Improvements to quantum search techniques for block-ciphers, with applications to AES

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

21st October 2020

[1]University of Bath, UK
[2]University of South Florida, USA

Overview of results

Q: Do we really need so many qubits to attack AES via quantum search?

A: No.

	Quantum Gates	Depth	Qubits
AES-128	$2^{83.42} \to 2^{82.25}$	$2^{75.11} \to 2^{75.05}$	$3329 \to 1667$
AES-192	$2^{115.58} \to 2^{114.44}$	$2^{107.19} \to 2^{107.08}$	$3969 \to 1987$
AES-256	$2^{148.47} \to 2^{146.77}$	$2^{139.36} \to 2^{139.38}$	$6913 \to 2307$

Table 1: Resources to attack AES, using Grover [JNRV20] and our modification.

Takeaway: cryptanalysis of block-ciphers requires fewer qubits/gates.

The key recovery problem for block-ciphers I

$\mathsf{Enc} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$ and $\mathsf{Dec} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$

such that for all $K \in \{0,1\}^k$ and $P \in \{0,1\}^n$ we have

$$\mathsf{Dec}\Big(K, \mathsf{Enc}\big(K, P\big)\Big) = P$$

Expected properties:

1. Fixing $K \in \{0,1\}^k$ gives us $\mathsf{Enc} : \{K\} \times \{0,1\}^n \longrightarrow \{0,1\}^n$ which behaves as a pseudorandom permutation.
2. Fixing $P \in \{0,1\}^n$ gives us $\mathsf{Enc} : \{0,1\}^k \times \{P\} \longrightarrow \{0,1\}^n$ which behaves as a pseudorandom function.

The key recovery problem for block-ciphers II

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

For our purposes — AES-k where $k \in \{128, 192, 256\}$

$$\mathsf{AES} : \{0,1\}^k \times \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$$

- Should take $\geq 2^k$ classical gates to break AES-k.
- Quantum search in **noise-free model** currently the leading technique.
- NIST security levels based on **concrete** cost of breaking AES-k.
- Interesting case-study in optimising quantum circuits.

The key-recovery cryptanalysis scenario

Cryptanalyst, you are given

1. $r \geq 1$ known plaintext-ciphertexts for an unknown $K_* \in \{0,1\}^k$

$$\Big\{(P_1, C_1), \ldots, (P_r, C_r) \;:\; \mathsf{Enc}(K_*, P_i) = C_i \;\text{ for }\; i = 1, \ldots, r\Big\}$$

2. The classical circuits for $\mathsf{Enc}, \mathsf{Dec} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$

Your mission[1]: recover the unknown $K_* \in \{0,1\}^k$.

[1] You choose to accept it

The key-recovery cryptanalysis scenario

Cryptanalyst, you are given

1. $r \geq 1$ known plaintext-ciphertexts for an unknown $K_* \in \{0,1\}^k$

$$\Big\{(P_1, C_1), \ldots, (P_r, C_r) \ : \ \mathsf{Enc}\big(K_*, P_i\big) = C_i \ \text{ for } \ i = 1, \ldots, r\Big\}$$

2. The classical circuits for Enc, Dec : $\{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$

Your mission[1]: recover the unknown $K_* \in \{0,1\}^k$.

Generic black-box method: brute-force search via $\chi : \{0,1\}^k \longrightarrow \{0,1\}$

$$\chi(K) \mapsto \Big(\mathsf{Enc}(K, P_1) \stackrel{?}{=} C_1\Big) \wedge \cdots \wedge \Big(\mathsf{Enc}(K, P_r) \stackrel{?}{=} C_r\Big)$$

[1] You choose to accept it

Known plaintext-unicity distance

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

$$\chi(K) \mapsto \left(\mathsf{Enc}(K, P_1) \stackrel{?}{=} C_1\right) \wedge \cdots \wedge \left(\mathsf{Enc}(K, P_r) \stackrel{?}{=} C_r\right)$$

How large does r have to be?

- 1 key K_* guaranteed by the scenario.
- $2^k - 1$ other keys.
- $K \neq K_*$ has probability $1/2$ that Enc(K, P_i) matches C_i on any bit.

$$\mathbb{E}\left[\#\text{matching keys}\right] = 1 + \left(2^k - 1\right) \cdot 2^{-rn} \approx 1 + 2^{k-rn}$$

AES-128/r=1: $1 + 2^{128-1\cdot 128} = 2$
AES-128/r=2: $1 + 2^{128-2\cdot 128} = 1 + 2^{-128}$

AES-128: r=2
AES-192: r=2
AES-256: r=3

Classical brute-force attacks

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

$\chi(K) \mapsto \chi_1(K) \wedge \cdots \wedge \chi_r(K)$ $\qquad$ $\chi_i(K) \mapsto \Big(\mathsf{Enc}(K, P_i) \stackrel{?}{=} C_i\Big)$

Naive brute-force search:

Evaluate $\chi(K)$

For $K \in \{0,1\}^k$:
    if $\chi(K) = 1$ **return** K

Cost: $O\big(2^k \cdot \chi\big)$

Brute-force search with filtering:

Evaluate $\chi(K)$ iff $\chi_1(K) = 1$

For $K \in \{0,1\}^k$:
    if $\chi_1(K) = 0$:
        continue
    else :
        if $\chi(K) = 1$ **return** K

Cost: $O\big(2^k \cdot \chi_1 + 2^{k-n} \cdot \chi\big)$

Quantum computation

- Quantum states consisting of k-qubits

$$|\psi\rangle = \sum_{x\in\{0,1\}^k} \alpha_x |x\rangle \qquad \text{where} \quad \alpha_x \in \mathbb{C} \quad \text{and} \quad \sum_{x\in\{0,1\}^k} |\alpha_x|^2 = 1$$

- Measurement of $|\psi\rangle$ collapses to $x \in \{0,1\}^k$ with probability $|\alpha_x|^2$.
- Quantum algorithms

$$U \in \mathbb{C}^{2^k\times 2^k} \qquad \text{where} \quad UU^\dagger = U^\dagger U = I$$

can be built out of quantum gates acting on one or two qubits.

- *Ancilla* qubits can decrease the cost of implementation

$$U \in \mathbb{C}^{2^{k+w}\times 2^{k+w}} \qquad\qquad V \in \mathbb{C}^{2^k\times 2^k}$$

$$U|\psi\rangle\,|0^w\rangle \mapsto |\psi'\rangle\,|0^w\rangle \qquad\qquad V|\psi\rangle \mapsto |\psi'\rangle$$

Cost models

Metrics [JS19]:

- #Quantum gates (number of operations)
- #Quantum circuit-depth (time)
- #Qubits (hardware)

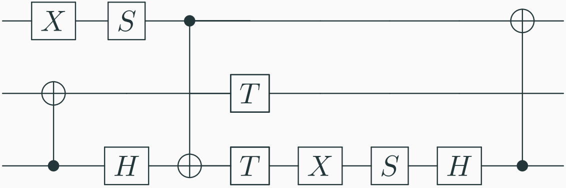
- G-cost # Quantum gates
- DW-cost Quantum circuit-Depth $\times$ circuit Width (# qubits)

Cost models

Metrics [JS19]:

- #Quantum gates (number of operations)
- #Quantum circuit-depth (time)
- #Qubits (hardware)

- G-cost # Quantum gates
- DW-cost Quantum circuit-Depth $\times$ circuit Width (# qubits)



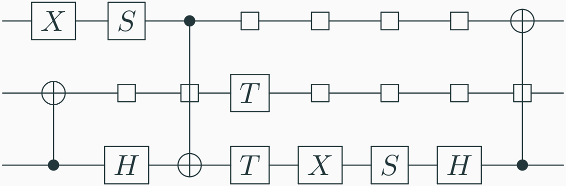
Qubits : 3
Depth : 8
G-Cost : 11

Cost models

Metrics [JS19]:

- #Quantum gates (number of operations)
- #Quantum circuit-depth (time)
- #Qubits (hardware)

- G-cost # Quantum gates
- DW-cost Quantum circuit-Depth $\times$ circuit Width (# qubits)



Qubits : 3
Depth : 8
G-Cost : 11
DW-Cost : 24 (8×3)

Quantum oracles

Classical circuit

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

Quantum oracle for $\chi : \{0,1\}^k \longrightarrow \{0,1\}$ acts for $x \in \{0,1\}^k$

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

Actually looks more like:

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

Quantum amplitude amplification and Grover's algorithm

Theorem (Quantum amplitude amplification [BHMT02])

- *Let $\mathcal{A}$ be a quantum algorithm with adjoint $\mathcal{A}^\dagger$, acting on k qubits.*
- *Let $\mathcal{O}_\chi$ be such that $\mathcal{O}_\chi \left|x\right\rangle \mapsto (-1)^{\chi(x)} \left|x\right\rangle$ where $\chi : \{0,1\}^k \longrightarrow \{0,1\}$.*
- *Measuring $\mathcal{A} \left|0^k\right\rangle$ gives $x \in \{0,1\}^k$ where $\chi(x) = 1$ with probability a.*

For $t \in \mathbb{N}_0$, there is a quantum algorithm $\mathcal{B}(t)$ where measuring the state $\mathcal{B}(t) \left|0^k\right\rangle$ gives an $x \in \{0,1\}^k$ such that $\chi(x) = 1$ with probability

$$b(t) = \sin^2\left(\left(2t+1\right) \cdot \arcsin\sqrt{a}\right)$$

and which requires t applications of $\mathcal{A}, \mathcal{A}^\dagger$ and $\mathcal{O}_\chi$.

