BIBLIOGRAPHY

[1] M. K. Ahmed, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi. Physical unclonable function based hardware security for resource constraint iot devices. *IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings*, pages 8–9, 2020. doi: 10.1109/WF-IoT48130.2020.9221357.

[2] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. A. Hawari. Internet of things market analysis forecasts, 2020-2030. *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 2020. doi: 10.1109/WorldS450073.2020.9210375.

[3] R. Ali, Y. Wang, H. Ma, Z. Hou, D. Zhang, E. Deng, and W. Zhao. A reconfigurable arbiter puf based on stt-mram. *Proceedings - IEEE International Symposium on Circuits and Systems*, 2021-May, 2021. ISSN 02714310. doi: 10.1109/ISCAS51556.2021.9401053.

[4] M. N. Aman, K. C. Chua, and B. Sikdar. Mutual authentication in iot systems using physical unclonable functions. *IEEE Internet of Things Journal*, 4, 2017. ISSN 23274662. doi: 10.1109/JIOT.2017.2703088.

[5] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In *2nd USENIX Workshop on Electronic Commerce (EC 96)*, Oakland, CA, Nov. 1996. USENIX Association. URL `https://www.usenix.org/conference/2nd-usenix-workshop-electronic-commerce/tamper-resistance-cautionary-note[Accessed:2024-04-30]`.

[6] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In B. Christianson, B. Crispo, M. Lomas, and M. Roe, editors, *Security Protocols*, pages 125–136, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg. ISBN 978-3-540-69688-9.

[7] F. Armknecht, R. Maes, A. R. Sadeghi, F. X. Standaert, and C. Wachsmann. A formal foundation for the security features of physical functions. *Proceedings - IEEE Symposium on Security and Privacy*, 2011. ISSN 10816011. doi: 10.1109/SP.2011.10.

[8] J. S. Arteaga-Falconi, H. A. Osman, and A. E. Saddik. Ecg authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement*, 65, 2016. ISSN 00189456. doi: 10.1109/TIM.2015.2503863.

[9] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer Networks*, 54, 2010. ISSN 13891286. doi: 10.1016/j.comnet.2010.05.010.

[10] S. Barman, H. P. Shum, S. Chattopadhyay, and D. Samanta. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. *IEEE Access*, 7, 2019. ISSN 21693536. doi: 10.1109/ACCESS.2019.2893185.

[11] A. Buriro, B. Crispo, F. DelFrari, and K. Wrona. Hold and sign: A novel behavioral biometrics for smartphone user authentication. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, 2016. doi: 10.1109/SPW.2016.20.

[12] D. Choi, S. H. Seo, Y. S. Oh, and Y. Kang. Two-factor fuzzy commitment for unmanned iot devices security. *IEEE Internet of Things Journal*, 6:335–348, 2019. ISSN 23274662. doi: 10.1109/JIOT.2018.2837751.

[13] S. Choto and N. Premasathian. A dynamic fuzzy commitment scheme using multiple commitments. *2012 International Symposium on Communications and Information Technologies, ISCIT 2012*, 2012. doi: 10.1109/ISCIT.2012.6380912.

[14] A. A. D. Conceic'ao, L. P. Ambrosio, T. R. Leme, A. C. Rosa, F. F. Ramborger, G. P. Aquino, and E. C. V. Boas. Internet of things environment automation: A smart lab practical approach. *Proceedings - 2022 2nd International Conference on Information Technology and Education, ICIT and E 2022*, 2022. doi: 10.1109/ICITE54466.2022.9759899.

[15] S. K. Dahel and Q. Xiao. Accuracy performance analysis of multimodal biometrics. *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, 2003. doi: 10.1109/SMCSIA.2003.1232417.

[16] J. Daugman. Biometric decision landscapes. *Technical Report-University of Cambridge Computer Laboratory*, 2000. ISSN 1476-2986.

[17] U. Demir and Özlem Aktaş. Raptor versus reed solomon forward error correction codes. *Proceedings of ISCN'06: 7th International Symosium on Computer Networks*, 2006, 2006. doi: 10.1109/ISCN.2006.1662545.

[18] R. Devi and P. Sujatha. A study on biometric and multi-modal biometric system modules, applications, techniques and challenges. *2017 Conference on Emerging Devices and Smart Systems, ICEDSS 2017*, 2017. doi: 10.1109/ICEDSS.2017.8073691.

