Grover Meets Simon- Quantumly attacking the FX-Construction

Authors:- Gregor Leander
and Alexander May

Presentation By: Manish Kumar
Ishan Pandey

Prelude: Quantum attacks on Block Ciphers:

1. Block Cipher and Grover's search attack
2. Even-Mansour Cipher and Simon's algorithm

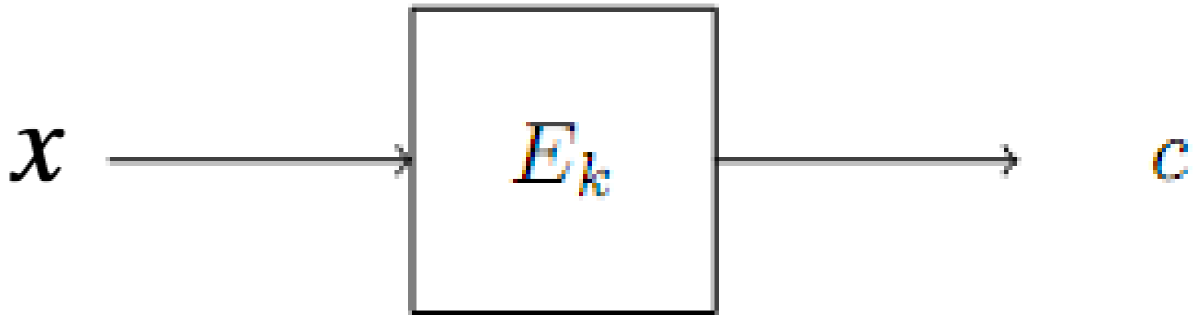
FX construction

Generalized search algorithm: Amplitude amplification
Simon's algorithm details

Combining Grover and Simon algorithms

Attack strategy to break FX construction

Attacks on Block Ciphers



- **Key Length : m**

- Classically requires 2^m steps
- Quantum Algorithm (Grover Search) requires $2^{m/2}$ steps