Quantum amplitude amplification and Grover's algorithm

Theorem (Quantum amplitude amplification [BHMT02])

- *Let $\mathcal{A}$ be a quantum algorithm with adjoint $\mathcal{A}^\dagger$, acting on k qubits.*
- *Let $\mathcal{O}_\chi$ be such that $\mathcal{O}_\chi |x\rangle \mapsto (-1)^{\chi(x)} |x\rangle$ where $\chi : \{0,1\}^k \longrightarrow \{0,1\}$.*
- *Measuring $\mathcal{A}\left|0^k\right\rangle$ gives $x \in \{0,1\}^k$ where $\chi(x) = 1$ with probability a.*

For $t \in \mathbb{N}_0$, there is a quantum algorithm $\mathcal{B}(t)$ where measuring the state $\mathcal{B}(t)\left|0^k\right\rangle$ gives an $x \in \{0,1\}^k$ such that $\chi(x) = 1$ with probability

$$b(t) = \sin^2\left(\left(2t+1\right) \cdot \arcsin\sqrt{a}\right)$$

and which requires t applications of $\mathcal{A}, \mathcal{A}^\dagger$ and $\mathcal{O}_\chi$.

Explicitly: $\mathcal{B}(t) = \left(\mathcal{A} R_0 \mathcal{A}^\dagger \mathcal{O}_\chi\right)^t \mathcal{A}\left|0^k\right\rangle$

Quantum amplitude amplification and Grover's algorithm

Theorem (Quantum amplitude amplification [BHMT02])

- *Let $\mathcal{A}$ be a quantum algorithm with adjoint $\mathcal{A}^\dagger$, acting on k qubits.*
- *Let $\mathcal{O}_\chi$ be such that $\mathcal{O}_\chi \left|x\right\rangle \mapsto (-1)^{\chi(x)} \left|x\right\rangle$ where $\chi : \{0,1\}^k \longrightarrow \{0,1\}$.*
- *Measuring $\mathcal{A}\left|0^k\right\rangle$ gives $x \in \{0,1\}^k$ where $\chi(x) = 1$ with probability a.*

For $t \in \mathbb{N}_0$, there is a quantum algorithm $\mathcal{B}(t)$ where measuring the state $\mathcal{B}(t)\left|0^k\right\rangle$ gives an $x \in \{0,1\}^k$ such that $\chi(x) = 1$ with probability

$$b(t) = \sin^2\Big(\big(2t+1\big) \cdot \arcsin\sqrt{a}\Big)$$

and which requires t applications of $\mathcal{A}, \mathcal{A}^\dagger$ and $\mathcal{O}_\chi$.

Repeatedly prepare $\mathcal{A}\left|0^k\right\rangle \quad \implies \quad O\Big(\frac{1}{a} \cdot (\mathcal{A} + \chi)\Big)$.

Prepare $\mathcal{B}(t)$ with $t \approx \frac{\pi}{4} \cdot \sqrt{\frac{1}{a}} \implies O\Big(\sqrt{\frac{1}{a}} \cdot \big(\mathcal{A} + \mathcal{A}^\dagger + \mathcal{O}_\chi\big)\Big)$ and $b(t) \approx 1$.

Quantum amplitude amplification and Grover's algorithm

Theorem (Quantum amplitude amplification [BHMT02])

- *Let $\mathcal{A}$ be a quantum algorithm with adjoint $\mathcal{A}^\dagger$, acting on k qubits.*
- *Let $\mathcal{O}_\chi$ be such that $\mathcal{O}_\chi \left|x\right\rangle \mapsto (-1)^{\chi(x)} \left|x\right\rangle$ where $\chi : \{0,1\}^k \longrightarrow \{0,1\}$.*
- *Measuring $\mathcal{A}\left|0^k\right\rangle$ gives $x \in \{0,1\}^k$ where $\chi(x) = 1$ with probability a.*

For $t \in \mathbb{N}_0$, there is a quantum algorithm $\mathcal{B}(t)$ where measuring the state $\mathcal{B}(t)\left|0^k\right\rangle$ gives an $x \in \{0,1\}^k$ such that $\chi(x) = 1$ with probability

$$b(t) = \sin^2\left(\left(2t+1\right) \cdot \arcsin\sqrt{a}\right)$$

and which requires t applications of $\mathcal{A}, \mathcal{A}^\dagger$ and $\mathcal{O}_\chi$.

Grover's algorithm: set $\mathcal{A} = H^{\otimes k}$ where $H^{\otimes k}\left|0^k\right\rangle \mapsto \frac{1}{2^{k/2}} \sum_{x\in\{0,1\}^k} \left|x\right\rangle$.

$H^{\otimes k}$ has negligible cost compared to $\mathcal{O}_\chi \implies$ Grover cost $\approx \frac{\pi}{4} 2^{k/2} \cdot \mathcal{O}_\chi$

Classical brute-force attacks

Naive brute-force search:
Evaluate $\chi(K)$

For $K \in \{0,1\}^k$:
    if $\chi(K) = 1$ **return** K

Cost: $O\big(2^k \cdot S_\chi\big)$

Grover's cost: $O\big(2^{k/2} \cdot \mathcal{O}_\chi\big)$

Brute-force search with filtering:
Evaluate $\chi(K)$ iff $\chi_1(K) = 1$

For $K \in \{0,1\}^k$:
    if $\chi_1(K) = 0$:
        continue
    else :
        if $\chi(K) = 1$ **return** K

Cost: $O\big(2^k \cdot \chi_1 + 2^{k-n} \cdot \chi\big)$

STO: $O\big(2^{k/2} \cdot \mathcal{O}_{\chi_1} + 2^{\frac{k-n}{2}} \cdot \mathcal{O}_\chi\big)$

(Search with Two Oracles)

The Search with Two Oracles [KYYLHH15] methodology I

We have two circuits $\chi, \gamma : \{0,1\}^k \longrightarrow \{0,1\}$ where

1. There is a unique $x_* \in \{0,1\}^k$ such that $\chi(x_*) = 1$.
2. We have $\gamma(x_*) = 1$ and know $S = \big|\{x \in \{0,1\}^k : \gamma(x) = 1\}\big|$.

$$x_* \in \gamma^{-1}(1) \subseteq \{0,1\}^k$$

The Search with Two Oracles [KYYLHH15] methodology I

We have two circuits $\chi, \gamma : \{0,1\}^k \longrightarrow \{0,1\}$ where

1. There is a unique $x_* \in \{0,1\}^k$ such that $\chi(x_*) = 1$.
2. We have $\gamma(x_*) = 1$ and know $S = \left|\{x \in \{0,1\}^k : \gamma(x) = 1\}\right|$.

$$x_* \in \gamma^{-1}(1) \subseteq \{0,1\}^k$$

Search-space = $\{0,1\}^k$

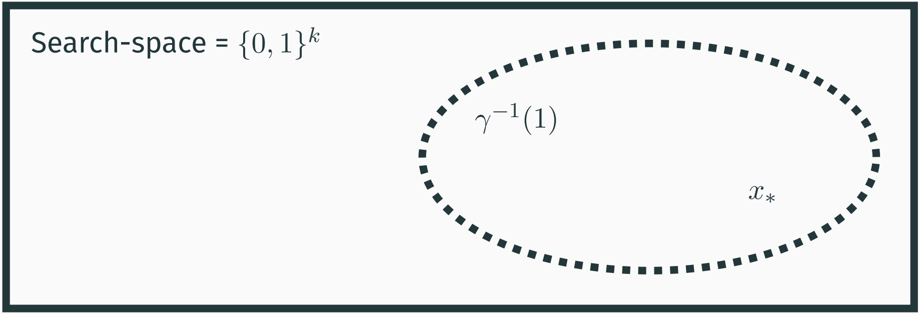
x_*

The Search with Two Oracles [KYYLHH15] methodology I

We have two circuits $\chi, \gamma : \{0,1\}^k \longrightarrow \{0,1\}$ where

1. There is a unique $x_* \in \{0,1\}^k$ such that $\chi(x_*) = 1$.
2. We have $\gamma(x_*) = 1$ and know $S = \left|\{x \in \{0,1\}^k : \gamma(x) = 1\}\right|$.

$$x_* \in \gamma^{-1}(1) \subseteq \{0,1\}^k$$



The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\,|0^k\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability*

$$b(t) \approx 1 \qquad \textit{if} \qquad t \approx \tfrac{\pi}{4} \cdot \tfrac{1}{\sqrt{a}}$$

1. **Define** $\mathcal{B}$ **with** $\mathcal{A} := H^{\otimes k}$**,** $\mathcal{O}_\gamma$ **and** $t \approx \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{S}}$**.**
2. Measure $\mathcal{B}\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ with prob 1

$$\Longrightarrow$$

Measure $\mathcal{B}\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{1}{S}$

3. Define $\mathcal{C}$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}$ and $\mathcal{O}_\chi$.
4. $\mathcal{C}$ requires $\approx \frac{\pi}{4} \cdot \sqrt{S}$ calls to $\mathcal{B}, \mathcal{B}^\dagger$ and $\mathcal{O}_\chi$.

