


# Mardi 10 novembre 2026

## Programme

Université de Montréal · Campus MIL · Conférences principalement en anglais.

**Dès 9 h** — **Accueil et café**
Atrium · aile B · rez-de-chaussée

### MATIN · AILE A, 3e ÉTAGE · A-3502.1

**10 h** — **Ouverture du symposium**

**10 h 15** — **Conversation avec Gilles Brassard**
David Deutsch, Nicolas Gisin et Sandu Popescu **(en ligne)**
Animation : Samuel Kuypers

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

**12 h** à 13 h — **Dîner**
Atrium · aile B · rez-de-chaussée

### APRÈS LE DÎNER · AILE A, 5e ÉTAGE · A-5502.1

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

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

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

**15 h** à 15 h 30 — **Pause café**
Foyer de A-5502.1 · aile A · 5e étage

**15 h 30** — **Charles H. Bennett**
*How Ideas from Physics Have Enriched Theoretical Computer Science Theory and What It Has Given Back*
Conférence publique du CRM · jusqu'à 16 h 30

**16 h 30** — **Bouchées offertes par le CRM**
Foyer de A-5502.1 · jusqu'à 17 h 30

**17 h 30** — **De la science à la magie**
Événement public en français · Atrium, aile B, rez-de-chaussée
Accueil à 17 h 30 · conférence de 18 h à 19 h 30
Inscription distincte sur Le Point de Vente

---

**Dîner non inclus.** Boîtes à lunch pour les personnes ayant réservé un repas et les invités pris en charge.

**Aide et accessibilité :** équipe d'accueil.

1375, avenue Thérèse-Lavoie-Roux, Montréal

Plans : 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.




# Mercredi 11 novembre 2026

## Programme

Université de Montréal · Campus MIL · Conférences principalement en anglais.

**Dès 9 h** — **Accueil et café**
Atrium · aile B · rez-de-chaussée

### MATIN · ATRIUM · AILE B, REZ-DE-CHAUSSÉE

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

**10 h 45** — **Connaissez-vous bien Gilles? / How well do you know Gilles?**
Un quiz animé par Louis Salvail

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

**12 h** à 13 h — **Dîner**
Atrium · aile B · rez-de-chaussée

### APRÈS LE DÎNER · AILE A, 3e ÉTAGE · A-3502.1

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

**13 h 45** — **Jian-Wei Pan**
Message vidéo préenregistré · jusqu'à 14 h

**14 h** — **Tal Mor**
*Benchmarking Various Quantum Computers via Protocols*

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

**15 h 15** à 16 h — **Pause café**
Foyer de A-3502.1 · aile A · 3e étage

**16 h** — **Gilles Brassard et Yoshua Bengio**
*Dialogue entre deux lauréats du prix Turing : penser l'informatique de demain*
En français · Animation : Frédéric Bouchard · jusqu'à 17 h 30

**17 h 30** — **Clôture et remerciements**
A-3502.1 · jusqu'à 17 h 45

**17 h 45** — **Cocktail de clôture**
Atrium · aile B · rez-de-chaussée · jusqu'à 19 h 30

**Dîner non inclus.** Boîtes à lunch pour les personnes ayant réservé un repas et les invités pris en charge.

**Aide et accessibilité :** équipe d'accueil.

1375, avenue Thérèse-Lavoie-Roux, Montréal

Plans : 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 et Sandu Popescu

## Conversation avec Gilles Brassard

*Modération : Samuel Kuypers*

**Présentation**

Conversation d'ouverture avec Gilles Brassard, David Deutsch, Nicolas Gisin et Sandu Popescu, animée par Samuel Kuypers. David Deutsch, Nicolas Gisin et Sandu Popescu participent à distance.

Samuel Kuypers est chercheur au Conjecture Institute, où il étudie les fondements de la théorie quantique. Il a effectué un stage postdoctoral auprès de Gilles Brassard à l'Université de Montréal en 2024–2025. Comme Gilles, Samuel explore les formulations locales de la mécanique quantique.

David Deutsch est professeur invité de physique à l'Université d'Oxford. Dans les années 1980, Gilles Brassard et lui comptaient parmi la poignée de chercheurs qui exploraient ce que la physique quantique rendait possible en matière de calcul et de communication. Tous deux défendent aussi la localité en physique quantique. Avec Patrick Hayden, David en a donné un exemple en montrant comment l'information se propage de proche en proche dans le protocole de téléportation de Gilles et de ses collègues. David et Gilles ont partagé avec Charles H. Bennett et Peter Shor le prix Breakthrough 2023 de physique fondamentale pour leurs travaux fondateurs en information quantique.

Nicolas Gisin est professeur d'information et de communication quantiques à l'Université Constructor, à Brême, et professeur honoraire à l'Université de Genève. Son amitié avec Gilles Brassard remonte à un atelier à Dagstuhl en 1993, où Nicolas lui a expliqué comment réaliser l'établissement quantique de clés sur des fibres optiques ordinaires. Au fil des ans, les deux amis en sont venus à débattre de ce qui se passe lors d'une mesure quantique et à se demander si les décimales d'une grandeur physique sont toutes déterminées d'avance.

