Improvements to low-qubit quantum resource estimates for quantum search

James H. Davenport[1] and Benjamin Pring[1,2]

5th April 2019

[1]University of Bath and [2]University of South Florida

Talk overview I

We'll be interested in the *single-target search problem*

Talk overview I

We'll be interested in the *single-target search problem*

$N = 2^n$ items

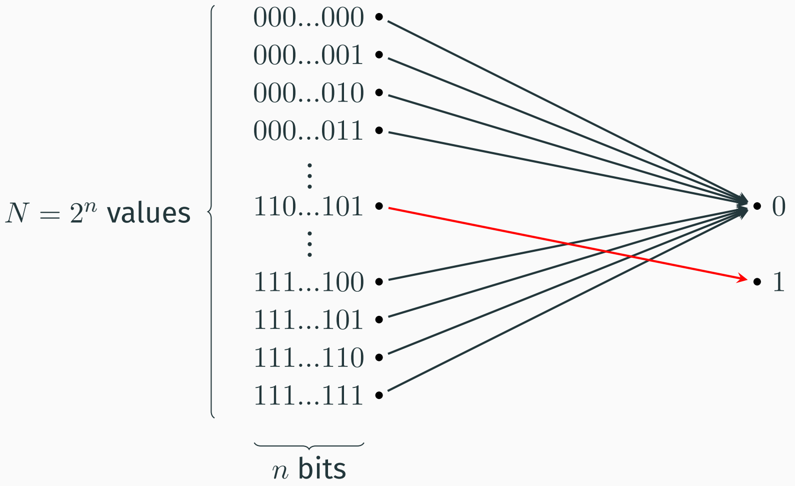
$$
N = 2^n \text{ values} \left\{
\begin{array}{l}
000\ldots000 \bullet \\
000\ldots001 \bullet \\
000\ldots010 \bullet \\
000\ldots011 \bullet \\
\quad\vdots \\
110\ldots101 \bullet \\
\quad\vdots \\
111\ldots100 \bullet \\
111\ldots101 \bullet \\
111\ldots110 \bullet \\
111\ldots111 \bullet
\end{array}
\right.
$$

$$\underbrace{\hphantom{111\ldots111}}_{n \text{ bits}}$$

Talk overview I

We'll be interested in the *single-target search problem*

$N = 2^n$ items and there exists a **unique** item that satisfies a property



Talk overview II

Cryptanalysis can be performed by solving the search problem

Talk overview II

Cryptanalysis can be performed by solving the search problem

$$\downarrow$$

Grover's quantum search algorithm solves the search problem with asymptotically fewer resources than classical computers

Talk overview II

Cryptanalysis can be performed by solving the search problem

$\downarrow$

Grover's quantum search algorithm solves the search problem with asymptotically fewer resources than classical computers

$\downarrow$

How can we optimise quantum search and what impact does this have on cryptanalysis?

Talk overview III

1. Defining the search problem and motivating examples
2. Quantum search and applications to cryptanalysis
3. Optimising quantum cryptographic search in the average-case
4. Ensuring success in the worst-case

The search problem I

What exactly does Grover's algorithm solve?

Definition (The unstructured search problem)

Let $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ and $M_\chi = |\chi^{-1}(1)|$.

The *unstructured search problem* is to find an $x \in \{0,1\}^n$ such that $\chi(x) = 1$, given only the ability to evaluate χ.

The search problem I

What exactly does Grover's algorithm solve?

Definition (The unstructured search problem)

Let $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ and $M_\chi = |\chi^{-1}(1)|$.

The *unstructured search problem* is to find an $x \in \{0,1\}^n$ such that $\chi(x) = 1$, given only the ability to evaluate χ.

Features of this definition

1. Makes no assumption about the function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$
2. Makes no assumptions about the distribution of solutions
3. As generic as possible — applicable to a wide variety of problems

The search problem II

What is the cost to solve the single-target search problem?

The search problem II

What is the cost to solve the single-target search problem?

Reduction to uniform distribution is simple

$$\downarrow$$

Choose a random permutation $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$ and define

$$\chi_\pi(x) \mapsto \chi(\pi(x))$$

The search problem II

What is the cost to solve the single-target search problem?

Reduction to uniform distribution is simple

$$\downarrow$$

Choose a random permutation $\pi : \{0,1\}^n \longrightarrow \{0,1\}^n$ and define

$$\chi_\pi(x) \mapsto \chi(\pi(x))$$

For any ordering $x_1, \ldots, x_{2^n} \in \{0,1\}^n$: simply test $\chi_\pi(x_1), \ldots, \chi_\pi(x_{2^n})$

- Average-case cost : $\frac{2^n+1}{2}$ evaluations of χ
- Worst-case cost : 2^n evaluations of χ

The search problem III

$O(2^n)$ evaluations or *queries* of the function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

The search problem III

$O(2^n)$ evaluations or *queries* of the function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

...but this ignores the cost of evaluating $\chi(x)$. Full cost:

$$O(2^n \cdot E_\chi)$$

where E_χ is the cost of evaluating χ in terms of bit-operations.

The search problem III

$O(2^n)$ evaluations or *queries* of the function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

...but this ignores the cost of evaluating $\chi(x)$. Full cost:

$$O(2^n \cdot E_\chi)$$

where E_χ is the cost of evaluating χ in terms of bit-operations.

Asymptotically negligible — but a very real-world cost.

The search problem IV

Cost of classical exhaustive search in the worst-case: $2^n \cdot E_\chi$

How can we improve upon this?

The search problem IV

Cost of classical exhaustive search in the worst-case: $2^n \cdot E_\chi$

How can we improve upon this?

1. Exploit structure to reduce the number of evaluations of χ
2. Exploit structure to reduce the cost of evaluating χ

No structure in the unstructured search problem(!)

The search problem V

Theorem (Grover's algorithm [Gro98])

There exists a quantum algorithm to solve the single-target unstructured search problem defined by $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ that requires $O(2^{n/2})$ calls to a quantum circuit $\mathcal{O}_\chi$ that evaluates χ.

$$O(2^{n/2} \cdot E_{\mathcal{O}_\chi})$$

The search problem VI

Consider the case $E_\chi \approx n^3$ and the unstructured search problem

$$\chi : \{0,1\}^{128} \longrightarrow \{0,1\} \qquad \text{where} \qquad M_\chi = |\chi^{-1}(1)| = 1$$

Cost in terms of classical bit operations :

$$\approx 2^{128} \cdot 128^3 \approx 2^{149}$$

Cost in terms of quantum gates :

$$\approx 2^{64} \cdot 128^3 \quad \approx 2^{85}$$

The search problem VI

Consider the case $E_\chi \approx n^3$ and the unstructured search problem

$$\chi : \{0,1\}^{128} \longrightarrow \{0,1\} \qquad \text{where} \qquad M_\chi = |\chi^{-1}(1)| = 1$$

Cost in terms of classical bit operations :

$$\approx 2^{128} \cdot 128^3 \approx 2^{149}$$

Cost in terms of quantum gates :

$$\approx 2^{64} \cdot 128^3 \quad \approx 2^{85}$$

Q. Why do we care?

The search problem VI

Consider the case $E_\chi \approx n^3$ and the unstructured search problem

$$\chi : \{0,1\}^{128} \longrightarrow \{0,1\} \qquad \text{where} \qquad M_\chi = |\chi^{-1}(1)| = 1$$

