

Frédéric Dupuis

www.iro.umontreal.ca/~dupuisf/

Renseignements personnels

- Naissance : 29.08.1983 à Sept-Îles, Québec
- Citoyenneté : Canada
- Langues parlées : français (langue maternelle), anglais (parlé couramment), allemand (intermédiaire)

Emplois académiques

Université de Montréal <i>Professeur adjoint, Département d'informatique et de recherche opérationnelle</i>	Montréal, Québec <i>août 2019—</i>
CNRS, affecté au LORIA, Université de Lorraine <i>Chargé de recherche, classe normale</i> (en détachement depuis août 2019)	Nancy, France <i>octobre 2017—</i>
Université Masaryk <i>Professeur adjoint, Faculté d'informatique</i>	Brno, République tchèque <i>janvier 2017—septembre 2017</i>
Université Masaryk <i>Chercheur scientifique, Faculté d'informatique</i> (Il s'agit d'un poste permanent)	Brno, République tchèque <i>septembre 2014—décembre 2016</i>
Université d'Aarhus <i>Chercheur postdoctoral, Département d'informatique</i> Chef du groupe recherche : Ivan Damgård	Aarhus, Danemark <i>janvier 2013—août 2014</i>
École polytechnique fédérale de Zürich (ETH Zürich) <i>Chercheur postdoctoral, Institut de physique théorique</i> Chefs du groupe de recherche : Renato Renner et Matthias Christandl	Zürich, Suisse <i>janvier 2010—décembre 2012</i>
Université de Toronto <i>Assistant de recherche, Département de génie électrique</i> Superviseur : Wei Yu	Toronto, Ontario <i>mai 2005—août 2005</i>
Université de Toronto <i>Assistant de recherche, Département de génie électrique</i> Superviseur : Wei Yu	Toronto, Ontario <i>mai 2004—août 2004</i>
Université de Toronto <i>Assistant de recherche, Département de génie électrique</i> Superviseur : Wei Yu	Toronto, Ontario <i>mai 2003—août 2003</i>

Formation

Université de Montréal <i>Doctorat en informatique</i> Titre de la thèse : <i>The decoupling approach to quantum information theory</i> Directeurs : Gilles Brassard et Patrick Hayden (Université McGill)	Montréal, Québec <i>sept 2005—déc 2009</i>
Université de Toronto <i>B.A.Sc, « Engineering Science », option Génie électrique</i> Titre du mémoire de quatrième année : <i>Optimizing the key generation rate in decoy state quantum cryptography</i> Superviseur du mémoire : Hoi-Kwong Lo	Toronto, Ontario <i>sept 2001—mai 2005</i>