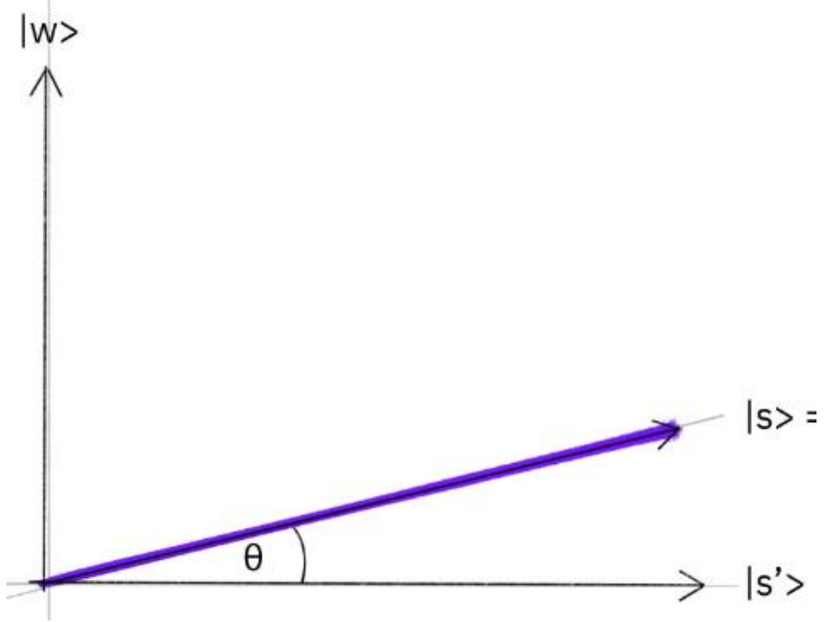
Quantum Search: Grover Algorithm

Context: Unstructured Database Search

Goal: Search a specific item

Classical: $\mathcal{O}(n)$

Quantum: $\sim \mathcal{O}(\sqrt{n})$

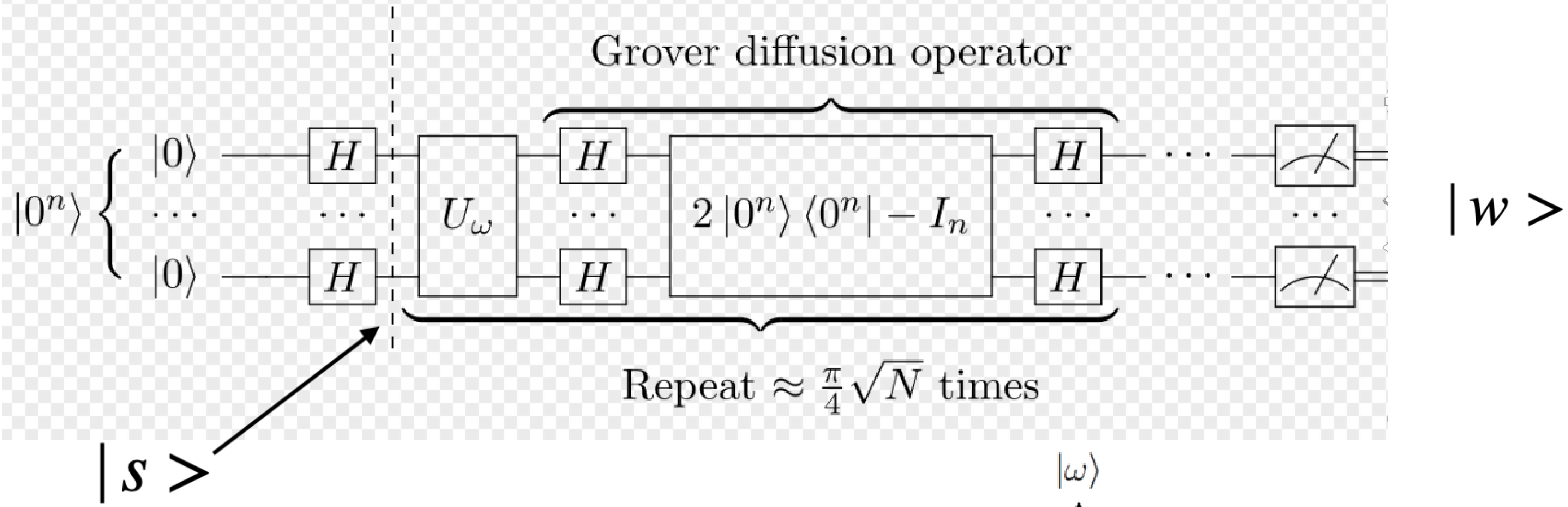


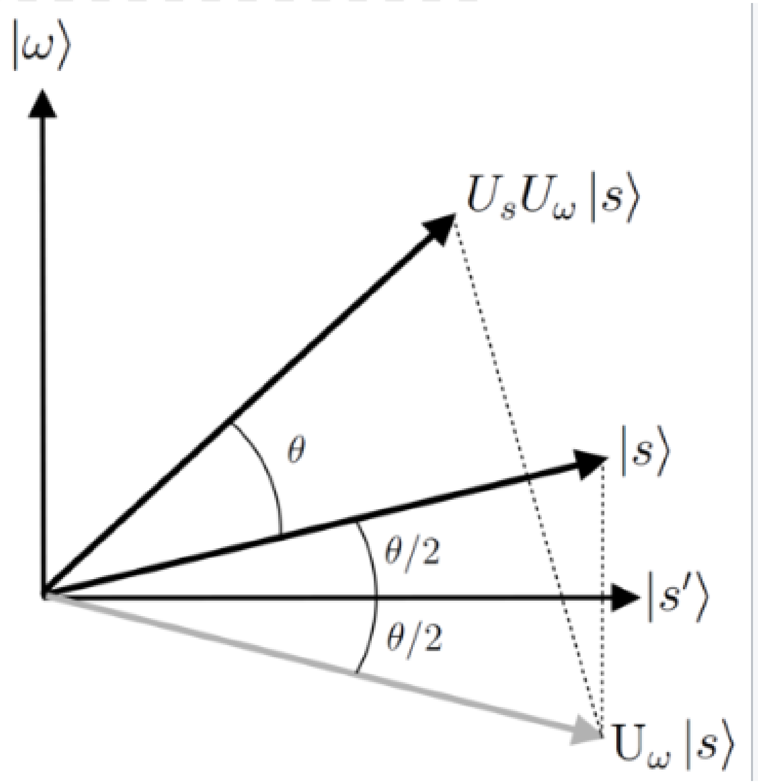
$$|w>$$

$$|s> \longrightarrow \boxed{\text{Oracle}} \longrightarrow |w>$$

Initial State
(like a Search space)

Measurement
Reslut



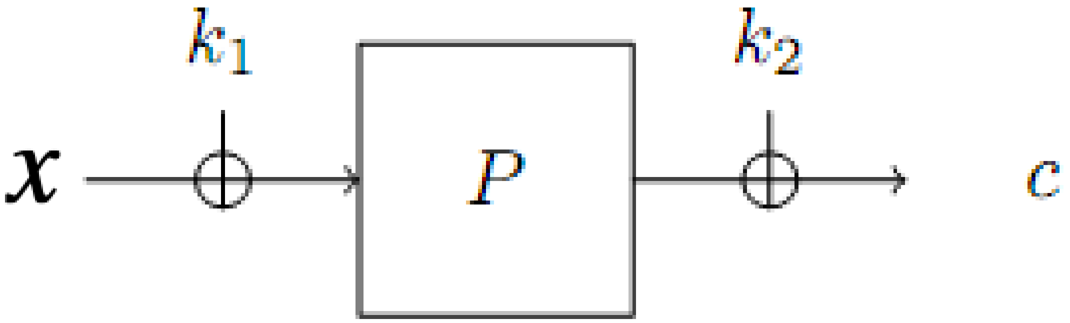


Notes: Optimal iteration $\sim \mathcal{O}(\sqrt{n})$

Success probability: $\sim [1 - \frac{1}{\sqrt{N}}]$

Can be generalized: Amplitude Amplification algorithm

Attacks on Even –Mansour Construction



k_1 & k_2 Key Length : n
P is public permutation block
(Unkeyed primitive)