Cost in terms of classical bit operations :

$$\approx 2^{128} \cdot 128^3 \approx 2^{149}$$

Cost in terms of quantum gates :

$$\approx 2^{64} \cdot 128^3 \quad \approx 2^{85}$$

Q. Why do we care?

1. Choosing secure parameters

The search problem VI

Consider the case $E_\chi \approx n^3$ and the unstructured search problem

$$\chi : \{0,1\}^{128} \longrightarrow \{0,1\} \qquad \text{where} \qquad M_\chi = |\chi^{-1}(1)| = 1$$

Cost in terms of classical bit operations :

$$\approx 2^{128} \cdot 128^3 \approx 2^{149}$$

Cost in terms of quantum gates :

$$\approx 2^{64} \cdot 128^3 \quad \approx 2^{85}$$

Q. Why do we care?

1. Choosing secure parameters
2. Quantifying the full resources required to attack schemes

The search problem VII

Say Grover's search algorithm is the best attack on a cryptosystem.

How do we derive parameters for a cryptographic scheme?

a) The lower-bound $O(2^{n/2})$?
    - Secure
    - Large parameters
b) The full cost $O(2^{n/2} \cdot E_{\mathcal{O}_\chi})$?
    - Smaller parameter sizes
    - Scheme is then vulnerable to optimisations of quantum search

The search problem VIII

Case study 1: The Gui cryptosystem

- Hidden Field Equations (HFE) public-key signature scheme
- Solve the *Multivariate Quadratic problem over* $\mathbb{F}_2 \implies$ break Gui.

The search problem VIII

Case study 1: The Gui cryptosystem

- Hidden Field Equations (HFE) public-key signature scheme
- Solve the *Multivariate Quadratic problem over* $\mathbb{F}_2 \implies$ break Gui.

Given $f^{(1)}, \ldots, f^{(m)} \in \mathbb{F}_2[x_1, \ldots, x_n]$ find $(x_1, \ldots, x_m) \in \mathbb{F}_2^n$ such that:

$$\begin{aligned}
f^{(1)}(x_1, \ldots, x_n) &= \sum_{1 \leq i < j \leq n} a_{i,j}^{(1)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(1)} x_i + c^{(1)} = 0 \\
&\vdots \\
f^{(m)}(x_1, \ldots, x_n) &= \sum_{1 \leq i < j \leq n} a_{i,j}^{(m)} x_i x_j + \sum_{1 \leq i \leq n} b_i^{(m)} x_i + c^{(m)} = 0
\end{aligned}$$

where $a_{i,j}^{(k)}, b_i^{(k)}, c_i^{(k)} \in \mathbb{F}_2$.

$$\chi : \{0,1\}^n \longrightarrow \{0,1\}$$

$$\chi(x_1 \ldots x_n) \mapsto \overline{f^{(1)}(x_1, \ldots, x_n)} \wedge \cdots \wedge \overline{f^{(m)}(x_1, \ldots, x_n)}$$

The search problem VIII

Case study 1: The Gui cryptosystem

- Hidden Field Equations (HFE) public-key signature scheme
- Solve the *Multivariate Quadratic problem over* $\mathbb{F}_2 \implies$ break Gui.

Timeline

2015 Gui cryptosystem proposed [PCY+15].

- No cost for the quantum circuit for Grover's algorithm known.
- Parameters chosen assuming cost of Grover is $O(2^{n/2})$.

The search problem VIII

Case study 1: The Gui cryptosystem

- Hidden Field Equations (HFE) public-key signature scheme
- Solve the *Multivariate Quadratic problem over* $\mathbb{F}_2 \implies$ break Gui.

Timeline

2015 Gui cryptosystem proposed [PCY+15].
- No cost for the quantum circuit for Grover's algorithm known.
- Parameters chosen assuming cost of Grover is $O(2^{n/2})$.

2016 Quantum circuits to solve the $\mathcal{MQ}$ over $\mathbb{F}_2$ with Grover [SW16].
- $n + m + 2$ qubits
- $n + \lfloor \log_2(m+1) \rfloor + 3$ qubits but double the #quantum gates
- Cost of Grover attack: $O(2^{n/2} \cdot mn^2)$

The search problem VIII

Case study 1: The Gui cryptosystem

- Hidden Field Equations (HFE) public-key signature scheme
- Solve the *Multivariate Quadratic problem over* $\mathbb{F}_2 \implies$ break Gui.

Timeline

2015 Gui cryptosystem proposed [PCY+15].

- No cost for the quantum circuit for Grover's algorithm known.
- Parameters chosen assuming cost of Grover is $O(2^{n/2})$.

2016 Quantum circuits to solve the $\mathcal{MQ}$ over $\mathbb{F}_2$ with Grover [SW16].

- $n + m + 2$ qubits
- $n + \lfloor \log_2(m+1) \rfloor + 3$ qubits but double the #quantum gates
- Cost of Grover attack: $O(2^{n/2} \cdot mn^2)$

2017 Parameters [PCDY17] derived from Grover costing $O(2^{n/2} \cdot mn^2)$

The search problem IX

Gui(n, D, a, v, k)	Security level	Cryptanalysis target	Source
Gui$(94, 17, 4, 4, 4)$	$\lambda = 80$ (classical)	$4\times\mathcal{MQ}(\mathbb{F}_2, 90, 90)$	[PCY+15]
Gui$(95, 9, 5, 5, 3)$	$\lambda = 80$ (classical)	$3\times\mathcal{MQ}(\mathbb{F}_2, 90, 90)$	[PCY+15]
Gui$(96, 5, 6, 6, 3)$	$\lambda = 80$ (classical)	$3\times\mathcal{MQ}(\mathbb{F}_2, 90, 90)$	[PCY+15]
Gui$(127, 9, 3, 4, 4)$	$\lambda = 120$ (classical)	$4\times\mathcal{MQ}(\mathbb{F}_2, 124, 124)$	[PCY+15]
Gui$(188, 17, 4, 4, 4)$	$\lambda = 80$ (quantum)	$4\times\mathcal{MQ}(\mathbb{F}_2, 184, 184)$	[PCY+15]
Gui$(190, 9, 5, 5, 3)$	$\lambda = 80$ (quantum)	$3\times\mathcal{MQ}(\mathbb{F}_2, 185, 185)$	[PCY+15]
Gui$(192, 5, 6, 6, 3)$	$\lambda = 80$ (quantum)	$3\times\mathcal{MQ}(\mathbb{F}_2, 186, 186)$	[PCY+15]
Gui$(254, 9, 3, 4, 4)$	$\lambda = 120$ (quantum)	$4\times\mathcal{MQ}(\mathbb{F}_2, 251, 251)$	[PCY+15]
Gui$(120, 9, 3, 3, 2)$	$\lambda = 80$ (quantum)	$2\times\mathcal{MQ}(\mathbb{F}_2, 117, 117)$	[PCDY17]
Gui$(212, 9, 3, 4, 2)$	$\lambda = 128$ (quantum)	$2\times\mathcal{MQ}(\mathbb{F}_2, 209, 209)$	[PCDY17]
Gui$(464, 9, 7, 8, 2)$	$\lambda = 256$ (quantum)	$2\times\mathcal{MQ}(\mathbb{F}_2, 457, 457)$	[PCDY17]

Table 1: Suggested parameters for the Gui cryptosystem [PCY+15, PCDY17].

