The Institution of Engineering and Technology

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Anirban Sengupta and Saraju P. Mohanty

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

Authors: Anirban Sengupta and Saraju P. Mohanty

Table of Contents

Chapter 2: Security in Consumer Electronics and Internet of Things (IoT)

2.1 Internet of Things (IoT) - A Broad Overview

2.1.1 IoT - Architecture

2.1.2 IoT - Driving Technology

2.1.3 IoT - Applications

2.1.4 IoT - Challenges

2.2 Security, Privacy, IP Right in IoT and CE Systems - A Big Picture

2.2.1 IoT Security - Attacks and Countermeasures

2.2.2 Trustworthy Consumer Electronic Systems

2.2.3 Hardware-Assisted Security and Protection

2.2.4 Different Aspects of Security and Privacy

2.2.5 Different Aspects of Intellectual Property (IP), Ownership Right, or Copyright Protection

2.3 Memory Security

2.3.1 Memory Security Attacks

2.3.2 Memory Security Solutions

2.4 Radio Frequency Identification (RFID) Security

2.4.1 RFID Security Attacks

2.4.2 RFID Security Solutions

2.5 Near Field Communications (NFC) Security

2.5.1 NFC Security Attacks

2.5.2 NFC Security Solutions

2.6 Smart Transportation Security

2.6.1 Smart Car Security

2.6.2 Unmanned Ariel Vehicle (UAV) Or Drone Security

2.7 Smart Healthcare Security

2.7.1 Smart Healthcare Security Attacks

Chapter 01

Introduction to IP Core Protection and Hardware-Assisted Security of Consumer Electronics

This chapter presents and overview of the book. Some discussions which can serve as introductory materials towards the overal text of the book. It is assumed the the readers have some background on areas like VLSI, embeded systems, hardware design flow before adopting this text.

1.1. Consumer Electronics and Security Perspectives

Consumer Electronics (CE), embracing high end devices ranging from digital camera, multi-spectral camera, IP TV, smart tablets, night vision camera to smart meter, accompanied by data and communication knowhow makes emerging smart cities and Internet of Things (IoT) a reality. In the world of CE and IoT, security, privacy, and protection of hardware and its information are critically imperative. It is universally acknowledged that for internet-of-things (IoT), security of underneath hardware is pivotal for correct operation. The underlying hardware may have been affected by several threat actors. An adversary may generate secret exist that leaks crucial data such as encryption key employed in secure transmission line, the maker could meddle the design by implanting hardware Trojans, or inserting artifacts with recognized dependability susceptibilities. Current generation designs assimilate IP blocks from manifold vendors; mass-produced and verified by diverse companies worldwide. Accordingly, numerous access points exist for hardware to be attacked. For a trusted hardware design, defense of intellectual property cores is of ultimate significance [(Sengupta & Kundu, 2017), (Sengupta, Mohanty & Rose, 2018)].

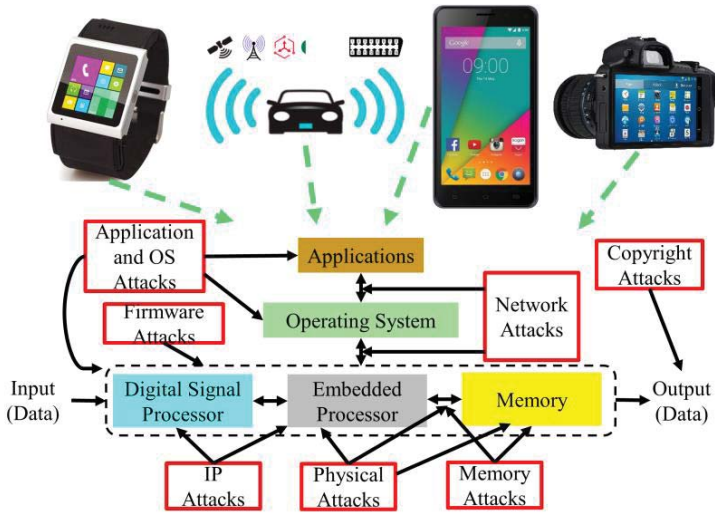

Fig. 1.1 Consumer electronics components and security vulnerability

A typical consumer electronic system presented in Fig. 1.1 has DSP, embedded processor, memory, system software, and application software. Significantly diverse forms of attacks can happen to this CE system including the following: system security, information security, system privacy, information privacy, network security, firmware security, system trustworthiness, hardware IP rights, information copyrights. The origins of these attacks are different, for example, remote or local. They can be either by software or

