
**F. J. Mendieta**, P. Gallion, P. Bellot, E. Garcia, J. A. Lopez, A. Arivu

*CICESE, Carretera Ensenada-Tijuana 3918, Ensenada, Baja California 22860, Mexico. email: mendiet@ciecse.mx

Telecom-Paristech, CNRS LTCI UMR 5141, 46 rue Barrault, Paris 75013, France. email: philippe.gallion@telecom-paristech.fr

Universidad Autónoma de Baja California. Calzada Tecnológico # 14418, Mesa de Otay. Tijuana, B.C. México

**Introduction**

Quantum-based security is limited only by the principles of physics and not in terms of resources that Eve could realistically have. However the needs of a time independent truly unconditional security will be very limited and costly, with weak economics or societal interest that can be performed. Unconditional security at the quantum layer is not sufficient to achieve an end-to-end security up to the application layer.

The conservative world of security is up to now a monopoly for the pure software-based classical security: present systems are mainly improved by increasing of the key length and cannot afford any technical risk of disruptive technologies. The only way for quantum security to keep a credible role and to create a wide range of applications is a progressive infiltration into the classically secured technology and culture. It has also to be included in an end-to-end security approach and to clarify its compatibility with optical fiber systems. The quantum technology may in fact provide a security level far from the ultimate quantum limit, but already much better than traditional security. It is therefore important to try to quantify objectively this security and to investigate the way for quantum technology to supplement and improve classical security.

**Quantum Security Infiltration**

Some researchers have already started to envision the prospective post-quantum world [PCQ], in which cryptographic algorithms can be solved with sub-exponential resources. Quantum Key Distribution (QKD) is much welcomed as a fundamental building block for post-quantum communications. However the information will still be relayed to the end-user via classical channel, and the interaction with the classical electronics is an issue to tackle (Figure 1) [BHASIN].

It is therefore important to think of the security in a holistic way, as of today the attacks do not target the cryptography, but its implementation that leaks precious information via side-channels; in the post-quantum world the attacker will no target frontally the quantum layer, but rather exploit the information leakage. The purpose of our project is to bring together the classical and quantum cryptography, since they are complementary and need to co-exist, with their boundary exchanges. The assessment of the security of such a complex compound system is an issue to tackle, in relation with its layered structure and the diverse types of attacks, such as the biasing of the randomness sources, and a predictive evaluation of the risks is necessary.

**End-to-End Quantum Based Security**

End-to-end security must be formally studied: it covers the different types of attacks that can be performed on a classical + quantum system; random number generation must be studied with particular interest. Quantum apparatus used in QKD cannot be error free, and many algorithms have to be applied in order to obtain unconditional security: bit reconciliation, privacy amplification and authentication steps (Figure 2) [BELLOT].

**Homodyne Quantum Key Distribution at Telecommunication Wavelength**

Diverse implementations of the quantum physical layer are today available. We select a phase modulation homodyne detection system, operating at the telecommunication wavelength that overcomes the costly and low performance photon counter and provides differential phase referencing and built-in optical synchronization [GALLION]. Some fundamental aspects on the role of the optical phase, acting as an additional security provider or as a possible attack parameter, must be investigated.

The synchronization at the optical layer is a though problem that is often evaded; nonetheless no realistic system can be deployed if the secret bits are not understood and are not shared by Alice & Bob. Therefore, the synchronization of the exchanges must be embedded into the optical channel(s), and the task of recovering the phase in a quantum context is an important point that needs to be treated (Figure 3) [MENDIETA].

Links in future networks will have quantum and classical channels operating in parallel: both will assist each other to accomplish communication security and advanced network functions. Ideally, a DWDM network should be minimally modified to accept QKD. Fiber impairments, light pulse generation, and detection all affect quantum measurements that must be carefully analyzed and its impact evaluated.

**References**


POS: http://pos2010.cased.de/