A Bibliography of Papers in *Lecture Notes in Computer Science* (2003) (Part 1 of 4)

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: http://www.math.utah.edu/~beebe/

14 October 2017
Version 1.06

Title word cross-reference

References

Back:2003:SRB

[1] Ralph-Johan Back. SFI: A refinement based layered software architecture. *Lecture Notes in Computer Science*, 2495:1–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950001.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950001.pdf`.

Liu:2003:DQS

[2] Shaoying Liu. Developing quality software systems using the SOFL formal engineering method. *Lecture Notes in Computer Science*, 2495:3–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950003.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950003.pdf`.

Hale:2003:MRI

[3] Mark A. Hale. Maintaining referential integrity on the Web. *Lecture Notes in Computer Science*, 2495:20–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950020.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950020.pdf`.

Jullig:2003:FME

[4] Richard Jüllig. Formal methods in enterprise computing. *Lecture Notes in Computer Science*, 2495:22–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950022.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950022.pdf`.

Woodcock:2003:UTP

[5] Jim Woodcock and Arthur Hughes. Unifying theories of parallel programming. *Lecture Notes in Computer Science*, 2495:24–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950024.htm; http://link.`

springer.de/link/service/series/0558/papers/2495/24950024.pdf.

Mei:2003:AAA

[6] Hong Mei, Feng Chen, Qianxiang Wang, and Yao-Dong Feng. ABC/ADL: An ADL supporting component composition. *Lecture Notes in Computer Science*, 2495:38–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950038.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950038.pdf.

Zheng:2003:DCO

[7] Hong Zheng and Shi xian Li. The description of CORBA objects based on Petri nets. *Lecture Notes in Computer Science*, 2495:48–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950048.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950048.pdf.

Heisel:2003:TFM

[8] Maritta Heisel, Thomas Santen, and Jeanine Souquières. Toward a formal model of software components. *Lecture Notes in Computer Science*, 2495:57–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950057.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950057.pdf.

Liu:2003:SBS

[9] Jing Liu, Huaikou Miao, and Xiaolei Gao. A specification-based software construction framework for reuse. *Lecture Notes in Computer Science*, 2495:69–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950069.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950069.pdf.

Chen:2003:SCM

[10] Xuejun Chen. Specifying a component model for building dynamically reconfigurable distributed systems. *Lecture Notes in Computer Science*, 2495:80–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950080.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950080.pdf.

Alagar:2003:TTS

[11] Vasu Alagar and Ralf Lämmel. Three-tiered specification of micro-architectures. *Lecture Notes in Computer Science*, 2495:92–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950092.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950092.pdf.

Chang:2003:MAC

[12] Jiayue Chang and Huadong Ma. Modeling the architecture for component-based E-commerce system. *Lecture*

Notes in Computer Science, 2495:98–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950098.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950098.pdf.

Cao:2003:CSW

[13] Fei Cao, Barrett R. Bryant, Rajeev R. Raje, Mikhail Auguston, Andrew M. Olson, and Carol C. Burt. Component specification and wrapper/glue code generation with two-level grammar using domain specific knowledge. *Lecture Notes in Computer Science*, 2495:103–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950103.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950103.pdf.

Smith:2003:ASO

[14] Graeme Smith and John Derrick. Abstract specification in Object-Z and CSP. *Lecture Notes in Computer Science*, 2495:108–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950108.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950108.pdf.

Attiogbe:2003:MIA

[15] J. Christian Attiogbé. Mechanization of an integrated approach: Shallow embedding into SAL/PVS. *Lecture Notes in Computer Science*, 2495:120–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950120.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950120.pdf.

Musser:2003:CUC

[16] David R. Musser and Zhiqing Shao. Concept use or concept refinement: An important distinction in building generic specifications. *Lecture Notes in Computer Science*, 2495:132–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950132.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950132.pdf.

Taguchi:2003:OMO

[17] Kenji Taguchi and Jin Song Dong. An overview of mobile object-Z. *Lecture Notes in Computer Science*, 2495:144–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950144.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950144.pdf.

Dong:2003:ZAS

[18] Jin Song Dong, Jing Sun, and Hai Wang. Z approach to Semantic Web. *Lecture Notes in Computer Science*, 2495:156–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950156.htm; http://link.

springer.de/link/service/series/0558/papers/2495/24950156.pdf.

Qin:2003:HSP

[19] Shengchao Qin, Jifeng He, Zongyan Qiu, and Naixiao Zhang. Hardware/software partitioning in Verilog. *Lecture Notes in Computer Science*, 2495: 168–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950168.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950168.pdf.

Pereira:2003:FMS

[20] Adriano Pereira, Mark Song, Gustavo Gorgulho, Wagner Meira Jr., and Sérgio Campos. A formal methodology to specify E-commerce systems. *Lecture Notes in Computer Science*, 2495:180–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950180.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950180.pdf.

Miller:2003:MBS

[21] Tim Miller and Paul Strooper. Model-based specification animation using testgraphs. *Lecture Notes in Computer Science*, 2495:192–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950192.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950192.pdf.

Arenas:2003:AMS

[22] Alvaro E. Arenas. An abstract model for scheduling real-time programs. *Lecture Notes in Computer Science*, 2495: 204–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950204.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950204.pdf.