Articles publiés dans des revues avec comité de lecture

- [1] Frédéric DUPUIS, Omar FAWZI et Renato RENNER. « Entropy accumulation ». In : *Communications in Mathematical Physics* (2020). DOI : 10.1007/s00220-020-03839-5. arXiv : 1607.01796.
- [2] Frédéric DUPUIS et Omar FAWZI. « Entropy accumulation with improved second-order term ». In : *IEEE Transactions on Information Theory* 65.11 (nov. 2019), p. 7596-7612. DOI : 10.1109/TIT.2019.2929564. arXiv : 1805.11652. HAL Id : 01925985.
- [3] Rotem ARNON-FRIEDMAN, Frédéric DUPUIS, Omar FAWZI, Renato RENNER et Thomas VIDICK. « Practical device-independent quantum cryptography via entropy accumulation ». In : *Nature Communications* 9.459 (1 2018). DOI : 10.1038/s41467-017-02307-4. HAL Id : 01992050.
- [4] Christian MAJENZ, Mario BERTA, Frédéric DUPUIS, Renato RENNER et Matthias CHRISTANDL. « Catalytic decoupling of quantum information ». In : *Phys. Rev. Lett.* 118 (fév. 2017), p. 080503. DOI : 10.1103/PhysRevLett.118.080503. arXiv : 1605.00514.
- [5] Frédéric DUPUIS et Mark M. WILDE. « Swiveled Rényi entropies ». In : *Quantum Information Processing* (2016), p. 1-37. DOI : 10.1007/s11128-015-1211-x. arXiv : 1506.00981.
- [6] Joseph M. RENES, David SUTTER, Frédéric DUPUIS et Renato RENNER. « Efficient quantum polar codes requiring no preshared entanglement ». In : *IEEE Transactions on Information Theory* 61.11 (nov. 2015), p. 6395-6414. DOI : 10.1109/TIT.2015.2468084. arXiv : 1307.1136.
- [7] Philippe FAIST, Frédéric DUPUIS, Jonathan OPPENHEIM et Renato RENNER. « The minimal work cost of information processing ». In : *Nature Communications* 7669 (juil. 2015). DOI : 10.1038/ncomms8669. arXiv : 1211.1037.
- [8] Frédéric DUPUIS, Omar FAWZI et Stephanie WEHNER. « Entanglement sampling and applications ». In : *IEEE Transactions on Information Theory* 61.2 (fév. 2015), p. 1093-1112. DOI : 10.1109/TIT.2014.2371464. arXiv : 1305.1316.
- [9] Frédéric DUPUIS. « Chain rules for quantum Rényi entropies ». In : *Journal of Mathematical Physics* 56.2, 022203 (2015). DOI : 10.1063/1.4907981. arXiv : 1410.5455.
- [10] Frédéric DUPUIS, Mario BERTA, Jürg WULLSCHLEGER et Renato RENNER. « One-shot decoupling ». In : *Communications in Mathematical Physics* 328.1 (2014), p. 251-284. DOI : 10.1007/s00220-014-1990-4. arXiv : 1012.6044.
- [11] Frédéric DUPUIS, Oleg SZEHR et Marco TOMAMICHEL. « A decoupling approach to classical data transmission over quantum channels ». In : *IEEE Transactions on Information Theory* 60.3 (mar. 2014), p. 1562-1572. DOI : 10.1109/TIT.2013.2295330. arXiv : 1207.0067.
- [12] Martin MÜLLER-LENNERT, Frédéric DUPUIS, Oleg SZEHR, Serge FEHR et Marco TOMAMICHEL. « On quantum Rényi entropies : a new generalization and some properties ». In : *Journal of Mathematical Physics* 54.12, 122203 (2013). DOI : 10.1063/1.4838856. arXiv : 1306.3142 [quant-ph].
- [13] Frédéric DUPUIS, Jan FLORJANCZYK, Patrick HAYDEN et Debbie LEUNG. « The locking-decoding frontier for generic dynamics ». In : *Proceedings of the Royal Society A* 469.2159 (2013). DOI : 10.1098/rspa.2013.0289. arXiv : 1011.1612.
- [14] Alexander VITANOV, Frédéric DUPUIS, Marco TOMAMICHEL et Renato RENNER. « Chain rules for smooth min- and max-entropies ». In : *IEEE Transactions on Information Theory* 59.5 (2013), p. 2603-2612. DOI : 10.1109/TIT.2013.2238656. arXiv : 1205.5231.
- [15] Oleg SZEHR, Frédéric DUPUIS, Marco TOMAMICHEL et Renato RENNER. « Decoupling with unitary approximate two-designs ». In : *New Journal of Physics* 15.5 (2013), p. 053022. DOI : 10.1088/1367-2630/15/5/053022. arXiv : 1109.4348.

