

Tuesday, 10 November 2026

Program

Université de Montréal · Campus MIL · Talks primarily in English.

From 09:00 — **Welcome and coffee**
Atrium · Wing B · Ground floor

MORNING · WING A, 3RD FLOOR · A-3502.1

10:00 — **Opening remarks**

10:15 — **Conversation with Gilles Brassard**
David Deutsch, Nicolas Gisin and Sandu Popescu **(joining online)**
Moderator: Samuel Kuypers

11:15 — **Christopher A. Fuchs**
The Quantum Foundations Octopus

12:00 to 13:00 — **Lunch**
Atrium · Wing B · Ground floor

AFTER LUNCH · WING A, 5TH FLOOR · A-5502.1

13:00 — **Harry Buhrman**
Compl(i+e)menting Gilles: Quantum Advantage, One Instance at a Time

13:45 — **Anne Broadbent**
Proofs, Knowledge and the Art of Convincing Gilles

14:30 — **Xavier Coiteux-Roy**
Quantum, Creativity and Precision

15:00 to 15:30 — **Coffee break**
Foyer outside A-5502.1 · Wing A · 5th floor

15:30 — **Charles H. Bennett**
How Ideas from Physics Have Enriched Theoretical Computer Science Theory and What It Has Given Back
CRM public lecture · until 16:30

16:30 — **Light bites courtesy of the CRM**
Foyer outside A-5502.1 · until 17:30

17:30 — **De la science à la magie**
Public event in French · Atrium, Wing B, ground floor
Welcome at 17:30 · lecture from 18:00 to 19:30
Separate registration on Le Point de Vente

Lunch not included. Boxed lunches for participants with meal reservations and hosted guests.

Assistance and accessibility: welcome team.

1375, avenue Thérèse-Lavoie-Roux, Montréal

Maps: Campus MIL · Atrium · A-3502.1

CENTRE DE RECHERCHES MATHÉMATIQUES

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Université de Montréal et du monde.



Wednesday, 11 November 2026

Program

Université de Montréal · Campus MIL · Talks primarily in English.

From 09:00 — **Welcome and coffee**
Atrium · Wing B · Ground floor

MORNING · ATRIUM · WING B, GROUND FLOOR

10:00 — **Norbert Lütkenhaus**
Implementation and Protocol Security of Quantum Key Distribution

10:45 — **Connaissez-vous bien Gilles? / How well do you know Gilles?**
A quiz hosted by Louis Salvail

11:15 — **Claude Crépeau**
In Search of Gilles's Least "Successful" "Serious" Paper.

12:00 to 13:00 — **Lunch**
Atrium · Wing B · Ground floor

AFTER LUNCH · WING A, 3RD FLOOR · A-3502.1

13:00 — **Daniel R. Simon**
A Polynomial-Time Quantum Algorithm for the Dihedral Coset Problem

13:45 — **Jian-Wei Pan**
Prerecorded video message · until 14:00

14:00 — **Tal Mor**
Benchmarking Various Quantum Computers via Protocols

14:45 — **Charles Alexandre Bédard**
Teleportation, Two Bits, Gravity

15:15 to 16:00 — **Coffee break**
Foyer outside A-3502.1 · Wing A · 3rd floor

16:00 — **Gilles Brassard and Yoshua Bengio**
Dialogue entre deux lauréats du prix Turing : penser l'informatique de demain
In French · Moderator: Frédéric Bouchard · until 17:30

17:30 — **Closing remarks and acknowledgements**
A-3502.1 · until 17:45

17:45 — **Closing reception**
Atrium · Wing B · Ground floor · until 19:30

Lunch not included. Boxed lunches for participants with meal reservations and hosted guests.

Assistance and accessibility: welcome team.

1375, avenue Thérèse-Lavoie-Roux, Montréal

Maps: Campus MIL · Atrium · A-3502.1

CENTRE DE RECHERCHES MATHÉMATIQUES

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Université de Montréal
et du monde.

