QUACC$^+$2025
Book of Abstracts

https://quacc2025.cft.edu.pl

Warszawa, May 12$^{\text{th}}$ – 14$^{\text{th}}$, 2025

Quantum Information is a rapidly developing field, attracting a large number of researchers, and leading to exciting fundamental discoveries and practical applications. The main aim of the Quantum Certification Conference 2025 (QUACC$^+$2025) workshop is to bring together young researchers working on widely understood quantum information sciences and related fields. The meeting is held in Warszawa, Poland, a lively Central European city with rich cultural and urban life.

This is a second edition of the workshop following the previous event: QUACC 2023.

Organizers (Center for Theoretical Physics PAS, Warsaw)

- Remigiusz Augusiak
- Wojciech Bruzda
- Arturo Konderak
- Jarosław Korbicz

Scientific Committee

- Antonio Acín (ICFO, Barcelona)
- Remigiusz Augusiak (CTP PAS, Warszawa)
- Wojciech Bruzda (CTP PAS, Warszawa)
- Omar Fawzi (Inria, ENS de Lyon)
- Arturo Konderak (CTP PAS, Warszawa)
- Jarosław Korbicz (CTP PAS, Warszawa)
- Stefano Pironio (Université Libre de Bruxelles)

Invited Talks

Click on the name or scroll down to show more.

1. **Antonio Acín** (Spain)
2. **Álvaro M. Alhambra** (Spain)
3. **Nicholas Chancellor** (UK)
4. **Omar Fawzi** (France)
5. **Maciej Lewenstein** (Spain)
6. **Edwin Lobo** (Belgium)
7. **Miguel Navascués** (Austria)
8. **Joschka Roffe** (Scotland)
9. **Francesco Tacchino** (Switzerland)
10. **Yuming Zhao** (Denmark)

Contributed Talks

1. **Flavio Baccari** (Italy)
2. **Carles Roch i Carceller** (Sweden)
3. **Christopher Corlett** (UK)
4. **Marianna Crupi** (Germany)
5. **Sophie Egelhaaf** (Switzerland)
6. **Patrick Emonts** (Netherlands)
7. **Ahana Ghoshal** (Germany)
8. **Felix Huber** (Poland)
9. **Marcin Kotowski** (Poland)
10. **Owidiusz Makuta** (Netherlands)
11. **James Mills** (UK)
12. **Mariana Navarro** (Spain)
13. **Tristan Nemoz** (France)
14. **Attila Portik** (Hungary)
15. **Albert Rico** (Spain)
16. **Michał Studziński** (Poland)
17. **Elna Svegborn** (Sweden)
18. **Peter Tirler** (Austria)
19. **Lewis Wooltorton** (France)

Posters

1. **Nicola D'Alessandro** (Sweden)
2. **Raffaele D'Avino** (Spain)
3. **Stefan Bäuml** (Germany)
4. **Tomas Crosta** (France)
5. **Hirak Kanti Ghosh** (UK)
6. **Mengyao Hu** (Netherlands)
7. **Hubert Kołcz** (Poland)
8. **Tomás Fernández Martos** (Spain)
9. **Piotr Masajada** (Poland)
10. **Patryk Michalski** (Poland)
11. **Morteza Moradi** (Poland)
12. **Younes Naceur** (Spain)
13. **Ranieri Vieira Nery** (Spain)
14. **Robert Okuła** (Poland)
15. **Ignacio Perito** (Spain)
16. **Aby Philip** (Poland)
17. **Martin J. Renner** (Spain)
18. **Michał Siemaszko** (Poland)
19. **Anna Steffinlongo** (Spain)
20. **Daiki Suruga** (Japan)
21. **Jakub Szczepaniak** (Poland)
22. **Krzysztof Szczygielski** (Poland)

Invited Talks

1. Antonio Acín ⇑

ICFO – The Institute of Photonic Sciences — Spain

Certified Many-Body Physics

When studying many-body systems, two approaches have been considered so far: analytical derivations and variational methods. The first provide exact results, as they do not involve any approximations, but scale exponentially with the number of particles, while the second scale much better but only provide estimates with no theoretical guarantees.

Polynomial optimisation methods offer an alternative approach somehow combining the advantage of exact and variational methods: it provides rigorous results, now in the form of upper and lower bounds, in a scalable way. We illustrate this new approach in two paradigmatic many-body problems: the estimation of expectation values in ground states of Hamiltonian operators and in steady states of quantum open systems.

---

2. Álvaro M. Alhambra ⇑

Instituto de Física Teórica (IFT) – CSIC, Madrid — Spain

Modelling Quantum Thermalization with Quantum Computers

In quantum computing and simulation, one of our main goals is to efficiently mimic natural physical phenomena in a controlled manner. The process of thermalization is one such crucial task, for which recently there has been relevant progress.

In this talk, we will showcase important parts of this progress by introducing a recent dissipative evolution that models thermalization in the many-body setting, and that is efficiently implementable in a quantum computer. We then prove the following facts about this dissipative evolution:

1. It faithfully reproduces the dissipation induced by weak coupling to a bath.
2. In the high temperature regime, it very quickly approaches equilibrium.
3. In the low temperature regime, it yields a computational model with the same power as arbitrary quantum computations (BQP-complete).

Taken together, our results show that a family of quasi-local dissipative evolutions has the potential to mirror the success of classical Monte Carlo methods. I will also outline the opportunities that this presents for learning and verification of quantum statistical mechanics.

