INTERNATIONAL YEAR OF
Quantum Science
and Technology

INDIAN INSTITUTE OF SCIENCE
भारतीय विज्ञान संस्थान

20th Edition of International Conference

# TQC - 2025

## Theory of Quantum Computing, Communication and Cryptography

15 –19 September 2025

National Science Seminar Complex,
Indian Institute of Science, Bengaluru, India

# Contents

# About TQC 2025

## TQC

The Theory of Quantum Computation, Communication and Cryptography (TQC) is a leading annual international conference for students and researchers working in the theoretical aspects of quantum information science. The scientific objective is to bring together the theoretical quantum information science community to present and discuss the latest advances in the field.

## TQC 2025

The 20th edition of the conference, TQC 2025 is being hosted by the Indian Institute of Science, Bengaluru (IISc), India. The conference is scheduled from 15 – 19 September 2025 at National Science Seminar Complex (J. N. Tata Auditorium), IISc. A pre-conference tutorials session is scheduled on 13 and 14 September 2025 at the TCS Smart X Hub Seminar Room G22 (IDR building, behind CeNSE), IISc.

The scientific program of TQC 2025 features four invited talks selected by the steering committee and 77 contributed talks with 200+ posters selected by the program committee after the peer review process.

## TQC 2025 Organizers

**Local Organizing Chair :**

C. M. Chandrashekar, IISc, Bengaluru
chandracm@iisc.ac.in

**Program Chair:**

Bill Fefferman, University of Chicago, USA
tqc2025chair@gmail.com

# Local Organizing Team – TQC 2025

The successful organization of TQC 2025 relies on the dedicated efforts of our local organising team. They are responsible for handling logistics, technical support, accommodation, registration, social events, and other key aspects of the conference. For any specific queries, participants may directly contact the concerned team members listed below.

| Name | Email ID | Logistics Support |
|---|---|---|
| Sujai Matta | sujaimatta@iisc.ac.in | Accommodation-related queries |
| Sanchari Chakraborti | sancharic@iisc.ac.in | International travel & visa assistance |
| Soumya Asokan | soumyaasokan@iisc.ac.in | Registration |
| Kanad Sengupta | kanads@iisc.ac.in | Technical support |
| Aastha Zalone | aasthapz@iisc.ac.in | Social events |
| Kunal Shukla | kunalshukla@iisc.ac.in | Technical support |
| Akshai Krishnan T | akshait@iisc.ac.in | Catering |
| Anirudh Verma | anirudhverma@iisc.ac.in | Technical support |
| Ajay J | ajayj1@iisc.ac.in | Volunteer coordination |
| Govinda | govinda@iisc.ac.in | Logistics |
| Sreyas P Dinesh | sreyasdinesh@iisc.ac.in | Catering |
| Midhuna | ms21249@iisermohali.ac.in | Social events |
| Namitha Revankar | namithar@iisc.ac.in | Logistics |

## Schedule for 15th September, 2025 (Day 1 - Monday)

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 09:00–10:30 | Registration | | |
| 10:30–11:00 | High Tea | | |
| 11:00–11:30 | Welcome Note | | |
| 11:30–12:30 | The New Frontier in Low-Overhead Fault-Tolerant Quantum Computation<br>*Hayata Yamasaki* | | |
| 12:30–14:00 | Lunch Break | | |
| 14:00–14:30 | The Clifford hierarchy for one qubit or qudit<br>*Nadish de Silva et al.* | Maximal device-independent randomness in every dimension<br>*Máté Farkas et al.* | Commuting Local Hamiltonians Beyond 2D<br>*John Bostanci et al.* |
| 14:30–15:00 | Rise of conditionally clean ancillae for efficient quantum circuit constructions<br>*Tanuj Khattar et al.* | A quantum cloning game with applications to quantum position verification<br>*Llorènc Escola Farràs et al.* | Optimal Hamiltonian simulation for low-energy states<br>*Rolando Somma et al.* |
| 15:00–15:30 | Locality and Parameter Tradeoffs for Subsystem Codes<br>*Samuel Dai et al.* | PKE and ABE with Collusion-Resistant Secure Key Leasing<br>*Fuyuki Kitagawa et al.* | Simulating chaos without chaos<br>*Andi Gu et al.* |
| 15:30–16:00 | Tea Break | | |
| 16:00–16:30 | Testing classical properties from quantum data<br>*Matthias C. Caro et al.* | Self-testing in the compiled setting via tilted-CHSH inequalities<br>*Connor Paddock et al.* | Quantum Routing and Entanglement Dynamics Through Bottlenecks<br>*Dhruv Devulapalli et al.* |
| 16:30–17:00 | Chasing shadows with Gottesman-Kitaev-Preskill codes<br>*Jonathan Conrad et al.* | Commitments are equivalent to statistically verifiable one-way state generators<br>*Rishabh Batra et al.* | Mixing time of quantum Gibbs sampling for random sparse Hamiltonians<br>*Akshar Ramkumar et al.* |
| 17:00–17:30 | Unitary Designs from Random Symmetric Quantum Circuits<br>*Hanqing Liu et al.* | Untelegraphable Encryption and its Applications<br>*Jeffrey Champion et al.* | A Hierarchy of Spectral Gap Certificates for Frustration-Free Spin Systems<br>*Kshiti Sneh Rai et al.* |
| 17:30–19:00 | Poster Session – 1 | | |
| 19:00–21:00 | Dinner | | |

## Schedule for 16th September, 2025 (Day 2 - Tuesday)

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 09:00–09:30 | | | |
| 09:30–10:30 | Composing Quantum Algorithms<br>*Stacey Jeffery* | | |
| 10:30–11:00 | Tea Break | | |
| 11:00–11:30 | Towards Non-Abelian Quantum Signal Processing: Efficient Control of Hybrid Continuous- and Discrete-Variable Architectures<br>*Shraddha Singh et al.* | Phase Error Rate Estimation in QKD with Imperfect Detectors<br>*Devashish Tupkary et al.* | Quantum Purity Amplification: Optimality and Efficient Algorithm<br>*Zhaoyi Li et al.* |
| 11:30–12:00 | Polylog-Time and Constant-Space-Overhead Fault-Tolerant Quantum Computation with Quantum LDPC Codes<br>*Shiro Tamiya et al.* | Asymptotic Robustness of Entanglement in Noisy Quantum Networks and Graph Connectivity<br>*Fernando Lledó et al.* | A Quantum Algorithm for Khovanov Homology<br>*Alexander Schmidhuber et al.* |
| 12:00–12:30 | Quantum Search with In-Place Queries<br>*Blake Holman et al.* | Adaptive Channel Reshaping for Improved Entanglement Distillation<br>*Dina Abdelhadi et al.* | Quantum Algorithm for Reversing Unknown Unitary Evolutions<br>*Yu-Ao Chen et al.* |
| 12:30–13:00 | The Complexity of Gottesman–Kitaev–Preskill (GKP) States<br>*Lukas Brenner et al.* | Quantum Position Verification in One Shot: Parallel Repetition of the f-BB84 and f-Routing Protocols<br>*Llorènc Escola Farràs et al.* | Classical and Quantum Algorithms for Characters of the Symmetric Group<br>*Sergey Bravyi et al.* |
| 13:00–14:00 | Lunch Break | | |

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 14:00–14:30 | Full Classification of Pauli Lie Algebras<br>*Gerard Aguilar Tapia et al.* | No Quantum Advantage Without Classical Communication: Fundamental Limitations of Quantum Networks<br>*Justus Neumann et al.* | Directed st-Connectivity with Few Paths is in Quantum Logspace<br>*Roman Edenhofer et al.* |
| 14:30–15:00 | Uniformity Testing When You Have the Source Code<br>*Clément Canonne et al.* | Generalized Inner Product Estimation with Limited Quantum Communication<br>*Srinivasan Arunachalam et al.* | The Space Just Above One Clean Qubit<br>*Dale Jacobs et al.* |
| 15:00–15:30 | A Full Practical Theory of the Clifford Group Commutant<br>*Lennart Bittel et al.* | Composably Secure Delegated Quantum Computation with Weak Coherent Pulses<br>*Maxime Garnier et al.* | Quantum Threshold is Powerful<br>*Jackson Morris et al.* |
| 15:30–16:00 | Factoring an Integer with Three Oscillators and a Qubit<br>*Lukas Brenner et al.* | Polynomial-Time Quantum and Classical Algorithms for Representation Theoretic Multiplicities<br>*Vojtěch Havlíček et al.* | Quantum Computational Complexity of Matrix Functions<br>*Santiago Cifuentes et al.* |
| 16:00–16:30 | Tea Break | | |
| 16:30–17:30 | Industry Talk - Quantum Computing at Fujitsu | | |
| 17:30–18:30 | Mentorship Session Between Junior and Senior Researchers | | |
| 19:00–21:00 | Dinner | | |

## Schedule for 17th September, 2025 (Day 3 - Wednesday)

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 09:00–09:30 | | | |
| 09:30–10:30 | Quantum algorithms for codes and lattices based on Regev's reduction (joint work with Jean-Pierre Tillich)<br>*André Chailloux* | | |
| 10:30–11:30 | Business Meeting and Tea Break | | |
| 11:30–12:00 | SPAM-Free Sound Certification of Quantum Gates via Quantum System Quizzing<br>*Nikolai Miklin et al.* | A Meta-Complexity Characterization of Quantum Cryptography<br>*Bruno Cavalar et al.* | Quantum SAT Problems with Finite Sets of Projectors Are Complete for a Plethora of Classes<br>*Ricardo Rivera Cardoso et al.* |
| 12:00–12:30 | Parallel Logical Measurements via Quantum Code Surgery<br>*Alexander Cowtan et al.* | Copy-Protecting Puncturable Functionalities, Revisited<br>*Prabhanjan Ananth et al.* | Classically Estimating Observables of Noiseless Quantum Circuits<br>*Armando Angrisani et al.* |
| 12:30–13:00 | Quantum Catalytic Space<br>*Harry Buhrman et al.* | Additivity and Chain Rules for Quantum Entropies via Multi-Index Schatten Norms<br>*Omar Fawzi et al.* | Forrelation Is Extremally Hard<br>*Uma Girish et al.* |
| 13:00–14:00 | Lunch Break | | |
| 14:00–16:00 | Poster Session – 2 | | |
| 16:00–17:30 | Poster + Tea Break | | |
| 17:30–19:30 | Cultural Event –Indian Musical Instruments Ensemble Concert by Layataranga | | |
| 19:30–21:00 | Dinner | | |

## Schedule for 18th September, 2025 (Day 4 - Thursday)

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 09:30–10:30 | Post-quantum security of lattice-based cryptosystems<br>*Rajendra Kumar* | | |
| 10:30–11:00 | Tea Break | | |
| 11:00–11:30 | Adaptive Syndrome Extraction<br>*Noah Berthusen et al.* | Pseudorandom Function-like States from Common Haar Unitary<br>*Minki Hhan et al.* | Quantum Perfect Matchings<br>*David Cui et al.* |
| 11:30–12:00 | Bounding the Computational Power of Bosonic Systems<br>*Varun Upreti et al.* | Efficient Quantum Pseudorandomness from Hamiltonian Phase States<br>*John Bostanci et al.* | Polynomial-Time Quantum Gibbs Sampling for Fermi-Hubbard Model at Any Temperature<br>*Štěpán Šmíd et al.* |
| 12:00–12:30 | X-Arability of Quantum States<br>*Harm Derksen et al.* | Quantum One-Time Programs, Revisited<br>*Aparna Gupte et al.* | Generalized Short Path Algorithms: Towards Super-Quadratic Speedup over Markov Chain Search for Combinatorial Optimization<br>*Shouvanik Chakrabarti et al.* |
| 12:30–14:00 | Lunch Break | | |
| 14:00–19:00 | Excursion: Bhoganandiswara Temple (9th Century Monument) and Nandi Hills | | |
| 19:00–21:00 | Banquet Dinner | | |

## Schedule for 19th September, 2025 (Day 5 - Friday)

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 09:00–09:30 | | | |
| 09:30–10:00 | A Unified Theory of Quantum Neural Network Loss Landscapes<br>*Eric R. Anschuetz et al.* | Strategic Codes: The Universal Spatio-Temporal Framework for Quantum Error-Correction<br>*Andrew Tanggara et al.* | Quantum Spin Chains and Symmetric Functions<br>*Marcos Crichigno et al.* |
| 10:00–10:30 | Online Learning of Quantum Processes<br>*(Asad Raza et al.)* | Tesseract: A Search-Based Decoder for Quantum Error Correction<br>*Laleh Aghababaie Beni et al.* | |
| 10:30–11:00 | Tea Break | | |
| 11:00–11:30 | Quantum Advantage for Learning Shallow Neural Networks with Natural Data Distributions<br>*Laura Lewis et al.* | Orthogonality Broadcasting and Quantum Position Verification<br>*(Ian George et al.)* | Testing and Learning Structured Quantum Hamiltonians<br>*Srinivasan Arunachalam et al.* |
| 11:30–12:00 | Hamiltonian Locality Testing via Trotterized Postselection<br>*John Kallaugher et al.* | Unitary Designs of Symmetric Local Random Circuits<br>*Yosuke Mitsuhashi et al.* | The Rotation-Invariant Hamiltonian Problem is QMAEXP-Complete<br>*Jon Nelson et al.* |
| 12:00–12:30 | Classical Estimation of the Free Energy and Quantum Gibbs Sampling from the Markov Entropy Decomposition<br>*Samuel Scalet et al.* | A New World in the Depths of Microcrypt: Separating OWSGs and Quantum Money from QEFID<br>*Amit Behera et al.* | Time-Dependent Hamiltonian Simulation via Magnus Expansion: Algorithms and Discrete Superconvergence for Unbounded Hamiltonians<br>*Di Fang et al.* |

| Time | Session 1 | Session 2 | Session 3 |
|---|---|---|---|
| 12:30–13:00 | Towards a Complexity-Theoretic Dichotomy for (2+1)-Dimensional TQFT Invariants<br>*Eric Samperton et al.* | Impossibility of Hyperefficient Shadow Tomography: Unbounded Multiple-Copy Secure Copy-Protection<br>*Alper Cakan et al.* | RE-Completeness of Entangled Constraint Satisfaction Problems<br>*Eric Culf et al.* |
| 13:00–13:30 | Closing Remarks | | |
| 13:30–14:30 | Lunch Break | | |
| 14:30–21:00 | Departure | | |

## Day 1: September 15, 2025, Monday

### Time: 11:30 (Invited talk)

### The New Frontier in Low-Overhead Fault-Tolerant Quantum Computation

*Hayata Yamasaki* [1]

IS

[1] The University of Tokyo , Japan

Fault-tolerant quantum computation (FTQC) is essential for unlocking the full potential of quantum computation, enabling the accurate simulation of noiseless quantum mechanics in our inherently noisy world. Conventionally, FTQC requires overheads that grow polylogarithmically in both the number of qubits and the computational runtime. However, a series of our recent works challenges this conventional understanding by introducing new protocols and analyses that substantially reduce these overheads. These developments open the door to the new frontier in low-overhead FTQC, offering improved scaling in space and time across a broad range of fault-tolerant protocols. In this talk, I will present an overview of our key contributions, highlight their conceptual foundations, and discuss their implications for the future design of scalable quantum computers.

## Session 1

Time: 14:00

### The Clifford hierarchy for one qubit or qudit

*Nadish de Silva*[1], *Oscar Lautsch*[1]

[1] Simon Fraser University

The Clifford hierarchy is a nested sequence of sets of quantum gates that can be fault-tolerantly performed using gate teleportation within standard quantum error correction schemes. The groups of Pauli and Clifford gates constitute the first and second ’levels’, respectively. Non-Clifford gates from the third level or higher, such as the T gate, are necessary for achieving fault-tolerant universal quantum computation. Since it was defined twenty-five years ago by Gottesman-Chuang, two questions have been studied by numerous researchers. First, precisely which gates constitute the Clifford hierarchy? Second, which subset of the hierarchy gates admit efficient gate teleportation protocols?

We completely solve both questions in the practically-relevant case of the Clifford hierarchy for gates of one qubit or one qudit of prime dimension. We express every such hierarchy gate uniquely as a product of three simple gates, yielding also a formula for the size of every level. These results are a consequence of our finding that all such hierarchy gates can be expressed in a certain form that guarantees efficient gate teleportation. Our decomposition of Clifford gates as a unique product of three elementary Clifford gates is of broad applicability.

# Day 1: September 15, 2025, Monday

## Session 1

Time: 14:30

### Rise of conditionally clean ancillae for efficient quantum circuit constructions

*Tanuj Khattar*[1], *Craig Gidney*[1]

[1] Google Quantum AI

We introduce *conditionally clean ancilla qubits*, a new quantum resource recently explored by [NZS24], that bridges the gap between traditional clean and dirty ancillae. Like dirty ancillae, they begin and end in an unknown state and can be borrowed from existing system qubits, thereby avoiding the space overhead of explicit qubit allocation. Like clean ancillae, they can be treated as initialized in a known state within specific computations, thus eliminating the overhead of toggle detection required for dirty ancillae.

We present new circuit constructions leveraging conditionally clean ancillae to achieve lower gate counts and depths, particularly in regimes with limited ancilla availability. Specifically, we provide constructions for:

1. an $n$-controlled NOT using $2n$ Toffolis and $\mathcal{O}(\log n)$ depth given 2 clean ancillae,
2. an $n$-qubit incrementer using $3n$ Toffolis given $\log^*(n)$ clean ancillae,
3. an $n$-qubit quantum–classical comparator using $3n$ Toffolis given $\log^*(n)$ clean ancillae,
4. unary iteration over $[0, N)$ using $2.5N$ Toffolis given $\log^*(n)$ clean ancillae,
5. unary iteration via a skew tree over $[0, N)$ using $1.25N$ Toffolis given $n$ dirty ancillae.

We also introduce *laddered toggle detection*, a technique to replace clean ancillae with dirty ancillae in all our constructions, incurring only a $2\times$ Toffoli gate overhead. Our results demonstrate that conditionally clean ancillae are a valuable tool for quantum circuit design, particularly in the resource-constrained early fault-tolerant era.

