Physics and Security - from Random Numbers to Secure Communication

806. WE-Heraeus-Seminar

05 – 08 March 2024

at the Physikzentrum Bad Honnef/Germany

WILHELM UND ELSE HERAEUS-STIFTUNG

Introduction

The Wilhelm und Else Heraeus-Stiftung is a private foundation that supports research and education in science with an emphasis on physics. It is recognized as Germany's most important private institution funding physics. Some of the activities of the foundation are carried out in close cooperation with the German Physical Society (Deutsche Physikalische Gesellschaft). For detailed information see https://www.we-heraeus-stiftung.de

Aims and scope of the 806. WE-Heraeus-Seminar:

The fields of cryptography and quantum physics have seen major leaps forward in the past 50 years. Cryptographic methods, such as asymmetric key-agreement and signatures using elliptic curves have been developed, which are now potentially endangered by a possible quantum computer. Therefore, crypto-systems which are assumed to be "quantum-secure" are at the focus of current cryptographic research. In parallel, the foundations of quantum mechanics are nowadays the base for developments in quantum technologies – a field which promises to secure messages, which are – in theory – guaranteed by the laws of physics, and not the assumption of a certain mathematical complexity. However, the security of real-world and wide-spread implementation of such methods still has to be proven.

This workshop addresses young quantum physicists who work on modern quantum technologies to understand the basics of information theory, number theory and cryptography. Similarly, the workshop addresses young researchers in information theory and computer science to understand the basics of quantum mechanics and the underlying physics which might endanger their crypto-systems or not.

Scientific Organizers:

Prof. Dr. Ilja Gerhardt, Leibniz Universität Hannover
E-mail: ilja.gerhardt@physics.uni-hannover.de

Dr. Manfred Lochter, Bundesamt für Sicherheit in der Informationstechnik, Bonn
E-mail: manfred.lochter@bsi.bund.de

M.Sc. Ömer Bayraktar, Max Planck Institute for the Science of Light, Erlangen
E-mail: oemer.bayraktar@mpl.mpg.de

Introduction

Administrative Organization:

Dr. Stefan Jorda
Martina Albert

Wilhelm und Else Heraeus-Stiftung
Kurt-Blaum-Platz 1
63450 Hanau, Germany

Phone +49 6181 92325-14
Fax +49 6181 92325-15
E-mail albert@we-heraeus-stiftung.de
Internet: www.we-heraeus-stiftung.de

Venue:

Physikzentrum
Hauptstraße 5
53604 Bad Honnef, Germany

Conference Phone +49 2224 9010-120

Phone +49 2224 9010-113 or -114 or -117
Fax +49 2224 9010-130
E-mail gomer@pbh.de
Internet: www.pbh.de

Taxi Phone +49 2224 2222

Registration:

Reception Office
Tuesday (16:00 - 20:30 h) and Wednesday morning

Program

Program (CET)

Tuesday, 05 March 2024

16:00 – 20:30	**Registration**	
From 18:30	*BUFFET SUPPER*	

Wednesday, 06 March 2024

08:00	*BREAKFAST*	
08:55 – 09:00	Scientific Organizers	**Welcome and Opening**
09:00 – 09:45	Renato Renner	**Quantum Advantage in Random Number Generation**
09:45 – 10:30	Torsten Schütze	**Binning, Generalized von Neumann and XOR, von Neumann Procedure – Digitization and Mathematical Post-processing in (Q)RNGs**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 11:45	Werner Schindler	**An Overview of AIS 20/31**
11:45 – 12:15	Mohamed Bourennane	**More than One Bit Quantum Randomness Certification and Expansion**
12:15 – 12:50	Joshua Bienfang	**Physical Random Number Generators: Practice and Pitfalls**
12:50 – 13:00	**Conference photo**	
13:00	*LUNCH*	
14:15 – 15:00	Elisabeth Oswald	**Explainable Side-Channel Leakage Assessments**
15:00 – 15:45	Carlos Abellan	**Entropy Monitoring: From Bell Tests to Products**
15:45 – 16:00	Stefan Jorda	**About the Wilhelm and Else Heraeus Foundation**

Program (CET)

Wednesday, 06 March 2024

16:00 – 16:30	*COFFEE BREAK*
16:30 – 17:30	**Panel Discussion 1** (Moderator: Norbert Lütkenhaus)
17:30 – 18:30	**Poster Flash Talks**
18:30	*HERAEUS DINNER* (social event with cold & warm buffet and complimentary drinks)
19:30 – 22:00	**Poster Session 1 & Discussions**

Program (CET)

Thursday, 07 March 2024

08:00	*BREAKFAST*	
09:00 – 09:45	Roger Colbeck	**Device-independent QKD with Arbitrarily Small Non-locality**
09:45 – 10:30	Tobias Hemmert	**QKD Security from BSI's Perspective**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 11:45	Paolo Villoresi	**Quantum Communications for Distant Interlocutors**
11:45 – 12:15	Esther Hänggi	**Security from Noise: The Wiretap Channel**
12:15 – 13:00	Christian Kurtsiefer	**Experimental Quantum Randomness - One Practical and One Not so Practical Approach**
13:00	*LUNCH*	
14:15 – 15:00	Michael Rosenbluh	**Chaotic Laser based Random Bit Generation**
15:00 – 15:45	Antonio Acin	**Randomness of Quantum States and Measurements**
15:45 – 16:00	Nicolas Spethmann	**Technology Transfer in Quantum Communication – The Umbrella Project Quantum Communication Germany (SQuaD)**
16:00 – 16:30	*COFFEE BREAK*	
16:30 – 17:15	Dagmar Bruss	**Quantum Conference Key Agreement**
17:15 – 17:45	Pepijn Pinkse	**Hardware Security for Quantum Authentication, Authenticated Quantum Communication and Quantum Computing**
17:45 – 18:30	Joppe Bos	**Post-Quantum Cryptography: The Embedded Challenge**
18:30	*DINNER*	
19:30	**Poster Session 2 & Discussions**	

Program (CET)

Friday, 08 March 2024

08:00	*BREAKFAST*	
09:00 – 09:45	Johanna Sepúlveda	**Demystifying Quantum-secure Communications: From Devices to Systems**
09:45 – 10:30	Christoph Marquardt	**Practical Aspects of Quantum Key Distribution in Space and on Ground**
10:30 – 11:00	*COFFEE BREAK*	
11:00 – 11:30	Pascal Kobel	**Random in Space - Quantum Cryptography and Randomness**
11:30 – 12:00	Viktor Fischer	**PLL-TRNG - Past, Present, and Future**
12:00 – 12:45	Norbert Lütkenhaus	**Security Statements for Practical QKD**
12:45– 13:15	**Panel Discussion 2** (Moderator: René Schwonnek)	
	Scientific organizers	**Poster Prize Awards & Closing Remarks**
13:15	*LUNCH*	

End of the seminar and departure

Posters

Poster Session 1, Wednesday, 6 March, 19:30 h (CET)

1	Tim Achenbach	CHSH inequalities are just linear isomorphisms between squares
2	Jennifer Bartlett	Mitigating Detection Asymmetry-Induced Excess Noise in LLO-Based CV-QKD
3	Jonas Berl	Continuous-Variable Quantum Key Distribution over Varying Operating Distances
4	Justus Christinck	The testbed for single-photon sources and detectors at PTB
5	Erdem Eray Cil	Continuous-Variable Quantum Key Distribution: Streamlining Information Reconciliation Hardware Efficiency
6	Daan de Ruiter	Time-domain Physical Unclonable Keys using Integrated Photonics
7	Christian Deppe	Semantic Security for Quantum Wiretap Channels
8	Lukas Eisemann	Current Challenges in Post-Processing for CV-QKD
9	Manuel Erhard / Max Riegler	From QKD Security Proofs to Certification: An Industrial Perspective
10	Mehrzad Firoozi + Maximiliane Weishäupl	Gain-Switching in Phase Noise Quantum Random Number Generators: An Experimental and Stochastic Analysis
11	Ilija Funk	Daylight Free-Space Quantum Key Distribution Utilizing the Sodium D2 Line

Poster Session 1, Wednesday, 6 March, 19:30 h (CET)

12	Soham Ghosh	Existential Unforgeability from Quantum Physical Unclonable Functions based on Random Measurement
13	Rodrigo Gómez	Entanglement-based quantum communication on a real-world fiber link between Jena and Erfurt
14	Zeshan Haider	Implementation of QKD BB84 Protocol in QisKit
15	Kiara Hansenne	Certifying the topology of quantum networks
16	Muhammad Imran	Quantum Random Number Generators (QRNGs): Theoretical and Experimental Investigation
17	Zhehui Kong	Effect of background noise in Continuous Variable Quantum Key Distribution from Space
18	Gereon Koßmann	Optimizing the relative Entropy under linear constraints
19	Seid Koudia	From Classical to Quantum Network Coding: Entanglement and Quantum Key Distribution in Quantum Networks
20	Manuel Kraft	Driving Innovation and Technology
21	Emma Medlock	Characterisation of a satellite-to-ground CV-QKD channel
22	Iyán Méndez Veiga	randExtract: a Reference Library to Test and Validate Privacy Amplification Implementations

Poster Session 2, Thursday, 7 March, 19:30 h (CET)

23	Fynn Otto	Achievable state transformations under rotational invariance
24	Karolina Paciorek	Optimization of high-dimensional QKD for deployment on a 1.7 km free-space link
25	Matej Pivoluska	Design trade-offs for QKD protocols based on numerical keyrate evaluation
26	Stefan Richter	A versatile fiber-coupled DM-CV-QKD system for the QuNET initiative
27	Stefan Röhrich	Usage of Hardware Random Number Generators
28	Karolina Schatz	Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link
29	Sebastian Schlösser	Refining classical protocols for transmitting quantum systems
30	Jan Schreck	Towards experimental implementation of a continuous-variable quantum key distribution scheme with unidirectional modulation of squeezed states
31	Rene Schwonnek	Optimizing the relative entropy under semi definite constraints - A new tool for estimating key rates in QKD
32	Philipp Sohr	Taking quantum key distribution from fundamental science to certified systems in space
33	Christopher Spiess	Robust Time Transfer with Single Photons on Hybrid Quantum Communication Scenarios in Fiber and Free-Space
34	Guilherme Stein	On measuring quantum noise

Poster Session 2, Thursday, 7 March, 19:30 h (CET)

35	Yagana Syed	Exploring the Bell Polytope experimentally
36	Dion Timmermann	The Marketing of and Education about Quantum Random Number Generators
37	Pablo Vazquez	Security of a commercial entanglement-based QKD system
38	Hüseyin Vural	A rack-integrated optical sender module for the feasibility study of CV-QKD in a mobile optical link during a flight campaign
39	Henning Weier	Quantum key distribution receiver with countermeasures against implementation attacks
40	Matthias Widmann	Room-Temperature NV-Based Quantum Computing: Pathways to Commercialization, Technological Progress, and Emerging Challenges
41	Jerome Wiesemann	Towards the certification of quantum key distribution systems
42	Ramona Wolf	Device-independent randomness amplification

Abstracts of Lectures

(in alphabetical order)

Entropy monitoring: from Bell tests to products.

W. Amaya[1], J. Martinez[1], G. Senno[1], M.W. Mitchell[2,3] and C. Abellan[1]

[1]Quside Technologies S.L., C/Esteve Terradas 1,Of. 305, 08860 Castelldefels, Spain
[2]ICFO – Institut de Ciències Fotòniques, The Barcelona Insitute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[3]ICREA – Institució Catalana de recerca i Estudis Avançats, 08010 Barcelona, Spain
E-mail: cabellan@quside.com

Random numbers are fundamental in many applications, including cryptography, high-performance computing, or online gaming. Quantum random number generators (QRNGs) have been developed due to their potential superior quality and the ability to rigorously measure conditional min-entropy bounds. In this talk, we will review progress in the implementation of photonic QRNGs based on the phase-diffusion process and their conditional min-entropy estimation in various device implementations.

Any real QRNG device is subject to noise and imperfections. The idea of applying metrology concepts to randomness generators was first introduced in 2014 [1]. It was then applied to the RNG devices that were used in the 2015 loophole-free Bell tests [2]. One of the main novelties was to account for multiple noise sources and factor them in the min-entropy estimation process, as for instance digitization noise, a highly non-linear effect that can have a material effect on the unpredictability of a QRNG.

In 2015, excess predictabilities below 2×10^{-4} were achieved, even when paranoidly considering the potential combination of different noise sources. Using a gate-level hardware implementation of a randomness extractor, random bits were delivered in about 26 ns. In 2022, a new loophole-free Bell test with superconducting qubits was realized, and the timing budget for randomness generation was tighter than in 2015. A new RNG hardware architecture was proposed [3], combining 8 parallel entropy sources and cascaded randomness extraction, which allowed for reduction of the freshness time to about 17 ns with conditional min-entropies above 5.2×10^{-6}.