References

E. Castillo, U. Meyer-Baese, A. Garc´ıa, L. Parrilla, and A. Lloris, “Ipp@ hdl: efficient intellectual property protection scheme for ip cores,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 15, no. 5, pp. 578–591, 2007.

F. Koushanfar, I. Hong, and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection,” ACM Trans. Des. Autom. Electron. Syst., vol. 10, no. 3, pp. 523–545, Jul. 2005. [Online]. Available: http://doi.acm.org/10.1145/1080334.1080338.

I. Hong and M. Potkonjak, “Behavioral synthesis techniques for intellectual property protection,” in Proceedings of the 36th annual ACM/IEEE Design Automation Conference. ACM, 1999, pp. 849–854.

Y. Alkabani, F. Koushanfar, and M. Potkonjak, “Remote activation of ICs for piracy prevention and digital right management,” in Computer- Aided Design, 2007. ICCAD 2007. IEEE/ACM International Conference on, Nov 2007, pp. 674–677.

Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” Circuits and Systems for Video Technology, IEEE Transactions on, vol. 16, no. 3, pp. 354–362, 2006.

L. Marvel, “Information hiding: Steganography and watermarking,” in Optical and Digital Techniques for Information Security, ser. Advanced Sciences and Technologies for Security Applications, B. Javidi, Ed. Springer New York, 2005, vol. 1, pp. 113–133. [Online]. Available: http://dx.doi.org/10.1007/0-387-25096-4.

Anirban Sengupta, Sandip Kundu "Securing IoT Hardware: Threat models and Reliable, Low-power Design Solutions", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Dec 2017, Volume: 25, Issue:12, pp. 3265 - 3267

Anirban Sengupta, SP Mohanty, Garrett Rose "Hardware - Assisted Design for Security and Protection of Consumer Electronics", IET Computers and Digital Techniques, Accepted, June 2018.

Miodrag Potkonjak, Vishwa Goudar "Public Physical Unclonable Functions", Proceedings of the IEEE , Vol. 102, No. 8, August 2014.

Anirban Sengupta, "Hardware Security of CE Devices: Threat Models and Defence against IP Trojans and IP Piracy", IEEE Consumer Electronics, Jan 2017, Volume: 6, Issue: 1 ,pp. 130 – 133.

Anirban Sengupta "Protection of IP-Core Designs for CE Products", IEEE Consumer Electronics, Vol 5, pp. 83- 89, Dec 2015

Anirban Sengupta "Protection of Reusable IP core at Architectural Level", IEEE VLSI Circuits & Systems Letter, Vol. 1, Issue 2, Oct 2015, pp. 14 – 17.

Christof Paar, Jan Pelzl “Understanding Cryptography - A Textbook for Students and Practitioners”, Springer-Verlag, eBook ISBN 978-3-642-04101-3, Number of Pages: XVIII, 372, Nov 2009.

Anirban Sengupta "Hardware Vulnerabilities and its Effect on CE Devices: Design-for-Security against Trojan", IEEE Consumer Electronics, Volume: 6, Issue: 3, July 2017, pp. 126 – 133.

Xilinx – Vivado HLS -- https://www.xilinx.com/products/design-tools/vivado/integration/esl-design.html, Last accessed on Feb 2018.

