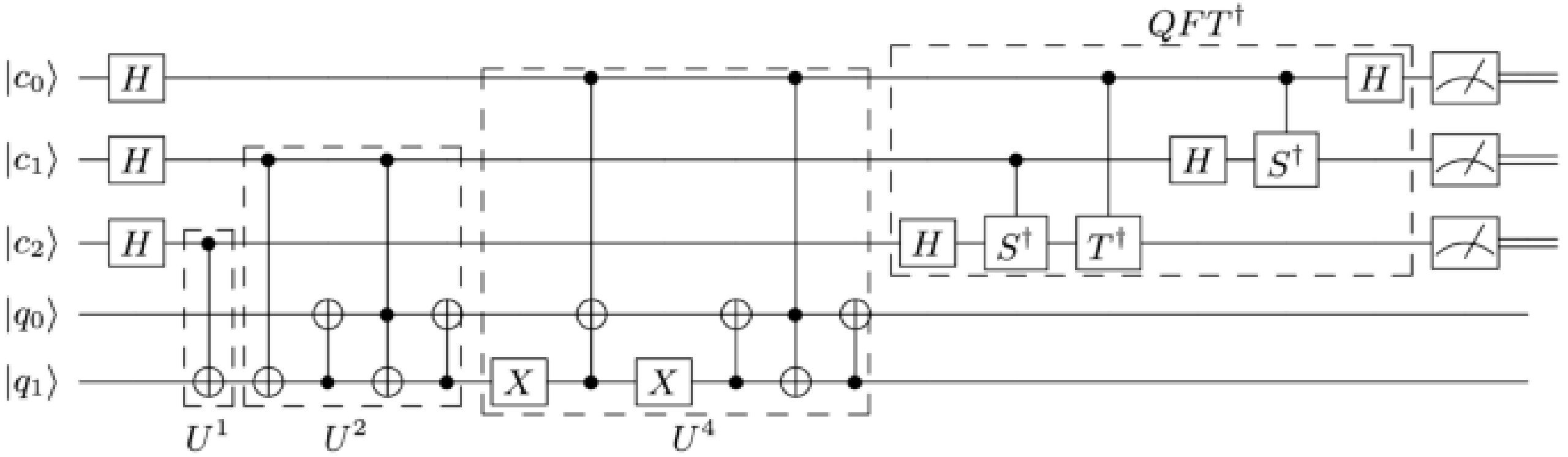
- Scalable Shor https://learn.qiskit.org/course/ch-labs/lab-7-scalable-shors-algorithm
- Iterative QPE https://learn.qiskit.org/course/ch-labs/lab-6-iterative-phase-estimation-algorithm



Reduced Shor

$$|1\rangle \mapsto |\log_4 1\rangle = |00\rangle,$$
$$|4\rangle \mapsto |\log_4 4\rangle = |01\rangle,$$
$$|16\rangle \mapsto |\log_4 16\rangle = |10\rangle.$$

- https://www.nature.com/articles/s41598-021-95973-w



Aplikasi Algoritma Shor

Memecahkan Kriptografi RSA

- Kita membutuhkan mekanisme untuk menerima pesan dari pengirim tanpa membutuhkan pertukaran informasi rahasia. Untuk mencapai ini, kita menggunakan bilangan prima untuk menghasilkan lalu mempublikasikan sebuah public key yang terdiri dari 2 angka (e,n).
- Pada skema RSA, indeks enkripsi (e) dapat berupa bilangan apapun yang kurang dari n selama bilangan tersebut koprima dengan fungsi totient Euler, $\phi=(p-1)\times(q-1)$
- untuk menghitung pesan Cipher, C, pengirim menggunakan rumus:

$$C = P^e (mod\ n)$$

- Penerima pesan akan menggunakan skema deskripsi berikut:

$$D = C^d (mod\ n)$$

- Dimana $e \times d \equiv 1\ mod\ \phi, 0 \leq d \leq n$

Aktivitas memecahkan kriptografi RSA

Kriptografi Kuantum

Kriptografi Kuantum

- Jika Alice dan Bob ingin mengirimkan pesan rahasia (seperti password bank) melalui channel yang tidak aman (misalnya internet), diperlukan enkripsi
- Misal Eve (pihak ketiga) menyediakan channel komunikasi klasik (misalnya sambungan telepon), maka Eve dapat menyadap tanpa ketahuan
- Tapi jika Eve menyediakan channel komunikasi kuantum (misalnya fiber-optic yang mengirim superposisi cahaya), maka dapat diketahui apakah Eve menyadap atau tidak

