Complete Publication List Ulrich Rührmair (as of September 2019)

Journals

1. U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, G. Csaba: *Applications of High-Capacity Crossbar Memories in Cryptography*. ***IEEE Transactions on Nanotechnology***, 2011.
2. C. Jaeger, M. Algasinger, U. Rührmair, G. Csaba, M. Stutzmann: *Random p-n-junctions for physical cryptography.* ***Applied Physics Letters*** 96 (172103), 2010.
3. H. Langhuth, S. Frederic, M. Kaniber, J. Finley, U. Rührmair: *Strong Photoluminescence Enhancement from Colloidal Quantum Dot Near Silver Nano-Island Films*. Journal of Fluorescence, 2010.
4. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, M. Stutzmann, U. Rührmair: *Circuit-based Approaches to SIMPL Systems.* Journal of Circuits, Systems and Computers, 2011.
5. P. Lugli, A. Mahmoud, M. Algasinger, M. Stutzmann, G. Csaba, U. Rührmair: *Physical Unclonable Functions based on Crossbar Arrays for Cryptographic Applications*. International Journal of Circuit Theory and Applications, 2013.
6. U. Rührmair, M. van Dijk: *On the Practical Use of Physical Unclonable Functions in Oblivious Transfer and Bit Commitment Protocols.* Journal of Cryptographic Engineering, 2013.
7. U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas: *PUF Modeling Attacks on Simulated and Silicon Data*. ***IEEE Transactions on Information Forensics and Security***, 2013.
8. P.H. Nguyen, D.P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, M. van Dijk: *The interpose puf: Secure puf design against state-of-the-art machine learning attacks*. IACR Transactions on CHES, 2019.

Conferences

9. Q. Chen, G. Csaba, X. Ju, S.B. Natarajan, P. Lugli, M. Stutzmann, U. Schlichtmann, U. Rührmair: *Analog Circuits for Physical Cryptography.* ISIC 2009. *(This paper received the Best Paper Award.)*
10. M. Steinebach, S. Zmudsinski, S. Katzenbeisser, U. Rührmair: *Audio watermarking forensics: detecting malicious re-embedding.* IS&T SPIE 2010.
11. U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, M. Stutzmann: *Security Applications of Diodes with Unique Current-Voltage Characteristics.* FC 2010.
12. G. Csaba, X. Ju, Z. Ma, Q. Chen, W. Porod, J. Schmidhuber, U. Schlichtmann, P. Lugli, U. Rührmair: *Application of Mismatched Cellular Nonlinear Networks for Physical Cryptography.* IEEE CNNA 2010.
13. U. Rührmair, Q. Chen, M. Stutzmann, P. Lugli, U. Schlichtmann, G. Csaba: *Towards Electrical, Integrated Implementations of SIMPL Systems.* WISTP 2010.
14. U. Rührmair, S. Katzenbeisser, M. Steinebach, S. Zmudzinski: *Watermark-Based Authentication and Key Exchange in Teleconferencing Systems.* CMS 2010.
15. U. Rührmair: *Oblivious Transfer based on Physical Unclonable Functions.* TRUST 2010.
16. F. Sehnke, C. Osendorfer, J. Sölter, J. Schmidhuber, U. Rührmair: *Policy Gradients for Cryptanalysis.* ICANN 2010.
17. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber: *Modeling Attacks on Physical Unclonable Functions.* ***ACM Conference on Computer and Communications Security (CCS)*** 2010.

