Contribution ID: **16** Type: **Poster**

Enhanced security bounds for quantum cryptography with arbitrary phase randomization

Quantum key distribution (QKD) is a technique for sharing a secret key between two separated communicating parties, usually referred to as Alice and Bob. When employed in conjunction with the one-time-pad encryption scheme, QKD provides information-theoretically secure communications, regardless of the future progress of classical or quantum technologies. In recent years, the field of QKD has made significant progress both theoretically and experimentally. However, certain challenges must still be overcome before this technology can be widely adopted. One of these challenges is to bridge the security gap that exists between theory and practice. This is because most QKD security proofs typically consider assumptions that the actual experimental implementations do not satisfy. Such differences could lead to security loopholes or so-called side-channels, which Eve could use to compromise the security of the generated key without being detected.

Practical QKD transmitters usually emit laser-generated weak coherent pulses (WCPs) which can contain multiple photons created in the same state, allowing an eavesdropper to split the multi-photon signals obtaining a copy of the signal photon.
This photon-number-splitting (PNS) gives Eve complete information about the portion of the key generated by the multiphoton pulses and thus causes the secret key rate of the BB84 protocol to scale quadratically with the system's transmittance.

The decoy-state method [1-3] is currently the most effective solution to overcome the PNS attack. It involves Alice sending Bob phase-randomized (PR)WCPs with various intensities selected at random. Phase-randomization means that the phase of each WCP is randomly chosen between 0 and 2π, with uniform probability (in other words, its probability density function, $g(\theta)$, satisfies $g(\theta) = 1/2\pi$). By analyzing the measurement statistics of different intensities, it is possible to estimate the yield and phase error rate of the single-photon emissions, which are used to generate the secret key. The decoy-state method has been successfully demonstrated in multiple experiments, delivering a secret key rate similar to that of single-photon sources.

PR-WCPs can be produced through two principal methods: by gain-switching, or by using an external phase modulator that is controlled by a random number generator. However, both methods have limitations that prevent $g(\theta)$ from being uniformly distributed, thus invalidating a critical requirement of most decoy-state security proofs. Previous works [4] have analyzed the case of perfect discrete phase-randomization, for which $g(\theta)$ satisfies $g(\theta) = \frac{1}{N}\sum_{k=0}^{N-1}\delta\left(\theta-\theta_k\right)$, where $\delta(x)$ represents the Dirac delta function and $\theta_k = 2\pi k/N$, with N being the total number of phases and $k \in \{0, 1, ..., N-1\}$. In this case, it has been shown that an approximation to the performance of the ideal case is possible with a low value of N [4]. However, flaws in the phase modulator and electronic noise frequently prevent the phases from being evenly distributed, negating the possibility of using these results in a practical configuration.

To solve this, in [5], we consider the more realistic scenario in which $g(\theta)$ could be an arbitrary, continuous or discrete, probability density function (PDF), and we provide asymptotic security bounds for this general situation. The key components of our analysis are two: the use of basis mismatched events, and a novel parameter estimation technique based on semi-definite programming (SDP) [6,7]. We show that with this technique it is possible to tightly estimate the relevant parameters required to determine the secret key rate. As a result, we find that the decoy-state method is quite resistant to faulty phase-randomization. Notably, given the perfect discrete phase-randomization condition, our technique provides secret key rates that are significantly greater than those in [4].

Our analysis can also be adapted to tackle the problem of imperfect phase-randomization when only partial information about $g(\theta)$ is available. For illustration purposes, in [5], we consider the case where Alice emits

pulses whose phase is located in a certain interval centered in $\theta_k = 2\pi k/N$, but its precise PDF $g(\theta)$ is unknown. We consider a parameter δ_{max} that denotes the maximum possible deviation between the selected phase θ_k and the actual imprinted phase and derive a lower bound for the secret key rate in this scenario.

Putting it all together, our results provide a fundamental step towards the security of practical QKD systems with phase imperfections. We note that our results are also relevant for other quantum communication protocols beyond QKD that use WCPs and decoy states.

[1] W.-Y. Hwang Physical Review Letters 91, 057901 (2003).
[2] X.-B. Wang Physical Review Letters 94, 230503 (2005).
[3] H.-K. Lo and X. Ma & K. Chen Physical Review Letters 94, 230504 (2005).
[4] Z. Cao, Z. Zhang, H.-K. Lo & X. Ma New Journal of Physics 17, 053014 (2015).
[5] X. Sixto, G. Currás-Lorenzo, K. Tamaki & M. Curty (In preparation, 2023).
[6] S. Nahar Master's thesis, University of Waterloo. Decoy-State Quantum Key Distribution with Arbitrary Phase Mixtures and Phase Correlations (2022).
[7] G. Currás-Lorenzo, K. Tamaki & M. Curty preprint arXiv:2210.08183 (2022).

Author: SIXTO, Xoel (UVigo)

Co-authors: CURRÁS-LORENZO, Guillermo (University of Toyama); TAMAKI, Kiyoshi (University of Toyama); CURTY, Marcos (UVigo)

Presenter: SIXTO, Xoel (UVigo)

Session Classification: Poster Session 1