Quantum safe cryptography: the big picture summary.

YOU ARE HERE

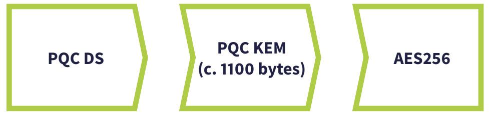
1. Current internet security

RSA2048
ECDH256
AES128

Cons:
- Currently threatened
- Data intercepted today can be decrypted in the future

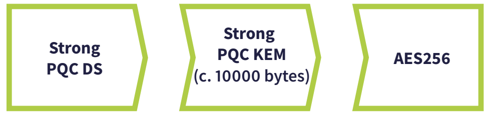
BROKEN

2. Future all-maths based 'streamlined' PQC for the Internet



Cons:
- Long-term security rests on sufficiently streamlined PQC KEM protocols

3. Future all-maths based high security PQC for critical applications



Cons:
- Long-term security rests on sufficiently streamlined PQC KEM protocols
- Significantly larger key sizes and processing overheads.

NOT FUTURE-PROOF

4. Fully in-band enhanced security using PQC/QKD

Strong PQC DS
QKD
AES256

Pros:
- QKD cannot be intercepted or stored for future attack
- Relies on PQC DS in real-time during initial authentication.

Cons:
- Long term security rests on AES.
- Stream ciphers can't match this use case as they need out-of-band delivery of an initial key

5. Fully in-band 'conditional' perfect security

Strong PQC DS
QKD
OTP

Pros:
- OTP allows for perfect secrecy.
- Removes all long-term dependence on computational hardness assumptions.

Cons:
- Low key-rates
- For low-volume users

6. Information-theoretic security

ITS DS
QKD
OTP

Pros:
- Stiff competition vs 'out-of-band' solutions

Cons:
- Requires initial pre-shared key.
- Low key-rates
- For low-volume users

★ SECURE BUT LIMITING

Quantropi QEEP™-KD can replace QKD for Key Agreement

- QKD makes the key agreement unmeasurable — untouchable.
- QEEP™-KD makes the key agreement uninterpretable — can be intercepted but all possible interpretations are equally likely.
- Works with existing network infrastructure, no need to deploy dark fibre.
- Can achieve transmission rates of up to 1 GBit/s.

7. Fully in-band enhanced security using PQC/QEEP™-KD

Strong PQC DS
QEEP™-KD
AES256

Pros:
- QEEP-KD™ is extension of Shannon Perfect Secrecy in Hilbert Space.
- Can be intercepted but message is uninterpretable.
- High-key rates.

Cons:
- Long term security rests on AES.

8. Fully in-band 'conditional' perfect security

Strong PQC DS
QEEP™-KD
OTP

Pros:
- Removes all long-term dependence on computational hardness assumptions.
- High-key rates. Can be employed by high volume users.

Cons:
- Significantly larger key sizes and processing overheads.

9. Information-theoretic security

ITS DS
QEEP™-KD
OTP

Pros:
- High-key rates. Can be employed by high volume users

Cons:
- Requires initial pre-shared key (e.g. baked in during manufacturing of device).

★ ★ SECURE, BUT WITH SOME CONSTRAINTS

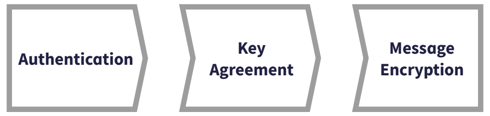
WE ARE HERE

10. Quantropi End-To-End Solution

GPK
QEEP™-KD
CipherSpace™

Pros:
- High-key rates. Can be employed by high volume users
- No pre-shared key is required

★ ★ ★ SECURE AND FAST



Red
Threatened now

Light green
Considered secure for most applications

Green
Information theoretically secure

Not secure / secure

Ease of set-up/ maintenance

High / low power use

Speed

Processing bottleneck: low transmission rates, range, and extra infrastructure required

PQC	Post-quantum cryptography
DS	Digital signature
KEM	Key encapsulation mechanism
OTP	One-time pad
QKD	Quantum key distribution
ITS	Information-theoretic secure
GPK	Galois Public Key

BASED ON A CHART BY MICHELE MOSCA.

Bring it on.

quantropi.com