Security of quantum key distribution with bit and basis dependent detector flaws*

Lars Lydersen and Johannes Skaar

Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

Detector efficiency mismatch

• The two bit values are detected with different probability.

• Eve may control timing => only selected bit value can be detected.
• Eve can compromise security with this loophole [1,2,3].

Detector efficiency curves measured on a commercial QKD-system [3]

Let \( \eta \) be the smallest ratio of the two detector efficiencies. (\( \eta \approx 0.2 \)).

There exists an attack which compromises security in QKD-systems with \( \eta < 0.25 \).*

Detector efficiency mismatch

Security analysis

Sketch of the security proof:

• In Koashi’s framework [4-5] for security proofs the secure key rate is found from the entropic uncertainty relation.

\[
R \geq [1-h(E)]-H_X,
\]

\( R \): Secure key generation rate in Z basis
\( h(\cdot) \): binary Shannon entropy function
\( E \): measured QBER in Z basis
\( H_X \): Bob’s entropic uncertainty per bit about a virtual X measurement at Alice.

• Receiver/channel/detector model: Basis dependent, possibly lossy, linear optical network followed by perfect detectors.
• Any linear optical operator acting on the photonic modes may be written \( U_Z F_Z V_Z \) (by svd).

\[
E_{\text{measured}} \leq \frac{1}{2} \left( \sum_{i=1}^{n} \max \left\{ \eta_i, 1 \right\} - 1 \right)
\]

\( \max \left\{ \eta_i, 1 \right\} \) is an array of beamsplitters describing the limited detection efficiency. \( \eta_i \) labels the optical modes (e.g. temporal modes).

\( U_Z, V_Z \) are unitary operators (mode mixing).

• Bob makes virtual X measurement

\[
E_{\text{measured}} \leq \frac{1}{2} \max \left\{ \sum_{i=1}^{n} \max \left\{ \eta_i, 1 \right\}, 1 \right\}.
\]

where \( F_Z F_Z^* = \sum_{i=1}^{n} \sum_{j=1}^{n} \eta_{ij} [n_Z(t_i, t_j)] \). The sum \( \eta \) is the minimum over all temporal modes.

• Equivalent to

\[
E_{\text{measured}} \leq \frac{1}{2} \sum_{i=1}^{n} \max \left\{ \eta_i, 1 \right\}.
\]

• Bob’s entropic uncertainty about Alice’s N bits is

\[
H_X N = N - \eta N [1-h(E^*)].
\]

where \( E^* \) is the QBER in the virtual measurement.

• \( E^* \) can be bounded from the measured \( E \) as \( E^* \leq E / \eta \).


Security bounds in terms of zero secret key rate (\( R=0 \)).

Improved bound for systems with four-state Bob.

Dashed line: The best known attack.

NTNU
Norwegian University of Science and Technology

Conclusion

The security proof covers the security of BB84 in the presence of any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver/detectors including any combination and basis dependence of:

• detector efficiency mismatch, mode-dependent detection efficiencies,
• multiple reflections, misalignments, losses,
• polarization mode dispersion, polarization dependent losses,

More general than previous proofs [6].