In production-grade environments, engineering limitations apply, including restricted measurement resources and a time limit to derive conditional min-entropy bounds. Additionally, it is of practical relevance that this quality estimation is realized on-the-fly, when the device is working in operational conditions. Today, Quside QRNG products implement various min-entropy estimation techniques, observing min-entropy bounds above 90% and obtained digitally in a few seconds with no manual intervention.

References

[1] M. W. Mitchell et al., Phys. Rev. A 91, 012314 (2015)
[2] C. Abellan et al., Phys. Rev. Lett. 115, 250403 (2015)
[3] S. Storz et al., Nature 617, 265-270 (2023)

Randomness of quantum states and measurements

Antonio Acín, ICFO

It is usually said that quantum physics contains an intrinsic form of randomness with no classical analogue, but what does this exactly mean? And how can this intrinsically quantum randomness be detected and quantified? The talk first introduces a framework for quantum randomness certification and highlights its differences with existing (classical) approaches. We then focus on two simple and fundamental questions: first, given a quantum state, how much randomness does it contain? That is, what's the maximum amount of randomness that can be extracted from it by performing a measurement? The second question looks at the other side of the problem: given a quantum measurement, how much randomness it can generate by applying it to a quantum state?

References

[1] Gabriel Senno, Thomas Strohm, and Antonio Acín, *Quantifying the Intrinsic Randomness of Quantum Measurements*, Phys. Rev. Lett. 131, 130202 (2023).
[2] Shuyang Meng, Fionnuala Curran, Gabriel Senno, Victoria J. Wright, Máté Farkas, Valerio Scarani, Antonio Acín, *Maximal intrinsic randomness of a quantum state*, arXiv:2307.15708.

Physical Random Number Generators: Practice and Pitfalls

J.C. Bienfang[1]

[1]*National Institute of Standards and Technology, Gaithersburg, MD, United States of America*

Turning the oft-cited dictum “God does not play dice” on its head and using the physical measurement of some convenient quantum state as a random bit generator (RBG) is broadly appealing and provides a compelling argument for why the source should be trusted, at least in theory. In practice implementing such sources of random bits is fraught with technical challenges as potential pitfalls that all too often can be swept under the rug with a little bit of post processing. We discuss practical aspects of random bit generators based on physical processes. We discuss design criteria and common pitfalls in their implementation and give some colorful examples of RBGs that have exhibited some issues. We also present the design, implementation and performance of a simple low-latency RBG used as entropy sources in loophole-free Bell tests [1], tests whose latency requirements preclude any post-processing.

References

[1] Lynden K. Shalm et al. Phys. Rev. Lett. **115**, 250402 (2015)

Post-Quantum Cryptography: The Embedded Challenge

Joppe W. Bos[1]

[1]*NXP Semiconductors, Interleuvenlaan 80, 3001 Leuven, Belgium*

Post-quantum cryptographic standards are coming: it doesn't matter if you believe in quantum computers or not. What is the impact of these new public-key algorithms on the billions of embedded devices as used in automotive or the Internet of Things (IoT)? Using some typical *embedded* use-cases we outline the challenges and show some recent solutions in this area.

References

[1] J. W. Bos, B. Carlson, J. Renes, M. Rotaru, A. Sprenkels and G. P. Waters: *Post-quantum secure boot on vehicle network processors*. 20th escar Europe - The World's Leading Automotive Cyber Security Conference, 2022.

[2] J. W. Bos, J. Renes and A. Sprenkels: *Dilithium for Memory Constrained Devices*. Africacrypt, LNCS, vol. 13503, pp. 217-235, Springer, 2022.

[3] J. W. Bos, M. Gourjon, J. Renes, T. Schneider and C. van Vredendaal: *Masking Kyber: First- and Higher-Order Implementations*. Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2021, Issue 4, pp. 173-214, IACR, 2021.

[4] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe and D. Stehlé: *CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM*. IEEE European Symposium on Security and Privacy - Euro S&P, pp. 353-367, IEEE, 2018

More than one bit quantum randomness certification and expansion

M. Bourennane

Department of Physics, Stockholm University

One of the striking properties of quantum mechanics is the occurrence of the Bell-type non-locality. They are a fundamental feature of the theory that allows two parties that share an entangled quantum system to observe correlations stronger than possible in classical physics. In addition to their theoretical significance, non-local correlations have practical applications, such as device-independent randomness generation, providing private unpredictable numbers even when they are obtained using devices delivered by an untrusted vendor. Thus, determining the quantity of certifiable randomness that can be produced using a specific set of non-local correlations is of significant interest. First, we present an experimental realization of recent Bell-type operators designed to provide private random numbers that are secure against adversaries with quantum resources. We use semi-definite programming to provide lower bounds on the generated randomness in terms of both min-entropy and von Neumann entropy in a device-independent scenario. Our results demonstrate the first experiment that certifies close to two bits of randomness from binary measurements of two parties. Apart from single-round certification, we provide an analysis of finite-key protocol for quantum randomness expansion using the Entropy Accumulation Theorem. Second, we present an efficient and practical method for certifying quantum randomness using generalized measurements. Indeed, we have derived a method for self-testing the presence of POVMs. We present the certification of more than one bit of min-entropy from a single POVM on one of the qubits of an entangled state using a variant of the elegant Bell inequality. We also obtain more than one bit of randomness in a prepare and measure scenario of a similar structure with a POVM on a single qubit. We provide numerical simulations to demonstrate the effectiveness of our randomness certification and expansion.

Quantum Conference Key Agreement

Federico Grasselli, Hermann Kampermann, Glaucia Murta, and Dagmar Bruß

Institute for Theoretical Physics III, Heinrich-Heine-University Düsseldorf, Germany

Establishing a common secret random key between more than two parties is referred to as conference key agreement (CKA). This talk provides an overview of some recent results for quantum conference key agreement (QCKA), where quantum properties are used to provide a secure conference key [1]. Note that QCKA goes beyond a mere generalisation of quantum key distribution between two parties, as some intricate new features arise in the security analysis.

The role of multipartite entanglement for QCKA will be discussed [2], and finite-size corrections to the secure conference key rate will be analysed [3]. For device-independent QCKA, a new type of multipartite Bell inequality is introduced [4]. When a suitable source for multipartite entanglement is available, QCKA offers a speed-up in certain quantum networks with bottlenecks [5].

References

[1] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, *Quantum Conference Key Agreement: A Review*, arXiv:2003.10186, Special issue "Advancing quantum technologies - chances and challenges" of Advanced Quantum Technologies, Wiley, Weinheim.

[2] G. Carrara, H. Kampermann, D. Bruß, and G. Murta, *Genuine multipartite entanglement is not a precondition for secure conference key agreement*, Phys. Rev. Research **3**, 013264 (2021).

[3] F. Grasselli, H. Kampermann, and D. Bruß, *Finite-key effects in multi-partite quantum key distribution protocols*, New J. Phys. **20**, 113014 (2018).

[4] T. Holz, H. Kampermann, and D. Bruß, *A Genuine Multipartite Bell Inequality for Device-Independent Conference Key Agreement*, Phys. Rev. Research **2**, 023251 (2020).

[5] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, *Multi-partite entanglement can speed up quantum key distribution in networks*, New J. Phys. **19**, 093012 (2017).

Device-independent QKD with arbitrarily small non-locality

Lewis Wooltorton[1,2], Peter Brown[3] and Roger Colbeck[1]

[1]Department of Mathematics, University of York, York, UK
[2]Quantum Engineering Centre for Doctoral Training, University of Bristol, Bristol, UK
[3]Télécom Paris - LTCI, Inria, 19 Place Marguerite Perey, 91120 Palaiseau, France

In standard QKD schemes, the security proof makes assumptions about how the devices used in the protocol operate. If real-world devices deviate from these assumptions then the security proof does not apply to them, and this could lead to possible hacking attacks (indeed, such attacks have been implemented, see, e.g. [1]). The aim of device-independence (DI) is to remove the need for assumptions on the workings of the quantum devices. In essence the protocol verifies that the devices must be working sufficiently well as it runs, and aborts if not. Importantly, this verification relies only on the classical input-output behaviour of devices.

Device-independence relies on observing non-local correlations (i.e., on violating a Bell inequality), and a natural question arises whether non-locality is sufficient for DI-QKD. In [2] it was shown that for typical DI-QKD protocols nonlocality is not sufficient: there are non-local correlations from which are impossible to use for DI-QKD using typical protocols. This might suggest that there is a minimum bound on the nonlocality required for DI-QKD. However, in recent work [3] we show that there is no such bound: there exist correlations with arbitrarily low non-locality from which arbitrarily good key can be generated device-independently.

In my talk I will give an introduction to device-independence, outlining the main ideas behind it before briefly discussing the relation between DI-QKD and nonlocality including the new result of [3].

References

[1] I. Gerhardt et al., Nature Communications **2**, 349 (2011)
[2] M. Farkas et al., Physical Review Letters **127**, 050503 (2021)
[3] L. Wooltorton, P. Brown and R. Colbeck, arXiv:2309.09650

PLL-TRNG - Past, Present, and Future

V. Fischer[1]

[1]*Hubert Curien Laboratory, Jean Monnet University, Saint-Etienne, France*

Field Programmable Gate Arrays (FPGAs) are used very often to implement cryptographic systems, which include most of the time also random number generators (RNGs). The main challenge related to the implementation of a generator generating truly random numbers inside FPGAs and other logic devices is that the physical source of randomness, such as jittered clock generator, is implemented in the logic area, i.e. in the close vicinity of noisy running algorithms, which can have significant impact on generated numbers or even serve to attack the generator. The significant advantage of using phase-locked loops (PLLs) as a source of randomness for the generator is their physical isolation from the rest of the device, rendering them practically independent from other activities.

The first PLL-based TRNG (PLL-TRNG) was presented at the conference *Cryptographic Hardware and Embedded Systems (CHES)* in 2002 [1]. The stochastic model of the generator was presented in the journal *Tatra Mountain Mathematical Publications* in 2010 [2]. The first embedded tests dedicated to the PLL-TRNG and based on its stochastic model were published in the journal *it - Information Technology* in 2019 [3].

In this talk, we will first present the principle of the PLL-based TRNG and discuss its main characteristics. Next, we will talk about its new enhanced stochastic model and corresponding dedicated embedded tests as presented at the last CHES conference [4]. Finally, we will present some perspectives of our future research.

References

[1] V. Fischer, and M. Drutarovský, True Random Number Generator Embedded in Reconfigurable Hardware. Cryptographic Hardware and Embedded Systems (CHES), Redwood Shore, USA, LNCS No. 2523, Springer, Berlin, Germany, 2002, pp. 415-430 (2002)

[2] F. Bernard, V. Fischer, and B. Valtchanov, Mathematical Model of Physical RNGs Based on Coherent Sampling, Tatra Mountains Mathematical Publications, Vol**.** 45, pp. 1-14 (2010).

[3] V. Fischer, F. Bernard, and N. Bochard, Modern random number generator design – Case study on a secured PLL-based TRNG, it - Information Technology, Vol. 61, Issue 1, pp. 3 - 13 (2019).

[4] V. Fischer, F. Bernard, N. Bochard, Q. Dallison, and M. Skórski, Enhancing Quality and Security of the PLL-TRNG, IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2023, No. 4, pp. 211–237 (2023).

Security from noise: the wiretap channel

E. Hänggi[1] and I. Méndez Veiga[1, 2] and L. Wang[1]

[1]Lucerne School of Information Technology, Lucerne University of Applied Sciences and Arts, Rotkreuz, Switzerland

[2] Institute for Theoretical Physics, ETH Zurich, Zurich, Switzerland

The wiretap channel - first studied by Wyner (1) and Csiszár and Körner (2) in the 1970's - reaches information-theoretic security based on noise in the communication channel. Its security proof always needs to make assumptions about the form of the channel to the adversary. Unlike in quantum key distribution (3), (4) these assumptions cannot be tested by the honest parties, but only be physically justified.

We discuss under which physical conditions the wiretap channel can reach security (5) and how these conditions are similar or different from the ones in quantum key distribution. We then explain an efficient protocol to implement secure communication over the wiretap channel (6).

Finally, we report on our recent work on this topic (7):So far, the security analysis of the wiretap channel has focused on identical repetitions of memoryless channels. We generalize this to the more realistic scenario where the channel may change over time or even be influenced by the adversary. We also raise some open questions about a quantum version of the wiretap channel and how the wiretap channel be combined with quantum key distribution.

References

1. *The wire-tap channel.* **Wyner, Aaron D.** 8, 1975, The Bell System Technical Journal, Vol. 54, pp. 1355-1387.

2. *Broadcast channels with confidential messages.* **Csiszár, Imre and Körner, János.** 3, 1978, IEEE Transactions on Information Theory, Vol. 24, pp. 339-348.