The search problem X

Gui(n, D, a, v, k)	Security level	Cryptanalysis target	Source
Gui$(192, 5, 6, 6, 3)$	$\lambda = 80$ (quantum)	$3\times\mathcal{MQ}(\mathbb{F}_2, 186, 186)$	[PCY+15]
Gui$(120, 9, 3, 3, 2)$	$\lambda = 80$ (quantum)	$2\times\mathcal{MQ}(\mathbb{F}_2, 117, 117)$	[PCDY17]

Table 2: Suggested parameters for the Gui cryptosystem [PCY+15, PCDY17].

Difference in public-key sizes

465 kB vs 113 kB

The search problem XII

Case study 2:

What resources required to attack block-ciphers with quantum search?

$$\mathsf{ENC} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

$$\mathsf{DEC} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

$$\forall K \in \{0,1\}^k : \mathsf{DEC}(K, \mathsf{ENC}(K, P)) = P$$

The search problem XII

Case study 2:

What resources required to attack block-ciphers with quantum search?

$$\mathsf{ENC}: \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

The search problem XII

Case study 2:

What resources required to attack block-ciphers with quantum search?

$$\mathsf{ENC} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

Scenario:

- Let $K \in \{0,1\}^k$ be an unknown fixed key.
- Say we possess r *known plaintext-ciphertext* pairs for K

$$\Big\{(P_1, C_1), \ldots, (P_r, C_r) \ : \ P_i, C_i \in \{0,1\}^n \text{ and } C_i = \mathsf{ENC}(K, P_i)\Big\}$$

The search problem XII

Case study 2:

What resources required to attack block-ciphers with quantum search?

$$\mathsf{ENC} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$$

Scenario:

- Let $K \in \{0,1\}^k$ be an unknown fixed key.
- Say we possess r *known plaintext-ciphertext* pairs for K

$$\Big\{(P_1, C_1), \ldots, (P_r, C_r) \;:\; P_i, C_i \in \{0,1\}^n \text{ and } C_i = \mathsf{ENC}(K, P_i)\Big\}$$

$$\chi : \{0,1\}^k \longrightarrow \{0,1\}$$

$$\chi(x_1 \ldots x_k) \mapsto \Big(\mathsf{ENC}(x_1 \ldots x_k, P_1) \stackrel{?}{=} C_1\Big) \wedge \cdots \wedge \Big(\mathsf{ENC}(x_1 \ldots x_k, P_r) \stackrel{?}{=} C_r\Big)$$

The search problem XIII

$$\chi : \{0,1\}^k \longrightarrow \{0,1\}$$

$$\chi(x_1 \dots x_k) \mapsto \left(\mathsf{ENC}(x_1 \dots x_k, P_1) \stackrel{?}{=} C_1\right) \wedge \dots \wedge \left(\mathsf{ENC}(x_1 \dots x_k, P_r) \stackrel{?}{=} C_r\right)$$

$$\Downarrow$$

We expect $1 + (2^k - 1) \cdot 2^{-rn}$ solutions to χ

The search problem XIII

$$\chi : \{0,1\}^k \longrightarrow \{0,1\}$$

$$\chi(x_1 \dots x_k) \mapsto \Big(\mathsf{ENC}(x_1 \dots x_k, P_1) \stackrel{?}{=} C_1\Big) \wedge \cdots \wedge \Big(\mathsf{ENC}(x_1 \dots x_k, P_r) \stackrel{?}{=} C_r\Big)$$

$$\Downarrow$$

We expect $1 + (2^k - 1) \cdot 2^{-rn}$ solutions to χ

$$\Downarrow$$

Just choose r large enough to uniquely specify the key.

- AES-128 requires $r \geq 2$
- AES-192 requires $r \geq 2$
- AES-256 requires $r \geq 3$

The search problem XIV

Common structure in both search problems $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x),$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

The search problem XIV

Common structure in both search problems $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x),$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

We can lower the classical cost of the search via a *filtering strategy*:

0. Choose an untested $x \in \{0,1\}^n$

The search problem XIV

Common structure in both search problems $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x),$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

We can lower the classical cost of the search via a *filtering strategy*:

0. Choose an untested $x \in \{0,1\}^n$
1. If $\chi_1(x) = 1$ then continue; otherwise restart

The search problem XIV

Common structure in both search problems $\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x),$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

We can lower the classical cost of the search via a *filtering strategy*:

0. Choose an untested $x \in \{0,1\}^n$
1. If $\chi_1(x) = 1$ then continue; otherwise restart
2. If $\chi_2(x) = 1$ then continue; otherwise restart

$\vdots$

i. If $\chi_i(x) = 1$ then continue; otherwise restart

$\vdots$

k. If $\chi_k(x) = 1$ then output $\chi(x) = 1$;

Quantum computing 101

1. For each $x \in \{0,1\}^n$ there exists a unique quantum basis state $|x\rangle$.

Quantum computing 101

1. For each $x \in \{0,1\}^n$ there exists a unique quantum basis state $|x\rangle$.
2. A quantum state consisting of n qubits can be expressed as

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \text{where} \qquad \alpha_x \in \mathbb{C}$$

   and where

$$\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1.$$

Quantum computing 101

1. For each $x \in \{0,1\}^n$ there exists a unique quantum basis state $|x\rangle$.
2. A quantum state consisting of n qubits can be expressed as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \qquad \text{where} \qquad \alpha_x \in \mathbb{C}$$

   and where

$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1.$$

3. Measurement of $|\psi\rangle$ results in $x \in \{0,1\}^n$ with probability $|\alpha_x|^2$ and *collapses* the quantum state to $|x\rangle$.

Quantum computing 101

1. For each $x \in \{0,1\}^n$ there exists a unique quantum basis state $|x\rangle$.
2. A quantum state consisting of n qubits can be expressed as

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \text{where} \qquad \alpha_x \in \mathbb{C}$$

   and where

$$\sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1.$$

3. Measurement of $|\psi\rangle$ results in $x \in \{0,1\}^n$ with probability $|\alpha_x|^2$ and *collapses* the quantum state to $|x\rangle$.
4. Quantum algorithms map quantum states to quantum states

$$\mathcal{A}\,|\psi\rangle \mapsto |\psi'\rangle$$

   and all *measurement-free* $\mathcal{A}$ have an inverse $\mathcal{A}^\dagger$ st. $\mathcal{A}^\dagger\mathcal{A} = I$.

Quantum computing 101

1. For each $x \in \{0,1\}^n$ there exists a unique quantum basis state $|x\rangle$.
2. A quantum state consisting of n qubits can be expressed as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \qquad \text{where} \qquad \alpha_x \in \mathbb{C}$$

   and where

$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1.$$

3. Measurement of $|\psi\rangle$ results in $x \in \{0,1\}^n$ with probability $|\alpha_x|^2$ and *collapses* the quantum state to $|x\rangle$.
4. Quantum algorithms map quantum states to quantum states

$$\mathcal{A}^\dagger \mathcal{A} |\psi\rangle \mapsto |\psi\rangle$$

   and all *measurement-free* $\mathcal{A}$ have an inverse $\mathcal{A}^\dagger$ st. $\mathcal{A}^\dagger \mathcal{A} = I$.