# Day 1: September 15, 2025, Monday

## Session 1

Time: 15:00

### Locality and Parameter Tradeoffs for Subsystem Codes

***Samuel Dai***[1], ***Ray Li***[2], ***Eugene Tang***[1]

[1] Northeastern University
[2] Santa Clara University

We study the tradeoffs between the locality and parameters of subsystem codes. We prove lower bounds on both the number and lengths of interactions in any $D$-dimensional embedding of a subsystem code. Specifically, we show that any embedding of a subsystem code with parameters $[[n, k, d]]$ into $\mathbb{R}^D$ must have at least $M^*$ interactions of length at least $\ell^*$, where

$$M^* = \Omega(\max(k, d)), \quad \text{and} \quad \ell^* = \Omega\left( \max\left( \frac{d}{n^{\frac{D-1}{D}}}, \left( \frac{kd^{\frac{1}{D-1}}}{n} \right)^{\frac{D-1}{D}} \right) \right).$$

We also give tradeoffs between the locality and parameters of commuting projector codes in $D$-dimensions, generalizing a result of Dai and Li (2024). We provide code constructions that show our bounds are optimal in both the interaction count and interaction length.

Time: 16:00

### Testing classical properties from quantum data

*Matthias C. Caro*[1], *Preksha Naik*[2], *Joseph Slote*[2]

[1] University of Warwick
[2] California Institute of Technology

Testing properties of Boolean functions is often dramatically faster than learning. However, this advantage usually disappears when testers are limited to random samples of the function—a natural setting for data science—rather than adaptive queries. In this work we investigate the *quantum* version of this "data science scenario": quantum algorithms that test properties of a function $f$ solely from quantum data in the form of copies of the function state $|f\rangle \propto \sum_x |x, f(x)\rangle$.

**New tests.** For three well-established properties—monotonicity, symmetry, and triangle-freeness—we show that the speedup lost when restricting classical testers to sampled data can be recovered by considering quantum data.

**Inadequacy of Fourier sampling.** Our new testers use techniques beyond quantum Fourier sampling, and we show that this necessary. In particular, there is no constant-complexity tester for symmetry relying solely on Fourier sampling and random classical samples.

**Classical queries vs. quantum data.** We exhibit a testing problem that can be solved from $\mathcal{O}(1)$ classical queries but that requires $\Omega(2^{n/2})$ function state copies. The Forrelation problem provides a separation of the same magnitude in the opposite direction, so we conclude that quantum data and classical queries are "maximally incomparable" resources for testing.

**Towards lower bounds.** We also begin the study of *lower bounds* for testing from quantum data. For quantum monotonicity testing, we prove that the ensembles used to prove exponential lower bounds for classical sample-based testing, do not yield any nontrivial lower bounds for testing from quantum data. New insights specific to quantum data will be required for proving copy complexity lower bounds for testing in this model.

Time: 16:30

## Chasing shadows with Gottesman-Kitaev-Preskill codes

*Jonathan Conrad*[1], *Jens Eisert*[2], *Steven T. Flammia*[3]

[1] Ecole Polytechnique Federale de Lausanne
[2] Freie Universität Berlin
[3] Virginia Tech

In this work, we consider the task of performing shadow tomography of a logical subsystem defined via the Gottesman-Kitaev-Preskill (GKP) error correcting code. We construct a logical shadow tomography protocol via twirling of Continuous Variable POVMs by displacement operators and Gaussian unitaries. In the special case of heterodyne measurement, the shadow tomography protocol yields a probabilistic decomposition of any input state into Gaussian states that simulate the encoded logical information of the input relative to a fixed GKP code and we prove bounds on the Gaussian compressibility of states in this setting. For photon-parity measurements, logical GKP shadow tomography is equivalent to a Wigner sampling protocol for which we develop the appropriate sampling schemes and finally we derive a Wigner sampling scheme via random GKP codes. This protocol establishes how Wigner samples of any input state relative to a random GKP codes can be used to estimate any sufficiently bounded observable on CV space. This construction shows how a description of the physical state of the system can be reconstructed from encoded logical information relative to a random code and further highlights the power of performing idealized GKP error correction as a tomographic resource.

# Day 1: September 15, 2025, Monday

## Session 1

Time: 17:00

### Unitary Designs from Random Symmetric Quantum Circuits

*Hanqing Liu*[1], *Austin Hulse*[2], *Iman Marvian*[2]

[1] TBD
[2] Duke University

In this work, we study distributions of unitaries generated by random quantum circuits containing only symmetry-respecting gates. We develop a unified approach applicable to all symmetry groups and obtain an operator satisfying a set of conditions that determines the exact design properties of such distributions. It has been recently shown that the locality of gates imposes various constraints on realizable unitaries, which in general, significantly depend on the symmetry under consideration. These constraints typically include restrictions on the relative phases between sectors with inequivalent irreducible representations of the symmetry. We call a set of symmetric gates semi-universal if they realize all unitaries that respect the symmetry, up to such restrictions. For instance, while 2-qubit gates are semi-universal for $\mathbb{Z}_2$, U(1), and SU(2) symmetries in qubit systems, SU($d$) symmetry with $d \geq 3$ requires 3-qudit gates for semi-universality. Failure of semi-universality precludes the distribution generated by the random circuits from being even a 2-design for the Haar distribution over symmetry-respecting unitaries. On the other hand, when semi-universality holds, under mild conditions, satisfied by U(1) and SU(2) for example, the distribution becomes a $t$-design for $t$ growing polynomially with the number of qudits, where the degree is determined by the locality of gates. More generally, we present a simple linear equation that determines the maximum integer $t_{\max}$ for which the uniform distribution of unitaries generated by the circuits is a $t$-design for all $t \leq t_{\max}$. Notably, for U(1), SU(2) and cyclic groups, we determine the exact value of $t_{\max}$ as a function of the number of qubits and locality of the gates, and for $(d)$, we determine the exact value of $t_{\max}$ for up to $4$-qudit gates.

Time: 14:00

## Maximal device-independent randomness in every dimension

*Máté Farkas*[1], *Jurij Volčič*[2], *Sigurd A. L. Storgaard*[3], *Ranyiliu Chen*[3], *Laura Mančinska*[3]

[1] University of York
[2] University of Auckland
[3] University of Copenhagen

Random numbers are used in a wide range of sciences. In many applications, generating unpredictable private random numbers is indispensable. Device-independent quantum random number generation is a framework that makes use of the intrinsic randomness of quantum processes to generate numbers that are fundamentally unpredictable according to our current understanding of physics. While device-independent quantum random number generation is an exceptional theoretical feat, the difficulty of controlling quantum systems makes it challenging to carry out in practice. It is therefore desirable to harness the full power of the quantum degrees of freedom (the dimension) that one can control. It is known that no more than 2log(d) bits of private device-independent randomness can be extracted from a quantum system of local dimension d. In this paper we demonstrate that this bound can be achieved for all dimensions d by providing a family of explicit protocols. In order to obtain our result, we develop new certification techniques that can be of wider interest in device-independent applications for scenarios in which complete certification ('self-testing') is impossible or impractical.

Time: 14:30

## A quantum cloning game with applications to quantum position verification

*Llorenc Escola Farras*[1,2], *Leo Colisson Palais, University Grenoble Alpes,), Florian Speelman*[1,2]

[1] QuSoft
[2] University of Amsterdam

We introduce a quantum cloning game in which k separate collaborative parties receive a classical input, determining which of them has to share a maximally entangled state with an additional party (referee). We provide the optimal winning probability of such a game for every number of parties k, and show that it decays exponentially when the game is played n times in parallel. These results have applications to quantum cryptography, in particular in the topic of quantum position verification, where we show security of the routing protocol (played in parallel), and a variant of it, in the random oracle model.

Day 1: September 15, 2025, Monday

Session 2

Time: 15:00

## PKE and ABE with Collusion-Resistant Secure Key Leasing

*Fuyuki Kitagawa*[1], *Ryo Nishimaki*[1], *Nikhil Pappu*[2]

[1] NTT Social Informatics Laboratories
[2] Portland State University

Secure key leasing (SKL) is an advanced encryption functionality that allows a secret key holder to generate a quantum decryption key and securely lease it to a user. Once the user returns the quantum decryption key (or provides a classical certificate confirming its deletion), they lose their decryption capability. Previous works on public key encryption with SKL (PKE-SKL) have only considered the single-key security model, where the adversary receives at most one quantum decryption key. However, this model does not accurately reflect real-world applications of PKE-SKL. To address this limitation, we introduce collusion-resistant security for PKE-SKL (denoted as PKE-CR-SKL). In this model, the adversary can adaptively obtain multiple quantum decryption keys and access a verification oracle which validates the correctness of queried quantum decryption keys. Importantly, the size of the public key and ciphertexts must remain independent of the total number of generated quantum decryption keys. We present the following constructions:

- A PKE-CR-SKL scheme based on the learning with errors (LWE) assumption.

- An attribute-based encryption scheme with collusion-resistant SKL (ABE-CR-SKL), also based on the LWE assumption.

- An ABE-CR-SKL scheme with classical certificates, relying on multi-input ABE with polynomial arity.

Time: 16:00

## Self-testing in the compiled setting via tilted-CHSH inequalities

*Connor Paddock*[1], *Arthur Mehta*[1], *Lewis Wooltorton*[2]

[1] University of Ottawa
[2] University of York

In a Bell scenario, a classical verifier interacts with two non-communicating (quantum) provers. To an observer the behaviour of the provers in this interaction is modelled by correlations. Certain correlations allow the verifier to certify, or self-test, the underlying quantum state and measurements. Self-testing underpins numerous device-independent quantum protocols with a classical verifier. A significant drawback of using self-tests in applications is the required no-communicating assumption between the provers. To address this issue Kalai et al. (STOC '23) introduce a cryptographic procedure which "compiles" these scenarios into a multi-round interaction between a verifier and a single computationally bounded prover. In this work, we formalize a notion of self-testing for compiled two-prover Bell scenarios. In addition, we prove that the quantum value is preserved under compilation for the family of tilted-CHSH inequalities (up to negligible factors). We also show that any maximal violation in the compiled setting of inequalities from this family satisfies a notion of self-testing in the compiled setting. More specifically, we show that maximal violations of these inequalities imply the existence of an efficient isometry that recovers the measurement action on the state after the first round.

Time: 16:30

## Commitments are equivalent to statistically-verifiable one-way state generators

*Rishabh Batra*[1], *Rahul Jain*[1]

[1] CQT, NUS

One-way state generators (OWSG) are natural quantum analogs to classical one-way functions. We consider statistically-verifiable OWSGs (sv-OWSG), which are potentially weaker objects than OWSGs. We show that O(n/log(n))-copy sv-OWSGs (n represents the input length) are equivalent to poly(n)-copy sv-OWSGs and to quantum commitments. Since known results show that o(n/log(n))-copy OWSGs cannot imply commitments, this shows that O(n/log(n))-copy sv-OWSGs are the weakest OWSGs from which we can get commitments (and hence much of quantum cryptography). Our construction follows along the lines of Hastad, Impagliazzo, Levin and Luby, who obtained classical pseudorandom generators (PRG) from classical one-way functions (OWF), however with crucial modifications. Our construction, when applied to the classical case, provides an alternative to the classical construction to obtain a classical mildly non-uniform PRG from any classical OWF. Since we do not argue conditioned on the output f(x), our construction and analysis is arguably simpler and may be of independent interest. For converting a mildly non-uniform PRG to a uniform PRG, we can use the classical construction.

# Day 1: September 15, 2025, Monday

## Session 2

Time: 17:00

### Untelegraphable Encryption and its Applications

*Jeffrey Champion*[1], *Fuyuki Kitagawa*[2], *Ryo Nishimaki*[2], *Takashi Yamakawa*[2]

[1] UT Austin
[2] NTT Social Informatics Laboratories

We initiate the study of untelegraphable encryption (UTE), founded on the no-telegraphing principle, which allows an encryptor to encrypt a message such that a binary string representation of the ciphertext cannot be decrypted by a user with the secret key, a task that is classically impossible. This is a natural relaxation of unclonable encryption (UE), inspired by the recent work of Nehoran and Zhandry (ITCS 2024), who showed a computational separation between the no-cloning and no-telegraphing principles.

In this work, we define and construct UTE information-theoretically in the plain model. Building off this, we give several applications of UTE and study the interplay of UTE with UE and well-studied tasks in quantum state learning, yielding the following contributions:

- A construction of collusion-resistant UTE from standard secret-key encryption (SKE). We additionally show that hyper-efficient shadow tomography (HEST) is impossible assuming collusion-resistant UTE exists. By considering a relaxation of collusion-resistant UTE, we are able to show the impossibility of HEST assuming only pseudorandom state generators (which may not imply one-way functions). This almost unconditionally answers an open inquiry of Aaronson (STOC 2018).

- A construction of UTE from a quasi-polynomially secure one-shot message authentication code (OSMAC) in the classical oracle model, such that there is an explicit attack that breaks UE security for an unbounded polynomial number of decryptors.

- A construction of everlasting secure collusion-resistant UTE, where the decryptor adversary can run in unbounded time, in the quantum random oracle model (QROM), and formal evidence that a construction in the plain model is a challenging task. We additionally show that HEST with unbounded post-processing time (which we call weakly-efficient shadow tomography) is impossible assuming everlasting secure collusion-resistant UTE exists.

- A construction of secret sharing for all polynomial-size policies that is resilient to joint and unbounded classical leakage from collusion-resistant UTE and classical secret sharing for all policies.

- A construction (and definition) of collusion-resistant untelegraphable secret-key functional encryption (UTSKFE) from single-decryptor functional encryption and plain secret-key functional encryption, and a construction of collusion-resistant untelegraphable public-key functional encryption from UTSKFE, plain SKE, and plain public-key functional encryption.

# Day 1: September 15, 2025, Monday

## Session 3

Time: 14:00

### Commuting Local Hamiltonians Beyond 2D

*John Bostanci*[1], *Yeongwoo Hwang*[2]

[1] Columbia University
[2] Harvard University

Local Hamiltonians are a quantum analogue to SAT in classical complexity. As a model of “intermediate” complexity, commuting local Hamiltonians provide a testing ground for studying many of the most interesting open questions in quantum information theory, including the quantum PCP conjecture and the nature of entanglement, while possibly being more amenable to analysis. Despite its simpler nature, the exact complexity of the commuting local Hamiltonian problem (CLH) remains elusive. A number of works [BV04; Sch11; AE11; AE15; IJ23] have shown that increasingly expressive families of commuting local Hamiltonians admit completely classical verifiers. Despite intense work, proofs placing CLH in NP rely heavily on an underlying 2D lattice structure, or a very constrained local dimension and locality.

In this work, we present a new technique to analyze the complexity of various families of commuting local Hamiltonians: guided reductions. Intuitively, these are a generalization of typical reduction where the prover provides a guide so that the verifier can construct a simpler Hamiltonian. The core of our reduction is a new rounding technique based on a combination of Jordan’s Lemma and the Structure Lemma. Our rounding technique is much more flexible than previous work and allows us to remove constraints on local dimension in exchange for a rank-1 assumption. Specifically, we prove the following two results: 1. 2D-CLH for rank-1 instances are contained in NP, independent of the qudit dimension. It is notable that this family of commuting local Hamiltonians has no restriction on the local dimension or the locality of the Hamiltonian terms. 2. 3D-CLH for rank-1 instances are in NP. To our knowledge this is the first time a family of 3D commuting local Hamiltonians has been contained in NP.

Our results apply to Hamiltonians with large qudit degree and remain non-trivial despite the quantumLov ´asz Local Lemma [AKS12].

## Session 3

Time: 14:30

# Optimal Hamiltonian simulation for low-energy states

***Rolando Somma***[1], ***Alexander Zlokapa***[2]

[1] Google
[2] MIT

We consider the task of simulating time evolution under a Hamiltonian $H$ within its low-energy subspace. Assuming access to a block-encoding of

$$H' = \frac{H - E}{\lambda}$$

for some constants $E$ and $\lambda$, the goal is to implement an approximation to the evolution operator for time $t$ when the initial state is confined to the subspace corresponding to eigenvalues $\left[-1, -1+\frac{\Delta}{\lambda}\right]$ of $H'$, where $\Delta/\lambda$ is small.

We present an optimal quantum algorithm that asymptotically improves over generic methods. Our quantum algorithm leverages spectral gap amplification together with the quantum singular value transform. We also provide lower bounds for low-energy simulation and show that our algorithm is tight in the query model (and also in the gate model) with respect to all problem parameters and in all simulation regimes.

Finally, we discuss some applications and point out that the techniques developed here have been recently used to obtain the best-known simulation algorithms for quantum chemistry.

Time: 15:00

## Simulating chaos without chaos

*Andi Gu*[1], *Yihui Quek*[2], *Susanne Yelin*[1], *Jens Eisert*[3], *Lorenzo Leone*[3]

[1] Harvard University
[2] Massachusetts Institute of Technology
[3] Free University of Berlin

Quantum chaos is a quantum many-body phenomenon that is associated with a number of intricate properties, such as level repulsion in energy spectra or distinct scalings of out-of-time ordered correlation functions. In this work, we introduce a novel class of "pseudochaotic" quantum Hamiltonians that fundamentally challenges the conventional understanding of quantum chaos and its relationship to computational complexity. Our ensemble is computationally indistinguishable from the Gaussian unitary ensemble (GUE) of strongly-interacting Hamiltonians, widely considered to be a quintessential model for quantum chaos. Surprisingly, despite this effective indistinguishability, our Hamiltonians lack all conventional signatures of chaos: it exhibits Poissonian level statistics, low operator complexity, and weak scrambling properties. This stark contrast between efficient computational indistinguishability and traditional chaos indicators calls into question fundamental assumptions about the nature of quantum chaos. We, furthermore, give an efficient quantum algorithm to simulate Hamiltonians from our ensemble, even though simulating Hamiltonians from the true GUE is known to require exponential time. Our work establishes fundamental limitations on Hamiltonian learning and testing protocols and derives stronger bounds on entanglement and magic state distillation. These results reveal a surprising separation between computational and information-theoretic perspectives on quantum chaos, opening new avenues for research at the intersection of quantum chaos, computational complexity, and quantum information. Above all, it challenges conventional notions of what it fundamentally means to actually observe complex quantum systems.