- [16] Joseph M. RENES, Frédéric DUPUIS et Renato RENNER. « Efficient Polar Coding of Quantum Information ». In : *Physical Review Letters* 109 (5 août 2012), p. 050504. DOI : 10.1103/PhysRevLett.109.050504. arXiv : 1109.3195.
- [17] Simon Pierre DESROSIERS et Frédéric DUPUIS. « Quantum entropic security and approximate quantum encryption ». In : *IEEE Transactions on Information Theory* 56.7 (juil. 2010), p. 3455-3464. DOI : 10.1109/TIT.2010.2048488. arXiv : 0707.0691.
- [18] Frédéric DUPUIS, Patrick HAYDEN et Ke LI. « A father protocol for quantum broadcast channels ». In : *IEEE Transactions on Information Theory* 56.6 (juin 2010), p. 2946-2956. DOI : 10.1109/TIT.2010.2046217. arXiv : quant-ph/0612155.
- [19] Frédéric DUPUIS, Nicolas Gisin, Avinatan HASSIDIM, André Allan MÉTHOT et Haran PILPEL. « No nonlocal box is universal ». In : *Journal of Mathematical Physics* 48.8, 082107 (2007), p. 082107. DOI : 10.1063/1.2767538. arXiv : quant-ph/0701142.
- [20] Xiongfeng MA, Fred Chi-Hang FUNG, Frédéric DUPUIS, Kai CHEN, Kiyoshi TAMAKI et Hoi-Kwong LO. « Decoy-state quantum key distribution with two-way classical postprocessing ». In : *Physical Review A* 74 (3 sept. 2006), p. 032330. DOI : 10.1103/PhysRevA.74.032330. arXiv : quant-ph/0604094.

Exposés dans des conférences avec arbitrage et comptes rendus

- [1] Frédéric DUPUIS, Ashutosh GOSWAMI, Mehdi MHALLA et Valentin SAVIN. « Purely Quantum Polar Codes ». In : *Proceedings of IEEE Information Theory Workshop*. 2019, p. 1-5. arXiv : 1904.04713.
- [2] Frédéric DUPUIS, Serge FEHR, Philippe LAMONTAGNE et Louis SALVAIL. « Secure Certification of Mixed Quantum States With Application To Two-Party Randomness Generation ». In : *Proceedings of Theory of Cryptography Conference (TCC)*. 2018, p. 282-314. DOI : 10.1007/978-3-030-03810-6_11. arXiv : 1804.04730. HAL Id : 01926631.
- [3] Frédéric DUPUIS, Serge FEHR, Philippe LAMONTAGNE et Louis SALVAIL. « Adaptive versus non-adaptive strategies in the quantum setting with applications ». In : *Proceedings of CRYPTO 2016*. 2016, p. 33-59. DOI : 10.1007/978-3-662-53015-3_2. arXiv : 1607.08168.
- [4] Ivan DAMGÅRD, Frédéric DUPUIS et Jesper Buus NIELSEN. « On the orthogonal vector problem and the feasibility of unconditionally secure leakage-resilient computation ». In : *Proceedings of ICITS 2015 (International Conference on Information-Theoretic Security)*. Version complète : <http://eprint.iacr.org/2014/282>. 2015, p. 87-104. DOI : 10.1007/978-3-319-17470-9_6.
- [5] Frédéric DUPUIS, Omar FAWZI et Stephanie WEHNER. « Achieving the limits of the noisy-storage model using entanglement sampling ». In : *Proceedings of CRYPTO 2013*. 2013, p. 326-343. DOI : 10.1007/978-3-642-40084-1_19. Version conférence de : « Entanglement sampling and applications » dans la section revues.
- [6] David SUTTER, Joseph M. RENES, Frédéric DUPUIS et Renato RENNER. « Efficient quantum channel coding scheme requiring no preshared entanglement ». In : *Proceedings of the 2013 IEEE International Symposium on Information Theory*. Juil. 2013, p. 354-358. DOI : 10.1109/ISIT.2013.6620247. arXiv : 1307.1136.
- [7] Frédéric DUPUIS, Jesper Buus NIELSEN et Louis SALVAIL. « Actively Secure Two-Party Evaluation of Any Quantum Operation ». In : *Proceedings of CRYPTO 2012*. T. 7417. Version complète : eprint.iacr.org/2012/304. 2012, p. 794-811. DOI : 10.1007/978-3-642-32009-5_46.
- [8] Frédéric DUPUIS, Lea KRÄMER, Philippe FAIST, Joseph M. RENES et Renato RENNER. « Generalized entropies ». In : *Proceedings of the International Congress on Mathematical Physics*. World Scientific Publishing, août 2012. arXiv : 1211.3141.

