References

[1] Kristina Altmann, Tibor Jager, and Andy Rupp. On black-box ring extraction and integer factorization. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 437–448. Springer-Verlag, Berlin-Heidelberg, 2008.

[2] Roland Axelsson, Keijo Heljanko, and Martin Lange. Analyzing context-free grammars using an incremental sat solver. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 410–422. Springer-Verlag, Berlin-Heidelberg, 2008.

[3] Martin Berger, Kohei Honda, and Nobuko Yoshida. Completeness and logical full abstraction in modal logics for typed mobile processes. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 99–111. Springer-Verlag, Berlin-Heidelberg, 2008.

[4] Lars Birkedal, Bernhard Reus, Jan Schwinghammer, and Hongseok Yang. A simple model of separation logic for higher-order store. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 348–360. Springer-Verlag, Berlin-Heidelberg, 2008.

[5] Henrik Björklund and Wim Martens. The tractability frontier for nfa minimization. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg,

Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 27–38. Springer-Verlag, Berlin-Heidelberg, 2008.

[6] Manuel Bodirsky and Martin Grohe. Non-dichotomies in constraint satisfaction complexity. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 184–196. Springer-Verlag, Berlin-Heidelberg, 2008.

[7] Bernard Boigelot, Julien Brusten, and Véronique Bruyère. On the sets of real numbers recognized by finite automata in multiple bases. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 112–123. Springer-Verlag, Berlin-Heidelberg, 2008.

[8] Mikołaj Bojańczyk and Luc Segoufin. Tree languages defined in first-order logic with one quantifier alternation. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 233–245. Springer-Verlag, Berlin-Heidelberg, 2008.

[9] Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell. On expressiveness and complexity in real-time model checking. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 124–135. Springer-Verlag, Berlin-Heidelberg, 2008.

[10] Tomáš Brázdil, Vojtěch Forejt, and Antonín Kučera. Controller synthesis and verification for markov decision processes with qualitative branching time objectives. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 148–159. Springer-Verlag, Berlin-Heidelberg, 2008.

[11] Ran Canetti. Composable formal security analysis: Juggling soundness, simplicity and efficiency. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 1–13. Springer-Verlag, Berlin-Heidelberg, 2008.

[12] Ran Canetti and Ronny Ramzi Dakdouk. Extractable perfectly one-way functions. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 449–460. Springer-Verlag, Berlin-Heidelberg, 2008.

[13] Ran Canetti, Dror Eiger, Shafi Goldwasser, and Dah-Yoh Lim. How to protect yourself without perfect shredding. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 511–523. Springer-Verlag, Berlin-Heidelberg, 2008.

[14] Hubie Chen. Quantified constraint satisfaction and the polynomially generated powers property. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part*

II (Reykjavik, Iceland, July 7-11, 2008), volume 5126 of *LNCS*, pages 197–208. Springer-Verlag, Berlin-Heidelberg, 2008.

[15] Bob Coecke and Ross Duncan. Interacting quantum observables. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 298–310. Springer-Verlag, Berlin-Heidelberg, 2008.

[16] Thomas Colcombet and Christof Löding. The non-deterministic mostowski hierarchy and distance-parity automata. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 398–409. Springer-Verlag, Berlin-Heidelberg, 2008.

[17] Anuj Dawar and Stephan Kreutzer. On datalog vs. lfp. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 160–171. Springer-Verlag, Berlin-Heidelberg, 2008.

[18] Jintai Ding, Vivien Dubois, Bo-Yin Yang, Owen Chia-Hsin Chen, and Chen-Mou Cheng. Could sflash be repaired? In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 691–701. Springer-Verlag, Berlin-Heidelberg, 2008.

[19] László Egri, Benoît Larose, and Pascal Tesson. Directed *st*-connectivity is not expressible in symmetric datalog. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part*

II (Reykjavik, Iceland, July 7-11, 2008), volume 5126 of *LNCS*, pages 172–183. Springer-Verlag, Berlin-Heidelberg, 2008.