Anirban Sengupta, Saraju P.Mohanty "High-Level Synthesis of Digital Circuits in the Nanoscale, Mobile Electronics Era", IET Book: Nano-CMOS and Post-CMOS Electronics: Circuits and Design, (Eds: Saraju P Mohanty& Ashok Srivastava), Invited Book Chapter, e-ISBN: 9781785610004, pp: 219 - 261, June 2016.

Y. M. Alkabani and F. Koushanfar. 2007. 'Active hardware metering for intellectual property protection and security', In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07), Niels Provos (Ed.). USENIX Association, Berkeley, CA, USA, , Article 20 , 16 pages.

J. A. Roy, F. Koushanfar and I. L. Markov, "EPIC: Ending Piracy of Integrated Circuits," 2008 Design, Automation and Test in Europe, Munich, 2008, pp. 1069-1074.

[Sengupta-2018] Anirban Sengupta and Dipanjan Roy, ‘Reusable intellectual property core protection for both buyer and seller,’ 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2018, pp. 1-3.

[Sengupta-2018-ICCE] Anirban Sengupta and Dipanjan Roy, ‘Multi-phase watermark for IP core protection,’ 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2018, pp. 1-3.

[Mohanty-2015] S. P. Mohanty, Nanoelectronic Mixed-Signal System Design. McGraw- Hill Education, 2015, no. 0071825711.

[Mohanty-2018-ICCE] S. P. Mohanty, Energy and Security Tradeoffs in CE Systems, Panel, IEEE International Conference on Consumer Electronics, Las Vegas, 2018.

[Mohanty-2018-ZINC] S. P. Mohanty, “Security and Energy Tradeoffs in Consumer Electronics”, Keynote Abstract, 3rd Zooming Innovation in Consumer Electronics International Conference (ZINC), 2018, Novi Sad, Serbia, 31st May 2018.

[Mohanty-2017-MAMI] S. P. Mohanty "Smart Cities - Demystified", Keynote Abstract, 2nd International Conference on Man and Machine Interfacing (MAMI), 2017, Bhubaneswar, India.

[Mohanty-2017-ICIT] S. P. Mohanty "Internet of Things (IoT) - Demystified", Keynote Abstract, 16th International Conference on Information Technology (ICIT), 2017, Bhubaneswar, India.

[Mohanty-2016-CEM] S. P. Mohanty, U. Choppali, and E. Kougianos, “Everything You wanted to Know about Smart Cities”, IEEE Consumer Electronics Magazine (CEM), Volume 5, Issue 3, July 2016, pp. 60--70.

[Yanambaka-2018-TSM] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security”, IEEE Transactions on Semiconductor Manufacturing (TSM), Volume 31, Issue 2, May 2018, pp. 285--294.

[Yanambaka-2017-ALOG] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT”, Springer Analog Integrated Circuits and Signal Processing Journal, Volume 93, Issue 3, December 2017, pp. 429--441.

[Joshi-2017-Potentials] S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything You Wanted to Know about PUFs”, IEEE Potentials Magazine, Volume 36, Issue 6, November-December 2017, pp. 38--46.

Chapter 02

Security in Consumer Electronics and Internet of Things (IoT)

In a typical consumer electronics including diverse forms of attacks, following are not the same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection. They hold a different meaning and each serve different purpose. This chapter aims at differentiating each of the terms in the context of Internet of Things (IoT). IoT is a very hot topic of research where different devices, sensors and computers are connected to a network, collect data and process it for different purposes. A network of devices and sensors connected to the cloud can complete many tasks that are without them, very difficult to achieve and complete. But there exists a problem of security and privacy everywhere. With all the different devices connected to the internet, attackers pose a huge threat to the system. When the system is implemented in home, for healthcare or running an entire city, this threat can be much more catastrophic.

This Chapter is organized as follows. Section 1 presents an introduction and broad overview of Internet of Things. Section 2 presents a broad view of security, energy, and cost trade-offs in Consumer Electronic systems. Section 3 presents different security threats and solutions to the memory modules of the system, Section 4 provides different threats and solutions to the RFID modules, Section 5 provide security flaws and how to mitigate them in an NFC module of the system. Section 6 discusses different security flaws in the Smart Vehicles, The Autonomous Cars and The UAVs. Section 7 discuss different ways an attacker can attack a healthcare device and solutions for some of the attacks, Section 8 discusses the threats on firmware of the devices and Section 9 discusses the emerging technology of blockchain, its advantages and issues. The conclusion and future directions are presented in Section 10.