3. *Quantum cryptography: Public key distribution and coin tossing.* **Bennett, Charles H. and Brassard, Gilles.** 1984. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing.

4. *Quantum cryptography based on Bell's theorem.* **Ekert, Artur K.** 6, 1991, Physical Review Letters, Vol. 76, pp. 661--663.

5. *Quantum keyless private communication versus quantum key distribution for space links.* **Vázquez-Castro, Ángeles and Rusca, Davide and Zbinden, Hugo.** 1, 2021, Physical Review Applied, Vol. 16, p. 014006.

6. *Semantic security for the wiretap channel.* **Bellare, Mihir and Tessaro, Stefano and Vardy, Alexander.** 2012. Advances in Cryptology - CRYPTO 2012. pp. 294-311.

7. **Hänggi, Esther, and Méndez Veiga, Iyán and Wang, Ligong.** *Security for Adversarial Wiretap Channels.* 2023.

QKD Security from BSI's Perspective

Tobias Hemmert[1]

[1]*Federal Office for Information Security, Bonn, Germany*

Quantum Key Distribution is often said to offer security based on the principles of quantum mechanics, setting it apart from classical key agreement schemes whose security is based on mathematical complexity assumptions. However, this statement can only refer to the theoretical security of a QKD protocol proven in a theoretical model. As for any cryptographic device, numerous other aspects need to be taken into consideration in order to have confidence in the security of a concrete QKD product. From the perspective of BSI as the Federal Cyber Security Authority in Germany, this talk explains what is required and what is still missing in order to obtain trustworthy QKD products.

The theoretical security of the implemented QKD protocol is a key aspect of the security of a QKD device. Over the past years, a lot of progress has been made on security proofs that quantify the level of security offered by QKD protocols. The talk will outline some of the requirements that QKD protocols and proofs should satisfy. This includes standardization of QKD protocols.

Even if a QKD protocol has been proven secure in a theoretical model, flaws or properties of the physical devices used to implement such a protocol can lead to vulnerabilities and enable attacks. Besides attacks on the classical IT components used in QKD products, such devices may allow attacks which exploit imperfections in the QKD-specific components such as photon detectors. The talk will present some of the results of a technical report on this subject that has recently been published by BSI [1].

Finally, QKD devices need to be rigorously evaluated in order to obtain confidence in their security, including both the theoretical security of the underlying QKD protocol and implementation security. The talk will outline some of the processes that can provide assurance about the security properties of IT security products, including QKD products.

References

1. BSI: Implementation Attacks against QKD Systems (2023), https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html

Random in Space - Quantum Cryptography and Randomness

P. Kobel[1], J. Janusch[1], M. Hutterer[1], W. Boxleitner[2], V. Duarte[1], C. Gohle[1] and N. Lemke[1]

[1]OHB System AG, Weßling, Germany
[2]Austrian Institute of Technology, Vienna, Austria

Satellite-based quantum key distribution (QKD) offers a paradigm-changing solution to the key distribution problem, enabling a new way of provably secure communication, especially over long distances [1]. In this context, cryptographically secure random number generators are an essential building block for secure systems. In this talk, we present the development of space-qualified quantum random number generators (QRNGs) at OHB, which we are advancing in several projects according to individual needs. From the many different quantum mechanical effects that can be used to build a QRNG [2,3], we present an approach that combines simplicity, cost efficiency, chip integrability, and high generation speed [4].

References

[1] N. Lemke et al., Luft- und Raumfahrt **2** (2022)
[2] A. Fine. PRL **48**, 291-295 (1982)
[3] X. Ma et al., npj Quantum Information **2,** 16021 (2016)
[4] H. P. Yuen, V. W. S. Chan, OPTICS LETTERS **8,** 177 (1983)

Experimental quantum randomness - one practical and one not so practical approach

Christian Kurtsiefer[1]

[1]*Centre for Quantum Technologies and Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543, SINGAPORE*

In this presentation, I review two of our approaches to generate randomness from quantum measurements: One practical approach, based on an optical homodyne measurement with a very lean optical setup [1], and another very complicated one, based on a loophole-free Bell measurement from a down-converted photon pair source [2].

References

[1] Yicheng Shi, Brenda Chng, Christian Kurtsiefer, Applied Physics Letters **109**, 041101 (2016), with a more practical approach

[2] Lijiong Shen, Jianwei Lee, Le Phuc Thinh, Jean-Daniel Bancal, Alessandro Cerè, Antia Lamas-Linares, Adriana Lita, Thomas Gerrits, Sae Woo Nam, Valerio Scarani, Christian Kurtsiefer, Phys. Rev. Lett. **121**, 150402 (2018).

Security Statements for Practical QKD

Norbert Lütkenhaus

Institute for Quantum Computing

Department of Physics and Astronomy

University of Waterloo

Waterloo, ON, Canada

Security statements about practical Quantum Key Distribution (QKD) implementations have two aspects: the mathematical security proof given the detailed protocol assuming model assumptions implementation devices, and the implementations security, which relates to deviations and testing of actual devices with respect to the model assumptions to develop confidence levels about the actual device implementation.

It is the goal of this presentation to clarify the status of both of these aspects and to discuss the final security statements we can make about actual implementations of QKD devices.

References

[1] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. 94, 025008 (2022)

[2] A. Winick, Norbert Lütkenhaus, P.J.Coles, Reliable numerical key rates for quantum key distribution, Quantum 2, 77 (2018)

[3] Open QKD Security Project http://openqkdsecurity.wordpress.com

[4] C. Marquardt et al, Implementation Attacks against QKD Systems, White Paper available at https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html

Explainable Side-Channel Leakage Assessments

E. Oswald[1]

[1]University of Birmingham, Birmingham, UK, and
University of Klagenfurt, Klagenfurt, AT

In this talk I will explain how to capture the concept of “explainability” (in the task of identifying side channel leakage in cryptographic implementations) in a statistical manner, so that concrete tests can be constructed that not only detect leakage, but also help to find its root cause. Along the way, I will recap the threat of side channels to cryptographic implementations, and the state of the art of attacks and countermeasures.

References

[1] S. Gao and E. Oswald, A Novel Framework for Explainable Leakage Assessment, Eurocrypt 2024 (to appear)

[2] S. Gao and E. Oswald, A Novel Completeness Test for Leakage Models and Its Application to Side Channel Attacks and Responsibly Engineered Simulators, Eurocrypt 2022: 254-283

Hardware Security for Quantum Authentication, Authenticated Quantum Communication and Quantum Computing[F]

Pepijn W.H. Pinkse[1]

[1] *MESA+ Institute for Nanotechnology, University of Twente, 7500AE Enschede, The Netherlands*

In this contribution I will report about our results in the areas of quantum authentication, authenticated communication and secure quantum information processing.

A physical unclonable function (PUF) is a unique physical key which cannot be physically copied with existing technology. Multiple-scattering samples form good optical PUFs. We have demonstrated authentication by quantum-secure optical readout of a PUF [1] and more recently, we have devised a quantum communication scheme based on PUFs [2]. In order to investigate the limits of state-of-the-art nanofabrication techniques, we started making multiple-scattering media by direct laser writing. A new class of PUFs we realize in the form of complex ring resonator networks implemented in integrated photonic circuits. They allow to be read-out at a distance through a single-mode telecommunication fiber.

For the purpose of achieving and exploiting a quantum advantage for computational tasks, scalable multiphoton interference with extreme programmability and ultralow loss is required. We believe the best way for that purpose is large-scale integrated photonics, which we are pursuing together with UT spin-off Quix Quantum. A programmable integrated photonic processor [3] recently allowed us to demonstrate quantum thermodynamics [4], an indistinguishability witness [5]. Finally, we will sketch a project with as goal to realize and demonstrate the QEnclave idea put forward by Kaplan, Kashefi and others [6].

References

[1] S. A. Goorden, *et al.*, Optica **1**, 421 (2014).
[2] R. Uppu *et al.*, Quantum Sci. Tech. **4**, 04501 (2019).
[3] C. Taballione *et al.,* ArXiv 2203.01801
[4] F.H.B. Somhorst *et al.*, Nat. Commun. **14**, 3895 (2023).
[5] R. van der Meer *et al.*, arXiv: 2112.00067
[6] Yao Ma, *et al.,* npj Q Inf. **8**, 128 (2022)

Quantum Advantage in Random Number Generation

Renato Renner

ETH Zurich, Zurich, Switzerland

In this talk, I will address the question to what extent Quantum Random Number Generators (QRNGs) are superior to devices that produce randomness based on classical physics, such as a Roulette wheel or hardware RNGs that draw entropy from thermal fluctuations. It is sometimes argued that there cannot be any fundamental difference between the two, for even the outcome of apparently classical devices ultimately depends on quantum processes.

To answer the question, I will introduce a criterion that allows us to assess the quality of randomness in a way relevant to applications, e.g., in cryptography. One may then apply this criterion to the different methods to produce randomness. The conclusion is that QRNGs provide a clear-cut advantage compared to any classical means of randomness generation.

Chaotic Laser based Random Bit Generation

Michael Rosenbluh

Bar-Ilan University, Physics Department, Ramat Gan, Israel

Random bit generation is essential for many applications. It is at the core of cryptographic encoding and communications and quantum key distribution as well as Monte Carlo simulations, learning algorithms in artificial intelligence applications and gambling and lottery applications. In the applications where there is also a need for security, the generation of the random bits based on an algorithmic protocol (known as a pseudo random sequence), even if the algorithmic seed is truly random provides a potential security loophole since the knowledge of the seed can lead to a totally predictable random sequence. In these situations there is a need for a true, physically based method for generating the random sequence. In addition, there is often a need for high speed generation of the random bits as the information being encrypted is generally very large, such as images or videos.

In recent years a very fast method of generating true random bits based on chaotic lasers has been developed and promises to provide a source of truly random bits at THz bit generation rates. In this presentation I will review the methods used in chaotic laser random bit generation, present current state of the art methods and results and provide some intriguing possibilities for privately sharing the random bit sequence between legitimate partners or in a predefined network. I will briefly discuss the method of checking the randomness of the bit sequence and compare it to optical quantum random bit generation methods.

An overview of AIS 20/31

W. Schindler

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn, Germany

Strong random number generators (RNGs) are essential for cryptographic applications.

The BSI evaluation guidelines for random number generators, AIS 20 and AIS 31, have been effective in the German Common Criteria certification scheme for over 20 years, last updated in 2011. The mathematical-technical reference, usually referred to as "AIS 20/31" for short, has been under revision. The final document will be published soon.

AIS 20/31 distinguishes between deterministic RNGs, physical RNGs and non-physical true RNGs. AIS 20/31 is technology neutral. Instead of approved designs, functionality classes are defined. Security requirements are specified that RNGs shall fulfil in order to comply. A central feature of AIS 20/31 is that the evaluation of a physical RNG requires a stochastic model, which allows the verification of a lower entropy bound for the outputted random numbers. Effective online tests and total failure tests are also needed.

In this talk key features and innovations of the revised AIS 20/31 are explained. The focus will be on physical RNGs.

Binning, Generalized von Neumann and XOR, von Neumann procedure – Digitization and mathematical post-processing in (Q)RNGs

Torsten Schütze

Rohde & Schwarz *SIT GmbH, Stuttgart*

torsten.schuetze@rohde-schwarz.com

In past QRNG workshops, an overview about common post-processing methods in True Physical Random Number Generators has been given. There exists a rich theory, but all / most methods are considered for *independent and identically (iid) distributed* bits. So, we all know, that for iid and biased bits, the (Generalized) von Neumann procedure removes the bias completely, while pairwise XOR *only* leads to quadratic damping.

In this contribution, we talk about our experiences with well-known digitization and post-processing methods in case of dependencies and perturbations. All results reported are from practical RNG evaluations, when things aren't going so well.

Specifically, we consider binning – equidistant subdivision of the cumulative distribution function – as a means for getting from normally distributed sample values to uniformly distributed numbers. Another method to go from an almost arbitrary, but independent, distribution of sample values to uniformly distributed bits working with differences of consecutive, but non-overlapping pairs of sample values is the Generalized von Neumann procedure. We illuminate both methods in case of perturbations, e.g., non-exact normal distributions. Binning as well as Generalized von Neumann procedure can be considered as part of the digitization process.

When we have already independent and identically distributed bits that still have a small bias $\epsilon \coloneqq P(b_j = 1) - 0.5$, then known mathematical post-processing techniques come into play as there are: XOR, von Neumann anti-biasing procedure, Peres / Generalized von Neumann procedure, length of runs methods, optimal XOR constructions, resilient functions, etc. We applied two of them, namely XOR with two or four bits and von Neumann procedure, to real data. Unfortunately, these data showed under some environmental conditions some dependencies, characterized by a higher correlation coefficient.

In theory, for biased, but otherwise iid bits, the von Neumann procedure should outperform the XOR of two or four bits. In practice, with correlation, we saw satisfactory results for XOR with four bits, only.