Session 3

Time: 16:00

## Quantum Routing and Entanglement Dynamics Through Bottlenecks

*Dhruv Devulapalli*[1], *Chao Yin*[2], *Andrew Guo*[3], *Eddie Schoute*[4], *Andrew Childs*[5], *Alexey Gorshkov*[5,6], *Andrew Lucas*[2]

[1] QuICS, University of Maryland
[2] University of Colorado, Boulder
[3] Quantinuum
[4] IBM Research
[5] University of Maryland
[6] NIST

To implement arbitrary quantum circuits in architectures with restricted interactions, one may effectively simulate all-to-all connectivity by *routing* quantum information. In order to implement general quantum operations while constraining the cost of doing so, we seek optimal protocols and lower bounds for routing.

We consider the entanglement dynamics and routing between two regions connected only through an intermediate *bottleneck* region with few qubits. In such systems, where the entanglement rate is restricted by a *vertex boundary* rather than an edge boundary of the underlying interaction graph $G$, existing results such as the small incremental entangling theorem give only a trivial constant lower bound on the routing time (the minimum time to perform an arbitrary permutation). We significantly improve the lower bound on the routing time in systems with a vertex bottleneck.

Specifically, for any system with two regions containing $N_L$ and $N_R$ qubits respectively, coupled only through an intermediate region of $N_C$ qubits, for any $\delta > 0$ we show a lower bound of

$$\Omega\left(\frac{N_R^{1-\delta}}{\sqrt{N_L}\,N_C}\right)$$

on the routing time. We also prove an upper bound on the average amount of bipartite entanglement that can be generated in time $t$ by an architecture-respecting Hamiltonian in systems constrained by vertex bottlenecks, improving the scaling in system size from $\mathcal{O}(N_L t)$ to $\mathcal{O}(\sqrt{N_L}\,t)$.

As a special case, when applied to the star graph (one central vertex connected to $N$ leaves), we obtain an

$$\Omega\left(\sqrt{N^{1-\delta}}\right)$$

lower bound on the routing time and on the time to prepare $N/2$ Bell pairs between the vertices. We also show that, in systems of free fermions, one can route optimally on the star graph in time $\Theta(\sqrt{N})$, illustrating a separation between gate-based and Hamiltonian quantum routing.

Session 3

Time: 16:30

## Mixing time of quantum Gibbs sampling for random sparse Hamiltonians

*Akshar Ramkumar*[1], *Mehdi Soleimanifar*[1]

[1] California Institute of Technology

Providing evidence that quantum computers can efficiently prepare low-energy or thermal states of physically relevant interacting quantum systems is a major challenge in quantum information science. A newly developed quantum Gibbs sampling algorithm [CKG23] provides an efficient simulation of the detailed-balanced dissipative dynamics of non-commutative quantum systems. The running time of this algorithm depends on the mixing time of the corresponding quantum Markov chain, which has not been rigorously bounded except in the high-temperature regime. In this work, we establish a polylog(n) upper bound on the mixing time of this algorithm for various families of random n×n sparse Hamiltonians at any constant temperature. We further analyze how the structure of the jump operators and the spectral properties of these sparse Hamiltonians influence the mixing time. Our results demonstrate that the quantum Gibbs sampler is a flexible approach capable of preparing the Gibbs state of a large family of Hamiltonians that are known to be quantumly easy.

Time: 17:00

## A Hierarchy of Spectral Gap Certificates for Frustration-Free Spin Systems

*Kshiti Sneh Rai*[1], *Ilya Kull*[2], *Patrick Emonts*[1], *Jordi Tura*[1], *Norbert Schuch*[2], *Flavio Baccari*[3]

[1] Leiden University
[2] University of Vienna
[3] University of Padova

Estimating spectral gaps of quantum many-body Hamiltonians is a highly challenging computational task, even under assumptions of locality and translation-invariance. Yet, the quest for rigorous gap certificates is motivated by their broad applicability, ranging from many-body physics to quantum computing and classical sampling techniques. Here we present a general method for obtaining lower bounds on the spectral gap of frustration-free quantum Hamiltonians in the thermodynamic limit. We formulate the gap certification problem as a hierarchy of optimization problems (semidefinite programs) in which the certificate—a proof of a lower bound on the gap—is improved with increasing levels. Our approach encompasses existing finite-size methods, such as Knabe's bound and its subsequent improvements, as those appear as particular possible solutions in our optimization, which is thus guaranteed to either match or surpass them. We demonstrate the power of the method on one-dimensional spin-chain models where we observe an improvement by several orders of magnitude over existing finite size criteria in both the accuracy of the lower bound on the gap, as well as the range of parameters in which a gap is detected.

## Day 2: September 16, 2025, Tuesday

### Time: 9:30 (Invited talk)

# Composing Quantum Algorithms

*Stacey Jeffery*[1]

IS

[1] Centrum Wiskunde  Informatica , Amsterdam, Netherlands

Composition is something we take for granted in classical algorithms design, and in particular, we take it as a basic axiom that composing “efficient” algorithms should result in an “efficient” algorithm – even using this intuition to justify our definition of “efficient.” Composing quantum algorithms is a much more subtle affair than composing classical algorithms. It has long been known that zero-error quantum algorithms do not compose, but it turns out that, using the right algorithmic lens, bounded-error quantum algorithms do. In fact, in the bounded-error setting, quantum algorithms can even avoid the log factor needed in composing bounded-error randomized algorithms that comes from amplifying the success probability via majority voting. This latter point hints at a fundamental difference between quantum and classical computing, and has recently been used to make progress on the complexity theoretic question of QMA vs. QMA1. In this talk, I will try to give some intuition for how composing quantum algorithms is different from the classical case, and what we might learn from this difference about the power of quantum computing in general.

## Day 2: September 16, 2025, Tuesday

## Session 1

Time: 11:00

# Towards Non-Abelian Quantum Signal Processing: Efficient Control of Hybrid Continuous- and Discrete-Variable Architectures

*Shraddha Singh*[1], *Baptiste Royer*[2], *Steven M. Girvin*[1]

[1] Yale University
[2] Université de Sherbrooke

Robust quantum control is crucial for operations below the quantum error correction threshold. Quantum Signal Processing (QSP) transforms a unitary parameterized by $\theta$ into one governed by a polynomial function $f(\theta)$, underpinning key quantum algorithms. Originating from composite pulse techniques in NMR, QSP enhances robustness against systematic control errors.

We extend QSP to multiple non-commuting control parameters, $\hat{\theta}_1, \hat{\theta}_2, \ldots$, representing quantum harmonic oscillator positions and momenta. We introduce a composite pulse sequence utilizing non-commuting controls, Gaussian-Controlled-Rotation ($\mathrm{GCR}$), which belongs to this new class of QSP, *non-abelian quantum signal processing*. This sequence achieves at least a $4.5\times$ reduction in circuit depth compared to the state-of-the-art abelian QSP pulse $\mathrm{BB1}$, while maintaining performance. Though quantum fluctuations in the control parameters are unavoidable, the richer commutator algebra enhances QSP's power and efficiency.

Non-Abelian QSP represents the highest tier of QSP variants tailored for CV-DV architectures, unlocking new possibilities for hybrid quantum systems. We demonstrate utility of $\mathrm{GCR}$ in high-fidelity preparation of CV states—including squeezed vacuum, cat states, Fock state $|1\rangle$, and GKP states—using analytical schemes that match numerically optimized methods in fidelity and depth while enabling error tracking. Furthermore, we propose a high-fidelity QSP-based end-of-the-line GKP readout and a measurement-free gate teleportation protocol for logical operations on GKP bosonic qudits, bridging the gap between theoretical and experimental GKP codespaces.

Finally, we showcase a $\mathrm{GCR}$-based phase estimation algorithm for oscillator-based quantum computing.

Time: 11:30

## Polylog-Time- and Constant-Space-Overhead Fault-Tolerant Quantum Computation with Quantum Low-Density Parity-Check Codes

*Shiro Tamiya*[1], *Masato Koashi*[2], *Hayata Yamasaki*[3]

[1] Nanofiber Quantum Technologies
[2] Department of Applied Physics, Graduate School of Engineering, The University of Tokyo
[3] Department of Physics, Graduate School of Science, The University of Tokyo

A major challenge in fault-tolerant quantum computation (FTQC) is to reduce both space overhead—the large number of physical qubits per logical qubit—and time overhead—the long physical gate sequences per logical gate. We prove that a protocol using non-vanishing-rate quantum low-density parity-check (QLDPC) codes, combined with concatenated Steane codes, achieves constant space overhead and polylogarithmic time overhead, even when accounting for non-zero classical computation time.

This protocol offers an improvement over existing constant-space-overhead protocols, which have polynomial time overhead using QLDPC codes and quasi-polylogarithmic time overhead using concatenated quantum Hamming codes. To ensure the completeness of this proof, we develop a technique called *partial circuit reduction*, which enables error analysis for the entire fault-tolerant circuit by examining smaller parts composed of a few gadgets. With this technique, we resolve a previously unaddressed logical gap in the existing arguments and complete the proof of the threshold theorem for the constant-space-overhead protocol with QLDPC codes.

Our work highlights that the QLDPC approach can realize FTQC with a negligibly small slowdown and a bounded overhead of physical qubits, similar to the code-concatenation approach, underscoring the importance of a comprehensive comparison of the future realizability of these two approaches.

# Day 2: September 16, 2025, Tuesday

## Session 1

Time: 12:00

### Quantum Search with In-Place Queries

Blake Holman[1], Ronak Ramachandran[2], Justin Yirka[2]

[1] Purdue University
[2] The University of Texas at Austin

Quantum query complexity is typically characterized in terms of *xor queries*,

$$|x, y\rangle \;\mapsto\; |x,\, y \oplus f(x)\rangle \,,$$

or *phase queries*, which ensure that even queries to non-invertible functions are unitary. Another natural model arises when querying a permutation, leading to *in-place queries* of the form

$$|x\rangle \;\mapsto\; |f(x)\rangle \,.$$

. Some problems are known to require exponentially fewer in-place queries than xor queries, but no separation has been shown in the opposite direction. A candidate for such a separation was the problem of inverting a permutation over N elements. This task, equivalent to unstructured search in the context of permutations, is solvable with O(sqrt(N)) xor queries but was conjectured to require Omega(N) in-place queries. We refute this conjecture by designing a quantum algorithm for Permutation Inversion using O(sqrt(N)) in-place queries. Our algorithm achieves the same speedup as Grover's algorithm despite the inability to efficiently uncompute queries or perform straightforward oracle-controlled reflections. Nonetheless, we show that there are indeed problems which require fewer xor queries than in-place queries. We introduce a subspace-conversion problem called Function Erasure that requires 1 xor query and Theta(sqrt(N)) in-place queries. Then, we build on a recent extension of the quantum adversary method to characterize exact conditions for a decision problem to exhibit such a separation, and we propose a candidate problem.

# Day 2: September 16, 2025, Tuesday

## Session 1

Time: 12:30

### The complexity of Gottesman-Kitaev-Preskill states

*Lukas Brenner*[1], *Libor Caha*[1], *Xavier Coiteux-Roy*[2], *Robert Koenig*[1]

[1] Technical University of Munich
[2] University of Calgary

We initiate the study of state complexity for continuous-variable quantum systems. Concretely, we consider a setup with bosonic modes and auxiliary qubits, where available operations include Gaussian one- and two-mode operations, single- and two-qubit operations, as well as qubit-controlled phase-space displacements. We define the (approximate) complexity of a bosonic state by the minimum size of a circuit that prepares an approximation to the state in trace distance.

We propose a new circuit which prepares an approximate Gottesman-Kitaev-Preskill (GKP) state $|_{\kappa,\Delta}\rangle$. Here $\kappa^{-2}$ is the variance of the envelope and $\Delta^2$ is the variance of the individual peaks. We show that the circuit accepts with constant probability and — conditioned on acceptance — the output state is polynomially close in $(\kappa, \Delta)$ to the state $|_{\kappa,\Delta}\rangle$. The size of our circuit is linear in $(\log 1/\kappa, \log 1/\Delta)$. To our knowledge, this is the first protocol for GKP-state preparation with fidelity guarantees for the prepared state. We also show converse bounds, establishing that the linear circuit-size dependence of our construction is optimal. This fully characterizes the complexity of GKP states.

Time: 14:00

## Full classification of Pauli Lie algebras

*Gerard Aguilar Tapia*[1], *Simon Cichy*[1], *Jens Eisert*[1], *Lennart Bittel*[1]

[1] FU Berlin

Lie groups, and therefore Lie algebras, are fundamental structures in quantum physics that determine the space of possible trajectories of evolving systems. However, their classification and characterization often becomes impractical for large systems. This work provides a comprehensive classification of Lie algebras generated by an arbitrary set of Pauli operators, from which an efficient method to characterize them follows. Mapping the problem to a graph setting, we identify a reduced set of equivalence classes for connected graphs: the free-fermionic Lie algebra, the set of all anti-symmetric Paulis, the Lie algebra of symplectic Paulis, and the space of all Pauli operators on qubits, as well as controlled versions thereof. Out of these, we distinguish 6 Clifford inequivalent cases, for which we give a physical interpretation of their dynamics. We then extend this result to general graphs with arbitrarily many connected components. Our findings reveal a no-go result for the existence of small Lie algebras beyond the free-fermionic case in the Pauli setting and offer efficiently computable criteria for universality and extendibility of gate sets. These results bear significant impact in ideas in a number of fields like quantum control, quantum machine learning, or classical simulation of quantum circuits.

# Day 2: September 16, 2025, Tuesday

## Session 1

Time: 14:30

### Uniformity testing when you have the source code

***Clément Canonne***[1], ***Robin Kothari***[2], ***Ryan O'Donnell***[3]

[1] University of Sydney
[2] Google
[3] Carnegie Mellon University

We study quantum algorithms for verifying properties of the output probability distribution of a classical or quantum circuit, given access to the source code that generates the distribution. We consider the basic tasks of uniformity testing, which is to decide if the output distribution is uniform on $[d]$ or $\epsilon$-far from uniform in total variation distance, and identity testing, which is the task of deciding if the output distribution equals a known hypothesis distribution or is $\epsilon$-far from it. For both problems, the previous best known upper bound was $O(\min\{d^{1/3}/\epsilon^2, d^{1/2}/\epsilon\})$. Here we improve the upper bound to $O(\min\{d^{1/3}/\epsilon^{4/3}, d^{1/2}/\epsilon\})$, which we conjecture is optimal.

Time: 15:00

## A full practical theory of the Clifford group commutant

*Lennart Bittel*[1], *Jens Eisert*[1], *Lorenzo Leone*[1], *Antonio Anna Mele*[1], *Salvatore Francesco Emanuele Oliviero*[2]

[1] Freie Universität Berlin
[2] Scuola Normale Superiore

Random Clifford unitaries play a crucial role in various areas of quantum information. However, a complete characterization of the Clifford group commutant — the key object for understanding its randomness properties — remains an open problem. The seminal work of Gross, Nezami, and Walter[ Commun. Math. Phys. 385, 1325–1393 (2021)] provides only a partial characterization (specifically, for tensor powers up to $k \leq n+1$, where $n$ is the number of qubits), which additionally might seem arguably not straightforward to use. In this work we present a complete and arguably simple characterization of the Clifford group commutant. We first show that the Clifford commutant is generated by the same generators of the unitary group commutant – permutations – plus at most crucially only three specific operators. We then construct an orthogonal basis for the Clifford commutant in all regimes (also $k > n+1$). We also develop a powerful graphical calculus tool to efficiently manipulate operators within the commutant. Finally, we discuss the implications of our results in the contexts of unitary $k$-designs and magic-state resource theory.

# Day 2: September 16, 2025, Tuesday

## Session 1

Time: 15:30

### Factoring an integer with three oscillators and a qubit

***Lukas Brenner***[1], ***Libor Caha***[1], ***Xavier Coiteux-Roy***[2], ***Robert Koenig***[1]

[1] Technical University of Munich
[2] University of Calgary

A common starting point of traditional quantum algorithm design is the notion of a universal quantum computer with a scalable number of qubits. This convenient abstraction mirrors classical computations manipulating finite sets of symbols, and allows for a device-independent development of algorithmic primitives. Here we advocate an alternative approach centered on the physical setup and the associated set of natively available operations. We show that these can be leveraged to great benefit by sidestepping the standard approach of reasoning about computation in terms of individual qubits.

As an example, we consider hybrid qubit–oscillator systems with linear optics operations augmented by certain qubit-controlled Gaussian unitaries. The continuous-variable (CV) Fourier transform has a native realization in such systems in the form of homodyne momentum measurements. We show that this fact can be put to algorithmic use. Specifically, we give a polynomial-time quantum algorithm in this setup which finds a factor of an $n$-bit integer $N$. Unlike Shor's algorithm, or CV implementations thereof based on qubit-to-oscillator encodings, our algorithm relies on the CV (rather than discrete) Fourier transform. The physical system used is independent of the number $N$ to be factored: It consists of a single qubit and three oscillators only.

Session 2

Time: 11:00

## Phase error rate estimation in QKD with imperfect detectors

***Devashish Tupkary**, Waterloo), Shlok nahar*[1]***, Pulkit Sinha***[1]***, Norbert Lutkenhaus, University of Waterloo)***

[1] Institute for Quantum Computing, University of Waterloo

We present a finite-size security proof of the decoy-state BB84 QKD protocol against coherent attacks, using entropic uncertainty relations, for imperfect detectors. We apply this result to the case of detectors with imperfectly characterized basis-efficiency mismatch. Our proof works by obtaining a suitable bound on the phase error rate, without requiring any new modifications to the protocol steps or hardware. It is applicable to imperfectly characterized detectors, and only requires the maximum relative difference in detection efficiencies and dark count rates of the detectors to be characterized. Moreover, our proof allows Eve to choose detector efficiencies and dark count rates in their allowed ranges in each round, thereby addressing an important problem of detector side channels. We quantitatively demonstrate the effect of basis-efficiency mismatch by applying our results to the decoy-state BB84 protocol. Our framework is general, and can be extended to include source imperfections, and passive detection setups as well.

# Day 2: September 16, 2025, Tuesday

## Session 2

Time: 11:30

### Asymptotic Robustness of Entanglement in Noisy Quantum Networks and Graph Connectivity

*Fernando Lledó*[1], *Carlos Palazuelos*[2], *Julio de Vicente*[1]

[1] Universidad Carlos III de Madrid & ICMAT
[2] Universidad Complutense de Madrid & ICMAT

Quantum networks are promising venues for quantum information processing. This motivates the study of the entanglement properties of the particular multipartite quantum states that underpin these structures. In particular, it has been recently shown that when the links are noisy two drastically different behaviors can occur regarding the global entanglement properties of the network. While in certain configurations the network displays genuine multipartite entanglement (GME) for any system size provided the noise level is below a certain threshold, in others GME is washed out if the system size is big enough for any fixed non-zero level of noise.

