PRESS RELEASE

Paris, May 5th, 2021

Quantum cryptography experimental battle-testing: thwart the easy attacks first!

Quantum cryptography will be a key asset for securing private and sensitive communications in the near future. To be efficient, technologies like Quantum Key Distribution (QKD) have to resist external attacks. Researchers from Télécom Paris, Institut Polytechnique de Paris, have shown in an experiment published in *Nature Scientific Reports* that a given security vulnerability can lead to attack paths exhibiting different experimental complexity. They introduce a comprehensive methodology to rate attacks. This enables the development of countermeasures against the easiest attacks to be prioritized and improves the design of quantum cryptographic hardware, paving the way for their security certification.

Being able to send messages that can be kept secret from possible eavesdroppers has always been of utmost importance in our society. From Julius Caesar, who used a form of encryption to communicate with his army generals, to some striking applications of telecommunication networks such as telemedicine, the ability to guarantee a high-security level has always been critical. In this context, Quantum Key Distribution (QKD) is an approach whereby a secret key between distant parties can be established.

Romain Alléaume, Associate Professor at Télécom Paris, Institut Polytechnique de Paris, explains: "Whereas the cryptographic techniques used today rely on the conjectured difficulty of some mathematical problems, QKD security, on the contrary, is solely based on the laws of quantum physics. It therefore makes it possible to establish keys whose security can be guaranteed in the future, even against an adversary with unbounded computational power, including a quantum computer."

Classical and quantum cryptography complementarity

Despite providing stronger security, QKD and more generally, quantum cryptography, is unlikely to replace classical cryptography, since it does not provide all the security services and is currently mostly restricted to metropolitan distances. QKD can nevertheless provide unprecedented security levels for some targeted applications when used in combination with classical cryptography. We can make a parallel between cars and networks: whereas we tend to drive ever faster, using seatbelts only (classical cryptography) may not provide enough security. In that respect, QKD plays a role analogous to the airbag: an additional security layer to protect data confidentiality in the long term. These attractive promises have encouraged recent deployments of QKD networks, notably in the UK, Japan, Korea, and on a large-scale, in China.

Need for Security Certification

In 2019, Europe launched the EuroQCI initiative aimed at deploying a pan-European quantum communication infrastructure in the next 10 years, connecting strategic public sites and contributing to European digital sovereignty. Among the specificities of EuroQCI, this infrastructure will combine classical and quantum cryptography and will be based on security certified QKD systems, that do not yet exist. The QKD promise of unconditional security is indeed not sufficient to guarantee high security for practical device implementations. The current need is for a standardized approach in order to evaluate and certify the security of QKD products. Security certification is a mandatory step to broaden the market of quantum cryptographic technologies, such as QKD and QRNG (Quantum Random Numbers Generator). It constitutes a complex task, requiring the collaboration of experts from different fields ranging from IT security, quantum engineering and theory. Several international standardization organizations, such as ISO and the ETSI[1] QKD Industry Specification Group are working actively towards this goal, under the unified Common Criteria[2] framework.

Quantum hacking and attack protection

Francesco Mazzoncini, PhD student at Télécom Paris and co-author of the article, explains: "Inspired by the methodology used for classical cryptographic hardware, we have conducted an experimental vulnerability assessment of a 'Continuous-Variable' QKD system against saturation attacks aimed at its detectors. To this end, we tested two attack strategies. The

[1] European Telecommunications Standards Institute
[2] https://www.commoncriteriaportal.org/

implementation of the first one was no picnic at all: it required a large coherent displacement to be performed, a task that is notoriously challenging. The second strategy, in comparison, went much more smoothly: it consisted of shining a well-controlled external laser to the QKD receiver."

The article he published together with his colleagues Rupesh Kumar and Hao Qin, both former members of Telecom Paris quantum research group, conveys a change of perspective for the design of quantum cryptographic hardware: while the quest for perfect security has oriented most of the efforts of quantum cryptographers towards studying and fighting complex attacks, it demonstrates experimentally that easy "dirty" attacks can be the most dangerous in practice, and therefore that they must be addressed first! "Luckily, we also designed a general countermeasure against both of our attacks that can be implemented in software and therefore has a low cost overhead: it simply consists in performing a statistical test ensuring that the calibrated detector is operated in its linearity range", says Romain Alléaume. With this approach, the researchers also initiate a reflection on the trade-off between the performance of the quantum communication system, its security level and its cost. Prioritizing attacks allows to invest in countermeasures that ensure the security of the system without altering its performance or overly increasing its cost.

"Our work introduces a comprehensive methodology, based on attack ratings, for the security evaluation of quantum cryptographic hardware. This also constitutes a concrete step towards the security certification of QKD."

To learn more about this QKD battle-testing:

Experimental vulnerability analysis of QKD based on attack ratings

Rupesh Kumar (University of York), Francesco Mazzoncini (Télécom Paris), Hao Qin (CAS Quantum Network Co.), and Romain Alléaume (Télécom Paris)

www.nature.com/articles/s41598-021-87574-4

About Télécom Paris – www.telecom-paris.fr/en

Télécom Paris is one of the top four engineering schools in France for training general engineers. Recognized for its close ties with businesses, this public graduate school ensures excellent employment prospects in all industries and is considered the number-one engineering school for digital technology. With its top-level innovative teaching, Télécom Paris is at the center of a unique innovation ecosystem, drawing on the interaction and cross-disciplinary nature of the school's academic programs, interdisciplinary research, two business incubators and its campuses (Paris and Sophia Antipolis – EURECOM). Its LTCI laboratory has been recognized by HCERES as an outstanding unit in the field of digital sciences for its international reputation and exceptional number of initiatives supporting the socio-economic world and industry, as well as for its great contribution to teaching. A founding member of Institut Polytechnique de Paris and an IMT (Institut Mines-Télécom) school, Télécom Paris is positioned as the college for digital innovation on the Paris-Saclay Campus.

PRESS CONTACTS TELECOM PARIS

Isabelle Mauriac
Press Manager
+33 1 43 38 75 35 • +33 6 27 70 71 60
imauriac@imedia-conseil.fr

Stéphane Menegaldo
Scientific communication manager
+33 1 75 31 98 53 • +33 6 16 60 06 76
stephane.menegaldo@telecom-paris.fr