Sandu Popescu est professeur de physique à l'Université de Bristol, où il étudie l'intrication et la non-localité quantiques. En 1994, il a introduit les ressources non-signalantes, ce qui est une notion centrale aux travaux récents de Gilles. En 1996, Sandu, Gilles Brassard et leurs collègues ont montré comment distiller l'intrication. À partir de nombreuses paires de particules imparfaitement intriquées, deux partenaires peuvent en extraire un plus petit nombre de paires presque parfaitement intriquées, puis s'en servir pour la téléportation. Le 4 juillet 1997, à Rome, Sandu a participé à la première expérience de téléportation quantique, réalisée grâce au dispositif optique qu'il avait conçu.

← Retour à l'horaire

# Christopher A. Fuchs

## The Quantum Foundations Octopus

**Résumé**

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 est professeur distingué de physique à l’Université du Massachusetts à Boston. Il a été stagiaire postdoctoral auprès de Gilles Brassard en 1996. Ils ont ensuite organisé ensemble trois rencontres sur les fondements de la physique quantique au Centre de recherches mathématiques, en 2000, 2002 et 2011.

← Retour à l’horaire



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

**Résumé**

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 est scientifique en chef pour les algorithmes et l'innovation chez Quantinuum. Son lien avec Gilles Brassard remonte à une conférence de 1992 qui a éveillé son intérêt pour l'informatique quantique. Ils ont ensuite collaboré sur la non-localité et la complexité de la communication, et Harry a animé le symposium organisé à Amsterdam en 2022 en l'honneur de Gilles et de Charles H. Bennett.

← Retour à l'horaire



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

# Anne Broadbent

## Proofs, Knowledge and the Art of Convincing Gilles

**Résumé**

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 est professeure titulaire au Département de mathématiques et de statistique de l'Université d'Ottawa et titulaire de la Chaire de recherche du Canada de niveau 1 en communications et cryptographie quantiques. Ses liens scientifiques avec Gilles Brassard se sont tissés au fil de ses recherches de maîtrise et de doctorat, codirigées par Gilles et Alain Tapp (M.Sc. 2004; Ph.D. 2008), sur la pseudotélépathie quantique, la non-localité, la cryptographie et la complexité.

← Retour à l'horaire



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

**Résumé**

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 est professeur adjoint en informatique ainsi qu'en physique et en astronomie à l'Université de Calgary. Son lien avec Gilles Brassard s'est noué pendant ses recherches de maîtrise sur la téléportation quantique (M.Sc. 2016), dirigées par Gilles. Leur collaboration se poursuit avec des travaux sur l'intrication multipartite, la pseudotélépathie quantique et une relecture de l'article fondateur de Turing.

← Retour à l'horaire



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

Résumé

The information revolution got started in the mid 20$^{th}$ 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 est chercheur à IBM Research, à Yorktown Heights. De leur première rencontre en 1979 au prix A.M. Turing 2025 de l'ACM qu'ils partagent, son parcours scientifique est intriqué à celui de Gilles Brassard. Ensemble, ils ont contribué à créer la science de l'information quantique, avec plus de vingt publications communes sur la cryptographie quantique, l'amplification de confidentialité et la téléportation, dont BB84 (1984) et l'article fondateur de la téléportation quantique (1993).

← Retour à l'horaire



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

# Norbert Lütkenhaus

## Implementation and Protocol Security of Quantum Key Distribution

**Résumé**

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 est professeur de physique et d'astronomie et directeur exécutif de l'Institut d'informatique quantique de l'Université de Waterloo. Avec Gilles Brassard, Tal Mor et Barry Sanders, il a étudié la sécurité de la cryptographie quantique en pratique dans un article paru en 2000. Ses collaborations avec Gilles comprennent également des travaux sur le déni plausible en établissement quantique de clés.

← Retour à l'horaire



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?

**Présentation**

Un quiz animé par Louis Salvail.

---

Louis Salvail est professeur d'informatique à l'Université de Montréal. Gilles Brassard est à la fois son ancien directeur de recherche et son collègue au département : il a dirigé les recherches de maîtrise de Louis (1991), puis codirigé son doctorat avec Claude Crépeau (1997). Leur longue collaboration a donné lieu à des publications sur la cryptographie quantique expérimentale, le protocole de réconciliation de clés Cascade et l'établissement classique de clés résistant aux attaques quantiques dans le modèle de l'oracle aléatoire.

← Retour à l'horaire



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

# Claude Crépeau

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

**Résumé**

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 est professeur à l'École de technologie supérieure. Gilles Brassard a dirigé ses recherches de maîtrise (M.Sc. 1986); leur collaboration s'est depuis enrichie d'une vingtaine de publications communes en cryptographie classique et quantique, dont l'article de 1993 qui a introduit la téléportation quantique.