$$\mathrm{Cost}(\mathcal{C}) \approx \frac{\pi}{4}\sqrt{S} \cdot \left(\mathcal{O}_\chi + 2\frac{\pi}{4}\sqrt{\frac{2^k}{S}} \cdot \mathcal{O}_\gamma\right) = \underbrace{\frac{\pi}{4}}_{\approx 0.79}\sqrt{S} \cdot \mathcal{O}_\chi + \underbrace{\frac{\pi^2}{8}}_{\approx 1.23} \cdot \sqrt{2^k} \cdot \mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\left|0^k\right\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability*

$$b(t) \approx 1 \qquad \textit{if} \qquad t \approx \tfrac{\pi}{4} \cdot \tfrac{1}{\sqrt{a}}$$

1. Define $\mathcal{B}$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \approx \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{S}}$.
2. **Measure** $\mathcal{B}\left|0^k\right\rangle$ **and obtain** $x \in \{0,1\}^k$ **where** $\gamma(x) = 1$ **with prob** 1

$$\Longrightarrow$$

Measure $\mathcal{B}\left|0^k\right\rangle$ **and obtain** $x \in \{0,1\}^k$ **where** $\chi(x) = 1$ **with prob** $\frac{1}{S}$

3. Define $\mathcal{C}$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}$ and $\mathcal{O}_\chi$.
4. $\mathcal{C}$ requires $\approx \frac{\pi}{4} \cdot \sqrt{S}$ calls to $\mathcal{B}, \mathcal{B}^\dagger$ and $\mathcal{O}_\chi$.

$$\text{Cost}(\mathcal{C}) \approx \frac{\pi}{4}\sqrt{S} \cdot \left(\mathcal{O}_\chi + 2\frac{\pi}{4}\sqrt{\frac{2^k}{S}} \cdot \mathcal{O}_\gamma\right) = \underbrace{\frac{\pi}{4}}_{\approx 0.79}\sqrt{S} \cdot \mathcal{O}_\chi + \underbrace{\frac{\pi^2}{8}}_{\approx 1.23} \cdot \sqrt{2^k} \cdot \mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\left|0^k\right\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability*

$$b(t) \approx 1 \qquad \textit{if} \qquad t \approx \tfrac{\pi}{4} \cdot \tfrac{1}{\sqrt{a}}$$

1. Define $\mathcal{B}$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \approx \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{S}}$.
2. Measure $\mathcal{B}\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ with prob 1

$$\Longrightarrow$$

Measure $\mathcal{B}\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{1}{S}$

3. **Define $\mathcal{C}$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}$ and $\mathcal{O}_\chi$.**
4. $\mathcal{C}$ requires $\approx \frac{\pi}{4} \cdot \sqrt{S}$ calls to $\mathcal{B}, \mathcal{B}^\dagger$ and $\mathcal{O}_\chi$.

$$\mathrm{Cost}(\mathcal{C}) \approx \frac{\pi}{4}\sqrt{S} \cdot \left(\mathcal{O}_\chi + 2\frac{\pi}{4}\sqrt{\frac{2^k}{S}} \cdot \mathcal{O}_\gamma\right) = \underbrace{\frac{\pi}{4}}_{\approx 0.79}\sqrt{S} \cdot \mathcal{O}_\chi + \underbrace{\frac{\pi^2}{8}}_{\approx 1.23} \cdot \sqrt{2^k} \cdot \mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ such that measuring $\mathcal{B}(t)\,|0^k\rangle$ gives $x \in \{0,1\}^k$ where $\chi(x) = 1$ with probability

$$b(t) \approx 1 \qquad \textit{if} \qquad t \approx \tfrac{\pi}{4} \cdot \tfrac{1}{\sqrt{a}}$$

1. Define $\mathcal{B}$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \approx \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{S}}$.
2. Measure $\mathcal{B}\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ with prob 1

$$\Longrightarrow$$

Measure $\mathcal{B}\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{1}{S}$

3. Define $\mathcal{C}$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}$ and $\mathcal{O}_\chi$.
4. **$\mathcal{C}$ requires $\approx \frac{\pi}{4} \cdot \sqrt{S}$ calls to $\mathcal{B}, \mathcal{B}^\dagger$ and $\mathcal{O}_\chi$.**

$$\mathrm{Cost}(\mathcal{C}) \approx \frac{\pi}{4}\sqrt{S} \cdot \left(\mathcal{O}_\chi + 2\frac{\pi}{4}\sqrt{\frac{2^k}{S}} \cdot \mathcal{O}_\gamma\right) = \underbrace{\frac{\pi}{4}}_{\approx 0.79}\sqrt{S} \cdot \mathcal{O}_\chi + \underbrace{\frac{\pi^2}{8}}_{\approx 1.23} \cdot \sqrt{2^k} \cdot \mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\left|0^k\right\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability* $b(t) = \sin^2\left((2t+1)\cdot\arcsin\sqrt{a}\right) \approx (2t+1)^2 \cdot a$ *for* $0 \le t \ll \frac{\pi}{4}\cdot\frac{1}{\sqrt{a}}$

1. Define $\mathcal{B}(t)$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \ll \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{S}}$.
2. Measure $\mathcal{B}(t)\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ w/prob $(2t+1)^2\cdot\frac{S}{2^k}$

$$\Longrightarrow$$

   Measure $\mathcal{B}(t)\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{(2t+1)^2}{2^k}$

3. Define $\mathcal{C}(t)$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}(t)$ and $\mathcal{O}_\chi$.
4. $\mathcal{C}(t)$ requires $\approx \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{(2t+1)^2}}$ calls to $\mathcal{B}(t), \mathcal{B}(t)^\dagger$ and $\mathcal{O}_\chi$.

$$\text{Cost}(\mathcal{C}(t)) \approx \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\left(\mathcal{O}_\chi + 2t\cdot\mathcal{O}_\gamma\right) = \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\mathcal{O}_\chi + \frac{\pi}{4}\cdot\frac{2t}{2t+1}\cdot\sqrt{2^k}\cdot\mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\left|0^k\right\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability* $b(t) = \sin^2\left((2t+1)\cdot\arcsin\sqrt{a}\right) \approx (2t+1)^2 \cdot a$ *for* $0 \le t \ll \frac{\pi}{4}\cdot\frac{1}{\sqrt{a}}$

1. **Define** $\mathcal{B}(t)$ **with** $\mathcal{A} := H^{\otimes k}$**,** $\mathcal{O}_\gamma$ **and** $t \ll \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{S}}$**.**
2. Measure $\mathcal{B}(t)\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ w/prob $(2t+1)^2\cdot\frac{S}{2^k}$

$$\Longrightarrow$$

Measure $\mathcal{B}(t)\left|0^k\right\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{(2t+1)^2}{2^k}$

3. Define $\mathcal{C}(t)$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}(t)$ and $\mathcal{O}_\chi$.
4. $\mathcal{C}(t)$ requires $\approx \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{(2t+1)^2}}$ calls to $\mathcal{B}(t), \mathcal{B}(t)^\dagger$ and $\mathcal{O}_\chi$.

$$\mathrm{Cost}(\mathcal{C}(t)) \approx \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\left(\mathcal{O}_\chi + 2t\cdot\mathcal{O}_\gamma\right) = \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\mathcal{O}_\chi + \frac{\pi}{4}\cdot\frac{2t}{2t+1}\cdot\sqrt{2^k}\cdot\mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\,|0^k\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability* $b(t) = \sin^2\left((2t+1)\cdot\arcsin\sqrt{a}\right) \approx (2t+1)^2 \cdot a$ *for* $0 \le t \ll \frac{\pi}{4}\cdot\frac{1}{\sqrt{a}}$

1. Define $\mathcal{B}(t)$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \ll \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{S}}$.
2. **Measure** $\mathcal{B}(t)\,|0^k\rangle$ **and obtain** $x \in \{0,1\}^k$ **where** $\gamma(x) = 1$ **w/prob** $(2t+1)^2\cdot\frac{S}{2^k}$

$$\Longrightarrow$$

Measure $\mathcal{B}(t)\,|0^k\rangle$ **and obtain** $x \in \{0,1\}^k$ **where** $\chi(x) = 1$ **with prob** $\frac{(2t+1)^2}{2^k}$

3. Define $\mathcal{C}(t)$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}(t)$ and $\mathcal{O}_\chi$.
4. $\mathcal{C}(t)$ requires $\approx \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{(2t+1)^2}}$ calls to $\mathcal{B}(t), \mathcal{B}(t)^\dagger$ and $\mathcal{O}_\chi$.

$$\text{Cost}(\mathcal{C}(t)) \approx \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\left(\mathcal{O}_\chi + 2t\cdot\mathcal{O}_\gamma\right) = \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\mathcal{O}_\chi + \frac{\pi}{4}\cdot\frac{2t}{2t+1}\cdot\sqrt{2^k}\cdot\mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A} R_0 \mathcal{A}^\dagger \mathcal{O}_\chi\right)^t \mathcal{A}$ *such that measuring* $\mathcal{B}(t)\,|0^k\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability* $b(t) = \sin^2\left((2t+1)\cdot \arcsin\sqrt{a}\right) \approx (2t+1)^2 \cdot a$ *for* $0 \leq t \ll \frac{\pi}{4} \cdot \frac{1}{\sqrt{a}}$