1 Internet of Things (IoT) - A Broad Overview

Communication has evolved in the world at a very fast pace. Many solutions has been proposed for communications, short or long distance. Technological growth also helped this in developing high performance computing devices making it a necessity needing newer inventions. All of them combined gave rise to “Internet of Things” which has become an integral part of every-day-life without realizing it. There are many definitions to IoT depending on the individual’s perspective. In an Internet of Things environment, all of the devices or “THINGS” are connected to a network and exchange data among themselves or send to the cloud [57]. The “3-I’s” in the context of IoT are shown in Figure 1. They are ‘Interconnection’, ‘Intelligence’ and ‘Instrumentation’. These three are the important aspects of an IoT environment, as shown in the figure, the Smart City environment. Interconnection is the communication platform that provides the network for the devices an Internet connection that helps in transmitting the data among themselves or to the cloud services where post processing takes place. Intelligence is the brain of the entire Environment and Instrumentation is various devices and sensors that are present in the environment. There are various devices present in an IoT environment like microcontrolleres, single board computers and sensors. Each of them should have a unique IP address to be considered as a THING for the IoT [55].

An IoT can be defined as Any TIME connection, Any THING connection and Any PLACE Connection as shown in Figure 2 [35]. IoT can be anywhere. Some of the IoT devices can be deployed in places where they are not monitored continuously. Their duty will be monitoring a parameter and transmitting the data over the air [111]. In such cases, it should be continuously connected to the internet which needs “Any PLACE Connection”, “Any TIME Connection” and “Any THING Connection”. With the technological advancements, various devices and board are attaining communication capabilities which can help in implementing an IoT environment at a very low cost.

