Twin field QKD with discrete phase randomisation

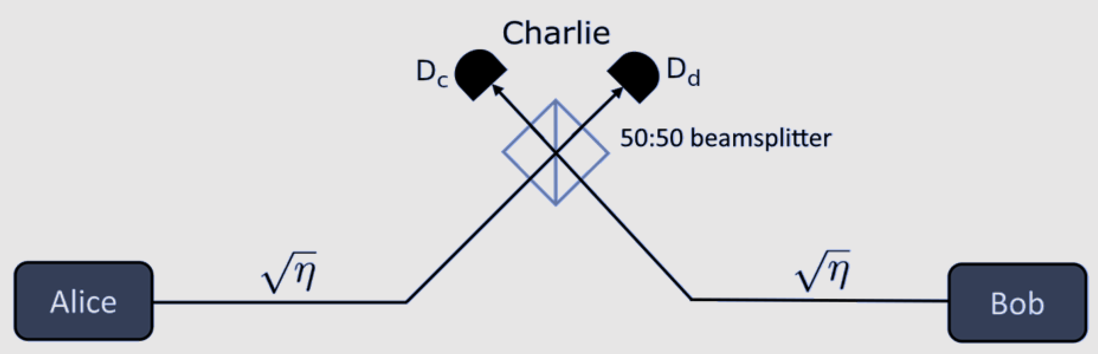
Guillermo Currás Lorenzo, Lewis Wooltorton, and Mohsen Razavi

School of Electronic and Electrical Engineering, University of Leeds
Leeds, United Kingdom

UNIVERSITY OF LEEDS

Twin-Field QKD

- **Twin-field QKD** offers **improved key-rate scaling** with channel loss, opening the way for **distance records**.



- Many practical variants with weak laser sources: sending-or-not sending, phase-matching…
- Almost all use the **decoy-state method**, which requires users to generate **phase-randomised coherent states**.

Continuous phase randomisation (CPR)

- **Key assumption** of the decoy state method: the phase is randomised **continuously** and **uniformly**.

$$\frac{1}{2\pi}\int_0^{2\pi} \left|\sqrt{\mu}e^{i\theta}\middle\rangle\!\middle\langle\sqrt{\mu}e^{i\theta}\right| d\theta = \sum_{n=0}^{\infty} p_{n|\mu}\,|n\rangle\!\langle n|$$

- 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 randomized 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

$$\sum_{n=0}^{M-1} \left|\sqrt{\mu}e^{\frac{2\pi n}{M}}\middle\rangle\!\middle\langle\sqrt{\mu}e^{\frac{2\pi n}{M}}\right| = \sum_{n=0}^{M-1} p_{n|\mu}\,|\lambda_n^{\mu}\rangle\!\langle\lambda_n^{\mu}|$$

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

$$|Y_n^{\mu} - Y_n^{\nu}| \leq \sqrt{1 - |\langle\lambda_n^{\nu}|\lambda_n^{\mu}\rangle|^2}$$

- 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.