---

3. Nicholas Chancellor ⇑

Newcastle University — United Kingdom

Understanding and Improving Quantum Annealing

This talk will cover a number of efforts which I am involved in to understand how quantum annealing works in the diabatic regime which is currently experimentally accessible, work on problem encoding in quantum annealing, and a brief discussion on work I have been involved in related to optical optimisation devices. On the topic of understanding the diabatic setting I will review past work, and particularly discuss the relationship between annealing and continuous-time quantum walks. This will focus on understanding beyond the adiabatic theorem based on the energetics of the problem.

I will then discuss recent work on this topic, including understanding how truly continuous time dynamics differs from gate-model digitisation in terms of solving optimisation problems, and efforts to use auxilliary qubits as an effective artificial bath which can aid problems solving by removing energy.

I will then discuss work on problem encoding. The theme here will be the idea of using "hardware aware" encoding methods, in other words, methods based on the knowledge that the problem will eventually be embedded on a device with limited connectivity and where the number of variables in the encoding should be minimised. This includes techniques such as domain-wall encoding (which I will review), but also other methods.

I will present examples where for example converting a quadratic constraint to a linear approximation can greatly reduce connectivity and therefore embedded problem size. I will also discuss a number of other techniques. A major theme here is that many considerations which are not considered very important in traditional optimisation become important when a problem is mapped to an analog annealer.

---

4. Omar Fawzi ⇑

Inria, ENS de Lyon — France

Generalized Quantum Asymptotic Equipartition

We establish a generalized quantum asymptotic equipartition property (AEP) beyond the i.i.d. framework where the random samples are drawn from two sets of quantum states. In particular, under suitable assumptions on the sets, we prove that all operationally relevant divergences converge to the quantum relative entropy between the sets. More specifically, both the smoothed min- and max-relative entropy approach the regularized relative entropy between the sets. Notably, the asymptotic limit has explicit convergence guarantees and can be efficiently estimated through convex optimization programs, despite the regularization, provided that the sets have efficient descriptions.

At a technical level, we establish new additivity and chain rule properties for the measured relative entropy which we expect will have more applications. Based on joint work with Kun Fang and Hamza Fawzi arXiv:2411.04035 and arXiv:2502.07745.

---

5. Edwin Lobo ⇑

Université Libre de Bruxelles — Belgium

Partial Joint-Measurability, Routed Bell Tests, and Their Application to DIQKD

Losses and noise in the transmission channel, which increase with distance, pose a major obstacle to photonics demonstrations of quantum nonlocality and its applications to device-independent protocols such as device-independent quantum key distribution (DIQKD).

Recently, Masini et al [Quantum 8, 1574 (2024)] introduced the notion of partial-joint-measurability to study the limitations that arise from losses and noise in the certification of realistic quantum devices. We generalize this notion slightly and develop simple attacks for DIQKD and randomness generation protocols that can be carried out by an adversary Eve. Our attacks contradict some of the results in literature and shows that post-selection can leak information to Eve, even when Eve is assumed to be memoryless and acting in an i.i.d fashion.

We then apply the insights gained from studying partial-joint-measurability to the certification of quantum correlations in Routed Bell experiments. In these experiments, Bob can route his quantum particle along two possible paths and measure it at two distinct locations - one near and another far from the source. We show that routed Bell protocols extend the distance over which quantum correlations can be certified compared to standard Bell experiments. Notably, quantum correlations generated by performing measurements on a two-qubit state can be used to certify quantum devices at arbitrary distances in a routed Bell experiment, provided Bob performs enough number of measurements.

We also study routed versions of simple DIQKD protocols and show that they are more robust to losses and noise than standard DIQKD protocols.

---

6. **Miguel Navascués** ⇑

Institute for Quantum Optics and Quantum Information (IQOQI), Vienna — Austria

Extrapolation of Quantum Time Series

We consider the problem of predicting future averages of a collection of quantum observables, given noisy averages at past times. The measured observables, the initial state of the physical system and even the nature of the latter are unknown. We nonetheless assume a promise on the energy distribution of the state.

For different types of energy constraints, we show that the optimal extrapolation can be computed up to arbitrary precision through hierarchies of semidefinite programs. Investigating to what extent extrapolation is possible in this framework, we discover highly problematic datasets that allow full predictability at time τ, but only when past averages are known up to precision superexponential in τ. We also find families of self-testing datasets, which allow full predictability under reasonable noise levels and whose approximate realization singles out specific Hamiltonians, states and measurement operators.

We identify "aha! datasets", which drastically increase the predictability of the future statistics of an unrelated measurement, as well as fairly simple datasets that exhibit complete unpredictability at some future time τ, but full predictability at a later time $\tau' > \tau$.

---

7. **Joschka Roffe** ⇑

University of Edinburgh — United Kingdom

Quantum Error Correction with Quantum Low-Density Parity-Check Codes

In this talk, I will discuss recent progress in the design of quantum low-density parity-check (QLDPC) codes as a promising alternative to the surface code for fault-tolerant quantum computation. While QLDPC codes typically demand greater qubit connectivity than the surface code, they offer the potential for significantly reduced qubit overhead.

I will outline methods for constructing QLDPC codes suitable for near-term devices and review recent developments in efficient compilation techniques for fault-tolerant logic.

Finally, I will address the engineering challenges involved in designing decoders for QLDPC codes.

---

8. **Francesco Tacchino** ⇑

IBM Research Zürich — Switzerland

Digital Quantum Simulations in the Era of Quantum Utility

Over the last few decades, quantum information processing has emerged as a gateway towards new, powerful approaches to scientific computing. Quantum technologies are nowadays experiencing a rapid development and could lead to effective solutions in domains ranging from fundamental physics and chemistry to life sciences, optimisation, and artificial intelligence.

In this talk, I will review the state-of-the-art and recent progress in the field, with a focus on the theory of universal quantum simulators, utility-scale quantum computation and quantum-centric supercomputing. I will highlight recent milestone experiments, offering an overview of the IBM Quantum technology and software stack.