References

1. Ahmadi, M., Rajamani, R., Sezen, S.: Transparent Flexible Active Faraday Cage Enables In Vivo Capacitance Measurement in Assembled Microsensor. IEEE Sensors Letters **1**(5), 1–4 (2017). DOI 10.1109/LSENS.2017.2737956
2. Al-Kuwari, M., Ramadan, A., Ismael, Y., Al-Sughair, L., Gastli, A., Benammar, M.: Smart-Home Automation Using IoT-Based Sensing and Monitoring Platform. In: 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), pp. 1–6 (2018). DOI 10.1109/CPE.2018.8372548
3. Alamri, A.: Monitoring System for Patients Using Multimedia for Smart Healthcare. IEEE Access **6**, 23,271–23,276 (2018). DOI 10.1109/ACCESS.2018.2826525
4. Almajali, S., Salameh, H.B., Ayyash, M., Elgala, H.: A Framework for Efficient and Secured Mobility of IoT Devices in Mobile Edge Computing. In: 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), pp. 58–62 (2018). DOI 10.1109/FMEC.2018.8364045
5. Alrabady, A.I., Mahmud, S.M.: Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. IEEE Transactions on Vehicular Technology **54**(1), 41–50 (2005). DOI 10.1109/TVT.2004.838829
6. Amazon: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011
7. Andrews, C.: Cyber Car Crime: Thieves Turn to High Tech [Transport Car Crime]. Engineering Technology **12**(2), 32–35 (2017). DOI 10.1049/et.2017.0200
8. Asplund, M., Nadjm-Tehrani, S.: Attitudes and Perceptions of IoT Security in Critical Societal Services. IEEE Access **4**, 2130–2138 (2016). DOI 10.1109/ACCESS.2016.2560919
9. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better – how to make bitcoin a better currency. In: International Conference on Financial Cryptography and Data Security, pp. 399–414 (2012)
10. Bhargava, B., Farkas, C., Lilien, L., Makedon, F.: Trust, Privacy, and Security Summary of a Workshop Breakout Session at the National Science Foundation Information and Data Management (IDM) Workshop held in Seattle, Washington, September 14 - 16, 2003 (Version 2) (2018). http://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2003-34.pdf
11. Bitcoin: Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper
12. Bolisetti, S.K., Patwary, M., Soliman, A.H., Abdel-Maguid, M.: RF Sensing Based Target Detector for Smart Sensing Within Internet of Things in Harsh Sensing Environments. IEEE Access **5**, 13,346–13,363 (2017). DOI 10.1109/ACCESS.2017.2728372
13. Carter, B., Green, S., Leeman, R., Chaulk, N.: SmartBay: Better Information - Better Decisions. In: OCEANS 2008, pp. 1–7 (2008). DOI 10.1109/OCEANS.2008.5151869
14. Catarinucci, L., de Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M.L., Tarricone, L.: An IoT-Aware Architecture for Smart Healthcare Systems. IEEE Internet of Things Journal **2**(6), 515–526 (2015). DOI 10.1109/JIOT.2015.2417684
15. Chang, C.H., Zheng, Y., Zhang, L.: A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement. IEEE Circuits and Systems Magazine **17**(3), 32–62 (2017). DOI 10.1109/MCAS.2017.2713305
16. Chaudhary, R., Jindal, A., Aujla, G.S., Kumar, N., Das, A.K., Saxena, N.: LSCSH: Lattice-Based Secure Cryptosystem for Smart Healthcare in Smart Cities Environment. IEEE Communications Magazine **56**(4), 24–32 (2018). DOI 10.1109/MCOM.2018.1700787
17. Choi, B.C., Lee, S.H., Na, J.C., Lee, J.H.: Secure Firmware Validation and Update for Consumer Devices in Home Networking. IEEE Transactions on Consumer Electronics **62**(1), 39–44 (2016). DOI 10.1109/TCE.2016.7448561
18. Dacus, C., Yannakogeorgos, P.A.: Designing Cybersecurity into Defense Systems: An Information Economics Approach. IEEE Security Privacy **14**(3), 44–51 (2016). DOI 10.1109/MSP.2016.49
19. Danese, A., Pravadelli, G., Bertacco, V.: Work-in-Progress: DOVE: Pinpointing Firmware Security Vulnerabilities via Symbolic Control Flow Assertion Mining. In: International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), pp. 1–2 (2017). DOI 10.1145/3125502.3125541
20. Dupuis, S., Flottes, M.L., Natale, G.D., Rouzeyre, B.: Protection Against Hardware Trojans With Logic Testing: Proposed Solutions and Challenges Ahead. IEEE Design Test **35**(2), 73–90 (2018). DOI 10.1109/MDAT.2017.2766170
21. Farooq, M.J., Zhu, Q.: On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT). IEEE Transactions on Wireless Communications **17**(4), 2618–2632 (2018). DOI 10.1109/TWC.2018.2799860
22. Ferreira, H.G.C., Canedo, E.D., de Sousa, R.T.: IoT architecture to enable intercommunication through REST API and UPnP using IP, ZigBee and arduino. In: IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 53–60 (2013). DOI 10.1109/WiMOB.2013.6673340
23. Freescale: http://www.nxp.com/assets/documents/data/en/supporting-information/DWF13_AMF_AUT_T0112_Detroit.pdf
24. Ghoneim, A., Muhammad, G., Amin, S.U., Gupta, B.: Medical Image Forgery Detection for Smart Healthcare. IEEE Communications Magazine **56**(4), 33–37 (2018). DOI 10.1109/MCOM.2018.1700817
25. Ghosh, S., Majumder, A., Goswami, J., Kumar, A., Mohanty, S.P., Bhattacharyya, B.K.: Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment. IEEE Consumer Electronics Magazine **6**(1), 82–93 (2017). DOI 10.1109/MCE.2016.2614522
26. Greene, J.: Intel Trusted Execution Technology. Tech. rep., Intel (2016)
27. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Elsevier Future Generation Computer Systems **29**(7) (2013)

