Quantum Information in Security Protocols

Sebastian Verschoor

David R. Cheriton School of Computer Science
University of Waterloo

September 20th, 2021

Acknowledgement

Committee:

- Harry Buhrman
- Ian Goldberg
- Douglas Stebila
- John Watrous

Supervisor:

- Michele Mosca

Introduction

- Information security is the goal
- Cryptography captures part of that goal formally
  - Operates in a security model
    - A mathematical abstraction of the real world
  - Inductive reasoning tests validity of the model
  - Operates under assumptions (many implicit)
- Many breaches of security occur by bypassing the model

Quantum information

- Constructive: No-cloning theorem
  - Quantum key distribution (QKD)
- Destructive: Faster cryptanalysis
  - Shor's algorithm
  - Grover's algorithm

Quantum Information is notorious for being unintuitive, increasing the reliance on mathematics for assessing security.

Thesis Statement

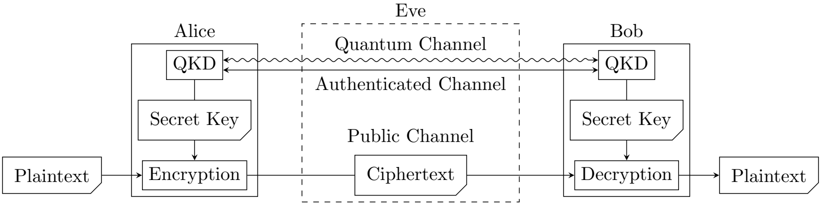
Information security in the context of quantum information has a strong dependency on mathematical definitions of security, yet sound engineering practices remain unavoidable in order to construct meaningfully secure cryptographic protocols.

Main contributions

1. Preventing key exhaustion in QKD
2. Terrorist fraud on quantum distance bounding
3. Key authentication from post-quantum KEMs

1. Preventing key exhaustion in QKD

Key exhaustion in QKD



- Classical post-processing of quantum communication
  - output is either an ITS key or abort
- Authenticated channels are realized by ITS MACs
  - a MAC tag is a universal hash + **one-time** pad
  - part of the shared key must be discarded
- Consumed key is replaced with fresh QKD output
  - but what if QKD aborts?

Key exhaustion in QKD

- Key exhaustion is achieved by
  - Noise on quantum channel
  - Tampering with post-processing
- Impact is more severe than common Denial-of-Service
  - abort all communication; or
  - recover (lowering security of future sessions)
- Applies to almost all practically deployed systems[1]

[1] at least the ones that are specified in sufficient detail

Preventing key exhaustion

UNIVERSITY OF WATERLOO

Solution:

- Computational authentication of each message
- ITS authentication of the transcript
  - resulting QKD output is ITS confidential and authenticated
- Simple implementation leads to desynchronization

I propose two solutions for preventing desynchronization

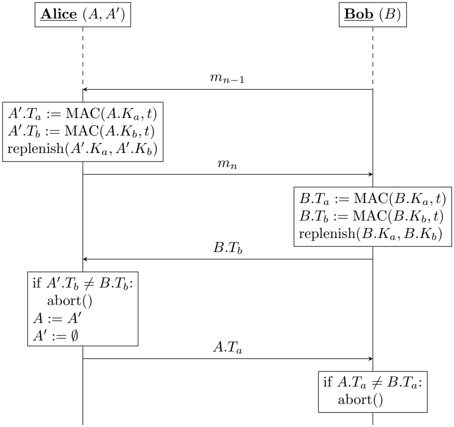
Preventing key-exhaustion

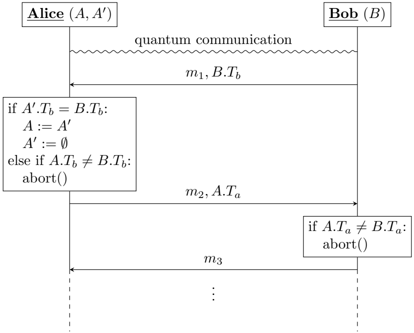
1. Decoy-based solution
   - Hide **when** the real ITS authentication is being done
     - N shared keys, of which ℓ may already be consumed
     - shared QKD output is already computationally authenticated
     - sample number of decoy rounds (d) from ℓ bits of QKD output
     - first send d decoy tags (with comp. auth.)
     - then send the two real ITS tags (with comp. auth.)
   - Adversary consumes one or two keys by blocking a real tag
     - block early tag: probably no key was consumed
     - block late tag: probably real tag was missed
     - block last tag is “optimal”
   - Exponentially many sessions must be attacked until all keys are exhausted