I will then present selected applications in the domain of condensed matter and high-energy physics.

---

9. **Yuming Zhao** ⇑

University of Copenhagen — Denmark

An Operator-Algebraic Formulation of Robust Self-Testing

In this talk, I will introduce an operator-algebraic formulation of self-testing in terms of states on C^*-algebras. Many nonlocal games of interest, including XOR games and synchronous games, have a "nice" game algebra in the sense that optimal/perfect strategies correspond to tracial states on the game algebra.

For these nonlocal games, I will show how self-testing is related to the uniqueness of tracial states on the game algebras. I will also discuss the stability of game algebras and the robustness of self-tests.

Based on arXiv:2301.11291 (with Connor Paddock, William Slofstra, and Yangchen Zhou) and arXiv:2411.03259.

Contributed Talks

1. **Flavio Baccari** ⇑

University of Padua — Italy

Average-Computation Benchmarking

Benchmarking schemes currently used in experiments suffer from a fundamental limitation: they cannot be run on the quantum computation of interest. Testing a classically-hard computation is restricted to small scale or shallow depth, where a brute force simulation is possible. There is nevertheless clear evidence that errors can change with the system size, the circuit depth and be gate-dependent. It is therefore essential to devise schemes that can test the behaviour of the actual computation in its final form.

I will present a benchmarking scheme that solves this issue and is applicable to any near-term quantum computation. The scheme is based on taking data from the desired computation and variations of it, chosen in a way that the average output over all computation admits a classical simulation, even when the single computations do not.

I will show benchmarking examples based on a family of solvable channels and argue how the average computation inherits relevant properties of the original computation.

---

2. **Carles Roch i Carceller** ⇑

Lund University — Sweden

Bound Entangled States are Useful in Prepare-and-Measure Scenarios

We show that bipartite bound entangled states make possible violations of correlation inequalities in the prepare-and-measure scenario. These inequalities are satisfied by all classical models as well as by all quantum models that do not feature entanglement.

In contrast to the known Bell inequality violations from bound entangled states, we find that the violations in the prepare-and-measure scenario are sizeable and significantly noise-tolerant.

Furthermore, we show that significantly stronger quantum correlations are made possible by considering bound entanglement with a larger dimension.

---

3. **Christopher Corlett** ⇑

University of Bristol — United Kingdom

Speeding up Quantum Measurement Using Space-Time Trade-Off

We present a scheme for speeding up quantum measurement. The scheme builds on previous protocols that entangle the system to be measured with ancillary systems.

In the idealized situation of perfect entangling operations and no decoherence, it gives an exact space-time trade-off meaning the readout speed increases linearly with the number of ancilla.

We verify this scheme is robust against experimental imperfections through numerical modeling of gate noise and readout errors, and under certain circumstances our scheme can even lead to better than linear improvement in the speed of measurement with the number of systems measured.

This hardware-agnostic approach is broadly applicable to a range of quantum technology platforms and offers a route to accelerate midcircuit measurement as required for effective quantum error correction.

---

4. Marianna Crupi ⇑

Max Planck Institute of Quantum Optics — Germany

Realistic Error Model for Efficient Noise Characterization in Near-Term Quantum Devices

Operations in current quantum devices are affected by various errors, making efficient and accurate noise characterization essential for advancing quantum technologies. Existing methods can only efficiently compute specific process features, leaving out potentially important information.

To resolve this issue we propose a noise model for which the complete process tomography is efficient by construction. Under the assumption that the errors in the device are well represented by a low-Pauli weight channel, our protocol is efficient in time and sample complexity and exhibits a scaling of $O(\text{poly}(n))$.

Our proposed tomography method is based on a randomized product state preparation and measurement scheme and can be applied even for noise characterization of a whole layer of two-qubit Clifford gates.

The scheme is independent of the specific physical implementation and can be readily applied to characterize correlated and coherent errors in 2D architectures of current quantum computers.

---

5. Sophie Egelhaaf ⇑

Université de Genève — Switzerland

Certifying High-Dimensional Quantum Channels

The use of high-dimensional systems for quantum communication opens interesting perspectives, such as increased information capacity and noise resilience. In this context, it is crucial to certify that a given quantum channel can reliably transmit high-dimensional quantum information.

Here we develop efficient methods for the characterization of high-dimensional quantum channels. We first present a notion of dimensionality of quantum channels, and develop efficient certification methods for this quantity.

We consider a simple prepare-and-measure setup, and provide witnesses for both a fully and a partially trusted scenario.

In turn we apply these methods to a photonic experiment and present extensive numerical simulations of the experiment, providing an accurate noise model for the fiber and exploring the potential of more sophisticated witnesses.

Our work demonstrates the efficient characterization of high-dimensional quantum channels, a key ingredient for future quantum communication technologies.

---

6. Patrick Emonts ⇑

Leiden University — Netherlands

Probing Many-Body Bell Correlation Depth with Superconducting Qubits

Quantum nonlocality is a crucial resource for achieving quantum advantages in a variety of applications, ranging from cryptography and certified random number generation via self-testing to machine learning. Nevertheless, the detection of nonlocality, especially in quantum many-body systems, is notoriously challenging.

Here, we report an experimental certification of multipartite Bell correlations in two distinct settings by employing energy as a Bell correlation witness and variationally decreasing the energy.

First, we experimentally prepare the low-energy state of a honeycomb model with 73 qubits and certify its Bell correlations by measuring an energy that surpasses the corresponding classical bound with up to 48 standard deviations.

Second, we certify genuine multipartite Bell correlations up to 24 qubits.

