National Cyber Security Centre

The UK National Cyber Security Centre's role in Post-Quantum Cryptography

Overview

- NCSC’s role and responsibilities
- Technical positions
- Current lines of work
- Migration challenges

NCSC’s role

- Authority within UK government for cyber-security and cryptography

NCSC's role

- Authority within UK government for cyber-security and cryptography
- Role is broadly *not* regulation or mandation

National Cyber Security Centre

NCSC's role

- Authority within UK government for cyber-security and cryptography
- Role is broadly *not* regulation or mandation
- We produce guidance and advice…

NCSC's role

- Authority within UK government for cyber-security and cryptography
- Role is broadly *not* regulation or mandation
- We produce guidance and advice…
- … and sometimes government standards

National Cyber Security Centre

NCSC's role

- Work primarily through sector groupings
- Also: incident response; skills development; and contribution of technical expertise to policy

National technical strategies

PQC is mentioned in a few places

- National Cyber Strategy
- Government Cyber Security Strategy
- National Quantum Strategy

Key technical positions

Motivation:

- Drive down overall cyber risk
- Follow secure-by-design principles

Key technical positions

Motivation:

- Drive down overall cyber risk
- Follow secure-by-design principles

Post-quantum cryptography has primarily been a topic for cryptographers.

In the future, it will primarily be an IT and OT problem.

National Cyber Security Centre

Key technical positions

- Standards are valuable, offering rigour and stability, and we are confident in recommending ML-KEM and ML-DSA for general use

National Cyber Security Centre

Key technical positions

- We're confident in the research underpinning NIST, and recommend ML-KEM and ML-DSA for general use
- Different users will have a range of needs from signature schemes – XMSS, LMS, SLH-DSA all have a place

Key technical positions

- We're confident in the research underpinning NIST, and recommend ML-KEM and ML-DSA for general use
- Different users will have a range of needs from signature schemes – XMSS, LMS, SLH-DSA all have a place
- Aim for PQC only end state – and bear that in mind if starting with PQC / traditional PKC in hybrid. Sometimes, that will mean doing things once, and well

National Cyber Security Centre

Key technical positions

- We're confident in the research underpinning NIST, and recommend ML-KEM and ML-DSA for general use

- Different users will have a range of needs from signature schemes – XMSS, LMS, SLH-DSA all have a place

- Aim for PQC only end state – and bear that in mind if starting with PQC / traditional PKC in hybrid. Sometimes, that will mean doing things once, and well

  (Similar arguments lead to our current lack of confidence in the utility of QKD as a general-purpose security technology)

Key technical positions

- Well planned discovery activities really matter – rushing migration will lead to bad cyber security outcomes

National Cyber Security Centre

Key technical positions

- Well planned discovery activities really matter – rushing migration will lead to bad cyber security outcomes
- Availability of well-implemented PQC is a necessary precursor to migration

National Cyber Security Centre

Key technical positions

- Well planned discovery activities really matter – rushing migration will lead to bad cyber security outcomes
- Migration timescales should be driven by availability of well-implemented PQC
- Plan migration as part of regular technical upgrades / refresh

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

National Cyber Security Centre

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

Costing Grover

Aim: set out a principled methodology for estimating overheads for Grover’s algorithm.

We consider 3 sources of overhead:

- Logical implementation
- Parallelisation
- Error correction

(https://csrc.nist.gov/csrc/media/Presentations/2024/practical-cost-of-grover-for-aes-key-recovery/images-media/sarah-practical-cost-grover-pqc2024.pdf)

Costing Grover – logical implementation

Quantum implementations of AES… different approaches optimise for different metrics.

Approach of Jang *et al.* (IACR 2022/683) minimises $(\text{circuit depth})^2$ x #qubits.

Costing Grover – Parallelisation

Current best performance for a single qubit cycle is around 200ns. That’s 1.78 years for a circuit of depth 2^{48}.

- Run parallel instances, with lower probability of success (or on a smaller part of the space)
- This increases #quantum processors and computational cost

Costing Grover – Error Correction

Focus on surface codes

- Exponentially suppress errors as code distance *d* increases
- Uses $2d^2 - 1$ physical qubits to produce one logical qubit

Overheads get higher as maximum circuit depth increases.

Costing Grover

Aim: set out a principled methodology for estimating overheads for Grover’s algorithm.

We consider 3 sources of overhead. For AES-128:

- Logical implementation: 31 bits
- Parallelisation: 8-32 bits (depending on maximum circuit depth)
- Error correction: 6-10 bits (depending on physical error rate)

Parallelisation and error correction overheads are negatively correlated.

Hybrid Terminology

Purpose: consistency and clarity of terminology across protocols, standards and organisations.

Defines, for example:

- Types of hybrid (composite, non-composite)
- Properties of hybrid (confidentiality, authentication, interoperability, backwards / forwards compatibility, *etc.*)
- Trade-offs

(https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/)

Deployment considerations for Hybrid KEMs

Draft Technical Report (multiple authors) within ETSI CYBER group.

Purpose: provide a framework for deciding whether / how to design and deploy hybrid KEMs, according to desired security and implementation considerations.

- Design considerations (security, efficiency, complexity)
- Deployment considerations (algorithm selection, key management, forward compatibility)
- Examples (with associated security notions)

National Cyber Security Centre

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

National Cyber
Security Centre

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

National Cyber Security Centre

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

National Cyber Security Centre

Lines of work

- Support to standards
- Regulators and regulated sectors
- Central government
- Defence
- Assurance / consultancy
- Guidance

Challenges in migration to PQC

- What’s the investment case?

Challenges in migration to PQC

- What’s the investment case?
- Legacy protocols, hardware

Challenges in migration to PQC

- What's the investment case?
- Legacy protocols, hardware
- Interoperability and complexity

Challenges in migration to PQC

- What's the investment case?
- Legacy protocols, hardware
- Interoperability and complexity
- Maintaining confidence in the face of academic advances

Challenges in migration to PQC

- What's the investment case?
- Legacy protocols, hardware.
- Interoperability, complexity, international differences
- Maintaining confidence in the face of academic advances.
- Maintaining confidence through claimed breaks

National Cyber Security Centre

Challenges in migration to PQC

- What's the investment case?
- Legacy protocols, hardware
- Interoperability and complexity
- Maintaining confidence in the face of academic advances
- Maintaining confidence through claimed breaks
- Engineering for agility, and cryptography as risk management

National Cyber Security Centre

Key messages

- Focus on discovery activities
- Build trust in implementations (primitives and protocols)
- Plan migration activities like any complex IT / OT programme