Preventing key-exhaustion

2. Ratchet-based solution
   - MAC key is only exhausted once the MAC tag is *sent*
     - not when the tag is *computed*

Preventing key-exhaustion



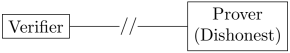


2. Terrorist fraud in quantum distance bounding
   - Many scenario's require authenticity of identity *and location*
     - Secure building access
     - Keyless car entry
     - Contactless payments
   - Solution: distance bounding protocols
   - Much DB literature is in an informal framework

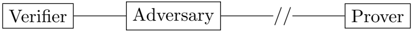
I demonstrate attacks on all (three) existing quantum distance bounding protocols

Distance Bounding

Distance Fraud:

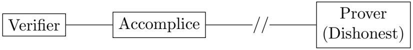


Mafia Fraud:



- Timed challenge-response protocol
  - generate ephemeral key from shared long-term key k
    - keyed hash function over public nonces
  - many single bit challenges (c_i) and responses (r_i)
  - time-of-flight gives upper bound on distance
  - (sometimes) concluded by a verification phase

Terrorist fraud



- Prover can assist the accomplice to fool the verifier
  - but cannot give long-term key k to the accomplice
- Classical countermeasure: two ephemeral keys
  - $d = g_k(N_v, N_p)$
  - $b = \text{Encrypt}_d(k)$
  - correct responses depend on both d and b

Quantum distance bounding

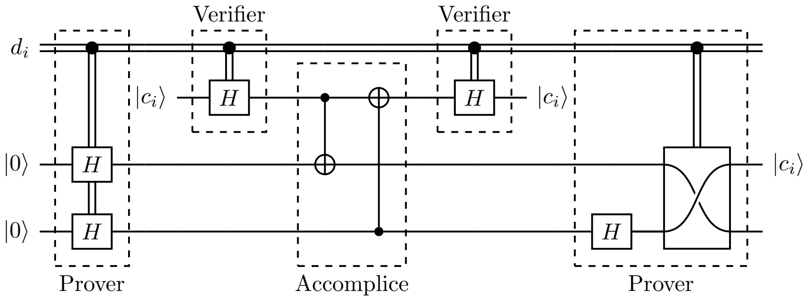
- Three QDB protocols exist
- Send qubits instead of bits in the rapid phase
  - challenge $|\phi_i\rangle$
  - response $|\psi_i\rangle$
- For all three protocols I show that
  - TF countermeasure with $b = d \oplus k$: leaks the key k
  - TF countermeasure with $b = \mathrm{AES}_d(k)$: does not prevent TF
  - no TF countermeasure: existing analysis is flawed

AMSP protocol

- The AMSP protocol [Abi+17]
  - first half: $|\phi_i\rangle = |\psi_i\rangle = H^{d_i}|c_i\rangle$
  - second half: $|\phi_{i+n}\rangle = |\psi_{i+n}\rangle = H^{b_i}|c_{i+n}\rangle$
  - prover concludes by sending $MAC_k(c)$
    - prevents simple reflection
- Extracting k from the prover (when $b = d \oplus k$)
  - send $|\phi_i\rangle = |0\rangle$
  - let x be the measurement outcome of $|\psi_i\rangle$
  - if $x \neq 0$, then $d_i = 1$
  - if both d_i and b_i leak in this manner, then k_i leaks
  - otherwise you have still gained partial information about k_i
    - use that to attack subsequent rounds more effectively
    - attacking 16 rounds extracts a full 128-bit key

AMSP protocol

- Terrorist fraud ($b = \mathsf{AES}_d(k)$)
- Blind cloning



Key authentication from post-quantum KEMs

3. Key authentication from PQ KEMs
   - Secure messaging
     - Success (also) depends on usabilty and adoptability of solutions
     - Reduced usability leads to lower security

