EIT Digital – Industrial PhD position proposal

PhD thesis information

PhD Thesis – Title		The cryptographic applications of quantum communication
PhD Thesis – Short summary	Max 100 words	Quantum key distribution (QKD) is a disruptive technology that enables provably secure transmission of information on a protocol level by replacing the hard problem based cryptographic public key exchange protocols with others relying only on the principles of quantum mechanics. The goal of the candidate is to propose new protocols that can improve the achievable key rate, distance, and security of the QKD transmission while it also enables scalability and real world deployability. This should be done with studying and evaluating the various free space and optical cable based methods, experimenting with real systems if possible.
Rationale/challenge – *describe the problem and why it is relevant*	Max 200 words	The currently used public key exchange methods will be soon obsolete as quantum computer algorithms that can break them are already developed. Post-quantum cryptography mitigates this issue with basin the algorithms on even harder problems. Hard problem based cryptography always relies on mathematical assumptions. QKD relies on quantum mechanics therefore it is a technology that can be used to establish a secret key-pair between the communicating parties, securely by the law of physics. Also with today's technology the key exchange itself cannot be recorded and stored for the long term for an attacker to perform measurements on quantum states in the future. Information successfully encrypted based on QKD will remain secure forever. (This cannot be said for RSA or any other post quantum method.) However, in its current state QKD faces challenges in terms of • Scalability • Transmission distance and efficiency • Price of technology • Massive deployment is the goal is to build a proof of concept prototype which device can by answering these challenges.
Innovation – *describe what is the intended solution and the advance w.r.t. the state-of-the-art*	Max 250 words	The goal of this thesis is to research and develop new techniques and protocols that are capable of solving the aforementioned issues. There are different methods how the information can be encoded in a QKD system which determines for example the detection techniques, price of the used technology and, in case of some of the protocols the level of security. While secuirty is provable for a technique, it lacks the promise of scalability and efficient key rate, while others work over larger distances but not provably secure. However, making security proofs for more scalable concepts reamains an untapped realm for most of the scenarios.

Research focus/topics – *describe <u>how</u> you are going to solve the problem*	Max 200 words	The first step is prototyping and studying a state-of-the-art QKD device, while at the same time adding new improvements and afterwards testing it in comprehensive simulation scenarios potentially in real networks. The simulation results will also provide valuable feedback to the design of the concepts and algorithms. The scenarios will be based on real industry use-cases by putting emphasis on deployability of the concepts. The solutions should achieve compatibility with the current network to minimize additional modification costs. Solving these problems will require intensive cooperation with Ericsson and possibly with other European University research groups. The goal of this research is to create a scalable QKD device that is applicable in real world scenarios. These solutions could become the backbone of next generation secure networks.
Deadlines/milestones (Gantt chart)	M6	• Finish the newly built state-of-the art QKD device • Start testing and simulation phase.
	M12	• Publish a concept paper at an international conference • Implementation of prototype in real network use case, simulations to be run in Ericsson labs
	M24	• Analysis of the concept in comprehensive simulations. • Make concepts on deployability and scalability taking into account industrial plans and constraints through strong interaction with Ericsson business and manufacturing teams. • Map potential costumers and use cases, how the product could be merchandised
	M36	• Optimization of the algorithms, real world verification • Compare different approaches, which method complements a real networks use case the best, in terms of scalability, performance and security • Finalize the Proof of Concept • The evaluation is done in cooperation with Ericsson and should cover all main aspects of deploying the solutions in real next-generation networks • Publish the findings in a journal paper.
	M48	Summarize the results and complete the PhD thesis.
Expected outcome – *describe the expected results of the PhD*	Max 100 words	The expected results of the PhD are new solutions to enable and leverage cooperative quantum key distribution solutions in Next-generation networks and thus improve security, performance and efficiency. The results shall include: • Working, verified prototype of new concepts • Detailed analysis of the impact on network performance and deployment considerations • Published papers describing the findings in high-quality academic journals • Potential patents, working in close cooperation with Ericsson Hungary

Relevance for the Action Line (section to be filled out by the Action Line Leader)

Action Line	AL	Digital Infrastructures
Alignment with Action Line – *statement from the Action Line Leader indicating the relevance for the AL from his perspective*	Max 150 words	The topic of cybersecurity is indeed part of the focus area of the Action Line. Devising new methods for encryption like Quantum key distribution that might withstand Quantum computers is indeed desirable. It would be very nice if the PhD student would participate in potential future IAs with investigations, workshops and similar.
Relevant IA – *List any relevant Innovation Activity (if applicable)*	Max 100 words	Currently we have no Innovation Activities dealing with this kind of encryption but we have several projects dealing cybersecurity.

Partnership/financial information

Action Line Leader	Name	
Industrial partner	Name	Ericsson Hungary Ltd.
Industry advisor – *name and short bio*	Max 100 words	Benedek Kovacs, PhD, Senior Specialista at Ericsson. MSc in Information Technology (2005) and PhD in Mathematics (2012), working for Ericsson from 2005. Solid knowledge in Telecommunications, networking and 5G networks. Studied quantum information technology during his MSC and now leading quantum technology related projects at Ericsson.
Academic/research partner		Budapest University of Technology and Economics (BME)
Academic/research supervisor – *name and short bio*	Max 100 words	Prof. Sándor Imre [M'93] Head of Dept. of Networked Systems and Sevices at the Budapest University of Technology (BME). He obtained dr. univ. degree in in probability theory and statistics 1996, Ph.D. degree in 1999 and DSc degree from the Hungarian Academy of Sciences in 2007. He is chairman of Telecommunication Scientific Committee of Hungarian Academy of Sciences. He was invited to join the Mobile Innovation Centre as R&D director in 2005. His research interests include mobile and wireless systems, quantum computing and communications. Especially he has contributions on different wireless access technologies, mobility protocols and their game theoretical approaches, reconfigurable systems, quantum computing based algorithms and protocols.
HEI granting the title		Budapest University of Technology and Economics (BME)
DTC location	Node	Budapest
Geographical mobility plan		KTH Royal Institute of Technology
No. of PhD positions	[#]	1
PhD duration	[#years]	3 years
Co-funding percentages: - Industry	[%]	20%
- Academia	[%]	30%
- EIT Digital	[%]	50%