References

[1] Michel Abdalla, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, and Nigel P. Smart. Identity-based encryption gone wild. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 300–311. Springer-Verlag, Berlin-Heidelberg, 2006.

[2] Luca Aceto, Taolue Chen, Wan Fokkink, and Anna Ingolfsdottir. On the axiomatizability of priority. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 480–491. Springer-Verlag, Berlin-Heidelberg, 2006.

[3] Luca Aceto, Wan Fokkink, Anna Ingolfsdottir, and Bas Luttik. A finite equational base for ccs with left merge and communication merge. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 492–503. Springer-Verlag, Berlin-Heidelberg, 2006.

[4] Pedro Adão and Cédric Fournet. Cryptographically sound implementations for communicating processes. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 83–94. Springer-Verlag, Berlin-Heidelberg, 2006.

[5] Rajeev Alur, Pavol Černý, and Steve Zdancewic. Preserving secrecy under refinement. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 107–118. Springer-Verlag, Berlin-Heidelberg, 2006.

[6] Frederik Armknecht and Matthias Krause. Constructing single- and multi-output boolean functions with maximal algebraic immunity. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 180–191. Springer-Verlag, Berlin-Heidelberg, 2006.

[7] Ittai Balaban, Amir Pnueli, and Lenore Zuck. Invisible safety of distributed protocols. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 528–539. Springer-Verlag, Berlin-Heidelberg, 2006.

[8] Michael Benedikt and Christoph Koch. Interpreting tree-to-tree queries. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 552–564. Springer-Verlag, Berlin-Heidelberg, 2006.

[9] Piero A. Bonatti, Carsten Lutz, Aniello Murano, and Moshe Y. Vardi. The complexity of enriched μ-calculi. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 540–551. Springer-Verlag, Berlin-Heidelberg, 2006.

[10] Michele Boreale. Quantifying information leakage in process calculi. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 119–131. Springer-Verlag, Berlin-Heidelberg, 2006.

[11] Patricia Bouyer, Serge Haddad, and Pierre-Alain Reynier. Timed petri nets and timed automata: On the discriminating power of zeno sequences. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo

Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 420–431. Springer-Verlag, Berlin-Heidelberg, 2006.

[12] Marius Bozga, Radu Iosif, and Yassine Lakhnech. Flat parametric counter automata. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 577–588. Springer-Verlag, Berlin-Heidelberg, 2006.

[13] Ricardo Corin and Jerry den Hartog. A probabilistic hoare-style logic for game-based cryptographic proofs. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 252–263. Springer-Verlag, Berlin-Heidelberg, 2006.

[14] Vincent Danos, Elham Kashefi, and Prakash Panangaden. The one way to quantum computation. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 13–21. Springer-Verlag, Berlin-Heidelberg, 2006.

[15] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis in presence of a homomorphism operator and exclusive or. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 132–143. Springer-Verlag, Berlin-Heidelberg, 2006.

[16] Yevgeniy Dodis and Renato Renner. On the impossibility of extracting classical randomness using a quantum computer. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, vol-

ume 4052 of *LNCS*, pages 204–215. Springer-Verlag, Berlin-Heidelberg, 2006.

[17] Vivien Dubois, Louis Granboulan, and Jacques Stern. An efficient provable distinguisher for hfe. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 156–167. Springer-Verlag, Berlin-Heidelberg, 2006.

[18] Cynthia Dwork. Differential privacy. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 1–12. Springer-Verlag, Berlin-Heidelberg, 2006.

[19] Kousha Etessami and Mihalis Yannakakis. Recursive concurrent stochastic games. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 324–335. Springer-Verlag, Berlin-Heidelberg, 2006.

[20] Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Sébastien Zimmer. Hardness of distinguishing the msb or lsb of secret keys in diffie-hellman schemes. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 240–251. Springer-Verlag, Berlin-Heidelberg, 2006.

[21] Jun Furukawa, Kaoru Kurosawa, and Hideki Imai. An efficient compiler from σ-protocol to 2-move deniable zero-knowledge. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 46–57. Springer-Verlag, Berlin-Heidelberg, 2006.

[22] Blaise Genest and Anca Muscholl. Constructing exponential-size deterministic zielonka automata. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 565–576. Springer-Verlag, Berlin-Heidelberg, 2006.

[23] Rosario Gennaro and Silvio Micali. Independent zero-knowledge sets. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 34–45. Springer-Verlag, Berlin-Heidelberg, 2006.

[24] Hugo Gimbert and Wiesław Zielonka. Deterministic priority mean-payoff games as limits of discounted games. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 312–323. Springer-Verlag, Berlin-Heidelberg, 2006.

[25] Stefano Guerrini and Patrizia Marzuoli. Commutative locative quantifiers for multiplicative linear logic. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 396–407. Springer-Verlag, Berlin-Heidelberg, 2006.