Our results establish a viable approach for preparing and certifying multipartite Bell correlations, which provide a finer benchmark beyond entanglement for quantum devices.

Preprint: `arXiv:2406.17841`.

---

7. Ahana Ghoshal

⇑

University of Siegen — Germany

Optimising Measurement of Correlators for Fermionic Quantum Simulators

Simulating many-body fermionic systems on quantum computers is challenging due to the overheads associated with the encoding of fermionic statistics in qubits, leading to the proposal of native fermionic simulators. This raises the question of characterising the state of a fermionic simulator, which often boils down to measuring certain overlapping sets of few-point correlators from the output of the quantum simulation.

We present a systematic framework for optimising the measurement of two- and four-point correlators in fermionic simulators based on their native fermionic gates. This is obtained by developing a graph representation for the set of correlators to be measured, which is then overlaid by a graph describing the constraints from the fermionic gates.

Optimising measurement settings is then mapped to graph theoretical problems, for which various algorithms can be applied.

We illustrate our methods for the recently proposed fermionic simulators with various sets of two- and four-point correlators.

---

8. Felix Huber

⇑

University of Gdańsk / ICTQT — Poland

Second Order Cone Relaxations for Quantum Max Cut

Quantum Max Cut (QMC), also known as the quantum anti-ferromagnetic Heisenberg model, is a QMA-complete problem relevant to quantum many-body physics and computer science. Semidefinite programming relaxations have been fruitful in designing theoretical approximation algorithms for QMC, but are computationally expensive for systems beyond tens of qubits.

We give a second order cone relaxation for QMC, which optimizes over the set of mutually consistent three-qubit reduced density matrices. In combination with Pauli level-1 of the quantum Lasserre hierarchy, the relaxation achieves an approximation ratio of 0.526 to the ground state energy.

Our relaxation is solvable on systems with hundreds of qubits and paves the way to computationally efficient lower and upper bounds on the ground state energy of large-scale quantum spin systems.

---

9. Marcin Kotowski

⇑

Center for Theoretical Physics, Polish Academy of Sciences (CFT PAN) — Poland

Recurrence in Isolated Quantum Systems and the Converse Quantum Speed Limit

For an isolated quantum system, the problem of recurrence asks for the minimal time when the evolved state returns to a neighborhood of the initial state. It has been a folklore claim that for generic Hamiltonians the recurrence time scales like exp(d), where d is the total dimension of the system.

We provide the first rigorous proof of this claim – we prove an exponential upper bound for arbitrary Hamiltonians and show that the bound is tight for generic (random) Hamiltonians. In the process we also prove an estimate we call the converse quantum speed limit, which is an upper bound on the time sufficient to exit the neighborhood of the initial state.

This is a joint work with M. Oszmaniec.

---

10. **Owidiusz Makuta** ⇑

Leiden University — Netherlands

Frustration Graph Formalism for Qudit Observables

The incompatibility of measurements is the key feature of quantum theory that distinguishes it from the classical description of nature.

Here, we consider groups of d-outcome quantum observables with prime d represented by non-Hermitian unitary operators whose eigenvalues are d^{th} roots of unity. We additionally assume that these observables mutually commute up to a scalar factor being one of the d^{th} roots of unity.

By representing commutation relations of these observables via a frustration graph, we show that for such a group, there exists a single unitary transforming them into a tensor product of generalized Pauli matrices and some ancillary mutually commuting operators.

Building on this result, we derive upper bounds on the sum of the squares of the absolute values and the sum of the expected values of the observables forming a group.

We finally utilize these bounds to compute the generalized geometric measure of entanglement for qudit stabilizer subspaces.

---

11. **James Mills** ⇑

University of Edinburgh — United Kingdom

Efficient Certification for Early Fault-Tolerant Quantum Devices

If experimental progress in building fault-tolerant quantum devices continues at its current pace, certifying the correctness of logical computations run on these machines using classical methods will soon become unfeasible.

In this work we present a protocol, termed logical accreditation, for efficiently certifying computations performed on early fault-tolerant quantum devices. The protocol is sensitive to far more general forms of noise than usually considered in the analysis of quantum error correction (QEC) code performance.

Numerical simulations of surface code performance indicate that this approach can be used to certify quantum advantage experiments involving encoded logical qubits, identify when encoded logical computations start to outperform computation with physical qubits, and assess whether logical circuit error rates are sufficiently low that error mitigation can be efficiently applied to improve the computational output.

---

12. **Mariana Navarro** ⇑

ICFO – The Institute of Photonic Sciences — Spain

Sampling Groups of Pauli Operators to Enhance Direct Fidelity Estimation

Direct fidelity estimation is a protocol that estimates the fidelity between an experimental quantum state and a target pure state. By measuring the expectation values of Pauli operators selected through importance sampling, the method is exponentially faster than full quantum state tomography.

We propose an enhanced direct fidelity estimation protocol that uses fewer copies of the experimental state by grouping Pauli operators before the sampling process. We derive analytical bounds on the measurement cost and estimator variance, showing improvements over the standard method.

Numerical simulations validate our approach, demonstrating that for 8-qubit Haar-random states, our method achieves a one-third reduction in the required number of copies and reduces variance by an order of magnitude using only local measurements.

These results underscore the potential of our protocol to enhance the efficiency of fidelity estimation in current quantum devices.

---

13. Tristan Nemoz ⇑

Télécom Paris — France

How Much Secure Randomness is in a Quantum State?

What is the maximal amount of cryptographically secure randomness can we extract from a given quantum state in the one-shot setting? This fundamental question lies at the heart of quantum cryptography and yet remains open.

In this work we provide simple entropic expressions that capture achievable rates of extraction using both projective measurements and POVMs, recovering the known rates in the asymptotic limit.

