Open discussions

- **Moderator: Hao Qin,** National University of Singapore (NUS), Singapore

- Workshop speakers & Invited & On site audiences

QKD protocol & Theoretical security

❑QKD protocol

- Information theoretic security - Independent of computation resources, quantum safe
- Unique security feature
- Security notions, finite size, epsilon security
- Security model, proof & framework

❑Standardization/Certification

- Protocol framework
- Security proof <> Challenging?
- Specific QKD protocols <> Challenging?
- Certified QKD protocol & product?

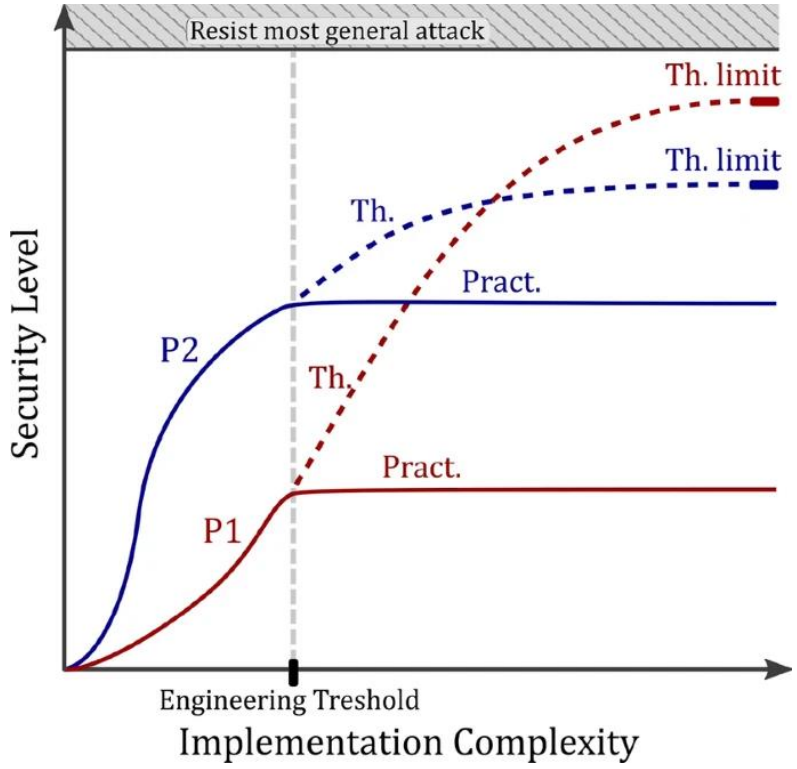
QKD module & Practical security

❑QKD module

- Implementation security
- Gap between models and devices
- Quantum hacking attacks
- Research activities
- Countermeasures

❑Standardization/Certification

- Need QKD protocol standards?
- Security requirements & measures
- Common criteria approach
- All security loopholes? <> practicality & challenging?
- Certified QKD product?
- QKDN <> additional protection & consideration?



Experimental vulnerability analysis of QKD based on attack ratings. Sci Rep 11, 9564 (2021)

Time line

❑Quantum key distribution (QKD)

- First QKD protocol invented by Charles Bennet and Gilles Brassard in 1984 (BB84)
- QKD & QKDN related standards: ETSI~2008, ITU-T~2018, ISO/IEC~2017
- Today is Nov 8 2022, time line for the first QKD protocol/framework standard? First certified QKD product? First certified QKDN?

❑Post quantum cryptography (PQC)

- Initiated in 2016, NIST 4th round 2022, Draft standards available 2022/2024*
- ETSI Cyber QSC (Created in 2014)

❑Cryptographic protocols

- RSA (1977), X.509(1988), RFC8017 (2016)
- DES (1977), AES(2001), ISO/IEC 10833-3(2005 -> 2010)

❑Optical communication protocols

- Trace back to radio frequency, SG 15 over decades, G series…

*https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Summary

- QKD protocols that implemented on QKD modules are the core of quantum layer in QKDN, but QKD protocol standards are missing
- QKD protocol standardization will need include various security topics
- Importance to standardize QKD protocols for different purposes: definition, confidence, certification, interoperability
- QKD protocols standardization (a high level framework) provides an understanding of the basic requirements of a QKD protocol
- Certified QKD products help wider adoptions of QKD technologies to end users
- Level-up the playing field for suppliers of QKD solutions to provide certified products/services with a certain recognised quality