1. Define $\mathcal{B}(t)$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \ll \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{S}}$.
2. Measure $\mathcal{B}(t)\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ w/prob $(2t+1)^2 \cdot \frac{S}{2^k}$

$$\Longrightarrow$$

Measure $\mathcal{B}(t)\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{(2t+1)^2}{2^k}$

3. **Define $\mathcal{C}(t)$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}(t)$ and $\mathcal{O}_\chi$.**
4. $\mathcal{C}(t)$ requires $\approx \frac{\pi}{4} \cdot \sqrt{\frac{2^k}{(2t+1)^2}}$ calls to $\mathcal{B}(t), \mathcal{B}(t)^\dagger$ and $\mathcal{O}_\chi$.

$$\mathrm{Cost}(\mathcal{C}(t)) \approx \frac{\pi}{4} \cdot \frac{\sqrt{2^k}}{2t+1} \cdot \left(\mathcal{O}_\chi + 2t \cdot \mathcal{O}_\gamma\right) = \frac{\pi}{4} \cdot \frac{\sqrt{2^k}}{2t+1} \cdot \mathcal{O}_\chi + \frac{\pi}{4} \cdot \frac{2t}{2t+1} \cdot \sqrt{2^k} \cdot \mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology II

Theorem (Quantum amplitude amplification)

There is a quantum algorithm $\mathcal{B}(t) = \left(\mathcal{A}R_0\mathcal{A}^\dagger\mathcal{O}_\chi\right)^t\mathcal{A}$ *such that measuring* $\mathcal{B}(t)\,|0^k\rangle$ *gives* $x \in \{0,1\}^k$ *where* $\chi(x) = 1$ *with probability* $b(t) = \sin^2\left((2t+1)\cdot\arcsin\sqrt{a}\right) \approx (2t+1)^2\cdot a$ *for* $0 \le t \ll \frac{\pi}{4}\cdot\frac{1}{\sqrt{a}}$

1. Define $\mathcal{B}(t)$ with $\mathcal{A} := H^{\otimes k}$, $\mathcal{O}_\gamma$ and $t \ll \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{S}}$.
2. Measure $\mathcal{B}(t)\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\gamma(x) = 1$ w/prob $(2t+1)^2\cdot\frac{S}{2^k}$

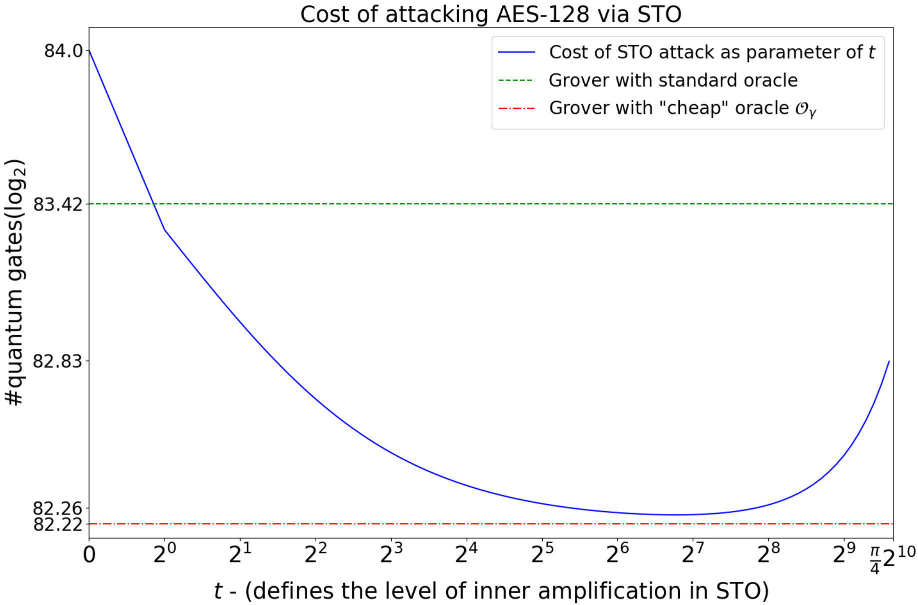
$$\Longrightarrow$$

Measure $\mathcal{B}(t)\,|0^k\rangle$ and obtain $x \in \{0,1\}^k$ where $\chi(x) = 1$ with prob $\frac{(2t+1)^2}{2^k}$

3. Define $\mathcal{C}(t)$ via amplitude amplification to use $\mathcal{A}' := \mathcal{B}(t)$ and $\mathcal{O}_\chi$.
4. **$\mathcal{C}(t)$ requires $\approx \frac{\pi}{4}\cdot\sqrt{\frac{2^k}{(2t+1)^2}}$ calls to $\mathcal{B}(t), \mathcal{B}(t)^\dagger$ and $\mathcal{O}_\chi$.**

$$\mathrm{Cost}(\mathcal{C}(t)) \approx \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\left(\mathcal{O}_\chi + 2t\cdot\mathcal{O}_\gamma\right) = \frac{\pi}{4}\cdot\frac{\sqrt{2^k}}{2t+1}\cdot\mathcal{O}_\chi + \frac{\pi}{4}\cdot\frac{2t}{2t+1}\cdot\sqrt{2^k}\cdot\mathcal{O}_\gamma$$

The Search with Two Oracles [KYYLHH15] methodology III



Designing quantum oracles I

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

Suffices to construct a *quantum evaluation*

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

and use the single qubit gate $Z|y\rangle \mapsto (-1)^y |y\rangle$

$$|x\rangle |0^w\rangle |0\rangle \overset{\mathcal{E}_\chi}{\mapsto} |g(x)\rangle |\chi(x)\rangle \overset{Z}{\mapsto} (-1)^{\chi(x)} |g(x)\rangle |\chi(x)\rangle \overset{\mathcal{E}_\chi^\dagger}{\mapsto} (-1)^{\chi(x)} |x\rangle |0^w\rangle$$

Designing quantum oracles II

In general for $f : \{0,1\}^n \longrightarrow \{0,1\}^m$

$$\mathcal{E}_f \left|x\right\rangle \left|0^w\right\rangle \left|0^m\right\rangle \mapsto \left|g(x)\right\rangle \left|f(x)\right\rangle$$

Standard methods to construct such circuits

- Single qubit X gates — $X \left|a\right\rangle \left|\bar{a}\right\rangle$
- Two qubit $\wedge_1(X)$/CNOT gates — $\wedge_1(X) \left|a\right\rangle \left|b\right\rangle \mapsto \left|a\right\rangle \left|b \oplus a\right\rangle$
- Three qubit QAND gates — QAND $\left|a\right\rangle \left|b\right\rangle \left|0\right\rangle \mapsto \left|a\right\rangle \left|b\right\rangle \left|ab\right\rangle$
  QAND† $\left|a\right\rangle \left|b\right\rangle \left|ab\right\rangle \mapsto \left|a\right\rangle \left|b\right\rangle \left|0\right\rangle$
- (Generalised Toffoli gates) $\wedge_k(X)$ for $k \geq 2$

$$\wedge_k(X) \left|a_1 \ldots a_k\right\rangle \left|b\right\rangle \mapsto \left|a_1 \ldots a_k\right\rangle \left|b \oplus a_1 \cdots a_k\right\rangle$$

[JNRV20] provides Q# code[2] for AES : $\{0,1\}^k \times \{0,1\}^{128} \longrightarrow \{0,1\}^{128}$

[2] `https://github.com/microsoft/grover-blocks`

Designing quantum oracles III

Design principles [GLRS16] for

$$\mathcal{E}_{\mathsf{AES}} \left|K\right\rangle \left|P\right\rangle \left|0^w\right\rangle \mapsto \left|g(x)\right\rangle \left|\mathsf{AES}(K,P)\right\rangle$$

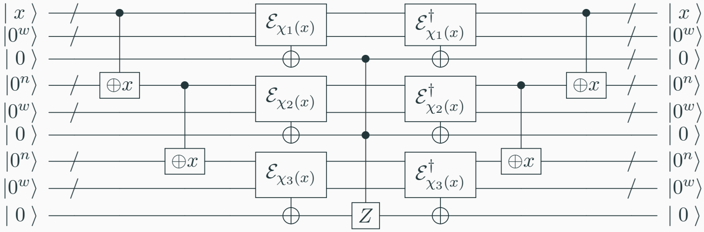
- Compose modular quantum circuits for MixColumns and S-Boxes.
- Combine with in-place KeyExpansion [JNRV20].
- Design for $\mathcal{E}_{\mathsf{AES}}$ is then based upon the classical circuit for AES.

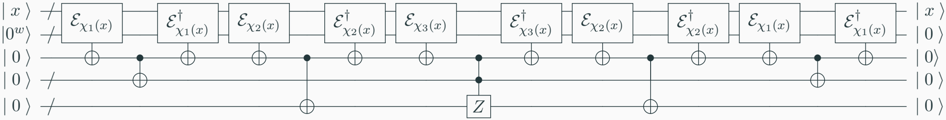
Concrete results based upon low-depth version from [JNRV20]:

$$\mathcal{E}_{\mathsf{AES}} \left|K\right\rangle \; \left|P\right\rangle \; \left|0^{128}\right\rangle \ldots \left|0^{128}\right\rangle \mapsto \; \left|\mathsf{Key}_N(K)\right\rangle \; \left|\mathsf{AES}_1(K,P)\right\rangle \ldots \left|\mathsf{AES}_N(K,P)\right\rangle$$

Our results apply to **any** choice of trade-off between qubits and depth.

