Finite-size analysis of thermal and CV-MDI quantum cryptography

Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola
Department of Computer Science, University of York, YO10 5GH, UK.
(Dated: July 7, 2017)

Quantum cryptography with continuous variables (CV) is moving towards the implementation in realistic scenarios [1]. For these practical purposes it is essential to study the performances of protocols including finite size effects [2]. These start to play an important role when we assume that the parties prepare the secret key sharing a finite number of signals. In such a case, they have a finite number of signals available to estimate the channel parameters and extract the secret key.

We adapt the method described in Ref. [3] in order to develop a systematic analysis of finite size effects in one-way thermal quantum cryptography. In this case, the parties use states with preparation imperfections to encode their variables, which are a result of trusted thermal noise [4–6]. This noise can be used as a defence against eavesdropping attacks for the direct reconciliation protocols. In addition to this, using thermal states we can extend the security analysis of the protocol to lower electromagnetic frequencies, e.g. for microwave telecommunications.

More specifically, we use the formula for the secret key rate for finite size effects adapted in the case of thermal states, where we have taken into consideration that a part of the signals exchanged between the parties was used for the channel parameter estimation. We express the rate with respect to the channel parameters which are the transmissivity τ and the excess noise variance V_ϵ and we define estimators for them. In fact, these estimators are dependent on the number of the signals sacrificed. Then we theoretically calculated the estimators' variances, the associated confidence intervals and we choose the most pessimistic values for the key-rate.

Similarly, we extend the security analysis of measurement-device-independent (MDI) QKD protocols [7, 8] including finite-size effects. In an MDI scheme the parties cannot access a direct link, but they can exploit an intermediate relay in order to share the key. The MDI configuration is very important because it represents the basis for more complex network communications.

[1] E. Diamanti *et al.*, Entropy **17**, 60726092 (2015).
[2] A. Leverrier *et al.*, Phys. Rev. A **81**, 062343 (2010).
[3] L. Ruppert *et al.*, Phys. Rev. A **90**, 062310 (2014).
[4] C. Weedbrook *et al.*, Phys. Rev. A **86**, 022318 (2012).
[5] V. C.Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[6] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[7] S. Pirandola *et al.*, Nat. Photonics **9**, 397402 (2015).
[8] C. Ottaviani *et al.*, Phys. Rev. A **91**, 022320 (2015).