Quantum computing II

Any quantum algorithm can be approximated by using gates from a *universal quantum gate set*.

—

Metric: logical quantum circuit-complexity using *Clifford+T* gate set:

- Circuit-size — number of elementary quantum gates
- Circuit-depth — number of timesteps
- Circuit-width — number of qubits we require

—

Recent papers indicate a Depth$\times$Width metric may be realistic.

Definition (Success probability of a quantum algorithm)

Let $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ be any boolean function.

Let $\mathcal{A}$ be any quantum algorithm acting on n qubits.

The success probability of $\mathcal{A}$ relative to $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ is the probability of measuring the state

$$\mathcal{A}\,|0^n\rangle$$

and obtaining an $x \in \{0,1\}^n$ such that $\chi(x) = 1$.

Quantum computing IV

A basic quantum algorithm

$$H^{\otimes n}|0^n\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle$$

- $M_\chi = |\chi^{-1}(1)| \implies$ success probability of $H^{\otimes n}$ relative to χ is $\frac{M_\chi}{2^n}$.

$$\begin{array}{lcl}
|0\rangle & \text{—}\boxed{H}\text{—} & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
|0\rangle & \text{—}\boxed{H}\text{—} & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
|0\rangle & \text{—}\boxed{H}\text{—} & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
|0\rangle & \text{—}\boxed{H}\text{—} & \frac{|0\rangle+|1\rangle}{\sqrt{2}}
\end{array}$$

Quantum computing V

Definition (Quantum phase oracle)

The quantum phase oracle $\mathcal{O}_\chi$ defined by $\chi : \{0,1\}^n$ is the quantum algorithm such that for all $x \in \{0,1\}^n$

$$\mathcal{O}_\chi|x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } \chi(x) = 1 \\ |x\rangle & \text{if } \chi(x) = 0 \end{cases}$$

$$|x\rangle \;\; -\!\!/\!\!- \boxed{\mathcal{O}_\chi} -\!\!/\!\!- \;\; (-1)^{\chi(x)}\,|x\rangle$$

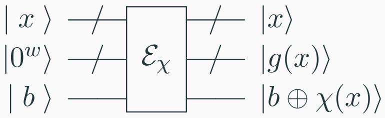
Quantum computing VI

Definition (Quantum evaluation of a boolean function)

A *quantum evaluation* $\mathcal{E}_\chi$ defined by $\chi : \{0,1\}^n \longrightarrow \{0,1\}$ is the quantum algorithm $\mathcal{E}_\chi$ such that for all $x \in \{0,1\}^n$ and $b \in \{0,1\}$

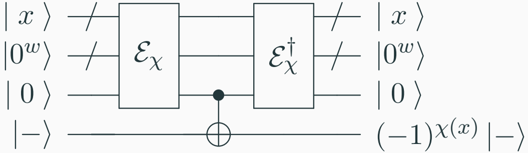
$$\mathcal{E}_\chi |x\rangle |0^w\rangle |b\rangle \mapsto |x\rangle |g(x)\rangle |b \oplus \chi(x)\rangle$$

where $g(x) \in \{0,1\}^w$ is the state of memory used to compute $\chi(x)$.



Quantum computing VII

$$
\begin{aligned}
|-\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
|- \oplus 0\rangle &= \frac{|0 \oplus 0\rangle - |1 \oplus 0\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \quad |-\rangle \\
|- \oplus 1\rangle &= \frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle
\end{aligned}
$$



Quantum computing VIII

Theorem (Amplitude amplification)

Let $\chi : \{0,1\}^n \longrightarrow$ *be any boolean function.*

Let $\mathcal{A}$ *be any quantum algorithm that uses no measurements with a success probability of* $a > 0$ *relative to* χ*.*

Then there exists a quantum algorithm $\mathcal{B}$ *that succeeds with probability* $\geq \max\{a, 1-a\}$ *and which costs*

$$E_{\mathcal{B}} = (2k+1)E_{\mathcal{A}} + k(E_{\mathcal{O}_\chi} + E_{\mathcal{O}_0})$$

where

$$k = \left\lfloor \frac{\pi}{4 \arcsin \sqrt{a}} \right\rfloor$$

Quantum computing VIII

Theorem (Amplitude amplification)

Let $\chi : \{0,1\}^n \longrightarrow$ be any boolean function.

Let $\mathcal{A}$ be any quantum algorithm that uses no measurements with a success probability of $a > 0$ relative to χ.

Then there exists a quantum algorithm $\mathcal{B}$ that succeeds with probability $\geq \max\{a, 1-a\}$ and which costs

$$E_{\mathcal{B}} \approx 2kE_{\mathcal{A}} + kE_{\mathcal{O}_\chi}$$

where

$$k \approx \frac{\pi}{4} \cdot \frac{1}{\sqrt{a}}$$

Quantum computing VIII

Theorem (Amplitude amplification)

Let $\chi : \{0,1\}^n \longrightarrow$ *be any boolean function.*

Let $\mathcal{A}$ *be any quantum algorithm that uses no measurements with a success probability of* $a > 0$ *relative to* χ*.*

Then there exists a quantum algorithm $\mathcal{B}$ *that succeeds with probability* $\geq \max\{a, 1-a\}$ *and which costs*

$$E_{\mathcal{B}} \approx 2kE_{\mathcal{A}} + kE_{\mathcal{O}_\chi}$$

where

$$k \approx \frac{\pi}{4} \cdot \frac{1}{\sqrt{a}}$$

- Set $\mathcal{A} = H^{\otimes n}$ then we have Grover's algorithm.

Quantum computing IX

Theorem (Grover's algorithm)

Let $\chi : \{0,1\}^n \longrightarrow$ *be a boolean function such that* $M_\chi = |\chi^{-1}(1)| = 1$*.*

Let $\mathcal{A} = H^{\otimes n}$ *which has a success probability of* $\frac{1}{2^n}$ *relative to* χ*.*

Then there exists a quantum algorithm $\mathcal{B}$ *that succeeds with probability* $\geq 1 - \frac{1}{2^n}$ *and which costs*

$$E_{\mathcal{B}} \approx 2kE_{H^{\otimes n}} + kE_{\mathcal{O}_\chi}$$

where

$$k \approx \frac{\pi}{4} \cdot \frac{1}{\frac{1}{2^{n/2}}} = \frac{\pi}{4} \cdot 2^{n/2}$$

- Set $\mathcal{A} = H^{\otimes n}$ then we have Grover's algorithm.