Mosbahi:2003:SVT

[23] Olfa Mosbahi, Leila Jemni, Samir Ben Ahmed, and Jacques Jaray. A specification and validation technique based on STATEMATE and FNLOG. *Lecture Notes in Computer Science*, 2495: 216–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950216.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950216.pdf.

Du:2003:FRA

[24] Yuyue Du and Changjun Jiang. Formal representation and analysis of batch stock trading systems by logical Petri net workflows. *Lecture Notes in Computer Science*, 2495:221–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950221.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950221.pdf.

Huang:2003:CMN

[25] Jinfeng Huang, Ad Verschueren, Henri Aalderink, and Johan Lukkien. A

calculus for mobile network systems. *Lecture Notes in Computer Science*, 2495:226–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950226.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950226.pdf`.

Li:2003:MRT

[26] Guangyuan Li and Zhisong Tang. Modelling real-time systems with continuous-time temporal logic. *Lecture Notes in Computer Science*, 2495:231–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950231.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950231.pdf`.

Liu:2003:CBD

[27] Ying Liu and Naixiao Zhang. On concept-based definition of domain-specific languages. *Lecture Notes in Computer Science*, 2495:237–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950237.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950237.pdf`.

Zhu:2003:FSE

[28] Hong Zhu. Formal specification of evolutionary software agents. *Lecture Notes in Computer Science*, 2495: 249–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950249.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950249.pdf`.

Liu:2003:DDA

[29] Yuan Liu, Baowen Xu, and Zhenqiang Chen. Detecting deadlock in Ada rendezvous flow structure based on process algebra. *Lecture Notes in Computer Science*, 2495:262–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950262.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950262.pdf`.

Yu:2003:FAR

[30] Huiqun Yu, Xudong He, Yi Deng, and Lian Mo. Formal analysis of real-time systems with SAM. *Lecture Notes in Computer Science*, 2495: 275–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950275.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950275.pdf`.

Ng:2003:TSV

[31] Muan Yong Ng and Michael Butler. Tool support for visualizing CSP in UML. *Lecture Notes in Computer Science*, 2495:287–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950287.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950287.pdf`.

Celiku:2003:TPS

[32] Orieta Celiku and Joakim von Wright. Theorem prover support for precondition and correctness calculation. *Lecture Notes in Computer Science*, 2495: 299–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950299.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950299.pdf`.

Dong:2003:XBS

[33] Jin Song Dong, Yuan Fang Li, Jing Sun, Jun Sun, and Hai Wang. XML-based static type checking and dynamic visualization for TCOZ. *Lecture Notes in Computer Science*, 2495: 311–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950311.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950311.pdf`.

Goldson:2003:CBS

[34] Doug Goldson, Greg Reeve, and Steve Reeves. μ-chart-based specification and refinement. *Lecture Notes in Computer Science*, 2495:323–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950323.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950323.pdf`.

Peuker:2003:TRC

[35] Sibylle Peuker and Ian Hayes. Towards a refinement calculus for concurrent real-time programs. *Lecture Notes in Computer Science*, 2495:335–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950335.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950335.pdf`.

Duran:2003:RAF

[36] Adolfo Duran, Ana Cavalcanti, and Augusto Sampaio. Refinement algebra for formal bytecode generation. *Lecture Notes in Computer Science*, 2495:347–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950347.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950347.pdf`.

Chen:2003:FMJ

[37] Jessica Chen. Formal modelling of Java GUI event handling. *Lecture Notes in Computer Science*, 2495:359–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950359.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950359.pdf`.

Cavalli:2003:NAS

[38] Ana Cavalli and Stéphane Maag. A new algorithm for service interaction detection. *Lecture Notes in Computer Science*, 2495:371–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.`

de/link/service/series/0558/bibs/2495/24950371.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950371.pdf.

Plosila:2003:SAC

[39] Juha Plosila and Tiberiu Seceleanu. Specification of an asynchronous on-chip bus. *Lecture Notes in Computer Science*, 2495:383–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950383.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950383.pdf.

Pang:2003:ASP

[40] Jun Pang. Analysis of a security protocol in μCRL. *Lecture Notes in Computer Science*, 2495:396–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950396.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950396.pdf.

Davrondjon:2003:DSC

[41] Gafurov Davrondjon and Tomasz Janowski. Developing a spell-checker for Tajik using RAISE. *Lecture Notes in Computer Science*, 2495:401–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950401.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950401.pdf.

Shukur:2003:MTT

[42] Zarina Shukur, Abdullah Md. Zin, and Ainita Ban. M2Z: A tool for translating a natural language software specification into Z. *Lecture Notes in Computer Science*, 2495:406–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950406.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950406.pdf.

Anderson:2003:AIT

[43] Hugh Anderson. Abstract interpretation with a theorem prover. *Lecture Notes in Computer Science*, 2495:411–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950411.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950411.pdf.

Roychoudhury:2003:FRA

[44] Abhik Roychoudhury. Formal reasoning about hardware and software memory models. *Lecture Notes in Computer Science*, 2495:423–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950423.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950423.pdf.