However, this difference has only been established considering the two extreme cases of maximally and minimally connected networks (i.e., complete graphs versus trees, respectively). In this contribution we investigate this question in much more depth and relate this behavior to the growth of several graph-theoretic parameters that measure the connectivity of the graph sequence that codifies the structure of the network as the number of parties increases. The strongest conditions are obtained when considering the degree growth.

Our main results are that a sufficiently fast degree growth (i.e., $\Omega(N)$, where $N$ is the size of the network) is sufficient for asymptotic robustness of GME, while if it is sufficiently slow (i.e., $o(\log N)$) then the network becomes asymptotically biseparable. We also present several explicit constructions related to the optimality of these results.

Session 2

Time: 12:00

## Adaptive Channel Reshaping for Improved Entanglement Distillation

***Dina Abdelhadi***[1]***, Tomas Jochym-O'Connor, Heights, NY, USA, & IBM Quantum, Almaden Research Center, San Jose, CA, USA), Vikesh Siddhu, Yorktown Heights, NY, USA, & IBM Research, IBM Research India, India), John Smolin, Heights, NY, USA)***

[1] EPFL

Quantum communication and computation heavily rely on entanglement distillation protocols. There is a plethora of distillation protocols for Pauli channels and also for some non-Pauli channels. However, an effort to relate the effectiveness of these protocols has been missing. For most quantum channels, the gap between the existing lower and upper bounds on distillation rates is substantial, and improvements of achievable rates have been stagnant for decades. In this work, we improve the best known distillation lower bounds, for both the amplitude damping and depolarizing channels. We build on a key observation that distillation protocols reshape several uses of a very noisy channel into a better effective channel. We apply this channel processing in an adaptive and recurrent manner. For the amplitude damping channel, our suggested protocol reshapes the channel into an erasure channel, achieving rates exceeding the best known lower bound given by the channel's reverse coherent information. For the depolarizing channel, we introduce the Greedy recurrence protocol with proven performance guarantees and construct a combined protocol improving upon previously known distillation rates. Improved bounds on attainable distillation rates give insights for both practical implementations and theoretical understanding of quantum information processing.

Session 2

Time: 12:30

## Quantum Position Verification in One Shot: Parallel Repetition of the f-BB84 and f-Routing Protocols

*Llorenç Escola Farràs*[1], *Florian Speelman*[1]

[1] QuSoft / University of Amsterdam

Quantum position verification (QPV) aims to verify an untrusted prover's location by timing communication with them. To reduce uncertainty, it is desirable for this verification to occur in a single round. However, previous protocols achieving one-round secure QPV had critical drawbacks: attackers pre-sharing an EPR pair per qubit could perfectly break them, and their security depended on quantum information traveling at the speed of light in vacuum, a major experimental challenge in quantum networks.

In this work, we prove that a single round of interaction suffices for secure position verification while overcoming these limitations. We show that security for a one-round protocol can rely only on the size of the classical information rather than quantum resources, making implementation more feasible, even with a qubit error tolerance of up to $3.6\%$, which is experimentally achievable with current technology — and showing that the timing constraints have to apply only to classical communication. In short, we establish parallel repetition of the f-BB84 and f-routing QPV protocols.

As a consequence of our techniques, we also demonstrate an order-of-magnitude improvement in the error tolerance for the sequential repetition version of these protocols, compared to the previous bounds of *Nature Physics* **18**, 623–626 (2022).

## Session 2

Time: 14:00

### No quantum advantage without classical communication: fundamental limitations of quantum networks

*Justus Neumann*[1], *Nikolai Wyderka*[1], *Tulja Varun Kondra*[1], *Kiara Hansenne*[2], *Lisa T. Weinbrenner*[3], *Hermann Kampermann*[1], *Otfried Gühne*[3], *Dagmar Bruß*[1]

[1] Heinrich Heine University
[2] Institut de Physique Théorique, Université Paris-Saclay
[3] Universität Siegen

Quantum networks connect systems at separate locations via quantum links, enabling a wide range of quantum information tasks between distant parties. Large-scale networks have the potential to enable global secure communication, distributed quantum computation, enhanced clock synchronization, and high-precision multiparameter metrology. For the optimal development of these technologies, however, it is essential to identify the necessary resources and sub-routines that will lead to the quantum advantage, but this is demanding even for the simplest protocols in quantum information processing. Here we show that quantum networks relying on the long-distance distribution of two-particle entanglement, combined with local operations and shared randomness, cannot achieve a relevant quantum advantage. Specifically, we prove that these networks do not help in preparing resourceful quantum states such as Greenberger-Horne-Zeilinger states or cluster states, despite the free availability of long-distance entanglement. At an abstract level, our work points towards a fundamental difference between two-particle and multiparticle entanglement. From a practical perspective, our results highlight the need for classical communication combined with quantum memories to fully harness the power of quantum networks.

# Day 2: September 16, 2025, Tuesday

## Session 2

Time: 14:30

### Generalized Inner Product Estimation with Limited Quantum Communication

*Srinivasan Arunachalam*[1], *Louis Schatzki*[2]

[1] IBM
[2] University of Illinois Urbana Champaign

We consider the task of distributed inner product estimation when allowed limited quantum communication. Here, Alice and Bob are given k copies of an unknown n-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$ respectively. They are allowed to communicate q qubits and unlimited classical communication, and their goal is to estimate $| \langle\psi|\phi\rangle |^2|$ up to constant accuracy. We show that $k = \Theta((nq)^{1/2})$ copies are essentially necessary and sufficient for this task (extending the work of Anshu, Landau and Liu (STOC'22) who considered the case when $q = 0$). Additionally, we consider estimating $| \langle\psi| M |\phi\rangle |^2$, for arbitrary Hermitian M. For this task we show that certain norms on M characterize the sample complexity of estimating $| \langle\psi| M |\phi\rangle |^2$ when using only classical communication.

## Day 2: September 16, 2025, Tuesday

## Session 2

Time: 15:00

# Composably Secure Delegated Quantum Computation with Weak Coherent Pulses

*Maxime Garnier*[1], *Dominik Leichtle*[2], *Luka Music*[3], *Harold Ollivier*[1]

[1] INRIA Paris
[2] University of Edinburgh
[3] Quandela

Secure Delegated Quantum Computation (SDQC) protocols allow a client to delegate a quantum computation to a powerful remote server while ensuring the privacy and the integrity of its computation. Recent resource-efficient and noise-robust protocols led to experimental proofs of concept. Yet, their physical requirements are still too stringent to be added directly to the roadmap of quantum hardware vendors.

To address part of this issue, this paper shows how to alleviate the necessity for the client to have a single-photon source. It proposes a protocol that ensures that, among a sufficiently large block of transmitted weak coherent pulses, at least one of them was emitted as a single photon. This can then be used through quantum privacy amplification techniques to prepare a single secure qubit to be used in an SDQC protocol. As such, the obtained guarantee can also be used for Quantum Key Distribution (QKD) where the privacy amplification step is classical. In doing so, it proposes a workaround for a weakness in the security proof of the decoy state method.

The simplest instantiation of the protocol with only 2 intensities already shows improved scaling at low transmittance and adds verifiability to previous SDQC proposals.

Time: 15:30

## Polynomial Time Quantum and Classical Algorithms for Representation Theoretic Multiplicities

Vojtech Havlicek[1], Martin Larocca[2], Greta Panova[3]

[1] IBM Research
[2] Los Alamos National Laboratory
[3] University of Southern California

We analyze computational problems that appear in the representation theory of the symmetric group and seem to be a natural target for attack with quantum algorithms: the computation of Kronecker, Littlewood–Richardson, Kostka, and Plethysm coefficients. The coefficients play an important role in the representation theory of the symmetric group $S_n$ and we give quantum algorithms for computing them that are enabled by the efficient implementation of the $S_n$ quantum Fourier transform. This, together with previously known results about hardness of their computation, led two of us to pose conjectures about super-polynomial quantum speedups achieved by these algorithms on a subset of inputs on which they remain efficient. Subsequent analysis by the third author showed that the conditions under which the desired super-polynomial quantum speedup can be achieved are somewhat limited. Our results isolate the narrow regime under which the problems may provide super-polynomial quantum speedups and lay ground for future work on polynomial or super-polynomial quantum speedups that may (or may not) be offered by this class of computational problems.

# Day 2: September 16, 2025, Tuesday

## Session 3

Time: 11:00

### Quantum Purity Amplification: Optimality and Efficient Algorithm

*Zhaoyi Li*[1], *Honghao Fu*[2], *Takuya Isogawa*[1], *Isaac Chuang*[1]

[1] Massachusetts Institute of Technology
[2] Concordia University

Quantum purity amplification (QPA) offers a novel approach to counteracting the pervasive noise that degrades quantum states. We present the optimal QPA protocol for general quantum systems against global depolarizing noise, which has remained unknown for two decades. We construct and prove the optimality of our protocol, achieving an exponential reduction in sample complexity compared to the best-known methods for strong depolarization. We examine the operational interpretation of the protocol and present an efficient algorithm for its implementation based on generalized quantum phase estimation (GQPE). Additionally, we introduce SWAPNET, a sparse and shallow circuit that makes QPA feasible for near-term experiments. We conduct numerical simulations to investigate the effectiveness of our protocol applied to quantum simulation of Hamiltonian evolution, demonstrating its ability to enhance fidelity even under gate-level noise. Our findings suggest that QPA could improve the performance of quantum information processing tasks, particularly in the context of Noisy Intermediate-Scale Quantum (NISQ) devices, where reducing the effect of noise with limited resources is critical.

## Day 2: September 16, 2025, Tuesday

### Session 3

Time: 11:30

### A quantum algorithm for Khovanov homology

*Alexander Schmidhuber*[1], ***Michele Reilly***[1], ***Paolo Zanardi***[2], ***Seth Lloyd***[1], ***Aaron Lauda***[2]

[1] MIT
[2] USC

Khovanov homology is a topological knot invariant that categorifies the Jones polynomial, recognizes the unknot, and is conjectured to appear as an observable in 4 supersymmetric Yang–Mills theory. Despite its rich mathematical and physical significance, the computational complexity of Khovanov homology remains largely unknown. To address this challenge, our work initiates the study of efficient quantum algorithms for Khovanov homology.

We provide simple proofs that increasingly accurate additive approximations to the ranks of Khovanov homology are DQC1-hard, BQP-hard, and P-hard, respectively. For the first two approximation regimes, we propose a novel quantum algorithm. Our algorithm is efficient provided the corresponding Hodge Laplacian thermalizes in polynomial time and has a sufficiently large spectral gap, for which we give numerical and analytical evidence.

Our approach introduces a pre-thermalization procedure that allows our quantum algorithm to succeed even if the Betti numbers of Khovanov homology are much smaller than the dimensions of the corresponding chain spaces, overcoming a limitation of prior quantum homology algorithms. We introduce novel connections between Khovanov homology and graph theory to derive analytic lower bounds on the spectral gap.

## Day 2: September 16, 2025, Tuesday

### Session 3

Time: 12:00

### Quantum Algorithm for Reversing Unknown Unitary Evolutions

***Yu-Ao Chen***[1]***, Yin Mo, (Guangzhou))***[2]***, Yingjian Liu, Technology***[2]***, Lei Zhang, (Guangzhou))***[2]***, Xin Wang, (Guangzhou))***[2]

[1] The Hong Kong University of Science and Technology (Guangzhou)
[2] Guangzhou)

Reversing an unknown quantum evolution is of central importance to quantum information processing and fundamental physics, yet it remains a formidable challenge as conventional methods necessitate an infinite number of queries to fully characterize the quantum process. Here we introduce the Quantum Unitary Reversal Algorithm (QURA), a deterministic and exact approach to universally reverse arbitrary unknown unitary transformations using $\mathcal{O}(d^2)$ calls of the unitary, where $d$ is the system dimension. Our quantum algorithm resolves a fundamental problem of time-reversal simulations for closed quantum systems by confirming the feasibility of reversing any unitary evolution without knowing the exact process. The algorithm also provides the construction of a key oracle for unitary inversion in many quantum algorithm frameworks, such as quantum singular value transformation. It notably reveals a sharp boundary between the quantum and classical computing realms and unveils a quadratic quantum advantage in computational complexity for this foundational task.

# Day 2: September 16, 2025, Tuesday

## Session 3

Time: 12:30

### Classical and Quantum Algorithms for Characters of the Symmetric Group

*Sergey Bravyi*[1], *David Gosset*[2], *Vojtech Havlicek*[1], *Louis Schatzki*[3]

[1] IBM
[2] University of Waterloo
[3] University of Illinois Urbana Champaign

Characters of irreducible representations are ubiquitous in group theory. However, computing characters of some groups such as the symmetric group Sn is a challenging problem known to be P-hard in the worst case. Here we describe a Matrix Product State (MPS) algorithm for characters of Sn. The algorithm computes an MPS encoding all irreducible characters of a given permutation. It relies on a mapping from characters of Sn to quantum spin chains proposed by Crichigno and Prakash. We also provide a simpler derivation of this mapping. We complement this result by presenting a poly(n) size quantum circuit that prepares the corresponding MPS obtaining an efficient quantum algorithm for certain sampling problems based on characters of Sn. To assess classical hardness of these problems we present a general reduction from strong simulation (computing a given probability) to weak simulation (sampling with a small error). This reduction applies to any sampling problem with a certain granularity structure and may be of independent interest.

## Day 2: September 16, 2025, Tuesday

### Session 3

Time: 14:00

### Directed st-connectivity with few paths is in quantum logspace

*Roman Edenhofer*[1], *Simon Apers*[2]

[1] Université Paris Cité, IRIF
[2] Université Paris Cité, CNRS, IRIF

We present a BQSPACE$(O(\log n))$-procedure to count $st$-paths on directed graphs for which we are promised that there are at most polynomially many paths starting in $s$ and polynomially many paths ending in $t$. For comparison, the best known classical upper bound in this case just to decide $st$-connectivity is DSPACE$(O(\log^2 n/\log\log n))$. The result establishes a new relationship between BQL and unambiguity and fewness subclasses of NL. Further, we also show how to *recognize* directed graphs with at most polynomially many paths between any two nodes in BQSPACE$(O(\log n))$. This yields the first natural candidate for a language separating BQL from L and BPL. Until now, all candidates potentially separating these classes were inherently promise problems.

Time: 14:30

## The Space Just Above One Clean Qubit

*Dale Jacobs*[1], *Saeed Mehraban*[1]

[1] Tufts University

Consider the model of computation where we start with two halves of a 2n-qubit maximally entangled state. We get to apply a universal quantum computation on one half, measure both halves at the end, and perform classical postprocessing. This model, which we call 1/2BQP, was defined in STOC 2017 [ABKM17] to capture the power of permutational computations on special input states. As observed in [ABKM17], this model can be viewed as a natural generalization of the one-clean-qubit model (DQC1) where we learn the content of a high entropy input state only after the computation is completed. An interesting open question is to characterize the power of this model, which seems to sit nontrivially between DQC1 and BQP. In this paper, we show that despite its limitations, this model can carry out many well-known quantum computations that are candidates for exponential speed-up over classical (or possibly DQC1) computations. In particular, 1/2BQP can simulate Instantaneous Quantum Polynomial Time (IQP) and solve the Deutsch-Jozsa problem, Bernstein-Vazirani problem, Simon's problem, and period finding. As a consequence, 1/2BQP also solves Order Finding and Factoring outside of the oracle setting. Furthermore, 1/2BQP can solve Forrelation and the corresponding oracle problem given by Raz and Tal [RT22] to separate BQP and PH. We also study limitations of 1/2BQP and show that similarly to DQC1, 1/2BQP cannot distinguish between unitaries which are close in trace distance, then give an oracle separating 1/2BQP and BQP. Due to this limitation, 1/2BQP cannot obtain the quadratic speedup for unstructured search given by Grover's algorithm [Gro96]. We conjecture that 1/2BQP cannot solve 3-Forrelation.

## Day 2: September 16, 2025, Tuesday

### Session 3

Time: 15:00

# Quantum Threshold is Powerful

*Jackson Morris*[1], *Daniel Grier*[1]

[1] University of California, San Diego

In 2005, Høyer and ˇSpalek showed that constant-depth quantum circuits augmented with multi-qubit Fanout gates are quite powerful, able to compute a wide variety of Boolean functions as well as the quantum Fourier transform. They also asked what other multi-qubit gates could rival Fanout in terms of computational power, and suggested that the quantum Threshold gate might be one such candidate. Threshold is the gate that indicates if the Hamming weight of a classical basis state input is greater than some target value.

We prove that Threshold is indeed powerful—there are polynomial-size constant-depth quan- tum circuits with Threshold gates that compute Fanout to high fidelity. Our proof is a gener- alization of a proof by Rosenthal that exponential-size constant-depth circuits with generalized Toffoli gates can compute Fanout. Our construction reveals that other quantum gates able to "weakly approximate" Parity can also be used as substitutes for Fanou.

# Day 2: September 16, 2025, Tuesday

## Session 3

Time: 15:30

### Quantum computational complexity of matrix functions

***Santiago Cifuentes*, UBA-CONICET), Samson Wang[1], Thais Lima Silva[2], Mario Berta[3], Leandro Aolita**

[1] Institute for Quantum Information and Matter, Caltech
[2] Technology Innovation Institute
[3] RWTH Aachen University

We investigate the dividing line between classical and quantum computational power in estimating properties of matrix functions. More precisely, we study the computational complexity of two primitive problems: (i) given a function $f$ and a Hermitian matrix $A$, compute a matrix element of $f(A)$, or (ii) compute a local measurement on $f(A)\,|0\rangle^{\otimes n}$, with $|0\rangle^{\otimes n}$ an $n$-qubit reference state, in both cases up to additive approximation error.

We consider four functions — monomials, Chebyshev polynomials, the time-evolution function, and the inverse function — and probe the complexity across a broad landscape covering different problem input regimes. Namely, we consider two types of matrix inputs (sparse and Pauli access), matrix properties (norm, sparsity), the approximation error, and function-specific parameters.