Quantum oracles I

$\chi : \{0,1\}^n \longrightarrow \{0,1\}$

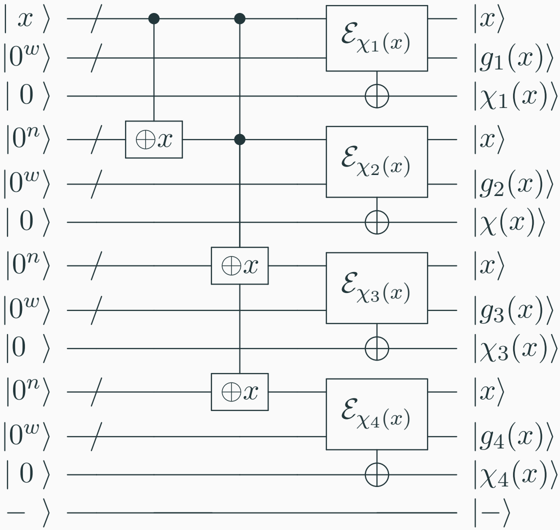
$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x)$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

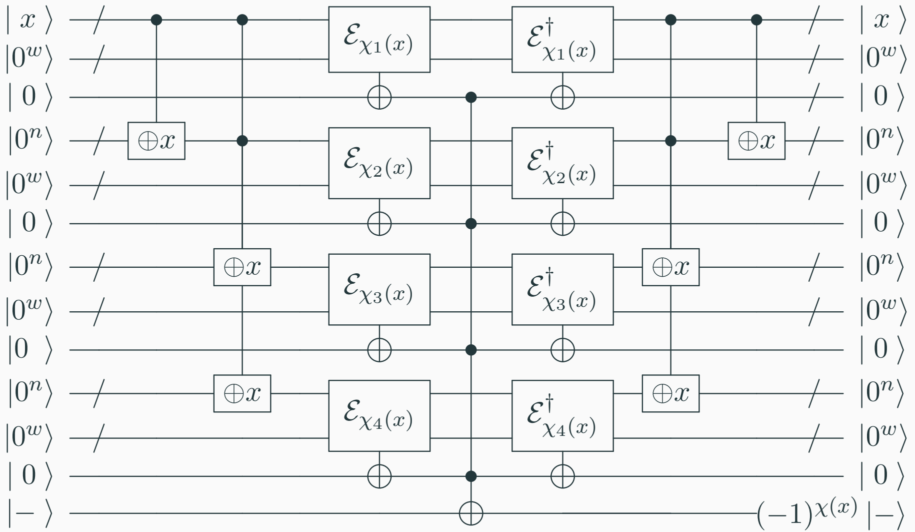
How can we implement this oracle using quantum evaluations of χ_i?

- Parallel evaluation : low depth but large number of qubits
- Serial evaluation : low number of qubits/high circuit-size

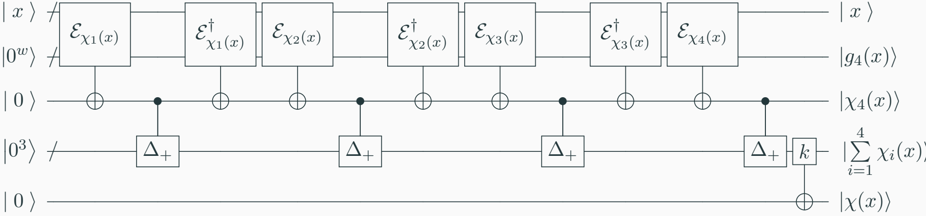
Quantum oracles II



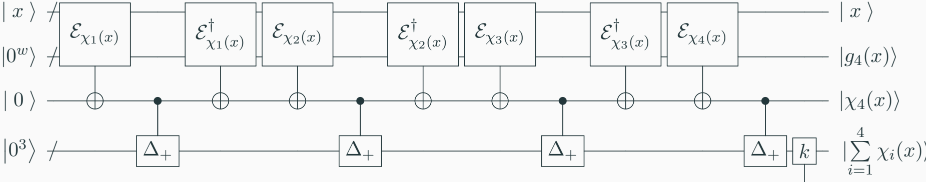
Quantum oracles III

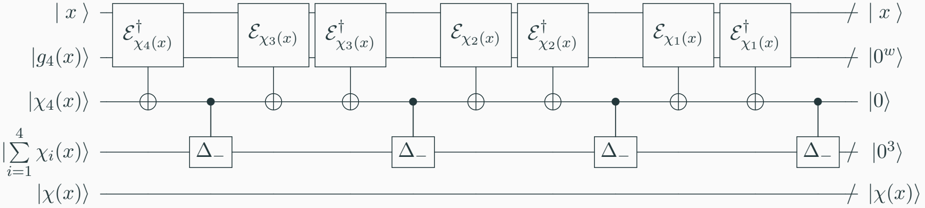


Quantum oracles IV



Quantum oracles IV





Quantum oracles V

$\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x)$$

where $\chi_1, \ldots, \chi_k : \{0,1\}^n \longrightarrow \{0,1\}$

1. n : #qubits required to represent the search space
2. w : #qubits required to implement a single $\mathcal{E}_{\chi_i}$

Parallel evaluation oracle	Counter-based oracle
Size : $\approx 2k$ evaluations	Size : $\approx 4k-2$ evaluations
Depth : ≈ 2 evaluations	Depth : $\approx 4k-2$ evaluations
Qubits: $\approx k(n+w+1)+1$	Qubits: $\approx n+w+\lfloor \log_2(k+1) \rfloor + 2$

The Search with Two Oracles problem I

Definition (The *Search with Two Oracles* problem)

Let $f_S, f_* : \{0,1\}^n \longrightarrow \{0,1\}$ be two boolean functions such that

$$f_*^{-1}(1) \subseteq f_S^{-1}(1)$$

that respectively define the quantum phase oracles $\mathcal{O}_{f_s}$ and $\mathcal{O}_{f_s}$.

The Search with Two Oracles problem I

Definition (The *Search with Two Oracles* problem)

Let $f_S, f_* : \{0,1\}^n \longrightarrow \{0,1\}$ be two boolean functions such that

$$f_*^{-1}(1) \subseteq f_S^{-1}(1)$$

that respectively define the quantum phase oracles $\mathcal{O}_{f_s}$ and $\mathcal{O}_{f_s}$.

We have the promise that $S = |f_s^{-1}(1)|$ and $|f_*^{-1}(1)| \in \{0,1\}$.

The Search with Two Oracles problem I

Definition (The *Search with Two Oracles* problem)

Let $f_S, f_* : \{0,1\}^n \longrightarrow \{0,1\}$ be two boolean functions such that

$$f_*^{-1}(1) \subseteq f_S^{-1}(1)$$

that respectively define the quantum phase oracles $\mathcal{O}_{f_s}$ and $\mathcal{O}_{f_s}$.

We have the promise that $S = |f_s^{-1}(1)|$ and $|f_*^{-1}(1)| \in \{0,1\}$.

Given $\mathcal{O}_{f_S}$ and $\mathcal{O}_{f_*}$, the *Search with Two Oracles* problem is to find an $x \in \{0,1\}^n$ such that $f_*(x) = 1$ or prove that no such element exists.

The Search with Two Oracles problem I

Definition (The *Search with Two Oracles* problem)

Let $f_S, f_* : \{0,1\}^n \longrightarrow \{0,1\}$ be two boolean functions such that

$$f_*^{-1}(1) \subseteq f_S^{-1}(1)$$

that respectively define the quantum phase oracles $\mathcal{O}_{f_s}$ and $\mathcal{O}_{f_s}$.

