thèses et mémoires

[Cré90a] 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.

[Cré86a] 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

[Cré94] C. Crépeau. Quantum Oblivious Transfer. *Journal of Modern Optics*, special issue on *Quantum Communication and Cryptography.* **to appear** 1994.

[BBCM93] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Privacy amplification against Probabilistic Information. *IEEE Transaction on Information Theory*, 1993. **submitted for publication**.

[BBC+93] 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.

[BCY91] G. Brassard, C. Crépeau, and M. Yung. Constant-round perfect zero-knowledge computationally convincing protocols. *Theoretical Computer Science*, 84:23–52, 1991.

[BBC+88] 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

[BBCM94] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Privacy amplification against Probabilistic Information (Abstract). Proceedings of the *IEEE Symposium on Information Theory*, 1994. **to appear**.

[CS94] C. Crépeau, and L. Salvail. Mutual Oblivious Identification. *Advances in Cryptology: Proceedings of Crypto '94*, **submitted for publication**, 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.

[Cré93] 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.

[CS91a] 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.

[CS91b] 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.

[Cré90b] 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.

[Cré88] 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.

[BBC+87] P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier, and C. Pomerance. Two observations on probabilistic primality testing. In A. M. Odlyzko, editor, *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 A. M. Odlyzko, editor, *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 A. M. Odlyzko, editor, *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 234–238. Springer-Verlag, 1987.

[Cré87] C. Crépeau. A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face. In A. M. Odlyzko, editor, *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 239–247. Springer-Verlag, 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.

[Cré86b] C. Crépeau. A secure poker protocol that minimizes the effects of player coalitions. In H. C. Williams, editor, *Advances in Cryptology: Proceedings of Crypto '85*, volume 218 of *Lecture Notes in Computer Science*, pages 73–86. Springer-Verlag, 1986.