In turn, our work provides a simple benchmarking tool for the performance of QRNGs and their security proofs, as well as highlighting some surprising features of secure randomness and measurements.

At the technical level we develop methods to analytically solve optimizations of sandwiched Rényi entropies and generalized Naimark dilations, which could be of independent interest.

This work is based on `arXiv:2410.16447`.

---

14. Attila Portik ⇑

HUN-REN Wigner Research Centre for Physics — Hungary

Scalable Volumetric Benchmarks Based on Clifford and Free-Fermion Operations

The present generation of quantum computers spans diverse platforms with qubit counts approaching the limits of classical simulation. Benchmarking these processors requires a scalable, platform-independent approach.

We propose a volumetric benchmarking framework based on randomly sampling operations from two important groups of unitaries: The Clifford and the free-fermion groups, that are both separately classically simulable but together yield a universal gate set.

A key strength of the proposed benchmark framework lies in its inherent flexibility: Our approach avoids platform-specific rules, enabling the benchmark circuits to be optimized directly for the device being tested. Moreover, these benchmarks are application-oriented, due to the importance of these operations in various tasks such as shadow tomography and quantum chemistry simulations.

By measuring fidelity witnesses rather than performing general state tomography, we avoid the exponential measurement overhead as the number of qubits increases.

---

15. Albert Rico ⇑

Universitat Autònoma de Barcelona — Spain

Certifying Nonlocality of Quantum Operations in the Presence of Noise

While nonlocality of states has been widely studied through Bell games for decades, analogous techniques for quantum channels started to receive attention recently. Yet, device-independently certifying nonlocal properties of quantum operations is essential to ensure performance of most quantum protocols.

In this Talk we present our recent results in channel nonlocality certification, only from the probabilistic correlations between their local inputs and outputs.

First we review the basic framework and related work. Then we present our results, which certify nonlocal resources (like entanglement or communication) present in target channels.

Finally we consider different models of decoherent noise, showing e.g., that dephasing models are in theory compatible with maximal entanglement generation. We quantify both the amount of nonlocality of channels and their component resisting complete dephasing noise, and show that the latter is in fact required even for decoherence-free quantum protocols.

---

16. Michał Studziński ⇑

University of Gdańsk / ICTQT — Poland

One-to-One Correspondence Between Deterministic Port-Based Teleportation and Unitary Estimation

Port-based teleportation (PBT) is a variant of quantum teleportation, where the receiver can choose one of the ports in his part of the entangled state shared with the sender, but cannot apply other recovery operations.

We show that the optimal fidelity of deterministic PBT (dPBT) using $N = n + 1$ ports to teleport a d-dimensional state is equivalent to the optimal fidelity of d-dimensional unitary estimation (UE) using n calls of the input unitary operation.

From any given dPBT, we can explicitly construct the corresponding UE protocol achieving the same optimal fidelity, and vice versa.

Using the obtained one-to-one correspondence between dPBT and UE, we derive the asymptotic optimal fidelity of PBT, which improves the previous results.

We also show that the optimal fidelity of UE for the case $n \leq d-1$ is $F = (n+1)/d^2$, and this fidelity is equal to the optimal fidelity of unitary inversion with $n \leq d+1$ calls of the input unitary operation even if we allow indefinite causal order among the calls.

---

17. Elna Svegborn ⇑

Lund University — Sweden

Quantum Inputs in the Prepare-and-Measure Scenario and Stochastic Teleportation

We investigate prepare-and-measure scenarios in which a sender and a receiver use entanglement to send quantum information over a channel with limited capacity. We formalise this framework, identify its basic properties and provide numerical tools for optimising quantum protocols for generic communication tasks.

The seminal protocol for sending quantum information over a classical channel is teleportation. We study a natural stochastic generalisation in which the sender holds N qubits from which the receiver can recover one on demand. We show that with two bits of communication alone, this task can be solved exactly for all N, if the sender and receiver have access to stronger-than-quantum nonlocality.

We then consider entanglement-based protocols and show that these can be constructed systematically. In particular, we show that by using multi-particle entangled measurements, one can construct a universal stochastic teleportation machine, whose teleportation fidelity is independent of the quantum input.

---

18. Peter Tirler ⇑

University of Innsbruck — Austria

Randomness Certification on a Qudit Trapped Ion Processor

High quality randomness is an important ingredient in many processes affecting our daily lives. Classical physics, however, being deterministic in nature, can only generate pseudorandom data, whereas in quantum physics its inherent randomness can be used to generate data that is provably random.

Nearly all commonly implemented protocols do so using a two-qubit Bell state measured in a set of orthogonal bases, generating up to one bit of randomness per party.

In our recent work we use higher-dimensional quantum states, so-called qudits, to move beyond the capabilities of bit-based randomness certification. This enables various more general schemes of randomness certification, and we can, e.g., use POVM four-outcome measurements to certify more than one bit of local randomness per party.

Using an ion trap quantum processor capable of qudit-based computation we can show that even in the presence of noise, the randomness certified exceeds the threshold of one bit of local randomness.

---

19. **Lewis Wooltorton** ⇑

Inria, ENS de Lyon — France

A composable Framework for Device-Independent State Certification with Local Operations and Classical Communication

Device-independent state certification (DISC) aims to certify the presence of a pure entangled state produced by a source without trusting its inner workings, or the measurements performed on it.

An important aspect of any DISC protocol is that the certified state can be used for a future task. For applications such as cryptography, it then becomes crucial that a composable security framework is adopted. This guarantees that the certification remains valid when using the protocol as a subroutine in larger system.

To address this need, we develop a composable approach to DISC under the assumption that the source prepares a finite sequence of independent but not identically distributed states.

Our composable security result is then expressed in terms of the "extractability" guaranteed by a given Bell violation, a DI variant of the fidelity introduced for robust self-testing.

We further develop techniques to bound this quantity in certain scenarios under local operations and classical communication.

This is a joint work with Rutvij Bhavsar and Joonwoo Bae.

Posters

1. Nicola D'Alessandro ⇑

Lund University — Sweden

Semidefinite Relaxations for High-Dimensional Entanglement in the Steering Scenario

We introduce semidefinite programming hierarchies for benchmarking relevant entanglement properties in the high-dimensional steering scenario.

Firstly, we provide a general method for detecting the entanglement dimensionality through certification of the Schmidt number. Its key feature is that the computational cost is independent of the Schmidt number under consideration.

Secondly, we provide a method to estimate the fidelity of the source with any maximally entangled state.

Using only basic computational means, we demonstrate the usefulness of these methods, which can be directly used to analyse experiments on high-dimensional systems.

---

2. Raffaele D'Avino ⇑

ICFO – The Institute of Photonic Sciences — Spain

Entanglement Assistance in Energy-Constrained Framework

The semi-device-independent approach offers a framework for prepare-and-measure quantum protocols where the devices involved do not need to be fully characterized or trusted.

This approach has been extensively studied under various physical constraints on the emitted states, including the scenario where the average energy of the states emitted by the source is bounded.

Under this condition, it has been shown that quantum correlations surpass classical correlations.

We observe, both numerically and analytically, that the inclusion of entanglement can further expand the achievable set of correlations. This finding has implications for randomness generation.

---

3. Stefan Bäuml ⇑

Free University of Berlin — Germany

Improved Finite-Size Key Rates for Discrete-Modulated Continuous Variable Quantum Key Distribution Under Coherent Attacks

Continuous variable quantum key distribution (CVQKD) with discrete modulation combines advantages of CVQKD, such as the implementability using readily available technologies, with advantages of discrete variable quantum key distribution, such as easier error correction procedures.

We consider a prepare-and-measure CVQKD protocol, where Alice chooses from a set of four coherent states and Bob performs a heterodyne measurement, the result of which is discretised in both key and test rounds.

We provide a security proof against coherent attacks in the finite-size regime based on the generalised entropy accumulation theorem. We compute the corresponding asymptotic key rate imposing a photon-number cutoff and recent advances in conic optimisation.

Our method yields significant improvements on key rates: at metropolitan distances, it provides positive key rates for block sizes of the order of 10^8 rounds, orders of magnitude smaller compared to previous works.

---

4. **Tomas Crosta** ⇑

Universite de Bordeaux — France

Ground State Estimation in Symmetric Hamiltonians of Quantum Max-Cut

Quantum Max-Cut consists in estimating the maximum energy of a Hamiltonian whose interactions are modulated by the Pauli matrices $XX + YY + ZZ$. This problem lies within the QMA complexity class, rendering it valuable for benchmarking state approximation algorithms.

In this contribution, we study Hamiltonians that are invariant under the action of a group G, thereby enabling the analysis of higher-dimensional systems.

---

5. **Hirak Kanti Ghosh** ⇑

University of Warwick — United Kingdom

Testing Identicality Under a Depolarizing Promise

In the NISQ era, quantum computations are inherently noisy, often compromising output reliability. This makes it essential to develop efficient methods for testing the quality of components, such as gates, in NISQ quantum computers.

By modelling noise as a black-box quantum channel acting after each gate, the problem can be cast as a quantum channel certification task; allowing gate quality to be quantified, in diamond or trace distance, by testing if the noise channel is either the identity channel or is "ε-far" from it.

If the black-box noise channel is promised to be depolarizing, with the depolarizing parameter unknown, we present a non-adaptive, ancilla-free tester with $O(1/\varepsilon^2)$ black-box queries and $O(1/\varepsilon)$ incoherent measurements.

In trace distance, the tester requires $O(1/\varepsilon)$ queries and $O(1/\varepsilon 0.5)$ incoherent measurements.

This compares favourably to the existing identity testing protocols, which assume no structure in the noise and have query complexities that scale with system size.

---

6. **Mengyao Hu** ⇑

Leiden University — Netherlands

Improved Nonlocality Certification via Bouncing between Bell Operators and Inequalities

Bell nonlocality, an intrinsic feature of quantum mechanics, can be certified via Bell inequality violations, making its experimental certification crucial. We propose an optimization scheme to improve nonlocality certification by exploring flexible mappings between Bell inequalities and Hamiltonians corresponding to the Bell operators; arXiv:2407.12347.

We show that several Hamiltonian models can be mapped to new inequalities with improved classical bounds than the original one, enabling a more robust detection of nonlocality. Conversely, mapping fixed inequalities to Hamiltonians maximizes quantum violations while accounting for experimental imperfections.

As a demonstration, we apply this method to an XXZ-like honeycomb-lattice model using over 70 superconducting qubits. The successful application of this technique may open new avenues for developing more practical and noise-resilient nonlocality certification techniques and enable broader experimental explorations.

---

7. **Hubert Kołcz** ⇑

Warsaw University of Technology — Poland

Verification of qRNG Using qGAN and Classification Models

The study presents a multi-modal framework for quantum random number generator (QRNG) verification, integrating quantum generative adversarial networks (qGANs) with classical machine learning. Benchmarking IBM Qiskit simulations against Rigetti Aspen-M-3 (79 qubits) and IonQ Aria-1 (25 qubits) hardware, we analyze CHSH game scores (Rigetti: 0.8036, IonQ: 0.8362) and gate fidelities (Rigetti: 93.6% vs. IonQ: 99.4% two-qubit fidelity). Three parallel methods are developed:

(a) A neural network classifier (58.7% accuracy in quantum-state discrimination);

(b) Markov chain-enhanced logistic regression identifying bit biases (59% '1' frequency in Type 2 vs. 54% in Types 1/3);

(c) A 12-qubit qGAN quantifying distribution similarity via relative entropy (near-zero) and discriminator loss (3.7–16).

Results show hybrid models enable platform-agnostic validation, with IonQ's higher-fidelity systems yielding superior certifiable randomness despite lower qubit counts, while classical simulators exhibit predictable biases.

---

8. **Tomás Fernández Martos** ⇑

ICFO – The Institute of Photonic Sciences — Spain

Measurement-Device-Independent QRNG Based on Mode-Competition in a Gain-Switched VCSEL

In this work, we present a new measurement-device-independent QRNG developed within Quside Technologies S.L. based on operating a vertical-cavity surface-emitting laser (VCSEL) in a gain-switching manner. We prove security in the finite-size regime using the Entropy Accumulation Theorem and obtain positive rates for as low as 7×10^4 rounds.

---

9. **Piotr Masajada** ⇑

Institute of Fundamental Technological Research, Polish Academy of Sciences (IPPT PAN) — Poland

Local Purity Distillation and the Geometric Entanglement

Quantifying entanglement in a given quantum state remains a challenging problem. Over the years, several entanglement measures have been developed, each with its own advantages and limitations. Among them, geometric entanglement stands out as a particularly useful quantifier. However, computing its value is computationally demanding.

In this poster, we present a method for efficiently computing geometric entanglement for mixed bipartite and pure multipartite systems using semi-definite programming. Our approach opens new possibilities for practical applications, particularly in entanglement detection and estimation.

We illustrate this by evaluating entanglement in a class of bound entangled states, as well as in output states of certain noisy quantum channels. Our method draws upon techniques from two fundamental quantum resource theories: the resource theory of entanglement and thermodynamics.

---

10. **Patryk Michalski** ⇑

University of Warsaw — Poland

All-in-One Bell Inequalities for Binary Observables

Bell inequalities not only reveal the nonlocal nature of quantum theory but also serve as tools for certifying quantum properties in device-independent protocols. Aiming to capture these two essential features, we address the problem of designing Bell inequalities for arbitrary numbers of binary measurements.

Central to our work is a general characterization of a matrix that enables the construction of both standard and bilocal Bell inequalities via a sum-of-squares decomposition. We derive the conditions that ensure the presence of quantum advantage and show that under certain further assumptions, the entire quantum realization can be weakly or exactly self-tested.

Our framework provides a unified toolset that covers several well-known examples from the literature – including the CHSH and elegant Bell inequalities – and supports the systematic exploration of quantum correlations in increasingly complex settings.

---

11. **Morteza Moradi** ⇑

University of Warsaw — Poland

Intrinsic Randomness of Noisy POVMs

Quantum measurements generate intrinsic randomness, a feature with no classical counterpart. For instance, measuring a pure state in a mutually unbiased basis yields outcomes that are fundamentally unpredictable, regardless of prior knowledge. In practice, measurements are noisy, introducing extrinsic randomness due to ignorance.

In adversarial models, this ignorance is represented by quantum side information held by an eavesdropper. We quantify the intrinsic randomness remaining in noisy quantum measurements by computing the optimal guessing probability, minimized over all input states, for two noise models.

Then, we show that when measuring a pure state in an unbiased basis, the noise can be fully attributed to either the state or the measurement device without affecting security. However, a case study reveals that distributing noise across both can significantly enhance the adversary's predictive power, highlighting a subtle dependence on noise allocation.

---

12. **Younes Naceur** ⇑

ICFO – The Institute of Photonic Sciences — Spain

Certified Exact Bounds on Optimization Problems in Quantum Theory

Obtaining lower bounds on optimization problems by making use of non-commutative Moment- and Sums-of-Squares hierarchies, such as the NPA-hierarchy, was shown to complement existing upper bound variational techniques for problems in quantum information theory and many-body quantum physics.

In the literature these bounds are said to certify, that a given solution to a problem, e.g., the ground state energy of a given Hamiltonian, doesn't exceed a numerical bound obtained by solving a series of semidefinite programs.

Due to the numerical nature of semidefinite programs, sometimes wrong numerical bounds on the objective function are issued by the solver due to limiting precision. Given this absence of properly certified bounds using numerical certificates as in the NPA-hierarchy, we present this method to obtain exact lower bounds on non-commutative optimization problems from possibly incorrect numerical bounds as obtained through semidefinite programs.

---

13. Ranieri Vieira Nery ⇑

ICFO – The Institute of Photonic Sciences — Spain

Certification of Entangled Measurements

We propose a test for entanglement of measurement operators—natural counterparts of shared states in generic quantum networks—in the form of a hierarchy of moment matrices, and inspired by the hierarchy of Moroder et al.

We introduce a description of the moment matrices in terms of separable channels, which allows for tests of the separability of measurement operators directly from the structure of the resulting matrices.

We show the functioning of the test by applying it to a distribution compatible with the bilocal network and we conclude by commenting on potential extensions of the test.

---

14. Robert Okuła ⇑

Gdańsk University of Technology — Poland

Device-Independent Shannon Entropy Certification

Quantum technologies promise advancements in information processing and communication technology, including random number generation (RNG). Using Bell inequalities, a user of a quantum RNG hardware can certify that the values provided by an untrusted device are truly random.

This problem has been extensively studied for von Neumann and min-entropy as the measure of randomness. However, in this paper, we analyze the feasibility of such verification for 2-bit quantum RNG using the Shannon entropy.

