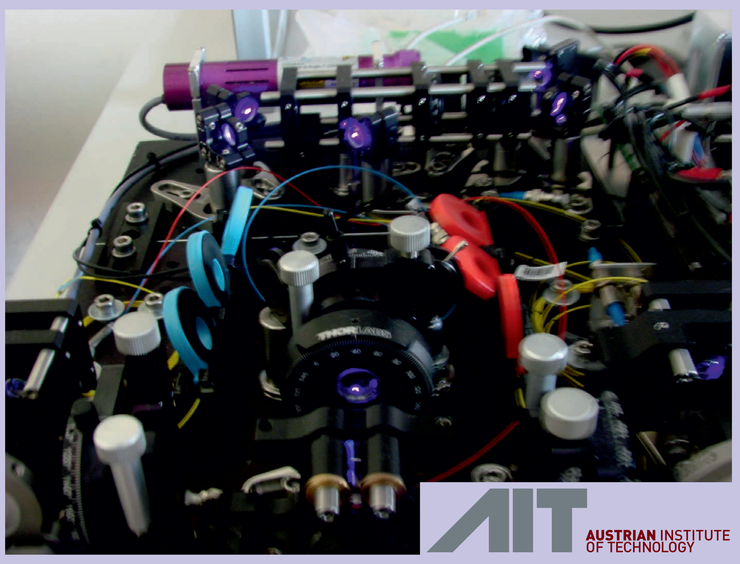
Wrocław University of Technology — WUT Institute of Informatics — WUT Institute of Physics

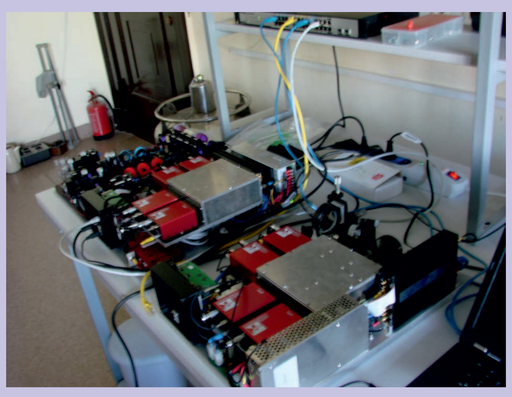
W. Donderowicz, A. Janutka, M. Jacak, J. Gruber, P. Tomczak, G. Kayyali, I. Jóźwiak, W. Jacak
Institute of Physics, Institute of Informatics, Wrocław University of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland

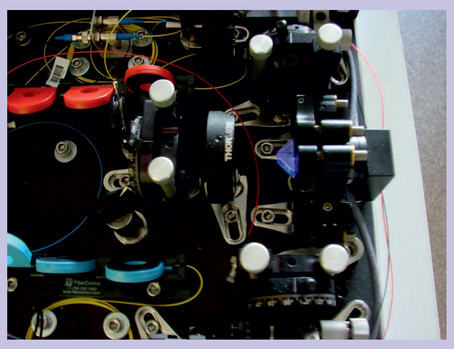
# WROCŁAW UNIVERSITY OF TECHNOLOGY QUANTUM CRYPTOGRAPHY LABORATORY RESEARCH PROGRAMME

QKD (quantum key distribution) is a technology of QIP providing theoretically unconditional security of information transmission. An advantage over classical cryptography follows from fundamental laws of QM - absolute arbitrariness of von Neumann projection. WUT QKD laboratory is newly equipped with both non-entanglement and entanglement based QKD R&D systems. It already cooperates in 2 national QKD research projects and is preparing to offer its cooperation for newly formulated international FP7-8 EU QKD related projects.



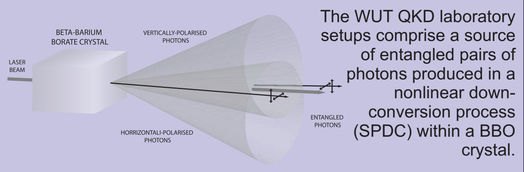




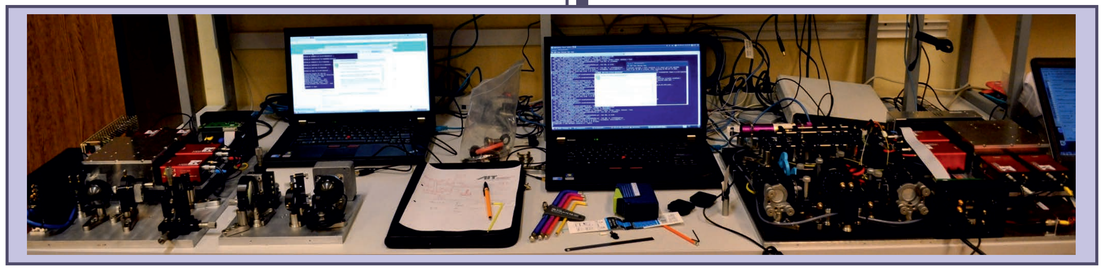
WUT laboratory of QKD is equipped with two R&D systems: the AIT EPR405 Quelle and the idQuantique Clavis$^2$. The first system uses entangled photons pair for transmission in quantum channel (coding qubits on polarizations and implementing the BB84 instead of the E91 protcol), while the second one non-entangled photons (coding qubits on phase differences and implementing BB84 and SARG04 protocols). Both systems use fiber optic channels, but the AIT EPR405 Quelle can operate also in open air via telescopic system. The distance for effectively coherent quantum communication is up to 100 km for the Clavis$^2$ and a bit shorter for the Quelle system (in open air up to 1 km). Both of the systems are the latest generation of setups from idQuantique SA and AIT, and their combination in a single laboratory creates an unique opportunity for QKD research and development based on these two leading standards.