18. U. Rührmair: *SIMPL Systems, Or: Can We Design Cryptographic Hardware without Secret Key Information?* SOFSEM 2011.
19. U. Rührmair, C. Jaeger, M. Algasinger: *An Attack on PUF-based Session Key Exchange, and a Hardware-based Countermeasure: Erasable PUFs.* FC 2011.
20. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *The Bistable Ring PUF: A New Architecture for Strong Physical Unclonable Functions.* HOST 2011. *(This paper was Best Paper Candidate.)*
21. Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, U. Rührmair: *Characterization of the Bistable Ring PUF.* DATE 2012.
22. U. Rührmair, M. van Dijk: *Practical Security Analysis of PUF-based Two-Player Protocols.* CHES 2012. *(This paper was Best Paper Candidate.* It was invited for subsequent submission to the Journal of Cryptographic Engineering as one of the best papers of CHES 2015.)
23. U. Rührmair, M. van Dijk: *PUFs in Security Protocols: Attack Models and Security Evaluations.* ***IEEE Symposium on Security and Privacy ("Oakland")*** 2013.
24. M. van Dijk, U. Rührmair: *Protocol Attacks on Advanced PUF Protocols and Countermeasures.* DATE 2014.
25. U. Rührmair, D. E. Holcomb: *PUFs at a Glance.* DATE 2014.
26. U. Rührmair, U. Schlichtmann, W. Burleson: *Special Session: How Secure are PUFs Really? On the Reach and Limits of Recent PUF Attacks.* DATE 2014.
27. U. Rührmair, J. Sölter: *PUF Modeling Attacks: An Introduction and Overview.* DATE 2014.
28. M. van Dijk, U. Rührmair: *PUF Interfaces and Their Security.* ISVLSI 2014.
29. U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, F. Koushanfar, W. Burleson: *Efficient Power and Timing Side Channels for Physical Unclonable Functions.* CHES 2014.
30. U. Rührmair, J.L. Martinez-Hurtado, X. Xu, C. Kraeh, C. Hilgers, D. Kononchuk, J. Finley, W. Burleson: *Virtual Proofs of Reality and Their Physical Implementation.* ***IEEE Symposium on Security and Privacy ("Oakland")*** 2015.
31. R. Horstmeyer, S. Assawaworrarit, U. Rührmair, C. Yang: *Physically secure and fully reconfigurable data storage using optical scattering.* HOST 2015
32. X. Xu, U. Rührmair, D. E. Holcomb, W. P. Burleson: *Security Evaluation and Enhancement of Bistable Ring PUFs*. RFIDSec 2015.
33. Q. Chen, U. Rührmair, S. Narayana, U. Sharif, U. Schlichtmann: *MWA Skew SRAM Based SIMPL Systems for Public-Key Physical Cryptography*. TRUST 2015.
34. S. Philippe, M. Kütt, M. McKeown, U. Rührmair, A. Glaser: *The Application of Virtual Proofs of Reality to Nuclear Safeguards and Arms Control Verifications*. INMM 2016.
35. M. Sauer, P. Raiola, L. Feiten, B. Becker, U. Rührmair, I. Polian: *Sensitized Path PUF: A Lightweight Embedded Physical Unclonable Function.* DATE 2017.
36. Chip-Hong Chang, Marten van Dijk, Farinaz Koushanfar, Ulrich Rührmair, Mark Tehranipoor: ASHES 2017: Workshop on Attacks and Solutions in Hardware Security. ***ACM Conference on Computer and Communications Security (CCS)*** 2017.
37. Chip-Hong Chang, Jorge Guajardo, Daniel Holcomb, Francesco Regazzoni, Ulrich Rührmair: ASHES 2018: Workshop on Attacks and Solutions in Hardware Security. ***ACM Conference on Computer and Communications Security (CCS)*** 2018.

Invited Book Chapters

38. U. Rührmair, H. Busch, S. Katzenbeisser: *Strong PUFs: Models, Constructions and Security Proofs.* In A.-R. Sadeghi, P. Tuyls (Editors): "Towards Hardware Intrinsic Security: Foundation and Practice". Springer 2010.

39. U. Rührmair, S. Devadas, F. Koushanfar: *Security based on Physical Unclonability and Disorder.* In M. Tehranipoor and C. Wang (Editors): "Introduction to Hardware Security and Trust". Springer 2011.
40. U. Rührmair: *SIMPL Systems as a Keyless Cryptographic and Security Primitive.* In: D. Naccache (Editor), Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday. Lecture Notes in Computer Science, Vol. 6805. Springer 2012.
41. U. Rührmair: *Disorder-based Security Hardware: An Overview.* In: Secure System Design and Trustable Computing, Chip Hong Chang and Miodrag Potkonjak (Ed.). Springer 2015.