We identify BQP-complete forms of both problems for each function, and then toggle the problem parameters to easier regimes to see where hardness remains, or where the problem becomes classically easy. As part of our results, we make concrete a hierarchy of hardness across the functions: in parameter regimes where we have classically efficient algorithms for monomials, all three other functions remain robustly BQP-hard, or hard under usual computational complexity assumptions.

In identifying classically easy regimes, we show, among others, that for any polynomial of degree $\mathrm{poly}(n)$ both problems can be efficiently classically simulated when $A$ has $O(\log n)$ non-zero coefficients in the Pauli basis. This contrasts with the fact that the problems are BQP-complete in the sparse-access model even for constant row sparsity, whereas the stated Pauli access efficiently constructs sparse access with row sparsity $O(\log n)$.

Our work thus provides a catalog of efficient quantum and classical algorithms for fundamental linear-algebra tasks.

Time: 9:30 (Invited Talk)

## Quantum algorithms for codes and lattices based on Regev's reduction

*André Chailloux*[1], *Jean-Pierre Tillich*[2]

IS

[1] French Institute for Research in Computer Science and Automation, France
[2] INRIA Paris

In recent years, Regev's reduction has been used as a quantum algorithmic tool to provide quantum advantage for variants of the decoding problem. Chen, Liu, and Zhandry (Quantum Algorithms for Variants of Average-Case Lattice Problems via Filtering, EUROCRYPT 2022) presented a novel quantum algorithm for $SIS_\infty$ in a parameter regime unachievable by classical computers. While this regime is far from the one used in post-quantum cryptography, the algorithm already demonstrates how to leverage Regev's reduction for quantum advantage. Following this line of work, a new quantum algorithm called Decoded Quantum Interferometry has been proposed by Jordan et al., which is capable of solving several optimization problems in quantum polynomial time. In particular, they study the Optimal Polynomial Interpolation (OPI) problem, which can be viewed as a decoding problem on Reed–Solomon codes.

In this talk, I will present an overview of this family of quantum algorithms as well as some of our contributions. I will first briefly introduce the main ideas from our paper. The Quantum Decoding Problem (Chailloux and Tillich, TQC 2024), where we conduct an extensive study of the decoding problem when errors are in quantum superposition, and show how this can be applied using Regev's reduction. Then, I will present in more detail our work Quantum Advantage from Soft Decoders (Chailloux and Tillich, STOC 2025). In this work, we provide natural and compelling decoding problems for which we believe a quantum advantage exists. Our proof techniques involve the use of a soft decoder for Reed–Solomon codes—namely, the decoding algorithm from Koetter and Vardy. To make this decoder compatible with the setting of Regev's reduction, we present a novel, generic reduction from a syndrome decoding problem to a coset sampling problem. This yields a powerful and easy-to-use theorem that generalizes previous work and is of independent interest. We also present an extensive study of OPI using the Koetter and Vardy algorithm.

# Day 3: September 17, 2025, Wednesday

## Session 1

Time: 11:30

### SPAM-free sound certification of quantum gates via quantum system quizzing

*Nikolai Miklin*[1], *Jan Nöller*[2], *Martin Kliesch*[1], *Mariami Gachechiladze, Darmstadt)*

[1] Hamburg University of Technology
[2] Technical University of Darmstadt

The rapid advancement of quantum hardware necessitates the development of reliable methods to certify its correct functioning. However, existing certification tests often fall short: they either rely on flawless state preparation and measurement, or fail to provide soundness guarantees, meaning that they do not ensure the correct implementation of the target operation by a quantum device. We introduce an approach, which we call quantum system quizzing, for certification of quantum gates in a practical server-user scenario, where a classical user tests the results of exact quantum computations performed by a quantum server. Importantly, this approach is free from state preparation and measurement (SPAM) errors. For a wide range of relevant gates, including a gate set universal for quantum computation, we demonstrate that our approach offers soundness guarantees based solely on the dimension assumption. Additionally, for a highly-relevant single-qubit phase gate - which corresponds experimentally to a pi/2-pulse - we prove that the method's sample complexity scales inverse-linearly relative to the average gate infidelity. By combining the SPAM-error-free and sound notion of certification with practical applicability, our approach paves the way for promising research into efficient and reliable certification methods for quantum computation.

## Session 1

Time: 12:00

### Parallel Logical Measurements via Quantum Code Surgery

***Alexander Cowtan***[1], ***Zhiyang He***[2], ***Dominic J. Williamson***[3], ***Theodore J. Yoder***[4]

[1] Oxford University
[2] MIT
[3] University of Sydney
[4] IBM

Quantum code surgery is a flexible and low overhead technique for perform- ing logical measurements on quantum error-correcting codes, which generalises lattice surgery. In this work, we present a code surgery scheme, applicable to any Calderbank-Shor-Steane quantum low-density parity check (LDPC) code, that fault-tolerantly measures many logical Pauli operators in parallel. For a collection of logically disjoint Pauli product measurements supported on t log- ical qubits, our scheme uses $O(t\omega(\log t + \log^3 \omega))$ ancilla qubits, where $\omega \geq d$ is the maximum weight of the single logical Pauli representatives involved in the measurements, and $d$ is the code distance. This is all done in time $O(d)$ independent of t. Our proposed scheme preserves both the LDPC property and the fault-distance of the original code, without requiring ancillary logical codeblocks which may be costly to prepare. This addresses a shortcoming of several recently introduced surgery schemes which can only be applied to mea- sure a limited number of logical operators in parallel if they overlap on data qubits.

## Day 3: September 17, 2025, Wednesday

## Session 1

Time: 12:30

### Quantum Catalytic Space

*Harry Buhrman*[1], *Marten Folkertsma*[2], *Ian Mertz*[3], *Florian Speelman*[4], *Sergii Strelchuk*[5], *Sathyawageeswar Subramanian*[6], *Quinten Tupker*[2]

[1] Quantinuum London & CWI
[2] CWI & QuSoft
[3] Charles University
[4] University of Amsterdam & QuSoft
[5] University of Oxford
[6] University of Cambridge

Space complexity is a key field of study in theoretical computer science. In tSpace complexity is a key field of study in theoretical computer science. In the quantum setting there are clear motivations to understand the power of space-restricted computation, as qubits are an especially precious and limited resource.

Recently, a new branch of space-bounded complexity called catalytic computing has shown that reusing space is a very powerful computational resource, especially for subroutines that incur little to no space overhead. While quantum catalysis in an information theoretic context, and the power of “dirty” qubits for quantum computation, has been studied over the years, these models are generally not suitable for use in quantum space-bounded algorithms, as they either rely on specific catalytic states or destroy the memory being borrowed.

We define the notion of catalytic computing in the quantum setting and show a number of initial results about the model. First, we show that quantum catalytic logspace can always be computed quantumly in polynomial time; the classical analogue of this is the largest open question in catalytic computing. This also allows quantum catalytic space to be defined in an equivalent way with respect to circuits instead of Turing machines. We also prove that quantum catalytic logspace can simulate log-depth threshold circuits, a class which is known to contain (and believed to strictly contain) quantum logspace, thus showcasing the power of quantum catalytic space. Finally we show that both unitary quantum catalytic logspace and classical catalytic logspace can be simulated in the one-clean qubit model.

## Day 3: September 17, 2025, Wednesday

### Session 2

Time: 11:30

### A Meta-Complexity Characterization of Quantum Cryptography

*Bruno Cavalar*[1], *Eli Goldin*[2], *Matthew Gray*[1], *Peter Hall*[2], *Taiga Hiroka*[3], *Tomoyuki Morimae*[3]

[1] University of Oxford
[2] NYU
[3] Kyoto University

We prove the first meta-complexity characterization of a quantum cryptographic primitive. We show that one-way puzzles exist if and only if there is some quantum samplable distribution of binary strings over which it is hard to approximate Kolmogorov complexity. Therefore, we characterize one-way puzzles by the average-case hardness of a uncomputable problem. This brings to the quantum setting a recent line of work that characterizes classical cryptography with the average-case hardness of a meta-complexity problem (Liu-Pass (FOCS 2020), Ilango-Ren-Santhanam (STOC 2022) and others). Moreover, since the average-case hardness of Kolmogorov complexity over classically polynomial-time samplable distributions characterizes one-way functions, this result poses one-way puzzles as a natural generalization of one-way functions to the quantum setting. Furthermore, our equivalence goes through probability estimation, giving us the additional equivalence that one-way puzzles exist if and only if there is a quantum samplable distribution over which probability estimation is hard. We also observe that the oracle worlds of Kretschmer (TQC 2021) and Kretschmer, Qian, Sinha and Tal (STOC 2023) rule out any relativizing characterization of one-way puzzles by the hardness of a problem in NP or QMA, which means that it may not be possible with current techniques to characterize one-way puzzles with another meta-complexity problem.

Session 2

Time: 12:00

## Copy-Protecting Puncturable Functionalities, Revisited

*Prabhanjan Ananth*[1], *Amit Behera*[2], *Zikuan Huang*[3]

[1] University of California, Santa Barbara
[2] Ben-Gurion University of the Negev
[3] Tsinghua University

Quantum copy-protection is a foundational notion in quantum cryptography that leverages the governing principles of quantum mechanics to tackle the problem of software anti-piracy. Despite progress in recent years, precisely characterizing the class of functionalities that can be copy-protected is still not well understood.

Two recent works, by [Coladangelo and Gunn, STOC 2024] and [Ananth and Behera, CRYPTO 2024], showed that puncturable functionalities can be copy-protected. Both works have significant caveats with regard to the underlying cryptographic assumptions and additionally restrict the output length of the functionalities to be copy-protected. In this work, we make progress towards simultaneously addressing both the caveats. We show the following:

• Revisiting Unclonable Puncturable Obfuscation (UPO): We revisit the notion of UPO introduced by [Ananth and Behera, CRYPTO 2024]. We present a new approach to constructing UPO and a variant of UPO called independent-secure UPO. Unlike UPO, we show how to base the latter notion on well-studied assumptions.

• Copy-Protection from Independent-secure UPO: Assuming independent-secure UPO, we show that any $m$-bit, for $m \geq 2$, puncturable functionality can be copy-protected.

• Copy-Protection from UPO: Assuming UPO, we show that any 1-bit puncturable functionality can be copy-protected.

Session 2

Time: 12:30

## Additivity and chain rules for quantum entropies via multi-index Schatten norms

***Omar Fawzi***[1]***, Jan Kochanowski, INRIA Saclay), Cambyse Rouzé, INRIA Saclay), Thomas van Himbeeck***[2]

[1] ENS Lyon, INRIA Lyon
[2] INRIA Paris

The primary entropic measures for quantum states are additive under the tensor product. In the analysis of quantum information processing tasks, the minimum entropy of a set of states, e.g., the minimum output entropy of a channel, often plays a crucial role. A fundamental question in quantum information and cryptography is whether the minimum output entropy remains additive under the tensor product of channels. Here, we establish a general additivity statement for the optimized sandwiched Rényi entropy of quantum channels. For that, we generalize the results of [Devetak, Junge, King, Ruskai, CMP 2006] to multi-index Schatten norms. As an application, we strengthen the additivity statement of [Van Himbeeck and Brown, 2025] thus allowing the analysis of time-adaptive quantum cryptographic protocols. In addition, we establish chain rules for Rényi conditional entropies that are similar to the ones used for the generalized entropy accumulation theorem of [Metger, Fawzi, Sutter, Renner, CMP 2024].

# Day 3: September 17, 2025, Wednesday

## Session 3

### Time: 11:30

### Quantum SAT Problems with Finite Sets of Projectors are Complete for a Plethora of Classes

***Ricardo Rivera Cardoso***[1], ***Alex Meiburg***[2], ***Daniel Nagaj***[1]

[1] Slovak Academy of Sciences
[2] University of Waterloo

Prior to this work, all known variations of the *Quantum Satisfiability* (QSAT) problem—consisting of determining whether a $k$-local ($k$-body) Hamiltonian is frustration-free—could be classified as being either in ¶, -complete, -complete, or $_1$-complete. Problems in the latter three classes are not known to be solvable efficiently. Here, we demonstrate new variations of this problem that are complete for $_1$, , , PI$(\mathrm{coRP}, \mathrm{NP})$, PI$(\mathrm{BQP}_1, \mathrm{NP})$, PI$(\mathrm{BQP}_1, \mathrm{MA})$, SoPU$(\mathrm{coRP}, \mathrm{NP})$, SoPU$(\mathrm{BQP}_1, \mathrm{NP})$, and SoPU$(\mathrm{BQP}_1, \mathrm{MA})$. Our result implies that a complete classification of quantum constraint satisfaction problems (QCSPs), analogous to Schaefer's dichotomy theorem for classical CSPs, must either include these $13$ classes, or otherwise show that some of them are equal. Furthermore, our result shows there are two new types of QSAT problems that can be decided efficiently, as well as the first nontrivial problem known to be complete for $_1$.

We first show that there are QSAT problems on qudits that are complete for $_1$, , and . These problems are constructed by restricting the allowed sets of Hamiltonians to consist of elements similar to $H_{init}$, $H_{prop}$, and $H_{out}$, seen in the circuit-to-Hamiltonian transformation. Normally, these are used to demonstrate hardness of QSAT and *Local Hamiltonian* problems, and so our proofs of hardness are relatively simple. We modify these terms to involve high-dimensional data and clock qudits, ternary logic, and either monogamy of entanglement or specific clock encodings to ensure that all Hamiltonians generated with these three elements can be decided in their respective classes.

We then prove that any QCSP can be reduced to a problem in qubits while maintaining the same complexity—something that is believed not to be possible classically. This allows us to obtain complete QSAT problems on qubits. The remaining six problems are obtained by considering "sums" and "products" of the previous seven QSAT problems. Before this work, the QSAT problems generated in this way resulted in complete problems for PI and SoPU classes that were trivially equal to , , or $_1$. We thus commence the study of these new and seemingly nontrivial classes.

While [**?**] first sought to prove completeness for , $_1$, and , we note that his constructions are flawed, leading to incorrect proofs of these statements. Here, we rework these constructions and obtain improvements on the required qudit dimensionality.

Session 3

Time: 12:00

## Classically estimating observables of noiseless quantum circuits

*Armando Angrisani*[1], *Alexander Schmidhuber*[2], *Manuel S. Rudolph*[1], *Marco Cerezo*[3], *Zoë Holmes*[1], *Hsin-Yuan Huang*[4]

[1] EPFL
[2] MIT
[3] Los Alamos National Laboratory
[4] Google Quantum AI, MIT, Caltech

We present a classical algorithm for estimating expectation values of arbitrary observables on most quantum circuits across all circuit architectures and depths, including those with all-to-all connectivity. We prove that for any architecture where each circuit layer is equipped with a measure invariant under single-qubit rotations, our algorithm achieves a small error epsilon on all circuits except for a small fraction delta. The computational time is polynomial in qubit count and circuit depth for any small constant epsilon and delta, and quasi-polynomial for inverse-polynomially small epsilon and delta.Given that most quantum circuits in an architecture exhibit chaotic and locally scrambling behavior, our work demonstrates that estimating observables of such quantum dynamics is classically tractable across all geometries.

# Day 3: September 17, 2025, Wednesday

## Session 3

Time: 12:30

### Forrelation is Extremally Hard

*Uma Girish*[1], *Rocco Servedio*[1]

[1] Columbia University

The Forrelation problem is a central problem that demonstrates exponential separations between quantum and classical capabilities. In this problem, given query access to $n$-bit Boolean functions $f$ and $g$, the goal is to estimate the Forrelation function $(f, g)$, which measures the correlation between $g$ and the Fourier transform of $f$.

Our work offers a fundamentally new perspective on the Forrelation problem – one that is linear algebraic as opposed to prior analytic approaches. We establish a novel connection between the Forrelation problem and *bent Boolean functions* and through this connection, analyze an *extremal* version of the Forrelation problem where the goal is distinguish between extremal instances of Forrelation, namely $(f, g)$ with $(f, g) = 1$ and $(f, g) = -1$.

Using this, we show the first example of a problem that can be solved with *one* quantum query and success probability *one*, yet requires $\tilde{\Omega}\left(2^{n/4}\right)$ classical randomized queries, even for algorithms with a one-third failure probability, highlighting the remarkable power of one exact quantum query. We also study a restricted variant of this problem where the inputs $f, g$ are computable by small classical circuits and show classical hardness under cryptographic assumptions.

## Time: 9:30 (Invited Talk)

### Post-quantum security of lattice-based cryptosystems

***Rajendra Kumar***[1]

IS

IIT Delhi , India

Classical number-theoretic cryptosystems (such as RSA and ElGamal) are not secure against adversaries equipped with fully-fledged quantum computers. Given the progress in quantum computing over the past two decades, there is a possibility of practical attacks on these traditional cryptosystems in the near future. For long-term security, we turn to post-quantum cryptosystems, which can be implemented on today's computers and are conjectured to be secure even against quantum attacks.

In this talk, I will discuss the post-quantum security of lattice-based cryptosystems, which is the most prominent candidates for post-quantum cryptography. We will explore recent classical and quantum attacks, and I will also talk about recent work on establishing fine-grained security guarantees for lattice-based schemes.

Time: 11:00

## Adaptive Syndrome Extraction

*Noah Berthusen*[1], *Shi Jie Samuel Tan*[1], *Eric Huang*[1], *Daniel Gottesman*[1]

[1] University of Maryland

Device error rates on current quantum computers have improved enough to where demonstrations of error correction below break-even are now possible. Still, the circuits required for quantum error correction introduce significant overhead and sometimes inject more errors than they correct. In this work, we introduce adaptive syndrome extraction as a scheme to improve code performance and reduce the quantum error correction cycle time by measuring only the stabilizer generators that are likely to provide useful syndrome information. We provide a concrete example of the scheme through the [[4,2,2]] code concatenated with a hypergraph product code and a syndrome extraction cycle that uses quantum error detection to modify the syndrome extraction circuits in real time. Compared to non-concatenated codes and non-adaptive syndrome extraction, we find that the adaptive scheme achieves over an order of magnitude lower logical error rates while requiring fewer CNOT gates and physical qubits. Furthermore, we show how to achieve fault-tolerant universal logical computation with [[4,2,2]]-concatenated hypergraph product codes.