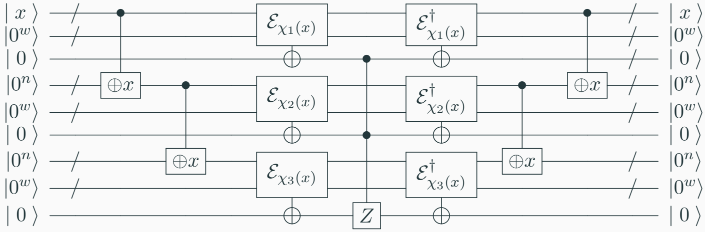
Two oracle designs

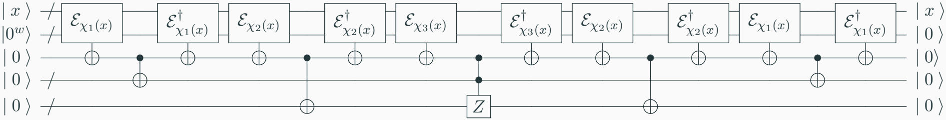




	≈ gates	≈ depth	≈ qubits
Parallel	$2r \cdot S_{\mathcal{E}_{\chi_i}}$	$2 \cdot D_{\mathcal{E}_{\chi_i}}$	$r \cdot (k + W_{\mathcal{E}_{\chi_i}})$
Serial	$(4r-2) \cdot S_{\mathcal{E}_{\chi_i}}$	$(4r-2) \cdot D_{\mathcal{E}_{\chi_i}}$	$k + W_{\mathcal{E}_{\chi_i}}$

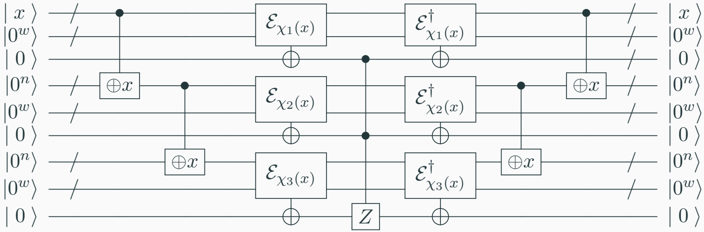
Two oracle designs

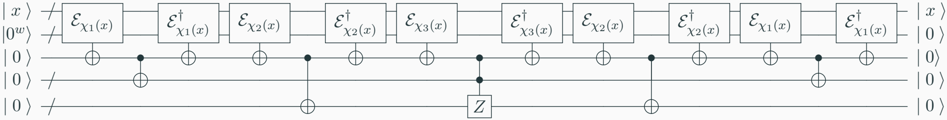




AES-256	$\approx$ gates	$\approx$ depth	$\approx$ qubits
Parallel	6	2	3
Serial	10	10	1

Two oracle designs





AES-128/192	≈ gates	≈ depth	≈ qubits
Parallel	4	2	2
Serial	6	6	1

Designing the the cheap quantum oracle

Error in STO reliant upon estimation of $\frac{1}{S}$ and $\frac{S}{2^k}$.

$$\hat{\gamma}(K) \mapsto \gamma(K) \ \vee \ \mathsf{CheckBits}_{20}(K)$$

where $\gamma, \mathsf{CheckBits} : \{0,1\}^k \longrightarrow \{0,1\}$

$$\gamma(K) \mapsto \text{Do Enc}(K, P_1) \text{ and } C_1 \text{ match on } 4 \text{ specific bytes?}$$

$$\mathsf{CheckBits}_{20}(K) \mapsto \text{Is } K \text{ of the form } 0^{20} \| x \text{ for some } x \in \{0,1\}^{k-20}\text{?}$$

Designing the the cheap quantum oracle

Error in STO reliant upon estimation of $\frac{1}{S}$ and $\frac{S}{2^k}$.

$$\hat{\gamma}(K) \mapsto \gamma(K) \ \vee\ \mathsf{CheckBits}_{20}(K)$$

where $\gamma, \mathsf{CheckBits} : \{0,1\}^k \longrightarrow \{0,1\}$

$$\gamma(K) \mapsto \text{Do Enc}(K, P_1) \text{ and } C_1 \text{ match on } 4 \text{ specific bytes?}$$

$$\mathsf{CheckBits}_{20}(K) \mapsto \text{Is } K \text{ of the form } 0^{20} \| x \text{ for some } x \in \{0,1\}^{k-20}\text{?}$$

- $S = |\{x \in \{0,1\}^k : \ \gamma(x) = 1 \ \}|$
- $\hat{S} = \left|\{x \in \{0,1\}^k : (\gamma(x) = 1) \vee (x = 0^{20} \| y \text{ for some } y \in \{0,1\}^{k-20})\}\right|$.

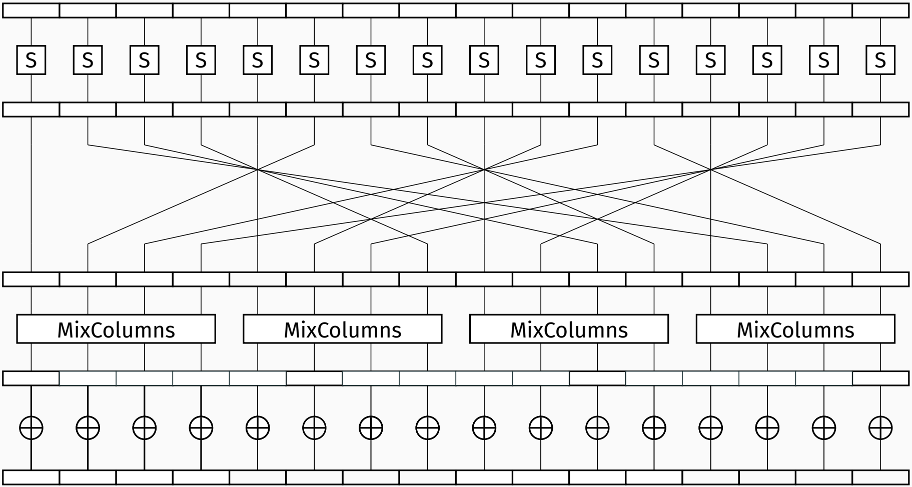
$$2^{k-33} \leq S \leq 2^{k-31}$$

$$\Downarrow$$

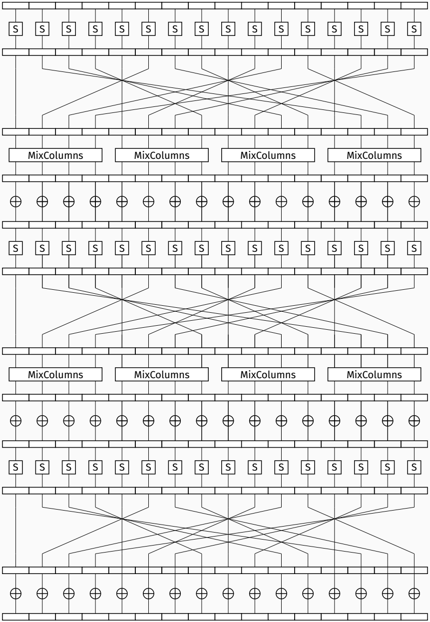
$$2^{k-20} \leq \hat{S} \leq 2^{k-20} + 2^{k-31} \approx 2^{k-20}$$

General structure of AES rounds

AES-128/192/256 — 10/12/14 rounds with similar structure.



