KU LEUVEN

Intro to Quantum Computation and Quantum Cryptanalysis

September, 2016

Alan Szepieniec

KU Leuven, ESAT/COSIC

Postulates of Quantum Computation

1. A quantum system is fully defined by its *state* $|\psi\rangle \in \mathcal{H}$ where $\mathcal{H} \subset \mathbb{C}^{2^k}$ is the Hilbert space of unit-length vectors, *i.e.*, $\||\psi\rangle\|_2^2 = |\psi\rangle^{*\mathsf{T}}|\psi\rangle = \langle\psi|\psi\rangle = 1$.
2. Any valid computation is a unitary transformation $T : \mathcal{H} \to \mathcal{H} : |\psi\rangle \mapsto T|\psi\rangle$ of the state and can be described by a unitary matrix $T \in \mathbb{C}^{2^k \times 2^k}$ such that $T^{*\mathsf{T}}T = I$.
3. The composition of two quantum states $|\psi\rangle \in \mathcal{H}_1 \subset \mathbb{C}^{2^k}$ and $|\phi\rangle \in \mathcal{H}_2 \subset \mathbb{C}^{2^\ell}$ is described by their *tensor product*: $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \subset \mathbb{C}^{2^{k+\ell}}$.

Tensor Product

Inner product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}^{\mathsf{T}} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = a_1 b_1 + a_2 b_2$$

Outer product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix}$$

Tensor product:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Postulates of Quantum Computation

1. A quantum system is fully defined by its *state* $|\psi\rangle \in \mathcal{H}$ where $\mathcal{H} \subset \mathbb{C}^{2^k}$ is the Hilbert space of unit-length vectors, *i.e.*, $\||\psi\rangle\|_2^2 = |\psi\rangle^{*\mathsf{T}}|\psi\rangle = \langle\psi|\psi\rangle = 1$.
2. Any valid computation is a unitary transformation $T : \mathcal{H} \to \mathcal{H} : |\psi\rangle \mapsto T|\psi\rangle$ of the state and can be described by a unitary matrix $T \in \mathbb{C}^{2^k \times 2^k}$ such that $T^{*\mathsf{T}}T = I$.
3. The composition of two quantum states $|\psi\rangle \in \mathcal{H}_1 \subset \mathbb{C}^{2^k}$ and $|\phi\rangle \in \mathcal{H}_2 \subset \mathbb{C}^{2^\ell}$ is described by their *tensor product*: $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \subset \mathbb{C}^{2^{k+\ell}}$.
4. Measurement M happens with respect to an orthogonal basis $|b_1\rangle, |b_2\rangle, \ldots, |b_k\rangle \in \mathcal{H}$ and fixes the state to one basis vector $M|\psi\rangle = |b_i\rangle$ with probability $\langle\psi|b_i\rangle\langle b_i|\psi\rangle$.

Quantum Computation Example

(4.) Use the basis $|0\rangle, |1\rangle$ for $\mathcal{H}$.

(1.) A qubit $|\psi\rangle \in \mathcal{H}$ is described by a vector $(\alpha, \beta) \in \mathbb{C}^2$ such that $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

(4.) Measuring yields $|0\rangle$ with probability $\alpha^*\alpha$ and $|1\rangle$ with $\beta^*\beta$.

- ▷ Let $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ be two qubits set to zero, *i.e.*, $|\psi\rangle = |\phi\rangle = |0\rangle$.

(3.) The composite system is described by $|\psi\phi\rangle = |\psi\rangle \otimes |\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ with e.g. $\alpha = 1$ and $\beta = \gamma = \delta = 0$.

(2.) Apply the unitary transformation

$$T = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & 0 & -\frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{2}\sqrt{2} & 0 & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix} \text{ to } |\psi\phi\rangle \cong \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}.$$

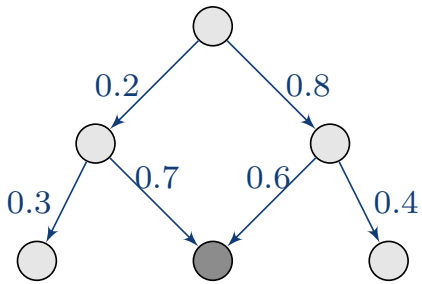
- ▷ Result: $T|\psi\phi\rangle = \frac{1}{2}\sqrt{2}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{2}\sqrt{2}|11\rangle$.

(4.) Measuring yields $|00\rangle$ with probability $\frac{1}{2}$ and $|11\rangle$ with $\frac{1}{2}$.

