Claude Crépeau

Curriculum Vitæ

Informations personnelles

citoyenneté: Canadien
langues parlées, lues et écrites: français et anglais
date de naissance: 17/2/62
lieu de naissance: Montréal, Québec

Adresses

Rés.: 280 rue Provencher, Mont St-Hilaire, Québec J3H 3M2 CANADA Tél.: +1 (514) 446-9441
Bur.: Département d'Informatique et R.O., Université de Montréal, Tél.: +1 (514) 343-2446
C.P. 6128 succ. C-V, Montréal, Québec H3S 3J7 CANADA FAX.: +1 (514) 343-5834
adresse électronique: crepeau@iro.umontreal.ca

Expérience de travail

institution *poste*	**période**
Université de Montréal, Dép. IRO, Montréal, Québec *Professeur Agrégé*	6/95–
Laboratoire d'Informatique de l'École Normale Supérieure, Paris, France *Chargé de recherches niveau 1 au C.N.R.S.*	10/91–6/95 (titularisé 4/93)
Université de Montréal, Dép. IRO, Montréal, Québec *Professeur Associé*	6/94–6/95
Université Paris–Sud, Laboratoire de Recherche en Informatique, Orsay, France *Maître de conférence associé/Chercheur postdoctoral*	12/89–10/91
Massachusetts Institute of Technology, Cambridge MA, U.S.A. *Assistant de recherche*	9/86–12/89
Université de Montréal, Dép. IRO, Montréal, Québec *Assistant d'enseignement*	9/85–5/86 9/83 - 12/84
Bell-Nothern Research, Îles des Soeurs (Verdun), Québec *Membre du personel scientifique*	5/84–9/86

Études

diplôme	**période** **institution**
Ph.D. Computer Science (cryptographie) dirigé par Silvio Micali	9/86–12/89 M. I. T.
Maîtrise ès Sciences Informatique (cryptographie) dirigé par Gilles Brassard	9/84–8/86 Université de Montréal
participation au "Crypto course" organisé par David Chaum	10/85 C.W.I.
Baccalauréat ès Sciences Mathématiques–Informatique	9/81–5/84 Université de Montréal

Contributions à la communauté scientifique

contributions	**période**
membre du comité de programme du colloque "ACM Conference on Computer and Communications Security'	A95
Associate Editor for Complexity and Cryptography de l'"IEEE Transactions on Information Theory"	1/95–1/98
membre du comité éditorial du "Journal of Cryptology"	1/91–1/95
membre du comité de programme des colloques "Eurocrypt '94" et "XIV International Conference of the Chilean Computer Science Society"	H94
membre du comité de programme du colloque "Eurocrypt '90"	H90
membre du comité de programme du colloque "Crypto '89"	H89

Visites Scientifiques

institution	**période**
Université de Montréal, Dép. IRO, Montréal, Québec	1–12/94 6–9/93 6–12/92
NEC Research, South Brunswick NJ, U.S.A	3/92
CWI, Amsterdam, les Pays-Bas	12/91 6–7/87
Université d'Århus, Århus, Danemark	10–11/91 6/88
IBM, Almaden Research Center, San José CA, U.S.A.	8/88
Bell Communication Research, Morristown NJ, U.S.A.	8/87

Enseignement

institution	**cours**	**niveau**	**durée**	**période**
Asian Institute of Tech.	Cryptographie		30h	12/94
Université de Montréal	Info. Théorique (IFT2102)	B.Sc.	60h	A94
	Cryptologie (IFT6180)	M.Sc.–Ph.D.	60h	A92 H94
École Normale Supérieure	Protocoles Cryptographiques	D.E.A.	12h	H92 H93 A93
École Nationale Supérieure de Technologie Avancée	Complexité et Cryptographie	3$^{\text{è}}$ année ingénieure	21h	H92 H93 A93
Université Paris–Sud	Calculabilité et Complexité	maîtrise	25h	H91 H92
	Cryptographie	D.E.A.	30h	H90 H91
	Algorithmique	M.I.A.G.	30h	H90

Direction d'étudiants

institution	**étudiants**	**période**
Université de Montréal, Dép. IRO, Montréal, Québec	2 M.Sc (co-dir.)	9/93–9/95
	1 Ph.D. (co-dir.)	1/92–9/95
	1 Ph.D. (co-dir.)	1/93–1/96
Université Paris-Sud, Orsay, France	1 D.E.A.	1/92–9/92
	1 Doctorat	9/93–9/96

Publications

thèses et mémoires

[Cr90a] C. Crépeau. Correct and Private Reductions among Oblivious Transfers. PhD thesis, Department of Elec. Eng. and Computer Science, Massachusetts Institute of Technology, 1990. Supervised by Silvio Micali.

[Cr86a] C. Crépeau. Protocole cryptographique de poker à l'aveugle permettant la confidentialié de la stratégie. Master's thesis, Département d'Informatique et de R.O., Université de Montréal, 1986. Supervised by Gilles Brassard.

revues scientifiques

[BBCM95] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized Privacy Amplification. *IEEE Transaction on Information Theory*, **to appear**, November 1995.

[Cr94] C. Crépeau. Quantum Oblivious Transfer. *Journal of Modern Optics*, special issue on *Quantum Communication and Cryptography.* Volume 41, Number 12, pp. 2445-2454, December 1994.

[BBCJPW93] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unkown quantum state by dual classical and EPR channels. *Physical Review Letter*, 70:1895–1898, 1993.