## Session 1

Time: 11:30

### Bounding the computational power of bosonic systems

*Varun Upreti*[1], *Ulysse Chabaud*[1]

[1] Ecole Normale Supérieure, Paris, France

Bosonic quantum systems operate in an infinite-dimensional Hilbert space, unlike discrete-variable quantum systems. This distinct mathematical structure leads to fundamental differences in quantum information processing, such as an exponentially greater complexity of state tomography [MMB+24] or a factoring algorithm in constant space [BCCRK24]. Yet, it remains unclear whether this structural difference of bosonic systems may also translate to a practical computational advantage over finite-dimensional quantum computers. Here, we take a step towards answering this question by showing that universal bosonic quantum computations can be simulated in exponential time on a classical computer, significantly improving the best previous upper bound requiring exponential memory [CJMM24]. In complexity-theoretic terms, we improve the best upper bound on CVBQP from EXPSPACE to EXP. This result is achieved using a simulation strategy based on finite energy cutoffs and approximate coherent state decompositions. While we propose ways to potentially refine this bound, we also present arguments supporting the plausibility of an exponential computational advantage of bosonic quantum computers over their discrete-variable counterparts. Furthermore, we emphasize the role of circuit energy as a resource and discuss why it may act as the fundamental bottleneck in realizing this advantage in practical implementations.

## Session 1

Time: 12:00

### X-arability of quantum states

*Harm Derksen*[1], *Nathaniel Johnston*[2], *Benjamin Lovitz*[1]

[1] Northeastern University
[2] Mount Allison University

The problem of determining when entanglement is present in a quantum system is one of the most active areas of research in quantum physics. Depending on the setting at hand, different notions of entanglement (or lack thereof) become relevant. Examples include separability (of bosons, fermions, and distinguishable particles), Schmidt number, biseparability, entanglement depth, and bond dimension. In this work, we propose and study a unified notion of separability, which we call X-arability, that captures a wide range of applications including these. We develop unified tools for studying X-arability, and prove efficiency guarantees for these tools. Our results include:

-A hierarchy of linear systems for the X-tangled subspace problem, which we prove terminates in polynomial time in many cases.

-A hierarchy of eigencomputations for optimizing a Hermitian operator over X. In particular, we prove a new fermionic de Finetti theorem, with applications to optimizing over Slater determinants in quantum chemistry.

# Day 4: September 18, 2025, Thursday

## Session 2

**Time: 11:00**

### Pseudorandom Function-like States from Common Haar Unitary

***Minki Hhan***[1], ***Shogo Yamada***[2]

[1] The University of Texas at Austin
[2] Kyoto University

Recent active studies have demonstrated that cryptography without one-way functions (OWFs) could be possible in the quantum world. Many fundamental primitives that are natural quantum analogs of OWFs or pseudorandom generators (PRGs) have been introduced, and their mutual relations and applications have been studied. Among them, pseudorandom function-like state generators (PRFSGs) [Ananth, Qian, and Yuen, Crypto 2022] are one of the most important primitives. PRFSGs are a natural quantum analogue of pseudorandom functions (PRFs), and imply many applications such as IND-CPA secret-key encryption (SKE) and EUF-CMA message authentication code (MAC). However, only known constructions of (many-query-secure) PRFSGs are ones from OWFs or pseudorandom unitaries (PRUs). In this paper, we construct classically-accessible adaptive secure PRFSGs in the invertible quantum Haar random oracle (QHRO) model which is introduced in [Chen and Movassagh, Quantum]. The invertible QHRO model is an idealized model where any party can access a public single Haar random unitary and its inverse, which can be considered as a quantum analog of the random oracle model. Our PRFSG constructions resemble the classical Even-Mansour encryption based on a single permutation, and are secure against any unbounded polynomial number of queries to the oracle and construction. To our knowledge, this is the first application in the invertible QHRO model without any assumption or conjecture. The previous best constructions in the idealized model are PRFSGs secure up to $o(/\log)$ queries in the common Haar state model [Ananth, Gulati, and Lin, TCC 2024] and (inverseless) PRUs in a relaxed QRHO model without inverse access [Ananth, Bostanci, Gulati, and Lin, Eurocrypt 2025]. We develop new techniques on Haar random unitaries to prove the selective and adaptive security of our PRFSGs. For selective security, we introduce a new formula, which we call the Haar twirl approximation formula. For adaptive security, we show the unitary reprogramming lemma and the unitary resampling lemma along with several technical tools for unitary oracle security proof with pure state queries. These have their own interest and may have many further applications. In particular, by using the approximation formula, we give an alternative proof of the non-adaptive security of the PFC ensemble [Metger, Poremba, Sinha, and Yuen, FOCS 2024] as an additional result. Finally, we prove that our construction is not PRUs or quantum-accessible non-adaptive PRFSGs by presenting quantum polynomial time attacks. Our attack is based on generalizing the hidden subgroup problem where the relevant function outputs quantum states.

# Day 4: September 18, 2025, Thursday

## Session 2

Time: 11:30

### Efficient Quantum Pseudorandomness from Hamiltonian Phase States

*John Bostanci*[1], *Jonas Haferkamp*[2], *Dominik Hangleiter*[3], *Alexander Poremba*[4]

[1] Columbia University
[2] Harvard University
[3] UC Berkeley
[4] MIT

Quantum pseudorandomness has found applications in many areas of quantum information, ranging from entanglement theory, to models of scrambling phenomena in chaotic quantum systems, and, more recently, in the foundations of quantum cryptography. Kretschmer (TQC '21) showed that both pseudorandom states and pseudorandom unitaries exist even in a world without classical one-way functions. To this day, however, all known constructions require classical cryptographic building blocks which are themselves synonymous with the existence of one-way functions, and which are also challenging to implement on realistic quantum hardware.

In this work, we seek to make progress on both of these fronts simultaneously—by decoupling quantum pseudorandomness from classical cryptography altogether. We introduce a quantum hardness assumption called the Hamiltonian Phase State (HPS) problem, which is the task of decoding output states of a random instantaneous quantum polynomial-time (IQP) circuit. Hamiltonian phase states can be generated very efficiently using only Hadamard gates, single-qubit Z rotations and CNOT circuits. We show that the hardness of our problem reduces to a worst-case version of the problem, and we provide evidence that our assumption is plausibly fully quantum; meaning, it cannot be used to construct one-way functions. We also show information-theoretic hardness when only few copies of HPS are available by proving an approximate t-design property of our ensemble. Finally, we show that our HPS assumption and its variants allow us to efficiently construct many pseudorandom quantum primitives, ranging from pseudorandom states, to quantum pseudoentanglement, to pseudorandom unitaries, and even primitives such as public-key encryption with quantum keys.

Time: 12:00

## Quantum One-Time Programs, Revisited

*Aparna Gupte*[1], *Jiahui Liu*[2], *Justin Raizes*[3], *Bhaskar Roberts*[4], *Vinod Vaikuntanathan*[1]

[1] MIT
[2] Fujitsu Research
[3] CMU
[4] UC Berkeley

One-time programs (Goldwasser, Kalai and Rothblum, CRYPTO 2008) are programs that can be run on any single input of a user's choice, but not on a second input. Classically, they are unachievable without trusted hardware, but the destructive nature of quantum measure- ments seems to provide an alternate path to constructing them. Unfortunately, Broadbent, Gutoski and Stebila (CRYPTO 2013) showed that even with quantum techniques, a strong no- tion of one-time programs, similar to ideal obfuscation, cannot be achieved for any non-trivial quantum function. On the positive side, Ben-David and Sattath (Quantum, 2023) showed how to construct a quantum one-time program for a certain (probabilistic) digital signature scheme, under a weaker notion of one-time program security. There is a vast gap between achievable and provably impossible notions of one-time program security, and it is unclear what function- alities are one-time programmable and which are not, under the achievable notions of security. In this work, we present new, meaningful, yet achievable definitions of one-time program security for probabilistic classical functions. We show how to construct one time programs satis- fying these definitions for all functions in the classical oracle model and for constrained pseu- dorandom functions in the plain model. Finally, we examine the limits of these notions: we show a class of functions which cannot be one-time programmed in the plain model, as well as a class of functions which appears to be highly random given a single query, but whose quantum one-time program leaks the entire function even in the oracle model.

Time: 11:00

## Quantum Perfect Matchings

*David Cui*[1], *Laura Mančinska*[2], *Seyed Sajjad Nezhadi*[3], *David E. Roberson*[4]

[1] MIT
[2] University of Copenhagen
[3] University of Maryland
[4] Technical University of Denmark

We investigate quantum and nonsignaling generalizations of perfect matchings in graphs using nonlocal games. Specifically, we introduce nonlocal games that test for $L$-perfect matchings in bipartite graphs, perfect matchings in general graphs and hypergraphs, and fractional perfect matchings. Our definitions come from the fact that these games are classical property tests for the corresponding matching conditions. We use the existence of perfect quantum and nonsignaling strategies for these games to define quantum and nonsignaling versions of perfect matchings. Finally, we provide characterizations of when graphs exhibit these extended properties: - For nonsignaling matchings, we give a complete combinatorial characterizations. In particular, a graph has a nonsignaling perfect matching if and only if it admits a fractional perfect matching that has bounded value on triangles. - In bipartite graphs, the nonsignaling $L$-perfect matching property is achieved exactly when the left component of the graph can be split into two disjoint subgraphs: one with a classical $L$-perfect matching and another with left-degree 2. - In the quantum setting, we show that complete graphs $K_n$ with odd $n \geq 7$ have quantum perfect matchings. We prove that a graph has a quantum perfect matching if and only if the quantum independence number of its line graph is maximal, extending a classical relationship between perfect matchings and line graph independence numbers. - For bipartite graphs, we establish that the $L$-perfect matching game does not exhibit quantum pseudotelepathy, but we characterize the quantum advantage for complete bipartite graphs $K_{n,2}$. - Additionally, we prove that deciding quantum perfect matchings in hypergraphs is undecidable and leave open the question of its complexity in graphs.

Session 3

Time: 11:30

## Polynomial Time Quantum Gibbs Sampling for Fermi-Hubbard Model at Any Temperature

***Štěpán Šmíd***[1], ***Richard Meister***[1], ***Mario Berta***[2], ***Roberto Bondesan***[1]

[1] Imperial College London
[2] RWTH Aachen University

Recently, there have been several advancements in quantum algorithms for Gibbs sampling. These algorithms simulate the dynamics generated by an artificial Lindbladian, which is meticulously constructed to obey a detailed-balance condition with the Gibbs state of interest, ensuring it is a stationary point of the evolution, while simultaneously having efficiently implementable time steps. The overall complexity then depends primarily on the mixing time of the Lindbladian, which can vary drastically, but which has been previously bounded in the regime of high enough temperatures.

In this work, we calculate the spectral gap of the Lindbladian for free fermions using third quantisation, and also prove a logarithmic bound on its mixing time by analysing corresponding covariance matrices. Then we prove a constant gap of the perturbed Lindbladian corresponding to interacting fermions up to some maximal coupling strength. This is achieved by using theorems about stability of the gap for lattice fermions. Our methods apply at any constant temperature and independently of the system size. The gap then provides an upper bound on the mixing time, proving that the purified Gibbs state of weakly interacting (quasi)-local fermionic systems of any dimension can be prepared in quasi-cubic time. As an application of Gibbs sampling, we explain how to calculate partition functions for the considered systems.

We provide exact numerical simulations for small system sizes supporting the theory and also identify different suitable jump operators and filter functions for the sought-after regime of intermediate coupling in the Fermi-Hubbard model.

Session 3

Time: 12:00

## Generalized Short Path Algorithms: Towards Super-Quadratic Speedup over Markov Chain Search for Combinatorial Optimization

*Shouvanik Chakrabarti*[1], *Dylan Herman*[1], *Guneykan Ozgul*[1], *Shuchen Zhu*[1,2], *Brandon Augustino*[1], *Tianyi Hao*[1,3], *Zichang He*[1], *Ruslan Shaydulin*[1], *Marco Pistoia*[1]

[1] JPMorganChase
[2] Duke University
[3] University of Wisconsin-Madison

We analyze generalizations of algorithms based on the short-path framework first proposed by Hastings [*Quantum* 2, 78 (2018)], which has been extended and shown by Dalzell et al. [STOC '23] to achieve super-Grover speedups for certain binary optimization problems. We demonstrate that, under some commonly satisfied technical conditions, an appropriate generalization can achieve super-quadratic speedups not only over unstructured search but also over a classical optimization algorithm that searches for the optimum by drawing samples from the stationary distribution of a Markov Chain. We employ this framework to obtain algorithms for problems including variants of Max-Bisection, Max Independent Set, the Ising Model, and the Sherrington Kirkpatrick Model, whose runtimes are asymptotically faster than those obtainable from previous short path techniques. For random regular graphs of sufficiently high degree, our algorithm is super-quadratically faster than the best rigorously proven classical runtimes for regular graphs. Our results also shed light on the quantum nature of short path algorithms, by identifying a setting where our algorithm is super-quadratically faster than any polynomial time Gibbs sampler, unless NP = RP. This provides evidence that a classical algorithm that is only quadratically slower cannot be constructed from a fast mixing Markov Chain. We conclude the paper with a numerical analysis that guides the choice of parameters for short path algorithms and raises the possibility of super-quadratic speedups in settings that are currently beyond our theoretical analysis.

Time: 09:30

### A Unified Theory of Quantum Neural Network Loss Landscapes

***Eric R. Anschuetz***[1]

[1] Caltech

Classical neural networks with random initialization famously behave as Gaussian processes in the limit of many neurons, which allows one to completely characterize their training and generalization behavior. No such general understanding exists for quantum neural networks (QNNs), which—outside of certain special cases—are known to not behave as Gaussian processes when randomly initialized. We here prove that QNNs and their first two derivatives instead generally form what we call Wishart processes, where certain algebraic properties of the network determine the hyperparameters of the process. This Wishart process description allows us to, for the first time: give necessary and sufficient conditions for a QNN architecture to have a Gaussian process limit; calculate the full gradient distribution, generalizing previously known barren plateau results; and calculate the local minima distribution of algebraically constrained QNNs. Our unified framework suggests a certain simple operational definition for the "trainability" of a given QNN model using a newly introduced, experimentally accessible quantity we call the degrees of freedom of the network architecture.

Day 5: September 19, 2025, Friday

Session 1

Time: 10:00

## Online learning of quantum processes

***Asad Raza*, Universität Berlin), Matthias C. Caro, Systems, Freie Universität Berlin**[1]**, Jens Eisert, Universität Berlin**[2]**, Sumeet Khatri, Universität Berlin, for Quantum Information Science and Engineering)***

[1] 2) Department of Computer Science, University of Warwick
[2] 2) Helmholtz-Zentrum Berlin für Materialien und Energie

Among recent insights into learning quantum states, online learning and shadow tomography procedures are notable for their ability to accurately predict expectation values even of adaptively chosen observables. In contrast to the state case, quantum process learning tasks with a similarly adaptive nature have received little attention. In this work, we investigate online learning tasks for quantum processes. Whereas online learning is infeasible for general quantum channels, we show that channels of bounded gate complexity as well as Pauli channels can be online learned in the regret and mistake-bounded models of online learning. In fact, we can online learn probabilistic mixtures of any exponentially large set of known channels. We also provide a provably sample-efficient shadow tomography procedure for Pauli channels. Our results extend beyond quantum channels to non-Markovian multi-time processes, with favorable regret and mistake bounds, as well as a shadow tomography procedure. We complement our online learning upper bounds with mistake as well as computational lower bounds. On the technical side, we make use of the multiplicative weights update algorithm, classical adaptive data analysis, and Bell sampling, as well as tools from the theory of quantum combs for multi-time quantum processes. Our work initiates a study of online learning for classes of quantum channels and, more generally, non-Markovian quantum processes. Given the importance of online learning for state shadow tomography, this may serve as a step towards quantum channel variants of adaptive shadow tomography.

Time: 11:00

## Quantum Advantage for Learning Shallow Neural Networks with Natural Data Distributions

*Laura Lewis*[1,2,3], *Dar Gilboa*[1], *Jarrod R. McClean*[1]

[1] Google Quantum AI
[2] University of Cambridge
[3] University of Edinburgh

The application of quantum computers to machine learning tasks is an exciting potential direction to explore in search of quantum advantage. In the absence of large quantum computers to empirically evaluate performance, theoretical frameworks such as the quantum probably approximately correct (PAC) and quantum statistical query (QSQ) models have been proposed to study quantum algorithms for learning classical functions.

Despite numerous works investigating quantum advantage in these models, we nevertheless only understand it at two extremes: either exponential quantum advantages for uniform input distributions or no advantage for potentially adversarial distributions. In this work, we make progress towards filling the gap between these two regimes by designing an efficient quantum algorithm for learning periodic neurons in the QSQ model over a broad range of non-uniform distributions, which includes Gaussian, generalized Gaussian, and logistic distributions.

To our knowledge, our work is also the first result in quantum learning theory for classical functions that explicitly considers real-valued functions. Recent advances in classical learning theory prove that learning periodic neurons is hard for any classical gradient-based algorithm, giving us an exponential quantum advantage over such algorithms, which are the standard workhorse algorithms of machine learning. Moreover, in some parameter regimes, the problem remains hard for classical statistical query algorithms and even general classical algorithms learning under small amounts of noise.

Time: 11:30

## Hamiltonian Locality Testing via Trotterized Postselection

*John Kallaugher*[1], *Daniel Liang*[2]

[1] Sandia National Laboratories
[2] Portland State University

The (tolerant) Hamiltonian locality testing problem, introduced in [Bluhm, Caro, Oufkir ‘24], is to determine whether a Hamiltonian $H$ is $\varepsilon_1$-close to being $k$-local (i.e. can be written as the sum of weight-$k$ Pauli operators) or $\varepsilon_2$-far from any $k$-local Hamiltonian, given access to its time evolution operator and using as little total evolution time as possible, with distance typically defined by the normalized Frobenius norm. We give the tightest known bounds for this problem, proving an O$(1/(\varepsilon_2 - \varepsilon_1)^2)$ evolution time upper bound and an $\Omega(1/(\varepsilon_2 - \varepsilon_1))$ lower bound. Our algorithm does not require reverse time evolution or controlled application of the time evolution operator, although our lower bound applies to algorithms using either tool. Furthermore, we show that if we are allowed reverse time evolution, this lower bound is tight, giving a matching $\Omega(1/(\varepsilon_2 - \varepsilon_1))$ evolution time algorithm.

