Hybrid quantum cryptography: everlasting security with performances beyond QKD

Romain Alléaume
Télécom ParisTech, LTCI - 46 rue Barrault, 75013 Paris, France

One typical use case for quantum key distribution (QKD) is data link encryption, where QKD-generated keys are used to feed the AES link encryption devices. This solution has the advantage of allowing to use fast AES encryptors, compatible with data rates in the Gbit/s range. On the other hand, the encryption security is only computational and the overall benefit of using QKD, instead of another computational key distribution technique, can be questioned [1, 2]. We propose here to reverse the perspective and to study how computational techniques be combined with quantum cryptographic techniques to enhance the performance of the latter, while keeping a clear advantage, in terms of everlasting security.

We propose to consider an hybrid security model in which computational one-way function are assumed to be perfectly secure during a relatively short time τ (say a few minutes), and broken afterwards. Conversely we also assume that quantum memories have a coherence time shorter than τ.

In this model, we construct a family of protocols for quantum key distribution, called High Dimensional Hybrid Quantum Key Distribution (HDH-QKD). HDH-QKD is based on the encoding of discrete classical information into high-dimensional coherent states quantum codewords followed by the application of a high-dimensional phase encryption operation. HDH-QKD allows to perform secret key establishment between distant Alice and Bob at performance levels (rates/distance) unreachable with QKD [3] and with everlasting security, unattainable by classical means .

One striking feature of HDH-QKD with d-dimensional encodings is that its security can be guaranteed with while sending much more than one photon per codeword. This allows to boost key rates in comparison with QKD and can moreover lead to an important increase of reachable distances, for implementations that can support a large number of modes. Security analysis against non-adaptative attacks indicates that if HDH-QKD can be operated with encodings in dimension $d = 10^3$, foreseeable in a near future, then the secure distance could be extended by $30dB$ with respect to conventional QKD.

[1] K. Paterson, F. Piper, R. Schack, *Why Quantum Cryptography?* quant-ph/0406147.
[2] R. Alléaume, et. al., *Using quantum key distribution for cryptographic purposes: a survey.* Theoretical Computer Science, 560, 62-81. (2014)
[3] Pirandola, S., Laurenza, R., Ottaviani, C. and Banchi, L. , *Fundamental limits of repeaterless quantum communications.* arXiv preprint arXiv:1510.08863. (2015).