Wang:2003:SHA

[45] Ji Wang, Wei Dong, and Zhi-Chang Qi. Slicing hierarchical automata for

model checking UML statecharts. *Lecture Notes in Computer Science*, 2495: 435–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950435.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950435.pdf`.

Zobair:2003:FVS

[46] M. Hasan Zobair and Sofiène Tahar. Formal verification of a SONET telecom system block. *Lecture Notes in Computer Science*, 2495:447–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950447.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950447.pdf`.

Abdel-Hamid:2003:EHV

[47] Amr T. Abdel-Hamid, Sofiène Tahar, and John Harrison. Enabling hardware verification through design changes. *Lecture Notes in Computer Science*, 2495:459–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950459.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950459.pdf`.

Wimmel:2003:SBT

[48] Guido Wimmel and Jan Jürjens. Specification-based test generation for security-critical systems using mutations. *Lecture Notes in Computer Science*, 2495:471–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950471.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950471.pdf`.

Diab:2003:FDF

[49] Hassan Diab, Marc Frappier, and Richard St-Denis. A formal definition of function points for automated measurement of B specifications. *Lecture Notes in Computer Science*, 2495: 483–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950483.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950483.pdf`.

Guo:2003:MCT

[50] Fan Guo, YiYun Chen, and Rong-Gui Hu. Machine code type safety. *Lecture Notes in Computer Science*, 2495:495–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/2495/24950495.htm`; `http://link.springer.de/link/service/series/0558/papers/2495/24950495.pdf`.

Jiang:2003:FSS

[51] Yan-Bing Jiang, Wei-Zhong Shao, Zhi-Yi Ma, and Yao-Dong Feng. On the formalized semantics of static modeling elements in UML. *Lecture Notes in Computer Science*, 2495:500–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL `http://link.springer.de/link/service/series/0558/bibs/`

2495/24950500.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950500.pdf.

Hammad:2003:BSU

[52] Ahmed Hammad, Bruno Tatibouët, Jean-Christophe Voisinet, and Weiping Wu. From a B specification to UML StateChart diagrams. *Lecture Notes in Computer Science*, 2495:511–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950511.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950511.pdf.

Miao:2003:FUM

[53] Huaikou Miao, Ling Liu, and Li Li. Formalizing UML models with Object-Z. *Lecture Notes in Computer Science*, 2495:523–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950523.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950523.pdf.

Liu:2003:UTS

[54] Zhiming Liu, Xiaoshan Li, and Jifeng He. Using transition systems to unify UML models. *Lecture Notes in Computer Science*, 2495:535–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950535.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950535.pdf.

Kim:2003:FMA

[55] Soon-Kyeong Kim and David Carrington. A formal metamodeling approach to a transformation between the UML state machine and Object-Z. *Lecture Notes in Computer Science*, 2495:548–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950548.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950548.pdf.

Bordbar:2003:UAD

[56] Behzad Bordbar, John Derrick, and Gill Waters. A UML approach to the design of open distributed systems. *Lecture Notes in Computer Science*, 2495:561–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950561.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950561.pdf.

Shankar:2003:SMR

[57] Subash Shankar. A semantic model of real-time UML. *Lecture Notes in Computer Science*, 2495:573–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950573.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950573.pdf.

Ming:2003:ROO

[58] Zhong Ming, Shi xian Li, and Xiu rong Fang. Research on ontology-

oriented domain analysis on MIS. *Lecture Notes in Computer Science*, 2495: 578–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950578.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950578.pdf.

Gan:2003:RDM

[59] Zaobin Gan, Chuanbo Chen, and Xiandeng Pei. A requirements description model based on conditional directed graphs. *Lecture Notes in Computer Science*, 2495:583–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950583.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950583.pdf.

Smith:2003:IRS

[60] Graeme Smith. Introducing reference semantics via refinement. *Lecture Notes in Computer Science*, 2495: 588–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950588.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950588.pdf.

Zhu:2003:SCN

[61] Huibiao Zhu, Jonathan P. Bowen, and Jifeng He. Soundness, completeness and non-redundancy of operational semantics for Verilog based on denotational semantics. *Lecture Notes in Computer Science*, 2495:600–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950600.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950600.pdf.

Sherif:2003:TTM

[62] Adnan Sherif and Jifeng He. Towards a time model for *Circus*. *Lecture Notes in Computer Science*, 2495: 613–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/bibs/2495/24950613.htm; http://link.springer.de/link/service/series/0558/papers/2495/24950613.pdf.

Anonymous:2003:AIg

[63] Anonymous. Author index. *Lecture Notes in Computer Science*, 2495: 625–??, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.de/link/service/series/0558/papers/2495/2495auth.pdf.