← Retour à l'horaire



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

# Daniel R. Simon

## A Polynomial-Time Quantum Algorithm for the Dihedral Coset Problem

**Résumé**

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 est ingénieur principal en sécurité au sein du groupe AWS Cryptography d'Amazon Web Services. Il a été stagiaire postdoctoral auprès de Gilles Brassard à l'Université de Montréal de 1992 à 1994. C'est durant cette période qu'il a développé l'algorithme de Simon, l'une des premières démonstrations d'une accélération quantique exponentielle, dont la découverte a été l'élément déclencheur qui a permis à Peter Shor de découvrir son célèbre algorithme quantique pour factoriser les grands entiers et mettre en péril toute la cryptographie utilisée pour soi-disant sécuriser l'Internet.

← Retour à l'horaire



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

## Message vidéo préenregistré

**Présentation**

Message de Jian-Wei Pan à Gilles Brassard, enregistré pour le symposium.

Jian-Wei Pan est professeur de physique à l'Université des sciences et technologies de Chine, à Hefei. En 1997, à Innsbruck, il a participé à l'une des premières expériences de téléportation quantique, quatre ans après la publication du protocole par Gilles Brassard et ses collègues. Jian-Wei a ensuite été le fer de lance du déploiement de la cryptographie quantique en Chine. Sous sa direction, son équipe a développé *Micius*, le premier satellite de communication quantique au monde, puis l'a intégré au réseau terrestre chinois de cryptographie quantique. Ce réseau compte aujourd'hui plus de 10 000 kilomètres de fibre optique. Jian-Wei est aussi l'un des rédacteurs invités du numéro spécial de la revue *Entropy* consacré aux 70 ans de Gilles.

← Retour à l'horaire



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

**Résumé**

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 est professeur d'informatique et mène des recherches en information quantique, en cryptographie et en calcul quantique. Il a été stagiaire postdoctoral auprès de Gilles Brassard en 1997–1998, puis est revenu comme professeur invité en 2008–2009. Ils ont cosigné une bonne dizaine d'articles sur la cryptographie quantique, l'intrication et la téléportation. Tal a également organisé QUBIT 2003, qui marquait les dix ans de la téléportation, et coprésidé QUBIT 2018, qui célébrait le prix Wolf de physique partagé par Gilles Brassard et Charles H. Bennett. Il a été à l'origine de numéros spéciaux de Theoretical Computer Science et de Natural Computing pour les trente ans de BB84, ainsi que d'un numéro d'Entropy pour les vingt-cinq ans de la téléportation. Le numéro de Theoretical Computer Science republie l'article original de BB84.

← Retour à l'horaire

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

# Charles Alexandre Bédard

## Teleportation, Two Bits, Gravity

Résumé

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 est chercheur postdoctoral à l'École de technologie supérieure et coordonnateur scientifique principal de l'Institut Gilles Brassard pour l'informatique quantique fondamentale. Gilles Brassard a guidé ses recherches doctorales (Ph.D. 2020), et leurs travaux communs relient les fondements de la physique quantique à la théorie algorithmique de l'information. La défense résolue de la localité par Gilles continue de façonner les recherches de Charles.

← Retour à l'horaire



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 et Yoshua Bengio

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

*En français · Animation : Frédéric Bouchard*

**Présentation**

Yoshua Bengio et Gilles Brassard, tous deux lauréats du prix A.M. Turing, se réunissent pour un échange sur l'avenir de l'informatique et sur ses répercussions sur nos sociétés.

L'intelligence artificielle se trouve aujourd'hui au cœur d'une réflexion à l'échelle planétaire. Elle redéfinit les rapports de force entre les États et soulève des questions de gouvernance, de sécurité et de responsabilité collective. Parallèlement, l'informatique quantique annonce des transformations profondes, notamment pour la sécurité des communications et pour les fondements mêmes du calcul.

Dans le contexte géopolitique actuel, ces deux pionniers croiseront leurs regards sur les enjeux présents et les défis à venir. Ce dialogue scientifique, également ouvert à la réflexion philosophique, portera sur une question commune : quelle informatique voulons-nous bâtir, à quel prix et au service de qui?

---

Yoshua Bengio est professeur titulaire d'informatique à l'Université de Montréal et coprésident et directeur scientifique de LoiZéro. Il a échangé avec Gilles Brassard, son collègue de département, lors de la discussion d'ouverture de l'événement de Mila et Québec Quantique sur l'intersection de l'IA et du quantique, le 12 janvier 2023.

---

Frédéric Bouchard est doyen de la Faculté des arts et des sciences et professeur titulaire de philosophie à l'Université de Montréal. Il préside le conseil de gouvernance de l'Institut Gilles Brassard pour l'informatique quantique fondamentale, créé en 2026, dont Gilles assure la direction scientifique.

← Retour à l'horaire