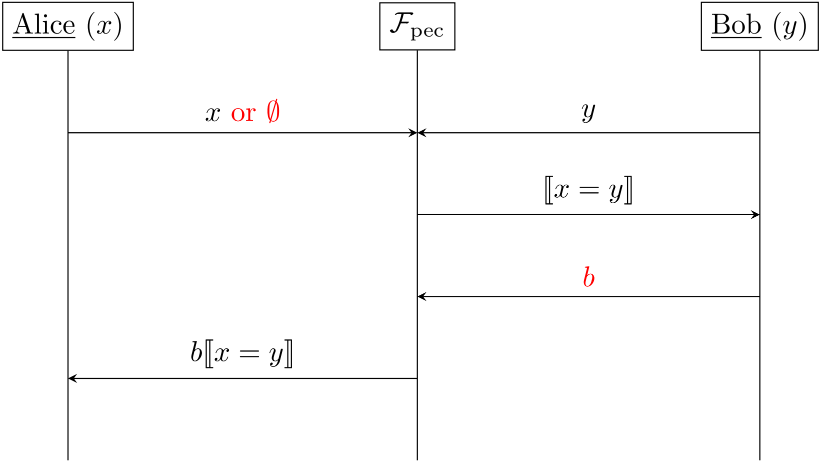
Key authentication

- Secure messaging
  - Initial key exchange between public keys
  - Key authentication “binds” those keys to the intended users
- Many existing solutions
  - Manual fingerprint verification: usability problems
  - Secret-based zero-knowledge verification
    - in-band, intuitive
    - Socialist Millionaire Protocol [BST01]
    - implemented in Off-the-Record [AG07]
    - based on Diffie-Hellman: not post-quantum
- I give a post-quantum replacement for the SMP in the context of key authentication

Private equality confirmation

- Alice and Bob share a (low-entropy) secret *pwd*
- Alice and Bob have set up an OTR channel using pk_A and pk_B
- Alice computes input $x = Hash(pk_A, pk_B, ssid, pwd)$
- Bob computes input $y = Hash(pk_A, pk_B, ssid, pwd)$
- The run the protocol to check if $x = y$ in *zero-knowledge*
  - but malicious parties are allow to slightly alter the functionality

Private equality confirmation



Protocol

- Inputs $x = x_1 x_2 \ldots x_n$ (Alice) and $y = y_1 y_2 \ldots y_n$ (Bob)
  - Run n OT's (Alice $\to$ Bob):
    - $((A_i[0], A_i[1]), y_i) \mapsto (\emptyset, A_i[y_i])$
  - Let $\alpha(x) = A_1[x_1] \oplus \cdots \oplus A_n[x_n]$
    - Alice knows $\alpha(\cdot)$, Bob learns $\alpha(y)$.
  - Run n OT's (Bob $\to$ Alice)
    - They learn $\beta(x)$ and $\beta(\cdot)$
  - Alice sends $G(\alpha(x)) \oplus \beta(x)$
  - Bob rejects or replies $\alpha(y) \oplus \beta(y)$
- Use an existing PQ OT protocol [MR21]
  - Built from (PQ) Key Encapsulation Mechanisms (KEMs)
  - UC-secure in the ROM

Security argument

- SUC-secure in the OT-hybrid model
  - $\Rightarrow$ UC-secure in the ROM
  - G should be pseudorandom and one-way
- Security argument follows the structure of a simple hybrid argument
  - $\Rightarrow$ can be lifted to post-quantum security
  - OT must be UC post-quantum secure
  - G must be PQ pseudorandom and PQ one-way

Implementation

2-RTT protocol

- Hybrid KEM
  - Kyber (Round3 CCA, NIST PQC lvl 5)
  - ECDH (Ed448 Goldilocks, Decaf)
- C99 ($\sim$2000 LoC)
- Side-channel protection

Benchmarks (80-bit inputs)

- Message size
  - 254 KiB, 508 KiB, 254 KiB, 32 B
- Speed
  - 22 ms, 114 ms, 106 ms, 15 ms

Conclusion

- A formal approach to cryptography is fundamental for security
- Sound engineering is required to narrow the gap between theory and practice
- Quantum information impacts both of these aspects of security

I have demonstrated

1. How to authenticate post-processing in QKD
2. How informal classical arguments are inadequate for quantum security (in distance bounding)
3. How to build in-band PQ key authentication

Thank you

[Abi+17] Aysajan Abidin et al. "Towards Quantum Distance Bounding Protocols". In: *Radio Frequency Identification and IoT Security 2016*. Ed. by Gerhard P. Hancke and Konstantinos Markantonakis. Cham: Springer International Publishing, 2017, pp. 151–162. ISBN: 978-3-319-62024-4. DOI: 10.1007/978-3-319-62024-4_11.

[AG07] Chris Alexander and Ian Goldberg. "Improved User Authentication in Off-the-Record Messaging". In: *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*. WPES '07. Alexandria, Virginia, USA: Association for Computing Machinery, Oct. 2007, pp. 41–47. ISBN: 9781595938831. DOI: 10.1145/1314333.1314340.

[BST01] Fabrice Boudot, Berry Schoenmakers, and Jacques Traoré. "A fair and efficient solution to the socialist millionaires' problem". In: *Discrete Applied Mathematics* 111.1 (2001). Coding and Cryptology, pp. 23–36. ISSN: 0166-218X. DOI: 10.1016/S0166-218X(00)00342-5.

[MR21] Daniel Masny and Peter Rindal. *Endemic Oblivious Transfer*. July 2021. iacr: 2019/706.