Unfortunately, the exact probability distribution of the XOR of two or four bits is not easy to calculate exactly, even in the case of one-step dependent Bernoulli experiments.

Demystifying quantum-secure communications: from devices to systems

Johanna Sepúlveda

Airbus Defence and Space, Taufkirchen, Germany

Public-key cryptography (PKC) is the basis of the secure connectivity. It relies on the hardness of factoring large integers (RSA) or computing discrete logarithms (ECC). However, the advent of quantum computers put classical cryptography at risk. Classical PKC will be broken in polynomial time. To ensure long-term communication security, quantum-secure solutions resistant to classical and quantum attacks are required. Currently there are two quantum-secure technologies: Post-Quantum Cryptography (PQC), based on alternative mathematical problems; and Quantum-Key-Distribution (QKD), leveraging on physics laws. Each technology has different security properties and it is envisioned that they work together in quantum-secured environments. The development of QKD and PQC has the potential to revolutionize cryptography and improve the security of defence applications. This talk will describe the quantum secure technologies as well as their challenges and opportunities into their deployment in real life applications.

References

[1] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press.

[2] N. I. of Standards and Technology, “Announcing request for nominations for public-key post-quantum cryptographic algorithms,” 2016

[3] Airbus Secure Communications, “Towards a better approach for Quantum-Key-Distribution (QKD) Networks key management“, April 2023, [Online], Available: https://securecommunications.airbus.com/ en/news/quantum-key-distribution-qkd-networks-key-management

[4] D. Marchsreiter and J. Sepulveda, “Hybrid post-quantum enhanced tls 1.3 on embedded devices,” in 2022 25th Euromicro Conference on Digital System Design (DSD), 2022, pp. 905–912.

[5] Fritzmann, T., Sigl, G., & Sepúlveda, J. (2020). RISQ-V: Tightly Coupled RISC-V Accelerators for Post-Quantum Cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 239–280. https://doi.org/10.13154/tches.v2020.i4.239-280

[6] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, “Efficient decoy-state quantum key distribution with quantified security,” 2013.

[7] M. M. Douglas Stebila, “Post-quantum key exchange for the internet and the open quantum safe project,” In Roberto Avanzi, Howard Heys, editors, Selected Areas in Cryptography (SAC) 2016, LNCS, vol. 10532, pp. 1–24. Springer, Oct. 2017. [Online]. Available: https://openquantumsafe.org

[8] J. R. Andreas Hülsing, “Xmss reference code, rfc 8391.” [Online]. Available: https://github.com/XMSS/xmss-reference

Quantum Communications for Distant Interlocutors

Marco Avesani, Costantino Agnesi, Elisa Bazzani, Tommaso Bertapelle, Federico Berra, Matia Bolanos, Lorenzo Coccia, Alberto De Toni, Massimo Giacomin, Ilektra Karakosta-Amarantidou, Matteo Padovan, Francesco Picciariello, Andrea Pompermaier, Edoardo Rossi, Mattia Sabatini, Francesco Santagiustina, Davide Scalcon, Andrea Stanco, Francesco Vedovato, Kannan Vijayadharan,

Giuseppe Vallone and Paolo Villoresi

QuantumFuture Research Group
Padua Quantum Technologies Research Center, Dept. Information Engineering,
University of Padua – Padova, Italy
paolo.villoresi@unipd.it

The quantum communications at long distances are described, from the suitable choice of the photons' degree of freedom to the scheme to encode them, to the peculiarities of the channels.
In particular, Space Quantum Communications require dedicated quantum devices suitable for the harsh environmental conditions and with enhanced performances.
Suitable solutions for advanced payload are presented, including record low noise qubit generators and synchronization methods.
Moreover, the developments of Quantum Communications require dedicated quantum devices suitable for the specific environmental conditions and with enhanced performances.

1. Vallone, G. et al. Experimental Satellite Quantum Communications. Phys. Rev. Lett. 115, 040502 (2015).
2. Vallone, G. et al. Interference at the Single Photon Level Along Satellite-Ground Channels. Phys. Rev. Lett. 116, 253601 (2016).
3. Vedovato, F. et al. Extending Wheeler's delayed-choice experiment to space. Sci. Adv. 3, e1701180 (2017).
4. Avesani, M., Marangon, D. G., Vallone, G. & Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nat. Commun. 9, 5365 (2018).
5. Avesani, M. et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 7, 93 (2021).
6. Avesani, M. et al. Resource-effective quantum key distribution: a field trial in Padua city center. Opt. Lett. 46, 2848 (2021).
7. Agnesi, C. et al. Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder. Optica 7, 284 (2020).

Abstracts of Posters

(in alphabetical order)

CHSH inequalities are just linear Isomorphisms between squares

T. Achenbach[1] **and M. Plávala**[1]

[1]*Universität Siegen, Siegen, Germany*

We interpret POVMs as maps from quantum states to column stochastic matrices, which implies that a behavior in a simple Bell type experiment corresponds to the maximal tensor product of sets of *2x2*-column stochastic matrices. We additionally consider the dual of this set and demonstrate that these two sets form convex cones embedded in ordered vector spaces, generated by squares. This enables us to show that linear isomorphisms between those two squares correspond to CHSH inequalities. Similar ideas yield to other fundamental results about steering and Bell nonlocality.

Mitigating Detection Asymmetry-Induced Excess Noise in LLO-Based CV-QKD

J. Bartlett[1] and R. Kumar[1]

[1]School of Physics, Engineering and Technology, and York Centre for Quantum Technologies, University of York, UK.

Continuous Variable Quantum Key Distribution (CV-QKD) is a promising alternative to Discrete Variable (DV) QKD due to its capacity for higher key rates at shorter distances [1]. Unlike single photon-based DV-QKD, CV-QKD operates on the amplitude and phase quadrature's of the electromagnetic field and therefore enables the transmission of higher-dimensional information [2]. Not only this, but CV-QKD also allows for an easy network implementation due to its superior compatibility with existing infrastructure [3].

In recent years, practical implementation of CV-QKD protocols has adopted the Local-local oscillator (LLO) based architecture, in which the transmitter, Alice, and the receiver, Bob, use independent lasers for the generation and the detection of CV-QKD signals [4]. For Bob, it is necessary to establish a common measurement phase reference, with Alice, for correlating the measured and transmitted quadrature information [5].

In this poster, we will discuss the asymmetry due to non-uniform detection gains, in the amplitude and phase quadrature measurements and its impact on the phase reference estimation error and secure key generation rate. We will also propose methods for mitigating the detector asymmetry-induced phase estimation error in CV-QKD.

References

[1] Laudenbach, F. et al. (2018) 'Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations', Advanced Quantum Technologies, 1(1). doi:10.1002/qute.201800011.

[2] Hajomer, A.A. et al. (2022) 'Modulation leakage-free continuous-variable quantum key distribution', npj Quantum Information, 8(1). doi:10.1038/s41534-022-00640-1.

[3] Luo, W. et al. (2023) 'Recent progress in quantum photonic chips for quantum communication and internet', Light: Science & Applications, 12(1). doi:10.1038/s41377-023-01173-8.

[4] Hajomer, A.A. et al. (2024) 'Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator', Science Advances, 10(1). doi:10.1126/sciadv.adi9474.

[5] Marie, A. and Alléaume, R. (2017) 'Self-coherent phase reference sharing for continuous-variable quantum key distribution', Physical Review A, 95(1). doi:10.1103/physreva.95.012316.

Continuous-Variable Quantum Key Distribution over Varying Operating Distances

Jonas Berl[1,2], Erdem Eray Cil[2], Tobias Fehenberger[1] and Laurent Schmalen[2]

[1]Adva Network Security GmbH, Berlin, Germany
[2] Karlsruhe Institute of Technology, Karlsruhe, Germany

Continuous-variable quantum key distribution (CV-QKD) is a promising candidate for post-quantum cryptosystems as it is envisioned to be compatible with commercial off-the-shelf optical components. A highly challenging part of CV-QKD is the information reconciliation step that is required to correct the errors between Alice's and Bob's correlated data. For the high channel loss of long-haul CV-QKD operations, the forward error correction (FEC) scheme must be heavily optimized to achieve the necessary reconciliation efficiencies for positive secret key rates. In practice, however, QKD-enabled network topologies exhibit a wide range of operating distances between adjacent QKD nodes, necessitating a reconciliation scheme that can be adjusted to varying operating distances. In this contribution, we compare different approaches to realize distance-adaptive reconciliation. These include the use of a set of fixed-rate FEC codes [1], exploiting trusted noise and trusted loss [2] to match a fixed-rate code with the observed channel loss, and the use of a rate-adaptive code [3,4]. We show through numerical simulations that state-of-the-art rate-adaptive coding schemes and exploiting trusted noise and loss outperform fixed-rate FEC codes.

References

[1] K. Gumus and L. Schmalen, “Low Rate Protograph-Based LDPC Codes for Continuous Variable Quantum Key Distribution,” in 2021 17th International Symposium on Wireless Communication Systems (ISWCS), Berlin, Germany.

[2] F. Laudenbach and C. Pacher, “Analysis of the Trusted‐Device Scenario in Continuous‐Variable Quantum Key Distribution,” Adv Quantum Tech, vol. 2, no. 11, p. 1900055, Nov. 2019.

[3] C. Zhou, X. Wang, Z. Zhang, S. Yu, Z. Chen, and H. Guo, “Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes,” Sci. China Phys. Mech. Astron., vol. 64, no. 6, p. 260311, Jun. 2021.

[4] H. Yang, S. Liu, S. Yang, Z. Lu, Y. Li, and Y. Li, “High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution,” Phys. Rev. A, vol. 109, no. 1, p. 012604, Jan. 2024.

The testbed for single-photon sources and detectors at PTB

J. Christinck[1]

[1]Physikalisch-Technische Bundesanstalt, Braunschweig, Germany

Secure communication relies on many different aspects, e.g., the detection of photons. In quantum communication, single-photon sources and detectors are widely used. The metrological aspect of these systems is investigated in ‘quantum radiometry’ or ‘photon-based radiometry’. In the long term, single-photon sources might be used as standard sources.

At PTB, Germanys national metrology institute, many different types of single-photon emitters are investigated for their suitability for application in quantum radiometry and quantum communication. These are, e.g., semiconductor quantum dots, single molecules, color centers in diamond.

Only single-photon detectors such as single-photon avalanche diode (SPAD) detectors are suitable in the low photon-flux regime. PTB performs calibrations of the detection efficiency of SPAD detectors as a metrological service. More advanced systems like superconducting nanowire single-photon detectors (SNSPDs) and transition-edge sensors (TES) are currently investigated in research projects.

Here, an overview of single-photon sources and detectors at PTB is given. An exemplary radiometric application of a germanium-vacancy center in diamond under a microfabricated solid immersion lens is shown. The germanium-vacancy center was used for the calibration of the detection efficiency ratio of two SPAD detectors and the results compared to the standard method using attenuated laser light.

Continuous-Variable Quantum Key Distribution: Streamlining Information Reconciliation for Hardware Efficiency

E. E. Cil and L. Schmalen

Communications Engineering Lab, KIT, Karlsruhe, Germany

The information reconciliation (IR) step is critical in continuous-variable quantum key distribution (CV-QKD) systems, as it determines the efficiency of raw key material generation from quantum information shared between two parties, commonly referred to as Alice and Bob. While various low-density parity-check (LDPC) codes have been proposed for IR, hardware (HW) implementation for long-distance CV-QKD remains a challenge. This is primarily due to the performance degradation caused by HW simplifications, which in turn reduces the secret key rate, and the prohibitive memory requirements for IR in HW, making long-distance CV-QKD unfeasible. Consequently, GPU-based IR schemes are commonly employed, although they are suboptimal for commercial CV-QKD systems.

To address these issues, we present two novel approaches for HW-implemented IR steps in long-distance CV-QKD. The first approach introduces an iteration-dependent scaled min-sum decoding algorithm for low-rate LDPC codes, which achieves near-sum product algorithm (SPA) performance with significantly reduced complexity, thereby enabling a more practical HW implementation [1]. The second approach proposes a novel log-log domain SPA for LDPC code decoding, specifically tailored for key reconciliation in CV-QKD systems. This algorithm notably decreases the fractional bit-width required for decoder messages, resulting in lower memory consumption during HW implementation. Our findings demonstrate that this algorithm not only achieves decoding accuracy comparable to or exceeding that of the SPA but also reduces the fractional bit width by at least 25%, offering a more efficient solution for HW-based IR in commercial CV-QKD systems [2].

References

[1] E. Eray Cil and L. Schmalen, "Iteration-dependent scaled min-sum decoding for low-complexity key reconciliation in CV-QKD," Proc. Opt. Fiber Commun. Conf. (OFC), San Diego, CA, USA, Mar. 2024, http://arxiv.org/abs/2312.12118S.

