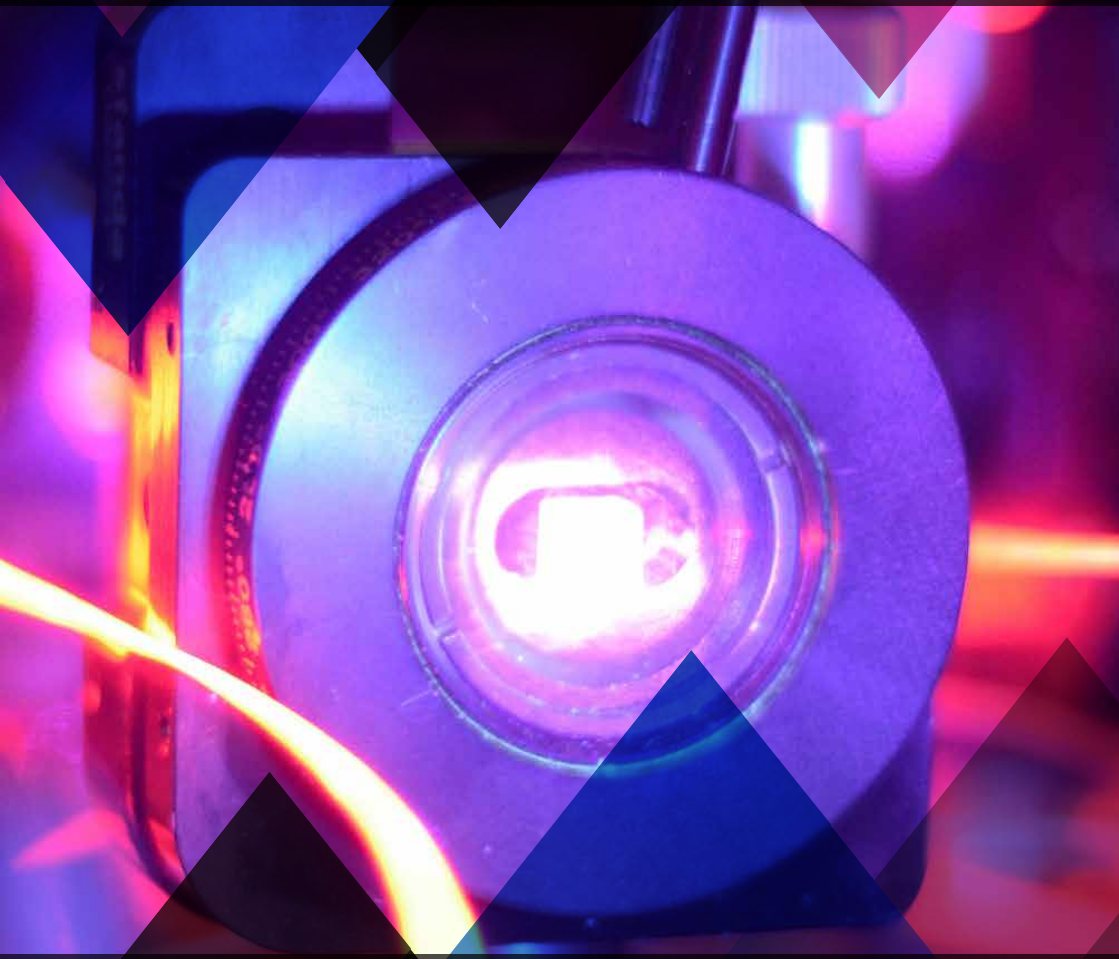
seQre 2014

Progress in Quantum Cryptography

The 5th Symposium
of Laboratory of Physical Foundations
of Information Processing