[20] Javier Esparza, Stefan Kiefer, and Michael Luttenberger. Newton's method for ω-continuous semirings. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 14–26. Springer-Verlag, Berlin-Heidelberg, 2008.

[21] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions revisited. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 655–666. Springer-Verlag, Berlin-Heidelberg, 2008.

[22] Mai Gehrke, Serge Grigorieff, and Jean-Éric Pin. Duality and equational theory of regular languages. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 246–257. Springer-Verlag, Berlin-Heidelberg, 2008.

[23] Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin. How to encrypt with the lpn problem. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 679–690. Springer-Verlag, Berlin-Heidelberg, 2008.

[24] Antonio Cano Gómez, Giovanna Guaiana, and Jean-Éric Pin. When does partial commutative closure preserve regularity? In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th*

International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008), volume 5126 of *LNCS*, pages 209–220. Springer-Verlag, Berlin-Heidelberg, 2008.

[25] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded ciphertext policy attribute based encryption. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 579–591. Springer-Verlag, Berlin-Heidelberg, 2008.

[26] Karin Greimel, Roderick Bloem, Barbara Jobstmann, and Moshe Vardi. Open implication. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 361–372. Springer-Verlag, Berlin-Heidelberg, 2008.

[27] Hermann Gruber and Markus Holzer. Finite automata, digraph connectivity, and regular expression size. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 39–50. Springer-Verlag, Berlin-Heidelberg, 2008.

[28] Sean Hallgren, Alexandra Kolla, Pranab Sen, and Shengyu Zhang. Making classical honest verifier zero knowledge protocols secure against quantum attacks. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 592–603. Springer-Verlag, Berlin-Heidelberg, 2008.

[29] Martin Hirt, Jesper Buus Nielsen, and Bartosz Przydatek. Asynchronous multi-party computation with quadratic communication.

In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 473–485. Springer-Verlag, Berlin-Heidelberg, 2008.

[30] Jonathan J. Hoch and Adi Shamir. On the strength of the concatenated hash combiner when all the hash functions are weak. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 616–630. Springer-Verlag, Berlin-Heidelberg, 2008.

[31] Stanisław Jarecki and Xiaomin Liu. Affiliation-hiding envelope and authentication schemes with efficient support for multiple credentials. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 715–726. Springer-Verlag, Berlin-Heidelberg, 2008.

[32] Artur Jeż and Alexander Okhotin. On the computational completeness of equations over sets of natural numbers. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 63–74. Springer-Verlag, Berlin-Heidelberg, 2008.

[33] Magnus Johansson, Joachim Parrow, Björn Victor, and Jesper Bengtson. Extended pi-calculi. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II*

(Reykjavik, Iceland, July 7-11, 2008), volume 5126 of *LNCS*, pages 87–98. Springer-Verlag, Berlin-Heidelberg, 2008.

[34] Tomasz Jurdziński. Leftist grammars are non-primitive recursive. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 51–62. Springer-Verlag, Berlin-Heidelberg, 2008.

[35] Yael Tauman Kalai and Ran Raz. Interactive pcp. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 536–547. Springer-Verlag, Berlin-Heidelberg, 2008.

[36] Shin-ya Katsumata. Attribute grammars and categorical semantics. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 271–282. Springer-Verlag, Berlin-Heidelberg, 2008.

[37] Jonathan Katz, Chiu-Yuen Koo, and Ranjit Kumaresan. Improving the round complexity of vss in point-to-point networks. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 499–510. Springer-Verlag, Berlin-Heidelberg, 2008.

[38] Delia Kesner. Perpetuality for full and safe composition (in a constructive setting). In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland,*

July 7-11, 2008), volume 5126 of *LNCS*, pages 311–322. Springer-Verlag, Berlin-Heidelberg, 2008.

