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

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