



**UNIVERSITÉ  
DE GENÈVE**

**FACULTÉ DES SCIENCES**  
Département de physique  
nucléaire et corpusculaire

## SÉMINAIRE DE PHYSIQUE CORPUSCULAIRE

**SUJET:**        **Quantum Computing and Cryptography**

**PAR:**         Prof. Hugo ZBINDEN  
Université de Genève - GAP

**DATE:**        Mercredi 16 janvier 2019

**LIEU:**         Ecole de physique, Grand Auditoire A - **11h15**  
24, Quai Ernest-Ansermet, Genève

### RÉSUMÉ:

The Quantum Computer is a threat for today's cryptography. Indeed, it could factorize large numbers efficiently and make the current public key cryptography obsolete. Interestingly, Quantum Physics is also at the origin of a solution of distributing keys in a secure way: The quantum key distribution.

In this talk I will briefly introduce the quantum computer (be aware I am not a specialist) and then explain how quantum key distribution works. I will present the state of the art of QKD and discuss the possibilities and limits.

INFORMATION : <http://www.unige.ch/dpnc>

ORGANISATEURS: [Anna.Sfyrla@unige.ch](mailto:Anna.Sfyrla@unige.ch) & [Domenico.Dellavolpe@unige.ch](mailto:Domenico.Dellavolpe@unige.ch)