28. Guin, U., Bhunia, S., Forte, D., Tehranipoor, M.M.: SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware. IEEE Transactions on Dependable and Secure Computing **14**(3), 265–278 (2017). DOI 10.1109/TDSC.2016.2615609
29. Halevi, T., Li, H., Ma, D., Saxena, N., Voris, J., Xiang, T.: Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks. IEEE Transactions on Emerging Topics in Computing **1**(2), 307–318 (2013). DOI 10.1109/TETC.2013.2290537
30. Harbison, C.: New Android NFC Attack Could Steal Money From Credit Cards Anytime Your Phone Is Near (2016). http://www.player.one/
31. Hartmann, K., Steup, C.: The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment. In: 5th International Conference on Cyber Conflict (CYCON), pp. 1–23 (2013)
32. He, D., Ye, R., Chan, S., Guizani, M., Xu, Y.: Privacy in the Internet of Things for Smart Healthcare. IEEE Communications Magazine **56**(4), 38–44 (2018). DOI 10.1109/MCOM.2018.1700809
33. He, J., Zhao, Y., Guo, X., Jin, Y.: Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **25**(10), 2939–2948 (2017). DOI 10.1109/TVLSI.2017.2727985
34. Heartfield, R., Loukas, G., Gan, D.: You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. IEEE Access **4**, 6910–6928 (2016). DOI 10.1109/ACCESS.2016.2616285
35. IEEE Internet Initiative: Towards a Definition of the Internet of Things (IoT). IEEE Internet of Things (2015)
36. Jalaian, B., Gregory, T., Suri, N., Russell, S., Sadler, L., Lee, M.: Evaluating LoRaWAN-Based IoT Devices for the Tactical Military Environment. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pp. 124–128 (2018). DOI 10.1109/WF-IoT.2018.8355225
37. Jayakrishnan, M.P., Vena, A., Sorli, B., Perret, E.: Solid-State Conductive-Bridging Reconfigurable RF-Encoding Particle for Chipless RFID Applications. IEEE Microwave and Wireless Components Letters **28**(6), 506–508 (2018). DOI 10.1109/LMWC.2018.2830702
38. Jin, J., Gubbi, J., Marusic, S., Palaniswami, M.: An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal **1**(2), 112–121 (2014). DOI 10.1109/JIOT.2013.2296516
39. Kaspersky: BEWARE THE THINGBOT! (2014). https://usa.kaspersky.com/blog/beware-the-thingbot/3060/
40. Kim, A., Wampler, B., Goppert, J., Hwang, I.: Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. In: Infotech at Aerospace Conference, pp. 1–30 (2012)
41. Kong, H.K., Kim, T.S., Hong, M.K.: A Security Risk Assessment Framework for Smart Car. In: 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 102–108 (2016). DOI 10.1109/IMIS.2016.42
42. Kott, A., Swami, A., West, B.J.: The Internet of Battle Things. Computer **49**(12), 70–75 (2016). DOI 10.1109/MC.2016.355
43. Krishnamurthy, R.K., Humble, T., Cheung, S.C., Lyke, J., Mohanty, S.P., Casto, M.: Energy and Cybersecurity Constraints on Consumer Electronics. http://www.icce.org/expert-panels/ (January 13, 2018). Last visited on 20th Nov 2017
