Phase-encoded BB84 experiments have unbalanced signal amplitudes due to loss in phase modulators.

Ref. [1, 2] turn the security proof into a standard BB84 proof using decoy states, signal tagging, and the qubit squashing model [3].

The qubit approach pessimistically assumes that Eve has full access to the information carried by multiphoton signals.

Our key rates are higher than [2]'s mainly in low-loss regime due to improved analysis and a higher tagged threshold photon number.

Here, our different proof technique achieves higher key rates.

**Protocol Description**

![Diagram of the phase-encoded BB84 protocol with unbalanced signal intensities.](image)

Alice’s output: $\sigma_x = (\frac{1}{2})^{1/2} (|\psi^0(\alpha)\rangle + |\psi^0(-\alpha)\rangle) = \sqrt{\alpha} e^{i\theta \sigma_x}$, $\sigma_y = (\frac{1}{2})^{1/2} (|\psi^0(\alpha)\rangle - |\psi^0(-\alpha)\rangle) = \sqrt{\alpha} e^{i\theta \sigma_y}$.

Phases: $\phi_x \in \{0, \frac{\pi}{2}, \frac{\pi}{4}, \frac{3\pi}{4}, \frac{\pi}{2}\}$, $\phi_y \in \{0, \frac{\pi}{2}\}$ (equally probable).

**Methods**

Differences between our approach and Refs. [1, 2]'s:

- We apply the numerical analysis formulated in [4] to obtain reliable lower bounds on the key rates.
- Source tag: tag the photon number of the signals and extend our analysis to a higher tagged threshold photon number.

\[
\rho \rightarrow \text{QND} \rightarrow \Lambda \rightarrow \{k\} \langle k | \langle k |
\]

\[ P_{\alpha, n \leq N_\alpha} + P_{\alpha, n > N_\alpha} = |k\rangle \langle k | \]

To avoid extra qubit errors from the qubit squashing model:

- Lower bound for $p(n \leq N_\alpha) = \text{Tr}(\rho_{\alpha, n \leq N_\alpha})$ preserve entanglement
- Preserve some parts of the multi-photon generated private information

Summary of technical details:

- Lower bound $p(n \leq N_\alpha)$ with Markov’s inequality + cross-click probability
- Infinite decoy + Eve’s QND photon counting + signal tagging
- Decomposition of privacy amplification (PA) term in key rate formula

\[
R_\infty \geq p_{\text{pass}} \min \sum_{\alpha=1}^{\alpha=2} D(\rho_{\alpha, n \leq N_\alpha}) - p_{\text{pass}} \frac{\alpha}{2} 2 E C
\]

- Each PA term independent of signal intensity $\alpha$ easy to optimise over

**Simulation**

- Loss-only channel + detection inefficiency $\alpha$ transmissivity $\eta$
- Two alternative loss scenarios:
  - Trusted loss: detector efficiency $\eta_{\text{det}}$
  - Untrusted loss: detector efficiency $\eta_{\text{det}} = 1$ (i.e. all loss due to Eve)

- Dark counts classical post-processing map
- Two alternative noise scenarios:
  - Trusted noise: each detector has the same dark count rate $p_d$
  - Untrusted noise: assume Bob’s detectors “dark count free” (i.e. Eve causes the dark counts)

\[ \Rightarrow \text{may lead to unphysical constraints} \]

\[ \Rightarrow \text{no replacement model for noise} \]

**Results**

- Parameters: Alice’s tagged photon number cutoff $N_\alpha = 3$, Bob’s flag-state photon number cutoff $N_\beta = 4$, $p_d = 8.5 \times 10^{-7}$, $f_{EC} = 1.22$

**Observation**

- Key rates increase with higher trusted loss ratio $\frac{f_{\text{Max}}}{f_{EC}}$.

\[ \Rightarrow \text{Discover untrusted noise may lead to unphysical constraints} \]

**Conclusion**

- New security proof:
  - Higher key rates than [2]'s in low-loss regime
  - Discover untrusted noise may lead to unphysical constraints
  - Explored trusted loss scenario (not allowed in [1, 2]'s proof)

**References**


Financial support for this work has been partially provided by Huawei Technologies Canada Co., Ltd.