[BCY90] G. Brassard, C. Crépeau, and M. Yung. Constant-round perfect zero-knowledge computationally convincing protocols. *Theoretical Computer Science*, 84:23–52, 1991.

[BBCGP8B] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance. The generation of random numbers that are probably prime. *Journal of Cryptology*, 1(1):53–64, 1988.

[BCC88a] G. Brassard, D. Chaum, and C. Crépeau. An introduction to minimum disclosure. *Quarterly*, 1:3–17, 1988.

[BCC88b] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 37:156–189, 1988.

compte-rendus de colloques avec comité de lecture

[CGT95] C. Crépeau, J. van de Graaf and A. Tapp. Committed Oblivious Transfer and Private Multi-Party Computations. *Advances in Cryptology: Proceedings of Crypto '95*, **to appear**, August 1995.

[CS95] C. Crépeau, and L. Salvail. Quantum Oblivious Mutual Identification. *Advances in Cryptology: Proceedings of Eurocrypt '95*, Springer-Verlag, pages 133-147, 1995.

[BBCM94] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized Privacy Amplification (Abstract). Proceedings of the *IEEE Symposium on Information Theory*, page 350. IEEE, 1994.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In 29^{th} *Symp. on Found. of Computer Sci.*, pages 42–52. IEEE, 1993.

[CK93] C. Crépeau and J. Kilian. Discreet solitary games. In *Advances in Cryptology: Proceedings of Crypto '93*, Lecture Notes in Computer Science. Springer-Verlag, pages 319–330,1993.

[Cr92] C. Crépeau. Cryptographic primitives and quantum theory. In *Proceedings of the second Physics of Computation Workshop, PhysComp '92*, pages 200–204, 1993.

[BBCS92] C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer protocols. In *Advances in Cryptology: Proceedings of Crypto '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer-Verlag, 1992.

[CS91b] C. Crépeau and M. Sántha. Efficient reductions among oblivious transfer protocols based on new self-intersecting codes. In *Sequences II, Methods in Communications, Security, and Computer Science*, pages 360–368. Springer-Verlag, 1991.

[BC91] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology: Proceedings of Crypto '90*, volume 537 of *Lecture Notes in Computer Science*, pages 49–61. Springer-Verlag, 1991.

[BCLL91] G. Brassard, C. Crépeau, S. Laplante, and C. Léger. Computationally convincing proofs of knowledge. In *Proceedings of STACS '91*, volume 480 of *Lecture Notes in Computer Science*, pages 251–262. Springer-Verlag, 1991.

[CS91a] C. Crépeau and M. Sántha. On the reversibility of oblivious transfer. In *Advances in Cryptology: Proceedings of Eurocrypt '91*, volume 547 of *Lecture Notes in Computer Science*, pages 106–113. Springer-Verlag, 1991.

[BC90] G. Brassard and C. Crépeau. Sorting out zero-knowledge. In *Advances in Cryptology: Proceedings of Eurocrypt '89*, volume 434 of *Lecture Notes in Computer Science*, pages 150–154. Springer-Verlag, 1990.

[Cr90b] C. Crépeau. Verifiable disclosure of secrets and applications. In *Advances in Cryptology: Proceedings of Eurocrypt '89*, volume 434 of *Lecture Notes in Computer Science*, pages 181–191. Springer-Verlag, 1990.

[BCY89] G. Brassard, C. Crépeau, and M. Yung. Everything in NP can be argued in perfect zero-knowledge in a constant number of rounds. In 16^{th} *ICALP*, volume 372 of *Lecture Notes in Computer Science*, pages 123–136. Springer-Verlag, 1989.

[CCD88] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In 19^{th} *Symp. on Theory of Computing*, pages 11–19. ACM, 1988.

[CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In 29^{th} *Symp. on Found. of Computer Sci.*, pages 42–52. IEEE, 1988.

[CK90] C. Crépeau and J. Kilian. Weakening security assumptions and oblivious transfer. In S. Goldwasser, editor, *Advances in Cryptology: Proceedings of Crypto '88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer-Verlag, 1990.

[Cr88] C. Crépeau. Equivalence between two flavours of oblivious transfers (abstract). In C. Pomerance, editor, *Advances in Cryptology: Proceedings of Crypto '87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354. Springer-Verlag, 1988.

[BBCGP87] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance. Two observations on probabilistic primality testing. In *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 443–450. Springer-Verlag, 1987.

[BC87] G. Brassard and C. Crépeau. Zero-knowledge simulation of boolean circuits (extended abstract). In *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 223–233. Springer-Verlag, 1987.

[BCR87] G. Brassard, C. Crépeau, and J.–M. Robert. All-or-nothing disclosure of secrets (extended abstract). In *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 234–238. Springer-Verlag, 1987.

[Cr87] C. Crépeau. A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face. In *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 239–247. Springer, 1987.

[BC86] G. Brassard and C. Crépeau. Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond. In 27^{th} *Symp. of Found. of Computer Sci.*, pages 188–195. IEEE, 1986.

[BCR86] G. Brassard, C. Crépeau, and J.–M. Robert. Information theoretic reductions among disclosure problems. In 27^{th} *Symp. of Found. of Computer Sci.*, pages 168–173. IEEE, 1986.

[Cr86b] C. Crépeau. A secure poker protocol that minimizes the effects of player coalitions. In *Advances in Cryptology: Proceedings of Crypto '85*, vol 218 of *LNCS*,pages 73–86. Springer, 1986.