Publications by Boris Škorić

[1] B. Škorić. Unclonable encryption revisited: 4x2=8, 2015. https://eprint.iacr.org/2015/1221.

[2] B. Škorić and W. de Groot. Generalized tally-based decoders for traitor tracing and group testing. In *IEEE Workshop on Information Forensics and Security (WIFS)*, 2015. https://eprint.iacr.org/2015/617.

[3] B. Škorić. Tally-based simple decoders for traitor tracing and group testing. *IEEE Transactions on Information Forensics and Security*, 2015. http://eprint.iacr.org/2014/781.

[4] A. Schaller, B. Škorić, and S. Katzenbeisser. On the systematic drift of physically unclonable functions due to aging. In *International Workshop on Trustworthy Embedded Devices (TrustED)*, 2015.

[5] A. Schaller, B. Škorić, and S. Katzenbeisser. Eliminating leakage in reverse fuzzy extractors, 2014. http://eprint.iacr.org/2014/741.

[6] B. Škorić, S.J.A. de Hoogh, and N. Zannone. Flow-based reputation with uncertainty: Evidence-Based Subjective Logic. *International Journal of Information Security*, 2014. http://arxiv.org/abs/1402.3319.

[7] S. Ibrahimi, B. Škorić, and J.-J. Oosterwijk. Riding the saddle point: asymptotics of the capacity-achieving simple decoder for bias-based traitor tracing. *EURASIP Journal on Information Security*, 2014:12, 2014.

[8] Boris Škorić and Niels de Vreede. The Spammed Code Offset Method. *IEEE Transactions on Information Forensics and Security*, 9(5):875–884, 2014.

[9] P.W.H. Pinkse, S.A. Goorden, M. Horstmann, B. Škorić, and A.P. Mosk. Quantum pattern recognition. In *International Quantum Electronics Conference (IQEC)*, page IA_3_6, 2013.

[10] Robbert van den Berg, Boris Škorić, and Vincent van der Leest. Bias-based modeling and entropy analysis of PUFs. In *international workshop on Trustworthy Embedded Devices (TrustED)*, pages 13–20. ACM, 2013.

[11] B. Škorić. Security analysis of Quantum-Readout PUFs in the case of challenge-estimation attacks, 2014. http://eprint.iacr.org/2013/479.

[12] B. Škorić, J.-J. Oosterwijk, and J. Doumen. The holey grail: A special score function for non-binary traitor tracing. In *Workshop on Information Forensics and Security (WIFS)*, pages 180–185. IEEE, 2013.

[13] B. Škorić, A.P. Mosk, and P.W.H. Pinkse. Security of Quantum-Readout PUFs against quadrature-based challenge-estimation attacks . *International Journal of Quantum Information*, 11(4):1350041–1 – 1350041–15, 2013.

[14] Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, Boris Škorić, and Pepijn W.H. Pinkse. Quantum-secure authentication of a physical unclonable key. *Optica*, 1(6):421–424, Dec 2014.

[15] Jan-Jaap Oosterwijk, Boris Škorić, and Jeroen Doumen. A capacity-achieving simple decoder for bias-based traitor tracing schemes, 2013. http://eprint.iacr.org/2013/389.

[16] J.-J. Oosterwijk, B. Škorić, and J. Doumen. Optimal suspicion functions for Tardos traitor tracing schemes. In *ACM Workshop on Information Hiding and Multimedia Security 2013*, pages 19–28.

[17] Antonino Simone and Boris Škorić. False Negative probabilities in Tardos codes. *Designs, Codes, and Cryptography*, 74(1):159–182, 2015.

[18] J.A. de Groot, B. Škorić, N. de Vreede, and J.-P.M.G. Linnartz. Diagnostic category leakage in helper data schemes for biometric authentication. In *SECRYPT*, pages 506–511. SciTePress, 2013.

[19] J. de Groot, B. Škorić, N. de Vreede, and J.-P. Linnartz. Quantization in continuous-source zero secrecy leakage helper data schemes, 2012. http://eprint.iacr.org/2012/566.

[20] A. Simone and B. Škorić. False Positive probabilities in q-ary Tardos codes: comparison of attacks. *Designs, Codes, and Cryptography*.

[21] A. Ranganathan, N.O. Tippenhauer, B. Škorić, D. Singelée, and S. Čapkun. Design and implementation of a terrorist fraud resilient distance bounding system. In *17th European Symposium on Research in Computer Security (ESORICS)*, volume 7459 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2012.

[22] Boris Škorić and Jan-Jaap Oosterwijk. Binary and q-ary Tardos codes, revisited. *Designs, Codes, and Cryptography*, 74(1):75–111, 2015.

[23] Dion Boesten and Boris Škorić. Asymptotic fingerprinting capacity in the Combined Digit Model. In *Information Hiding 2012*, pages 255–268. Springer. LNCS Vol. 7692.

[24] Antonino Simone, Boris Škorić, and Nicola Zannone. Flow-based reputation: more than just ranking. *International Journal of Information Technology & Decision Making*, 11(3):551–578, 2012.