# Day 5: September 19, 2025, Friday

## Session 1

Time: 12:00

### Classical Estimation of the Free Energy and Quantum Gibbs Sampling from the Markov Entropy Decomposition

*Samuel Scalet*[1], *Angela Capel*[1], *Anirban Chowdhury*[2], *Hamza Fawzi*[1], *Omar Fawzi*[3], *Isaac Kim*[4], *Arkin Tikku*[5]

[1] University of Cambridge
[2] IBM Quantum
[3] Inria, ENS Lyon
[4] UC Davis
[5] University of Sydney

We revisit the Markov Entropy Decomposition, a classical convex relaxation algorithm introduced by Poulin and Hastings to approximate the free energy in quantum spin lattices. We identify a sufficient condition for its convergence, namely the decay of the effective Hamiltonian. We prove that this condition is satisfied for systems in 1D at any temperature as well as in the high-temperature regime under a certain commutativity condition on the Hamiltonian. This yields polynomial and quasi-polynomial time approximation algorithms in these settings respectively. We further prove that the decay of the effective Hamiltonian implies the decay of the conditional mutual information for the Gibbs state of the system. We then use this fact to devise a rounding scheme that maps the solution of the convex relaxation to a global state and show that the scheme can be efficiently implemented on a quantum computer, thus proving efficiency of quantum Gibbs sampling under our assumption of decay of the effective Hamiltonian.

Time: 12:30

### Towards a complexity-theoretic dichotomy for (2+1)-dimensional TQFT invariants

*Eric Samperton*[1], *Nicolas Bridges*[1]

[1] Purdue University

We show that for any fixed $(2 + 1)$-dimensional TQFT over $\mathbb{C}$ of either Turaev-Viro-Barrett-Westbury or Reshetikhin-Turaev type, the problem of exactly computing its invariants on closed 3-manifolds is either solvable in polynomial time, or else it is P-hard to (exactly) contract certain tensors that are built from the TQFT's fusion category. Our proof is an application of a dichotomy result of Cai and Chen [J. ACM, 2017] concerning weighted constraint satisfaction problems over $\mathbb{C}$. We leave for future work the issue of reinterpreting the conditions of Cai and Chen that distinguish between the two cases (i.e. P-hard tensor contractions vs. polynomial time invariants) in terms of fusion categories. We expect that with more effort, our reduction can be improved so that one gets a dichotomy directly for TQFTs' invariants of 3-manifolds rather than more general tensors built from the TQFT's fusion category.

Time: 09:30

## Strategic Codes: The Universal Spatio-Temporal Framework for Quantum Error-Correction

***Andrew Tanggara***[1], ***Mile Gu***[2], ***Kishor Bharti***[3]

[1] Centre for Quantum Technologies
[2] Nanyang Technological University
[3] Agency for Science, Technology and Research (A*STAR)

The susceptibility of quantum systems to noise hinders a scalable quantum computational speed-up, highlighting the need for quantum error-correcting codes (QECC). The emerging paradigm of dynamical QECC has revealed a plethora of possibilities on temporal noise-resilient encoding of quantum information through a sequence of operations, as opposed to a fixed spatial many-body encoding in conventional static QECCs. Although it has lead to progress in our understanding of error-correction and discoveries of more resource-efficient QECCs, an understanding of the physical extent of error-correction is still limited due to the lack of a unified framework. We overcome this by proposing the "strategic code" framework, the most general QECC framework encompassing all existing and physically plausible QECCs yet to be discovered, as well as the most general noise with spatial and temporal correlations. The framework uses an "interrogator" device, which models the most general quantum processes which adaptively interacts with the noise over multiple time-steps. Using the framework, we establish necessary and sufficient error-correction conditions, which include the analogous static QECC conditions as a special case, as well as propose an optimization-theoretic approach to construct a strategic code that recovers logical information up to a desired fidelity under a general noise model.

Time: 10:00

## Tesseract: A Search-Based Decoder for Quantum Error Correction

*Laleh Aghababaie Beni*[1], *Oscar Higgott*[1], *Noah Shutty*[1]

[1] Google Quantum AI

Tesseract is a Most-Likely-Error decoder designed for low-density-parity-check quantum error-correcting codes. Tesseract conducts a search through a graph on the set of all subsets of errors to find the lowest cost subset of errors consistent with the input syndrome. Although this graph is exponentially large, the search can be made efficient in practice for random errors using A$^*$ search technique along with a few pruning heuristics. We show through benchmark circuits for surface, color, and bivariate-bicycle codes that Tesseract is significantly faster than integer programming-based decoders while retaining comparable accuracy at moderate physical error rates. We also find that Tesseract can decode transversal CNOT protocols for surface codes on neutral atom quantum computers. Finally, we compare surface and bivariate bicycle codes using most-likely error decoding.

Session 2

Time: 11:00

## Orthogonality Broadcasting and Quantum Position Verification

*Ian George*[1], *Rene Allerstorfer*[2], *Philip Verduyn Lunel*[3], *Eric Chitambar*[4]

[1] National University of Singapore
[2] QuSoft, CWI, Amsterdam
[3] Sorbonne Universite
[4] University of Illinois at Urbana-Champaign

The no-cloning theorem leads to information-theoretic security in various quantum cryptographic protocols. However, this security typically derives from a possibly weaker property that classical information encoded in certain quantum states cannot be broadcast. To formally capture this property, we introduce the study of "orthogonality broadcasting." When attempting to broadcast the orthogonality of two different qubit bases, we establish that the power of classical and quantum communication is equivalent. However, quantum communication is shown to be strictly more powerful for broadcasting orthogonality in higher dimensions. We then relate orthogonality broadcasting to quantum position verification and provide a new method for establishing error bounds in the no pre-shared entanglement model that can address protocols previous methods could not. Our key technical contribution is an uncertainty relation that uses the geometric relation of the states that undergo broadcasting rather than the non-commutative aspect of the final measurements.

Session 2

Time: 11:30

## Unitary Designs of Symmetric Local Random Circuits

*Yosuke Mitsuhashi*[1], *Ryotaro Suzuki*[2], *Tomohiro Soejima*[3], *Nobuyuki Yoshioka*[4]

[1] RIKEN
[2] Freie Universität Berlin
[3] Harvard University
[4] University of Tokyo

We have established the method of characterizing the unitary design generated by a symmetric local random circuit. Concretely, we have shown that the necessary and sufficient condition for the circuit forming an approximate t-design is given by simple integer optimization for general symmetry and locality. By using the result, we explicitly give the maximal order of unitary design under the Z2, U(1), and SU(2) symmetries for general locality. This work reveals the relation between the fundamental notions of symmetry and locality in terms of randomness.

## Session 2

Time: 12:00

### A New World in the Depths of Microcrypt: Separating OWSGs and Quantum Money from QEFID

*Amit Behera*[1], *Giulio Malavolta*[2], *Tomoyuki Morimae*[3], *Tamer Mour*[2], *Takashi Yamakawa*[4]

[1] Ben-Gurion University of the Negev
[2] Bocconi University
[3] Kyoto University
[4] NTT Social Informatics Laboratories

While in classical cryptography, one-way functions (OWFs) are widely regarded as the “minimal assumption,” the situation in quantum cryptography is less clear. Recent works have put forward two concurrent candidates for the minimal assumption in quantum cryptography: One-way state generators (OWSGs), postulating the existence of a hard search problem with an efficient verification algorithm, and EFI pairs, postulating the existence of a hard distinguishing problem. Two recent papers [Khurana and Tomer STOC’24; Batra and Jain FOCS’24] showed that OWSGs imply EFI pairs, but the reverse direction remained open.

In this work, we give strong evidence that the opposite direction does not hold: We show that there is a quantum unitary oracle relative to which EFI pairs exist, but OWSGs do not. In fact, we show a slightly stronger statement that also holds for EFI pairs that output classical bits (QEFID pairs).

As a consequence, we separate, via our oracle, QEFID pairs and one-way puzzles from OWSGs and several other Microcrypt primitives, including efficiently verifiable one-way puzzles and unclonable state generators. In particular, this solves a problem left open in [Chung, Goldin, and Gray Crypto’24].

Using similar techniques, we also establish a fully black-box separation (which is slightly weaker than an oracle separation) between private-key quantum money schemes and QEFID pairs.

One conceptual implication of our work is that the existence of an efficient verification algorithm may lead to qualitatively stronger primitives in quantum cryptography.

Day 5: September 19, 2025, Friday

Session 2

Time: 12:30

## Impossibility of Hyperefficient Shadow Tomography: Unbounded Multiple-Copy Secure Copy-Protection

*Alper Cakan*[1], *Vipul Goyal*[2]

[1] Carnegie Mellon University
[2] NTT Research

The quantum no-cloning theorem gives rise to the intriguing possibility of quantum copy protection, where we encode a program or functionality in a quantum state such that a user in possession of $k$ copies cannot create $k+1$ copies, for any $k$. Introduced by Aaronson (CCC'09) over a decade ago, copy protection has proven to be notoriously hard to achieve. Previous work has been able to achieve copy-protection for various functionalities only in restricted models: (i) in the bounded collusion setting where $k \rightarrow k+1$ security is achieved for an a-priori fixed collusion bound $k$ (in the plain model with the same computational assumptions as ours, by Liu, Liu, Qian, Zhandry [TCC'22]), or (ii) only $k \rightarrow 2k$ security is achieved (relative to a structured quantum oracle, by Aaronson [CCC'09]). In this work, we give the first unbounded collusion-resistant (i.e., multiple-copy secure) copy-protection schemes, answering the long-standing open question of constructing such schemes, raised by multiple previous works starting with Aaronson (CCC'09). More specifically, we obtain the following results. • We construct (i) public-key encryption, (ii) public-key functional encryption, (iii) signature, and (iv) pseudorandom function schemes whose keys are copy-protected against unbounded collusions in the plain model (i.e., without any idealized oracles), assuming (post-quantum) subexponentially secure iO and LWE. • We show that any unlearnable functionality can be copy-protected against unbounded collusions, relative to a classical oracle. • As a corollary of our results, we rule out the existence of hyperefficient quantum shadow tomography,

- even given non-black-box access to the measurements, assuming subexponentially secure iO and LWE, or
- unconditionally relative to a quantumly accessible classical oracle,

and hence answer an open question by Aaronson (STOC'18). We obtain our results through a novel technique which uses identity-based encryption to construct multiple-copy secure copy-protection schemes from $1$-copy $\rightarrow$ $2$-copy secure schemes. We believe our technique is of independent interest.

Along the way, we also obtain the following results. • We define and prove the security of new collusion-resistant monogamy-of-entanglement games for coset states. • We construct a classical puncturable functional encryption scheme whose master secret key can be punctured at all functions $f$ such that $f(m_0) \neq f(m_1)$. This might also be of independent interest.

Day 5: September 19, 2025, Friday

Session 3

Time: 09:30

## Quantum Spin Chains and Symmetric Functions

*Marcos Crichigno*[1], *Anupam Prakash*[2]

[1] Phasecraft US
[2] JPM Quantum

We consider the question of what quantum spin chains naturally encode in their Hilbert space. It turns out that quantum spin chains are rather rich systems, naturally encoding solutions to various problems in combinatorics, group theory, and algebraic geometry. In the case of the XX Heisenberg spin chain these are given by skew Kostka numbers, skew characters of the symmetric group, and Littlewood-Richardson coefficients. As we show, this is revealed by a fermionic representation of the theory of "quantized" symmetric functions formulated by Fomin and Greene, which provides a powerful framework for constructing operators extracting this data from the Hilbert space of quantum spin chains. Furthermore, these operators are diagonalized by the Bethe basis of the quantum spin chain. Underlying this is the fact that quantum spin chains are examples of "quantum integrable systems." This is somewhat analogous to bosons encoding permanents and fermions encoding determinants. This points towards considering quantum integrable systems, and the combinatorics associated with them, as potentially interesting targets for quantum computers.

Time: 11:00

## Testing and Learning structured quantum Hamiltonians

***Srinivasan Arunachalam***[1], ***Arkopal Dutt***[1], ***Francisco Escudero Gutiérrez***[2]

[1] IBM Quantum, USA
[2] CWI & QuSoft, Amsterdam

We consider the problems of testing and learning an $n$-qubit Hamiltonian

$$H = \sum_x \lambda_x \sigma_x,$$

expressed in its Pauli basis, from queries to its evolution operator $U = e^{-iHt}$.

For testing, we provide a tolerant protocol to decide whether a Hamiltonian is $\varepsilon_1$-close to $k$-local or $\varepsilon_2$-far from $k$-local in the $\ell_2$ norm of the coefficients, with query complexity $\mathcal{O}\left(\frac{1}{(\varepsilon_2-\varepsilon_1)^4}\right)$. This resolves two open questions posed in recent work by Bluhm, Caro, and Oufkir. We further give a protocol for testing whether a Hamiltonian is $\varepsilon_1$-close to being $s$-sparse or $\varepsilon_2$-far from being $s$-sparse in the $\ell_2$ norm, with query complexity $\mathcal{O}\left(\frac{s^6}{(\varepsilon_2^2-\varepsilon_1^2)^6}\right)$.

For learning, we present a protocol to $\varepsilon$-learn an unstructured Hamiltonian in the $\ell_\infty$ norm of the coefficients using $\mathcal{O}\left(\frac{1}{\varepsilon^4}\right)$ queries. Combining this with the non-commutative Bohnenblust–Hille inequality, we obtain an algorithm for learning $k$-local Hamiltonians in the $\ell_2$ norm with query complexity $\mathcal{O}\big(\exp(k^2 + k\log(1/\varepsilon))\big)$. For Hamiltonians that are $s$-sparse in the Pauli basis, we achieve learning in the $\ell_2$ norm with $\mathcal{O}\left(\frac{s^2}{\varepsilon^4}\right)$ queries.

These learning results are independent of the system size $n$, but they require $n$-qubit quantum memory. To address this, we provide subroutines that reproduce all the above learning results without quantum memory, at the cost of squaring the query complexity and introducing a $\log n$ overhead in the $k$-local case and an $n$-factor in the sparse case. For testing without quantum memory, we introduce a new subroutine called *Pauli hashing*, which enables tolerant testing of $s$-sparse Hamiltonians in the $\ell_2$ norm with query complexity $\mathcal{O}\left(\frac{s^{14}}{(\varepsilon_2^2-\varepsilon_1^2)^{18}}\right)$. A key ingredient is showing that $s$-sparse Pauli channels can be tested in a tolerant fashion for being $\varepsilon_1$-close to $s$-sparse or $\varepsilon_2$-far under the diamond norm, with query complexity $\mathcal{O}\left(\frac{s^2}{(\varepsilon_2-\varepsilon_1)^6}\right)$ via Pauli hashing.

To establish these results, we prove new structural theorems for local Hamiltonians, sparse Pauli channels, and sparse Hamiltonians. Our learning algorithms are complemented by lower bounds that are only polynomially weaker. Furthermore, all our algorithms rely only on short-time evolutions and do not assume prior knowledge of the Pauli spectrum support, i.e., they do not require prior knowledge of the support of the Hamiltonian terms.

Session 3

Time: 11:30

## The rotation-invariant Hamiltonian problem is QMAEXP-complete

*Jon Nelson*[1], *Daniel Gottesman*[1]

[1] University of Maryland

In this work we study a variant of the local Hamiltonian problem where we restrict to Hamiltonians that live on a lattice and are invariant under rotations of the lattice. In the one-dimensional case this problem is known to be QMAEXP-complete. On the other hand, if we fix the lattice length then in the high-dimensional limit the low-energy states become unentangled due to arguments from mean-field theory. We take steps towards understanding this complexity spectrum by studying a problem that is intermediate between these two extremes. Namely, we consider the regime where the lattice dimension is arbitrary but fixed and the lattice length is scaled. We prove that this rotationally-invariant Hamiltonian problem is QMAEXP-complete answering an open question of [Gottesman-Irani-18]. This extends the known parameter range in which these rotationally-invariant Hamiltonians maintain their complexity.

Time: 12:00

## Time-dependent Hamiltonian Simulation via Magnus Expansion: Algorithms and Discrete Superconvergence for Unbounded Hamiltonians

*Di Fang*[1], *Yonah Borns-Weil*[2], *Diyi Liu*[3], *Rahul Sarkar*[4], *Jiaqi Zhang*[1]

[1] Duke University
[2] University of California, Berkeley
[3] University of Minnesota
[4] Stanford University

Hamiltonian simulation becomes more challenging as the underlying unitary becomes more oscillatory. In such cases, an algorithm with commutator scaling and only weak dependence (such as logarithmic) on the derivatives of the Hamiltonian is desired. In the first manuscript, we introduce a new time-dependent Hamiltonian simulation algorithm based on the Magnus expansion that exhibits both of these features. Importantly, when applied to unbounded Hamiltonian simulation in the interaction picture, we prove that the commutator in the second-order algorithm leads to a surprising fourth-order superconvergence, with an error preconstant independent of the number of spatial grids.

In the second manuscript, we provide the first superconvergence estimate in the fully discrete setting with a finite number of spatial discretization points $N$, and show that it holds with an error constant uniform in $N$. The proof is based on the two-parameter symbol class, which, to our knowledge, is applied for the first time in algorithm analysis. We believe this approach may have broader applications in algorithm analysis beyond the specific context of this work.

Time: 12:30

## RE-completeness of entangled constraint satisfaction problems

***Eric Culf***[1], ***Kieran Mastel***[1]

[1] University of Waterloo

Constraint satisfaction problems (CSPs) are a natural class of decision problems where one must decide whether there is an assignment to variables that satisfies a given formula. Schaefer's dichotomy theorem, and its extension to all alphabets due to Bulatov and Zhuk, shows that CSP languages are either efficiently decidable, or NP-complete. It is possible to extend CSP languages to quantum assignments using the formalism of nonlocal games. Due to the equality of complexity classes MIP$^* =$ RE, general succinctly-presented entangled CSPs are RE-complete. In this work, we show that a wide range of NP-complete CSPs become RE-complete in this setting, including all boolean CSPs, such as 3SAT, as well as $3$-colouring. This also implies that these CSP languages remain undecidable even when not succinctly presented.

To show this, we work in the weighted algebra framework introduced by Mastel and Slofstra, where synchronous strategies for a nonlocal game are represented by tracial states on an algebra. Along the way, we improve the subdivision technique in order to be able to separate constraints in the CSP while preserving constant soundness, construct commutativity gadgets for all boolean CSPs, and show a variety of relations between the different ways of presenting CSPs as games.

# List of Posters

**Poster stand no.** **Poster title (Presenting author)**

1. Riemannian-geometric generalizations of quantum fidelities and Bures-Wasserstein distance (A. Afham).

2. Quantum Information Inspired Ansatz for Relativistic Atomic Ground State Energy Calculations (Abdul Kalam).

3. Variational Quantum Eigensolver with Measurement-Based Quantum Computing (MBQC) and Tensor Networks (Abdullah Kazi).

4. A quantum information theoretic analysis of reinforcement learning-assisted quantum architecture search (Abhishek Sadhu).

5. KANQAS: Kolmogorov-Arnold Network for Quantum Architecture Search (Abhishek Sadhu).

6. Performance of rotation symmetric bosonic codes under random telegraph noise-characterisation of non-Markovianity in the system (Adithi Udupa).

7. Visualizing the transition from Chaos to Order on an NISQ quantum computer (Aditi Rath, Dinesh Kumar Panda).

8. Efficacy of information causality principle in ruling out extreme compositions (Akarshit Baranwal, Vishnu Purushothaman).

9. Beyond quantum success probability in a communication task and the role of information causality (Akarshit Baranwal, Vishnu Purushothaman).

10. Quantum computing and persistence in topological data analysis (Alexander Schmidhuber).

11. Entanglement-Assisted Zero-Error Nash Equilibrium in Bayesian Games (Ambuj, Tushar).

12. Nature of correlation in triangle network (Amit Kundu).

13. Measurement-Device-Independent Certification of Schmidt Number (Amit Kundu, Pratik Ghosal, Saheli Mukherjee, Arun Kumar Das, Bivas Mallick).

14. Learning genuine network nonlocality for non-ideal scenarios: A domain-informed machine learning approach (Anantha Krishnan Sunilkumar, Debashis Saha).

15. Classically Spoofing System Linear Cross Entropy Score Benchmarking (Andrew Tanggara, Kishor Bharti).

16. Simple Construction of Qudit Floquet Codes on a Family of Lattices (Andrew Tanggara, Kishor Bharti).

17. Quantifying Diabatic Error in Coupled Photonic Waveguides (Ankit Singh Bhadauriya).

18. Decoding Quantum LDPC Codes using Collaborative Check Node Removal (Ankur Raina).

19. Time series forecasting using Quantum Fractal Interpolation Method (Anupama K).

20. Shot-frugal and Robust quantum kernel classifiers (Apoorva D Patel).

21. Efficient simulation of quantum circuits with non-unital noise using Pauli propagation (Armando Angrisani).

22. Efficient quantum-enhanced classical simulation for patches of quantum landscapes (Armando Angrisani).

23. A framework to solve protein folding problem in a quantum computer (Ashwini Kannan).

24. Communication-Efficient Quantum Secret Sharing in the presence of Malicious Adversaries (Avik Mukhopadhyay).

25. Variational Quantum Approach for Protein Folding with a Novel Encoding Framework (Ayushi).

26. Phase estimation using Dicke superposition state probes (B N Karthik).

27. Unlocking Quantum Acceleration for Classical Fully Homomorphic Encryption: A New Frontier in Secure Computation (Bhagyasree Yadlapalli).

28. Expedited Noise Spectroscopy of Transmon Qubits (Bhavesh Gupta).

29. Quantum Speed Up for Non-Maximum Suppression in Object Detection (Bhavin Makwana).

30. Non-Classicalities Exhibited by Superposition of Single Photon Added Coherent State with Vacuum (Bhawna).

31. Higher-dimensional entanglement detection and quantum channel characterization using moments of generalized positive maps (Bivas Mallick).

32. On the characterization of Schmidt number breaking and annihilating channels (Bivas Mallick).

33. Applications of the Quantum Phase Difference Estimation Algorithm to the Excitation Energies in Spin Systems on Classical and a Noisy Intermediate Scale Quantum Computers (Boni Paul).

34. Depth Reduction in Quantum Circuits via Parallelization and Classical Offloading (Boris Arseniev).

35. On the Advantage of Conjugated Clifford Circuits over Fragments of the Clifford Group (Chaitanya Karamchedu).

36. Optimization Driven Quantum Circuit Reduction (Christoph Hirche).

37. Consumable Data via Quantum Communication (Dar Gilboa).

38. Monogamy of Nonlocal Games (David Cui).

39. A Computational Tsirelson's Theorem for All Compiled Nonlocal Games (David Cui).

40. Communication complexity scenarios lead to robust self-testing of n-party GHZ basis measurements (Debashis Saha, Sagnik Ray, Barnik Nath Bhaumik).

41. An operational approach to classifying measurement incompatibility (Debashis Saha, Saheli Mukherjee, Arun Kumar Das).

42. Entangled states are not always useful for single shot distinguishability of unitaries (Debashis Saha, Satyaki Manna).

43. Efficient Relaxation of Generalized Noncontextual Polytopes and Quantum violation of their Facet Inequalities (Debashis Saha, Soumyabrata Hazra).

44. Entanglement dynamics via Geometric phases in Trapped-ions (Dharmaraj Ramachandran).

45. Entanglement dynamics via Geometric phases in Trapped-ions (Dharmaraj Ramachandran).

46. Quantum cryptographic protocols for dual-messaging via 2D alternate quantum walk of a single-photon and genuine 3-way and nonlocal 2-way entanglement (Dinesh Kumar Panda).

47. Fault-Tolerant Implementation of the Deutsch-Jozsa Algorithm (Divyanshu Singh).

48. Improved coherence time of a non-Hermitian qubit in a PT-symmetric Environment (Duttatreya).

49. Routed Bell tests and their application to device-independent quantum key distribution (Edwin Peter Lobo).

50. Learning junta distributions, quantum junta states, and QAC0 circuits (Francisco Escudero Gutiérrez).

51. On the Fourier Linear Cross-Entropy Benchmark (Francisco Escudero Gutiérrez).

52. Entanglement structure for finite system under dual unitary dynamics (Gaurav Rudra Malik, Sudhanva Joshi).

53. Decomposition of a system in pseudo-Hermitian quantum mechanics (Himanshu Badhani).

54. Volume of Assistance: a genuine entanglement measure (Indranil Biswas, Subrata Bera).

55. A single Change in Temperature can Solve the Deutsch – Josza Problem : An Exploration of Thermodynamic Query Complexity (Jake Xuereb).

56. Repeater-Based Quantum Communication Protocol: Maximizing Teleportation Fidelity with Minimal Entanglement (Jatin Ghai).

57. Oracle Separation Between Quantum Commitments and Quantum One-wayness (John Bostanci).

58. Fault-tolerant quantum memory using low-depth random circuit codes (Jon Nelson).

59. Polynomial-Time Classical Simulation of Noisy Quantum Circuits with Naturally Fault-Tolerant Gates (Jon Nelson).

60. Pseudorandom quantum authentication (Kishor Bharti).

61. Pseudorandom density matrices (Kishor Bharti).

62. Multivariate Bicycle Codes (Kishor Bharti).

63. Scalable & Noise-Robust Communication Advantage of Multipartite Quantum Entanglement (Kunika Agarwal, Pratik Ghosal, Sahil Gopalkrishna Naik, Ananya Chakraborty).

64. Nonlocality-Assisted Enhancement of Error-Free Communication in Noisy Classical Channels (Kunika Agarwal, Pratik Ghosal, Sahil Gopalkrishna Naik, Ananya Chakraborty).

65. Quantum Incompatibility in Parallel vs Antiparallel Spins (Kunika Agarwal, Snehasish Roy Chowdhury, Sahil Gopalkrishna Naik).

66. Classical simulation of noisy quantum circuits via locally entanglement-optimal unravelings (Lennart Bittel).

67. Quantum Simulations of Chemical Reactions: Achieving Accuracy with NISQ Devices (Maitreyee Sarkar).

68. Persistent Homology and Quantum Kernels for Image Texture Analysis (Maneesha K K).

69. Qudit Topological Subsystem Color Codes (Manoj Gowda).

70. A comparative study on encoding rule specificity in quantum dialogue protocols (Meera Ramachandran).

71. Quantum Walks on Simplicial Complexes and Harmonic Homology: Application to Topological Data Analysis with Superpolynomial Speedups (Min-Hsiu Hsieh).

72. Computational Complexity of Learning Efficiently Generatable Pure States (Min-Hsiu Hsieh,

Taiga Hirooka).

73. Develop a Novel Quantum Cryptographic Algorithm Resistant to Quantum Attacks (Minakshi Soni).

74. Hybrid classical-quantum image processing via polar Walsh basis functions (Mohit Rohida).

75. Finite and Asymptotic Key Analysis for CubeSat-Based BB84 QKD with Elliptical Beam Approximation (Muskan).

76. Bidirectional quantum teleportation using quantum walks (N C Randeep).

77. Adversarial Learning of the Quantum Autoencoder Latent Space for Quantum Data Generation (Naipunnya Raj, Rajiv Sangle, Avinash Singh, Krishnakumar Sabapathy).

78. Fidelity-Based Conclusive Quantum Secret Sharing in Noisy Environments (Nancy).

79. A Tokenized Signature Scheme Construction in the Linear Optical Quantum Computing Setting (Natarajan Venkatachalam, M. Prem Laxman Das).

80. A Tokenized Signature Scheme Construction in the Linear Optical Quantum Computing Setting (Natarajan Venkatachalam, M. Prem Laxman Das).

81. Quantum Shield :Revolutionizing Text and Image Data encryption with one time pad scheme (Nagesh N)

82. A Quantum Bagging Framework with QRAM-Based Subsampling and Shallow Quantum Clustering (Neeshu Rathi).

83. Efficient explicit gate construction of block-encoding for Hamiltonians needed for simulating partial differential equations (Nikita Guseynov, Xiajie Huang).

84. Contextuality sans incompatibility in the simplest scenario: Communication supremacy of a qubit (Partha Patra).

85. Enhancing the Harrow-Hassidim-Lloyd (HHL) algorithm in systems with large condition numbers (Peniel Bertrand Tsemo).

86. Exact Feasibility of NPA Hierarchy for Quantum Isomorphism in Polynomial Time (Peter Zeman, Prem Nigam Kar).

87. Harnessing Causal Indefiniteness for Accessing Locally Inaccessible Data (Pratik Ghosal, Ananya Chakraborty).

88. Antidistinguishability of Pauli Operators (Pratik Ghosal, Debanjan Roy).

89. Sequential Attack Impairs Security in Device-independent Quantum Key Distribution (Pritam Roy).

90. Boosting Coherence-Based Protocols with Correlated Catalysts (Priyabrata Char).

91. Enhancing variational quantum algorithms by balancing training on classical and quantum hardware (Rahul Bhowmick, Harsh Wadhwa, Avinash Singh, Krishnakumar Sabapathy, Tania Sidana).

92. Evaluating Binary and Integer Linear Programming Models for Fleet Assignment Problems in Airline Operations: A Comparative Study of Classical and Quantum Annealing Based Solvers (Rahul Rana, Kuntal Adak).

93. Grid-Partitioned MWIS Solving with Neutral Atom Quantum Computing for QUBO Problems (Rahul Rana, Suman Kumar Roy).

94. Progressive Graph Fragmentation for Efficient Solving of Large QUBO Instances (Rahul Rana, Suman Kumar Roy, Ankit Khandelwal).

95. Self-testing of multiple unsharpness parameters through sequential violations of non-contextual inequality (Rajdeep Paul).

96. QSETH strikes again: finer quantum lower bounds for lattice problem, strong simulation, hitting set problem, and more (Rajendra Kumar).

97. Fine-Grained Complexity via Quantum Natural Proofs (Rajendra Kumar).

98. Lattice Based Crypto breaks in a Superposition of Spacetimes (Rajendra Kumar, Shashwat Agrawal).

99. Dynamics of Majorana Zero Modes in a Hybrid Kitaev Chain (Rajiv Kumar).

100. Quantum Advantage in Distributed Sensing with Noisy Quantum Networks (Rajkumar Kettimuthu).

101. Self-testing of Nonmaximal Genuine Entangled States using Tripartite Hardy Relations (Ranendu Adhikary).

102. Quantum encoder for fixed Hamming-weight subspaces (Renato M S Farias, Thiago O. Maciel).

103. Random pure states are not useful in quantum metrology with many-body locally diagonalizable Hamiltonians (Rina Miyajima).

104. Robust Self-testing of m-partite GHZ state and measurements (Ritesh Singh).

105. Shadow Hamiltonian simulation (Rolando Somma, Robin Kothari).

106. PDQMA = DQMA = NEXP: QMA With Hidden Variables and Non-collapsing Measurements (Ronak Ramachandran).

107. Faster training of variational Quantum Boltzmann Machines using collective optimization

(Ruchira V Bhat).

108. No-go theorem in phase estimation with unbalanced interferometer – An approach based on optical coherence functions (S. Ajay).

109. Minimal no-go theorems for maximally psi-epistemic models (Sagnik Ray, Debashis Saha).

110. Detecting genuine multipartite entanglement using moments of positive maps (Saheli Mukherjee, Sahil Gopalkrishna Naik, Bivas Mallick).

111. No-Go Theorem for Generic Simulation of Qubit Channels with Finite Classical Resources (Sahil Gopalkrishna Naik).

112. Certified algorithms for quantum Hamiltonian learning via energy-entropy inequalities (Samuel Scalet).

113. Quantum steganography with degenerate entanglement-assisted quantum codes (Sanjoy Dutta).

114. Vertex congestion bounds via Laplacian eigenvalues and their application to tensor networks with arbitrary geometry (Sayan Mukherjee).

115. Single-qubit quantum gate at an arbitrary speed (Seongjin Ahn).

116. Unstructured Adiabatic Quantum Optimization: Optimality with Limitations (Shantanav Chakraborty).

117. Quantum GAN : Bridging Quantum Computing and Generative Modeling (Shashanka Shekhar Sharma, Ritisha Katiyar).

118. Effective Distance of Higher Dimensional HGPs and Weight-Reduced Quantum LDPC Codes (Shi Jie Samuel Tan).

119. Lightweight Estimation of Layout Noise in a Quantum Computer using Quality Indicator Circuits (Shikhar Srivastava).

120. Black-Box Separation Between Pseudorandom Unitaries and Pseudorandom Function-Like States (Shogo Yamada).

121. Multi-mode correlated attacks for Continuous Variable Quantum Key Distribution in Multiple-Input Multiple-Output Settings (Shradhanjali Sahu).

122. Noiseless subspace and Markovian revival of genuine multipartite entanglement under collective decoherence (Shubhodeep Gangopadhyay).

123. Effect of lattice boundary on Anderson localization of nonclassical light in optical waveguide arrays (Shubradeep Majumder).

124. How to compute the volume in low dimension? (Simon Apers).

125. Quantum property testing in sparse directed graphs (Simon Apers).

126. Single-shot distinguishability and antidistinguishability of quantum measurements (Sneha Suresh, Debashis Saha, Satyaki Manna).

127. Ergodiscord: An Operational and Distinct Notion of Quantumness of Correlations (Snehasish Roy Chowdhury).

128. Local Inaccessibility of Random Classical Information and Their Implications in the Change Point Problem (Snehasish Roy Chowdhury).

129. On the performance of underparametrized Quantum Approximate Optimization Algorithm (Soumik Adhikary).

130. Online Learning of Pure States is as Hard as Mixed States (Soumik Adhikary).

131. IQP computations with intermediate measurements (Soumik Ghosh).

132. Online learning of a panoply of quantum objects (Soumik Ghosh, Akshay Bansal).

133. Characterizing the set of Classical Correlations and Quantum Advantage under (Anti-)Distinguishability constraints in Multipartite Communication (Soumyabrata Hazra, Debashis Saha, Satyaki Manna, Ankush Pandit).

134. Majority agreed key distribution using absolutely maximally entangled states (Sowrabh Sudevan).

135. Majority-Agreed Key Distribution using Absolutely Maximally Entangled Stabilizer States (Sowrabh Sudevan).

136. Local surrogates for quantum machine learning models using window functions (Sreeraj Rajindran Nair).

137. Strong Inequivalence of Quantum Nonlocal Resources (Subhendu Bikash Ghosh, Snehasish Roy Chowdhury).

138. Local Yet Resourceful: Activating Hidden Nonlocality from Local Sets (Subrata Bera, Indranil Biswas).

139. SYK model based regime dependent two-qubit dynamical wormhole-inspired teleportation protocol simulation (Sudhanva Joshi).

140. Efficient detection of nonclassicality using moments of the Wigner moments (Sudip Chakrabarty, Saheli Mukherjee, Bivas Mallick).

141. Shadows of quantum error correction: Learning and interpretation (Sumeet Khatri, Lennart

Bittel).

142. Samllest quantum codes for amplitude-damping noise (Sourav Dutta)

143. All multiparty quantum systems have state with unconditionally superposition-robust entanglement (Swati Choudhary).

144. Experimental reconstruction of 3-qubit W-state using ibm_osaka and its visualization in terms of canonical ellispoids inscribed within the Bloch sphere (Talath Humera).

145. Quantum channels and some absolute properties of quantum states (Tapaswini Patro).

146. Partition function estimation with a quantum coin toss (Thais Lima Silva).

147. Coherence manipulation in asymmetry and thermodynamics (Tulja Varun Kondra).

148. Interplay of resources for universal continuous-variable quantum computing (Varun Upreti).

149. An efficient quantum state verification framework and its application to bosonic systems (Varun Upreti).

150. Re-engineering Quantum Walk Teleportation: 1D, 2D and 3D Lattices (Vivek P, N C Randeep).

151. Conditional entropy and information of quantum processes (Vivek Pandey).

152. A Robust Quantum Image Encryption Framework using a Simple Memristive Hopfield Neural Network based on Mixed Piecewise Linear Activation Functions and Quantum Block-Based Unitary Operations (Vivek Verma).

153. Bayesian Optimization for Quantum Error Correction Code Discovery (Yihua Chengyu, Roberto Bondesan).

154. Symmetric channel verification for purifying noisy quantum channels (Yosuke Mitsuhashi).

155. Non-Haar random circuits form unitary designs as fast as Haar random circuits (Yosuke Mitsuhashi, Toshihiro Yada).