44. Kundu, S., Islam, K.A., Jui, T.T., Rail, S., Hossain, M.A., Chowdhury, I.H.: Cyber Crime Trend in Bangladesh, an Analysis and Ways Out to Combat the Threat. In: 2018 20th International Conference on Advanced Communication Technology (ICACT), pp. 474–480 (2018). DOI 10.23919/ICACT.2018.8323800
45. Lee, H.C., Ke, K.H.: Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation. IEEE Transactions on Instrumentation and Measurement pp. 1–11 (2018). DOI 10.1109/TIM.2018.2814082
46. Lee, Y.T., Hsiao, W.H., Lin, Y.S., Chou, S.C.T.: Privacy-Preserving Data Analytics in Cloud-Based Smart Home with Community Hierarchy. IEEE Transactions on Consumer Electronics **63**(2), 200–207 (2017). DOI 10.1109/TCE.2017.014777
47. Li, C., Raghunathan, A., Jha, N.K.: Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, pp. 150–156 (2011). DOI 10.1109/HEALTH.2011.6026732
48. Li, H., Chen, Y., He, Z.: The Survey of RFID Attacks and Defenses. In: 8th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4 (2012). DOI 10.1109/WiCOM.2012.6478720
49. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A Survey on the Security of Blockchain Systems. Future Generation Computer Systems (2017). DOI https://doi.org/10.1016/j.future.2017.08.020
50. Lopez, T., Ranasinghe, D., Harrison, M., McFarlane, D.: Adding sense to the internet of things an architecture framework for smart objective systems. Pervasive Ubiquitous Computing **16** (2012)
51. Luo, B., Wang, Y., Liu, Y.: Sensor fusion for vision-based indoor head pose tracking. In: 2009 Fifth International Conference on Image and Graphics, pp. 677–682 (2009). DOI 10.1109/ICIG.2009.145
52. Mazurczyk, W., Holt, T., Szczypiorski, K.: Guest Editors'; Introduction: Special Issue on Cyber Crime. IEEE Transactions on Dependable and Secure Computing **13**(2), 146–147 (2016). DOI 10.1109/TDSC.2015.2502407
53. McGowen, R., Poirier, C.A., Bostak, C., Ignowski, J., Millican, M., Parks, W.H., Naffziger, S.: Power and Temperature Control on a 90-nm Itanium Family Processor. IEEE Journal of Solid-State Circuits **41**(1), 229–237 (2006). DOI 10.1109/JSSC.2005.859902
54. Mohanty, S.P.: Everything you Wanted to Know about Internet of Things (IoT). https://cesoc.ieee.org/images/files/pdf/Mohanty_IEEE-DL_IoT.PDF (16th November, 2017). Last visited on 20th Nov 2017
55. Mohanty, S.P.: Internet of Things (IoT) - Demystified. http://www.smohanty.org/Presentations/2017/Mohanty_ICIT-2017_Keynote_IoT.PDF (16th November, 2017). Last visited on 14 Feb 2018
56. Mohanty, S.P.: Nanoelectronic Mixed-Signal System Design. 9780071825719. McGraw-Hill Education (2015)
57. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything You Wanted to Know About Smart Cities: The Internet of things is The Backbone. IEEE Consumer Electronics Magazine **5**(3), 60–70 (2016). DOI 10.1109/MCE.2016.2556879