- [9] David SUTTER, Joseph M. RENES, Frédéric DUPUIS et Renato RENNER. « Achieving the capacity of any DMC using only polar codes ». In : *Information Theory Workshop (ITW), 2012 IEEE*. Sept. 2012, p. 114-118. DOI : 10.1109/ITW.2012.6404638. arXiv : 1205.3756.
- [10] Frédéric DUPUIS, Jesper Buus NIELSEN et Louis SALVAIL. « Secure two-party quantum evaluation of unitaries against specious adversaries ». In : *Proceedings of CRYPTO 2010*. Springer, 2010, p. 685-706. DOI : 10.1007/978-3-642-14623-7_37.
- [11] Frédéric DUPUIS. « The capacity of quantum channels with side information at the transmitter ». In : *IEEE International Symposium on Information Theory*. Juin 2009, p. 948-952. DOI : 10.1109/ISIT.2009.5205591. arXiv : 0805.3352.
- [12] Frédéric DUPUIS, Wei YU et Frans M. J. WILLEMS. « Blahut-Arimoto algorithms for computing channel capacity and rate-distortion with side information ». In : *IEEE International Symposium on Information Theory*. Juin 2004, p. 179. DOI : 10.1109/ISIT.2004.1365218.

Exposés dans des conférences avec arbitrage sans comptes rendus

- [1] Frédéric DUPUIS, Ashutosh GOSWAMI, Mehdi MHALLA et Valentin SAVIN. *Purely quantum polar codes*. QIP 2020 (Quantum Information Processing), Shenzhen, Chine.
- [2] Frédéric DUPUIS, Serge FEHR, Philippe LAMONTAGNE et Louis SALVAIL. *Secure Certification of Mixed Quantum States With Application To Two-Party Randomness Generation*. Conférence CEQIP (Central European Quantum Information Processing) 2018, Smolenice, Slovaquie. Juin 2018.
- [3] Rotem ARNON-FRIEDMAN, Frédéric DUPUIS, Omar FAWZI, Renato RENNER et Thomas VIDICK. *Entropy accumulation in device-independent protocols*. QIP 2017 (Quantum Information Processing), Seattle, WA.
- [4] Christian MAJENZ, Mario BERTA, Frédéric DUPUIS, Renato RENNER et Matthias CHRISTANDL. *Catalytic decoupling of quantum information*. QIP 2017 (Quantum Information Processing), Seattle, WA.
- [5] Frédéric DUPUIS, Serge FEHR, Philippe LAMONTAGNE et Louis SALVAIL. *Adaptive versus non-adaptive strategies in the quantum setting with applications*. Conférence QCrypt 2016, Washington DC. 2016. arXiv : 1607.08168.
- [6] Ivan DAMGÅRD, Frédéric DUPUIS et Jesper Buus NIELSEN. *A quantum protocol for the orthogonal vector problem and leakage-resilient computation*. Conférence QCrypt 2014, Paris, France, septembre 2014.
- [7] Joseph M. RENES, David SUTTER, Frédéric DUPUIS et Renato RENNER. *Efficient secret key distillation over quantum channels*. Conférence QCrypt 2014, Paris, France, septembre 2014.
- [8] Frédéric DUPUIS, Omar FAWZI et Stephanie WEHNER. *Entanglement sampling and applications*. QIP 2014 (Quantum Information Processing), Barcelone, Espagne, février 2014.
- [9] Frédéric DUPUIS, Serge FEHR, Martin MÜLLER-LENNERT, Oleg SZEHR, Marco TOMAMICHEL, Mark WILDE, Andreas WINTER et Dong YANG. *A new quantum generalization of the Rényi divergence with applications to the strong converse in quantum channel coding*. QIP 2014 (Quantum Information Processing), Barcelone, Espagne, février 2014.
- [10] Frédéric DUPUIS, Omar FAWZI et Stephanie WEHNER. *Achieving the limits of the noisy-storage model using entanglement sampling*. Conférence QCrypt 2013, Waterloo, Ontario, août 2013.
- [11] Joseph M. RENES, Frédéric DUPUIS et Renato RENNER. *Quantum polar coding*. QIP 2012 (Quantum Information Processing), Montréal, Québec, décembre 2011.