Gilles Brassard, David Deutsch, Nicolas Gisin and Sandu Popescu

Conversation with Gilles Brassard

Moderator: Samuel Kuypers

Description

Opening conversation with Gilles Brassard, David Deutsch, Nicolas Gisin and Sandu Popescu, moderated by Samuel Kuypers. David Deutsch, Nicolas Gisin and Sandu Popescu participate remotely.

Samuel Kuypers is a researcher at the Conjecture Institute, where he studies the foundations of quantum theory. He was a postdoctoral researcher with Gilles Brassard at the Université de Montréal in 2024–2025. Like Gilles, Samuel explores local formulations of quantum mechanics.

David Deutsch is a visiting professor of physics at the University of Oxford. In the 1980s, he and Gilles Brassard were among a handful of researchers exploring what quantum physics could make possible in computation and communication. Both have also argued for locality in quantum physics. With Patrick Hayden, David illustrated this idea by showing how information travels through local interactions in the teleportation protocol devised by Gilles and his colleagues. David and Gilles shared the 2023 Breakthrough Prize in Fundamental Physics with Charles H. Bennett and Peter Shor for their foundational work in quantum information.

Nicolas Gisin is a professor of quantum information and communication at Constructor University in Bremen and professor emeritus at the University of Geneva. His friendship with Gilles Brassard began at a workshop in Dagstuhl in 1993, where Nicolas explained how quantum key establishment could work over ordinary optical fibre. Over the years, the two friends have debated what happens in a quantum measurement and whether the digits of a physical quantity are all fixed in advance.

Sandu Popescu is a professor of physics at the University of Bristol, where he studies quantum entanglement and nonlocality. In 1994, he introduced nonsignalling resources, a notion central to Gilles's most recent work. In 1996, Sandu, Gilles Brassard and their colleagues showed how to distil a smaller number of nearly perfect entangled pairs from a supply of noisy ones and use them for teleportation. On 4 July 1997, Sandu took part in the first quantum teleportation experiment, carried out in Rome using an optical scheme he had devised.

← Back to the program

Christopher A. Fuchs

The Quantum Foundations Octopus

Abstract

If I write an abstract—with the lone exception of “If I write an abstract, Gilles won’t enjoy the talk as much.”—Gilles won’t enjoy the talk as much.

Christopher A. Fuchs is Distinguished Professor of Physics at the University of Massachusetts Boston. He was a postdoctoral researcher with Gilles Brassard in 1996. They subsequently coorganized three meetings on quantum foundations at the Centre de recherches mathématiques, in 2000, 2002 and 2011.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d’informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal et du monde.

Harry Buhrman

Compl(i+e)menting Gilles: Quantum Advantage, One Instance at a Time

Abstract

Quantum algorithms can outperform classical algorithms—but where, exactly, does the advantage lie? Can we identify individual instances that are easy for a quantum computer yet difficult for a classical one?

In celebration of Gilles Brassard, I will explore this question through *queasy instances*. Kolmogorov complexity provides a way to ask how much instance-specific information an algorithm needs, revealing a perspective on quantum advantage beyond the usual comparison of running times. The requirement that an algorithm remain correct on other instances makes this a surprisingly subtle question: knowing the answer and knowing how to answer are different things.

The talk connects these ideas to the interplay between information and computation that runs through Gilles's work—with a little complementing, plenty of complimenting, and a special role for Charlie Bennett.

Harry Buhrman is Chief Scientist for Algorithms and Innovation at Quantinuum. His connection with Gilles Brassard began with a 1992 lecture that sparked his interest in quantum computing. They later collaborated on nonlocality and communication complexity, and Buhrman moderated the 2022 Amsterdam symposium honouring Brassard and Charles H. Bennett.

← Back to the program

Anne Broadbent

Proofs, Knowledge and the Art of Convincing Gilles

Abstract

What would it take to convince Gilles Brassard that something is true? A proof, presumably. But what kind? A mathematical proof? A proof that you know something? A proof that you really did something? And can we convince Gilles, without him learning anything whatsoever about the claimed proof?

