

Publications by Stefan Lucks

Books and Chapters in Books

1. A. Weimerskirch, D. Westhoff, S. Lucks, E. Zenner, “Efficient Pairwise Authentication Protocols for Sensor Networks: Theory and Performance Analysis”, IEEE Press: “Sensor Network Operations”, September 2004.
2. C. Wolf, S. Lucks, P.-W. Yau (eds.), “Western European Workshop on Research in Cryptology”, GI-Edition - Lecture Notes in Informatics (LNI), P-74, Köllen Verlag (2005), ISSN 1617-5468, ISBN 3-88579-403-9.

Fully Refereed International Publications

3. S. Lucks, “How to Exploit the Intractability of Exact TSP for Cryptography”, Fast Software Encryption '94, Springer LNCS 1008, 1994, 298–304.
4. S. Lucks, “How Traveling Salespersons Prove their Identity”, Fifth IMA Conference on Cryptography and Coding, Springer LNCS 1025, 1995, 142–149.
5. S. Lucks, “Faster Luby-Rackoff Ciphers”, Fast Software Encryption '96, Springer LNCS 1039, 1996, 189–203.
6. S. Lucks, “BEAST: A fast block cipher for arbitrary block sizes”, Proc. IFIP'96, Conference on Communication and Multimedia Security (ed. P. Horster), Chapman & Hall, 1996, 144–153.
7. S. Lucks, “On the Security of Remotely Keyed Encryption”, Fast Software Encryption '97, Springer LNCS 1267, 219–229.
8. S. Lucks, “Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys”, Security Protocols: 5th international workshop 1997, Springer LNCS 1361, 79–90.
9. S. Lucks, “Attacking Triple Encryption”, Fast Software Encryption '98, Springer LNCS 1372, Springer, 1998, 239–253.
10. R. Weis, S. Lucks, “The Performance of Modern Block Ciphers in JAVA”, Smart Card, Research and Applications, 3rd international conference, CARDIS '98, Springer LNCS 1820.
11. S. Lucks, R. Weis, V. Hilt, “Fast Encryption for Set-Top Technologies”, Multimedia Computing and Networking '99, Proceedings of SPIE, Vol. 3654, 84–94.
12. S. Lucks, “On the Security of the 128-bit Block Cipher DEAL”, Fast Software Encryption '99, Springer LNCS 1636, 60–70.

13. S. Lucks, "Accelerated Remotely Key Encryption", Fast Software Encryption '99, Springer LNCS 1636, 112–123.
14. S. Lucks, R. Weis, "Remotely Keyed Encryption Using Non-Encrypting Smart Cards", USENIX Workshop on Smartcard Technology, USENIX Association, 1999.
15. S. Lucks, "Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys", AES3: The Third Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (2000).
16. S. Lucks, "The Sum of PRPs is a Secure PRF", Eurocrypt 2000, Springer LNCS 1807, 470–484.
17. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting, "Improved Cryptanalysis of Rijndael", Fast Software Encryption 2000, Springer LNCS 1978, 213–230.
18. R. Weis, W. Effelsberg, S. Lucks, "Remotely Keyed Encryption with Java Cards: A Secure and Efficient Method to Encrypt Multimedia Streams", IEEE International Conference on Multimedia and Expo (2000).
19. S. Lucks, R. Weis, "How to Make DES-Based Smartcards fit for the 21-st Century" Proceedings of IFIP CARDIS 2000, Kluwer Academic Publisher.
20. R. Weis, W. Effelsberg, S. Lucks, "Combining Authentication and Light-Weight Payment for Active Networks", Proceedings of Smartnet 2000, Kluwer (2000).
21. R. Weis, J. Vogel, W. Effelsberg, W. Geyer, S. Lucks, "How to Make a Digital Whiteboard Secure - Using JAVA-Cards for Multimedia Application", Proc. of 7th Workshop on Interactive Distributed Multimedia Systems and Telecommunication Services, IDMS 2000.
22. R. Weis, B. Bakker, S. Lucks, "Security on your hand: Secure File Systems with a "non-cryptographic" JAVA-Ring", Java on Smart Cards: Programming and Security, First International Workshop, JavaCard 2000, Springer LNCS 2041.
23. M. Krause, S. Lucks, "On the Minimal Hardware Complexity of Pseudorandom Function Generators", 18th Annual Symposium of Theoretical Aspects of Computer Science (STACS), 2001, Springer LNCS 2010, 419-430.
24. S. Lucks, "The Saturation Attack - a Bait for Twofish", Fast Software Encryption 2001, Springer LNCS 2355.
25. P. Crowley, S. Lucks "Bias in the LEVIATHAN Stream Cipher", Fast Software Encryption 2001, Springer LNCS 2355.