[2] E. Eray Cil and L. Schmalen, "Log-log domain sum-product algorithm for information reconciliation in continuous-variable quantum key distribution," Proc. Conf. Inform. Sciences Syst. (CISS), Princeton, NJ, USA, Mar. 2024, https://arxiv.org/abs/2401.13748.

Semantic Security for Quantum Wiretap Channels

Holger Boche[1], Minglai Cai[1], Christian Deppe[2], Roberto Ferrara[1], Moritz Wiese[1]

[1]Technical University of Munich, Munich, Germany
[2] Technical University of Braunschweig, Braunschweig, Germany

We consider the problem of semantic security via classical-quantum and quantum wiretap channels and use explicit constructions to transform a non-secure code into a semantically secure code, achieving capacity by means of biregular irreducible functions. Explicit parameters in finite regimes can be extracted from theorems. We also generalize the semantic security capacity theorem, which shows that a strongly secure code guarantees a semantically secure code with the same secrecy rate, to any quantum channel, including the infinite-dimensional and non-Gaussian ones.

References

[1] Boche, Holger; Cai, Minglai; Deppe, Christian; Ferrara, Roberto; Wiese, Moritz: Semantic security for quantum wiretap channels. Journal of Mathematical Physics 63 (9), 2022, 092204

Time-domain Physical Unclonable Keys using Integrated Photonics

D.J. de Ruiter[1] , D.P. Stellinga[1], M.C. Velsink[1], L. van der Hoven[1] and P.W.H. Pinkse[1]

[1]MESA+ Institute for Nanotechnology, University of Twente, Enschede, The Netherlands

The security of conventional public-key cryptosystems makes assumptions about the inversion of certain computations being infeasibly hard. If these assumptions prove to be wrong, notably for instance through the construction of a sufficiently strong quantum computer, then the security of such cryptosystems would be compromised. Instead, physical unclonable keys (PUKs) are physical objects with a particular challenge-response behaviour which is highly specific to its physical construction, and whose construction is sufficiently complex that it is completely infeasible to either create an accurate copy of the key, or to emulate its challenge-response behaviour. Previous work has found optical scattering media to be a promising candidate for PUK behaviour. However, this approach is inherently limited to short distances. In this work, we design photonic integrated circuits with the aim of providing scattering behaviour in the time domain instead of the spatial domain, allowing for the challenges and responses to be transported over a single spatial mode, such as a fibre-optic cable. Additionally, we consider the integration of such keys in schemes for authentication and secure messaging. These schemes incorporate single-photon states of light, which enables quantum-secure authentication through the no-cloning principle of quantum mechanics.

A compact, fiber-coupled DM-CV-QKD receiver for the QuNET initiative

S. Richter[12], H. Vural[12], L. Eisemann[12], J. Schreck[12] and C. Marquardt[12]

[1] Chair of Optical Quantum Technologies, Institute of Optics, Information and Photonics, FAU Erlangen-Nürnberg, Erlangen, Germany
[2] Max Planck Institute for the Science of Light, Erlangen, Germany

Quantum key distribution is an important tool for establishing provably secure shared secret keys between distant parties over untrusted communication channels. This is a crucial part of the ongoing efforts to provide future-proof cryptography resistant to the growing threat posed by next-generation quantum computers. Due to its compatibility with classical optical communications, continuous-variable quantum key distribution (CV-QKD) is well positioned for providing this essential function in short- to mid-range metropolitan fiber networks.

We present a prototype of a versatile CV-QKD receiver based on double balanced homodyne measurements with a transmitted local oscillator laser. It is capable of shot-noise limited detection of quantum states with a bandwidth of up to 500MHz, with automated routines for input polarization optimization and regular re-calibration. We show details of the implementation and our proposed solutions for some of the technical challenges associated with shot-noise limited coherent communication, like signal offset estimation and phase recovery. Asymptotic keyrate estimates are discussed as a performance metric, with a focus on the additional constraints imposed on CV-QKD protocols by the available error correction implementions.

From QKD Security Proofs to Certification: An Industrial Perspective

M. Erhard[1], M. Pivoluska[1], M. Riegler[1], P. Sohr[1], S. Ecker[1], R. Solar[1], T. Scheidl[1], P. Daly[2], H. Weier[2], F. Tiefenbacher[3], R. Ursin[3]

[1]Quantum Technology Laboratories GmbH, Vienna Austria

[2]Quantum Space Systems, Munich Germany

[3]Quantum Industries GmbH, Vienna Austria

Developing a unified approach to security and trust for quantum key distribution (QKD) systems necessitates collaboration across the entire ecosystem. This includes users, academic partners, industry players, security accreditation authorities, national security agencies, standardization organizations, and certification bodies.

In our talk, we would like to give an insight of the status and view of this joint effort to establish a holistic framework for QKD systems:

1. Defining Secrecy and Correctness:
Establish a standardized, mathematically rigorous definition of secrecy and key correctness, such as an "epsilon parameter" or "security parameter," to enable objective assessment.

2. Ensuring Protocol Security:
Create comprehensive and transparent documentation detailing the assumptions underlying the mathematical security proofs of QKD protocols. This documentation should encompass a complete mathematical proof, tracing the derivation from the security definition to the expected final secure key rate.

3. Bridging the Gap between Theory and Actual Implementation:
Recognize that the theoretical security of QKD hinges on the validity of the underlying assumptions. It is crucial to evaluate the degree to which the "protocol security proof" aligns with the actual physical implementation. Standardized evaluation tests are deemed essential for rigorous assessment.

4. Standardization for Comparability:
Standardize the methodologies employed in QKD security proofs to ensure comparable security parameters across different systems. This facilitates direct comparisons and informed decision-making.

5. Enabling Certification:
Create a network of independent and accredited certification bodies equipped with the requisite expertise and technical resources to objectively evaluate QKD systems based on the established framework.

Collaboration and shared commitment are critical to achieving this crucial objective. By working together, we can build a robust and trustworthy foundation for the widespread adoption of QKD, unlocking its potential to revolutionize secure communication.

Gain-Switching in Phase Noise Quantum Random Number Generators:
An Experimental and Stochastic Analysis

Mehrzad Firoozi[1], Maximiliane Weishäupl[2],

René Kirrbach[3], Fabian Klingmann[4]

[1,3,4] Fraunhofer IPMS, Dresden, Germany
[2] University of Regensburg, Regensburg, Germany

True random numbers constitute a widely sought-after ingredient for enabling new methods and technologies in information security, data processing and simulations. Random number generators driven by quantum events such as vacuum fluctuations or phase diffusion in a laser diode have gained great attraction due to their performance, stochastic modelability, and potential for miniaturisation. However, there still exist open challenges concerning both theoretical models and hardware constructions for fulfilling the promise of true random number generation by quantum mechanics.

We consider two alternative gain-switched (GS) phase-noise QRNGs, utilizing (a) a single beam splitter [1] and (b) balanced photodetection, respectively. Each of these setups is compared to its continuous-wave counterpart, and to a conventional gain-switched phase noise QRNG based on an unbalanced Mach-Zehnder interferometer and standard photodetection [2].

For benchmarking, we generate both experimental and numerical data, which are then analyzed and compared by using statistical methods including probability plots and distribution tests.

References

[1] Jie Yang, Jinlu Liu, Qi Su, Zhengyu Li, Fan Fan, Bingjie Xu, and Hong Guo, "5.4 Gbps real time quantum random number generator with simple implementation," Opt. Express 24, 27475-27481 (2016)

[2] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express 22, 1645-1654 (2014)

Daylight Free-Space Quantum Key Distribution Utilizing the Sodium D_2 Line

Ilija Funk[1], Yagana Syed[1] and Ilja Gerhardt[1]

[1]Institut für Festkörperphysik (Leibniz University Hannover), Hannover, Germany

Quantum key distribution is a promising pathway to secure communication in the future. Currently, quantum communication channels usually are realized through a fiber or a free-space network. While the latter offers much longer transmission distances of hundreds of kilometers compared to fiber links, it suffers from reduced transmission rates during daytime due to increased detection noise from sunlight.

To circumvent this problem, we propose a free-space link based on entangled photon pairs with a wavelength of 589 nm. This wavelength coincides with the sodium D_2 line which is one of the most prominent Fraunhofer lines. Hence during daytime, the reduced amount of sunlight at this wavelength should allow for an improved transmission rate. Our research project includes the creation of entangled photon pairs at 589 nm, setting up a free-space link over several kilometers using telescopes, and demonstrating quantum key distribution using the BBM92 protocol. We report on our latest progress.

Existential Unforgeability from Quantum Physical Unclonable Functions based on Random Measurement

Soham Ghosh*, Vladlen Galetsky*, Christian Deppe† and Roberto Ferrara*
*Technical University of Munich
†Technical University of Braunschweig

Physical unclonable functions (PUFs) are hardware structures in a physical system (e.g. semiconductor, crystals etc.) that are used to enable unique identification of the semiconductor or to secure keys for cryptographic processes. A PUF thus generates a noisy secret reproducible at runtime. This secret can either be used to authenticate the chip, or it is available as a cryptographic key after removing the noise. Latest advancements in the field of quantum hardware, in some cases claiming to achieve quantum supremacy, highly target the fragility of current RSA type classical cryptosystems. As a solution, one would like to develop Quantum PUFs to mitigate such problem. There are several approaches for this technology. In our work we compare these different approaches and introduce the requirements for QTOKSim, a quantum token based authentication simulator testing its performance on a multi-factor authentication protocol. [Ško10; DKD+21; GGD+22].

References

[DKD+21] Mina Doosti, Niraj Kumar, Mahshid Delavar, and Elham Kashefi. "Client-Server Identification Protocols with Quantum PUF". In: *ACM Transactions on Quantum Computing* 2.3 (2021). ISSN: 2643-6809. DOI: 10.1145/3484197. URL: https://doi.org/10.1145/3484197.

[GGD+22] Vladlen Galetsky, Soham Ghosh, Christian Deppe, and Roberto Ferrara. "Comparison of Quantum PUF models". In: *2022 IEEE Globecom Workshops (GC Wkshps)*. 2022, pp. 820–825. DOI: 10.1109/GCWkshps56602.2022.10008722.

[Ško10] Boris Škorić. "Quantum Readout of Physical Unclonable Functions". In: *Progress in Cryptology – AFRICACRYPT 2010*. Ed. by Daniel J. Bernstein and Tanja Lange. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 369–386. ISBN: 978-3-642-12678-9.

Entanglement-based quantum communication on a real-world fiber link between Jena and Erfurt

R. Gómez[1,2], U. Chandrashekara[1,2], C. Spiess[1,2], F. Steinlechner[1,2]

[1] Fraunhofer Institute for Applied Optics and Precision Engineering IOF, Albert-Einstein-Straße 7, 07745 Jena, Germany
[2] Institute of Applied Physics, Abbe Center of Photonics, Friedrich Schiller University Jena, Albert-Einstein-Straße 6, 07745 Jena, Germany

There are several ongoing efforts to demonstrate Quantum Key Distribution (QKD) in practical settings. These efforts involve protocols such as BB84 and twin-field QKD. However, there are still challenges to overcome in establishing practical QKD networks, including dispersion and polarization compensation, clock synchronization, and improving detector detection rates. One particular area of interest is entanglement based QKD networks, which rely on protocols like BBM92. These networks offer the added benefit of security through entanglement, and the measurement of correlation among photon pairs provides information about potential attackers. In this report, we discuss our ongoing efforts to develop inter-city QKD networks using practical and efficient entangled photon sources (EPS) that operate at telecom wavelengths. Our EPS design is based on the auto-balancing double beam-displacer source design and is compact enough to fit in a 30cm x 30cm breadboard. Our EPS achieves high visibilities (>99%) and high entangled pair rates (>8 million pairs per second per mW of pump power), with a heralding efficiency of over 48%. The source is broadband, making it suitable for use with wave division multiplexers to improve transmission quality and increase the number of receivers for entangled photon pairs. We have successfully utilized the EPS in a QKD network spanning approximately 75km of dark fibers between the cities of Jena and Erfurt. Initial results show entanglement transmission of over 4,000 coincidences per second. We have also made progress in dispersion, polarization compensation, and real-time data processing, which paves the way for establishing a functional QKD network between Jena and Erfurt.

References

[1] R. Horn, T. Jennewein, Optics Express, 27 017369 (2019).
[2] S. Wengerowsky, S.K. Joshi, F. Steinlechne, H. Hübel and R. Ursin. Nature 564, 225–228 (2018).
[3] E. Brambila, R. Gómez, R. Fazili, M. Gräfe, and F. Steinlechner, Opt. Express 31, 16107-16117 (2023).