Bellare:2003:FSP

[64] Mihir Bellare and Bennet Yee. Forward-security in private-key cryptography. *Lecture Notes in Computer Science*, 2612:1–18, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dodis:2003:IRP

[65] Yevgeniy Dodis, Matt Franklin, Jonathan Katz, Atsuko Miyaji, and Moti Yung. Intrusion-resilient public-key encryption. *Lecture Notes in Computer Science*, 2612:19–32, 2003. CODEN

LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kurosawa:2003:TTK

[66] Kaoru Kurosawa and Tetsu Iwata. TMAC: Two-key CBC MAC. *Lecture Notes in Computer Science*, 2612:33–49, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Whiting:2003:MPH

[67] Douglas L. Whiting and Michael J. Sabin. Montgomery prime hashing for message authentication. *Lecture Notes in Computer Science*, 2612:50–67, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Lee:2003:APS

[68] Jung-Yeun Lee, Jung Hee Cheon, and Seungjoo Kim. An analysis of proxy signatures: Is a secure channel necessary? *Lecture Notes in Computer Science*, 2612:68–79, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Galbraith:2003:IAU

[69] Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmer signatures. *Lecture Notes in Computer Science*, 2612:80–97, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boneh:2003:SSS

[70] Dan Boneh, Ilya Mironov, and Victor Shoup. A secure signature scheme from bilinear maps. *Lecture Notes in Computer Science*, 2612:98–110, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smart:2003:ACU

[71] Nigel P. Smart. Access control using pairing based cryptography. *Lecture Notes in Computer Science*, 2612: 111–121, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Hoffstein:2003:NDS

[72] Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joseph H. Silverman, and William Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. *Lecture Notes in Computer Science*, 2612:122–140, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Courtois:2003:AXA

[73] Nicolas T. Courtois and Jacques Patarin. About the XL algorithm over $GF(2)$. *Lecture Notes in Computer Science*, 2612:141–157, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Bertoni:2003:EAA

[74] Guido Bertoni, Jorge Guajardo, Sandeep Kumar, Gerardo Orlando, Christof Paar, and Thomas Wollinger. Efficient $GF(p^m)$ arithmetic architectures for cryptographic applications. *Lecture Notes in Computer Science*, 2612: 158–175, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Xiao:2003:HPC

[75] Lu Xiao and Howard M. Heys. Hardware performance characterization of block cipher structures. *Lecture Notes in Computer Science*, 2612:176–192, 2003. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ding:2003:SIB

[76] Xuhua Ding and Gene Tsudik. Simple identity-based cryptography with mediated RSA. *Lecture Notes in Computer Science*, 2612:193–210, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Malone-Lee:2003:TBO

[77] John Malone-Lee and Wenbo Mao. Two birds one stone: Signcryption using RSA. *Lecture Notes in Computer Science*, 2612:211–225, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Berson:2003:CAB

[78] Tom Berson. Cryptography after the bubble: How to make an impact on the world. *Lecture Notes in Computer Science*, 2612:226, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kim:2003:RCC

[79] Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng. Rethinking chosen-ciphertext security under Kerckhoffs' assumption. *Lecture Notes in Computer Science*, 2612:227–243, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Moller:2003:PSP

[80] Bodo Möller. Provably secure public-key encryption for length-preserving Chaumian mixes. *Lecture Notes in Computer Science*, 2612:244–262, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

DArco:2003:FTD

[81] Paolo D'Arco and Douglas R. Stinson. Fault tolerant and distributed broadcast encryption. *Lecture Notes in Computer Science*, 2612:263–280, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Wang:2003:SGP

[82] Huaxiong Wang and Josef Pieprzyk. Shared generation of pseudo-random functions with cumulative maps. *Lecture Notes in Computer Science*, 2612: 281–294, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Goodrich:2003:ADS

[83] Michael T. Goodrich, Roberto Tamassia, Nikos Triandopoulos, and Robert Cohen. Authenticated data structures for graph and geometric searching. *Lecture Notes in Computer Science*, 2612: 295–313, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Jakobsson:2003:FMT

[84] Markus Jakobsson, Tom Leighton, Silvio Micali, and Michael Szydlo. Fractal Merkle tree representation and traversal. *Lecture Notes in Computer Science*, 2612:314–326, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Shamir:2003:RS

[85] Adi Shamir. RSA shortcuts. *Lecture Notes in Computer Science*, 2612:327, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okeya:2003:WNM

[86] Katsuyuki Okeya and Tsuyoshi Takagi. The width-w NAF method provides small memory and fast elliptic scalar multiplications secure against side channel attacks. *Lecture Notes in Computer Science*, 2612:328–342, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Montgomery:2003:FEC

[87] Peter L. Montgomery, Kirsten Eisenträger, and Kristin Lauter. Fast elliptic curve arithmetic and improved Weil pairing evaluation. *Lecture Notes in Computer Science*, 2612:343–354, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Xu:2003:TEP

[88] Shouhuai Xu and Ravi Sandhu. Two efficient and provably secure schemes for server-assisted threshold signatures. *Lecture Notes in Computer Science*, 2612:355–372, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Gennaro:2003:SAP

[89] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure applications of Pedersen's distributed key generation protocol. *Lecture Notes in Computer Science*, 2612:373–390, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Walter:2003:STM

[90] Colin D. Walter. Seeing through MIST given a small fraction of an RSA private key. *Lecture Notes in Computer Science*, 2612:391–402, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Crepeau:2003:SBR

[91] Claude Crépeau and Alain Slakmon. Simple backdoors for RSA key generation. *Lecture Notes in Computer Science*, 2612:403–416, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Anonymous:2003:FM

[92] Anonymous. Front matter. *Lecture Notes in Computer Science*, 2656: i–xiv, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/bfm:978-3-540-39200-2/1.pdf.

