h e p i a
Haute école du paysage, d'ingénierie et d'architecture de Genève

INIT
Institut d'ingénierie informatique et des télécommunications
Rue de la Prairie 4
CH-1202 Genève

Tél. +41 (0)22 546 24 00
Fax +41 (0)22 546 24 10

hepia@hesge.ch
www.hesge.ch/hepia

# Secure High-Speed Communication based on Quantum Key Distribution

**Acronyme**: QCRYPT

**Type**: Nano-tera

**Dates approximatives**: du 01.03.2010 au 31.02.2013

**Coût estimatif total** : 4342 kCHF

**Coût estimatif hepia/INIT** : 192 kCHF

**Partenaires**

- Université de Genève (GAP-O)
- ETHZ
- HES-SO (heig-vd, **hepia**)
- IdQuantique

**Résumé (en anglais)**

Today's information society relies heavily on storing and transferring data in digital form. Cryptography provides the means that is necessary to securely exchange data securely. It relies on two fundamental parts: first, one needs a secret key; second, this secret key is used to encrypt the data with a mathematical algorithm. Secret keys can be transmitted using a trusted messenger, or in a more convenient way, using public key infrastructure (PKI). The security of PKI is based on computational complexity and suffers from the lack of a mathematical proof for the class of complexity. Modern encryption, using algorithms like the Advanced Encryption Standard (AES), is generally considered unbreakable, provided the keys are sufficiently long. However, absolute security can only be guaranteed by the so-called one-time-pad (OTP), where secret keys as long as the message, have to be used.

Our project aims to considerably improve cryptography on both the key distribution level and the encryption level. Quantum Key Distribution is a secure way to generate keys, which is based on the fundamental laws of quantum mechanics. However, existing systems are too slow. The new QKD system will be capable of producing keys at 1Mbps rate, which means it will allow 1MHz OTP encryption for high-level applications. In standard applications the data exchange rates continue to increase.

Today's commercial encryptors are already approaching 10Gbps. Consequently we will develop a future proof encryption engine for up to 100 Gbps and look to combine this high-speed encryption with high rate QKD, to allow for changing the keys rapidly, thus considerably improving the security and simplifying the key management.

This project will develop advanced prototypes for very-high-speed QKD and encryption. Both of these systems will greatly surpass any technology currently available. This is only possible by combining the outstanding competencies of the partners in such diverse fields as quantum optics, high-speed electronics and integrated circuit programming as well as cryptographic and network security. Our modular approach will provide flexible solutions for diverse communication scenarios by operating the devices in unison or stand-alone. Finally, in contrast to current quantum key distribution systems, they will be compatible with standard optical networks and capable of using wavelength multiplexing.

**Contact hepia**

Fabien Vannel (fabien.vannel@hesge.ch)