Designing quantum oracles IV

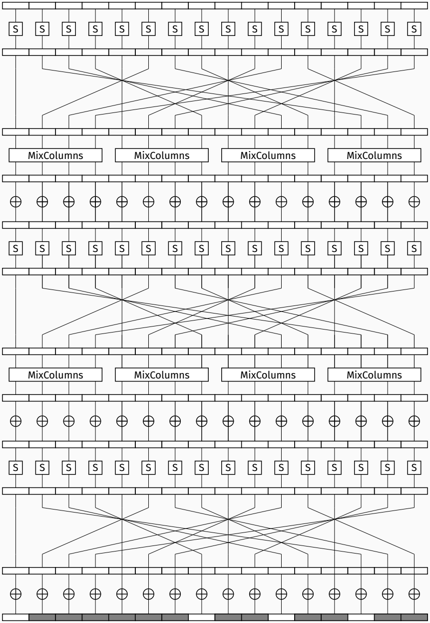


Round N-2

Round N-1

Round N

Designing quantum oracles IV

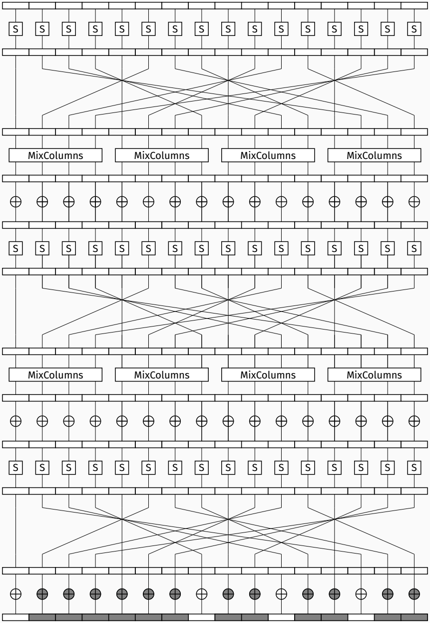


Round N-2

Round N-1

Round N

Designing quantum oracles IV

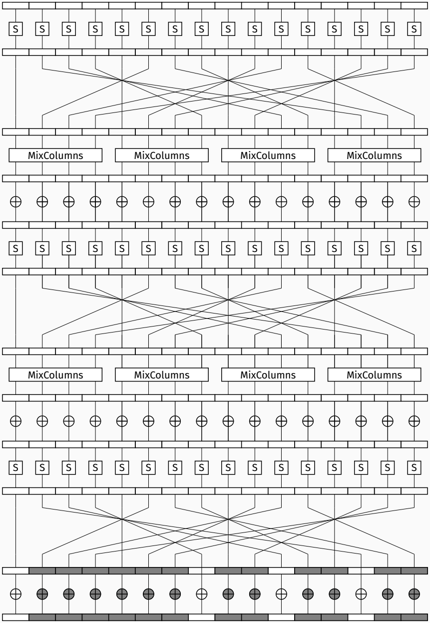


Round N-2

Round N-1

Round N

Designing quantum oracles IV

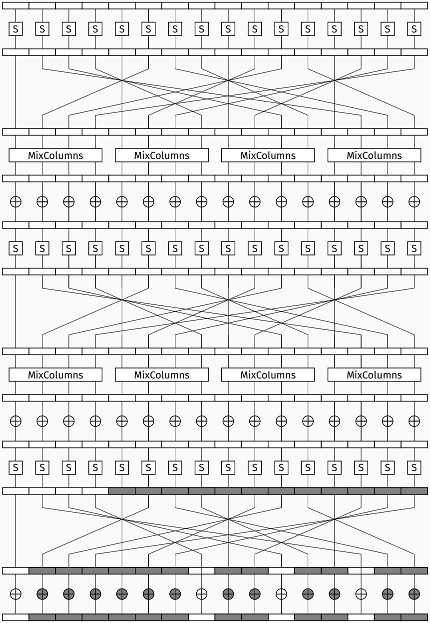


Round N-2

Round N-1

Round N

Designing quantum oracles IV

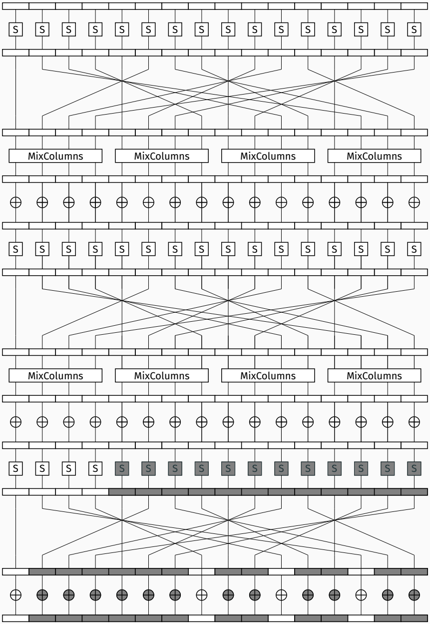


Round N-2

Round N-1

Round N

Designing quantum oracles IV

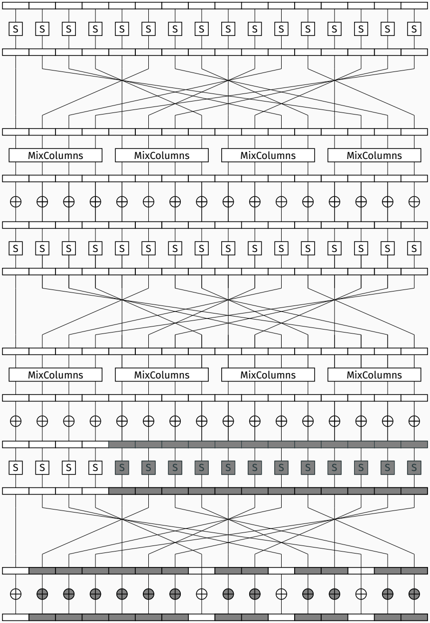


Round N-2

Round N-1

Round N

Designing quantum oracles IV



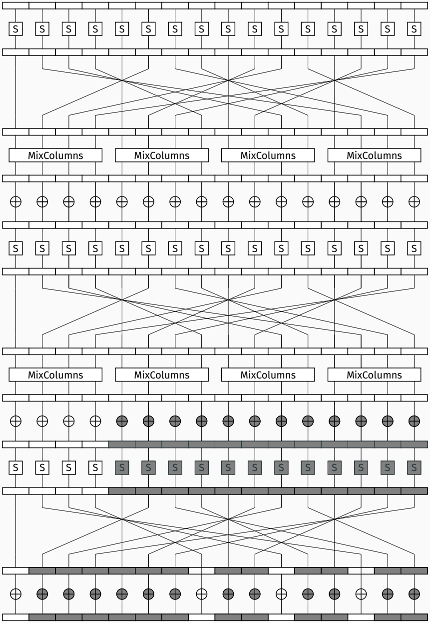
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



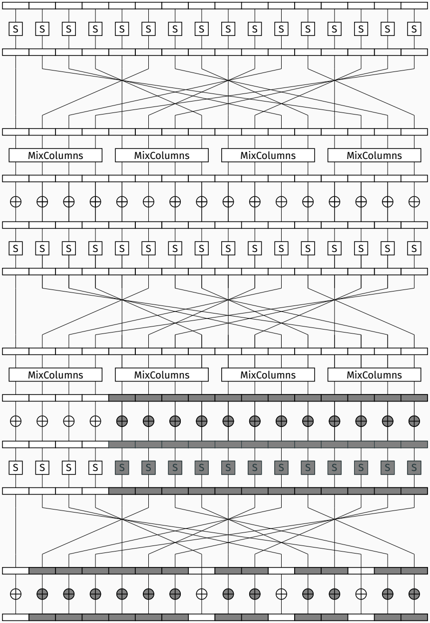
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



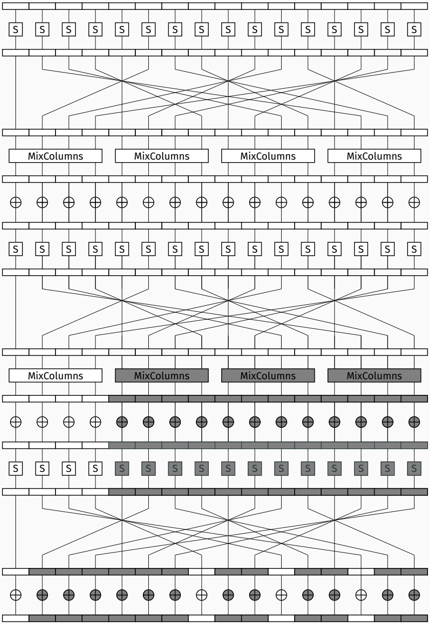
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



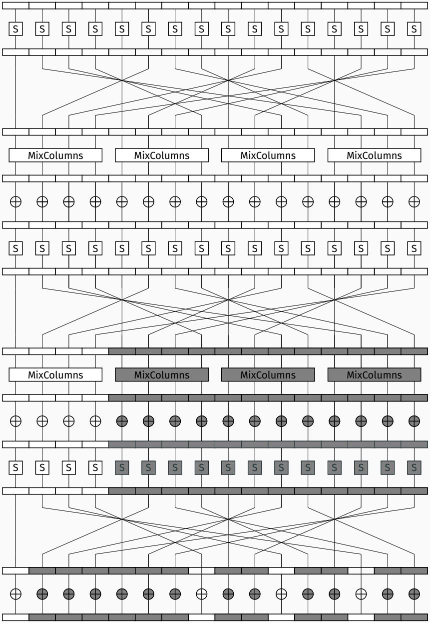
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



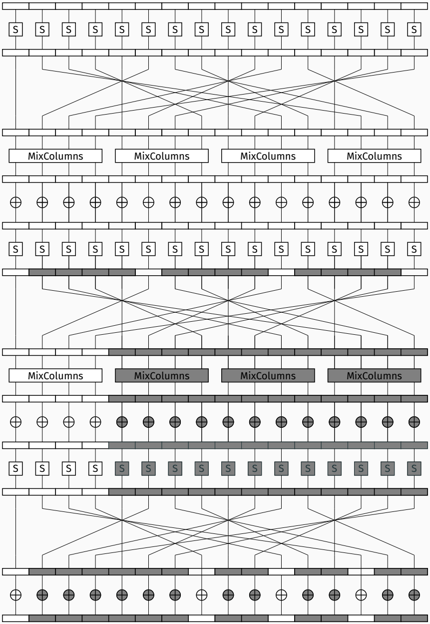
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