We have the promise that $S = |f_s^{-1}(1)|$ and $|f_*^{-1}(1)| \in \{0,1\}$.

Given $\mathcal{O}_{f_S}$ and $\mathcal{O}_{f_*}$, the *Search with Two Oracles* problem is to find an $x \in \{0,1\}^n$ such that $f_*(x) = 1$ or prove that no such element exists.

Can we do better than Grover's algorithm if $E_{f_S} < E_{f_*}$?.

The Search with Two Oracles problem II

Solution by Kimmel et al. lies in a variant of amplitude amplification.

Theorem (Exact amplitude amplification)

Let $\mathcal{A}$ be any measurement-free quantum algorithm with a **known** *success probability $a > 0$ relative to $\chi : \{0,1\}^n \longrightarrow \{0,1\}$.*

Then we can construct a quantum algorithm $\mathcal{B}$ that succeeds with probability 1 relative to the boolean function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$.

The quantum algorithm $\mathcal{B}$ requires $2k+1$ applications of $\mathcal{A}$ and k applications of $\mathcal{O}_\chi$, where $k = \left\lceil \frac{\pi}{4 \arcsin \sqrt{a}} \right\rceil$.

The Search with Two Oracles problem II

Solution by Kimmel et al. lies in a variant of amplitude amplification.

Theorem (Exact amplitude amplification)

Let $\mathcal{A}$ be any measurement-free quantum algorithm with a **known** *success probability $a > 0$ relative to $\chi : \{0,1\}^n \longrightarrow \{0,1\}$.*

Then we can construct a quantum algorithm $\mathcal{B}$ that succeeds with probability 1 relative to the boolean function $\chi : \{0,1\}^n \longrightarrow \{0,1\}$.

The quantum algorithm $\mathcal{B}$ requires $2k+1$ applications of $\mathcal{A}$ and k applications of $\mathcal{O}_\chi$, where $k = \left\lceil \frac{\pi}{4 \arcsin \sqrt{a}} \right\rceil$.

- #Calls to $\mathcal{A}$ and $\mathcal{O}_\chi$ approximately that of amplitude amplification.
- Our modification will only use amplitude amplification.

The Search with Two Oracles problem

Define $\mathcal{A} = H^{\otimes n}$ so that

$$\mathcal{A}\left|0\right\rangle = H^{\otimes n}\left|0\right\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} \left|x\right\rangle$$

Then relative to $\mathcal{O}_{f_S}$ this has a success probability of $\frac{|S|}{2^n} = |S| \cdot |\frac{1}{2^{n/2}}|^2$.

The Search with Two Oracles problem

Define $\mathcal{A} = H^{\otimes n}$ so that

$$\mathcal{A}\left|0\right\rangle = H^{\otimes n}\left|0\right\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} \left|x\right\rangle$$

Then relative to $\mathcal{O}_{f_S}$ this has a success probability of $\frac{|S|}{2^n} = |S| \cdot |\frac{1}{2^{n/2}}|^2$.

Use EAA with $\mathcal{A}$ and $\mathcal{O}_{f_S}$ to construct a quantum algorithm $\mathcal{B}$ so that

$$\mathcal{B}\left|0\right\rangle = \frac{1}{|S|^{1/2}} \sum_{x \in f_S^{-1}(1)} \left|x\right\rangle$$

The Search with Two Oracles problem

Define $\mathcal{A} = H^{\otimes n}$ so that

$$\mathcal{A}\,|0\rangle = H^{\otimes n}\,|0\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Then relative to $\mathcal{O}_{f_S}$ this has a success probability of $\frac{|S|}{2^n} = |S| \cdot |\frac{1}{2^{n/2}}|^2$.

Use EAA with $\mathcal{A}$ and $\mathcal{O}_{f_S}$ to construct a quantum algorithm $\mathcal{B}$ so that

$$\mathcal{B}\,|0\rangle = \frac{1}{|S|^{1/2}} \sum_{x \in f_S^{-1}(1)} |x\rangle$$

$\mathcal{B}$ has a success probability of 1 relative to f_S.

The Search with Two Oracles problem

Define $\mathcal{A} = H^{\otimes n}$ so that

$$\mathcal{A} |0\rangle = H^{\otimes n} |0\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Then relative to $\mathcal{O}_{f_S}$ this has a success probability of $\frac{|S|}{2^n} = |S| \cdot |\frac{1}{2^{n/2}}|^2$.

Use EAA with $\mathcal{A}$ and $\mathcal{O}_{f_S}$ to construct a quantum algorithm $\mathcal{B}$ so that

$$\mathcal{B} |0\rangle = \frac{1}{|S|^{1/2}} \sum_{x \in f_S^{-1}(1)} |x\rangle$$

$\mathcal{B}$ has a success probability of 1 relative to f_S.
$\mathcal{B}$ has a success probability of $\frac{1}{|S|}$ relative to f_* as $f_*^{-1}(1) \subseteq f_S^{-1}(1)$.

The Search with Two Oracles problem

Define $\mathcal{A} = H^{\otimes n}$ so that

$$\mathcal{A}\left|0\right\rangle = H^{\otimes n}\left|0\right\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} \left|x\right\rangle$$

Then relative to $\mathcal{O}_{f_S}$ this has a success probability of $\frac{|S|}{2^n} = |S| \cdot |\frac{1}{2^{n/2}}|^2$.

Use EAA with $\mathcal{A}$ and $\mathcal{O}_{f_S}$ to construct a quantum algorithm $\mathcal{B}$ so that

$$\mathcal{B}\left|0\right\rangle = \frac{1}{|S|^{1/2}} \sum_{x \in f_S^{-1}(1)} \left|x\right\rangle$$

$\mathcal{B}$ has a success probability of 1 relative to f_S.
$\mathcal{B}$ has a success probability of $\frac{1}{|S|}$ relative to f_* as $f_*^{-1}(1) \subseteq f_S^{-1}(1)$.

Use EAA with $\mathcal{B}$ and $\mathcal{O}_{f_*}$ to construct a quantum algorithm $\mathcal{C}$.
$\mathcal{C}$ has a success probability of 1 relative to f_*.

The Search with Two Oracles problem

What is the cost?

1. $\mathcal{A} = H^{\otimes n}$ is simply n Hadamard gates.
2. $\mathcal{B}$ costs $\approx 2\sqrt{\frac{2^n}{M_S}}$ applications of $\mathcal{A}$ and $\sqrt{\frac{2^n}{M_S}}$ applications of $\mathcal{O}_{f_S}$.
3. $\mathcal{C}$ costs $\approx 2\sqrt{M_S}$ applications of $\mathcal{B}$ and $\sqrt{M_S}$ applications of $\mathcal{O}_{f_*}$.