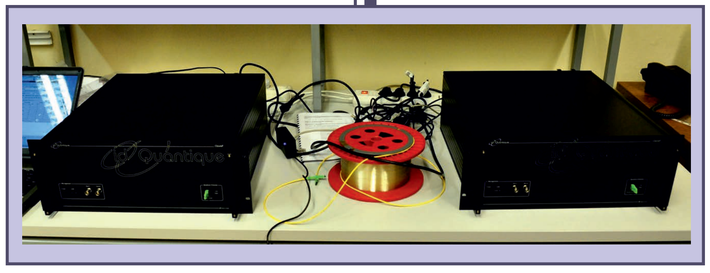
**Planned research:** validating blinding attacks and the new countermeasures, integrating with standard networks (telco noisy fibers, multiplexing schemes).

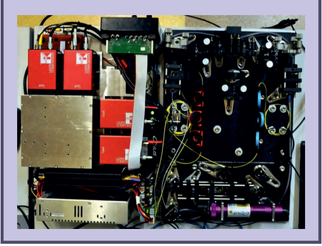

The WUT QKD laboratory setups comprise a source of entangled pairs of photons produced in a nonlinear down-conversion process (SPDC) within a BBO crystal.

**Planned research:** enhancements in entanglement based QKD protocols, prolonging entanglement conservation (avoiding reduction to standard BB84 protocol), experiments with quantum channels (integration in standard telco fibers, atmospheric thermal decoherence), QKD protocol stack enhancements, reduction of detectors number.

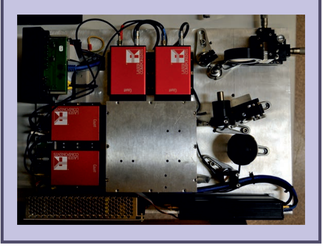




## ALICE



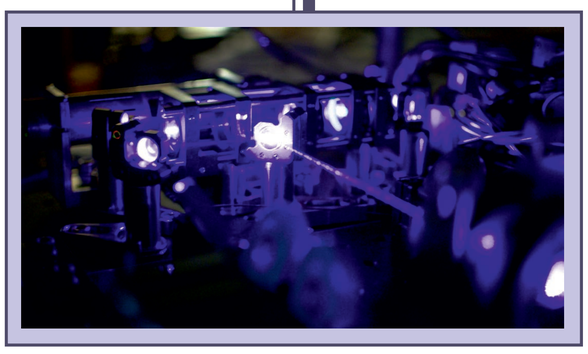
## BOB



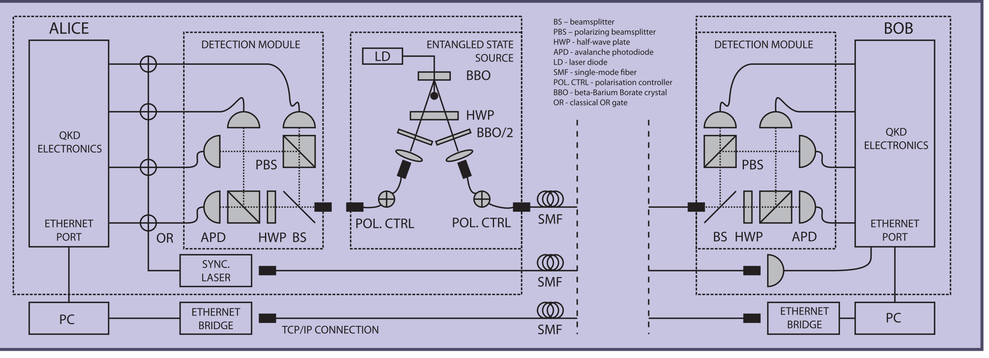
**Outline of a research programme for the QKD laboratory at WUT encompasses:**

1. Development and industry research towards test-deployment of both systems in standard telecom infrastructures.
2. A common investigation with idQuantique on using standard noisy fiber channels to transfer qubits of quantum signal (dark channel).
3. A possible joint setup of entangled and non-entangled system in order to enhance security in view of recent reports on attack on Clavis setup; verification of the blinding attack methods and testing of the countermeasures.
4. Enhancements in the QKD protocols stack (both entanglement and non-entanglement systems), in physical layer reduction of needed detectors, in higher layers: development of key reconciliation, privacy amplification and error corrections procedures.
5. Development of new protocol concepts and modifications for the existing protocols.
6. Deployment of additional equipment (both systems) within the common R&D project with a WUT spin-off CompSecur company (towards test-deployments of quantum networks, improving of software, star topology).
7. Analysis of decoherence effects in both systems in different channels: open air through atmosphere, optical fibers (different types), and special purpose connections: out of atmosphere (satellite).
8. Development of the software layer in both protocols to enhance functionalities and possible applications.
9. Development of new applications of hybrid QKD-classical systems based on latest progress in classical IT security.
10. Participation in international research towards new quantum mechanics based applications in IT security (quantum digital signature, architecture of the global satellite based QKD concepts) and standardization efforts.

**Planned research:** combining both systems in a multi-node quantum network, indirect 1-1-1 QKD schemes, preparing systems to be test-deployed in classical telecommunication networks infrastructures.



Scheme of the AIT EPR405 Quelle system




Scheme of the idQuantique Clavis$^2$ system