- Classically for q number of queries, attacker's advantage is $q^2/2^n$
- Completely insecure using Simon's Algorithm with following equation.

$$f(x) := \mathrm{Enc}_{EM}(x) + P(x) = P(x + k_1) + k_2 + P(x)$$

Note: '+' is the bitwise XOR

Observation: $f(x) = f(x + k_1)$ [With period '$\mathbf{k_1}$']

Using Simon's algorithm, could be broken in O(n) Quantum queries

Period finding problem: Simon Algorithm

Context: Given function 'f' (either 1:1 or 2:1)

$$\text{given } x_1, x_2 : \quad f(x_1) = f(x_2)$$
$$\text{it is guaranteed } : \quad x_1 \oplus x_2 = b$$

Goal: find 'b'.

Classical: $\sim \mathcal{O}(2^{n-1})$

Quantum: $\sim \mathcal{O}(n)$

$$\boxed{\text{Simon}} \longrightarrow |z_i>$$

Measurement Reslut

$$\begin{cases} b \cdot z_1 = 0 \\ b \cdot z_2 = 0 \\ \vdots \\ b \cdot z_n = 0 \end{cases}$$

Assume: $b = b_1 b_2 \ldots b_n$

Solve for 'b'

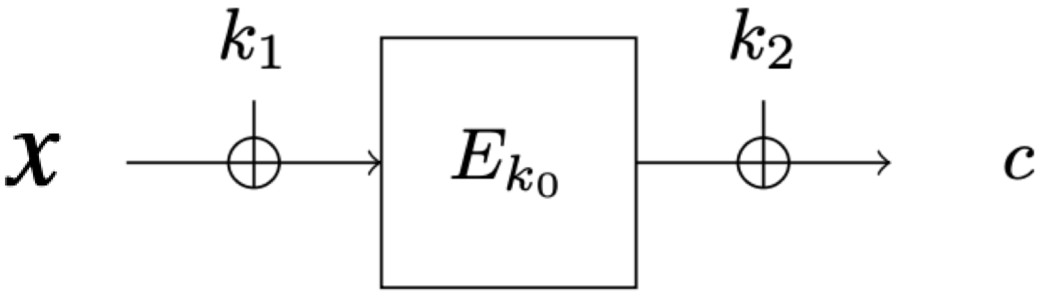
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle^{\otimes n} \longrightarrow |\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \longrightarrow |\psi_4\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |y\rangle) \longrightarrow |\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} [(-1)^{x \cdot z} + (-1)^{y \cdot z}] |z\rangle$$

$$\downarrow$$

$$(-1)^{x \cdot z} = (-1)^{y \cdot z} \longrightarrow$$

$$\begin{aligned} x \cdot z &= y \cdot z \\ x \cdot z &= (x \oplus b) \cdot z \\ x \cdot z &= x \cdot z \oplus b \cdot z \\ b \cdot z &= 0 \pmod 2 \end{aligned}$$

FX Construction



k_1 & k_2 Key Length : n
'E' is the block cipher with key k_0 of length: m- bits

Classically for q number of queries, attacker's success probability is bounded by $q^2/2^{n+m}$

Quantum Algorithms (Grover or Simon individually) does not provide significant improvements.

FX Construction

- Quantum Algorithms (Grover or Simon individually) does not provide significant improvements.

$$f(k,x) = \mathrm{Enc}(x) + E_k(x) = E_{k_0}(x + k_1) + k_2 + E_k(x).$$

- Grover algorithm finds k_0 and Simon finds k_1, but both are interdependent on each other

Idea Proposed

Parallel execution of Simon and Grover algorithm.

Deferred measurement.

Using this setup, FX Construction can be broken in $O(L+n).2^{L/2}$, approx same as without key whitening.

Merging Simon and Grover

Challenge

- Grover algorithm requires all possible states to be in superposition while Simon algorithm extracts the period bit wise and requires several instances to find the period.

Solution

"l" parallel instances of simon algorithm is embedded.