[25] T. Laarhoven, J. Doumen, P. Roelse, B. Škorić, and B. de Weger. Dynamic Tardos traitor tracing schemes. *IEEE Transactions on Information Theory*, 59(7):4230–4242.

[26] Dion Boesten and Boris Škorić. Asymptotic fingerprinting capacity for non-binary alphabets. In *Information Hiding 2011*, volume 6958 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2011.

[27] Antonino Simone and Boris Škorić. Asymptotically false-positive-maximizing attack on non-binary tardos codes. In *Information Hiding 2011*, volume 6958 of *Lecture Notes in Computer Science*, pages 14–27. Springer, 2011.

[28] Antonino Simone and Boris Škorić. Accusation probabilities in Tardos codes: beyond the Gaussian approximation. *Designs, Codes and Cryptography*, 63(3):379–412, 2012.

[29] Boris Škorić. Quantum Readout of Physical Unclonable Functions. *International Journal of Quantum Information*, 10(1):1250001–1 – 125001–31, 2012.

[30] Boris Škorić. Quantum Readout of Physical Unclonable Functions. In Bernstein and Lange [31], pages 369–386.

[31] D.J. Bernstein and T. Lange, editors. *Progress in Cryptology - AFRICACRYPT 2010, 3rd Int. Conf. on Cryptology in Africa, Stellenbosch, South Africa, May 3-6, 2010. Proceedings*, volume 6055 of *LNCS*. Springer, 2010.

[32] Boris Škorić and Marc X. Makkes. Flowchart description of security primitives for controlled Physical Unclonable Functions. *International Journal of Information Security*, 9(5):327–335, 2010.

[33] Klaus Kursawe, Ahmad-Reza Sadeghi, Dries Schellekens, Boris Škorić, and Pim Tuyls. Reconfigurable Physical Unclonable Functions – enabling technology for tamper-resistant storage. In *2nd IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, pages 22–29. IEEE, 2009.

[34] B. Škorić, S. Katzenbeisser, H.G. Schaathun, and M.U. Celik. Tardos Fingerprinting Codes in the Combined Digit Model. *IEEE Transactions on Information Forensics and Security*, 6(3):906–919, 2011.

[35] Boris Škorić, Stefan Katzenbeisser, Hans Georg Schaathun, and Mehmet Celik. Tardos fingerprinting codes in the combined digit model (extended abstract). In *IEEE Workshop on Information Forensics and Security (WIFS) 2009*. IEEE Press, 2009.

[36] B. Škorić and P. Tuyls. An efficient fuzzy extractor for limited noise. In *Symposium on Information Theory in the Benelux*, pages 193–200, 2009.

[37] Sebastiaan de Hoogh, Berry Schoenmakers, Boris Skoric, and José Villegas. Verifiable rotation of homomorphic encryptions. In Stanislaw Jarecki and Gene Tsudik, editors, *Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 393–410. Springer, 2009.

[38] Evgeny A. Verbitskiy, Pim Tuyls, Chibuzo Obi, Berry Schoenmakers, and Boris Škorić. Key extraction from general nondiscrete signals. *IEEE Transactions on Information Forensics and Security*, 5(2):269–279, 2010.

[39] B. Škorić, C. Obi, E. Verbitskiy, and B. Schoenmakers. Sharp lower bounds on the extractable randomness from non-uniform sources. *Information and Computation*, 209:1184–1196, 2011.

[40] J. Guajardo, B. Škorić, P. Tuyls, S.S. Kumar, T. Bel, A.H.M. Blom, and G.J. Schrijen. Anti-counterfeiting, key distribution, and key storage in an ambient world via Physical Unclonable Functions. *Information Systems Frontiers*, 11(1):19–41, 2009.

[41] B. Škorić, T. Bel, A.H.M. Blom, B.R. de Jong, H. Kretschman, and A.J.M. Nellissen. Randomized resonators as uniquely identifiable anti-counterfeiting tags. In *Secure Component and System Identification (SECSI) Workshop*, 2008.

[42] Boris Škorić. On the entropy of keys derived from laser speckle; statistical properties of Gabor-transformed speckle. *Journal of Optics A: Pure and Applied Optics*, 10(5):055304–055316, 2008.

[43] Boris Škorić. Steganography from weak cryptography. `http://arxiv.org/abs/0804.0659`.

[44] Stefan Katzenbeisser, Boris Škorić, Mehmet Celik, and Ahmad-Reza Sadeghi. Combining Tardos fingerprinting codes and fingercasting. In *Information Hiding 2007*, pages 294–310. Springer, 2007. LNCS Vol. 4567/2008.

[45] Boris Škorić, Stefan Katzenbeisser, and Mehmet Utku Celik. Symmetric Tardos fingerprinting codes for arbitrary alphabet sizes. *Designs, Codes and Cryptography*, 46(2):137–166, 2008.

[46] Neil Bird, Claudine Conrado, Jorge Guajardo, Stefan Maubach, Geert Jan Schrijen, Boris Škorić, Anton M. H. Tombeur, Peter Thueringer, and Pim Tuyls. Algsics - combining physics and cryptography to enhance security and privacy in rfid systems. In Frank Stajano, Catherine Meadows, Srdjan Capkun, and Tyler Moore, editors, *ESAS*, volume 4572 of *Lecture Notes in Computer Science*, pages 187–202. Springer, 2007.

