Enhancements to Prepare and Measure QKD

Peter Y A Ryan
Université du Luxembourg

Quantum Key Distribution

- Relies on principles of quantum mechanics rather than computationally hard problems.
- Heisenberg, no-cloning etc.
- Eavesdropping is detectable.
- Aims for unconditional secrecy.
- Literature often rather vague about how and when authentication is performed.

Authenticated Key Establishment

- Fundamental lesson from analysis of classical AKEs: key establishment and authentication must be inextricably intertwined.
- So, for example, the session key is constructed as a function of the ephemeral and long-term randoms.
- In QKD we have two quite distinct phases: quantum (KE) and classical (Authentication etc.)
- Not clear how these are intertwined.

QM Elements

- Measuring a quantum state causes it to “collapse” probabilistically into one of the Eigenstates of the the measurement operator.
- Coding convention.
- Operational semantics.

BB'84

- Work with states of circular polarization of photons.
- Sender uses four non-orthogonal states: 0° (↕) [0], 45° (↙) [0], 90° (↔) [1] and 135° (↘) [1].
- Receiver uses two possible measurement bases: vertical/horizontal (⊕), diagonal (⊗).
- Assume Anne and Bob share an prior secret string s as a basis for authentication.

Operational semantics

- $\oplus|\updownarrow\rangle \Rightarrow \updownarrow$
- $\oplus|\nearrow\rangle \Rightarrow \updownarrow \; or_{0.5} \; \leftrightarrow$
- etc....
- In essence: if you use the “correct” basis you get the correct result, if you use the wrong basis you get random result.

Quantum Phase

- Anne sends a stream of photons each polarized in one of the four states, chosen at random. She records the state of each.
- We assume that they have a way to consistently label each photon with an index. Call the indexing set I.
- For each photon Bob measures the polarization with one of the two bases, chosen at random. He records the basis and the outcome.

Key Sifting

- Key sifting: for roughly half the photons, Bob will have chosen the "correct" basis. For these photons, in the absence of noise or eavesdropping, they should agree on the encoded bits.
- They establish the indices of the photons in this set by open discussion. Call this set (of indices) I_1.
- Note: Yves may learnt this information too.

Eavesdropping Detection

- Detection of eavesdropping: now they need to detect if they have been any eavesdropping on the quantum channel.
- They agree a randomly selected subset of I1, that we will denote I2, on which they will compare bits.
- Again, this agreement is performed over open channels (possibly authenticated).
- If the QER is sufficiently low they proceed, else abort.

Key Reconciliation

- Information reconciliation: they now work with I3:=I1/I2. For these indices Anne and Bob should have approximately the same, secret bits.
- They need to eliminate any discrepancy between these strings. Typically done using a “cascade” protocol: comparing the parity of randomly chosen blocks.

Secrecy Amplification

- Secrecy amplification: after phase 3 they should have exactly matching strings, but Yves may have learnt some information about this string from eavesdropping on phase 3 and possibly some "below the radar" eavesdropping on the quantum channel.
- To reduce Yves' information to a negligible level they execute a secrecy amplification algorithm: distill the string to a shorter one, k, with "purer" entropy from Yves' point of view.

Key Confirmation

- Key confirmation: they can exchange hashes of the session key k, keyed with parts of s.
- At a minimum, this provides mutual authentication.
- They should now have a secret, shared key string, which can be used either in OTP mode or in a block or stream cipher-but of course the latter sacrifices unconditional secrecy.

Discussion

- How authentication of performed is typically vague and often inconsistent across publications.
- Apparently sound proofs of the quantum phase, followed by an argument that authentication is dealt with using unconditional MACs, e.g. Carter-Wegman style.
- But we know that we have to be very careful to "intertwine" the key establishment and the authentication.

The new twist

- Rather than agreeing the eavesdropping index set I2 in the clear, we arrange for Anne and Bob to calculate it based on part of the *s* string, and possibly some additional fresh entropy.
- They then communicate the corresponding bits the detect eavesdropping.
- Note: provides implicit authentication

Countering MPC attacks

- This enhancement also seems, inter alia, to provide a counter to the Multiple Photon Counter attack.
- Seems more efficient that the SARG protocol, that has a lower bite rate: has the throw away 75% of bits.

Discussion

- Key establishment and authentication are closely intertwined, with explicit authentication early on.
- Analysis: the first enhancement can be reduced to the conventional approach.

Twist 2

- Note that we now reveal the bits of the I2 sequence, but Yves should not learn where they lie in I.
- So, potential to increase the bit rate by using bits from the I1 set-but great care needed:
  - need more ferocious distillation
  - possible forward secrecy implications.

A further twist...?

- Rather than choosing the bases at random, Anne and Bob use a PRNG seeded with part of the s string (plus perhaps some freshly generated and exchanged entropy).
- Is this secure? Proofs will certainly be harder.
- Note: Yves' measurements will not reveal any info about the bases.

Twist 3

- Analysis: the key threat seems to be Yves making measurements early in the Q phase and deriving information about the PR stream, and predicting later values.
- But measurements on the photons seems to leak nothing about the choice of preparation/ measurement bases.

Conclusions

- An enhancement to QKD that leads to deeper "entanglement" of key establishment and authentication.
- Early authentication.
- Leaks less info and results in higher bit rates.
- Need full analysis covering both the classical and quantum phases, or maybe tighter composition arguments.