in Section 4.3.1. To avoid such conditions, the generated digital key must account for saturating DIPs, or the AMS circuit must be dependent on the key for all the possible inputs.

(2) Independently securing digital and analog blocks must be avoided. Therefore, a technique is proposed in the paper to link the analog and digital keys. Such dependencies prevent an adversary from extracting circuit information by partially altering the key of an activated IC, which is discussed in Section 4.3.2.

(3) Ensure that the scan chain and internal testing points are inaccessible to adversaries. The AMS pipeline was highly susceptible to attack as every register within the digital block was accessible. The observability of all of the registers permits access to the ADC output, which results in increased isolation of the analog and digital circuit blocks. Obfuscation, or limitation, of the scan chain and testing circuits is needed to prevent an adversary from efficiently determining the key used for logic locking.

7 CONCLUSIONS

This paper proposes a novel obfuscation methodology to protect AMS circuits against IP piracy and theft by implementing logic and performance locking techniques on the digital and analog domains, respectively. Security analysis utilizing a SMT-based attack on an obfuscated peak detection circuit is performed, indicating a vulnerability when independently implementing obfuscating techniques in the analog and digital circuit sub-blocks. Both saturating conditions of the analog block and application of a partial key to an activated IC allow for the determination of the keys for each circuit block in isolation. To force an adversary to concurrently consider the keys of both circuit blocks, the key inputs between the analog and digital blocks are linked. The interconnection of the keys from the two blocks results in a 3x increase in the number of DIPs required to determine the key of the AMS circuit. Accounting for the security of the entire AMS circuit as opposed to the individual circuit blocks is, therefore, critical when designing an AMS system.

ACKNOWLEDGMENTS

This research is supported in part by the Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a, Drexel Ventures Innovation Fund, and the National Science Foundation under Grant CNS-1648878 and Grant CNS-1751032.

REFERENCES

[1] S. Skorobogatov and C. Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 23–40, September 2012.
[2] U.S Department of Commerce, "Defense Industrial Base Assessment: Counterfeit Electronics," 2010.
[3] 112th Congress, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," May 2012.
[4] IHS Technology Press Release, "Top 5 Most Counterfeited Parts Represent A $169 Billion Potential Challenge for Global Semiconductor Market," April 2012.
[5] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending Piracy of Integrated Circuits," *Computer*, Vol. 43, No. 10, pp. 30–38, October 2010.
[6] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," *IEEE Design and Test of Computers*, Vol. 27, No. 1, pp. 66–75, February 2010.
[7] J. Rajendran, H. Zhang, C. Zhang, G. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault Analysis-Based Logic Encryption," *IEEE Transactions on Computers*, Vol. 64, No. 2, pp. 410–424, February 2015.
[8] R. D. Newbould, D. L. Irby, J. D. Carothers, J. J. Rodriguez, and W. T. Holman., "Mixed Signal Design Watermarking for IP Protection," *Proceedings of the Southwest Symposium on Mixed-Signal Design*, pp. 249–265, January 2003.
[9] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "IP Protection for VLSI Designs Via Watermarking of Routes," *Proceedings of the IEEE International ASIC/SOC Conference*, pp. 406–410, September 2001.
[10] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Pan, "Provably Secure Camouflaging Strategy for IC Protection," *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, pp. 1–8, November 2016.
[11] F. Koushanfar, "Provably Secure Active IC Metering Techniques for Piracy Avoidance and Digital Rights Management," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, pp. 51–63, February 2012.
[12] IHS Markit, "IoT Trend Watch 2018," 2018.
[13] V. V. Rao and I. Savidis, "Protecting Analog Circuits with Parameter Biasing Obfuscation," *Proceedings of the IEEE Latin American Test Symposium (LATS)*, pp. 1–6, March 2017.
[14] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-Secure Logic Locking: From Theory To Practice," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pp. 1601–1618, November 2017.
[15] K. Juretus and I. Savidis, "Reduced Overhead Gate Level Logic Encryption," *Proceedings of the IEEE/ACM Great Lakes Symposium on VLSI*, pp. 15–20, May 2016.
[16] K. Juretus and I. Savidis, "Reducing Logic Encryption Overhead Through Gate Level Key Insertion," *Proceedings of the IEEE International Conference on Circuits and Systems*, pp. 1714–1717, May 2016.
[17] S. Dupuis, P. S. Ba, G. Di Natale, M. L. Flottes, and B. Rouzeyre, "A Novel Hardware Logic Encryption Technique for Thwarting Illegal Overproduction and Hardware Trojans," *Proceeding of the IEEE International On-Line Testing Symposium*, pp. 49–54, July 2014.
[18] M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri, "On Improving the Security of Logic Locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 35, No. 9, pp. 1411–1424, September 2016.
[19] K. Juretus and I. Savidis, "Increasing the SAT Attack Resiliency of In-Cone Logic Locking," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2019.
[20] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the Security of Logic Encryption Algorithms," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 137–143, May 2015.
[21] Y. Xie and A. Srivastava, "Mitigating SAT Attack on Logic Locking," *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 127–146, June 2016.
[22] M. Yasin, B. Mazumdar, J. Rajendran, and O. Sinanoglu, "SARLock: SAT Attack Resistant Logic Locking," *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 236–241, May 2016.
[23] M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Z. Pan, "Provably Secure Camouflaging Strategy for IC Protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1–14, September 2018.
[24] K. Juretus and I. Savidis, "Time Domain Sequential Locking for Increased Security," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2018.
[25] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal Attacks on Logic Locking and Camouflaging Techniques," *IEEE Transactions on Emerging Topics in Computing*, Vol. 64, No. 9, September 2017.
[26] D. H. K. Hoe, J. Rajendran, and R. Karri, "Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors," *Proceedings of the IEEE Computer Society Annual Symposium on VLSI*, pp. 516–521, July 2014.
[27] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu, "Thwarting Analog IC Piracy Via Combinational Locking," *Proceedings of the IEEE International Test Conference (ITC)*, pp. 1–10, October 2017.
[28] V. V. Rao and I. Savidis, "Mesh Based Obfuscation of Analog Circuit Properties," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 1–5, May 2019.
[29] V. V. Rao and I. Savidis, "Transistor Sizing for Parameter Obfuscation of Analog Circuits Using Satisfiability Modulo Theory," *Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pp. 102–106, October 2018.
[30] J. Leonhard, M. Yasin, S. Turk, M. T. Nabeel, R. C. Avot M. M. Louërat, O. Sinanoglu H. Aboushady, and H. G. Stratigopoulos, "MixLock: Securing Mixed-Signal Circuits via Logic Locking," *Proceedings of the IEEE Design, Automation Test in Europe Conference Exhibition*, p. PP, March 2019.
[31] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards Provably-secure Analog and Mixed-signal Locking Against Overproduction," *Proceedings of the International Conference on Computer-Aided Design*, pp. 1–8, November 2018.