QI 26: Quantum Communication I: Theory

Time: Thursday 11:00–12:45 Location: HS IX

Invited Talk QI 26.1 Thu 11:00 HS IX

Device-independent randomness amplification — •Ramona Wolf — Universität Siegen

Randomness is a regular part of our (more or less) daily lives: from drawing lottery numbers to running computer simulations and the security of cryptographic schemes, various applications rely on random numbers. But does true randomness actually exist? If so, can we create truly random numbers in our labs? Conventional random number generators based on classical physical processes face a fundamental problem, namely the possibility that attackers can predict their results by examining the microscopic degrees of freedom, thereby eroding their fundamental unpredictability. Fortunately, quantum physics exhibits intrinsic randomness, which opens up the possibility of creating perfect randomness from an imperfect and even publicly accessible source. However, its practical realisation relies on the successful execution of a Bell test with sufficiently high Bell violation and repetition rate, making it a challenging endeavour.

In this talk, I will discuss what is necessary to realize quantum random number generators, starting with how to properly define randomness (which is a surprisingly nontrivial task!) up to explaining how to design protocols for experimentally generating truly random numbers, and reporting on recent experimental progress.

QI 26.2 Thu 11:30 HS IX

Quantum Steering for Security Analysis of Quantum Key Distribution Protocols — •Ritu Dhaulakhandi and Ramona Wolf — Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Germany

Quantum Key Distribution (QKD) protocols exploit fundamental quantum mechanical principles to ensure secure communication, even in the presence of adversaries with unlimited computational resources. The use of quantum steering, particularly steering inequalities, provides a powerful framework for analysing correlations in scenarios involving untrusted or semi-trusted devices. Inspired by the CHSH inequality, this research explores the construction and application of asymmetric CHSH-like steering inequalities (allows adaptation to unbalanced measurement settings or noise levels between communicating parties) to establish security based on locally verifiable assumptions for QKD protocols. The inequality bounds the set of correlations explainable by local hidden variable local hidden state (LHV-LHS) models, ensuring that any violation implies genuine quantum correlations. The geometric insights from the convex characterisation of the LHV-LHS model provide a robust method to verify security while minimising trust assumptions. We investigate how such inequalities can quantify the nonlocal correlations required for secure key generation and establish their operational significance in one-sided device-independent (1SDI) QKD protocols. The steering criteria derived is tailored to practical QKD setups, allowing identification of the noise and loss thresholds necessary for their violation.

QI 26.3 Thu 11:45 HS IX

Iterative Sifting in QKD — •Yien Liang, Hermann Kampermann, and Dagmar Bruss — Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, D-40225 Düsseldorf, Germany

We investigate the security of a QKD scheme, where Bob announces publicly his choice of measurement basis right after each detection. Such a scheme saves memory and avoids sending all the classical information only at the end of each block. In previous work the security of such a scheme is based on Azuma's inequality [1], with reduced key rate in comparison to conventional sifting. Our work improves the bound for iterative sifting, restoring the key rate of conventional sifting. We will additionally show how to save classical communication for privacy amplification in the conventional and the iterative scheme.

Reference:

[1] Kiyoshi Tamaki et al 2018 Quantum Sci. Technol. 3 014002

QI 26.4 Thu 12:00 HS IX

Secure quantum bit commitment from separable operations — •Ziad Chaoui[1], Anna Pappa[1], and Matteo Rosati[2] — [1]Technische Universität Berlin, Berlin, Germany — [2]Università degli studi di Roma Tre, Rome, Italy

Bit Commitment is a fundamental cryptographic primitive in both classical and quantum cryptography and a building block for many two party cryptographic protocols, such as zero-knowledge proofs. However it has been proven that unconditionally secure quantum bit commitment cannot exist. We show that restricting the committing party to separable operations leads to secure quantum bit commitment schemes. Specifically, we prove that in any perfectly hiding bit commitment protocol, a committing party restricted to separable operations will be detected with high probability when attempting to switch their commitment. To illustrate our results, we present an example protocol.

QI 26.5 Thu 12:15 HS IX

Security of an ensemble based quantum token against optimized atacks — •Bernd Bauerhenne[1], Lucas Tsunaki[2], Malwin Xibraku[1], Boris Naydenov[2], Martin Garcia[1], and Kilian Singer[1] — [1]Department of Physics, University of Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany — [2]Helmholtz-Zentrum Berlin, Hahn-Meitner-Platz 1, 14109 Berlin, Germany

We introduce quantum coins, which are composed of discrete quantum tokens, each containing an ensemble of identical qubits. These quantum coins are initialized by a banking entity that encodes a unique, secret quantum state into each token by aligning all qubits in a token to a uniform state. The integrity of the coin is subsequently verified through sequential assessments of these quantum tokens. During this verification process, the bank executes measurements on the qubits using the known secret angles from the initialization. A quantum token is deemed valid if a critical threshold number of its qubits are measured in the ground state. A coin is considered authentic and accepted if it contains a sufficient number of validated tokens.

Our discussion also explores potential vulnerabilities to forgery, examining scenarios wherein a malicious actor attempts to replicate the quantum coins. We present a detailed analysis of various attack strategies and demonstrate that, even with optimized methods, the probability of such counterfeit coins being accepted by the bank is negligibly small. This analysis not only emphasizes the robustness of our proposed quantum coin system against duplication attempts but also enhances its application potential in secure quantum currency systems.

QI 26.6 Thu 12:30 HS IX

Security of Super Dense Coding under Pauli Noise — •Ghislaine Coulter-de Wit, Hermann Kampermann, and Dagmar Bruss — Institute for Theoretical Physics III, Heinrich Heine University Düsseldorf, D-40225 Düsseldorf, Germany

Super dense coding is a form of quantum communication utilizing shared entanglement such that - in the simplest formulation - Bob receives a message 2 bits long from one qubit sent by Alice.

The real world contains noise and untrustworthy parties (eavesdroppers). Building off the work of Zarah Shadman et al. [New Journal of Physics 12, 073042 (2010)] on noisy super dense coding, we are interested in the security of the transmitted classical data. As such, we focus on the amount of information that a disreputable party could determine. To do this, we consider Pauli noise for different scenarios of the entanglement distribution. We compare and contrast the super dense coding capacity for the given scenarios through the Holevo quantity and explore bounds on the information which an eavesdropper can obtain.