Preprints

42. U. Rührmair: *SIMPL Systems: On a Public Key Variant of Physical Unclonable Functions.* Cryptology ePrint Archive, Report 2009/255, 2009.
43. U. Rührmair, J. Sölter, F. Sehnke: *On the Foundations of Physical Unclonable Functions.* Cryptology ePrint Archive, Report 2009/277, 2009.
44. U. Rührmair, Q. Chen, P. Lugli, M. Stutzmann, G. Csaba: *Towards Electrical, Integrated Implementations of SIMPL Systems.* Cryptology ePrint Archive, Report 2009/278, 2009.
45. G. Csaba, X. Ju, Q. Chen, W. Porod, J. Schmidhuber, U. Schlichtmann, P. Lugli, U. Rührmair: *On-Chip Electric Waves: An Analog Circuit Approach to Physical Unclonable Functions.* Cryptology ePrint Archive, Report 2009/246, 2009.
46. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber: *Modeling Attacks on Physical Unclonable Functions.* Cryptology ePrint Archive, Report 2010/251, 2010.
47. U. Rührmair: *Physical Turing Machines and the Formalization of Physical Cryptography.* Cryptology ePrint Archive, Report 2011/188, 2011.
48. U. Rührmair: *SIMPL Systems as a Keyless Cryptographic and Security Primitive.* Cryptology ePrint Archive, Report 2011/189, 2011.
49. M. van Dijk, U. Rührmair: *Physical Unclonable Functions in Cryptographic Protocols: Security Proofs and Impossibility Results.* Cryptology ePrint Archive, Report 2012/228, 2012.
50. U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas: *PUF Modeling Attacks on Simulated and Silicon Data*. Cryptology ePrint Archive, Report 2013/112, 2013.
51. U. Rührmair, C. Hilgers, S. Urban, A. Weiershäuser, E. Dinter, B. Forster, C. Jirauschek: *Optical PUFs Reloaded*. Cryptology ePrint Archive, Report 2013/215, 2013.
52. A. Mahmoud, U. Rührmair, M. Majzoobi, F. Koushanfar: *Combined Modeling and Side Channel Attacks on Strong PUFs.* Cryptology ePrint Archive, Report 2013/632, 2013.
53. U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, F. Koushanfar, W. Burleson: *Power and Timing Side Channels for PUFs and their Efficient Exploitation.* Cryptology ePrint Archive, Report 2013/851, 2013.
54. U. Rührmair: *Virtual Proofs of Reality.* Cryptology ePrint Archive, Report 2014/215, 2014.
55. Xiaolin Xu, Ulrich Rührmair, Daniel E. Holcomb, Wayne P. Burleson: *Security Evaluation and Enhancement of Bistable Ring PUFs*. Cryptology ePrint Archive, Report 2015/443, 2015.
56. Chenglu Jin, Xiaolin Xu, Wayne P. Burleson, Ulrich Rührmair, Marten van Dijk: *PLayPUF: Programmable Logically Erasable PUFs for Forward and Backward Secure Key Management.* Cryptology ePrint Archive, Report 2015/1052, 2015.
57. U. Rührmair: *On the Security of PUF Protocols under Bad PUFs and PUFs-inside-PUFs Attacks*. Cryptology ePrint Archive, Report 2016/322, 2016.
58. P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, M. van Dijk: *The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks.* IACR Cryptology ePrint Archive, Report 2018/350, 2018.

59. Y. Gao, C. Jin, J. Kim, H. Nili, X. Xu, W. Burleson, O. Kavehei, M. van Dijk, D. C. Ranasinghe, U. Rührmair: *Efficient Erasable PUFs from Programmable Logic and Memristors.* IACR Cryptology ePrint Archive, Report 2018/358, 2018.
60. U. Rührmair: *Towards Secret-Free Security.* IACR Cryptology ePrint Archive, Report 2019/388, 2019.

Editorials

61. Chip-Hong Chang, Ulrich Rührmair, Wei Zhang: *Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security, ASHES@CCS 2017, Dallas, TX, USA, November 3, 2017*. ACM 2017, ISBN 978-1-4503-5397-7.
62. Chip-Hong Chip, Ulrich Rührmair, Daniel Holcomb, Jorge Guajardo: *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security, ASHES@CCS 2018, Toronto, ON, Canada, October 19, 2018.* ACM 2018, ISBN 978-1-4503-5996-2.

Filed Patent Applications

As independent applicant and co-inventor, together with TU Munich:

63. European patent application Nr. 09 003 763.1
    Filing date: March 16, 2009
    Title: "System and method for security purposes"
64. European patent application Nr. 09 003 764.9
    Filing date: March 16, 2009
    Title: "Method for security purposes"
65. European patent application Nr. 09 157 043.2
    Filing date: March 31, 2009
    Title: "Method for security purposes"
66. European patent application Nr. 09 004 847.1
    Filing date: April 1, 2009
    Title: "SRAM for use in physical cryptography"
67. European patent application Nr. 09 157 041.6
    Filing date: March 31, 2009
    Title: "Method for security purposes"
68. European patent application Nr. 09 163 641.5
    Filing date: June 24, 2009
    Title: "Applications of High-Capacity Crossbar Memories in Cryptography"
69. European patent application Nr. 09 175 069.5
    Filing date: 04. November 2009
    Title: "System and method for security purposes"