Approximate cost of $\mathcal{C}$ (*STO*)

Applications of $\mathcal{O}_{f_*}$: $\frac{\pi}{4}\sqrt{M_S}$
Applications of $\mathcal{O}_{f_S}$: $\frac{\pi^2}{8}\sqrt{2^n}$
Applications of $\mathcal{A} = H^{\otimes n}$: $\frac{\pi^2}{4}\sqrt{2^n}$

$$O(2 \cdot \sqrt{2^n} E_{\mathcal{O}_{f_S}} + \sqrt{M_S} E_{\mathcal{O}_{f_*}})$$

Approximate cost of Grover's algorithm

$$O(\sqrt{2^n} \cdot E_{\mathcal{O}_{f_*}})$$

The Search with Two Oracles problem

$\chi : \{0,1\}^n \longrightarrow \{0,1\}$

$$\chi(x) \mapsto \chi_1(x) \wedge \cdots \wedge \chi_k(x)$$

where $\chi_i : \{0,1\}^n \longrightarrow \{0,1\}$.

STO: choose $i_1, \ldots, i_r \subseteq \{1, \ldots, k\}$

- $f_S(x) \mapsto \chi_{i_1}(x) \wedge \cdots \wedge \chi_{i_r}(x)$
- $f_*(x) \mapsto \ \chi_1(x) \wedge \cdots \wedge \chi_k(x)$

- AES : choose a subset of the plaintext-ciphertext pairs
- $\mathcal{MQ}$: choose a subset of the equations

The Search with Two Oracles problem

What if we only know $M_* = 1$ and have to guess $M_S = M'_S$?

The Search with Two Oracles problem

What if we only know $M_* = 1$ and have to guess $M_S = M'_S$?

$$c = \sin^2\left(\left(2\hat{k}_2 + 1\right) \cdot \arcsin\sqrt{z \cdot \frac{M'_S}{M_S} \cdot \sin^2\left(\frac{\pi}{4\hat{k}_2 + 2}\right)}\right) \cdot \left(\frac{b_g - b \cdot b_g}{b_g - b \cdot \hat{b}_g}\right) + \frac{b \cdot b_g - b \cdot \hat{b}_g}{b_g - b \cdot \hat{b}_g}$$

where $b_g = \frac{1}{M'_S}$, $\hat{k}_2 = \left\lceil \frac{\pi}{4\arcsin\sqrt{b_g}} \right\rceil$, $\hat{b}_g = \sin^2\left(\frac{\pi}{4\hat{k}_2+2}\right)$, $b = \frac{z}{M_S}$ and where

$$z = \sin^2\left(\left(2\hat{k}_1 + 1\right) \cdot \arcsin\sqrt{\frac{M_S}{M'_S} \cdot \sin^2\left(\frac{\pi}{4\hat{k}_1 + 2}\right)}\right) \cdot \left(\frac{a_g - a \cdot a_g}{a_g - a \cdot \hat{a}_g}\right) + \frac{a \cdot a_g - a \cdot \hat{a}_g}{a_g - a \cdot \hat{a}_g}$$

where $a_g = \frac{M'_S}{2^n}$, $\hat{k}_1 = \left\lceil \frac{\pi}{4\arcsin\sqrt{a_g}} \right\rceil$, $\hat{a}_g = \sin^2\left(\frac{\pi}{4\hat{k}_1+2}\right)$ and $a = \frac{M_S}{2^n}$.

The Search with Two Oracles problem

What if we only know $M_* = 1$ and have to guess $M_S = M'_S$?

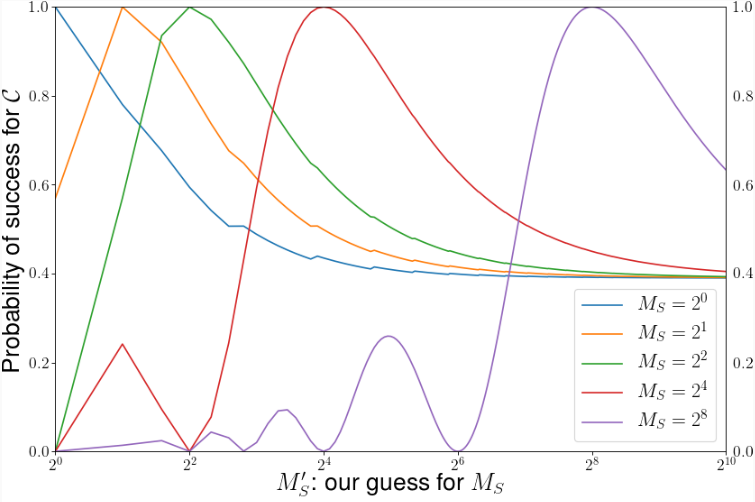


Figure 1: Search space size: 2^{10} elements

The Search with Two Oracles problem

Research question: can we restore correctness in the worst-case?

$$c = \sin^2\left(\left(2\hat{k}_2+1\right)\cdot \arcsin\sqrt{z\cdot\frac{M_S'}{M_S}\cdot\sin^2\left(\frac{\pi}{4\hat{k}_2+2}\right)}\right)\cdot\left(\frac{b_g-b\cdot b_g}{b_g-b\cdot\hat{b}_g}\right)+\frac{b\cdot b_g-b\cdot\hat{b}_g}{b_g-b\cdot\hat{b}_g}$$

where $b_g = \frac{1}{M_S'}$, $\hat{k}_2 = \left\lceil\frac{\pi}{4\arcsin\sqrt{b_g}}\right\rceil$, $\hat{b}_g = \sin^2\left(\frac{\pi}{4\hat{k}_2+2}\right)$, $b = \frac{z}{M_S}$ and where

$$z = \sin^2\left(\left(2\hat{k}_1+1\right)\cdot \arcsin\sqrt{\frac{M_S}{M_S'}\cdot\sin^2\left(\frac{\pi}{4\hat{k}_1+2}\right)}\right)\cdot\left(\frac{a_g-a\cdot a_g}{a_g-a\cdot\hat{a}_g}\right)+\frac{a\cdot a_g-a\cdot\hat{a}_g}{a_g-a\cdot\hat{a}_g}$$

where $a_g = \frac{M_S'}{2^n}$,$\hat{k}_1 = \left\lceil\frac{\pi}{4\arcsin\sqrt{a_g}}\right\rceil$, $\hat{a}_g = \sin^2\left(\frac{\pi}{4\hat{k}_1+2}\right)$ and $a = \frac{M_S}{2^n}$.

The Search with Two Oracles problem

Research question: can we restore correctness in the worst-case?

$$c = \sin^2\left(\left(2\left\lfloor\frac{\pi}{4\arcsin\sqrt{\frac{1}{M'_S}}}\right\rfloor+1\right)\cdot\arcsin\sqrt{\frac{b}{M_S}}\right)$$

where

$$b = \sin^2\left(\left(2\left\lfloor\frac{\pi}{4\arcsin\sqrt{\frac{M'_S}{2^n}}}\right\rfloor+1\right)\cdot\arcsin\sqrt{\frac{M_S}{2^n}}\right)$$

The Search with Two Oracles problem

Research question: can we restore correctness in the worst-case?

$$c \approx \sin^2\left(\left(\frac{\pi}{2}\cdot\sqrt{\frac{M_S'}{M_S}}+\sqrt{\frac{1}{M_S}}\right)\cdot\sqrt{b}\right)$$

where

$$b \approx \sin^2\left(\frac{\pi}{2}\cdot\sqrt{\frac{M_S}{M_S'}}+\sqrt{\frac{M_S}{N}}\right)$$