- [12] Frédéric DUPUIS, Jan FLORJANCZYK, Patrick HAYDEN et Debbie LEUNG. *The locking-decoding frontier for generic dynamics*. 6th Conference on Theory of Quantum Computation, Communication and Cryptography, Madrid, Espagne, 24–26 mai 2011.
- [13] Simon Pierre DESROSIERS et Frédéric DUPUIS. *Quantum entropic security and approximate quantum encryption*. QIP 2008 (Quantum Information Processing), New Delhi, Inde, décembre 2007.

Exposés invités

Conférences et colloques

- *Device-independent quantum cryptography via entropy accumulation*, Conférencier invité, Central European Quantum Information Processing (CEQIP) Workshop, Smolenice, Slovaquie, 31 mai au 3 juin 2017.
- *Entropy accumulation*, Conférencier invité, Colloque « Beyond i.i.d. in information theory », Barcelone, Espagne, 18 au 22 juillet 2016.
- *Entropy accumulation*, Conférencier invité, « Workshop on Quantum Cryptography and Quantum Computation », Université d'Aarhus, Aarhus, Danemark, 19 au 22 octobre 2015.
- *Chain rules for quantum Rényi entropies*, Colloque « Beyond i.i.d. in information theory », Banff International Research Station, Banff, Canada, 5 au 10 juillet 2015.
- *Quantum error correction and polar codes*, Conférencier invité, Colloque « New Frontiers of Quantum Information Theory », Ascoli-Piceno, Italie, 7 au 11 juillet 2014.
- *Bounding the uncertainty of constrained adversaries*, Conférencier invité, Central European Quantum Information Processing (CEQIP) Workshop, Znojmo, République tchèque, 5 au 8 juin 2014.
- *On quantum Rényi entropies : a new definition and some properties*, Colloque « Beyond i.i.d. in information theory », Centre for Quantum Technologies, Université nationale de Singapour, Singapour, 19 au 21 mai 2014.
- *Bounding the uncertainty of constrained adversaries*, Rencontre de l'Institut transdisciplinaire d'information quantique (INTRIQ), Bromont, Québec, 6 et 7 mai 2014.
- *A new definition for the quantum conditional Rényi entropy*, Colloque « New Mathematical Directions for Quantum Information », Isaac Newton Institute for Mathematical Sciences, Cambridge, Royaume-Uni, 2 au 6 septembre 2013.
- *Quantum two-party computation*. Workshop on Cryptography, Bellairs Research Institute, Barbade, 3 au 7 mars 2013. (Mini-cours de 6 heures)
- *Classical coding via dequantizing*. Colloque « Beyond i.i.d. in information theory », Cambridge, Royaume-Uni, 8 au 11 janvier 2013.
- *Efficient quantum polar coding*, « Tsinghua-Aarhus CTIC Workshop on Quantum Information Science », Université Tsinghua, Pékin, 21 mai 2012.
- *Classical coding via decoupling*. Colloque « Quantum Information : Codes, Geometry and Random Structures », Centre de recherches mathématiques, Montréal, 25 octobre 2011.
- *Approximate quantum encryption and entropic security*. Conférencier invité, Second QuantumWorks Annual General Meeting, Calgary, Alberta, 26 septembre 2007.
- *Introduction to quantum information theory*. Conférencier invité, « Workshop on One-Shot Quantum Information and Applications to Physics », Bellairs Research Institute, Barbade, 12 mars 2007.
- *Practical Quantum Key Distribution with Decoy States*. Conférencier invité, CIFAR Quantum Information Group Annual Meeting, Halifax, Nouvelle-Écosse, 2 juin 2005.

Séminaires

- *Quantum cryptography with untrusted devices*, Colloque du département d'informatique, Université McGill, Montréal, Québec, 14 décembre 2018.