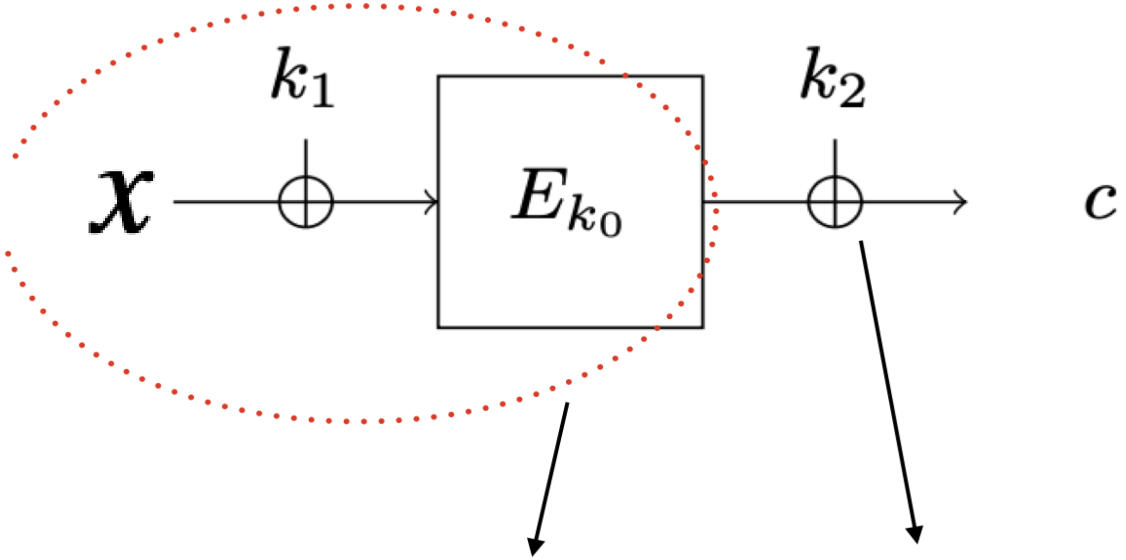
The operator used for amplitude amplification, $Q = A\ S_0\ A^{-1}\ S_{B}$.

A operator allows parallel embedding of Simon Algorithm.

Requires m+nl+nl qubits for execution.

State of qubits defines the possible candidate for (k_0, K_1).

Breaking FX- Construction: Computation and resource analysis



$k_0 \in \mathbb{F}_2^m \qquad k_1 \in \mathbb{F}_2^n$

$k_2 \in \mathbb{F}_2^n \qquad x \in \mathbb{F}_2^n$

$$f(k_0, k_1, k_2, x) \to g(k_0, k_1 + x) + k_2$$

- Adversary power: Quantum oracle access to $f_{k_0, k_1, k_2}(\cdot)$ and $g(\cdot, \cdot)$
- Success probability to estimate tuple (k_0, k_1, k_2): at least $\frac{2}{5}$ using:-
- Resources: $m + 4n(n + \sqrt{n})$ qubit.
- Cost: $2^{m/2} \cdot \mathcal{O}(m + n)$ oracle queries.

Breaking FX- Construction: Main ideas and Strategies

- Strategy-I : $f'(k_0, x) = g(k_0, x + k_1) + k_2 + g(k_0, x)$, $\forall x$
- Nature of $g(k_0, x)$ is like a random function for $k \neq k_0$.
- For $k = k_0$, $f'(k_0, x + k_1) = f'(k_0, x)$; hence periodic with $period = k_1$

- Strategy-II : Amplitude amplification for searching k_0
- Strategy-III : Simon Algorithm to estimate period of $f'(k, \cdot)$

- Caveat: Analysis fails for the trivial case $k_1 = 0^n$
- Because, $f'(k_0, x) = g(k_0, x) + k_2 + g(k_0, x) = k_2$

Case $k_1 = 0^n$: Fixing by Deutsch-Josza Algorithm:

- Recall for $k \neq k_0$, $g(k, \cdot\,)$ is like a random function.
- Hence, $f'\ (k, \cdot\,)$ is balanced in each output bits.
- Otherwise it is Constant. ('Good' state)
- D-J algorithm for balanced and constant function.