[47] Boris Škorić, Tatiana U. Vladimirova, Mehmet Celik, and Joop C. Talstra. Tardos Fingerprinting is Better Than We Thought. *IEEE Transactions on Information Theory*, 54(8):3663–3676, 2008.

[48] Pim Tuyls and Boris Škorić. Physical Unclonable Functions for Enhanced Security of Tokens and Tags. In *Highlights of the Information Security Solutions Europe (ISSE) 2006 Conference*, pages 30–37. Vieweg, 2006. Part 1.

[49] Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, and Boris Škorić. Towards an information-theoretic framework for analyzing intrusion detection systems. In *European Symposium on Research in Computer Security (ESORICS)*, volume 4189 of *LNCS*, pages 527–546. Springer, Sep 2006.

[50] Pim Tuyls, Geert Jan Schrijen, Boris Škorić, Jan van Geloven, Nynke Verhaegh, and Rob Wolters. Read-proof hardware from protective coatings. In *Cryptographic Hardware and Embedded Systems (CHES)*, volume 4249 of *LNCS*, pages 369–383. Springer-Verlag, 2006.

[51] Tanya Ignatenko, Geert-Jan Schrijen, Boris Škorić, Pim Tuyls, and Frans M. J. Willems. Estimating the Secrecy Rate of Physical Uncloneable Functions with the Context-Tree Weighting Method. In *Proc. IEEE International Symposium on Information Theory 2006*, pages 499–503, Seattle, USA, July 2006.

[52] Boris Škorić, Stefan Maubach, Tom Kevenaar, and Pim Tuyls. Information-theoretic analysis of capacitive Physical Unclonable Functions. *Journal of Applied physics*, 100:024902, 2006.

[53] Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, and Boris Škorić. Measuring intrusion detection capability: an information-theoretic approach. In *ASIACCS*, pages 90–101, 2006.

[54] Toine Staring and Boris Škorić. Revocation in the video content protection system. In *International Conference on Consumer Electronics (ICCE)*, pages 105–106, 2006.

[55] B. Škorić, P. Tuyls, and W. Ophey. Robust key extraction from physical uncloneable functions. In *Applied Cryptography and Network Security (ACNS) 2005*, volume 3531 of *LNCS*, pages 407–422. Springer, 2005.

[56] P. Tuyls, B. Škorić, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information-theoretic security analysis of physical uncloneable functions. In A.S. Patrick and M. Yung, editors, *9th Conf. on Financial Cryptography and Data Security*, volume 3570 of *LNCS*, pages 141–155. Springer, 2005.

[57] P. Tuyls, B. Škorić, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information-theoretic model for Physical Uncloneable Functions. In *IEEE International Symposium on Information Theory (ISIT)*, page 141, 2004.

[58] R. van Wesenbeeck, B. Škorić, W. IJzerman, M. Krijn, and P. Engelaar. Tracking and deflection coil design for vertical colour selection. In *International Meeting on Information Display (IMID)*, pages 130–133, 2003.

[59] P. Tuyls, B. Škorić, K. Schep, H. Boots, and J. Penninga. 3D Simulation Tool for RAC Magnetic Deflection Units. *SID Digest*, pages 1017–1019, 2001.

[60] M. Krijn, M. de Jong, R.J. Lange, B. Škorić, P. Tuyls, R.J. van Wesenbeeck, and M.H. Wassink. Transposed Scanning: The Way to Realize Super-Slim CRTs. *SID Digest*, pages 1008–1011, 2001.

[61] B. Škorić. Arc perturbation theory of magnetic deflection. *Journal of the SID*, 9(4):257–260, 2001.

[62] B. Škorić. New perturbative approach to magnetic deflection. In *Information Display Workshop (IDW)*, pages 533–536, 2000.

[63] M.A. Baranov, A.M.M. Pruisken, and B. Škorić. The problem of Coulomb interactions in the theory of the quantum Hall effect. In *Usp.Fiz.Nauk. (Suppl)*, volume 171, pages 44–49, 2000.

[64] A.M.M. Pruisken and B. Škorić. The fractional quantum Hall effect: Chern-Simons mapping, duality, Luttinger liquids and the instanton vacuum. *Nucl.Phys.B*, 559:637–672, 1999.

[65] A.M.M. Pruisken, B. Škorić, and M.A. Baranov. (Mis-)handling gauge invariance in the theory of the quantum Hall effect III: The instanton vacuum and chiral edge physics. *Phys.Rev.B*, 60(24):16838–16864, 1999.

[66] M.A. Baranov, A.M.M. Pruisken, and B. Škorić. (Mis-)handling gauge invariance in the theory of the quantum Hall effect II: Perturbative results. *Phys.Rev.B*, 60(24):16821–16837, 1999.

[67] A.M.M. Pruisken, B. Škorić, and M.A. Baranov. (Mis-)handling gauge invariance in the theory of the quantum Hall effect I: Unifying action and the nu=1/2 state. *Phys.Rev.B*, 60(24):16807–16820, 1999.