[39] Vladimir Kolesnikov and Charles Rackoff. Password mistyping in two-factor-authenticated key exchange. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 702–714. Springer-Verlag, Berlin-Heidelberg, 2008.

[40] Vladimir Kolesnikov and Thomas Schneider. Improved garbled circuit: Free xor gates and applications. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 486–498. Springer-Verlag, Berlin-Heidelberg, 2008.

[41] Kaoru Kurosawa and Jun Furukawa. Universally composable undeniable signature. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 524–535. Springer-Verlag, Berlin-Heidelberg, 2008.

[42] Sylvain Lebresne. A systemf with call-by-name exceptions. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 323–335. Springer-Verlag, Berlin-Heidelberg, 2008.

[43] Keye Martin. A domain theoretic model of qubit channels. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the*

35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008), volume 5126 of *LNCS*, pages 283–297. Springer-Verlag, Berlin-Heidelberg, 2008.

[44] Christian Mathissen. Weighted logics for nested words and algebraic formal power series. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 221–232. Springer-Verlag, Berlin-Heidelberg, 2008.

[45] Moni Naor, Gil Segev, and Udi Wieder. History-independent cuckoo hashing. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 631–642. Springer-Verlag, Berlin-Heidelberg, 2008.

[46] Matthias Neubauer and Peter Thiemann. Placement inference for a client-server calculus. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 75–86. Springer-Verlag, Berlin-Heidelberg, 2008.

[47] Rafail Ostrovsky, Giuseppe Persiano, and Ivan Visconti. Constant-round concurrent non-malleable zero knowledge in the bare public-key model. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 548–559. Springer-Verlag, Berlin-Heidelberg, 2008.

[48] Krzysztof Pietrzak and Johan Sjödin. Weak pseudorandom functions in minicrypt. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg,

Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 423–436. Springer-Verlag, Berlin-Heidelberg, 2008.

[49] Manoj Prabhakaran and Mike Rosulek. Homomorphic encryption with cca security. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 667–678. Springer-Verlag, Berlin-Heidelberg, 2008.

[50] Bartosz Przydatek and Jürg Wullschleger. Error-tolerant combiners for oblivious primitives. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 461–472. Springer-Verlag, Berlin-Heidelberg, 2008.

[51] Jean-François Raskin and Frédéric Servais. Visibly pushdown transducers. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 386–397. Springer-Verlag, Berlin-Heidelberg, 2008.

[52] Sven Schewe. Atl* satisfiability is 2exptime-complete. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 373–385. Springer-Verlag, Berlin-Heidelberg, 2008.

[53] Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg,

Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 560–578. Springer-Verlag, Berlin-Heidelberg, 2008.

[54] Thomas Shrimpton and Martijn Stam. Building a collision-resistant compression function from non-compressing primitives. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 643–654. Springer-Verlag, Berlin-Heidelberg, 2008.

[55] Robert J. Simmons and Frank Pfenning. Linear logical algorithms. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 336–347. Springer-Verlag, Berlin-Heidelberg, 2008.

[56] Vladimeros Vladimerou, Pavithra Prabhakar, Mahesh Viswanathan, and Geir Dullerud. Stormed hybrid systems. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 136–147. Springer-Verlag, Berlin-Heidelberg, 2008.

[57] Stephanie Wehner and Jürg Wullschleger. Composable security in the bounded-quantum-storage model. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 604–615. Springer-Verlag, Berlin-Heidelberg, 2008.

[58] Tetsuo Yokoyama, Holger Bock Axelsen, and Robert Glück. Reversible flowchart languages and the structured reversible program the-

orem. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Proceedings of the 35th International Colloquium on Automata, Languages and Programming, ICALP'2008, Part II (Reykjavik, Iceland, July 7-11, 2008)*, volume 5126 of *LNCS*, pages 258–270. Springer-Verlag, Berlin-Heidelberg, 2008.