Terminology for Post-Quantum Traditional Hybrid Schemes

draft-driscoll-pqt-hybrid-terminology

PQUIP – IETF 116 – 31st March 2023
Context

- IETF protocols will need to be updated to permit use of post-quantum asymmetric algorithms.
- During the algorithm transition period there may be a desire for protocols which use both post-quantum and traditional algorithms, so called “hybrids”.
- Terminology for this topic is a challenge so we proposed an informational draft at SECDISPATCH at IETF 114.
- Adoption of a draft on hybrid terminology is a milestone for PQUIP.
- -02 version posted in March 2023.
Proposal

• An informational draft to standardise a glossary for Post-Quantum Traditional Hybrids.

• Aims:
  • Ensure consistency across different protocols, standards and organisations.
  • Make it clear what security properties a particular hybrid construction claims.
  • Enable easier comparison of solutions.
Content

• Primitives
  • Types of algorithms (Traditional, Post-Quantum)
  • Abstract use of algorithms in schemes
  • Post-Quantum Traditional (PQ/T) Hybrid Schemes (KEM, PKE, Signature)

• Cryptographic Elements
  • Component and Composite Cryptographic Elements, Combiners

• Protocols
  • PQ/T Hybrid Protocol
  • Composite and Non-Composite PQ/T Hybrid Protocols

• Functionality
  • Hybrid Confidentiality, Hybrid Authentication, Hybrid Interoperability

• Certificates
  • PQ/T Hybrid Certificates
  • Types of certificate chain

• Algorithm Specification
Next Steps

- Does this language work for the PQ/T hybrid schemes and protocols being developed?

- What are we missing?

- Is this ready for adoption by PQUIP?

- If not – what changes would you like to see?
Thanks

florence.d@ncsc.gov.uk
https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology/
What do we call the algorithm types?
(Bonus Slide)

Traditional Algorithm: An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms or elliptic curve discrete logarithms.

Post-Quantum Algorithm: An asymmetric cryptographic algorithm that is believed to be secure against attacks using quantum computers as well as classical computers.
Post-Quantum Algorithms
(Bonus Slide)

• Alternatives:
  • Quantum-safe
  • Quantum-resistant

• Reasons for choosing Post-Quantum
  • Currently the most widely used term.
  • Quantum-safe and quantum-resistant both suggest properties of the achieved security of the algorithms, rather than the security goals.
  • Quantum-safe has previously been used to include both PQC and QKD (e.g. by ETSI).
  • Fits with the name of this group!
Traditional Algorithms (Bonus Slide)

• Alternatives:
  • Classical
  • Discrete-log-or-integer-factorisation-based (or similar)
  • Conventional
  • Pre-Quantum
  • Vintage

• Reasons for choosing Traditional
  • Doesn’t begin with a “C” or “PQ” so can form a helpful and non-confusing acronym.
  • Classical describes a type of computer, and PQ algorithms are run on classical computers.
  • Not too long.
  • Doesn’t suggest that these types of algorithm are already insecure (before the existence of a CRQC).