National Cyber Security Centre

On the practical cost of Grover for AES key recovery

Sarah D.
UK NCSC

Quantum Computing and Cryptography

- Shor's algorithm – period finding
  - Clear threat to public key algorithms.
  - New post-quantum algorithms recently standardised by NIST.
  - Protocol adaptation underway in IETF and elsewhere.

- Grover's algorithm – unstructured search problem
  - Possible limited threat to symmetric key algorithms.

- Where should mitigation efforts be focused?

Aims

- Assess impact of Grover on symmetric cryptography for near-term quantum hardware.
  - AES considered here, analysis similar for other symmetric algorithms.
- Estimate logical implementation and parallelisation overheads on any hardware.
  - Logical qubit-cycles.
- Estimate error correction overheads when using planar surface code.
  - Surface code cycles and physical qubit count.

Unstructured Search Problem

- For a set X with $|X| = N$ and a function $f: X \to \{0, 1\}$, find unique $x \in X$ such that $f(x) = 1$
- Unstructured means that we cannot do better than brute force, i.e. repeatedly evaluating f on values in X.
- Expected number of queries to f on a classical computer is therefore $\frac{N}{2}$

Unstructured Search Problem – Relation to Cryptography

- Can set up the key recovery problem for a symmetric block cipher (e.g. AES-128) as an unstructured search problem.
- Given ciphertext $C = Enc(K, P)$ for some unknown key K and some cribbed (guessed) plaintext P.
- Let X be the set of all possible key values and define $f: X \to \{0,1\}$:

$$f(x) = \begin{cases} 1 & \text{if } \mathrm{Enc}(x, P) = C, \\ 0 & \text{otherwise.} \end{cases}$$

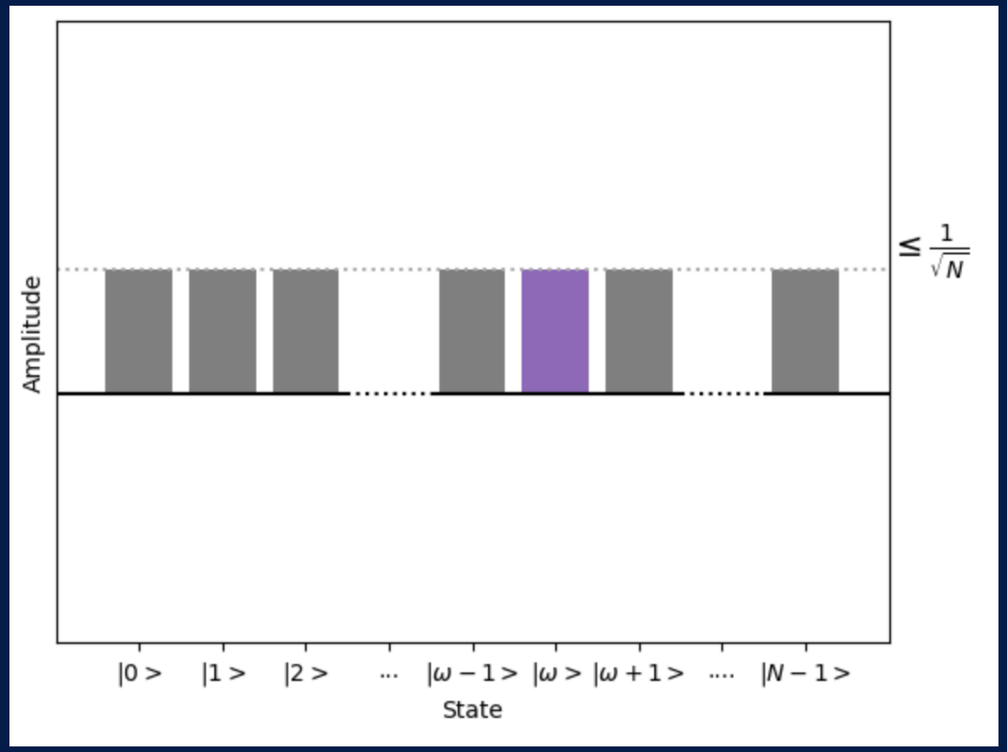
Grover's Algorithm

- Published by Lov Grover in 1996.
- Solves the unstructured search problem with $O(\sqrt{N})$ quantum queries to the oracle function f.
- Asymptotically optimal for this problem (Zalka, 1997)

Grover's Algorithm - Initialisation

Start with evenly distributed amplitudes in superposition:

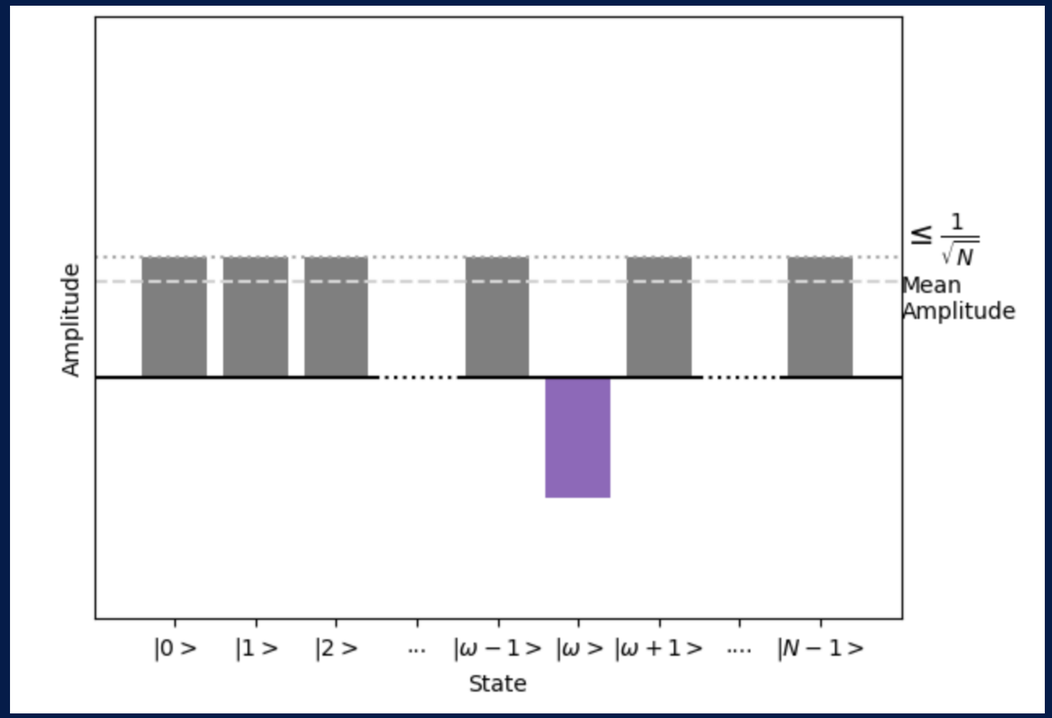
$$\frac{1}{\sqrt{N}} \sum_{x} |x\rangle$$



Grover's Algorithm – Oracle Function

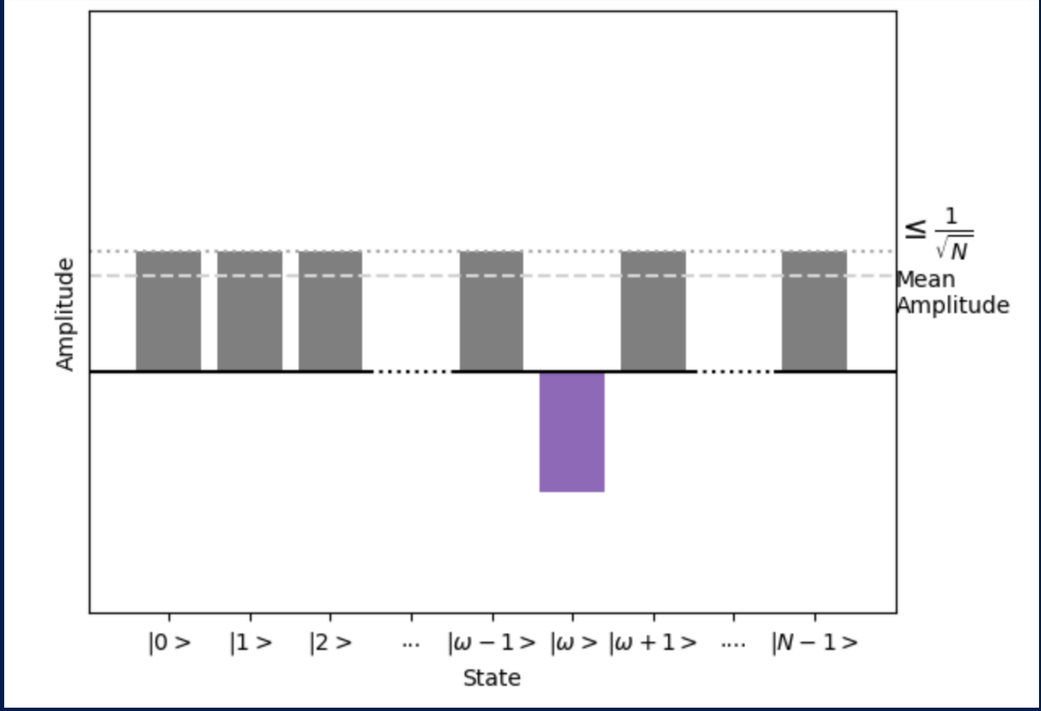
Flip the sign of the exceptional value:

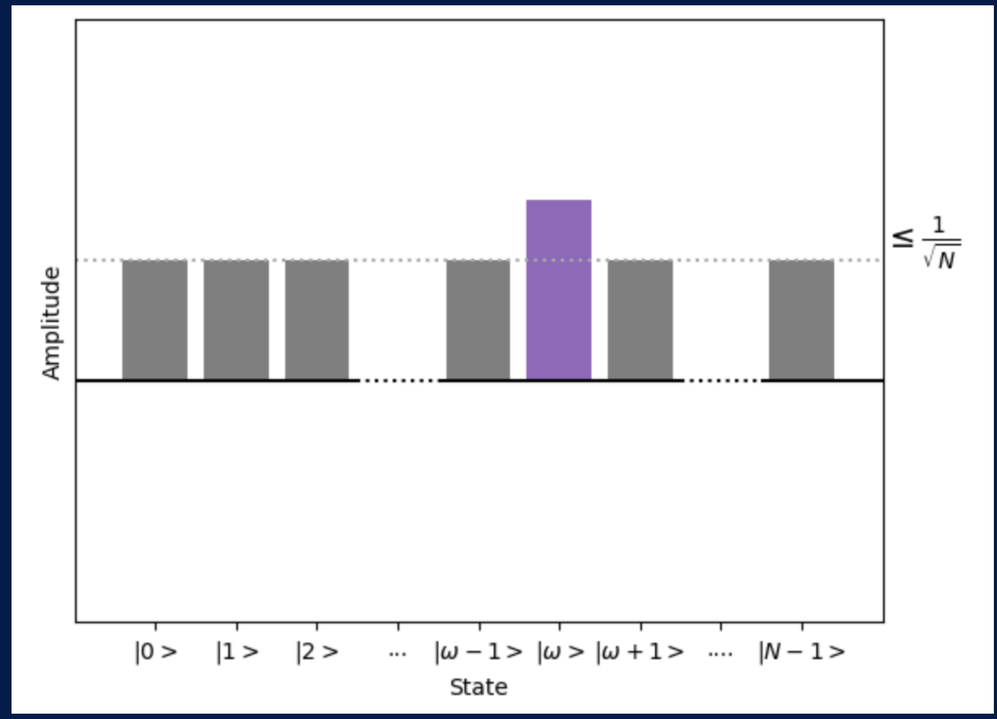
$$\frac{1}{\sqrt{N}}\sum_{x}|x\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}}\sum_{x}(-1)^{f(x)}|x\rangle$$



Grover’s Algorithm - Reflection

Reflect amplitudes in the “average amplitude” line





Grover's Algorithm – Iteration and Measurement

- Iterate oracle and reflection operators $O(\sqrt{N})$ times and finally measure to recover desired state ω with high probability.
- Oracle queries are made sequentially.
- Terminating early (e.g. making only $\frac{N}{S}$ queries) reduces success probability by a factor S^2.

Grover's Algorithm – Implications for Cryptography

- Can apply Grover to AES with key length k bits ($k \in \{128, 192, 256\}$).
- Succeeds with high probability after $(\pi/4)\sqrt{2^k}$ quantum AES queries.
- For AES-128, Grover takes around 2^{64} quantum AES queries compared with 2^{127} classical queries for brute force exhaustion.
- This is sometimes reported as "Grover's halves the effective key length of symmetric algorithms."