27th - 28th January 2014
Wroclaw University of Technology
Wrocław, Poland



|LFPPI⟩ Laboratory of Physical Foundations of Information Processing

National Laboratory for Quantum Technologies

Wrocław University of Technology

CompSecur IT Solutions

seQre2014

The 5th LFPPI Symposium on Progress in Quantum Cryptography

Date: **27th-28th January 2014**
Location: Wroclaw University of Technology (WUT), Wroclaw, Poland

Organizers:
- Laboratory of Physical Foundations of Information Processing (LFPPI), Wroclaw branch
- National Laboratory for Quantum Technologies (NLTK), Wroclaw branch
- Institute of Physics, Institute of Informatics, Electronics Faculty, WUT
- CompSecur, WUT spin-off company

Symposium registration deadline: 25th January 2014

Other deadlines (only for authors of contributions):
Abstract submission deadline: **20th December 2013**
Notification of acceptance (oral/poster): **8th January 2014**
Accepted paper submission deadline: **20th February 2014**

http://www.seqre.net/seqre2014
E-mail: seqre2014@seqre.net
Tel. +48 71 7070077

The 5th LFPPI Symposium: Progress in Quantum Cryptography SeQre2014 is a unique international event that will present both the current scientific and application prospects of quantum cryptography in view of recent progress in development of quantum computers, aiming to bring together academic societies of outstanding quantum physicists, computer scientists and engineers with representatives of industry considering quantum cryptography deployment.

The symposium is organized on the occasion of Wroclaw metropolitan QKD network deployment (one of the first few quantum networks worldwide) based on experimental non-entanglement and entanglement QKD systems. During the symposium a practical demonstration of QKD systems by leading companies addressed to industry and security sector of finance and administration is planned. The Symposium aims also to elevate interest and commercial support for QKD systems development from the side of bank and administration representatives invited to participate in the event.

The LFPPI Symposium series consists of small scale events addressed to progress in quantum information and communication traditionally honored by distinguished invited speakers (in the past the symposium was honored by the lectures of among others prof. Artur Ekert, prof. Christopher Fuchs and prof. Gerard 't Hooft). The 5th LFPPI Symposium will be focused on the progress of quantum cryptography and will take only two days, creating though an opportunity for discussion among most advanced experts in modern quantum cryptography (including authors of the most important concepts in this field, as well as companies commercializing already maturing systems).

Conference location:
Wrocław University of Technology
A-1 Bulding (main entrance
and Aula - main auditorium, 2nd floor)
Institute of Physics
Wyb. Wyspiańskiego 27
50-370 Wrocław, Poland

Scan this QR Code to get directions

Programme

1st day - 27th January (Monday)

8:30-10:00	Registration at conference front desk
10:00-10:20	Greetings and introduction from the organizers
Scientific session 1 - invited lectures	
10:20-11:05	Opening lecture: Future of quantum communication: quantum networks, quantum repeaters and device-independent QKD **Prof. Nicolas Gisin** (University of Geneva, IDQuantique)
11:05-11:50	Invited lecture: The ultimate limits of privacy for the paranoid ones **Prof. Artur Ekert** (University of Oxford, National University of Singapore, Center for Quantum Technologies)
11:50-12:35	Invited lecture: How secure is quantum cryptography in practice? **Prof. Vadim Makarov** (University of Waterloo, Quantum Hacking Laboratory)
12:35-13:20	Invited lecture: Quantum information theory and its resources **Prof. Marek Kuś** (Polish Academy of Science, Warsaw)
End of Scientific session 1	
13:20-14:20	Lunch break
Industry session 1 - invited companies	
14:20-14:40	Technical lecture / Product presentation **AIT (Austria)**
14:40-15:00	Technical lecture / Product presentation **IDQuantique (Switzerland)**
15:00-15:20	Technical lecture / Product presentation **Toshiba (Japan)**
15:20-15:40	Technical lecture / Product presentation **NTT (Japan)**
15:40-16:00	Technical lecture / Product presentation **SeQureNet SA (France)**
16:00-16:20	Technical lecture / Product presentation **MagiQ Inc. (USA)**
End of Industry session 1	
16:20-16:40	Coffee break
Scientific session 2	
16:40-18:00	Invited LFPPI lectures on progress in quantum cryptography and quantum information
End of Scientific session 2	
18:00	Transfer of guests to hotels
19:30-21:00	Dinner at the city old square