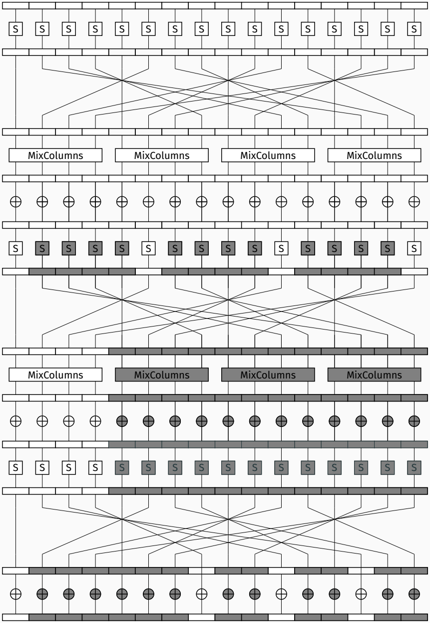
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



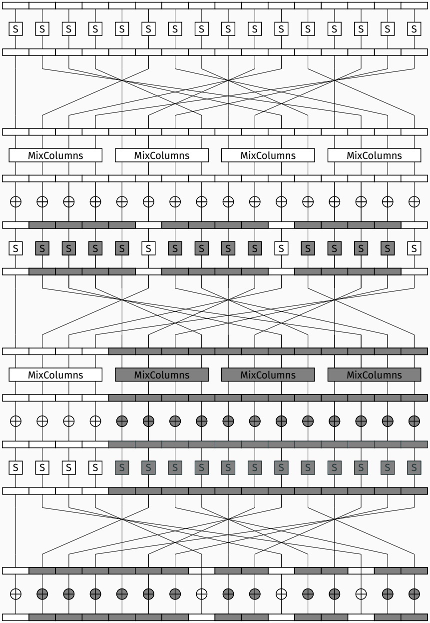
Round N-2

Round N-1

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



Round N-2

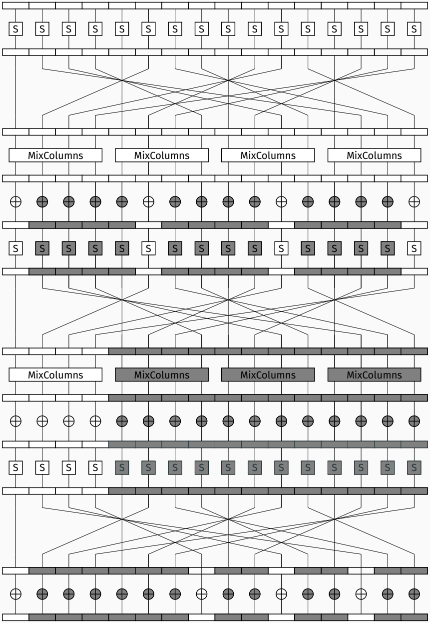
Round N-1 new cost:

- 4/16 S-boxes
- 1/4 MixColumns operations
- 32/128 CNOTs (KeyExpansion)

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



Round N-2

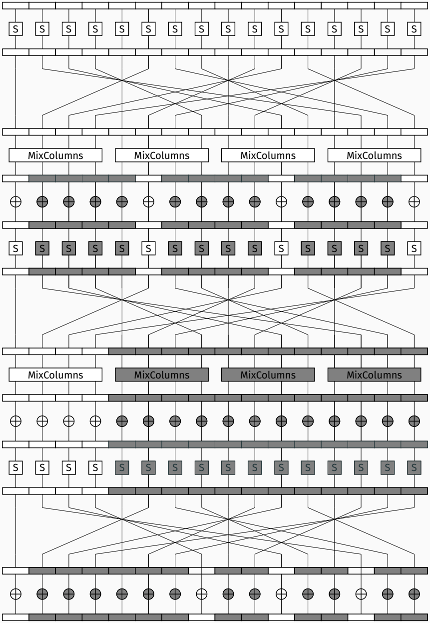
Round N-1 new cost:

- 4/16 S-boxes
- 1/4 MixColumns operations
- 32/128 CNOTs (KeyExpansion)

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



Round N-2

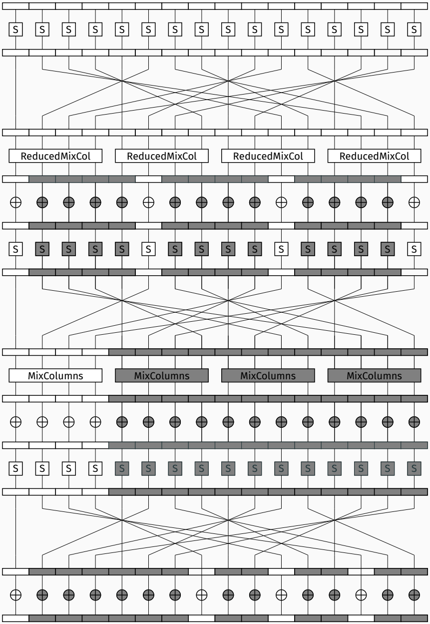
Round N-1 new cost:

- 4/16 S-boxes
- 1/4 MixColumns operations
- 32/128 CNOTs (KeyExpansion)

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



Round N-2 new cost:

- 16 S-boxes (no change)
- 152/1108 CNOTs (MixColumns)
- Depth 111 $\longrightarrow$ Depth 6 (MixColumns)
- 28/128 CNOTs (KeyExpansion)

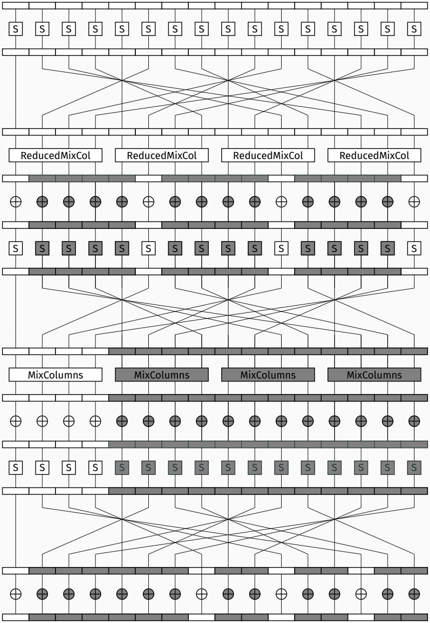
Round N-1 new cost:

- 4/16 S-boxes
- 1/4 MixColumns operations
- 32/128 CNOTs (KeyExpansion)

Round N new cost:

- 4/16 S-boxes
- 32/128 CNOTs (KeyExpansion)

Designing quantum oracles IV



Total savings $\approx$ 1.5 rounds.

- AES-128 $\log_2$ savings — ≈ 0.23
- AES-192 $\log_2$ savings — ≈ 0.19
- AES-256 $\log_2$ savings — ≈ 0.16

No major change in depth.

Saved qubits can be repurposed.

Concrete oracle statistics[3] from Q#

- Reduced cost oracles programmed[4] and unit-tested in Q#.
- Based upon circuits from [JNRV20][5].

Oracle type/MixColumns	r/bits compared	$\# \wedge_1 (X)$	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 (IP) [JNRV20]	1/128	292313	84428	54908	13727	121	2816	1665
AES-128 (IP) (this paper)	1/32	255195	73597	47996	12255	121	2656	1466
AES-128 (IP) [JNRV20]	2/256	585051	169184	109820	27455	121	2815	3329
AES-128 (IP) (serial [JNRV20])	2/256	876637	252156	164728	41182	363	8434	1667

[3] Note that there is currently a bug in the Microsoft Q# resource estimator: `https://github.com/microsoft/qsharp-runtime/issues/192`

[4] Code available at: `https://github.com/public-ket/reduced-aes`

[5] Code based upon: `https://github.com/microsoft/grover-blocks`

Concrete oracle statistics[3] from Q#

- Reduced cost oracles programmed[4] and unit-tested in Q#.
- Based upon circuits from [JNRV20][5].

Oracle type/MixColumns	r/bits compared	$\# \wedge_1 (X)$	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 (IP) [JNRV20]	**1/128**	**292313**	**84428**	**54908**	**13727**	**121**	**2816**	**1665**
AES-128 (IP) (this paper)	1/32	255195	73597	47996	12255	121	2656	1466
AES-128 (IP) [JNRV20]	**2/256**	**585051**	**169184**	**109820**	**27455**	**121**	**2815**	**3329**
AES-128 (IP) (serial [JNRV20])	2/256	876637	252156	164728	41182	363	8434	1667

[3] Note that there is currently a bug in the Microsoft Q# resource estimator: `https://github.com/microsoft/qsharp-runtime/issues/192`

[4] Code available at: `https://github.com/public-ket/reduced-aes`

[5] Code based upon: `https://github.com/microsoft/grover-blocks`

Concrete oracle statistics[3] from Q#

- Reduced cost oracles programmed[4] and unit-tested in Q#.
- Based upon circuits from [JNRV20][5].