[19] S. Elgendy and E. Y. Tawfik. Impact of physical design on puf behavior: A statistical study. *Proceedings - IEEE International Symposium on Circuits and Systems*, 2021-May, 2021. ISSN 02714310. doi: 10.1109/ISCAS51556.2021.9401140.

[20] T. S. Enamamu, N. Clarke, P. Haskell-Dowland, and F. Li. Smart watch based body-temperature authentication. *Proceedings of the IEEE International Conference on Computing, Networking and Informatics, ICCNI 2017*, 2017-January, 2017. doi: 10.1109/ICCNI.2017.8123790.

[21] G. Fortino, W. Russo, C. Savaglio, M. Viroli, and M. C. Zhou. Opportunistic cyber-physical services: A novel paradigm for the future internet of things. *IEEE World*

Forum on Internet of Things, WF-IoT 2018 - Proceedings, 2018-January, 2018. doi: 10.1109/WF-IoT.2018.8355174.

[22] Z. He, W. Chen, L. Zhang, G. Chi, Q. Gao, and L. Harn. A highly reliable arbiter puf with improved uniqueness in fpga implementation using bit-self-test. *IEEE Access*, 8: 181751–181762, 2020. ISSN 21693536. doi: 10.1109/ACCESS.2020.3028514.

[23] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas. *Proceedings - 2010 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2010*, pages 298–303, 2010. doi: 10.1109/ReConFig.2010.24.

[24] T. Ignatenko and F. Willems. Achieving secure fuzzy commitment scheme for optical pufs. *IIH-MSP 2009 - 2009 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009. doi: 10.1109/IIH-MSP.2009.310.

[25] D. Jeon and B. D. Choi. Circuit design of physical unclonable function for security applications in standard cmos technology. *2016 IEEE International Conference on Electron Devices and Solid-State Circuits, EDSSC 2016*, 2016. doi: 10.1109/EDSSC.2016.7785216.

[26] A. Juels and M. Wattenberg. Fuzzy commitment scheme. *Proceedings of the ACM Conference on Computer and Communications Security*, pages 28–36, 1999. doi: 10.1145/319709.319714.

[27] M. Khalafalla and C. Gebotys. Pufs deep attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter pufs. *Proceedings of the 2019 Design, Automation and Test in Europe Conference and Exhibition, DATE 2019*, 2019. doi: 10.23919/DATE.2019.8714862.

[28] C. Labrado and H. Thapliyal. Design of a piezoelectric-based physically unclonable function for iot security. *IEEE Internet of Things Journal*, 6, 2019. ISSN 23274662. doi: 10.1109/JIOT.2018.2874626.

[29] S. Lee, M. K. Oh, Y. Kang, and D. Choi. Implementing a phase detection ring oscillator puf on fpga. *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, 2018. doi: 10.1109/ICTC.2018.8539624.

[30] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. V. Dijk, and S. Devadas. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13, 2005. ISSN 10638210. doi: 10.1109/TVLSI.2005.859470.

[31] S. Lin and D. J. Costello. *Error Control Coding: Fundamentals and Applications*. Prantice-Hall, Inc., 1983. ISBN 0-13-283796-X.

[32] L. Lu, Y. Z. Chen, and T. T. H. Kim. A configurable randomness enhanced rram puf with biased current sensing scheme. *Proceedings - IEEE International Symposium on Circuits and Systems*, 2021-May, 2021. ISSN 02714310. doi: 10.1109/ISCAS51556.2021.9401390.

[33] K. L. Lueth. State of the iot 2018: Number of iot devices now at 7b – market accelerating. *IoT Analytics*, 2018.

[34] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer. Implementation and characterization of a physical unclonable function for iot: A case study with the tero-puf. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37, 2018. ISSN 19374151. doi: 10.1109/TCAD.2017.2702607.

[35] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young. A puf taxonomy. *Applied Physics Reviews*, 6, 2019. ISSN 19319401. doi: 10.1063/1.5079407.

[36] K. Mergu. Performance analysis of reed-solomon codes concatenated with convolutional codes over awgn channel. *APTIKOM Journal on Computer Science and Information Technologies*, 1, 2016. ISSN 2528-2417. doi: 10.34306/csit.v1i1.41.

[37] S. H. Moghadas and G. Fischer. Robust iot communication physical layer concept with improved physical unclonable function. *Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics*, 2017-October, 2017. ISSN 21592160. doi: 10.1109/PRIMEASIA.2017.8280373.

[38] B. R. Naidu, K. V. Bhavani, C. S. Rao, and P. V. P. Reddy. Comparative analysis of three single trait biometric authentication models. *Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019*, 2019. doi: 10.1109/ICCSP.2019.8698041.