[26] Esfandiar Haghverdi. Typed goi for exponentials. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 384–395. Springer-Verlag, Berlin-Heidelberg, 2006.

[27] Iftach Haitner, Danny Harnik, and Omer Reingold. Efficient pseudorandom generators from exponentially hard one-way functions. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors,

Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006), volume 4052 of *LNCS*, pages 228–239. Springer-Verlag, Berlin-Heidelberg, 2006.

[28] Danny Harnik and Moni Naor. On everlasting security in the hybrid bounded storage model. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 192–203. Springer-Verlag, Berlin-Heidelberg, 2006.

[29] Kohei Honda, Martin Berger, and Nobuko Yoshida. Descriptive and relative completeness of logics for higher-order functions. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 360–371. Springer-Verlag, Berlin-Heidelberg, 2006.

[30] Radha Jagadeesan, Alan Jeffrey, Corin Pitcher, and James Riely. λ-rbac: Programming with role-based access controll. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 456–467. Springer-Verlag, Berlin-Heidelberg, 2006.

[31] Tomasz Jurdziński. On complexity of grammars related to the safety problem. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 432–443. Springer-Verlag, Berlin-Heidelberg, 2006.

[32] Detlef Kähler, Ralf Küsters, and Thomas Wilke. A dolev-yao-based definition of abuse-free protocols. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming,*

ICALP'2006, Part II (Venice, Italy, July 10-14, 2006), volume 4052 of *LNCS*, pages 95–106. Springer-Verlag, Berlin-Heidelberg, 2006.

[33] Juhani Karhumäki, Michal Kunc, and Alexander Okhotin. Communication of two stacks and rewriting. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 468–479. Springer-Verlag, Berlin-Heidelberg, 2006.

[34] Wong Karianto, Aloys Krieg, and Wolfgang Thomas. On intersection problems for polynomially generated sets. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 516–527. Springer-Verlag, Berlin-Heidelberg, 2006.

[35] Akinori Kawachi and Tomoyuki Yamakami. Quantum hardcore functions by complexity-theoretical quantum list decoding. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 216–227. Springer-Verlag, Berlin-Heidelberg, 2006.

[36] Eryk Kopczyński. Half-positional determinacy of infinite games. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 336–347. Springer-Verlag, Berlin-Heidelberg, 2006.

[37] Paul Blain Levy. Jumbo λ-calculus. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 444–455. Springer-Verlag, Berlin-Heidelberg, 2006.

[38] Markus Lohrey and Géraud Sénizergues. Theories of hnn-extensions and amalgamated products. In Michele Bugliesi, Bart Preneel, Vladimiro

Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 504–515. Springer-Verlag, Berlin-Heidelberg, 2006.

[39] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 144–155. Springer-Verlag, Berlin-Heidelberg, 2006.

[40] Daniele Micciancio and Saurabh Panjwani. Corrupting one vs. corrupting many: The case of broadcast and multicast encryption. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 70–82. Springer-Verlag, Berlin-Heidelberg, 2006.

[41] Rasmus Ejlers Møgelberg. Interpreting polymorphic fpc into domain theoretic models of parametric polymorphism. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 372–383. Springer-Verlag, Berlin-Heidelberg, 2006.

[42] Filip Murlak. The wadge hierarchy of deterministic tree languages. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 408–419. Springer-Verlag, Berlin-Heidelberg, 2006.

[43] Duong Hieu Phan, Reihaneh Safavi-Naini, and Dongvu Tonien. Generic construction of hybrid public key traitor tracing with full-public-traceability. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part*

II (Venice, Italy, July 10-14, 2006), volume 4052 of *LNCS*, pages 264–275. Springer-Verlag, Berlin-Heidelberg, 2006.

[44] Krzysztof Pietrzak. A tight bound for emac. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 168–179. Springer-Verlag, Berlin-Heidelberg, 2006.

[45] Colin Stirling. A game-theoretic approach to deciding higher-order matching. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 348–359. Springer-Verlag, Berlin-Heidelberg, 2006.

[46] Tamir Tassa and Nira Dyn. Multipartite secret sharing by bivariate interpolation. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 288–299. Springer-Verlag, Berlin-Heidelberg, 2006.

[47] Damien Vergnaud. New extensions of pairing-based signatures into universal designated verifier signatures. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 58–69. Springer-Verlag, Berlin-Heidelberg, 2006.

[48] Ivan Visconti. Efficient zero knowledge on the internet. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 22–33. Springer-Verlag, Berlin-Heidelberg, 2006.

[49] Douglas Wikström and Jens Groth. An adaptively secure mix-net without erasures. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone,

and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 276–287. Springer-Verlag, Berlin-Heidelberg, 2006.

[50] Qiqi Yan. Lower bounds for complementation of ω-automata via the full automata technique. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP'2006, Part II (Venice, Italy, July 10-14, 2006)*, volume 4052 of *LNCS*, pages 589–600. Springer-Verlag, Berlin-Heidelberg, 2006.