Joux:2003:CEM

[93] Antoine Joux. Cryptanalysis of the EMD mode of operation. *Lecture Notes in Computer Science*, 2656:1–16, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_1.pdf.

Junod:2003:OLD

[94] Pascal Junod. On the optimality of linear, differential, and sequential distinguishers. *Lecture Notes in Computer Science*, 2656:17–32, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_2.pdf.

Biryukov:2003:TCL

[95] Alex Biryukov, Christophe De Cannière, An Braeken, and Bart Preneel. A toolbox for cryptanalysis: Linear and affine

equivalence algorithms. *Lecture Notes in Computer Science*, 2656:33–50, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_3.pdf.

Fitzi:2003:TTB

[96] Matthias Fitzi, Martin Hirt, Thomas Holenstein, and Jürg Wullschleger. Two-threshold broadcast and detectable multi-party computation. *Lecture Notes in Computer Science*, 2656:51–67, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_4.pdf.

Canetti:2003:LUC

[97] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *Lecture Notes in Computer Science*, 2656:68–86, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_5.pdf.

Pinkas:2003:FST

[98] Benny Pinkas. Fair secure two-party computation. *Lecture Notes in Computer Science*, 2656:87–105, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_6.pdf.

Gaj:2003:FME

[99] Kris Gaj and Arkadiusz Orłowski. Facts and myths of Enigma: Breaking stereotypes. *Lecture Notes in Computer Science*, 2656:106–122, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_7.pdf.

Zhao:2003:RZK

[100] Yunlei Zhao, Xiaotie Deng, C. H. Lee, and Hong Zhu. Resettable zero-knowledge in the weak public-key model. *Lecture Notes in Computer Science*, 2656:123–139, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_8.pdf.

Micciancio:2003:SCE

[101] Daniele Micciancio and Erez Petrank. Simulatable commitments and efficient concurrent zero-knowledge. *Lecture Notes in Computer Science*, 2656:140–159, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_9.pdf.

Pass:2003:SQP

[102] Rafael Pass. Simulation in quasi-polynomial time, and its application to protocol composition. *Lecture Notes in Computer Science*, 2656:160–176, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_10.pdf.

Garay:2003:SZK

[103] Juan A. Garay, Philip MacKenzie, and Ke Yang. Strengthening zero-knowledge protocols using signatures. *Lecture Notes in Computer Science*,

2656:177–194, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_11.pdf.

Hast:2003:NOS

[104] Gustav Hast. Nearly one-sided tests and the Goldreich–Levin predicate. *Lecture Notes in Computer Science*, 2656: 195–210, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_12.pdf.

Katz:2003:ENM

[105] Jonathan Katz. Efficient and non-malleable proofs of plaintext knowledge and applications. *Lecture Notes in Computer Science*, 2656:211–228, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_13.pdf.

Augot:2003:PKE

[106] Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. *Lecture Notes in Computer Science*, 2656:229–240, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_14.pdf.

Lindell:2003:SCC

[107] Yehuda Lindell. A simpler construction of CCA2-secure public-key encryption under general assumptions. *Lecture Notes in Computer Science*, 2656: 241–254, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_15.pdf.

Canetti:2003:FSP

[108] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. *Lecture Notes in Computer Science*, 2656:255–271, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_16.pdf.

Gentry:2003:CBE

[109] Craig Gentry. Certificate-based encryption and the certificate revocation problem. *Lecture Notes in Computer Science*, 2656:272–293, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_17.pdf.

vonAhn:2003:CUH

[110] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford. CAPTCHA: Using hard AI problems for security. *Lecture Notes in Computer Science*, 2656:294–311, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_18.pdf.

Dodis:2003:CAA

[111] Yevgeniy Dodis and Jee Hea An. Concealment and its applications to authenticated encryption. *Lecture Notes in Computer Science*, 2656:312–329, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL

http://link.springer.com/content/pdf/10.1007/3-540-39200-9_19.pdf.

Ekdahl:2003:PSG

[112] Patrik Ekdahl, Willi Meier, and Thomas Johansson. Predicting the shrinking generator with fixed connections. *Lecture Notes in Computer Science*, 2656:330–344, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_20.pdf.

Courtois:2003:AAS

[113] Nicolas T. Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. *Lecture Notes in Computer Science*, 2656:345–359, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_21.pdf.

Lercier:2003:CPE

[114] Reynald Lercier and David Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. *Lecture Notes in Computer Science*, 2656:360–373, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_22.pdf.

Hess:2003:GAR

[115] Florian Hess. The GHS attack revisited. *Lecture Notes in Computer Science*, 2656:374–387, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_23.pdf.

Ciet:2003:IAE

[116] Mathieu Ciet, Tanja Lange, Francesco Sica, and Jean-Jacques Quisquater. Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms. *Lecture Notes in Computer Science*, 2656:388–400, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_24.pdf.

Goh:2003:SSS

[117] Eu-Jin Goh and Stanisław Jarecki. A signature scheme as secure as the Diffie–Hellman problem. *Lecture Notes in Computer Science*, 2656:401–415, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_25.pdf.

