UNIVERSITÉ DE GENÈVE

PRESS RELEASE

Geneva | September 25th, 2019

The EU supports secure quantum communication

Four Swiss organisations, including UNIGE, receive funding from the European Union (EU) through OPENQKD, a secure quantum communication infrastructure.

September 2019 marks the launch of a 3-year European research project, named OPENQKD for Open Quantum Key Distribution, that will install test quantum communication infrastructures in several European countries. It will boost the security of critical applications in the fields of telecommunication, finance, health care, electricity supply and government services. For this €15 million project, the European Union has selected 38 companies and research institutes across the continent, including four Swiss organizations all from Geneva: University of Geneva (UNIGE), Services Industriels de Genève (SIG), ID Quantique and Mt Pelerin.

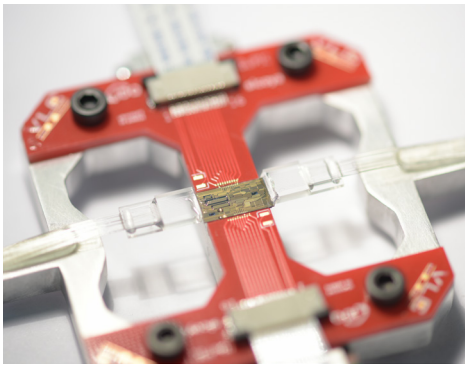
OPENQKD aims to change the way we see, understand and use quantum communication. Its main focus is to create and test communication network infrastructures with a built-in quantum element, known as Quantum Key Distribution (QKD). The secret keys distributed through QKD enable an ultra-secure form of encryption that allows data to be transmitted with a very high level of security. It will lay the groundwork for a pan-European quantum communication infrastructure that uses satellite as well as ground-based solutions.

Building closer European links

The Europe Commission chose to fund OPENQKD following a Horizon 2020 call for proposals in 2018. Its mission is to develop experimental testbeds based on QKD and to test the interoperability of equipment supplied by different manufacturers of quantum systems among which ID Quantique (IDQ), UNIGE'S spin-off and the global leader in quantum communications and quantum sensing, based in Switzerland. OPENQKD's activities will take place all over Europe (in Austria, Spain, Poland, Germany, Netherlands, Switzerland, France, Italy, UK, Greece and the Czech Republic). It will focus on several key fields of operations, especially the telecommunications sector, where data security is critical. Other applications, such as securing medical, governmental or energy grid data will also be demonstrated and evaluated.

Four use cases in Geneva

As part of Open QKD, UNIGE, ID Quantique (IDQ), the manufacturer of quantum communication solutions, the Services Industriels de Genève (SIG), Geneva's provider of energy, water, optical fibers and waste-treatment networks and Mt Pelerin, the Swiss leader in blockchain technology for banking and finance, are working together on at least four uses cases which will be implemented in Geneva.



Integrated photonics chip, as they will be used in QKD systems.

High resolution pictures

Long-term encryption

Encryption is more and more often required for securing critical data. This is particularly the case for user electronic data like the one of hospital patients frequently encrypted. As such storage is long term (10 years at least, possibly during the patients' lifetimes), it is key to use state-of-the-art technologies. UNIGE will be evaluating the use of QKD for strong and long-term encryption by measuring the delay to re-encrypt data due to key or algorithm change.

A quantum vault

The Quantum Vault is a new kind of Digital Asset Custody system designed by Mt Pelerin in cooperation with ID Quantique. This custody infrastructure aims at providing ultra-secure storage of digital assets by financial institutions such as global custodians, cryptocurrency exchanges, asset managers and central banks. The Quantum Vault relies on a QKD infrastructure provided by IDQ and transported over the SIG network. By adding this extra layer of quantum-safe security on top of a bank-grade custody solution, the Quantum Vault ensures that the safe storage of private keys (the proof of a digital asset's ownership) is "Information-Theoretically Secure" (ITS). ITS means that according to information theory, such a system cannot be hacked by an external adversary even with unlimited computing power.

A testbed in Geneva

Over the next seven years, SIG will create a smart grid network to connect its power stations in Geneva. To secure data transmission and detection intrusion (hackers taking control of the electricity distribution network), SIG will test quantum technology provided by IDQ in a real production and operational environment. To this end, SIG will connect five power stations to the QKD testbed and assess available QKD technologies and services offered by the consortium.

SIG also intends to implement a quantum-safe solution between 2 main datacenters used as primary / backup. Data replication, fail over and load balancing imply the transfer of a large amount of highly sensitive data. Communication will be secured though QKD. This use case will focus on demonstrating high availability, high performance and failover solutions.

With this testbed in Geneva and its corresponding use-cases, OPEN-QKD will develop an innovation ecosystem and training ground as well as help to grow the technology and solution supply chains for quantum communication technologies and services.

contact

Hugo Zbinden
Associate Professor
Department of Applied Physics
Faculty of Science
+41 22 379 05 04
Hugo.Zbinden@unige.ch

UNIVERSITÉ DE GENÈVE
Communication Department
24 rue du Général-Dufour
CH-1211 Geneva 4

Tel. +41 22 379 77 17

media@unige.ch
www.unige.ch