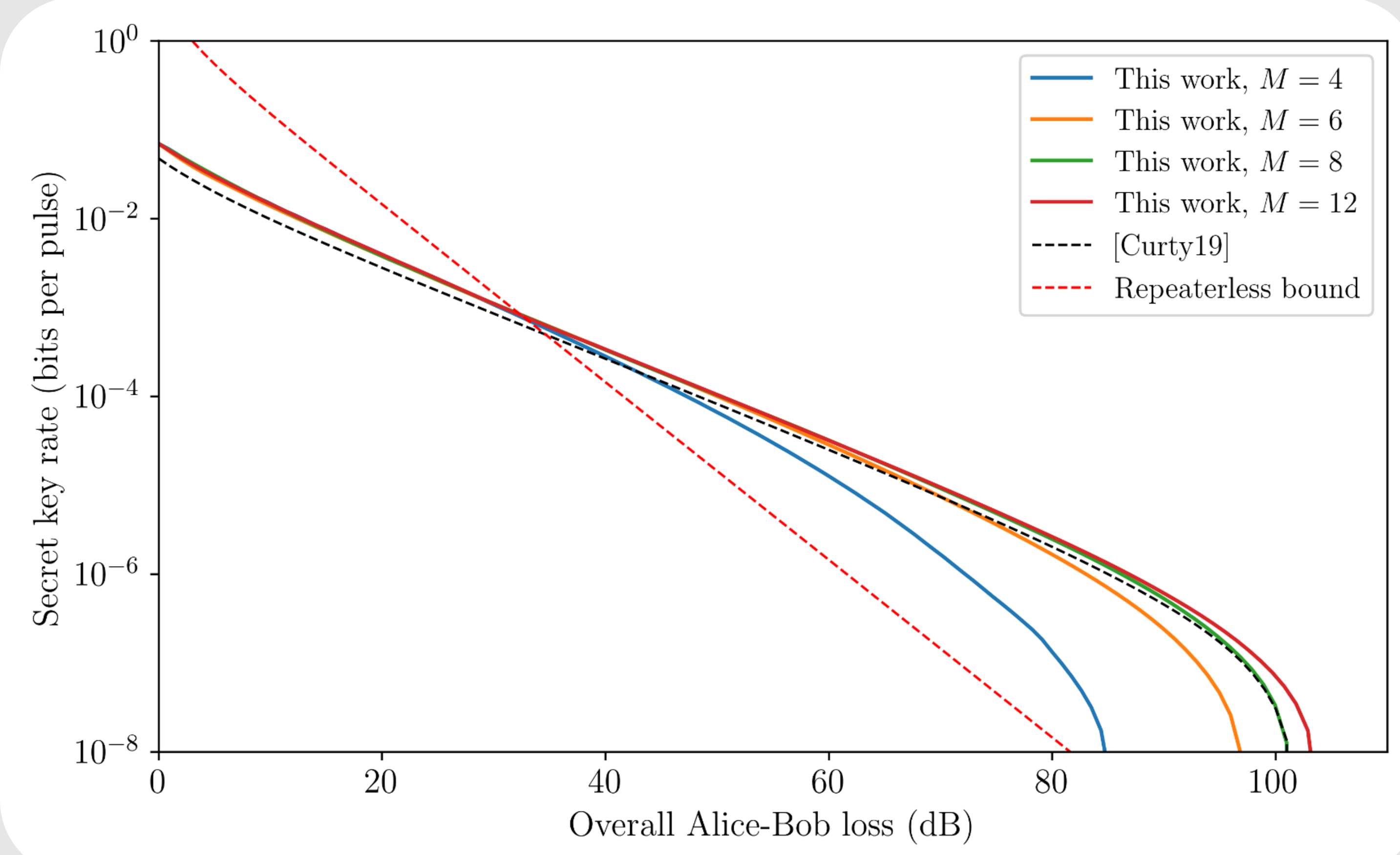
TF-QKD with DPR

- 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 $O(n^4)$, 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**.

Results



- Remarkably, we obtain **better results** than [Curty19]!
- The key reason is that, using DPR, we can **postselect** the test mode rounds in which the users used the same (or opposite) phases. We can use the postselected data to obtain a **better estimate** for the **phase-error rate**.
- This post-selection is not possible using CPR, as Alice and Bob have infinitely many phase choices, and they will never use exactly the same phase.

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

[Curty19] Curty, M., Azuma, K., & Lo, H. K. (2019). Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Information, 5(1)*, 1-6.
[Cao14] Cao, Z., Zhang, Z., Lo, H. K., & Ma, X. (2015). Discrete-phase-randomized coherent state source and its application in quantum key distribution. *New Journal of Physics, 17(5)*, 053014.
[Primaatmaja19] Primaatmaja, I. W., Lavie, E., Goh, K. T., Wang, C., & Lim, C. C. W. (2019). Versatile security analysis of measurement-device-independent quantum key distribution. *Physical Review A, 99(6)*, 062332.

* This project is funded by the European Innovative Training Network **Quantum Communications for ALL (QCALL),** project 675662, under the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015. Please visit www.qcall-itn.eu for more information.