Boneh:2003:AVE

[118] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. *Lecture Notes in Computer Science*, 2656:416–432, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_26.pdf.

Szydlo:2003:HLR

[119] Michael Szydlo. Hypercubic lattice reduction and analysis of GGH and NTRU signatures. *Lecture Notes in Computer Science*, 2656:433–448, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_27.pdf.

Stern:2003:WPS

[120] Jacques Stern. Why provable security matters? *Lecture Notes in Computer Science*, 2656:449–461, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_28.pdf.

Fouque:2003:SR

[121] Pierre-Alain Fouque and Guillaume Poupard. On the security of RDSA. *Lecture Notes in Computer Science*, 2656:462–476, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_29.pdf.

Lee:2003:CPK

[122] Eonkyung Lee and Je Hong Park. Cryptanalysis of the public-key encryption based on braid groups. *Lecture Notes in Computer Science*, 2656:477–490, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_30.pdf.

Bellare:2003:TTR

[123] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. *Lecture Notes in Computer Science*, 2656:491–506, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_31.pdf.

DiRaimondo:2003:PST

[124] Mario Di Raimondo and Rosario Gennaro. Provably secure threshold password-authenticated key exchange. *Lecture Notes in Computer Science*, 2656:507–523, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_32.pdf.

Gennaro:2003:FPB

[125] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. *Lecture Notes in Computer Science*, 2656:524–543, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_33.pdf.

Maurer:2003:SMR

[126] Ueli Maurer and Krzysztof Pietrzak. The security of many-round Luby–Rackoff pseudo-random permutations. *Lecture Notes in Computer Science*, 2656:544–561, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_34.pdf.

Renner:2003:NBS

[127] Renato Renner and Stefan Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. *Lecture Notes in Computer Science*, 2656:562–577, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_35.pdf.

Katz:2003:REM

[128] Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Round efficiency of multi-

party computation with a dishonest majority. *Lecture Notes in Computer Science*, 2656:578–595, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_36.pdf.

Cramer:2003:EMP

[129] Ronald Cramer, Serge Fehr, Yuval Ishai, and Eyal Kushilevitz. Efficient multi-party computation over rings. *Lecture Notes in Computer Science*, 2656:596–613, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_37.pdf.

Bellare:2003:FGS

[130] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. *Lecture Notes in Computer Science*, 2656:614–629, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_38.pdf.

Kiayias:2003:EGS

[131] Aggelos Kiayias and Moti Yung. Extracting group signatures from traitor tracing schemes. *Lecture Notes in Computer Science*, 2656:630–648, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/10.1007/3-540-39200-9_39.pdf.

Anonymous:2003:BM

[132] Anonymous. Back matter. *Lecture Notes in Computer Science*, 2656:649, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://link.springer.com/content/pdf/bbm:978-3-540-39200-2/1.pdf.

Shamir:2003:FLN

[133] Adi Shamir and Eran Tromer. Factoring large numbers with the TWIRL device. *Lecture Notes in Computer Science*, 2729:1–26, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Blomer:2003:NPK

[134] Johannes Blömer and Alexander May. New partial key exposure attacks on RSA. *Lecture Notes in Computer Science*, 2729:27–43, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Faugere:2003:ACH

[135] Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases. *Lecture Notes in Computer Science*, 2729:44–60, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Vadhan:2003:CLC

[136] Salil P. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. *Lecture Notes in Computer Science*, 2729:61–77, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Renner:2003:UAP

[137] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. *Lecture Notes in Computer Science*, 2729:78–95, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Naor:2003:CAC

[138] Moni Naor. On cryptographic assumptions and challenges. *Lecture Notes in Computer Science*, 2729:96–109, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Katz:2003:SPA

[139] Jonathan Katz and Moti Yung. Scalable protocols for authenticated group key exchange. *Lecture Notes in Computer Science*, 2729:110–125, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Camenisch:2003:PVE

[140] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. *Lecture Notes in Computer Science*, 2729: 126–144, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ishai:2003:EOT

[141] Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank. Extending oblivious transfers efficiently. *Lecture Notes in Computer Science*, 2729:145–161, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Armknecht:2003:AAC

[142] Frederik Armknecht and Matthias Krause. Algebraic attacks on combiners with memory. *Lecture Notes in Computer Science*, 2729:162–175, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Courtois:2003:FAA

[143] Nicolas T. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. *Lecture Notes in Computer Science*, 2729:176–194, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Biryukov:2003:CS

[144] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of Safer++. *Lecture Notes in Computer Science*, 2729:195–211, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cheon:2003:PTA

[145] Jung Hee Cheon and Byungheup Jun. A polynomial time algorithm for the braid Diffie–Hellman conjugacy problem. *Lecture Notes in Computer Science*, 2729:212–225, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Howgrave-Graham:2003:IDF

[146] Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, and William Whyte. The impact of decryption failures on the security of NTRU encryption. *Lecture Notes in Computer Science*, 2729:226–246, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Damgaard:2003:UCE

[147] Ivan Damgård and Jesper Buus Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. *Lecture Notes in Computer Science*, 2729:247–264, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canetti:2003:UCJ