26. E. Zenner, M. Krause, S. Lucks, “Improved Cryptanalysis of the Self-Shrinking Generator”, Information Security and Privacy, 6th Australasian Conference, ACISP 2001, Springer LNCS 2119.
27. S. Fluhrer, S. Lucks, “Analysis of the E_0 Encryption System”, Selected Areas in Cryptography, 2001, Springer LNCS.
28. M. Krause, S. Lucks, “Pseudorandom Functions in TC^0 and Cryptographic Limitations of Proving Lower Bounds”, Journal of Computational Complexity, Volume 10 , Issue 4 (May 2002), Pages: 297 – 313.
29. S. Lucks, “A Variant of the Cramer-Shoup Cryptosystem for Groups of Unknown Order”, Asiacrypt 2002, Springer LNCS 2501.
30. S. Lucks, R. Weis, “How to turn a PIN into an Iron Beam – A patent-free and practical protocol for secure communication using a weak common secret”, 18th IFIP International Information Security Conference, 2003.
31. N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, T. Kohno, “Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive”, Fast Software Encryption 2003, Springer LNCS.
32. S. Lucks, “Ciphers Secure Against Related-Key Attacks” Fast Software Encryption 2004, Springer LNCS.
33. F. Armknecht, S. Lucks, “Linearity of the AES key schedule”, Fourth Conference on the Advanced Encryption Standard (AES) ’AES - State of the Crypto Analysis’, 2004, Springer LNCS.
34. S. Lucks, “Two-Pass Authenticated Encryption faster than Generic Composition”, Fast Software Encryption 2005, Springer LNCS 3557.
35. E. Tatli, D. Stegemann, S. Lucks, “Security Challenges in Mobile Commerce”, Second IEEE International Workshop on Mobile Commerce and Services (WM-CS’05), 2005.
36. S. Lucks, N. Schmoigl, E. Tatli, “Issues on Designing a Cryptographic Compiler”, WEWoRC 2005, Springer LNI, ISBN 3-88579-403-9.
37. U. Kuehn, K. Kursawe, S. Lucks, A.-R. Sadeghi, C. Stueble, “Secure Data Management in Trusted Computing”, Cryptographic Hardware and Embedded Systems (CHES) 2005, Springer LNCS 3659.
38. S. Lucks, “A Failure-Friendly Design Principle for Hash Functions”, Asiacrypt 2005, Springer LNCS 3788.

39. Z. Benenson, E. Hammerschmidt, F. Freiling, S. Lucks, L. Pimenidis, “Tampering with Motes: Real-World Attacks on Sensor Networks”, accepted for 3rd International Conference on Security in Pervasive Computing (SPC).
40. Z. Benenson, E. Hammerschmidt, F. Freiling, S. Lucks, L. Pimenidis, “Authenticated Query Flooding in Sensor Networks”, accepted for 21st IFIP International Information Security Conference SEC 2006.
41. J. Kelsey, S. Lucks, “Collisions and Near-Collisions for Reduced-Round TIGER”, accepted for Fast Software Encryption 2006, Springer LNCS.

Fully Refereed National Publications

42. S. Lucks, E. Zenner, A. Weimerskirch, D. Westhoff “Entity Recognition for Sensor Network Motes (Extended Abstract)”, Vol. 2, Proceedings of INFORMATIK 2005 – the 35th Annual Conference of the Gesellschaft für Informatik e.V. (GI), page 145–149, Lecture Notes in Informatics (LNI), Vol. P-68, ISBN 3-88579-379-0.

International Publications, Refereed by Abstract

43. B. Bakker, R. Weis, S. Lucks, “How to Ring a Swan – Adding Tamper Resistant Authentication to Linux IPsec”, SANE 2000 – 2nd International System Administration and Networking Conference (2000).
44. R. Weis, S. Lucks, “All your key bits belong to us, the true story of black box cryptography”, SANE 2002, Maastricht, 2002.
45. A. Bock, S. Lucks, R. Weis, “TCG 1.2 – fair play with the ‘Fritz’ chip?”, SANE 2004.
46. S. Lucks, R. Weis, “Cryptographic Hash Functions – Recent Results on Cryptanalysis and their Implications on System Security”, accepted for SANE 2006.

Selected Journal Publications in German

47. R. Weis, S. Lucks, “Sicherheitsprobleme bei Authentifizierung und Verschlüsselung in GSM-Netzen”, in Datenschutz und Datensicherheit, DuD 09/98, Vieweg, 1998.
48. R. Weis, S. Lucks, “KEA”, in Datenschutz und Datensicherheit, DuD 10/98, Vieweg, 1998.
49. R. Weis, S. Lucks, “Advanced Encryption Standard”, in Datenschutz und Datensicherheit, DuD 10/99, Vieweg, 1999.

50. R. Weis, S. Lucks, "Sichere, Standardisierte, Symmetrische Verschlüsselung auf Basis von DES und AES", Praxis der Informationsverarbeitung und Kommunikation, PIK 12/99.
51. R. Weis, S. Lucks, W. Geyer, "Stand der Faktorisierungsforschung", in Datenschutz und Datensicherheit, DuD 03/00, Vieweg, 2000.
52. E. Zenner, R. Weis, S. Lucks, "Sicherheit des GSM-Verschlüsselungsstandard A5", in Datenschutz und Datensicherheit, DuD 07/00, Vieweg, 2000.
53. R. Weis, S. Lucks, "Die dritte AES Konferenz in New York", in Datenschutz und Datensicherheit, DuD 07/00, Vieweg, 2000.
54. R. Weis, S. Lucks, "Standardmäßige Wave-LAN Unsicherheit", in Datenschutz und Datensicherheit, DuD 25/01, Vieweg, 2001.
55. S. Lucks, R. Weis, "Neue Ergebnisse zur Sicherheit des Verschlüsselungsstandards AES", Datenschutz und Datensicherheit, DuD 11/02, Vieweg, 2002.
56. R. Weis, S. Lucks, A. Bogk, "Sicherheit von 1024bit RSA Schlüsseln gefährdet", Datenschutz und Datensicherheit, DuD 06/2003, Vieweg, 2003.
57. R. Weis, S. Lucks, "Hashfunktionen gebrochen", Datenschutz und Datensicherheit, DuD 04/2005, Vieweg, 2005.

Doctoral Thesis

58. S. Lucks, "Systematische Entwurfsmethoden für praktikable Kryptosysteme", Cuvillier Verlag, Göttingen, 1997, Dissertation, Universität Göttingen.