Proses

- Alice memilih string random dan memilih basis random untuk setiap bit
- Alice encode setiap bit menurut basis yang dipilih lalu mengirim ke Bob
- Bob mengukur setiap qubit dengan basis random
- Alice dan Bob share basis yang mereka gunakan. Jika basis yang digunakan sama, bisa dipakai untuk bagian secret key. Jika tidak, maka buang bit tersebut
- Alice dan Bob share random sample dari key mereka, jika sample match maka tidak ada penyadapan

Alice

- Memilih string random:

  1000101011010100

- Memilih basis random:

  ZZXZXXXZXZXXXXXX

- Encode bit menurut basis:

$$|1\rangle|0\rangle|+\rangle|0\rangle|-\rangle|+\rangle|-\rangle|0\rangle|-\rangle|1\rangle|+\rangle|-\rangle|+\rangle|-\rangle|+\rangle|+\rangle$$

Bob

- Bob mengukur setiap qubit dengan basis random:
  XZZZXZXZXZXZZZXZ

Alice dan Bob

- Share basis yang mereka gunakan
  - Alice: ZZXZXXXZXZXXXXXX
  - Bob : XZZZXZXZXZXZZZXZ
- Jika basis yang digunakan sama, bisa dipakai untuk bagian secret key. Jika tidak, maka buang bit tersebut
  - Secret basis: ZZXXZXZXX
  - Secret key : 001101100
- Share random sample dari key mereka, jika sample match maka tidak ada penyadapan

Quantum Key Distribution

- Mekanisme pembuatan quantum key

Alice	Channel Eve	Bob
Bits Alice		
Basis Alice		
String	String	String
		Basis Bob
		Hasil Bob
	Basis Alice	Basis Alice
Basis Bob	Basis Bob	
Kunci Alice		Kunci Bob
Sampel Bob	Sampel Bob	Sampel Bob
Sampel Alice	Sampel Alice	Sampel Alice
Shared Key		Shared Key

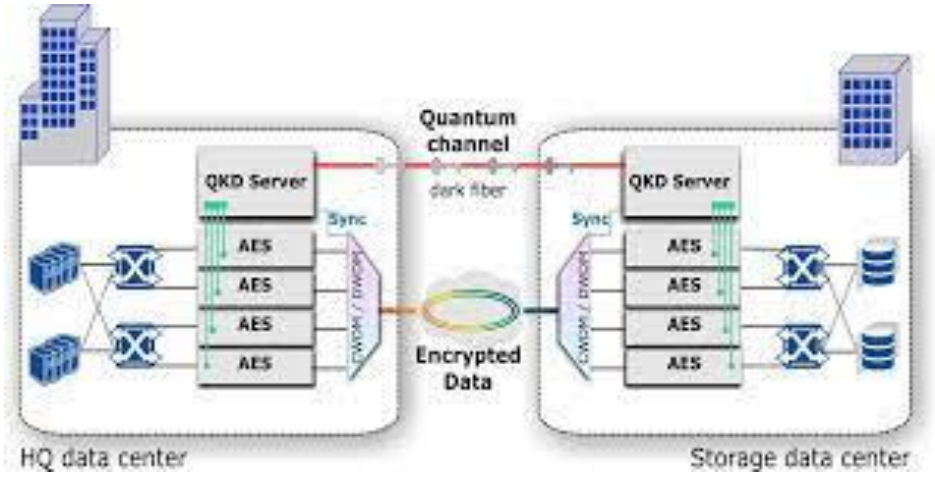
CALVIN INSTITUTE OF TECHNOLOGY

Aktivitas

- Quantum key distribution

Instalasi kriptografi kuantum

- https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/
- Kriptografi kuantum pernah digunakan untuk mengamankan proses pemilu di swiss



REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

Tuhan Memberkati