In this talk, I'll explore a few increasingly quantum notions of proofs, culminating in quantum proofs of knowledge, where we ask not only whether a prover can convince us, but what they must actually possess in order to do so. Along the way, we'll encounter cryptography, nonlocal games, quantum computation, and the rather delicate question of what, ultimately, we are willing to believe.

Anne Broadbent is a Full Professor in the Department of Mathematics and Statistics and Tier 1 Canada Research Chair (CRC) in Quantum Communications and Cryptography at the University of Ottawa. Her scientific ties to Gilles Brassard grew through her master's and doctoral research, jointly supervised by Gilles and Alain Tapp (M.Sc. 2004; Ph.D. 2008), on quantum pseudotelepathy, nonlocality, cryptography and complexity.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Xavier Coiteux-Roy

Quantum, Creativity and Precision

Abstract

Can quantum computing and communication make networks of computers faster? Until recently, the only technique to find quantum lower bounds in distributed computing was based on physical causality — information can only act locally. In this talk, we will look at the round complexity of a simple problem that evades this approach: Can quantum computers arranged in a loop, starting from identical states and running identical programs, produce outputs that are not all the same, with probability one?

Xavier Coiteux-Roy is an Assistant Professor in Computer Science and in Physics and Astronomy at the University of Calgary. His connection with Gilles Brassard grew out of his master's research on quantum teleportation (M.Sc. 2016), which Gilles supervised. Their collaboration continues through work on multipartite entanglement, quantum pseudotelepathy and a re-examination of Turing's foundational paper.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Charles H. Bennett

How Ideas from Physics Have Enriched Theoretical Computer Science Theory and What It Has Given Back

Abstract

The information revolution got started in the mid 20th century when Turing, Shannon, and von Neumann boldly reconceptualized the processing of information as independent from its physical embodiment. In subsequent decades, informatics matured by adopting ideas from thermodynamics and quantum mechanics that physicists had mistakenly thought belonged solely to their field. Aside from its practical applications, this enlarged theory has a beauty accessible to nonspecialists and potential implications as far afield as cosmology and ethics.

Charles H. Bennett is an IBM Fellow at IBM Research in Yorktown Heights. From their first meeting in 1979 to their shared 2025 ACM A.M. Turing Award, his scientific life has been entangled with Gilles Brassard's. Together, they helped create quantum information science, with more than twenty joint publications spanning quantum cryptography, privacy amplification and teleportation, including BB84 (1984) and the landmark teleportation paper (1993).

← Back to the program

Norbert Lütkenhaus

Implementation and Protocol Security of Quantum Key Distribution

Abstract

Quantum Key Distribution (QKD) is maturing toward commercial applications. One of the hurdles is ensuring that deployed QKD devices meet their promised security guarantees. In cryptography, the standardization of protocols and the certification of devices provide such assurance. In this contribution we will review the important concept and approaches in security proofs, emphasize some common gaps and misconceptions, and show what questions do we currently address.

When investigating the security of deployed QKD devices, it is important to distinguish between protocol security and implementation security. Protocol security is effectively a mathematical theorem that establishes the security of a fully specified protocol under a set of model assumptions about the physical devices. As we know from science, there is always a gap between models and reality. The question is how large this gap is and how it affects the statements derived from the model. This is the subject of implementation security in QKD.

We will clarify what the security statement for a QKD implementation entails. We will also examine device imperfections that influence QKD performance and may affect the validity of security proofs.

Norbert Lütkenhaus is Professor of Physics and Astronomy and Executive Director of the Institute for Quantum Computing at the University of Waterloo. With Gilles Brassard, Tal Mor and Barry Sanders, he studied the security of practical quantum cryptography in a 2000 paper. His collaborations with Brassard also include work on deniability in quantum key establishment.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Louis Salvail

Connaissez-vous bien Gilles? / How well do you know Gilles?

Description

A quiz hosted by Louis Salvail.

Louis Salvail is a Professor of Computer Science at Université de Montréal. Gilles Brassard is both his former supervisor and his departmental colleague: Louis worked with him for his master's degree (1991) and, jointly with Claude Crépeau, for his PhD (1997). Their long-standing collaboration produced publications on experimental quantum cryptography, the Cascade key-reconciliation protocol and classical key establishment secure against quantum attacks in the random-oracle model.

← Back to the program

Claude Crépeau

In Search of Gilles's Least "Successful" "Serious" Paper.

Abstract

This talk will explore one inglorious paper of Gilles. How does one define "successful" and "serious"? I cannot tell you all about it yet, you must see the presentation... But if you try to find out, just be aware that a very similar talk was presented six months ago for his co-author...

Claude Crépeau is a Professor at École de technologie supérieure. Gilles Brassard was his master's supervisor (M.Sc. 1986); their collaboration has since grown to encompass around twenty joint publications in classical and quantum cryptography, including the 1993 paper introducing quantum teleportation.

← Back to the program

Daniel R. Simon

A Polynomial-Time Quantum Algorithm for the Dihedral Coset Problem

Abstract

We present a polynomial-time quantum algorithm for the Dihedral Coset Problem (DCP). The algorithm is based on Regev's polynomial-time reduction of the Dihedral Subgroup Problem (DSP) to the modular subset sum problem, but uses a different technique to erase sample bits without use of a subset sum oracle. The algorithm can thus combine with Regev's reduction of lattice problems to DCP, improved by Brakerski, Kirshanova, Stehlé and Wen, to yield polynomial-time quantum algorithms for various lattice problems, such as finding a polynomial-factor approximation to the shortest vector in an n-dimensional lattice (SVP), and the "learning with errors" problem (LWE). The algorithm can tolerate a faulty sample rate as high as $1/O(\log n)$, allowing the algorithm-reduction combination to efficiently solve, for example, SVP with a $\sqrt{n}$ polylog(n) approximation factor, or LWE instances with $\alpha = \sqrt{n}$ polylog(n).

Daniel R. Simon is a Principal Security Engineer in the AWS Cryptography group at Amazon Web Services. He was a postdoctoral researcher with Gilles Brassard at Université de Montréal from 1992 to 1994. It was during this period that he developed Simon's algorithm, an early demonstration of an exponential quantum speedup, whose discovery was the trigger that enabled Peter Shor to discover his celebrated quantum algorithm for factoring large integers and jeopardising all the cryptography used to supposedly secure the Internet.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Jian-Wei Pan

Prerecorded video message

Description

A message to Gilles Brassard recorded by Jian-Wei Pan for the symposium.

Jian-Wei Pan is a professor of physics at the University of Science and Technology of China in Hefei. In 1997, he took part in one of the earliest quantum teleportation experiments, carried out in Innsbruck four years after Gilles Brassard and his colleagues published the protocol. Jian-Wei went on to spearhead China's effort to build a national quantum cryptography network. Under his leadership, his team developed *Micius*, the world's first quantum communication satellite, and integrated it into China's terrestrial quantum cryptography network. That network now spans more than 10,000 kilometres of optical fibre. Jian-Wei is also a guest editor of the special issue of *Entropy* honouring Gilles on his 70th birthday.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Tal Mor

Benchmarking Various Quantum Computers via Protocols

Abstract

Measuring the underlying "quantumness" of quantum chips and subchips is essential for assessing their potential readiness for practical applications and for guiding future progress and research. In a series of papers, we utilized a "benchmarking via protocols" strategy applicable for comparing various architectures by measuring the existence of "quantumness" directly, on whole chips and on their optimal sub-chips.

Distinct from existing metrics, our approach employs rigorous binary fidelity thresholds on "classicality" versus "quantumness". These are derived from well known limits on LOCC - local operations and classical communication, inspired by older work on teleportation and entanglement swapping.

Both superconducting and ion-trap quantum architectures are leaders in the current landscape of the quantum computing field, each with distinct characteristics and operational constraints. We applied our quality assurance strategy to test hardware platforms from both technologies, focusing on IBM and AQT chips.

This comparison via a protocol-based evaluation of quantumness advantage not only reveals the strengths and weaknesses of each tested chip and its sub-chips, but also offers a common language for their assessment. We believe that the field still lacks a fair performance strategy, and that our method provides a more balanced comparison.