[148] Ran Canetti and Tal Rabin. Universal composition with joint state. *Lecture Notes in Computer Science*, 2729: 265–281, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Micciancio:2003:SZK

[149] Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. *Lecture Notes in Computer Science*, 2729:282–298, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barak:2003:DC

[150] Boaz Barak, Shien Jin Ong, and Salil Vadhan. Derandomization in cryptography. *Lecture Notes in Computer Science*, 2729:299–315, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pass:2003:DCR

[151] Rafael Pass. On deniability in the common reference string and random oracle model. *Lecture Notes in Computer Science*, 2729:316–337, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cheng:2003:PPO

[152] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. *Lecture Notes in Computer Science*, 2729:338–348, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Rubin:2003:TBC

[153] Karl Rubin and Alice Silverberg. Torus-based cryptography. *Lecture Notes in Computer Science*, 2729:349–365, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Komano:2003:EUP

[154] Yuichi Komano and Kazuo Ohta. Efficient universal padding techniques for multiplicative trapdoor one-way permutation. *Lecture Notes in Computer Science*, 2729:366–382, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Boyen:2003:MIB

[155] Xavier Boyen. Multipurpose identity-based signcryption: A Swiss Army knife for identity-based cryptography. *Lecture Notes in Computer Science*, 2729: 383–399, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Krawczy:2003:SSM

[156] Hugo Krawczy. SIGMA: The "SIGn-and-MAc" approach to authenticated Diffie–Hellman and its use in the IKE protocols. *Lecture Notes in Computer Science*, 2729:400–425, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dwork:2003:MBF

[157] Cynthia Dwork, Andrew Goldberg, and Moni Naor. On memory-bound functions for fighting spam. *Lecture Notes in Computer Science*, 2729:426–444, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Buchbinder:2003:LUB

[158] Niv Buchbinder and Erez Petrank. Lower and upper bounds on obtaining history independence. *Lecture Notes in Computer Science*, 2729:445–462, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ishai:2003:PCS

[159] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. *Lecture Notes in Computer Science*, 2729: 463–481, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Halevi:2003:TEM

[160] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. *Lecture Notes in Computer Science*, 2729: 482–499, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cary:2003:MAC

[161] Matthew Cary and Ramarathnam Venkatesan. A message authentication code based on unimodular matrix groups. *Lecture Notes in Computer Science*, 2729:500–512, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Patarin:2003:LRR

[162] Jacques Patarin. Luby–Rackoff: 7 rounds are enough for security. *Lecture Notes in Computer Science*, 2729: 513–529, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Horvitz:2003:WKA

[163] Omer Horvitz and Virgil Gligor. Weak key authenticity and the computational completeness of formal encryption. *Lecture Notes in Computer Science*, 2729: 530–547, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Herzog:2003:PAK

[164] Jonathan Herzog, Moses Liskov, and Silvio Micali. Plaintext awareness via key registration. *Lecture Notes in Computer Science*, 2729:548–564, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canetti:2003:RCC

[165] Ran Canetti, Hugo Krawczyk, and Jesper B. Nielsen. Relaxing chosen-ciphertext security. *Lecture Notes in Computer Science*, 2729:565–582, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Canvel:2003:PIS

[166] Brice Canvel, Alain Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. *Lecture Notes in Computer Science*, 2729:583–599, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barkan:2003:ICO

[167] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. *Lecture Notes in Computer Science*, 2729:600–616, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Oechslin:2003:MFC

[168] Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. *Lecture Notes in Computer Science*, 2729:617–630, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Stajano:2003:SCU

[169] Frank Stajano. The security challenges of ubiquitous computing. *Lecture Notes in Computer Science*, 2779:1, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Agrawal:2003:MCA

[170] Dakshi Agrawal, Josyula R. Rao, and Pankaj Rohatgi. Multi-channel attacks. *Lecture Notes in Computer Science*, 2779:2–16, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Karlof:2003:HMM

[171] Chris Karlof and David Wagner. Hidden Markov model cryptanalysis. *Lecture Notes in Computer Science*, 2779:17–34, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Ors:2003:PAA

[172] Sıddıka Berna Örs, Elisabeth Oswald, and Bart Preneel. Power-analysis attacks on an FPGA — first experimental results. *Lecture Notes in Computer Science*, 2779:35–50, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Geiselmann:2003:HSS

[173] Willi Geiselmann and Rainer Steinwandt. Hardware to solve sparse systems of linear equations over GF(2). *Lecture Notes in Computer Science*, 2779:51–61, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tsunoo:2003:CIC

[174] Yukiyasu Tsunoo, Teruo Saito, Tomoyasu Suzaki, Maki Shigeri, and Hiroshi Miyauchi. Cryptanalysis of DES implemented on computers with cache. *Lecture Notes in Computer Science*, 2779:62–76, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Piret:2003:DFA

[175] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. *Lecture Notes in Computer Science*, 2779:77–88, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Coron:2003:NAS

[176] Jean-Sébastien Coron and Alexei Tchulkine. A new algorithm for switching from arithmetic to Boolean masking. *Lecture Notes in Computer Science*, 2779:89–97, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Golic:2003:DNP