Grover's Algorithm – Implications for Cryptography

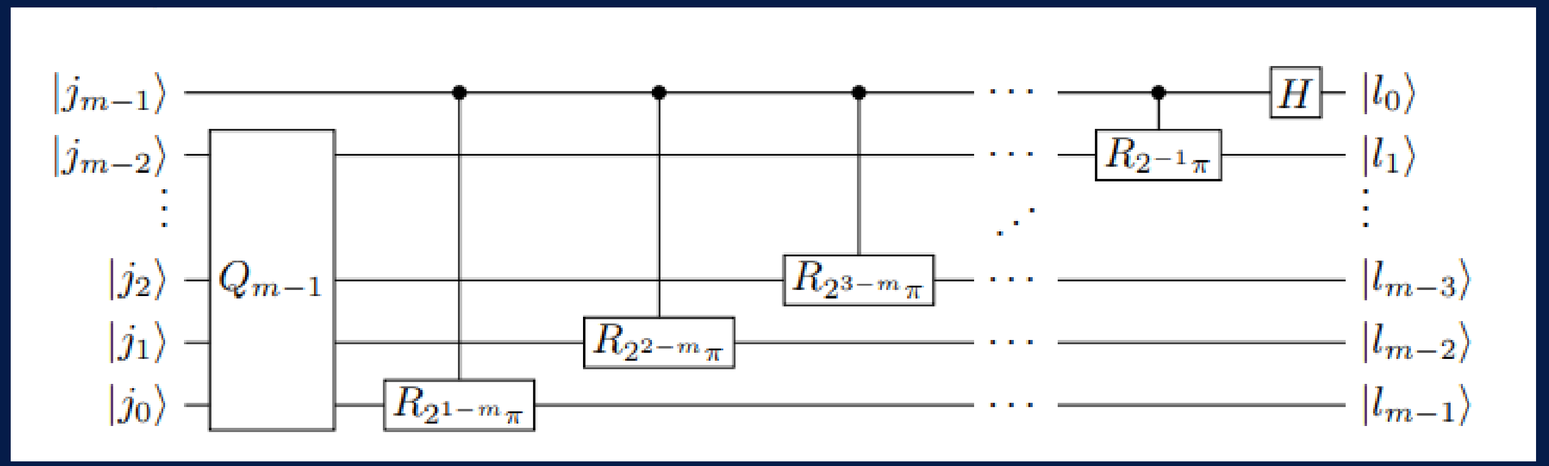
- However, the square-root speed-up headline neglects significant details:
  - The cost of quantum AES implementations.
  - The fact that the AES queries must be sequential.
  - The overheads from quantum error correction.

Oracle Implementation

- Depth – the number of sequential quantum gates that must be executed.
- Width – the maximal number of qubits needed during execution.

Depth

Width



Oracle implementation

- Different implementations optimise for different metrics.
- We use Jang et al. “Quantum analysis of AES”, IACR ePrint 2022/683:
  - Minimises (circuit depth)^2 x (number of qubits).

AES Key Size	Depth	Qubits	Depth^2 x Qubits
128	731	3428	$2^{30.8}$
192	874	3748	$2^{31.4}$
256	1025	4036	$2^{32.0}$

Maximum depth

Max depth	Cycle time		
	1µs	200ns	1ns
2^{40}	12.7 days	2.55 days	18.3 mins
2^{48}	8.92 years	1.78 years	3.26 days
2^{56}	2,280 years	457 years	2.28 years
2^{64}	585,000 years	117,000 years	585 years

Parallelisation

- Limiting maximum depth limits number of iterations that can be performed.
- Reducing number of iterations by a factor of S reduces success probability by S^2.
- Alternatively, we can split the search space into subsets of size N/S^2.
- Either way, S^2 quantum processors are needed to cover the same search space.
- Overall costs (compute cost x time taken) have increased by a factor of S.

Costing Methodology – When Parallelisation Is Required

1. Calculate number of AES iterations per run from the implementation depth and MAX DEPTH choice.

$$N_{iter} = \frac{D_{max}}{D_{AES}}$$

2. Calculate the number of quantum processors needed, i.e. find S such that.

$$N_{iter} = \left(\frac{\pi}{4}\right) \frac{2^{k/2}}{\sqrt{S}}$$

3. Calculate the total number of logical qubits required.

$$W_{tot} = SW_{AES}$$

4. Calculate the cost in terms of number of logical qubit cycles.

$$C_{tot} = W_{tot}D_{max} = SW_{AES}D_{max} = \left(\frac{4}{2^{k/2}\pi}\, N_{iter}\right)^{-2} W_{AES}D_{max} = \boxed{2^k \left(\frac{\pi}{4}\right)^2 \frac{D_{AES}^2 W_{AES}}{D_{max}}}$$

AES-128 logical costs

- Using logical qubit-cycles accounts for the non-trivial cost of idle qubits.