Implementation of QKD BB84 Protocol in QisKit

Muhammad Haroon Saeed, Hassan Sattar, Muhammad Hanif Durad, and Zeshan Haider

National Institute of Lasers and Optronics College, Pakistan Institute of Engineering and Applied Sciences, Nilore, Islamabad 45650, Pakistan

Quantum cryptography is a practical method of secret communication that guarantees the foolproof secrecy. This study presents the simulation for implementation of a Quantum Key Distribution (QKD) protocol BB84, the pioneering, and most basic and fundamental protocol. We use the quantum computing platform developed by IBM named as Qiskit for the simulation of the BB84 protocol, implementing it with and without an Eve eavesdropper for studying the relative outcomes. Recently, Qiskit is globally very popular for quantum simulations because it provide us the opportunity to simulate quantum logic circuit on classical computer as well as real quantum computers owned by IBM. As per our best knowledge, there is no any proposal published for quantum circuit by anyone for BB84 QKD. We performed experimentation on local as well as cloud simulators: 1) The “qasm_simulator” was used as local machine simulator, and 2) The “ibmqx2” simulator was used as IBM cloud quantum simulator. The outcome of local as well as IBM simulator with and without an eavesdropper, between the two parties involved in key exchange were recorded and presented in the results section.

Quantum Random Number Generators (QRNGs): Theoretical and Experimental Investigation

Zeshan Haider , Muhammad Haroon Saeed, Muhammad Ehsan-ul-Haq Zaheer, Zeeshan Ahmed Alvi, Muhammad Ilyas, Tahira Nasreen, Muhammad Imran, Rameez Ul Islam, Manzoor Ikram

National Institute of Lasers and Optronics College, Pakistan Institute of Engineering and Applied Sciences, Nilore, Islamabad 45650, Pakistan

Quantum Random Number Generators (QRNGs) emerged as a promising solution for generating truly random numbers. We give an overview of QRNGs and present the in-depth experimental explorations for building and characterizing QRNG using the homodyne detection technique to measure the quadrature amplitude of quantum vacuum fluctuations. Since entropy assessment plays a fundamental role in authenticating the true randomness, a comprehensive description of entropy and how it evaluates the quality of randomness of the source is illustrated. Our experimental setup, apart from the hardware, includes a diverse set of testing techniques including NIST statistical/entropy suites, Dieharder tests battery, and auto correlation coefficient to verify the randomness and statistical properties of the generated random numbers. We believe that our experimental investigations provide a valuable resource for building QRNGs for a wide range of applications.

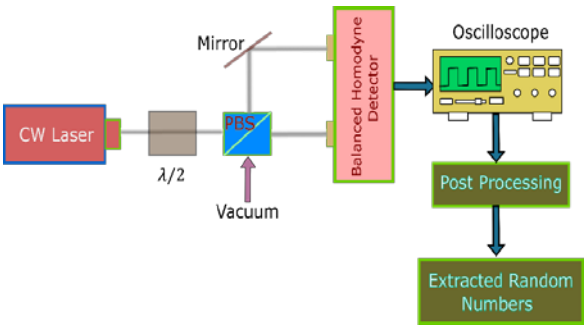

Fig A. Experimental Schematics for QRNG based on Quantum Vacuum Noise

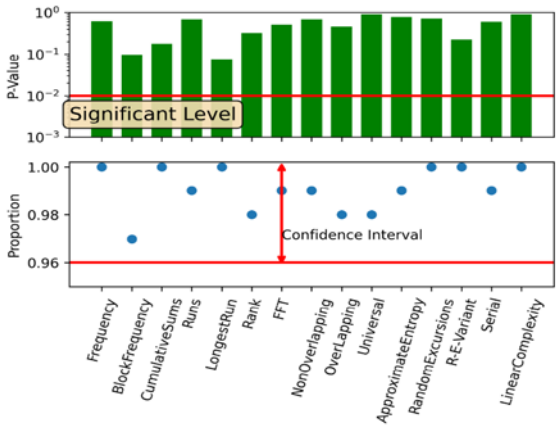

Fig B. Typical results of standard NIST Statistical Test Suite. For each test term, the bar values represent the P values of the worst cases of our test outcomes.

References

[1] M. H. Collantes, J. C. G. Escartin, Rev. Mod. Phys. **89**, 015004 (2017)

[2] X. Ma, X. Yuan, Z. Cao, B. Qi, Z. Zhang, Npj Quantum Inform. **2,** 1 (2016)

[3] Y. Shi, B. Chng, C. Kurtsiefer, Appl. Phys. Lett. **109**, 041101 (2016)

[4] Z. Haider , M. H. Saeed, M. E. Zaheer, Z. A. Alvi, M. Ilyas, T. Nasreen, M. Imran, R. Islam, M. Ikram, Eur. Phys. J. Plus **138,** 797 (2023)

Effect of background noise in Continuous Variable Quantum Key Distribution from Space

Zhehui Kong[1,2], Rupesh Kumar[1] and Andy Vick[2]

[1]School of Physics, Engineering and Technology, University of York, UK
[2] RAL Space, Harwell, UK
E-mail: rhr516@york.ac.uk

The security of quantum key distribution (QKD) is well known to be resilient to the risks posed by advances in quantum computers. Already, many projects exist to build QKD networks within and between cities for secure communication. As the technology becomes more developed, it will become feasible and indeed, desirable, to develop quantum communication networks between countries and even continents. While early QKD networks were built in fiber, this becomes unfeasible over long distances due to high channel losses. Satellite-based QKD is an attractive alternative option for long distance fiber-based QKD. However, there is the notable disadvantage of being susceptible to high levels of background noise, as well as dependence on atmospheric conditions, for successful secure key generation.

Continuous Variable (CV) QKD encodes information into the properties of the electromagnetic field, such as its amplitude and phase. Shot noise sensitive coherent detection is used to decode the keys. CVQKD shows higher resilience to background noise photons than the single photon based Discrete Variable (DV) QKD. In this poster, we will show the effect of different atmospheric conditions on the performance of CVQKD and the key generation rate round the clock.

Optimizing the relative Entropy under linear constraints

Gereon Koßmann
RWTH Aachen / Germany

René Schwonnek
Leibniz Universität Hannover / Germany
(Dated: January 2024)

Optimizing the quantum relative entropy under linear constraints is a central problem in Quantum Key Distribution (QKD) and other fields of (Quantum) Shannon theory. In particular providing provable lower and upper bounds is a highly relevant task. We provide a practical and resource efficient method for this problem. At the core of our work stands a recently described, and pleasingly elegant, integral representation of the quantum relative entropy, which we employ in order to formulate the problem of reliably bounding it as an iteration of semi definite programs (SDP). In contrast to existing techniques, our method comes with a provable convergence guarantee of quadratic order, whilst staying resource efficient with the matrix dimension of the underlying SDPs. We furthermore can provide an estimate for the gap to the optimum at each stage of the iteration. Combining this with some clever heuristics for the iteration, we find that convergence can in practice be actually achieved much faster then theoretically guaranteed.

From Classical to Quantum Network Coding: Entanglement and Quantum Key Distribution in Quantum Networks

Seid Koudia[1,2]

[1]*Department of Physics Ettore Pancini, University of Naples Federico II*
[2]*The Interdisciplinary Centre for Security, Reliability, and Trust (SnT), Luxembourg, Luxembourg*

We explore the transition from classical store-and-forward mechanisms to network coding within quantum networks, specifically focusing on its impact on entanglement distribution (ED) and quantum key distribution (QKD). For entanglement distribution, our research emphasizes the advantages of implementing quantum codes in relay nodes. Through the integration of quantum network coding strategies, we aim to reduce latency, minimize quantum memory overhead, and enable the allocation of multiple end-to-end entanglement distribution requests. This innovative approach has the potential to revolutionize quantum networks by enhancing scalability and responsiveness and gives them an inherent tolerance to errors and losses. In the realm of QKD, we investigate the application of network coding at relay nodes. By leveraging network coding techniques, our goal is to decrease key material consumption and enhance end-to-end key distribution requests. This approach not only improves the efficiency of quantum key management systems but also addresses the resource-intensive nature of classical methods.

References

[1] S. Koudia, Physica Scripta **99**, 015115 (2024)

Driving Innovation and Technology

Manuel Kraft

VDI/VDE-IT, Steinplatz 1, 10623 Berlin, Germany

Funding programmes strengthen the German and European research and industry location. As project manager, we support and advise the German federal government, the German state governments and the EU to efficiently use public funds. We advise public contracting authorities during the design of research programmes and, at the same time, motivate research institutes and industry to apply for funding for their promising projects. Our experts assess the projects regarding their innovation potential and financial feasibility. We support and manage projects and networks, which receive funding from our customers throughout the entire duration of the project. That means, we manage the funds, assume responsibility for the reporting and controlling and act as contact person for the sponsors and project implementers at all times.

References

[1] https://vdivde-it.de/en/portfolio/funding

Characterisation of a satellite-to-ground CV-QKD channel

Emma Tien Hwai Medlock[1], Vinod Rao[1,2], and Rupesh Kumar[1,2]

[1]University of York, York, UK
[2] Quantum Communications Hub, York, UK

Continuous variable quantum key distribution (CVQKD) uses modulation of amplitude and phase of electromagnetic fields to encode information and shot noise limited detectors for decoding [1,2]. The shot noise limited detection shows superior tolerance to noise [3] and therefore a promising candidate for space-to-ground quantum communications, especially in daylight conditions. The parameters that affect the secure key generation rate of CVQKD systems are the channel parameters- transmittance and uncalibrated noise (excess noise) [3]. On a typical static channel, such as an optical fibre link, the channel transmittance stays constant over a long period of signal transmission [4]. On a dynamic channel, such as a Low Earth Orbit (LEO) based satellite to ground optical link, the transmittance of the channel varies concerning the elevation of the satellite [5].

In this poster, we will discuss the impact of the variation of channel transmittance in satellite to ground CVQKD link and propose a method for maximising the key rate.

References

[1] Hajomer, A.A., Jain, N., Mani, H., Chin, H.M., Andersen, U.L. and Gehring, T., 2022. Modulation leakage-free continuous-variable quantum key distribution. *npj Quantum Information*, *8*(1), p.136.

[2] Hirano, T., Ichikawa, T., Matsubara, T., Ono, M., Oguri, Y., Namiki, R., Kasai, K., Matsumoto, R. and Tsurumaru, T., 2017. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, *2*(2), p.024010.

[3] Huang, D., Huang, P., Lin, D. and Zeng, G., 2016. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific reports*, *6*(1), p.19201.

[4] Wei, S., Huang, P., Wang, S., Wang, T. and Zeng, G., 2023. High-precision data acquisition for free-space continuous-variable quantum key distribution. *Optics Express*, *31*(5), pp.7383-7397.

[5] Sidhu, J.S., Brougham, T., McArthur, D., Pousa, R.G. and Oi, D.K., 2022. Finite key effects in satellite quantum key distribution. *npj Quantum Information*, *8*(1), p.18.

randExtract: a Reference Library to Test and Validate Privacy Amplification Implementations

Iyán Méndez Veiga[1,2]

[1]*School of Computer Science and Information Technology, Hochschule Luzern (HSLU), 6343 Rotkreuz, Switzerland*
[2] *Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland*

Classical post-processing is a crucial step in any quantum key distribution and quantum randomness generation protocol. In particular, privacy amplification guarantees that a protocol is ε-secure or, in other words, that the output is independent and uniform from an attacker's point of view, except with an arbitrary small probability ε. That is one of the reasons why all quantum cryptographic protocols always require and assume reliable classical computation. Although there has been a lot of theoretical work in this field, and practical algorithm are known, there is still not an off-the-shelf library that is open source, well documented and whose correctness can easily be verified. Instead, labs and commercialized devices used, most of the time, their own high-performance implementations using accelerators such as GPUs or FPGAs. This makes it difficult for end users or other researchers to validate the privacy amplification step. In this poster we present randExtract, a Python package we have developed that implements the most used randomness extractors in current experiments QKD experiments. Our goal is to make a reference implementation whose code is easy to read and audit, and provide a simple interface to test and validate other high-performance implementations. We demonstrate this by testing a Rust and a GPU [1] implementation of the Toeplitz hashing extractor, and the C++ implementation [2] of the Trevisan's extractor, both used in actual experiments.

References

[1] Grünenfelder, F., Boaron, A., Resta, G.V. *et al.* Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nat. Photon.* **17**, 422–426 (2023). https://doi.org/10.1038/s41566-023-01168-2

[2] Mauerer, W., Portmann, C., & Scholz, V.B. A modular framework for randomness extraction based on Trevisan's construction. ArXiv, abs/1212.0520 (2012). https://doi.org/10.48550/arXiv.1212.0520

Achievable state transformations under rotational invariance

Fynn Otto and Konrad Szymański

Universität Siegen, Germany

Rotational invariance is a fundamental characteristic of physical interactions, naturally leading to rotationally covariant dynamics. In communication between distant parties, the lack of a common reference frame imposes similar constraints on the effective transformations: they must be independent of the unknown reference, and thus are rotationally invariant as well. This feature is captured by the formalism of SU(2)-covariant operations: those that commute with the actions of all group elements. We present an analytical characterization of covariant transformations and introduce semidefinite programs to examine which states are reachable from a given input using SU(2)-covariant channels. Our results improve our understanding of the transformations of directional information carriers and showcase the mechanisms of quantum operations lacking a reference frame.

References

[1] F. Otto, K. Szymański, *Rotational invariance restricts available quantum states*, arXiv:2401.06064 (2024)

[2] I. Marvian, PhD thesis, *Symmetry, Asymmetry and Quantum Information* (2012)

[3] G. Gour, R.W. Spekkens, *New J. Phys.* **10** 033023 (2008)

Optimization of high-dimensional QKD for deployment on a 1.7 km free-space link

Karolina Paciorek[1], Christopher Spiess[1,2] , Sarika Mishra[1], and Fabian Steinlechner[1,2]

[1]Fraunhofer Institute for Applied Optics and Precision Engineering, Albert-Einstein-Strasse 7, Jena 07745, Germany
[2]Friedrich Schiller University, Institute of Applied Physics, Abbe Center of Photonics, Albert-Einstein-Strasse 15, Jena 07745, Germany

Quantum Key Distribution (QKD) is a method for establishing a secure encryption key using a quantum optical sender, a transmission link, and an optical receiver. When QKD is implemented over short distances with low losses, such as in data centers or intercity links, then the maximum secure key rate is typically limited by saturation of the single-photon detectors at the receiver [1-4]. To overcome this limitation, high-dimensional QKD protocols can be implemented. High-dimensional QKD protocols enable encoding more information into one photon, which enables operation at photon rates that no longer saturate the detectors [6, 7]. We show this at the example of a weak coherent source in a time-phase encoding scheme. Furthermore, we will demonstrate the transfer of key material over a 1.7 km intercity free-space link. Our demonstration is accompanied by finite-key analysis with an extensive parameter optimization in experiment and simulations to maximize the key rate [8]. Our results show that high-dimensional QKD with weak coherent sources is a promising avenue towards versatile communication scenarios, including areas with difficult access such as rapidly changing metropolitan spaces or in satellite communication [5, 8].

References

[1] C. Ci Wen Lim, M. Curty et al. "Concise security bounds for practical decoy-state quantum key distribution", Phys. Rev. A **89**, 022307, (2014).
[2] M. Tomamichel, C. Lim, N. Gisin et al. "Tight finite-key analysis for quantum cryptography." Nat Commun **3**, 634 (2012).
[3] D. Rusca; A. Boaron; F. Grünenfelder et al. "Finite-key analysis for the 1-decoy state QKD protocol " Applied Physics Letters **112**, 171104 (2018)
[4] Avesani, M., Calderaro et al. "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics" npj Quantum Inf **7**, 93 (2021)
[5] T. Schmitt-Manderbach, H. Weier et al. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km." Physical review letters **98**, 010504, (2007)
[6] I. Vagniluca, et al. "Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution", Phys. Rev. Applied **14**, 014051, (2020)
[7] Nurul T. Islam et al. "Provably secure and high-rate quantum key distribution with time-bin qudits." Sci. Adv. **3**, e170149, (2017).
[8] C. Spiess, F.Steinlechner, "Clock synchronization with pulsed single photon sources", arXiv:2212.12589, (2022)

A versatile fiber-coupled DM-CV-QKD system for the QuNET initiative

S. Richter[1,2], H. Vural[1,2], J. Schreck[1,2], K. Jaksch[1,2], Ö. Bayraktar[1,2], T. Dirmeier[1,2], W. Elser[1,2], D. Elser[1,2] and C. Marquardt[12]

[1] Chair of Optical Quantum Technologies, Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen, Germany
[2] Max Planck Institute for the Science of Light, Erlangen, Germany

Quantum key distribution is an important tool for establishing provably secure shared secret keys between distant parties over untrusted communication channels. This is a crucial part of the ongoing efforts to provide future-proof cryptography resistant to the growing threat posed by next-generation quantum computers. Due to its compatibility with classical optical communications, continuous-variable quantum key distribution (CV-QKD) is well positioned for providing this essential function in short- to mid-range metropolitan fiber networks.

We present our prototype of a CV-QKD system developed for the QuNET initiative, which is based on the discrete modulation of coherent states and a double balanced homodyne measurement scheme. It is compact, mountable in a 19" server rack and capable of generating and receiving shot-noise-limited discrete modulations of coherent quantum states with a bandwidth of up to 500MHz. We discuss the requirements of practical CV-QKD systems as well as some technical challenges faced by current implementation efforts and provide an overview of our proposed solutions in the wider context of QuNET.

Usage of Hardware Random Number Generators

Stefan Röhrich

Rohde & Schwarz Cybersecurity GmbH, Germany

This talk will focus on the usage of random numbers after their generation. As the usage may be different depending on the device, there are several topics which influence the practicability of using a specific random number generator hardware in a system.

Besides the obvious topic of the generation speed, also the interface hardware and protocols can be important, while buffering adds an additional layer of complexity.

The talk will close with a look in common possible errors in software implementations, which, even when trying to use a secure hardware random number generator, may lead to insufficient randomness when integrating a random number generator in a complex system, possibly integrating third party libraries and products.

Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link

K.P. Schatz[1], B. Amies-King[1], H. Duan[1], A. Biswas[1], S. Albosh[1], R. Kumar[1], M. Lucamarini[1]

[1]School of Physics, Engineering & Technology and York Centre for Quantum Technologies, Institute for Safe Autonomy, University of York, YO10 5FT York, U.K.

Quantum cryptography, especially Quantum Key Distribution (QKD) technology, is rapidly moving from the laboratory environment to real-world implementations, laying the foundations for a future quantum internet [1]. An essential aspect for wide-spread establishment of quantum communications is the ability to leverage existing optical infrastructures such as deployed fibre connections.

Real-world QKD implementations have been demonstrated in a number of field trials over the past years, achieving ever greater distances and complexity [2]. However, few demonstrations explore undersea-fibres, especially in an international setting [3]. These types of channels hold special promise for QKD operations due to their potentially superior environmental stability.

We performed a feasibility study of quantum communications over an industrial 224 km submarine optical fibre link deployed between Southport in the United Kingdom (UK) and Portrane in the Republic of Ireland (IE) [4]. Our characterisation of phase drift, polarisation stability and the arrival time of entangled photons covers many of the most prevalent degrees of freedom employed in current QKD technology. We thus demonstrate the suitability of this link to support a number of different QKD protocols. This study constitutes the first venture into international UK-IE quantum communications.

References

[1] Wehner, S.; Elkouss, D.; and Hanson, R.;, Science **362**, 6412 (2018)
[2] Liu, Y; Zhang, W. J.; Jiang, C. et. al., Phys. Rev. Lett. **130**, 210801 (2023)
[3] Wengerowsky, S.; Joshi, S.K.; Steinlechner, F. et. al. NPJ Quantum Inf. **6**, 5 (2020)
[4] Amies-King, B.; Schatz, K.P.; Duan, H. et. al. Entropy **25**, 1572 (2023)

Refining classical protocols for transmitting quantum systems

S. Schlösser[1] and M. Kleinmann[1]

[1]Universität Siegen, Siegen, Germany

We study a scenario in which Alice transmits a quantum state to Bob, who then performs a quantum measurement. Here, the state is not known to Bob and the measurement is not known to Alice. A classical simulation of this scenario requires communication of at least one bit, but the quantitative advantage of quantum systems is an open question. The problem was addressed by Toner and Bacon and the most recent results establish that two bits of communication and shared randomness are sufficient for the case of one qubit and generalized measurements. We refine this recent protocol and show that a perfect simulation for a single round can be achieved by transmitting only 1.89 bits on average. The reduction in communication cost raises the question of whether a further reduction is possible in the qubit case. Importantly, for a qutrit, it is not even known whether a finite amount of communication is sufficient to simulate the quantum statistics. We investigate other state spaces to gain a comprehensive understanding of the problem and aim to extend the protocol to the qutrit case.

References

[1] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003)
[2] M. J. Renner et. al., Phys. Rev. Lett. **130**, 120801 (2023)
[3] M. J. Renner et. al., Quantum **7**, 1149 (2023)

Towards experimental implementation of a continuous-variable quantum key distribution scheme with unidirectional modulation of squeezed states

J. Schreck[12], T. Dirmeier[12], K. Günthner, K. Jaksch and C. Marquardt[12]

[1]Max Planck Institute for the Science of Light, Erlangen, Germany
[2] Chair of Optical Quantum Technologies, Institute of Optics, Information and Photonics, FAU Erlangen-Nürnberg, Erlangen, Germany

Continous-variable quantum key distribution (CV-QKD) presents an opportunity to establish quantum-secure cryptography using off the shelf classical telecommunication technology. In free space optical links, polarization is a promising degree of freedom to encode QKD signals. Moreover, unidirectional modulated polarization squeezed states of light promise a simple experimental CV-QKD implementation which can make CV-QKD more robust against channel noise and finite postprocessing efficiency [1,2]. This work introduces our concept of a sender and receiver utilizing a source of squeezed states of light.

References

[1] V. C. Usenko, PHYSICAL REVIEW A **98**, 032321 (2018)

[2] V. C. Usenko, V. C. Usenko and A. n. Oruganti, "Role of anti-squeezing noise in continuous-variable quantum cryptography" 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, 2020, pp. 421-425

Optimizing the relative entropy under semi definite constraints

- A new tool for estimating key rates in QKD

G. Koßmann[2] and R.Schwonnek[1]

[1]Leibniz Universität Hannover, Hannover, Germany
[2] RWTH Aachen, Aachen, Germany

Optimizing the quantum relative entropy under linear constraints is a central problem in Quantum Key Distribution (QKD) and other fields of (Quantum) Shannon theory. In particular providing provable lower and upper bounds is a highly relevant task.

We provide a practical and resource efficient method for this problem. At the core of our work stands a recently described, and pleasingly elegant, integral representation

of the quantum relative entropy, which we employ in order to formulate the problem of reliably bounding it as an iteration of semi definite programs (SDP). In contrast to existing techniques, our method comes with a provable convergence guarantee of quadratic order, whilst staying resource efficient with the matrix dimension of the underlying SDPs. We furthermore can provide an estimate for the gap to the optimum at each stage of the iteration. Combining this with some clever heuristics for the iteration, we find that convergence can in practice be actually achieved much faster then theoretically guaranteed.

Taking quantum key distribution from fundamental science to certified systems in space

P. Sohr[1,2,3], M. Pivoluska[1,2,3], S. Ecker[3] and M. Erhard[3]

[1]Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria
[2] Vienna University of Technology, Vienna, Austria
[3]Quantum Technology Laboratories GmbH, Vienna, Austria

To fully exploit the inimitable security offered by quantum key distribution (QKD), it must be available over any distance on Earth. Satellite-based QKD provides the propagation capabilities needed to achieve global reach [1].

Here, we outline our ongoing work and the challenges we are facing. We aim to develop a consistent, fully comprehensive QKD protocol for decoy-state BB84 in space that, in conjunction with a rigorous security analysis, is suitable for implementation in accredited systems. Based on meticulously selected assumptions, we model our characterized devices, allowing for a composable security proof within the abstract cryptography framework [2, 3]. Where the model is unable to accurately represent reality, we ensure security with an exhaustive side-channel analysis.

Our research faces various challenges as we try to bridge the gap between fundamental research and practical implementation. Implicit as well as contradictory assumptions impede the consolidation of existing results [4]. Indisputably, the protocol must provide composable security without making assumptions about the adversary. Satellite-based implementations pose additional challenges due to resource limitations, including finite-key size effects and constraints in terms of size, weight, power, computational capabilities, and data storage. The limited resources directly affect the definition and implementation of the block size [5]. We actively support the design of the faint pulse source and the detection module to ensure the compliance with the assumptions and to facilitate a thorough side-channel analysis. Ultimately, the security statement of the system, the security proof and the side-channel analysis must convince accreditation authorities and users.

As we refine and iterate the protocol, our future goals include increasing the key rate while maintaining the unprecedented level of security achieved. The lessons learned from designing this protocol will guide the evolution towards QKD implementations that are highly resistant to side-channels, while ensuring robust key rates.

References

[1] S.-K. Liao et al., Phys. Rev. Lett. **120**, 030501 (2018)
[2] R. Renner, arXiv:quant-ph 0512258 (2006)
[3] J. Müller-Quade and R. Renner, New J. Phys. **11**,085006 (2009)
[4] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017)
[5] C. C.-W. Lim et al, Phys. Rev. Lett. **126**, 100501 (2021)

Robust Time Transfer with Single Photons on Hybrid Quantum Communication Scenarios in Fiber and Free-Space

Christopher Spiess[1,2,*], Pritom Paul[1,2], Karolina Paciorek[2], Sarika Mishra[2], Fabian Steinlechner[1,2]

[1]Friedrich Schiller University, Institute of Applied Physics, Abbe Center of Photonics, Albert-Einstein-Strasse 15, Jena 07745, Germany
[2] Fraunhofer Institute for Applied Optics and Precision Engineering IOF, Albert-Einstein-Strasse 7, 07745 Jena
**E-mail: christopher.spiess@iof.fraunofer.de*

As quantum networks become more complex, synchronization becomes challenging. Single photons, central to quantum communications, serve as excellent timing carriers for synchronizing quantum communication networks with minimal resource overhead [1]. We investigate timing performance in a 70 km fiber link and a 1.7 km free-space link, achieving robust time transfer down to 100 ps time deviation at 1-second integration time using unstable crystal oscillators. Our experiments use a faint pulse source at 1550 nm for quantum key distribution and time transfer. Clocks with significant frequency fluctuations are frequency-locked by single photons over 3.8 days on a 70 km fiber link and 13 hours on a 1.7 km free-space link. Single-mode fiber coupling mitigates daylight noise in the free-space measurement. These results demonstrate the potential of single photons as timing carriers in quantum communication networks [2,3] and other applications such as single-photon ranging or metrology. Our findings contribute to the development of a strong, independent, and secure quantum communication network without external hardware.

References

[1] Caleb Ho et al., New J. Phys. **11** (4), 45011 (2009)
[2] C. Spiess et al., Quantum Sci. Technol. **9,** 015019 (2024)
[3] C. Spiess et al., Phys. Rev. Applied **19**, 054082 (2023)

On measuring quantum noise

Guilherme Alexander Stein[1]

[1] *light&matter group, Leibniz Universität Hannover*

Non-classical states of light express interesting poperties throughout different fields. The most obvious being a laser, other such states encompass single photon sources or squeezed light. Squeezed light can be used for sensitive measurements, where one of the quadratures, e.g. the amplitude, is squeezed. Thus offering a higher precision than classical light would allow, due to the Heisenberg uncertainty.
Here we are interested in the effect squeezing exhibits on noise. A simple method to generate random bits, is the use of properties of the vacuum state, since we always have uncertainties in conjugate variables. Even in the ground state. This means that neither the variance of momentum nor impulse, or rather the quantized respecting quadratures of the fields, are zero at any given moment. This can be leveraged to collect random bits from the vacuum and use squeezing as determination of randomness. Since true randomness can never be "proven" or "checked", the generation of good randomness™ has to rely on, and draw its confidence from, the method it was generated by.

References

[1] Measurement of the quantum states of light
(G. Breitenbach, S.Schiller, J. Mlynek, Nature 1997)
[2] Sensitivity Enhancement of Optomechanical Measurements using Squeezed Light
(L.M. Kleybolte, Thesis 2019)
[3] Coherent and Incoherent states of the radioation field
(Roy Glauber, PRL 1963)
[4] Nonlinear Optics
(Robert Boyd, Elsevier 2020)
[5] Experimental Generation and Manipulation of Quantum Squeezed Vacuum
(T.S. Horom, Thesis 2013)
[6] Spatial Multi-Mode Structure of Atom-Generated Squeezed Light
(Mi Zhang et al., PRA 2017)
[7] Source-Device-Independent Ultrafast Quantum Random Number Generation
(D.G. Marangon, G. Vallone, and P. Villoresi, PRL 2017)

Exploring the Bell Polytope experimentally

Yagana Syed[1], Ilija Funk[1], Ilja Gerhardt [1]

[1] Leibniz University Hannover, light & matter group, Appelstrasse 2, 30167 Hannover, Germany

The Bell Polytope is a mathematical structure that defines the boundaries of classical and quantum explanations behind correlations in entangled quantum systems, based on the principle of Bell inequality. Our project includes generating orthogonal entangled photon pairs created via type II spontaneous parametric down conversion process, and sending them to two sets of quadrant detectors measuring their correlations at four polarization angles simultaneously. We aim to explore the impact of rotating our detectors by various polarizing angles and of dark counts on the correlations between the generated photon pairs and thus achieve the optimal alignment of our experiment by the end.

The Marketing of and Education about Quantum Random Number Generators

D. Timmermann[1]

[1]*Physikalisch-Technische Bundesanstalt (PTB), Braunschweig, Germany*

Quantum effects offer superb sources for randomness in random number generators (RNGs). In the last years, and especially with the advent of commercial quantum communication systems, quantum random number generators (QRNGs) have become more and more common on the market.

QRNGs are often marketed as being superior due to their use of quantum effects. They are advertised to use “objective randomness” [1] in contrast to other RNGs, which are claimed to be, “by principle, predictable and deterministic” [2]. Also in quantum technology education, QRNGs are commonly used as introductory examples for the application of quantum technology. In both cases, an overemphasis on the physical processes producing random results suggests that QRNGs are novel or secure.

Physical RNGs are primarily used in security applications. The certification of RNGs (see e. g. AIS 31) defines many requirements that a device must fulfil, such as a reliable start-up test, total failure test, and online test. The used randomness source only influences the stochastic model of its output and thus the statistical tests the device must pass. Being “quantum” has no direct impact on the certification of an RNG. Thus, what is relevant for the certification of an RNG is not primarily the physics of its randomness source, but the engineering of the device.

This contribution discusses different ways QRNGs are presented in education and marketing. These are contrasted with a broad overview of research on the security of various types of RNGs, allowing for a realistic judgement on the possibilities, challenges, and limitations of QRNG.

References

[1] Quantum Flagship, https://qt.eu/quantum-principles/sensing-and-metrology/qrng (2024)

[2] Quside, https://quside.com/quantum-random-number-generators-why-how-where/ (2024)

Security of a commercial entanglement-based QKD system

P. Vazquez[1]

[1]*Quantum Optics Jena GmbH, Jena, Germany*

The security proof for a Quantum Key Distribution (QKD) protocol often are general and does not consider the specifics of the hardware in a commercial setting. In this work, we introduce a formal and detailed model as in [1] of a commercially available QKD system including the hardware components. We then derive the security proof following the methods used by Tomamichel *et. al.* [2] except for the parameter estimation step that is replaced by a more direct calculation of qber after error correction that allows for tighter bounds only at the expense of robustness.

References

[1] M. Tomamichel *et. al.*, Quantum **1**, 14 (2017)

[2] M. Tomamichel *et. al.*, Nat Commun 3, 634 (2012)

A rack-integrated optical sender module for the feasibility study of CV-QKD in a mobile optical link during a flight campaign

H. Vural[1,2], S. Richter[1,2] and C. Marquardt[1,2]

[1]Chair of Optical Quantum Technologies, Institute of Optics, Information and Photonics, FAU Erlangen-Nürnberg, Erlangen, Germany
[2] Max Planck Institute for the Science of Light, Erlangen, Germany

Continuous-variable (CV) quantum key distribution (QKD) offers the possibility of establishing quantum-secure cryptography within classical telecommunication frameworks [1]. While discrete-modulated CV-QKD with phase-amplitude modulation has already been extensively explored for metropolitan fiber links, its potential for links in free space is still relatively unexplored. This work introduces our concept: a rack-integrated sender module tailored for deployment in a QuNET flight campaign. This campaign aims to establish a mobile quantum link between airborne and ground stations, providing a unique platform to explore the viability of QKD in this dynamic scenario [2]. Our discussion includes the protocol developed and strategic design considerations to meet the challenges of a moving and fluctuating optical channel.

References

[1] F. Grosshans, Phys. Rev. Lett. **88**, 057902 (2002)
[2] S. Nauert, Nat. Photonics **7**, 382-386 (2013)

Quantum key distribution receiver with countermeasures against implementation attacks

P. Daly[1], P. Freiwang[1], P. Menz[1] F. Sax[1], H. Weier[1]

[1]Quantum Space Systems GmbH, Munich, Germany

The vulnerability of quantum key distribution systems to implementation attacks [1] poses a significant challenge to their security. Quite extensive research has shown that the so-called detector-control attacks can potentially render QKD systems completely insecure while using technology that is available today [2]. Several general countermeasures have been proposed to protect against these attacks. Examples include monitoring the optical intensity at the receiver with extra detectors [3]; the use of optical filters to block non-signal photons [4]; monitoring the electrical parameters of the detectors [2].

Here we present a design of a receiver module that takes into account some of these proposed countermeasures.

References

[1] Ch. Marquardt et al *BSI P575* (2023)

[2] Henning Weier et al *New J. Phys.* **13** 073024 (2011)

[3] S.N. Molotkov *J. Exp. Theor. Phys.* **130**, 809–832 (2020)

[4] N. Gisin et al *Phys. Rev. A* **73**, 022320 (2006)

Room-Temperature NV-Based Quantum Computing: Pathways to Commercialization, Technological Progress, and Emerging Challenges

Matthias Widmann[1], Danial Majidi[1], Nils Herrmann[1], Lykourgos Bougas[1], Felix Engel[1], Georg Wachter[1], Torsten Rendler[1], Charles Babin[1], Florian Preis[1], Mariam Akhtar[2], Stefan Prestel[1], Andrew Horsley[2], Marcus Doherty[2], and [2]

[1]Quantum Brilliance GmbH, Colorado Tower Industriestr. 4, 70565 Stuttgart, Germany
[2]Quantum Brilliance Pty Ltd, 60 Mills Road,Acton ACT 2601, Australia

As we approach the commercialization of NV-based quantum computers, this poster presents initial successes with a diamond-based system operational in a high-performance computing center. Highlighting a milestone, we showcase the first application of quantum machine learning (QML) on an on-site room-temperature quantum computer at the Pawsey Supercomputing Centre, Australia. Utilizing a two-qubit system, we address multi-class classification challenges with a model trained via the Adam optimizer, achieving classification accuracies comparable to ideal simulations. Our research delineates also an innovative architecture and fabrication methodology conducive to scalable qubit integration, from fabrication to implementation. This poster elucidates the inherent challenges in scaling NV-based quantum microprocessors, contributing significantly to the field of commercial quantum computing by advancing the scalability and practical implementation of these devices.

References

[1] N. Herrmann et al., *arXiv:2312.11673v1* (2023).

Towards the certification of quantum key distribution systems

J. Wiesemann[1], J. Krause[1], D. Rusca[2] and N. Walenta[1]

[1]Fraunhofer Heinrich-Hertz Institut HHI, 10587 Berlin, Germany
[2]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain

In recent years, thanks to the various advances in quantum technologies, quantum key distribution (QKD) has emerged as a promising security scheme, transitioning from a scientific research field to a commercially viable solution. Despite the existence of commercial QKD systems, the shortage of standards for implementation and evaluation, particularly concerning side-channel attacks, has been a recurring point of criticism, hindering its widespread adoption as a standard cryptographic tool. This work aims to address some of these challenges by focusing on the process of preparing an in-house QKD system for evaluation. We present a consolidated, accessible, and comprehensive security proof of the one-decoy state protocol with finite-keys, expressed in a unified language. Furthermore, we tackle some of the most critical side-channel attacks by discussing existing countermeasures that can be implemented both in the QKD system and within the security proof, where applicable. By providing a critical evaluation of our QKD system and incorporating robust countermeasures against side-channel attacks, our research contributes to advancing the practical implementation and evaluation of QKD as a trusted security solution.

References

[1] D. Rusca et al., Applied Physics Letters **112**, 171104 (2018)
[2] C. Lim et al., Physical Review A **89**, 022307 (2014)
[3] V. Makarov et al., preprint **2310.20107** [quant-ph] (2023)
[4] S. Sajeed et al., Scientific Reports **11**, 5110 (2021)

Device-independent randomness amplification

A. Kulikov[1], S. Storz[1], J. Schär[1], M. Sandfuchs[2], R. Wolf[2], R. Renner[2] and A. Wallraff[1]

[1]Laboratory for Solid State Physics, ETH Zürich, 8093 Zürich, Switzerland
[2]Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland

The quest for achieving perfect randomness assumes paramount significance across multifarious applications, notably in the realms of cryptography and computational simulations. Conventional random number generators, rooted in classical physical processes, grapple with a foundational concern – the potential for adversaries to predict their outputs by scrutinizing the microscopic degrees of freedom, thereby eroding their essential unpredictability. Fortunately, quantum physics exhibits intrinsic randomness, which opens up the possibility of creating perfect randomness from an imperfect and publicly accessible source, as substantiated by recent advances. Even more, it allows us to do so in a device-independent way, i.e., without relying on the precise characterisation of the quantum devices. However, since its practical realisation relies on the successful execution of a Bell test with reasonably high Bell violation and repetition rate, presenting significant challenges to experimentalists, which is why it has not yet been demonstrated – until now. In a collaboration with experimentalists at ETH Zürich, we combine recent theoretical process on randomness amplification protocols with new experimental developments in Bell tests and achieve the first successful demonstration of device-independent randomness amplification. Our demonstration, based on a Bell test with superconducting circuits, marks a significant advancement within the domain of quantum technologies, heralding the ability to weaken the prior necessity for perfect randomness.