Modes of Computation

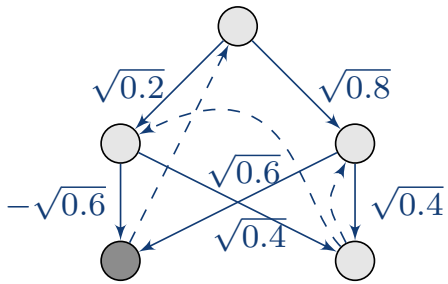
$P = 1$

deterministic



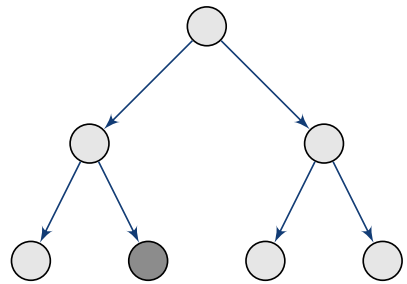
$P = 0.2 \times 0.7 + 0.8 \times 0.6 = 0.62$

probabilistic



$P = \left(-\sqrt{0.2}\sqrt{0.6} + \sqrt{0.8}\sqrt{0.6}\right)^2 \approx 0.35^2 \approx 0.12$

quantum



$P = 1$

nondeterministic

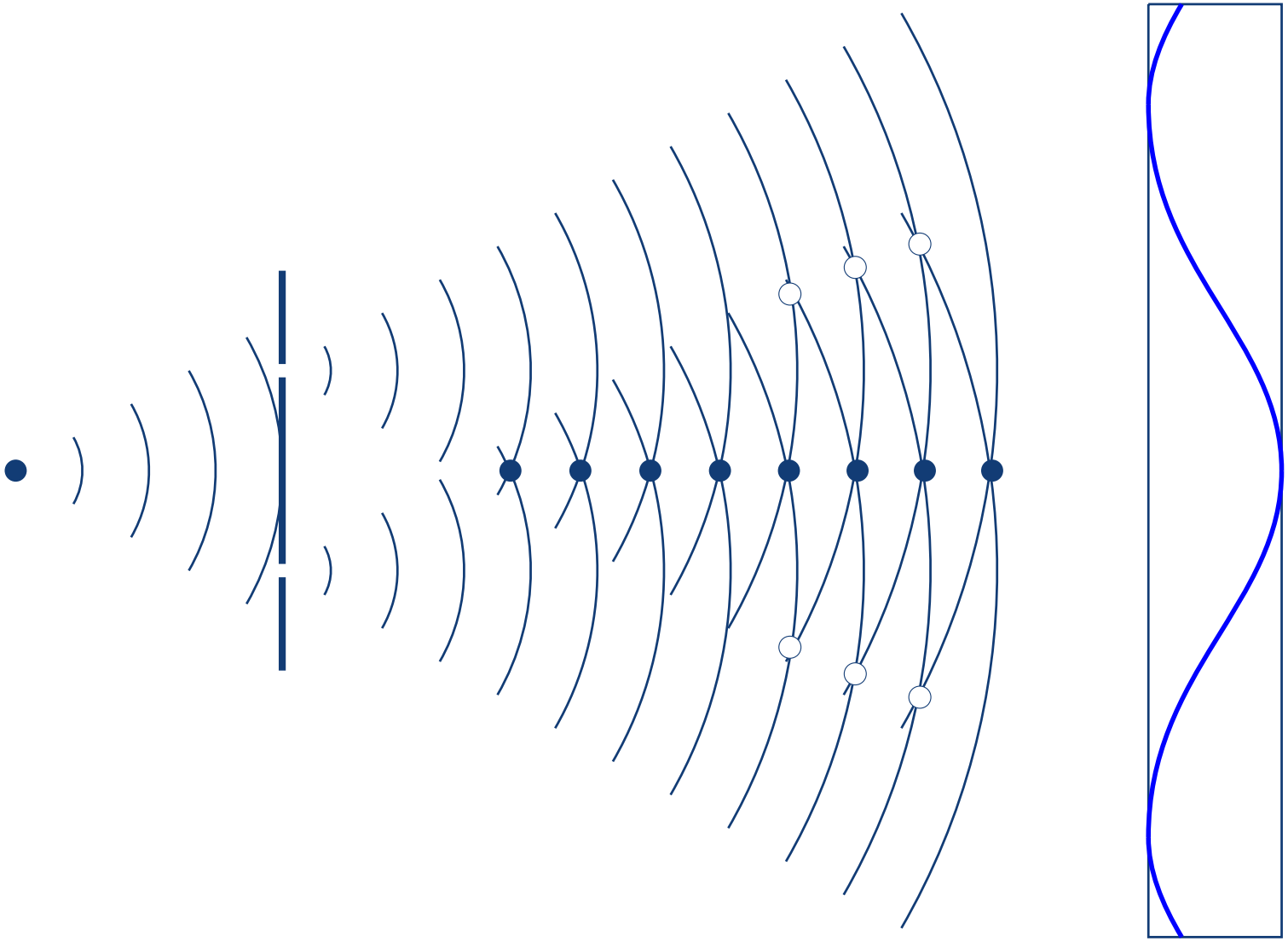
Postulates of Probabilistic Computation

1. A ~~quantum~~ probabilistic system is fully defined by its *state* (or *probability distribution*) $\psi \in [0;1]^{2^k}$ having ~~ℓ_2~~ ℓ_1-norm equal to 1
2. Any valid computation is a transformation $T : \psi \mapsto T\psi$ of the state and can be described by a ~~unitary~~ stochastic matrix $T \in [0;1]^{2^k \times 2^k}$ such that all rows and columns sum to 1.
3. The composition of two states $\psi \in [0;1]^{2^k}$ and $\phi \in [0;1]^{2^\ell}$ is described by their *tensor product*: $\psi \otimes \phi \in [0;1]^{2^{k+\ell}}$.
4. ~~Measurement~~ Sampling (denoted by M) happens with respect to an orthogonal basis $b_1, b_2, \ldots, b_k \in [0;1]^{2^k}$ and fixes the state to one basis vector $M\psi = b_i$ with probability ~~$\langle\psi|b_i\rangle\langle b_i|\psi\rangle$~~ $b_i^\mathsf{T}\psi$.

Quantum Computation in 2 Easy Steps

0. Start with probabilistic computation.
1. Compute with *probability distributions* as opposed to *samples*.
   - sample afterwards
2. Use *continuous* transitions opposed to *discrete* ones.
   - the nth root of a computation is always well defined
   - $\longrightarrow$ complex numbers, ℓ_2 norm
   - fixedness of quantum circuits is a minor detail
   - use *unitary local* transformations

Interference

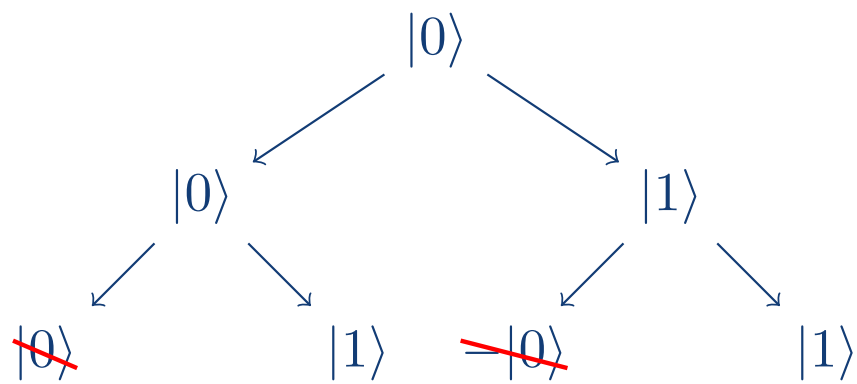


Interference for Quantum Computers

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

$$U|0\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \text{ and } U^2|0\rangle = |1\rangle$$

observable outcomes:



- *destructive interference is the source of all quantum wierdness*
- quantum algorithm design = engineering interference

Shor's Algorithm

factorize $n = pq$

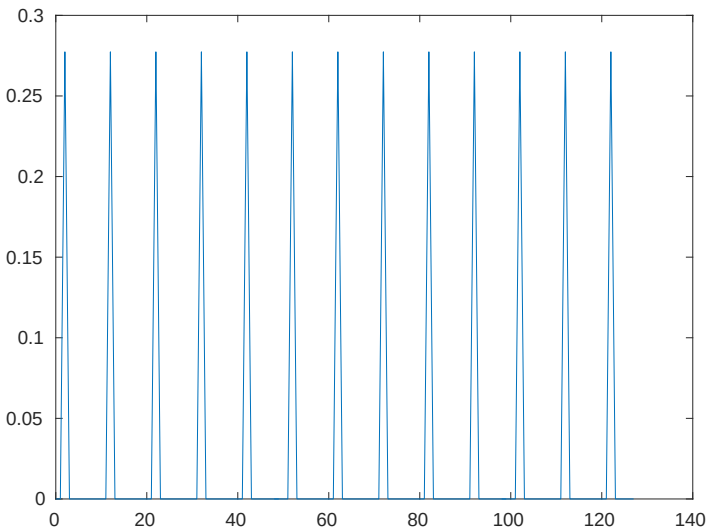
$\Leftrightarrow$ obtain order $\varphi(n)$ of $\mathbb{Z}/n\mathbb{Z}, \times$

$\triangleright$ $|a\rangle, |b\rangle$ are both quantum registers of $k > |n|$ qubits

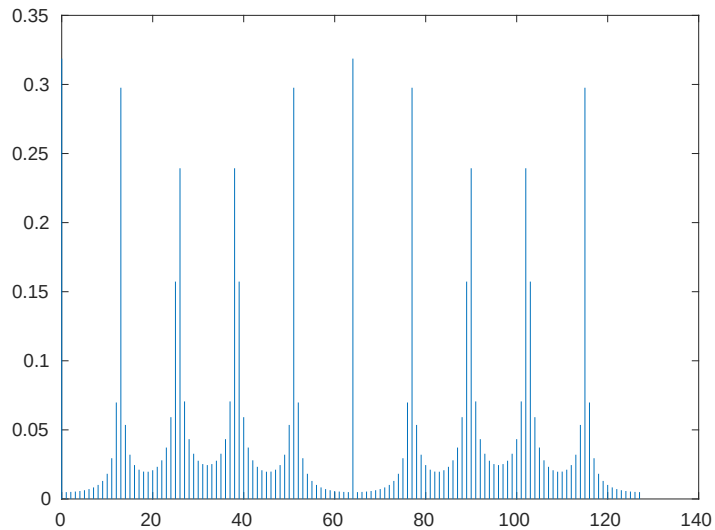
1. Set $|a\rangle = |b\rangle = |0^k\rangle$. result: $|a, b\rangle = |0, 0\rangle$
2. Apply $H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$ to each qubit of $|a\rangle$. result: $|a, b\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=0}^{2^k-1} |i, 0\rangle$
3. Apply $f : |a, b\rangle \mapsto |a, b \oplus x^a \bmod n\rangle$. result: $|a, b\rangle = \cdot \sum_{i=0}^{2^k-1} |i, x^i\rangle$
4. Measure *only* $|b\rangle$. result: $|b\rangle = |x^y\rangle$
   result: $|a\rangle = \cdot \sum_{i \in (y+\varphi(n)\mathbb{Z})} |i\rangle$
5. Apply $g : |a\rangle \mapsto |\mathrm{QFT}(a)\rangle$ result: $|a\rangle = \sum_j \cdot \left| j \frac{2^k}{\varphi(n)} \right\rangle$
6. Measure $|a\rangle$ result: $|a\rangle = \left| \left\lfloor j \frac{2^k}{\varphi(n)} \right\rceil \right\rangle$
7. Repeat.

DFT Example

- factorize $n = 35$
- $b = 6 \quad \longrightarrow$ order $r = 10$



$|a\rangle$



$|\mathrm{QFT}(a)\rangle$

Discrete Logarithm

- discrete logarithm: given $g, g^x \in \mathbb{G}$, find $x \in \mathbb{Z}$
- define function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{G} : (y, z) \mapsto (g^x)^{-y} g^z$
- $\forall (y, z) \in \mathbb{Z} \times \mathbb{Z} \,.\, f(y, z) = f(y + 1, z + x)$
- f has *period* $p = (1, x)$
- algorithm:
  1. operate on 3 registers of N qubits, initially $|a, b, c\rangle = |0, 0, 1\rangle$
  2. set to uniform superposition $|a\rangle = |b\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$
  3. compute f: apply $|a, b, c\rangle \mapsto |a, b, c \times f(a, b)\rangle$
  4. apply Fourier transform: apply $|a\rangle \mapsto |\mathsf{QFT}(a)\rangle$ and $|b\rangle \mapsto |\mathsf{QFT}(b)\rangle$
  5. measure the state; w.h.p. $b/a \approx x$

- period in $\mathbb{Z}$ $\longrightarrow$ QFT
- period in $\mathbb{Z} \times \mathbb{Z}$ $\longrightarrow$ QFT $\times$ QFT
- generalizations possible?

Simon's Algorithm

- problem: given a function $f : \{0,1\}^k \to \{0,1\}^\ell$ with an unknown period $p \in \{0,1\}^k$ s.t. $\forall x \,.\, f(x) = f(x \oplus p)$, find p

1. init 2 registers $|a, b\rangle = |0^k 0^\ell\rangle$
2. apply $H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$ to each qubit of $|a\rangle$
   result: $|a\rangle = \frac{1}{2^{k/2}} \sum_{i \in \{0,1\}^k} |i\rangle$
3. apply $|a, b\rangle \mapsto |a, b \oplus f(a)\rangle$
   result: $|a, b\rangle = \frac{1}{2^{k/2}} \sum_{x \in \{0,1\}^k} |x, f(x)\rangle$
4. ~~measure *only* $|b\rangle$~~
   result: $|a, b\rangle = \frac{1}{\sqrt{2}}|\hat{x}, b\rangle + \frac{1}{\sqrt{2}}|\hat{x} \oplus p, b\rangle$
   where $\hat{x}$ s.t. $f(\hat{x}) = b$
5. apply $H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$ to each qubit of $|a\rangle$
   $\to$ bitflips cause interference
   recall: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
   and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
   result: $|a, b\rangle = \cdot \sum_{y \in \{0,1\}^k} |y \wedge \bar{p}, b\rangle$
6. measure $|a\rangle$
   result: random $y \in \{0,1\}^k$ s.t. $y \wedge p = 0$
7. repeat — obtain many samples

Simon's Algorithm IS Shor's Algorithm

Shor: factorize

1. uniform $|a\rangle$
2. apply $|b\rangle \mapsto |b + f(a)\rangle$ with $f(a) = x^a \bmod n$
3. measure $|b\rangle$
4. QFT-$2^{|n|}$ on $|a\rangle$
5. measure $|a\rangle$
6. repeat (if necessary)

Shor: dlog

1. uniform $|a\rangle, |b\rangle$
2. apply $|c\rangle \mapsto |c + f(a,b)\rangle$ with $f(a,b) = (g^x)^{-a} g^b$
3. measure $|c\rangle$
4. QFT-$2^{|p|}$ $\times$ QFT-$2^{|p|}$ on $|a,b\rangle$
5. measure $|a\rangle, |b\rangle$
6. repeat (if necessary)

Simon

1. uniform $|a\rangle$
2. apply $|b\rangle \mapsto |b \oplus f(a)\rangle$
3. measure $|b\rangle$
4. QFT-2 $\times \ldots \times$ QFT-2 on $|a\rangle$
5. measure $|a\rangle$
6. repeat

Hidden Subgroup Problem

Definition

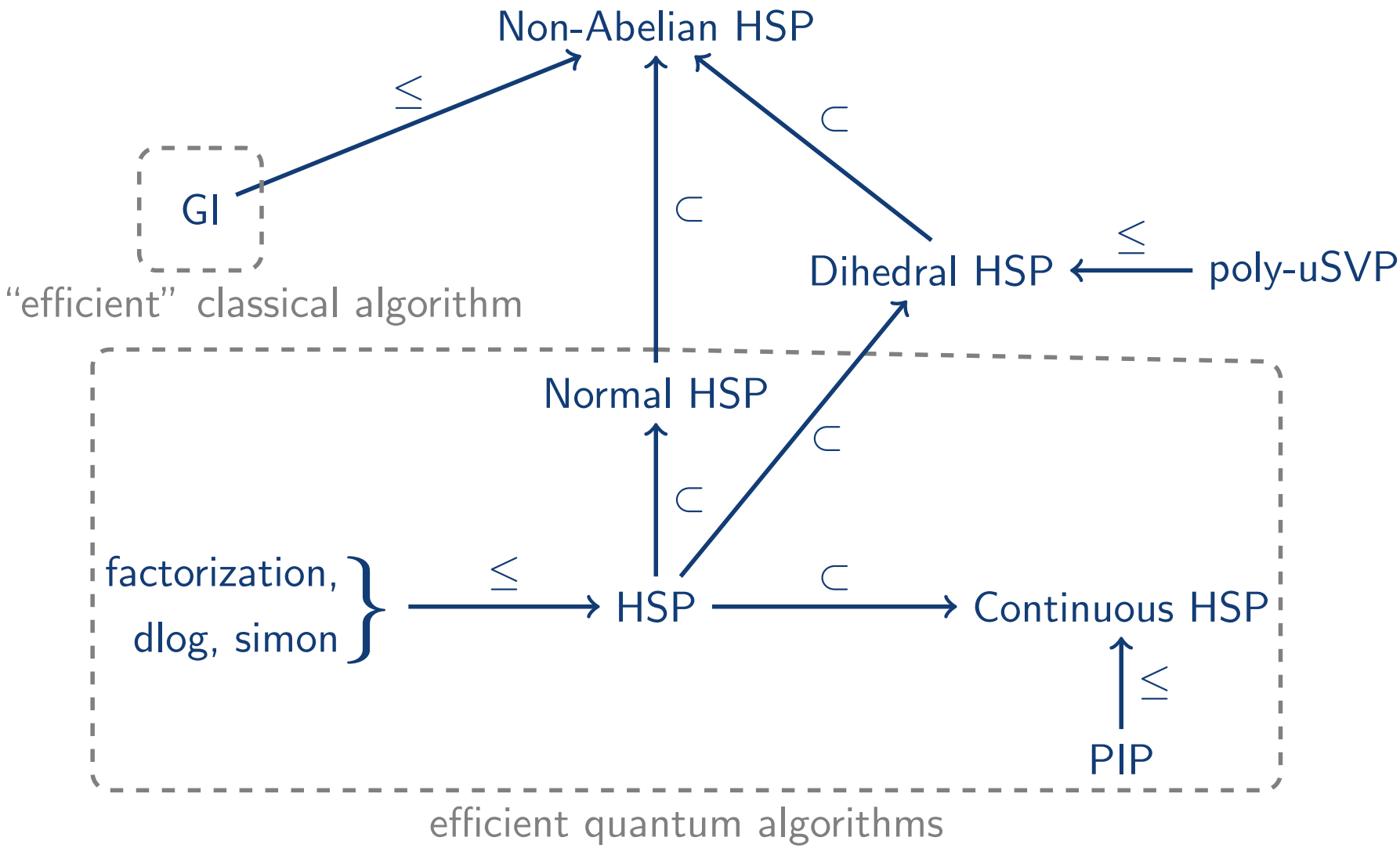
Let $G, +$ be a group with subgroup H. Let $f : G \to \{0,1\}^*$ be a function that produces the same image iff its inputs are from the same coset of H, *i.e.*,

$$\forall g_1, g_2 \in G \,.\, g_1 - g_2 \in H \Leftrightarrow f(g_1) = f(g_2) \ .$$

The *Hidden Subgroup Problem (HSP)* is to find a generating set of H given oracle access to f.

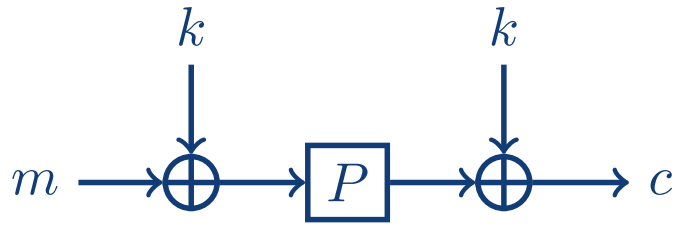
- factorization: $G = \mathbb{Z}, +$ and $H = \varphi(n)\mathbb{Z}, +$
- discrete logarithm: $G = \mathbb{Z} \times \mathbb{Z}, +$ and $H = \mathbb{Z} \begin{pmatrix} 1 \\ x \end{pmatrix}, +$
- Simon's problem: $G = \{0,1\}^k, \oplus$ and $H = \{0, p\}, \oplus$

Environment of HSP

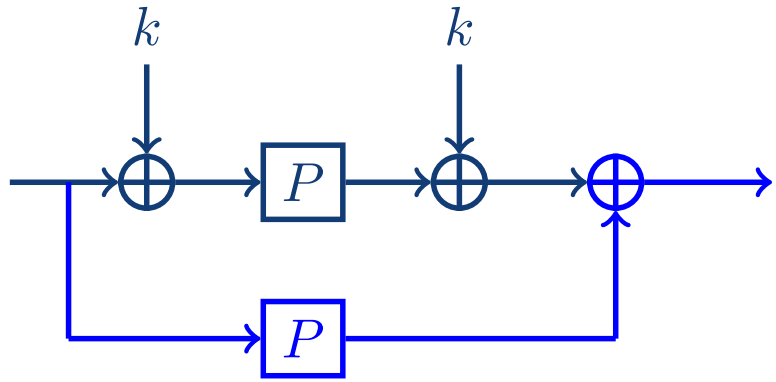


Simon vs. Even-Mansour

- Even-Mansour construction:



- given quantum access to the circuit $\mathcal{C}|m\rangle = |c\rangle$ and given P; find k
- solution[1]:



- $f(x) = P(x \oplus k) \oplus k \oplus P(x)$
- $f(x \oplus k) = P(x) \oplus k \oplus P(x \oplus k)$
- period is k!

[1] H. Kuwakado, M. Morii. "Security on the Quantum-type Even-Mansour Cipher" IEICE 2012

Simon vs. Other Constructions

secure? [2]	CBC-MAC	PMAC	GMAC	GCM	OCB
classical queries	✓	✓	✓	✓	✓
quantum queries	×	×	×	×	×

secure? [3]	CBC	CFB	OFB	CTR	XTS
classical queries	✓	✓	✓	✓	?
quantum queries	×/✓	×/✓	✓	✓	×

- but all attacks require *quantum access* to *keyed primitive*

[2] M. Kaplan *et al.* "Breaking Symmetric Cryptosystems using Quantum Period Finding"

[3] M. Vivekanand *et al.* "Post-quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation"

Quantum Oracle Queries

- Enc/Dec/Sig are typically accessible over classical channels only
  - non-trivial quantum states will collapse
  - IND-qCPA vs. IND-CPA and EUF-qCMA vs. EUF-CMA
- RO should be accessible quantumly ($\rightarrow$ QROM)
- also any known circuit (Enc/Dec/Sig but without secret key)
- is quantum access to keyed primitive worth studying?
  - quantum encryption
  - accidental quantum computers
  - white-box cryptography

  } yeah ... right ...
  - protocols and game-based proofs $\longleftarrow$ big deal
- key principle: *no quantum interaction with secret key material*

Grover's Algorithm

- Let $F : \{0,1\}^k \to \{0,1\}^k$ be OWF with 1 preimage a to $b = F(a)$
- task: given oracle access to F and given b; find a
- best classical algorithm: exhaustive search — $O(2^k)$
- quantum oracle access: $\mathcal{F}|a\rangle \mapsto |b\rangle = |F(a)\rangle$
- best quantum algorithm: Grover — $O(2^{k/2})$

Grover's Algorithm: Elements

- $\mathcal{A}$ — uniform sampler
  - $\mathcal{A}|0^k\rangle = \frac{1}{\sqrt{2^k}} \sum_{i=0}^{2^k-1} |i\rangle = |\Psi\rangle$
  - Apply a Hadamard gate to each qubit
- working plane
  - the vectors $|a\rangle = |\Psi_1\rangle$ and $|\Psi\rangle$ span a plane
  - let $|\Psi_0\rangle$ lie in this plane, perpendicular to $|a\rangle$
- $\mathbf{S}_0$ — mirror about $|0^k\rangle$
  - $\mathbf{S}_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0 \\ |x\rangle & \text{else} \end{cases}$
  - compute $|x, q\rangle \mapsto |x, q \oplus (x = 0)\rangle$ and keep $|q\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$
  - $1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle) \mapsto 1/\sqrt{2}|x\rangle(|0\rangle - |1\rangle)$ (if $x \neq 0$)
  - $1/\sqrt{2}|0\rangle(|0\rangle - |1\rangle) \mapsto 1/\sqrt{2}|0\rangle(|1\rangle - |0\rangle) = -1/\sqrt{2}|0\rangle(|0\rangle - |1\rangle)$
- $\mathbf{S}_\chi$ — mirror about $|\Psi_0\rangle$
  - $\mathbf{S}_\chi|x\rangle = \begin{cases} -|x\rangle & \text{if } F(x) = b \\ |x\rangle & \text{if } F(x) \neq b \end{cases}$
  - compute $|x, q\rangle \mapsto |x, q \oplus (F(x) = b)\rangle$ and keep $|q\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$

Grover's Algorithm: Step-by-Step

Single iteration: $|\Phi\rangle \mapsto \mathcal{Q}|\Phi\rangle = -\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$

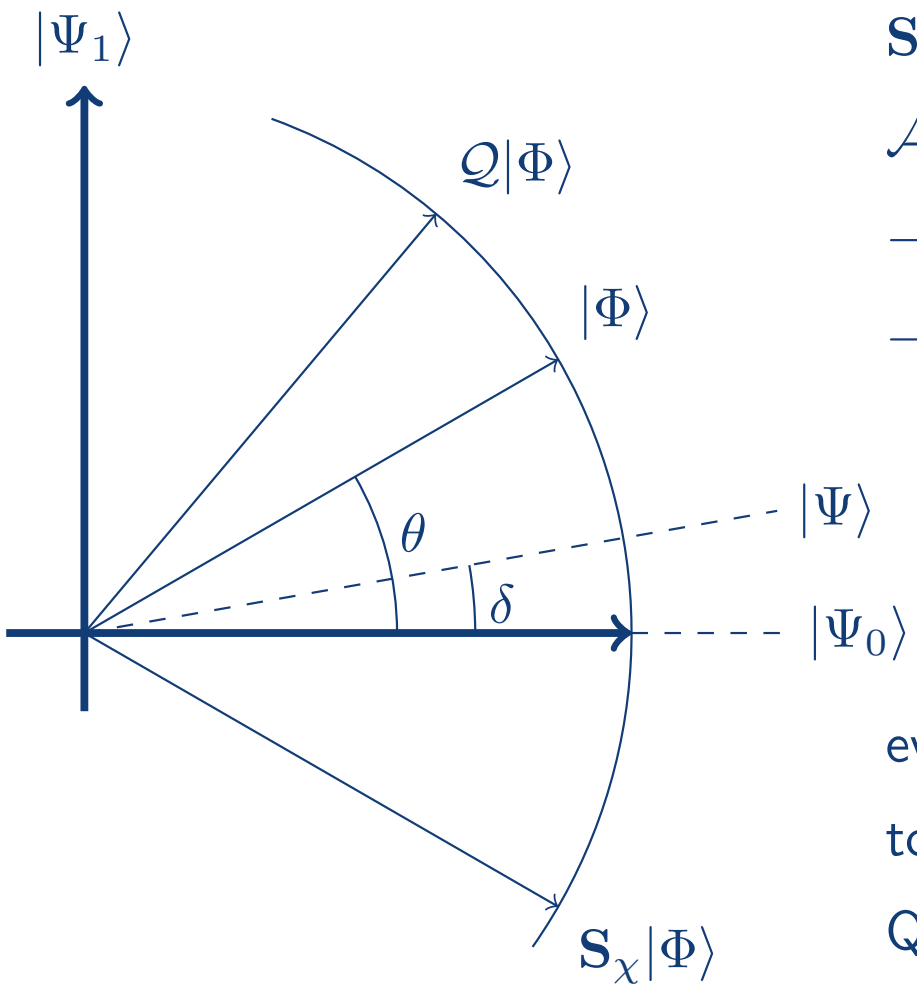
$|\Phi\rangle$ current state

$\mathbf{S}_\chi|\Phi\rangle$: flip about $|\Psi_0\rangle$

$\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: change of basis

$-\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: flip about $|\Psi\rangle$

$-\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi|\Phi\rangle$: undo change of basis

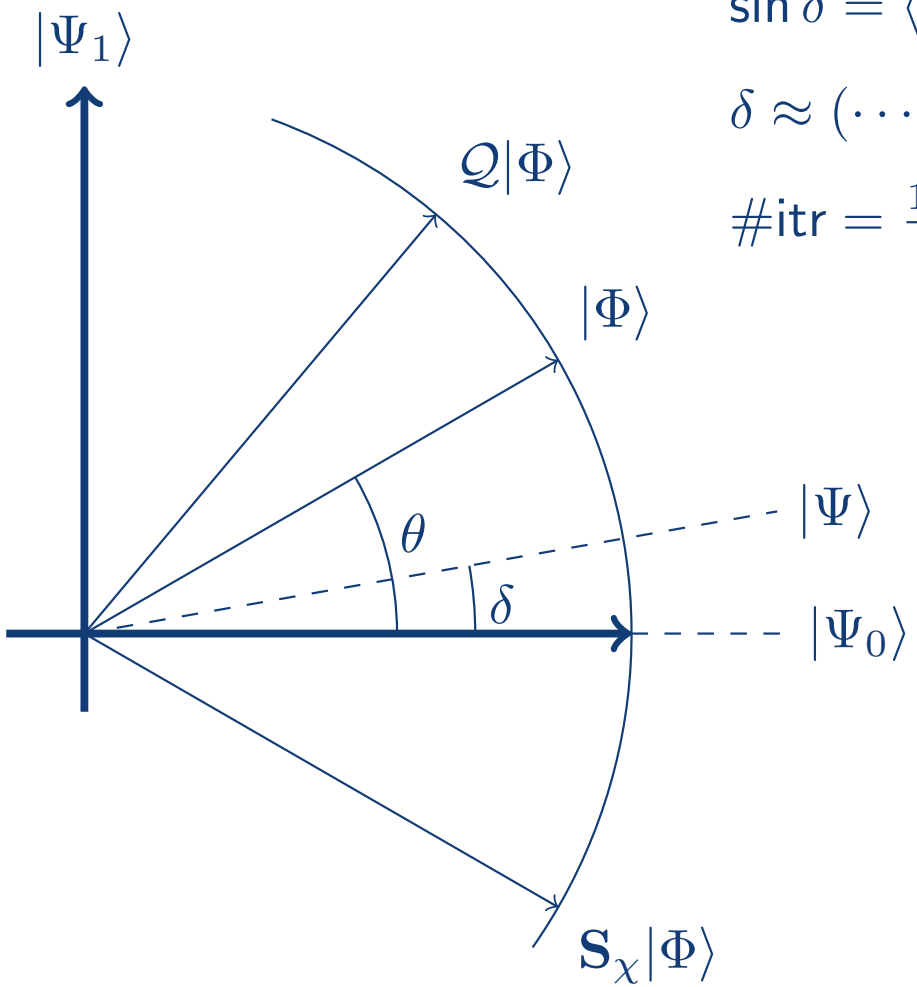


every iteration moves $|\Phi\rangle$ closer

to $|\Psi_1\rangle$ by an angle 2δ

Q: what are δ and (initially) θ?

Grover's Algorithm: Complexity

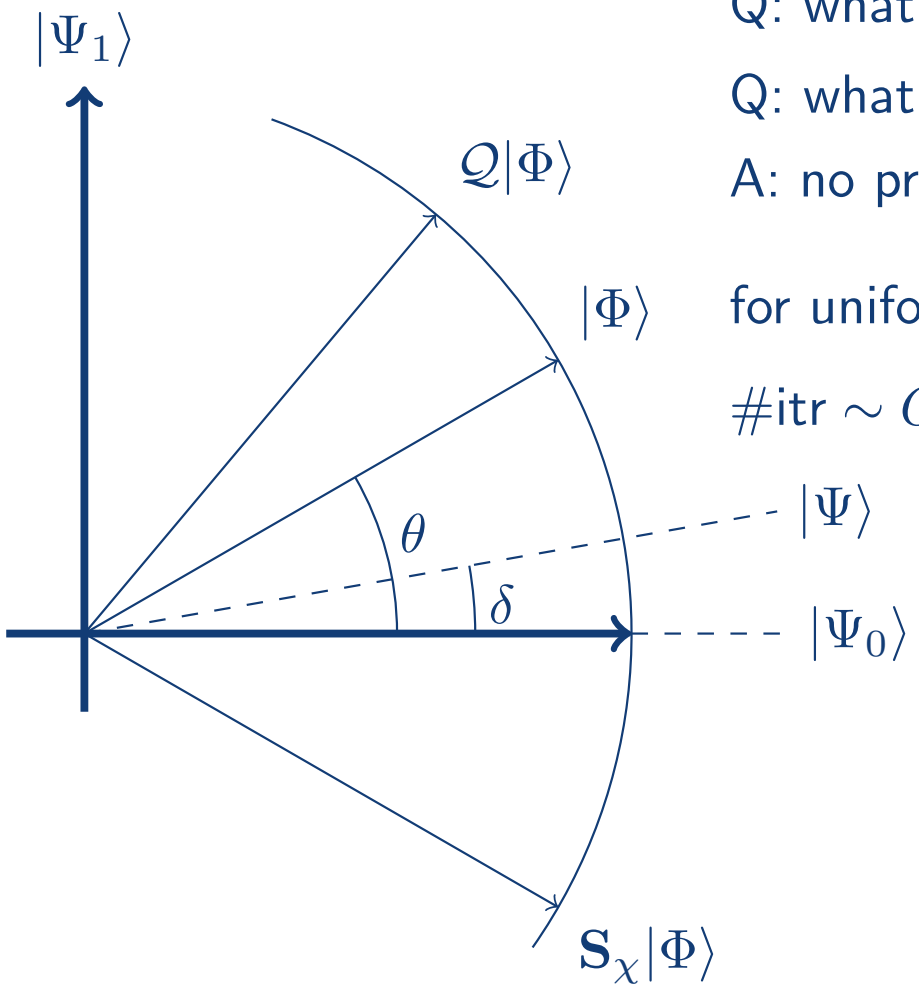


$$\sin\delta = \langle\Psi_1|\Psi\rangle$$

$$\delta \approx (\cdots 0\,1\,0\cdots)(\cdots 1/\sqrt{2^k}\cdots)^{\mathsf{T}} = 1/\sqrt{2^k}$$

$$\#\mathsf{itr} = \frac{1/2-\theta_{\mathsf{init}}}{2\delta} = \frac{1/2-\delta}{2\delta} \approx \frac{1}{2}2^{k/2} - \frac{1}{2}$$

Amplitude Amplification



Q: what if $\#A = \#\{x \mid F(x) = b\} > 1$?

Q: what if $\mathcal{A}$ is better than uniform?

A: no problem

for uniform $\mathcal{A}$ and $\#A > 1$ holds:

$\#\text{itr} \sim O(\sqrt{2^k/\#A})$