Max depth	Iterations	Parallel instances	Logical qubits	Logical qubit-cycles
2^{40}	$2^{30.5}$	$2^{66.3}$	$2^{78.1}$	$2^{118.1}$
2^{48}	$2^{38.5}$	$2^{50.3}$	$2^{62.1}$	$2^{110.1}$
2^{56}	$2^{46.5}$	$2^{34.3}$	$2^{46.1}$	$2^{102.1}$
2^{64}	$2^{54.5}$	$2^{18.3}$	$2^{30.1}$	$2^{94.1}$
∞	$2^{63.7}$	1	$2^{12.7}$	$2^{85.9}$

Quantum error correction

- Important to distinguish between perfect logical qubits and noisy physical qubits.
- Logical qubits are built from many physical qubits using quantum error correction.
- The planar surface code is currently the best studied QEC scheme.
  - Exponentially suppresses errors as code distance d increase.
  - Uses $2d^2 - 1$ physical qubits to produce one logical qubit.

Quantum error correction

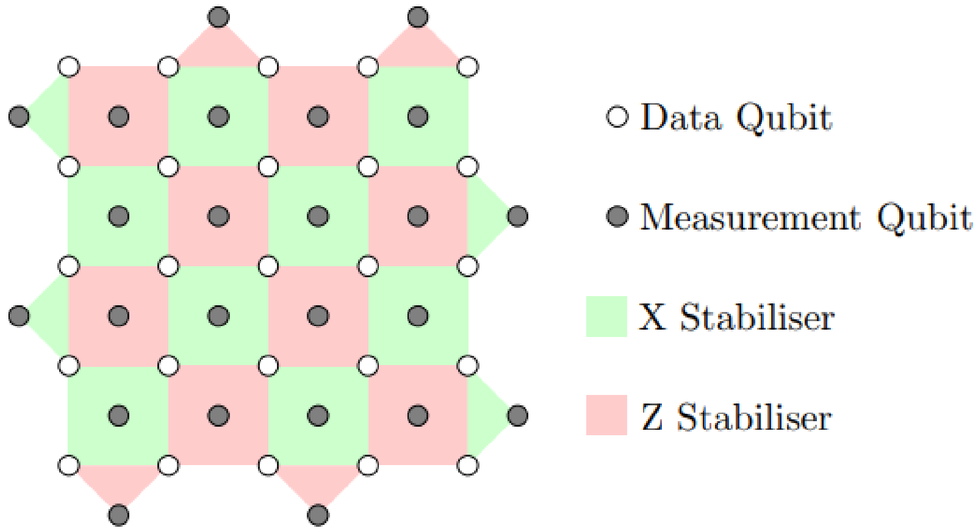


Figure 1: A surface code qubit with $d = 5$

Quantum error correction

- All error correction schemes have quantum gates that cannot be applied directly.
- These can instead be applied by producing “magic states”, which can be combined with basic gates to produce the desired non-basic gate.
- Creating high accuracy magic states will be done via magic state distillation, which creates them by combining many lower accuracy states.
- Magic state distillation requires additional quantum hardware, known as magic state factories or distilleries.

AES-128 surface code costs

Maximum depth	10^{-4} physical error		10^{-6} physical error	
	Physical qubits	Surface code cycles	Physical qubits	Surface code cycles
2^{40}	$2^{97.1}$	$2^{128.7}$	$2^{91.6}$	$2^{125.0}$
2^{48}	$2^{81.7}$	$2^{120.9}$	$2^{76.7}$	$2^{117.4}$
2^{56}	$2^{66.3}$	$2^{112.8}$	$2^{62.9}$	$2^{111.5}$
2^{64}	$2^{51.1}$	$2^{105.3}$	$2^{48.1}$	$2^{104.2}$

AES-128 overheads

- Logical implementation: 31 bits
- Parallelisation: 8 - 32 bits (depending on maximum depth)
- Error correction: 6 - 10 bits (depending on physical error rate)
  - *Distillation: 1 - 3 bits (included in error correction overhead)*

These are not entirely independent: less parallelisation needs more error correction.

Potential cost reductions

- Smaller AES implementations.
- Faster cycle times.
- Better physical error rates.
- More efficient error correcting codes.

Conclusions

- The practical security impact of Grover with existing techniques on plausible near-term quantum hardware is limited.
  - Bounding the length of time an adversary is prepared to wait introduces unavoidable overheads from parallelisation.
  - Error correction adds further overheads, but these are less significant.
  - Early post-quantum migration efforts should focus on traditional public-key algorithms.