We investigate how the usability of various Bell inequalities differs depending on the presence of noise. Moreover, we present the benefit of certification for Shannon compared to min-entropy.

---

15. Ignacio Perito ⇑

ICFO – The Institute of Photonic Sciences — Spain

Device-Independent Randomness Certification Without Self-Testing

Most security protocols rely on pseudorandomness generators that are assumed secure against current attacks. As quantum measurements are the only source of true randomness known in nature, harnessing this in a device-independent manner – without trusting the functioning of the devices – is crucial for technologies that aim to remain secure regardless of improvements in attack strategies.

One way to achieve this is through self-testing, but this is only proven in some cases and checking the feasibility of real world applications requires numerical approaches that are very expensive.

Here, I will focus on a more flexible approach based on weaker notions of certification that, without need of full characterization, still guarantee the presence of true randomness. I will discuss how this is related to the geometry of the correlation set and illustrate it with some examples.

I will also show how qudit systems can be used to outperform qubits when it comes to randomness generation in an experimentally accessible way.

---

16. Aby Philip ⇑

Institute of Fundamental Technological Research, Polish Academy of Sciences (IPPT PAN) — Poland

Device-Independent Certification of Multipartite Distillable Entanglement

Quantum networks consist of various quantum technologies, spread across vast distances, and involve various users at the same time. Certifying the functioning and efficiency of the individual components is a task that is well studied and widely used. However, the power of quantum networks can only be realized by integrating all the required quantum technologies and platforms across a large number of users.

In this work, we demonstrate how to certify the distillable entanglement available in multipartite states produced by quantum networks, without relying on the physical realization of its constituent components. We do so by using the paradigm of device independence.

---

17. Martin J. Renner ⇑

ICFO – The Institute of Photonic Sciences — Spain

Exact Steering Bound for Two-Qubit Werner States

We propose a local hidden state model for two-qubit Werner states with a visibility of 1/2. Our model applies to the full class of positive operator-valued measures (POVMs), extending Werner's original model, which was limited to projective measurements.

Being tight, our model determines the exact steering bound for two-qubit Werner states. Notably, we demonstrate that for this family of states, POVMs do not offer any advantage over projective measurements in demonstrating quantum steering. This not only resolves a long-standing open question but also marks a significant step toward understanding the role of generalized measurements (POVMs) in certifying quantumness, particularly in the context of quantum steering and Bell nonlocality.

Additionally, our findings contribute to the study of measurement incompatibility, as we identify the critical visibility beyond which all qubit measurements become jointly measurable.

---

18. Michał Siemaszko ⇑

University of Warsaw — Poland

Time Series Prediction with Photonic Quantum Memristor

Time series prediction is essential in fields like weather forecasting and finance. Reservoir Computing provides a powerful approach by projecting inputs into a nonlinear dynamical space. Recently, quantum systems have been explored as reservoirs due to their potential advantages in memory and nonlinearity.

In this work, we use a photonic quantum memristor as the key component of a quantum reservoir. We show that it provides both nonlinearity and temporal memory, enabling accurate performance on the NARMA benchmark task. A single memristor achieves an average relative error below 5%.

We also present numerical simulations involving multiple memristors to analyze how their configuration affects the reservoir's predictive capabilities.

---

19. Anna Steffinlongo ⇑

ICFO – The Institute of Photonic Sciences — Spain

Simulating Noncausality with Quantum Control of Causal Orders

We demonstrate that a quantum switch—a physically realizable process with indefinite causal order—can be used to simulate the structure of a noncausal process, the Lugano process, by implementing the SHIFT measurement.

Although previously thought to witness noncausality, this measurement instead certifies causal nonseparability. We further generalize this approach by showing that a broader class of noncausal processes can be simulated with quantum control of classical communication.

These results pave the way toward physically realizing noncausal processes.

---

20. Daiki Suruga ⇑

Nagoya University – Japan

Direct Sum Theorems Beyond Query Complexity

A fundamental question in computer science is: Is it harder to solve k instances independently than to solve them simultaneously? This question, known as the direct sum question or direct sum theorem, has been paid much attention in several research fields including query complexity, communication complexity and information theory. Despite its importance, however, little has been discovered in many other research fields.

In this paper, we introduce a novel framework that extends to classical/quantum query complexity, PAC-learning for machine learning, statistical estimation theory, and more. Within this framework, we establish several fundamental direct sum theorems.

---

21. Jakub Szczepaniak ⇑

University of Warsaw — Poland

Entanglement Detection in Hilbert Spaces of Arbitrary Local Dimension

Realization of many protocols in quantum technologies depends on the entanglement. Thus, before applying them, we would like to ensure that the states we are using are entangled. One way to detect entanglement is by entanglement witnesses. Here we present a method of it that offers good robustness against noise and simple experimental realization.

Additionally, the witnesses that we constructed show better robustness against noise for Hilbert spaces of local dimension higher than 2, thus they show another advantage of considering higher local dimensions.

---

22. Krzysztof Szczygielski ⇑

University of Gdańsk — Poland

Covariant Decomposable Maps on C^*-Algebras and Quantum Dynamics

We characterize covariant positive decomposable maps between unital C^*-algebras in terms of a dilation theorem, which generalizes a seminal result by H. Scutaru; `Rep. Math. Phys. 16 (1):79-87, (1979)`.

As a case study, we provide a certain characterization of the operator sum representation of maps on matrix algebras, covariant with respect to the maximal commutative subgroup of $\mathbb{U}(n)$.

A connection to quantum dynamics is established by specifying sufficient and necessary conditions for covariance of D-divisible (decomposably divisible) quantum evolution families, recently introduced in `J. Phys. A: Math. Theor.` **56** `(2023) 485202`.