[177] Jovan D. Golić. DeKaRT: A new paradigm for key-dependent reversible circuits. *Lecture Notes in Computer Science*, 2779:98–112, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Karri:2003:PBC

[178] Ramesh Karri, Grigori Kuznetsov, and Michael Goessel. Parity-based concurrent error detection of substitution-permutation network block ciphers. *Lecture Notes in Computer Science*, 2779: 113–124, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Tiri:2003:SEA

[179] Kris Tiri and Ingrid Verbauwhede. Securing encryption algorithms against DPA at the logic level: Next generation Smart Card technology. *Lecture Notes in Computer Science*, 2779:125–136, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fournier:2003:SEA

[180] Jacques J. A. Fournier, Simon Moore, Huiyun Li, Robert Mullins, and George Taylor. Security evaluation of asynchronous circuits. *Lecture Notes in Computer Science*, 2779:137–151, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Epstein:2003:DIT

[181] Michael Epstein, Laszlo Hars, Raymond Krasinski, Martin Rosner, and Hao Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. *Lecture Notes in Computer Science*, 2779:152–165, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Barak:2003:TRN

[182] Boaz Barak, Ronen Shaltiel, and Eran Tromer. True random number generators secure in a changing environment. *Lecture Notes in Computer Science*, 2779:166–180, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dichtl:2003:HPO

[183] Markus Dichtl. How to predict the output of a hardware random number generator. *Lecture Notes in Computer Science*, 2779:181–188, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Reyhani-Masoleh:2003:LCB

[184] Arash Reyhani-Masoleh and M. Anwar Hasan. On low complexity bit parallel polynomial basis multipliers. *Lecture Notes in Computer Science*, 2779: 189–202, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Dhem:2003:EMR

[185] Jean-François Dhem. Efficient modular reduction algorithm in and its application to “left to right” modular multiplication in. *Lecture Notes in Computer Science*, 2779:203–213, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chevallier-Mames:2003:FDS

[186] Benoît Chevallier-Mames, Marc Joye, and Pascal Paillierinst. Faster double-size modular multiplication from Eu-

clidean multipliers. *Lecture Notes in Computer Science*, 2779:214–227, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Kwon:2003:EEC

[187] Soonhak Kwon, Chang Hoon Kim, and Chun Pyo Hong. Efficient exponentiation for a class of finite fields GF(2^n) determined by Gauss periods. *Lecture Notes in Computer Science*, 2779: 228–242, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Joye:2003:GFA

[188] Marc Joye and Pascal Paillier. GCD-free algorithms for computing modular inverses. *Lecture Notes in Computer Science*, 2779:243–253, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fouque:2003:AUR

[189] Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard. Attacking unbalanced RSA–CRT using SPA. *Lecture Notes in Computer Science*, 2779:254–268, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Fouque:2003:DAW

[190] Pierre-Alain Fouque and Frederic Valette. The doubling attack — why upwards is better than downwards. *Lecture Notes in Computer Science*, 2779: 269–280, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Smart:2003:AGR

[191] Nigel P. Smart. An analysis of Goubin's refined power analysis attack. *Lecture Notes in Computer Science*, 2779: 281–290, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Cathalo:2003:NTT

[192] Julien Cathalo, François Koeune, and Jean-Jacques Quisquater. A new type of timing attack: Application to GPS. *Lecture Notes in Computer Science*, 2779: 291–303, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Satoh:2003:UHA

[193] Akashi Satoh and Sumio Morioka. Unified hardware architecture for 128-bit block ciphers AES and Camellia. *Lecture Notes in Computer Science*, 2779: 304–318, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Chodowiec:2003:VCF

[194] Paweł Chodowiec and Kris Gaj. Very compact FPGA implementation of the AES algorithm. *Lecture Notes in Computer Science*, 2779:319–333, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Standaert:2003:EIR

[195] Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. Efficient implementation of Rijndael encryption in reconfigurable hardware: Improvements and design tradeoffs. *Lecture Notes in Computer Science*, 2779:334–350, 2003. CO-

DEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Pelzl:2003:HCC

[196] Jan Pelzl, Thomas Wollinger, Jorge Guajardo, and Christof Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. *Lecture Notes in Computer Science*, 2779: 351–365, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Avanzi:2003:CAD

[197] Roberto M. Avanzi. Countermeasures against differential power analysis for hyperelliptic curve cryptosystems. *Lecture Notes in Computer Science*, 2779: 366–381, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Itoh:2003:PCA

[198] Kouichi Itoh, Tetsuya Izu, and Masahiko Takenaka. A practical countermeasure against address-bit differential power analysis. *Lecture Notes in Computer Science*, 2779:382–396, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Okeya:2003:MFC

[199] Katsuyuki Okeya and Tsuyoshi Takagi. A more flexible countermeasure against side channel attacks using window method. *Lecture Notes in Computer Science*, 2779:397–410, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Clulow:2003:SP

[200] Jolyon Clulow. On the security of PKCS #11. *Lecture Notes in Computer Science*, 2779:411–425, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).

Klima:2003:ARB

[201] Vlastimil Klíma, Ondrej Pokorný, and Tomá š Rosa. Attacking RSA-based sessions in SSL/TLS. *Lecture Notes in Computer Science*, 2779:426–440, 2003. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic).