Twin-field QKD with discrete phase randomisation

Guillermo Currás Lorenzo, Lewis Wooltorton, and Mohsen Razavi
School of Electronic and Electrical Engineering, University of Leeds
Leeds, United Kingdom

**Twin-Field QKD**
- Twin-field QKD offers improved key-rate scaling with channel loss, opening the way for distance records.
- Continuous phase randomisation (CPR)
  - Key assumption of the decoy state method: the phase is randomised continuously and uniformly.
  - However, this is hard to achieve in practice!
  - Two methods: Passive randomisation. Turning the laser on and off. But there are correlations between one pulse and the next.
  - Active randomisation: Using a phase modulator. But this approach randomised over a discrete set.
  - Both methods may have security loopholes...

**BB84 with DPR**
- The security of decoy-state BB84 with discrete phase randomisation (DPR) has been considered in [Cao14].
- There, the authors show that a DPR coherent state can be decomposed as

\[ \sum_{n=0}^{M-1} \sqrt{\mu_n} |\tilde{\mu}_n^r \rangle \langle \tilde{\mu}_n | = \sum_{n=0}^{M-1} \sqrt{\mu_n} |\tilde{\mu}_n^l \rangle \langle \tilde{\mu}_n | = \sum_{n=0}^{M-1} \sqrt{\mu_n} |\lambda_n \rangle \langle \lambda_n | \]

where the states $|\lambda_n \rangle$ have a small dependency on $\mu$. The yield probabilities for two states arising from different intensities can be bounded by the trace distance bound

\[ |n_m^n - n_l^n| \leq \sqrt{1 - (|\lambda_n^l| |\lambda_n^r|)^2} \]

- Thanks to this, the security of the protocol can be proved, in combination with linear programming techniques.
- Results show that the performance is close to CPR with only ten random phases.

**TF-QKD with DPR**
- Using similar ideas, we propose a TF-QKD variant that relies exclusively on discrete phase randomisation.
- It has a similar setup as in [Curty19], but the phase of test mode emissions is randomised discretely rather than continuously.
- Because of DPR, it is very difficult to find an analytical expression for the phase-error rate.

**Numerical security analysis**
- The linear programming approach of [Cao14] doesn’t work well here.
- Instead, we express a bound on the phase-error rate as the solution of a semidefinite program (SDP), where the constraints use the data from the test mode emissions.
- For this, we modify the approach proposed in [Primaatmaja, 19], which can prove the security of any discretely modulated MDI-QKD type protocol using semidefinite programming.
- In principle, their results should be directly applicable here. However, the number of constraints is $O(n^3)$, where $n$ is the number of pure states sent by each user. The large number of states sent here makes this approach unfeasible.
- Instead, we use a far smaller number of constraints, mostly based on the trace distance bound.

**Conclusions**
- Most TF-QKD variants rely on the emission of laser pulses with a continuous random phase, which is difficult to achieve in practice.
- We propose a TF-QKD variant that relies on discrete phase randomisation.
- The use of discrete randomisation allows to perform a test mode phase post-selection.
- Because of this, our proposal obtains higher secret key rates than a similar protocol based on continuous randomisation.

**References**