2nd day - 28th January (Tuesday)

Scientific session 3 - oral contributions		
10:00-12:00	Series of contributed lectures on progress in quantum cryptography	Parallel certified training session for business and administration in Polish language
End of Scientific session 3		
12:00-13:00	Lunch Break	
Industry session 2 / QKD hands-on training second session for business and industry representatives		
13:00-15:30	Technical lectures and training demonstrations of entanglement and non-entanglement QKD systems with hands-on workshops. Presented systems: among others entanglement based AIT EPR SYS-405 (Austria), non-entanglement based IDQuantique Clavis2 (Switzerland), continous variable based SeQureNet Cygnus (France). Technical consultancies: **AIT, IDQuantique, SeQureNet, NTT, Toshiba, MagiQ, CompSecur, NLTK WUT**.	
End of Industry session 2		
15:30-16:00	Coffee break with poster session (with networking reception)	
Summary and discussion		
16:00-18:00	Discussion panel and closing of the symposium. Also including establishment of a CMQCRD consortium and discusion of prospects for international cooperation with leading research centers and commercial companies in scope of QKD development	
Excursion to "Panorama of the Battle of Racławice" exhibition.		

Certified quantum cryptography training for business
2nd day - 28th January

On the 2nd day of the seQre2014 Symposium a certified QKD training in Polish language for business and administration will take place. Training will cover fundamental theoretical and practical aspects of quantum cryptography. Quantum key distribution systems will be subject of hands-on workshops. The Laboratory of Quantum Cryptography within the WUT National Laboratory for Quantum Technologies along with CompSecur R&D will provide QKD systems for training purposes (both non-entanglement and entanglement based systems will be included).

Training conducted in Polish language will be free of additional charge. Each participant will have an opportunity to familiarize with high-end QKD technology in the area of modern communication security. Also comprehensible theoretical lectures will allow to understand most important issues connected with this technology from a business and administration points of view.

After completing training session each participant will obtain a personal certification document issued by the organizing consortium LFPPI/NLTK/IPWUT/CompSecur, formally confirming acquired knowledge.

Invited speakers

Prof. Nicholas Gisin, Group of Applied Physics, University of Geneva, ID Quantique SA

Prof. Nicolas Gisin was born in Geneva, Switzerland, in 1952. After a post-doctoral degree at the University of Rochester, NY, in 1984 he joined a start-up company, Alphatronix, dedicated to fiber instrumentation for the telecommunication industry.

In 1988 an opportunity to join the Group of Applied Physics at the University of Geneva as head of the optics section brought him back to the academic life. At the time the optics section was mostly working on classical communication. Prof. Gisin invented the measurement technique for Polarization Mode Dispersion most widely used today. In the early 1990's Prof. Gisin started research in quantum optics. The main focus is to combine the group's broad expertise in optical fibers with a study of basic quantum effects. In 1993 his group demonstrated quantum cryptography under Lake Geneva.

In 2009 he received the first John S. Bell award for the demonstrations of long distance entanglement and quantum teleportation, together with his numerous contributions to the theory of Bell inequalities. His group is world leader in quantum communication. In 2001 he co-founded ID Quantique.

Prof. Artur Ekert, University of Oxford, National University of Singapore, Centre for Quantum Technologies Singapore

Prof. Artur Ekert (born in 1961 in Wrocław, Poland) is a Professor of Quantum Physics at the Mathematical Institute, University of Oxford, and a Lee Kong Chian Centennial Professor at the National University of Singapore and also the Director of CQT (Centre for Quantum Technologies). His research interests extend over most aspects of information processing in quantum-mechanical systems, with a focus on quantum communication and quantum computation. He is best known as one of the inventors of quantum cryptography.

Artur Ekert's research extends over most aspects of information processing in quantum-mechanical systems, with a focus on quantum cryptography and quantum computation. Building on the idea of quantum non-locality and Bell's inequalities he introduced entanglement-based quantum key distribution in his 1991 paper which generated a spate of new research that established a vigorously active new area of physics and cryptography, and is still the most cited paper in the field.

He is a recipient of several awards, including the 1995 Maxwell Medal and Prize by the Institute of Physics and the 2007 Royal Society Hughes Medal.

Prof. Vadim Makarov, University of Waterloo, Institute for Quantum Computing, Quantum Hacking Laboratory

Prof. Vadim Makarov (born in 1974 in Leningrad, currently St. Petersburg) is a widely acknowledged specialist in quantum hacking, a discipline which aims to find loopholes in imperfect physical implementations of otherwise theoretically unconditionally secure quantum cryptographic commercial systems. He is an author of the so called blinding attack on some commercial versions of QKD systems, allowing to take control over single photon detector by appropriately blinding it with a high intensity light and thus rendering QKD procedure effectively insecure (by eavesdropping of the exchanged symmetric key).

Prof. Vadim Makarov is currently supervising investigations of other possible attack classes on different imperfect QKD physical implementations by heading the Quantum Hacking Laboratory within the Institute of Quantum Computing at University of Waterloo, and is also additionally consulting leading quantum cryptography companies in patching their QKD systems against proven attacks.

Prof. Marek Kuś, Center for Theoretical Physics, Polish Academy of Sciences Warsaw, Head of Scientific Council of the National Quantum Information Center in Gdansk

Prof. Marek Kuś (born 1955 in Warsaw, Poland) is a Professor of Physics at the Center for Theoretical Physics of the Polish Academy of Sciences in Warsaw, Poland and the Head of Scientific Council of the National Quantum Information Center in Gdańsk, Poland. He obtained his Ph. D. degree from the Department of Physics of the University of Warsaw, Poland and continued his research as a post-doc and a visiting professor at universities in United States, Germany and France.

His scientific interests encompass quantum chaos and quantum information theory with a special emphasis on applications of algebraic and differential geometry to description of composite quantum systems and theory of entanglement.

Invited companies

AIT Austrian Institute of Technology

Safety and Security Department of AIT, one of the world-leading centers in development of entanglement based quantum cryptography. Austria's largest non-university research institute of public shareholders. The areas of research range from theoretical quantum information and the development of low level new algorithms for processing quantum keys, over the development of novel highly integrated quantum optical components to the development of key distribution networks and concepts for the integration into existing critical high security applications and infrastructures. Represented by: **Dr. Andreas Poppe**, AIT Austrian Institute of Technology, Safety and Security Department

ID Quantique SA

Leader in high-performance multi-protocol network encryption based on conventional and quantum technologies (Quantum Key Distribution QKD). Provider of optical instrumentation products, notably photon counters and related electronics. The company provides network security solutions and services to the financial industry, defence and government organizations and other enterprises globally. IDQ maintains close ties with leading academic institutions by participating to several Swiss and European R&D programs and plays a leading role in cutting-edge projects such as the SwissQuantum quantum key distribution testbed. IDQ offers a broad range of high-security layer 2 encryptors for high-speed networks up to 10Gbps. Represented by: **Dr. Grégoire Ribordy**, IDQuantique CEO

SeQureNet

SeQureNet brings to the market products relying on continuous variable quantum key distribution (CVQKD) in order to provide high security assurances for network services and practical applications. Building on the work done on continuous variables prototypes during SECOQC and SEQURE research projects, SeQureNet brings CVQKD to the market through software and hardware products and services. These are aimed both at the academic and the IT security usage; complete systems as well as building blocks for reseachers devising their own experiments are available. Represented by: **Dr. Sébastien Kunz-Jacques**, CTO and **Dr. Paul Jouguet**, R&D Engineer - CEO

MagiQ Inc.

One of the pioneering companies to commercialize QKD systems. Beyond QKD MagiQ areas of expertise include fiber optics, high-speed electronics and RF, acoustics, active feedback, FPGAs and software. MagiQ Research Labs provides custom products, design engineering, and contract research and development services for optics, quantum information, fiber sensing, aerospace and defense applications. MRL also contracts directly with private firms and government agencies such as the Navy, Army, DARPA, and NASA. Represented by: **Dr. Anton Zavriev**, Director of MagiQ Research Labs

NTT (The Nippon Telegraph and Telephone Corporation)

A Japanese telecommunications company headquartered in Tokyo, Japan. Ranked 29th in Fortune Global 500, NTT is the largest telecommunications company in the world in terms of revenue. The NTT Basic Research Laboratories conducts research in many different fields, inter alia nanotechnology, quantum information technology, quantum computers, quantum bits and quantum cryptography. NTT is taking a part in The Tokyo QKD network constructed in a part of the NICT open test-bed network "Japan Giga Bit Network 2 plus", inaugurated on 14th October 2010, together with project teams consisting of NICT, NEC, Mitsubishi Electric, Toshiba Research Europe, ID Quantique, the Austrian Institute of Technology, the Institute of Quantum Optics and Quantum Information and the University of Vienna. Represented by: **Dr. Kiyoshi Tamaki**, Quantum Optical State Control Research Group, NTT Basic Research Laboratories.

Toshiba (Toshiba Research Europe Ltd.)

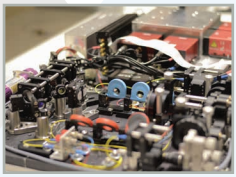
Toshiba is developing a new approach to information technology that applies the fundamental laws of Quantum Physics to network communications and computing. Toshiba is at the forefront of quantum information R&D and have developed one of the world's leading system for quantum cryptography. In parallel Toshiba creates the advanced nanotechnology required in future quantum information systems. Toshiba Research Europe Limited (TREL) is part of Toshiba's global R&D activity. The Cambridge Research Laboratory of TREL conducts research on quantum information technology, as well as speech recognition and synthesis. Represented by: **Dr. Andrew Shields**, Assistant Managing Director, Toshiba Research Europe Ltd.

Wrocław QKD network

Due to significant investments in Wrocław University of Technology laboratory equipment encompassing current state-of-the-art quantum cryptography technologies within the Polish National Quantum Technologies Laboratory NLTK network programme, as well as technological partnerships with internationally leading vendors of quantum cryptographic systems and national information security institutions and companies, city of Wroclaw now hosts a unique metropolitan quantum network research and development project.

An analysis of the backbone architecture of Wroclaw metropolitan network and its key nodes is carried out towards identifying connections of a highest potential in regard to securing with quantum cryptography (analysis includes classification of the threats on the particular nodes and the connection lines, technical characteristics of optical fibers connecting the backbone network nodes and levels of nodes importance from technical network, business and administration perspective).

National Quantum Technologies Laboratory NLTK, Wrocław University of Technology



Experimental and even early commercial QKD implementations are very susceptible to technical conditionings of the transmitting media (i.e. optical fiber infrastructure and associated alignment of the quantum optics) therefore deployment of QKD systems in real metropolitan optical fiber infrastructure network poses a challenge.

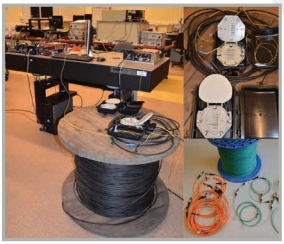
The optical infrastructure is determined by the city telecommunication canalization layout. Dark fibers connecting two, even not very distant metropolitan locations physically sharing an industry-standard telecom line with many parallel fibers (constituting the initial P2P topology and medium for QKD network) are divided in a series of thermally welded interconnections and junctions at telecom canalization crossings, which are main reason for decoherence and quantum signal losses, resulting with increased QBER and with infeasibility of key distribution in practical scenarios (this is specifically addressed to dark fiber infrastructure of metropolitan backbone telecom networks with multiple interconnections of telecommunication optical lines, which are implemented by thermal weldings – a connection between two locations separated by ca. 4-5 km distance, is usually divided by even several fiber weldings)

Research project:

- The project combines industrial and pre-deployment research over practical aspects of decoherence of qubits in quantum channels constituted by different types of optical fibers and standardized telecommunication optical connectors along with technological imperfections of qubit sources and detectors, which together stand as the most fundamental obstacles in practical applications of QKD towards realistic deployments in metropolitan networks combining both the no-entanglement and entanglement based QKD methods as implemented in the project laboratories by the no-entanglement IdQuantique Clavis II and the entanglement based Austrian Institute of Technology EPR Quelle QKD systems.
- The ongoing research programme includes technical characteristics and conditionings of the entangled and non-entangled qubits sources, channels and detectors for the experimental QKD systems, topological network configurations concepts, authentication problems, development of classical protocols stack responsible for the QKD key sifting, error correction and privacy amplification, network (hardware) and software integration interfaces and proper configuration towards deployment of experimental systems in metropolitan network environments.

Research programme:

- Technical conditioning of non-entangled and entangled quantum information carriers sources, and the possibilities to encode information in QKD systems (laser operation characteristics, parametric down conversion characteristics).
- Decoherence of quantum information carriers in different technical configurations of optical fiber telecommunication networks in non-entanglement and entanglement based QKD systems.
- Technical conditioning of quantum information carriers detection in non-entanglement and entanglement based QKD systems.
- Conditioning of topological configuration of non-entanglement and entanglement based QKD systems in realistic metropolitan fiber optics network environments.
- Quantum cryptographic session authentication problem for non-entanglement and entanglement based QKD systems.
- Development of QKD protocol stack (including classical algorithms of key reconciliation, error correction and privacy amplification) and interface systems.
- Evaluation of commercial backbone telecom networks deployment feasibility of non-entanglement and entanglement based QKD systems.
- Development of technical documentation for installation and configuration of the experimental QKD systems in commercial backbone telecom networks.



Research on QKD deployment in practical telecommunication network environments resulted in evaluation of boundary conditions for QKD feasibility versus quantum channel and transmission parameters and a successful resolution of channel quality problem by proper alignment of experimental QKD setups. The fiber optics line of the SMF28 standard has been used to test different connection and welding configurations for two R&D QKD approaches based on the IdQuantique Clavis2 setup (non-entanglement QKD, encoding qubits on interfering phase shifts of laser impulses in Mach-Zehnder interferometers) and the AIT Quelle setup (entanglement QKD, encoding qubits on polarizations of entangled photon pairs generated in non-linear PDC process in a BBO crystal). The main optics fiber line (single mode SMF28 standard) has been subsequently modified in laboratory test runs by welded or interconnected F3000/APC and FC/PC adapters. The interconnectors resulted with high QBER increases, thus favoring thermal welding which in proper proximity distribution were characterized by ca. 10 times lower loss induction than interconnectors (ca. 0.01 dB per welding, depending on the proximities). Next the industry standard telecom fiber optics line tests have been carried out towards welding and interconnections configuration optimizing in regard to QBER and conditioning of the metropolitan network deployment. Primary focus was directed towards the non-entanglement based setup which turned out to be operating properly with an acceptable raw key exchange rate (RKER) generating targeted amount of distilled secret bits (DSB) under laboratory simulation of real optic fiber backbone metropolitan network configuration with required optimization of interconnections and welding infrastructure. The entanglement based QKD has been tested for the first time in a real telecom network environment and proved to be also feasible but within a very narrow gap of optical elements alignment and poor (unpractical) values of QBER and RKER with high additional instability of operation parameters.

The 5th LFPPI Symposium Progress in Quantum Cryptography seQre2014

SCIENTIFIC COMMITTEE

- **Prof. LUCJAN JACAK**
  Head of LFPPI WUT Laboratory
  of Physical Foundations of Information Processing,
  Head of NLTK WUT National Laboratory for Quantum Technologies,
  Institue of Physics, Wrocław Universit of Technology
- **Prof. IRENEUSZ JÓŹWIAK**
  Head of Division of Security And Reliability of Computer Systems,
  Institute of Informatics,Wrocław University of Technology
- **Prof. JAN ZARZYCKI**
  Dean of the WUT Faculty of Electronics, Head of Signal Theory
  Department, Wrocław University of Technology
- **Prof. MAREK KUŚ**
  Head of Scientific Council of the National Quantum Information
  Center in Gdansk, Center for Theoretical Physics, Polish Academy of
  Sciences Warsaw
- **Prof. RYSZARD GONCZAREK**
  V-ce Dean of WUT Faculty of Fundamental Problems of Technology,
  Institue of Physics, Wrocław University of Technology

LOCAL ORGANISATION COMMITTEE

- **Dr. WITOLD JACAK**
  Institue of Physics, WUT (chairman)
- **Dr. WOJCIECH DONDEROWICZ**
  CompSecur
- **M. Sc. PRZEMYSLAW TOMCZAK**
  CompSecur
- **Dr. JACEK GRUBER**
  Institute of Informatics, WUT
- **Dr. ADAM GONCZAREK**
  Institute of Informatics, WUT
- **Dr. JANUSZ JACAK**
  Institue of Physics, WUT
- **M. Sc. DAMIAN MELNICZUK**
  NLTK, WUT

Symposium secretary:

- **M. Sc. MAŁGORZATA HAMBERG**
  NLTK, WUT
- **M. Sc. BEATA CZARKOWSKA**
  CompSecur

ORGANIZERS

|LFPPI⟩ Laboratory of Physical Foundations of Information Processing

The Laboratory of Physical Foundations of Information Processing is a Polish scientific network under Committee of Science, which groups about 20 Polish Scientific Institutions, that undertake active research in scope of quantum information.

CompSecur IT Solutions

CompSecur is an academic WUT spin-off profiled in IT security. The company is accredited by PARP National Agency in scope of IT security services and has implemented R&D projects in cooperation with WUT in quantum cryptography practical deployment.

Wrocław University of Technology

National Laboratory for Quantum Technologies

The National Laboratory for Quantum Technologies, NLTK (Polish national network of state of the art quantum university laboratories) was created by the initiative of the National Center for Research and Development in cooperation with the LFPPI. NLTK consortium is implementing a large research infrastructure programme in context of quantum technologies, including especially quantum optics laboratory equipment. NLTK at Institute of Physics WUT includes state-of-the-art Quantum Cryptography Laboratory that consists of prototype QKD devices and commercially available R&D systems.

HONORARY PATRONAGE

Prof. Tadeusz Więckowski
Rector of Wroclaw University of Technology

Dr. Rafał Dutkiewicz
Mayor of the City of Wroclaw

Prof. Krzysztof Kurzydłowski
Director of The National Center
for Research and Development

MEDIA PATRONAGE

Scientific American Świat Nauki
IDG International Data Group Poland SA
Wiedza i Życie
Gazeta Bankowa
Hack.pl
niebezpiecznik.pl
CareerCon
Czasopismo Zabezpieczenia

INSTITUTIONAL PATRONAGE

Polskie Towarzystwo Fizyczne 1920
Polskie Towarzystwo Informatyczne
EITCI
Instytut Rozwoju Społeczeństwa Informacyjnego
ISSA
PIIT

http://www.seqre.net/seqre2014