Further Information

- *On the practical cost of Grover for AES key recovery*, Sarah D. and Peter C., NIST Fifth PQC Standardisation Conference

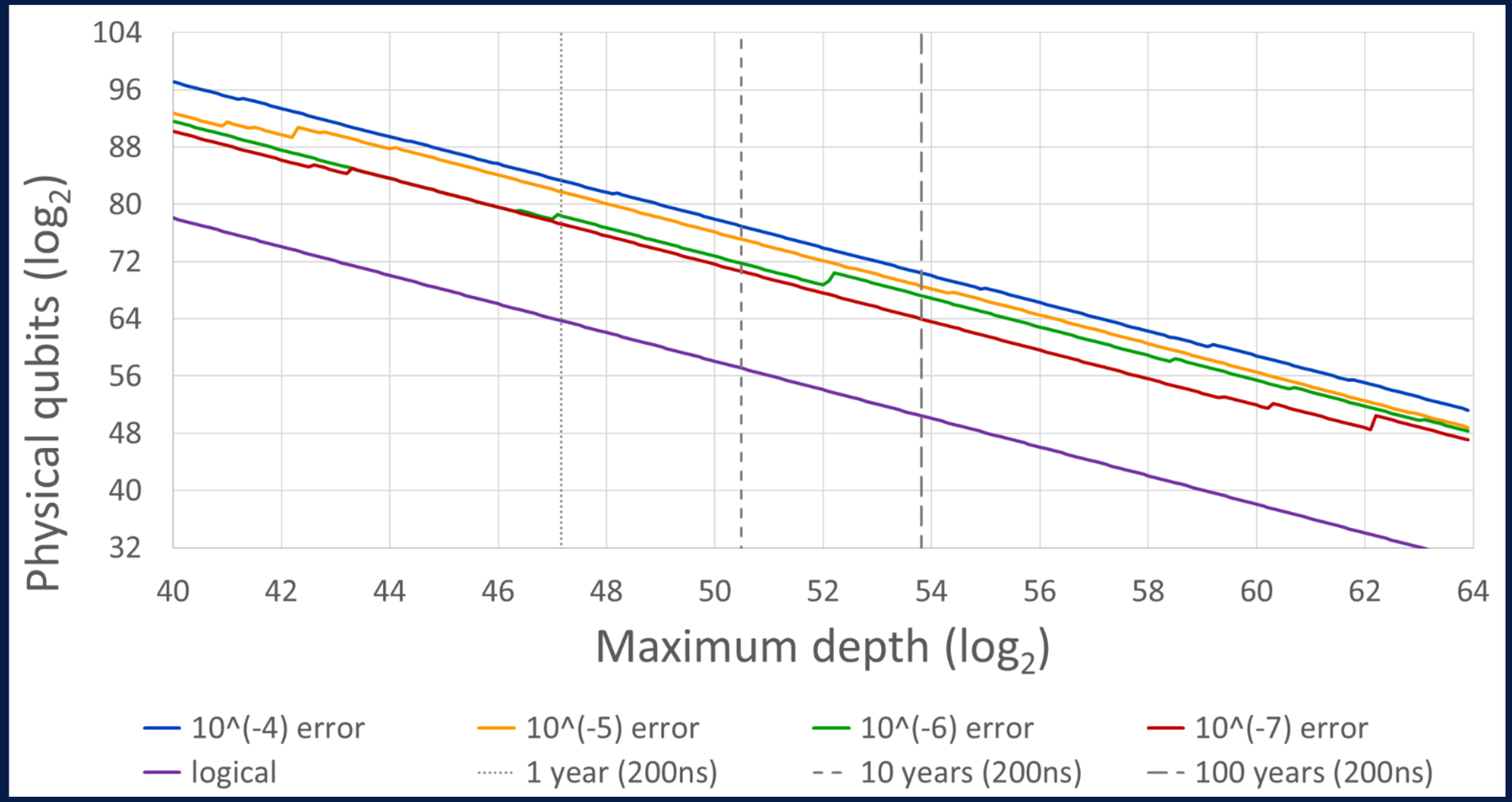
- Forthcoming ETSI QSC Report: ETSI TR 103 967
  - Other symmetric algorithms, including hash functions

National Cyber Security Centre

Thank you.

National Cyber Security Centre

AES-128: Physical qubits



National Cyber Security Centre

AES-128: Surface code cycles