- *Sampling mixed quantum states*, Séminaire du groupe d'information quantique, Universitat Autònoma de Barcelona (UAB), Barcelone, Espagne, 11 mai 2018.
- *A quantum protocol for the orthogonal vector problem and leakage-resilient computation*, Séminaire du groupe d'information quantique, Universitat Autònoma de Barcelona (UAB), Barcelone, Espagne, 29 octobre 2014.
- *Bounding the uncertainty of constrained adversaries*, Séminaire du groupe de cryptographie, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, Pays-Bas, 4 juillet 2014.
- *An introduction to « one-shot » quantum information theory*, Séminaire du groupe d'information quantique, Télécom Paris, Paris, France, 29 avril 2014.
- *A tutorial on min- and max-entropies and their applications*, Séminaire du groupe d'information quantique, Université Masaryk, Brno, République tchèque, 14 janvier 2014.
- *Min-entropy sampling and cryptography in the bounded storage model*, Quantum Information Seminar, Leibniz-Universität Hannover, Allemagne, 10 avril 2013.
- *Secure two-party quantum computation against specious adversaries*, Conférencier invité, Colloquium of the Institute for Quantum Information, Université de Waterloo, Waterloo, Ontario, 21 mars 2011.
- *The decoupling theorem*, Conférencier invité, Université de Bristol, Royaume-Uni, octobre 2009.
- *The decoupling theorem*, Conférencier invité, École polytechnique fédérale de Zürich (ETH Zürich), Suisse, octobre 2009.
- *The decoupling theorem*, Conférencier invité, Université nationale de Singapour, septembre 2009.
- *Approximate quantum encryption and entropic security*. Conférencier invité, Center for Quantum Information and Quantum Control, Université de Toronto, 26 octobre 2007.

Activités pédagogiques

- Enseignement :
 - Cours magistraux, IFT6080 « Théorie de l'information », Université de Montréal, hiver 2020.
 - Cours magistraux, IFT2105 « Introduction à l'informatique théorique », Université de Montréal, automne 2019, automne 2020.
 - Cours magistraux, cours de M2 « Modèles de calcul » à l'Université de Lorraine, hiver 2019. J'ai enseigné la deuxième moitié du cours, une introduction de 12h à l'informatique quantique.
 - Démonstrateur (chargé de TD), IV111 « Probability in Computer Science », Université Masaryk, printemps 2017.
 - Démonstrateur (chargé de TD), PB071 « Principles of low-level programming », Université Masaryk, printemps 2017.
 - Démonstrateur (chargé de TD), IB000 « Mathematical Foundations of Computer Science », Université Masaryk, automne 2016.
 - Démonstrateur (chargé de TD), MA015 « Graph Algorithms », Université Masaryk, automne 2015 et 2016.
 - Démonstrateur (chargé de TD), IB101 « Introduction to logic », Université Masaryk, printemps 2015 et 2016.
 - Démonstrateur (chargé de TD), IA170 « Randomness and Communication », Université Masaryk, automne 2015.
 - Démonstrateur (chargé de TD), MA010 « Graph Theory », Université Masaryk, automne 2014.
 - Cours magistraux, cours « Quantum Information Processing » à l'Université d'Aarhus, dispensé lors des deux premières sessions de l'année 2013–2014. J'ai enseigné la deuxième moitié du cours, la première ayant été enseignée par Ivan Damgård.
 - Démonstrateur (chargé de TD), cours IFT2105 (Informatique théorique), Université de Montréal, automne 2008. Professeur : Alain Tapp.
- Supervision d'étudiants :
 - Louis Lemonnier (Stage de L3, ENS Paris-Saclay, 2018)
 - Luděk Matyska (Master en informatique, Université Masaryk, 2015–2016)
 - Martin Müller-Lennert (Master en mathématiques, ETH Zürich, 2012–2013)
 - Emilio Onorati (Projet de semestre et master en physique, ETH Zürich, 2012–2013)
 - David Sutter (Master en génie électrique, ETH Zürich, 2012)
 - Richard Küng (Master en physique, ETH Zürich, 2012)
 - Alexander Vitanov (Master en physique, ETH Zürich, 2011)
 - Oleg Szehr (projet de semestre et master en physique, ETH Zürich, 2010)
- Supervision de projets « Proseminar », ETH Zürich. (Il s'agit d'un cours d'initiation à la recherche de niveau baccalauréat. Les étudiants doivent écrire un rapport d'une vingtaine de pages et faire un exposé d'une heure sur un sujet en physique.)

Leadership, administration

- Président du comité de programme :
 - QCrypt 2020, 10 au 14 août 2020, Amsterdam, Pays-Bas (*aura lieu en ligne*)

- Membre du comité de programme :
 - QIP 2019, 14 au 18 janvier 2019, Boulder, CO, États-Unis
 - QCrypt 2018, 27 au 31 août 2018, Shanghai, Chine
 - ICITS (International Conference on Information Theoretic Security) 2017, 29 nov–2 déc 2017, Hong Kong, Chine
 - CEQIP (Central European Quantum Information Processing) 2017, 31 mai au 3 juin 2017, Smolenice, Slovaquie
 - TQC (Theory of Quantum Computation, Communication and Cryptography) 2016, 27 au 29 septembre 2016, Berlin, Allemagne
 - QCrypt 2016, 12 au 16 septembre 2016, Washington DC, États-Unis
 - ICITS (International Conference on Information Theoretic Security) 2016, 9 au 12 août 2016, Tacoma WA, États-Unis
 - CEQIP (Central European Quantum Information Processing) 2016, 16 au 19 juin 2016, Valtice, République tchèque
 - CEQIP (Central European Quantum Information Processing) 2015, 18 au 21 juin 2015, Telč, République tchèque
 - TQC (Theory of Quantum Computation, Communication and Cryptography) 2015, 20 au 22 mai 2015, Bruxelles, Belgique
 - ICITS (International Conference on Information Theoretic Security) 2015, 2 au 5 mai 2015, Lugano, Suisse
 - CEQIP (Central European Quantum Information Processing) 2014, 5 au 8 juin 2014, Znojmo, République tchèque
 - QCrypt 2014, 1^{er} au 5 septembre 2014, Paris, France.
 - QCrypt 2013, 5 au 9 août 2013, Waterloo, Ontario.
- Organisation d'événements scientifiques
 - Organisateur d'une session sur l'information quantique, *International Symposium on Quantum Theory and Symmetries*, Centre de recherches mathématiques, Montréal, Québec, 1–5 juillet 2019.
 - Organisateur (avec Sébastien Gambs) de la Conférence étudiante canadienne d'information quantique 2008, Université de Montréal, 16 au 20 juin 2008
 - Organisateur (avec Simon Perdrix) des Journées informatique quantique 2018 au LORIA, Nancy, 8–9 nov 2018.

Prix et distinctions

Bourses.....

- Bourse postdoctorale CRSNG, Janvier 2010–Décembre 2011 (40000 \$/année)
- Bourse d'études supérieures du Canada (CRSNG), niveau doctorat, septembre 2006–septembre 2009 (35000 \$/année)
- Bourse d'études supérieures du Canada (CRSNG), niveau maîtrise, septembre 2005–septembre 2006 (17500 \$)
- Bourse de la Fondation Marc-Bourgie (10000 \$), 2008–2009
- Bourse J.-Armand-Bombardier (10000 \$), 2007–2008
- Bourse d'admission, Université de Montréal (10000 \$)
- Stanford Graduate Fellowship (32300 \$/année, décliné), 2005
- Princeton University First Year Fellowship (30713 \$/année, décliné), 2005

- Bourse de recherche de premier cycle (CRSNG), été 2003.

Prix.....

- Médaille de bronze, Olympiades internationales de physique 2001, Antalya, Turquie
- Mention honorable, Olympiades internationales de physique 2000, Leicester, Royaume-Uni
- Première place au Canada, Concours de l'Association canadienne des physiciens, 2001
- Sixième place au Canada, Concours de l'Association canadienne des physiciens, 2000