An additional point we would like to emphasize is that most companies do not provide fair pricing for small research teams, or independent qubit availability. We would like to encourage more hardware companies to follow AQT and IBM's suit and create the conditions which allow researchers to perform such assessments.

Finally, I will also discuss an important future goal, namely employing our "benchmarking via protocols" also for connected-chips, and for fault-tolerant quantum computers, to enable the comparison of superconducting, ion trap, and neutral atoms architectures for logical qubits.

Tal Mor is a professor of computer science whose research spans quantum information, cryptography and computation. He was a postdoctoral researcher with Gilles Brassard in 1997–1998 and returned as a visiting professor in 2008–2009. They coauthored around a dozen papers on quantum cryptography, entanglement and teleportation. He also organized QUBIT 2003, marking ten years of teleportation, and co-chaired QUBIT 2018, celebrating the Wolf Prize in Physics shared by Gilles Brassard and Charles H. Bennett. He initiated special issues of Theoretical Computer Science and Natural Computing marking thirty years of BB84, as well as an Entropy special issue marking twenty-five years of teleportation. The Theoretical Computer Science issue republishes the original BB84 paper.

← Back to the program

Charles Alexandre Bédard

Teleportation, Two Bits, Gravity

Abstract

In 1993, Gilles and his collaborators showed that shared entanglement and a two-bit classical message suffice to *teleport* an arbitrary qubit state. Yet Alice's Bell outcome is uniformly random and reveals nothing about the input state, while Bob recovers that state exactly. How can this work? At the turn of the millennium, Deutsch and Hayden gave a local answer: in their Heisenberg-picture account, the underlying quantum systems carrying the two-bit message also transmit the input-state dependence. That account exposes a sharp distinction between effective classicality—emerging through the decoherence of fundamentally quantum carriers—and fundamental classicality, if the latter exists at all. What, then, might those two bits tell us about gravity? In joint work with Simone Rijavec and Maria Violaris, we formulate the principle of locally mediated information and prove that, together with no-cloning, it forbids perfect teleportation through a fundamentally classical channel. We therefore propose using gravity to transmit the two bits: under local mediation, successful teleportation would show that the gravitational channel is not fundamentally classical, without requiring coherent control of the source masses.

Charles Alexandre Bédard is a postdoctoral researcher at École de technologie supérieure and Principal Scientific Coordinator of the Institut Gilles Brassard for Fundamental Quantum Informatics. Gilles Brassard guided his doctoral research (Ph.D. 2020), and their joint work connects quantum foundations with algorithmic information theory. Gilles's steadfast defence of locality continues to shape Charles's own research.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal
et du monde.

Gilles Brassard and Yoshua Bengio

Dialogue entre deux lauréats du prix Turing : penser l'informatique de demain

In French · Moderator: Frédéric Bouchard

Description

Yoshua Bengio and Gilles Brassard, both A.M. Turing Award laureates, come together for a conversation about the future of computing and its implications for our societies.

Artificial intelligence is now at the heart of a global debate. It is reshaping the balance of power between nations and raising questions of governance, security and collective responsibility. At the same time, quantum computing promises profound transformations, particularly in the security of communications and the very foundations of computation.

Against today's geopolitical backdrop, these two pioneers will exchange perspectives on present issues and future challenges. This scientific dialogue, also open to philosophical reflection, will address a shared question: what kind of computing do we want to build, at what cost, and in whose service?

Yoshua Bengio is a Professor of Computer Science at Université de Montréal and Co-President and Scientific Director of LawZero. On 12 January 2023, he and his departmental colleague Gilles Brassard opened Mila and Québec Quantique's event on the intersection of AI and quantum with a joint discussion.

Frédéric Bouchard is Dean of the Faculty of Arts and Sciences and Professor of Philosophy at Université de Montréal. He chairs the governing board of the Institut Gilles Brassard for Fundamental Quantum Informatics, established in 2026, where Gilles serves as Scientific Director.

← Back to the program

CENTRE DE RECHERCHES MATHÉMATIQUES
Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences
Université de Montréal et du monde.