The Search with Two Oracles problem

Research question: can we restore correctness in the worst-case?

$$c \approx \sin^2\left(\left(\frac{\pi}{2} \cdot \sqrt{\frac{M'_S}{M_S}} + \sqrt{\frac{1}{M_S}}\right) \cdot \sqrt{b}\right)$$

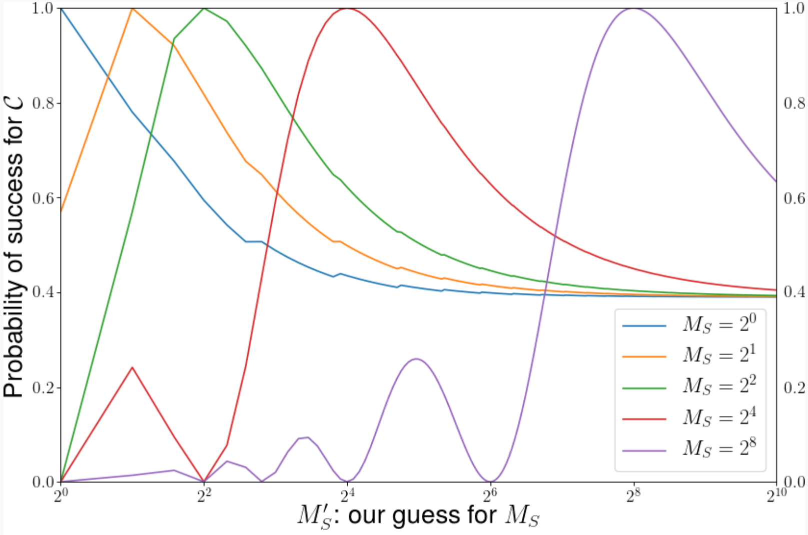
where

$$b \approx \sin^2\left(\frac{\pi}{2} \cdot \sqrt{\frac{M_S}{M'_S}} + \sqrt{\frac{M_S}{N}}\right)$$

Observations:

1. Error is down to the *ratio* $M_S : M'_S$.
2. $M'_S < M_S$: the errors are compounded
3. $M'_S > M_S$: some of the errors compensate $c \to \sin^2\left(\left(\frac{\pi}{2}\right)^2\right) \approx 0.39$

The Search with Two Oracles problem



Search space: 2^{10} elements

The Search with Two Oracles problem

- If χ_i are pseudorandom then good enough in the average-case.
- Better to overestimate than underestimate.
- *STO* can fail in worst-case analysis or be non-optimal.
- Two errors are introduced by the ratio $M_S : M_S'$

The Search with Two Oracles problem

- If χ_i are pseudorandom then good enough in the average-case.
- Better to overestimate than underestimate.
- *STO* can fail in worst-case analysis or be non-optimal.
- Two errors are introduced by the ratio $M_S : M'_S$

Solution: artificially control the ratio $M_S : M'_S$

A modification to the *STO* method

Define $f_{S \cup Z_t} : \{0,1\} \longrightarrow \{0,1\}$ by

$$f_{S \cup Z_t}(x) \mapsto \begin{cases} 1 & \text{if } f_S(x) = 1 \text{ or } x \in 1^{n-t} \times \{0,1\}^t \\ 0 & \text{otherwise.} \end{cases}$$

A modification to the *STO* method

Define $f_{S\cup Z_t} : \{0,1\} \longrightarrow \{0,1\}$ by

$$f_{S\cup Z_t}(x) \mapsto \begin{cases} 1 & \text{if } f_S(x) = 1 \text{ or } x \in 1^{n-t} \times \{0,1\}^t \\ 0 & \text{otherwise.} \end{cases}$$

1. Cheap modification: $O(n-t)$ quantum gates
2. Guarantees that $M_{S\cup Z_t} \geq 2^t$
3. New ratio:

   $$M_{S\cup Z_t} : M'_{S\cup Z_t} \approx M_S + 2^t : M'_S + 2^t$$

   approaches 1 as $t \to n$.
4. New cost:

   $$O(2 \cdot \sqrt{2^n} E_{\mathcal{O}_{f_{S\cup Z_t}}} + \sqrt{M_{S\cup Z_t}} E_{\mathcal{O}_{f_*}})$$

New quantum resource estimations I

λ	$n=m$	[SW16]	[SW16] (counter)	[Pri18]
80	117	$2^{80.9}/237/1$	$2^{81.9}/127/1$	$2^{78.6}/230/1$
128	209	$2^{129.4}/421/1$	$2^{130.4}/220/1$	$2^{126.3}/415/1$
256	457	$2^{256.7}/915/1$	$2^{257.7}/468/1$	$2^{252.9}/905/1$
λ	$n=m$	Our method	Our method (counter)	Our method (hybrid)
80	117	$2^{79.7}/237/0.9999$	$2^{80.8}/127/0.9999$	$2^{79.9}/153/0.9999$
128	209	$2^{127.5}/421/0.9999$	$2^{128.5}/220/0.9999$	$2^{127.6}/246/0.9999$
256	457	$2^{253.8}/915/0.9999$	$2^{254.8}/468/0.9999$	$2^{253.9}/497/0.9999$

Table 3: Quantum circuit-size/qubits/minimal probability of success for quantum search applied to cryptanalysis of Gui [PCY$^+$15, PCDY17].

New quantum resource estimations II

AES-k	[GLRS16] ($r = 2/3$)	Our method ($r = 10$)	Our method (counter) ($r = 10$)
128	$2^{86.87}/1969/1$	$2^{86.53}/1969/1$	$2^{86.53}/988/1$
192	$2^{119.23}/2225/1$	$2^{118.89}/2225/1$	$2^{118.89}/1115/1$
256	$2^{151.96}/4009/1$	$2^{151.03}/4009/1$	$2^{151.03}/1340/1$

Table 4: Comparison of quantum resource estimates for Grover vs the modified *STO* algorithm applied to cryptanalysis of single-target AES

Conclusions

- Interesting quantum optimisations out there
- Quantum search may be more practical than previously thought
- Be careful when choosing parameters

Thanks! Questions?

- Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt, Applying Grover's algorithm to AES: quantum resource estimates, International Workshop on Post-Quantum Cryptography, Springer, 2016, pp. 29–43.
- Lov K Grover, Quantum computers can search rapidly by using almost any transformation, Physical Review Letters **80** (1998), no. 19, 4329.
- Albrecht Petzoldt, Ming-Shing Chen, Jintai Ding, and Bo-Yin Yang, HMFEV- an efficient multivariate signature scheme, International workshop on post-quantum cryptography, Springer, 2017, pp. 205–223.

- Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding, Design principles for HFEv-based multivariate signature schemes, Int. Conference on the Theory and Application of Cryptology and Information Security, Springer, 2015, pp. 311–334.
- Benjamin Pring, Exploiting preprocessing for quantum search to break parameters for mq cryptosystems, Arithmetic of Finite Fields-7th International Workshop, WAIFI 2018, Revised Selected Papers., WAIFI, 2018.
- Peter Schwabe and Bas Westerbaan, Solving binary $\mathcal{MQ}$ with Grover's algorithm, SPACE 2016, Springer, 2016, pp. 303–322.