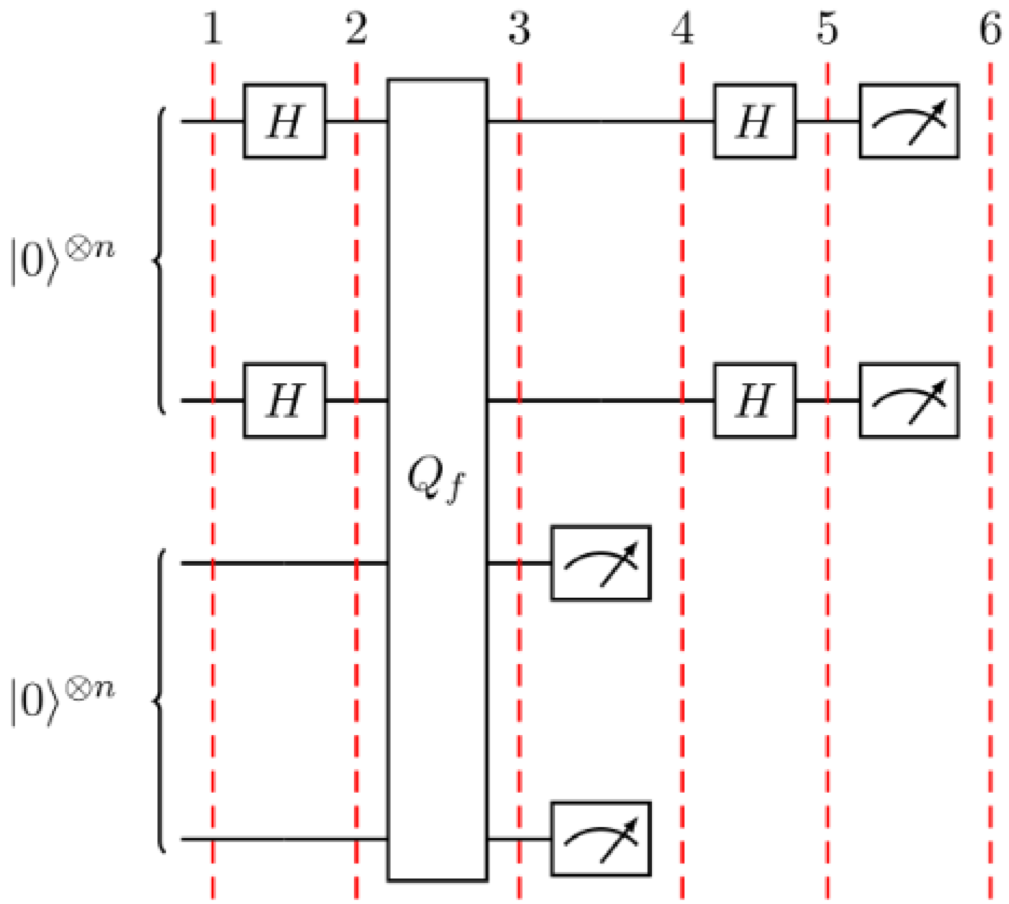
Computational Cost: $2^{\frac{m}{2}} \cdot \mathcal{O}(m)$ quantum queries.

Simon Algorithm circuit

$$\begin{cases} b \cdot z_1 = 0 \\ b \cdot z_2 = 0 \\ \quad \vdots \\ b \cdot z_n = 0 \end{cases}$$

Take: $b = b_1 b_2 \ldots b_n$

Solve for 'b'

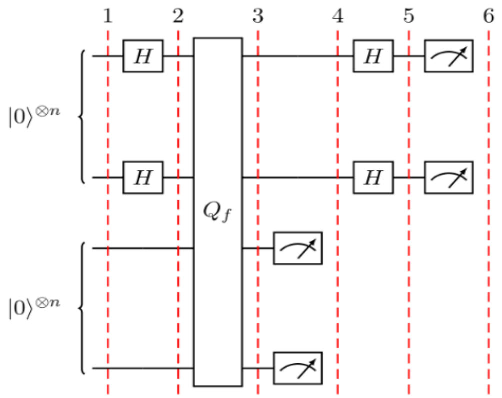


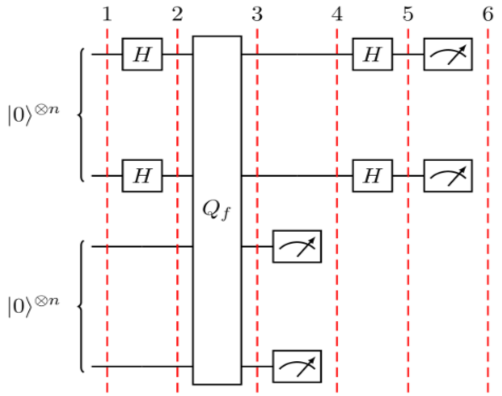
$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

- Measure second register
- Measure First register to get 'z'

Pic Ref: Qiskit

Avoiding measurement: Parallel Run of Simon



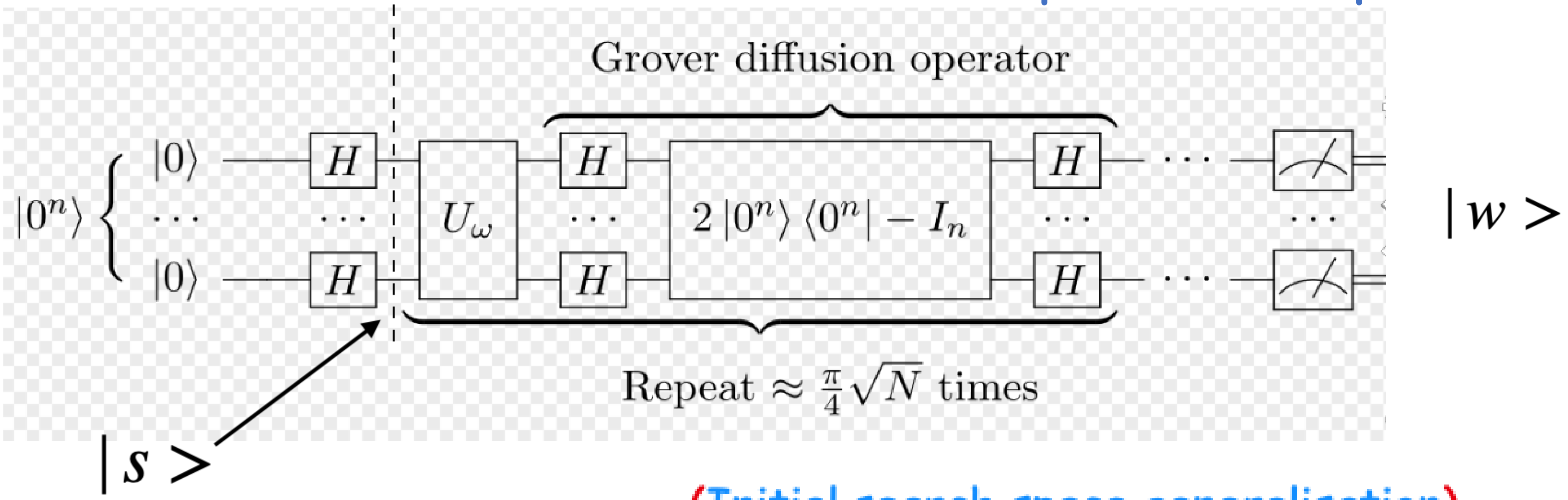


$$\begin{cases} b \cdot z_1 = 0 \\ b \cdot z_2 = 0 \\ \quad \vdots \\ b \cdot z_n = 0 \end{cases}$$

Assume: $b = b_1 b_2 \ldots b_n$

Solve for 'b'

Generalization of Grover: Amplitude Amplification



(Initial search space generalisation)

- Generalise equal superposition |s > to arbitrary superposition [A|0 >].
- Interpret A|0 > as output of an algorithm acting on state |0 >.

(Grover's U_w generalisation)

- Now $S_{\mathbb{B}}$ categorising states as 'good' and 'bad' states
- Changes sign of the 'good' state that get amplifies further on.

Example: $A|0> \rightarrow [p_0|Good> + p_1|Bad_1> + p_2|Bad_2> + \ldots.]$

Pic Ref: Wiki image

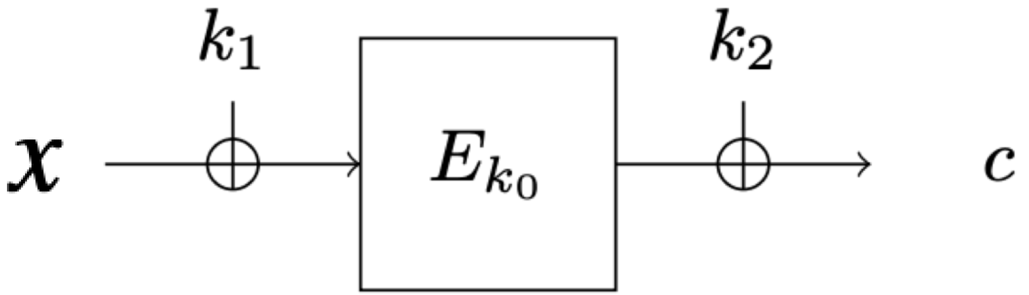
(Number of optimal iteration 'k')

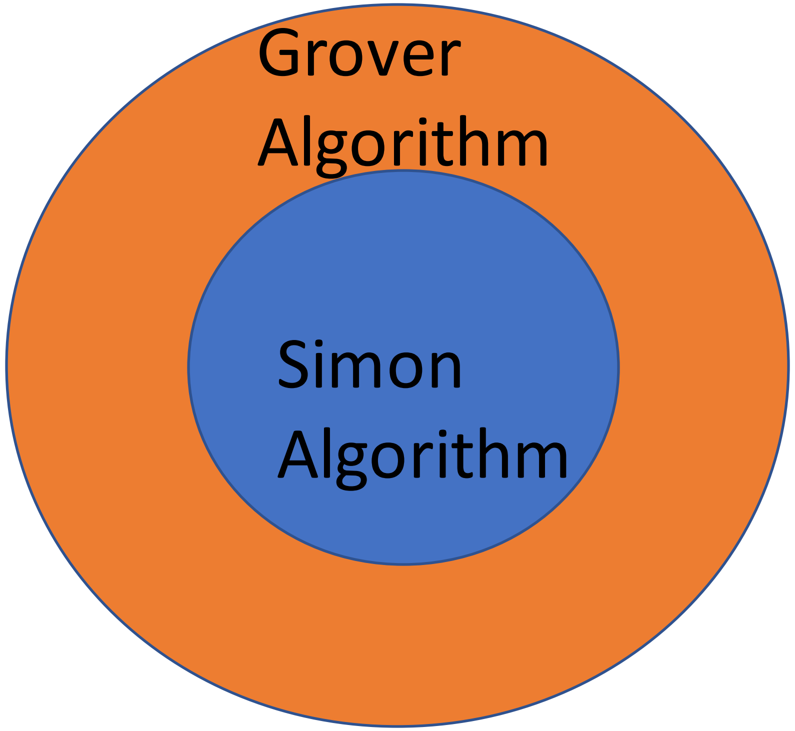
- Depends on probability of 'good state' in the superposition state.
- If $p = sin^2(\theta)$, then $k = \lceil \frac{\pi}{4 \cdot \theta} \rceil$.
-

(Search iteration operator)

- 'k' iteration of $Q = -AS_0A^{\dagger}S_B$ on $A|0>$
- Measure $Q^kA\,|\,0>$ to get 'good' state with high probability

Algorithmic Symbiosis: Grover + Simon





Expectation from grover: Quadratic speed up for k_0 search

Grover need help: 'good' and 'bad' state classifier (!)

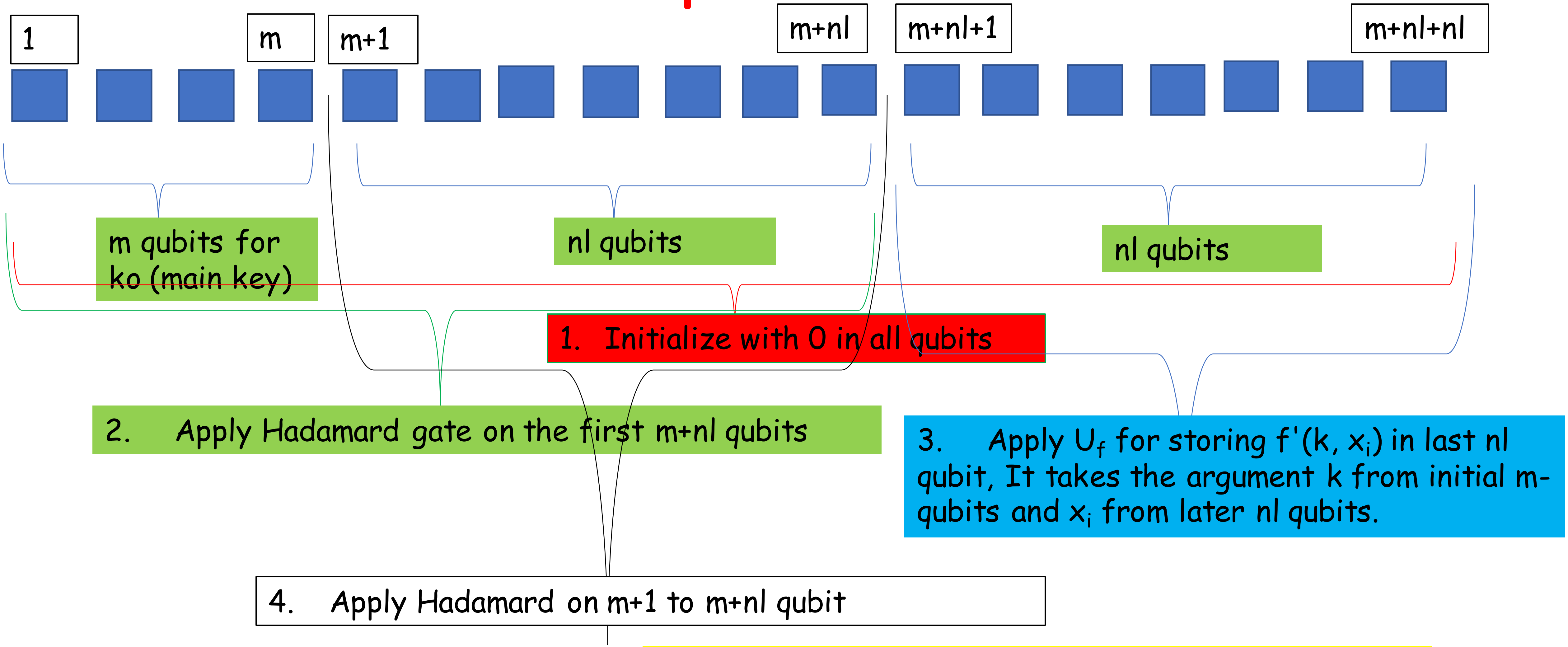
Expectation from Simon: Find period k_1 in polynomial no. of queries.

Simon requirement: Given function shall have some nice structure.

Simon helps in 'good' and 'bad' state classification. 'Good ' get amplified.

Simon has nice structure if guess $k = k_0$ is correct.

Construction of Operator 'A'



After 4th step, final state becomes the following form

$$|\psi\rangle = \left(\frac{1}{2}\right)^{\frac{m+nl}{2}} \left(\frac{1}{2}\right)^{\frac{nl}{2}} \sum_{\{k,u_j,x_j\}} |k\rangle (-1)^{\langle u_1,x_1\rangle} |u_1\rangle \ldots (-1)^{\langle u_l,x_l\rangle} |u_l\rangle \left|f'(k,x_1)\right\rangle \ldots \left|f'(k,x_l)\right\rangle$$

Analysis of the state (wavefunction)

Corresponds to candidates of block cipher key k_0

Simon oracle Query U_f

$$|\psi\rangle = \sum_{\substack{k\in\mathbb{F}_2^m,\ u_1,\ldots,u_\ell\in\mathbb{F}_2^n,\\ x_1,\ldots,x_\ell\in\mathbb{F}_2^n}} |k\rangle(-1)^{\langle u_1,x_1\rangle}|u_1\rangle\ldots(-1)^{\langle u_\ell,x_\ell\rangle}|u_{n-1}\rangle|h(k,x_1,\ldots,x_\ell)\rangle.$$

Relates to Simon instances

$$|z_i> = (-1)^{<u_i|x_i>}|u_i>$$

After Measurement

- After applying A-oprator, the last |Ψ> state was obtained.
- Measurement is performed on last 'nl' bits, which collapses |Ψ> to :-

$$|h(k, x_1, \ldots, x_\ell)\rangle = |f'(k, x_1)||f'(k, x_2)||\ldots||f'(k, x_\ell)\rangle$$

- Assuming k = ko, the collapsed f'(k, x_i) in 'm+nl+1' to 'm+2nl' qubits entangled with corresponding qubit states from 'm+1' to 'm+nl'.
- Considering |**f'(k, x)** > is proper (have two preimages), then corresponding preimages are :-

$$\left((-1)^{\langle u_i, x_i\rangle} + (-1)^{\langle u_i, x_i + k_1\rangle}\right)|u_i\rangle = (-1)^{\langle u_i, x_i\rangle}\left(1 + (-1)^{\langle u_i, k_1\rangle}\right)|u_i\rangle.$$

- For non-vanishing amplitude in RHS, $< \mathbf{u_i} \mid \mathbf{k_1} > = \mathbf{0}$. [condition for period]

'Good' and 'Bad' state Classifier (For Grover)

Classifier: mark states as 'good' (if, $k' = k_o$), otherwise bad ($k' \neq k_o$).

- U_i's value obtained from parallel Simon's instances , satisfies $< u_i , k_1 > = 0$.

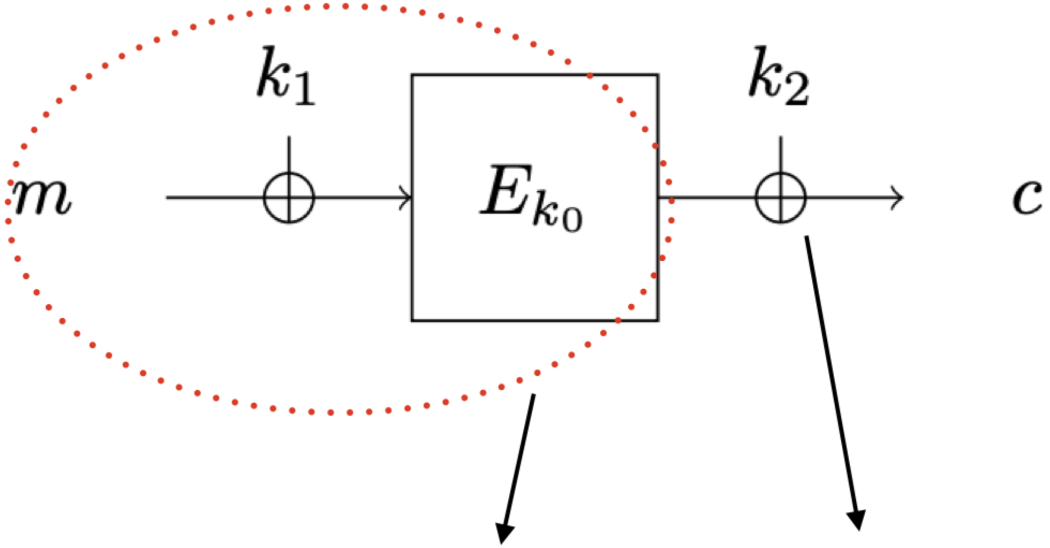
- If $k = k_o$, then obtained k_1 is the periodicity in f(k, .).
- Those states are classified as 'good' states, otherwise 'bad'.

- If classifier succeeds in finding candidates (k', k'_1) as candidate for (ko, k_1), then (k', k'_1) are checked for validity with message and cipher text pairs.

$$c_i + c_i' = \mathrm{Enc}(m) + \mathrm{Enc}(m') = E_{k_0}(m_i + k_1) + E_{k_0}(m_i' + k_1)$$
$$\stackrel{?}{=} E_k(m_i + k_1') + E_k(m_i' + k_1').$$

For message x=m,m'

Final Step for recovery of the key-set



$$f(k_0,\ k_1,\ k_2,\ x) \to g(k_0,\ k_1 + x) + k_2$$

- With recovery of $k_0,\ k_1$, the crypto system has weekend a lot.
- To recover k_2 , we make the query as :
- $k_2 = f_{k_0,\ k_1,\ k_2} + g(k_0, x + k_0)$
- Finally we have, $(k_0,\ k_1,\ k_2)$

References:

Gregor Leander and Alexander May (Grover meets Simon)
https://www.iacr.org/archive/asiacrypt2017/106240174/106240174.pdf

Qiskit tutorial

Thanks!