[39] T. A. T. Nguyen, D. T. Nguyen, and T. K. Dang. A multi-factor biometric based remote authentication using fuzzy commitment and non-invertible transformation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9357, 2015. ISSN 16113349. doi: 10.1007/978-3-319-24315-3_8.

[40] C. Nixon, M. Sedky, and M. Hassan. Practical application of machine learning based online intrusion detection to internet of things networks. *2019 IEEE Global Conference on Internet of Things, GCIoT 2019*, 2019. doi: 10.1109/GCIoT47977.2019.9058410.

[41] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical one-way functions. *Science*, 297(5589):2026–2030, 2002. doi: 10.1126/science.1074376. URL `https://www.science.org/doi/abs/10.1126/science.1074376[Accessed:2024-04-30]`.

[42] N. Premasathian. A multiple fuzzy commitment scheme. *International Conference on Computer Applications Technology, ICCAT 2013*, 2013. doi: 10.1109/ICCAT.2013.6521958.

[43] F. F. Pulungan, D. W. Sudiharto, and T. Brotoharsono. Easy secure login implementation using pattern locking and environmental context recognition. *Proceedings of the 2018 International Conference on Applied Engineering, ICAE 2018*, 2018. doi: 10.1109/INCAE.2018.8579359.

[44] N. F. Rajani, G. Dar, R. Biswas, and C. K. Ramesha. Solution to the tic-tac-toe problem using hamming distance approach in a neural network. *Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011*, 2011. doi: 10.1109/ISMS.2011.70.

[45] U. Rührmair, H. Busch, and S. Katzenbeisser. *Strong PUFs: Models, Constructions, and Security Proofs*, pages 79–96. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. ISBN 978-3-642-14452-3. doi: 10.1007/978-3-642-14452-3_4. URL `https://doi.org/10.1007/978-3-642-14452-3_4`.

[46] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. *Proceedings of the ACM Conference on Computer and Communications Security*, 2010. ISSN 15437221. doi: 10.1145/1866307.1866335.

[47] A. Samuel and C. Sipes. Making internet of things real. *IEEE Internet of Things Magazine*, 2, 2019. ISSN 2576-3180. doi: 10.1109/iotm.2019.1907777.

[48] G. S. Shehu, A. M. Ashir, and A. Eleyan. Character recognition using correlation hamming distance. *2015 23rd Signal Processing and Communications Applications Conference, SIU 2015 - Proceedings*, 2015. doi: 10.1109/SIU.2015.7129937.

[49] J. Singh and J. Singh. A comparative study of error detection and correction coding techniques. *Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012*, 2012. doi: 10.1109/ACCT.2012.2.

[50] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. *Proceedings - Design Automation Conference*, 2007. ISSN 0738100X. doi: 10.1109/DAC.2007.375043.

[51] B. M. B. Talukder, F. Ferdaus, and M. T. Rahman. Memory-based pufs are vulnerable as well: A non-invasive attack against sram pufs. *IEEE Transactions on Information Forensics and Security*, 16, 2021. ISSN 15566021. doi: 10.1109/TIFS.2021.3101045.

[52] J. C. Talwana and H. J. Hua. Smart world of internet of things (iot) and its security concerns. *Proceedings - 2016 IEEE International Conference on Internet of*

Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, 2017. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.64.

[53] J. Tou and R. Gonzalez. *Pattern Recognition Principles*. Applied mathematics and computation. Addison-Wesley Publishing Company, 1974. ISBN 9780201075878.

[54] W. You, X. Chen, H. Dong, X. Tong, and S. Qing. Research and application of physical unclonable functions. *Proceedings of 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference, ITOEC 2018*, 2018. doi: 10.1109/ITOEC.2018.8740432.

[55] F. Zerrouki, S. Ouchani, and H. Bouarfa. Quantifying security and performance of physical unclonable functions. *2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020*, 2020. doi: 10.1109/IOTSMS52051.2020.9340212.

[56] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng. A privacy-aware pufs-based multiserver authentication protocol in cloud-edge iot systems using blockchain. *IEEE Internet of Things Journal*, 8, 2021. ISSN 23274662. doi: 10.1109/JIOT.2021.3068410.

[57] X. Zhou and C. Busch. Measuring privacy and security of iris fuzzy commitment. *Proceedings - International Carnahan Conference on Security Technology*, 2012. ISSN 10716572. doi: 10.1109/CCST.2012.6393553.