Oracle type/MixColumns	r/bits compared	$\# \wedge_1 (X)$	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 (IP) [JNRV20]	1/128	292313	84428	54908	13727	121	2816	1665
AES-128 (IP) (this paper)	**1/32**	**255195**	**73597**	**47996**	**12255**	**121**	**2656**	**1466**
AES-128 (IP) [JNRV20]	2/256	585051	169184	109820	27455	121	2815	3329
AES-128 (IP) (serial [JNRV20])	**2/256**	**876637**	**252156**	**164728**	**41182**	**363**	**8434**	**1667**

[3] Note that there is currently a bug in the Microsoft Q# resource estimator: `https://github.com/microsoft/qsharp-runtime/issues/192`

[4] Code available at: `https://github.com/public-ket/reduced-aes`

[5] Code based upon: `https://github.com/microsoft/grover-blocks`

Effect on quantum cryptanalysis of AES

Source	G-cost	DW-cost	#Depth	#Qubits	#Success%
AES-128 [JNRV20] ($r = 1$)	$2^{82.42}$	$2^{85.81}$	$2^{75.11}$	1665	$\frac{1}{e} \approx 0.37$
AES-128 [JNRV20] ($r = 2$)	$2^{83.42}$	$2^{86.81}$	$2^{75.11}$	3329	≈ 1
AES-128 (This paper)	$2^{82.25}$	$2^{85.75}$	$2^{75.05}$	1667	≈ 1
AES-192 [JNRV20] ($r = 2$)	$2^{115.58}$	$2^{119.14}$	$2^{107.19}$	3969	≈ 1
AES-192 (This paper)	$2^{114.44}$	$2^{118.04}$	$2^{107.08}$	1987	≈ 1
AES-256 [JNRV20] ($r = 2$)	$2^{147.88}$	$2^{151.54}$	$2^{139.37}$	4609	$\frac{1}{e} \approx 0.37$
AES-256 [JNRV20] ($r = 3$)	$2^{148.47}$	$2^{152.11}$	$2^{139.36}$	6913	≈ 1
AES-256 (This paper)	$2^{146.77}$	$2^{150.42}$	$2^{139.38}$	2307	≈ 1

Effect on quantum cryptanalysis of AES

Source	G-cost	DW-cost	#Depth	#Qubits	#Success%
AES-128 [JNRV20] ($r = 1$)	$2^{82.42}$	$2^{85.81}$	$2^{75.11}$	1665	$\frac{1}{e} \approx 0.37$
AES-128 [JNRV20] ($\mathbf{r = 2}$)	$\mathbf{2^{83.42}}$	$\mathbf{2^{86.81}}$	$\mathbf{2^{75.11}}$	**3329**	$\approx \mathbf{1}$
AES-128 (This paper)	$\mathbf{2^{82.25}}$	$\mathbf{2^{85.75}}$	$\mathbf{2^{75.05}}$	**1667**	$\approx \mathbf{1}$
AES-192 [JNRV20] ($\mathbf{r = 2}$)	$\mathbf{2^{115.58}}$	$\mathbf{2^{119.14}}$	$\mathbf{2^{107.19}}$	**3969**	$\approx \mathbf{1}$
AES-192 (This paper)	$\mathbf{2^{114.44}}$	$\mathbf{2^{118.04}}$	$\mathbf{2^{107.08}}$	**1987**	$\approx \mathbf{1}$
AES-256 [JNRV20] ($r = 2$)	$2^{147.88}$	$2^{151.54}$	$2^{139.37}$	4609	$\frac{1}{e} \approx 0.37$
AES-256 [JNRV20] ($\mathbf{r = 3}$)	$\mathbf{2^{148.47}}$	$\mathbf{2^{152.11}}$	$\mathbf{2^{139.36}}$	**6913**	$\approx \mathbf{1}$
AES-256 (This paper)	$\mathbf{2^{146.77}}$	$\mathbf{2^{150.42}}$	$\mathbf{2^{139.38}}$	**2307**	$\approx \mathbf{1}$

Effect on quantum cryptanalysis of AES

Source	G-cost	DW-cost	#Depth	#Qubits	#Success%
AES-128 [JNRV20] ($\mathbf{r} = 1$)	$\mathbf{2^{82.42}}$	$\mathbf{2^{85.81}}$	$\mathbf{2^{75.11}}$	**1665**	$\mathbf{\frac{1}{e} \approx 0.37}$
AES-128 [JNRV20] ($r = 2$)	$2^{83.42}$	$2^{86.81}$	$2^{75.11}$	3329	≈ 1
AES-128 (This paper)	$\mathbf{2^{82.25}}$	$\mathbf{2^{85.75}}$	$\mathbf{2^{75.05}}$	**1667**	≈ 1
AES-192 [JNRV20] ($\mathbf{r} = \mathbf{2}$)	$\mathbf{2^{115.58}}$	$\mathbf{2^{119.14}}$	$\mathbf{2^{107.19}}$	**3969**	≈ 1
AES-192 (This paper)	$\mathbf{2^{114.44}}$	$\mathbf{2^{118.04}}$	$\mathbf{2^{107.08}}$	**1987**	≈ 1
AES-256 [JNRV20] ($\mathbf{r} = 2$)	$\mathbf{2^{147.88}}$	$\mathbf{2^{151.54}}$	$\mathbf{2^{139.37}}$	**4609**	$\mathbf{\frac{1}{e} \approx 0.37}$
AES-256 [JNRV20] ($r = 3$)	$2^{148.47}$	$2^{152.11}$	$2^{139.36}$	6913	≈ 1
AES-256 (This paper)	$\mathbf{2^{146.77}}$	$\mathbf{2^{150.42}}$	$\mathbf{2^{139.38}}$	**2307**	≈ 1

NIST and the MAXDEPTH constraint I

MAXDEPTH = limit on maximum quantum allowable circuit depth.

MAXDEPTH $\in \{2^{40}, 2^{64}, 2^{96}\}$ for NIST PQ standardisation effort [oST16].

Inner parallelism: fix $0 \leq p \leq k$ bits and run $P = 2^p$ instances.

$$\mathbb{E}\Big[\text{\# keys on correct choice of } x_1 \dots x_p\Big] = 1 + 2^{k-p-rn}$$

Effect on Grover's algorithm (cost dependent on r):

$$\frac{\pi}{4} \cdot \sqrt{2^k} \cdot r \cdot \mathcal{O}_{\mathsf{AES}} \longrightarrow 2^p \cdot \frac{\pi}{4} \cdot \sqrt{2^{k-p}} \cdot \hat{r} \cdot \mathcal{O}_{\mathsf{AES}} \quad = \frac{\pi}{4} \cdot 2^{\frac{k+p}{2}} \cdot \hat{r} \cdot \mathcal{O}_{\mathsf{AES}}$$

Effect on STO algorithm (cost negligibly dependent on r):

$$\frac{\pi}{4} \cdot 2^{k/2} \cdot \mathcal{O}_{\mathsf{AES}_{\mathsf{reduced}}} \longrightarrow 2^p \cdot \frac{\pi}{4} \cdot 2^{\frac{k-p}{2}} \cdot \mathcal{O}_{\mathsf{AES}_{\mathsf{reduced}}} \quad = \frac{\pi}{4} \cdot 2^{\frac{k+p}{2}} \cdot \mathcal{O}_{\mathsf{AES}_{\mathsf{reduced}}}$$

NIST and the MAXDEPTH constraint II

MAXDEPTH = ∞ — use $r = 2/2/3$ for AES-128/192/256.

MAXDEPTH = $2^{40}/2^{64}$ — use $\hat{r} = 1$ plaintext-ciphertexts.

MAXDEPTH = 2^{96} — use $\hat{r} = 2$ plaintext-ciphertexts.

NIST Security level	Source	G-cost for MAXDEPTH ($\log_2$) 2^{40}	2^{64}	2^{96}
1 AES-128	[oST16, GLRS16]	130.0	106.0	87.5
	[JNRV20]	117.1	93.1	83.4
	This paper	**116.9**	**92.9**	**82.3**
3 AES-192	[oST16]	193.0	169.0	137.0
	[JNRV20]	181.1	157.1	126.1
	This paper	**180.9**	**156.9**	**125.0**
5 AES-256	[oST16]	258.0	234.0	202.0
	[JNRV20]	245.5	221.5	190.5
	This paper	**245.3**	**221.3**	**189.3**

Conclusions and takeaways

- Minor gains — but applicable to cryptanalysis of **all** block-ciphers.
- AES one bit less secure in NIST MAXDEPTH$= 2^{96}$ scenario.
- Fewer qubits required is advantageous for cryptanalysis timeline.
- Zero impact upon query-complexity — $\frac{\pi}{4} \cdot 2^{k/2}$ a safe lower-bound.

Acknowledgements

The authors kindly thank the reviewers for their constructive feedback and for pointing out the resource estimation bug in Q#.

Benjamin Pring was funded during the development of this research by EPRSC grant EP/M50645X/1, National Science Foundation grant 183980, NIST grant 60NANB17D184, a Seed grant of the Florida Center for Cybersecurity and a USF proposal enhancement grant.

An early version of these results was first announced at the International Workshop on Coding and Cryptography 2019.

References i

- Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp, Quantum amplitude amplification and estimation, Contemporary Mathematics **305** (2002), 53–74.
- 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.
- Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia, Implementing grover oracles for quantum key search on aes and lowmc, Advances in Cryptology – EUROCRYPT 2020 (Cham) (Anne Canteaut and Yuval Ishai, eds.), Springer International Publishing, 2020, pp. 280–310.

References ii

- Samuel Jaques and John M. Schanck, Quantum cryptanalysis in the ram model: Claw-finding attacks on sike, Advances in Cryptology – CRYPTO 2019 (Cham) (Alexandra Boldyreva and Daniele Micciancio, eds.), Springer International Publishing, 2019, pp. 32–61.
- Shelby Kimmel, Cedric Yen-Yu Lin, and Lin Han-Hsuan, Oracles with costs, 2015.
- National Institute of Standards and Technology., Submission requirements and evaluation criteria for the post-quantum cryptography standardization process., 2016.