58. Mohanty, S.P., Sengupta, A., Guturu, P., Kougianos, E.: Everything You Want to Know About Watermarking. IEEE Consumer Electronics Magazine **6**(3), 83–91 (2017)
59. g. Moon, J., Jang, J.J., Jung, I.Y.: Bot Detection via IoT Environment. In: 2015 IEEE 17th International Conference on High Performance Computing and Communications,, pp. 1691–1692 (2015). DOI 10.1109/HPCC-CSS-ICESS.2015.116
60. Nawir, M., Amir, A., Yaakob, N., Lynn, O.B.: Internet of Things (IoT): Taxonomy of Security Attacks. In: 2016 3rd International Conference on Electronic Design (ICED), pp. 321–326 (2016). DOI 10.1109/ICED.2016.7804660
61. Ngo, D.: (2014). https://cointelegraph.com/news/david-and-joyces-wedding-demonstrates-how-easy-it-is-to-
62. Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., Brumley, D.: GPS Software Attacks. In: ACM conference on Computer and communications security, pp. 450–461 (2012)
63. Nimgaonkar, S., Gomathisankaran, M., Mohanty, S.P.: MEM-DnPA Novel Energy Efficient Approach for Memory Integrity Detection and Protection in Embedded Systems. Circuits, Systems and Signal Processing **32**(6), 2581–2604 (2013)
64. Notario, M.A.: Privacidad vs Seguridad (2016). https://blogs.deusto.es/master-informatica/privacidad-vs-seguridad/
65. Obuchi, Y., Yamasaki, T., Aizawa, K., Toriumi, S., Hayashi, M.: Measurement and Evaluation of Comfort Levels of Apartments Using IoT Sensors. In: 2018 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–6 (2018). DOI 10.1109/ICCE.2018.8326169
66. Oh, D., Kim, N.S., Chen, C.C.P., Davoodi, A., Hu, Y.H.: Runtime Temperature-Based Power Estimation for Optimizing Throughput of Thermal-Constrained Multi-Core Processors. In: 2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 593–599 (2010). DOI 10.1109/ASPDAC.2010.5419815
67. OWASP: OWASP Internet of Things (IoT) Project. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
68. Pacheco, J., Satam, S., Hariri, S., Grijalva, C., Berkenbrock, H.: IoT Security Development Framework for Building Trustworthy Smart Car Services. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 237–242 (2016). DOI 10.1109/ISI.2016.7745481
69. Petit, J., Feiri, M., Kargl, F.: Revisiting Attacker Model for Smart Vehicles. In: IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC), pp. 1–5 (2014). DOI 10.1109/WIVEC.2014.6953258
70. Petit, J., Shladover, S.E.: Potential Cyberattacks on Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems **16**(2), 546–556 (2015). DOI 10.1109/TITS.2014.2342271
71. Plos, T., Hutter, M., Feldhofer, M., Stiglic, M., Cavaliere, F.: Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **21**(11), 1965–1974 (2013). DOI 10.1109/TVLSI.2012.2227849
72. Project, H.: https://www.hyperledger.org/
73. Prokofiev, A.O., Smirnova, Y.S., Surov, V.A.: A Method to Detect Internet of Things Botnets. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 105–108 (2018). DOI 10.1109/EIConRus.2018.8317041
74. Rauf, A., Shaikh, R.A., Shah, A.: Security and Privacy for IoT and Fog Computing Paradigm. In: 2018 15th Learning and Technology Conference (L T), pp. 96–101 (2018). DOI 10.1109/LT.2018.8368491
75. RS Components: 11 Internet of Things (IoT) Protocols You Need to Know About (2015). https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about
76. Satam, P., Pacheco, J., Hariri, S., Horani, M.: Autoinfotainment Security Development Framework (ASDF) for Smart Cars. In: International Conference on Cloud and Autonomic Computing (ICCAC), pp. 153–159 (2017). DOI 10.1109/ICCAC.2017.22
77. Schinianakis, D.: Alternative Security Options in the 5G and IoT Era. IEEE Circuits and Systems Magazine **17**(4), 6–28 (2017). DOI 10.1109/MCAS.2017.2757080
78. Schneier, B.: IoT Security: What's Plan B? IEEE Security Privacy **15**(5), 96–96 (2017). DOI 10.1109/MSP.2017.3681066
79. Sedjelmaci, H., Senouci, S.M., Ansari, N.: A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems pp. 1–13 (2017). DOI 10.1109/TSMC.2017.2681698
80. Sedjelmaci, H., Senouci, S.M., Messous, M.A.: How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network? In: IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2016). DOI 10.1109/GLOCOM.2016.7841878
81. Sengupta, A.: Intellectual property cores: Protection designs for ce products. IEEE Consumer Electronics Magazine **5**(1), 83–88 (2016). DOI 10.1109/MCE.2015.2484745
82. Sengupta, A.: Hardware vulnerabilities and their effects on ce devices: Design for security against trojans [hardware matters]. IEEE Consumer Electronics Magazine **6**(3), 126–133 (2017). DOI 10.1109/MCE.2017.2684940
83. Sengupta, A., Kundu, S.: Guest editorial securing iot hardware: Threat models and reliable, low-power design solutions. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **25**(12), 3265–3267 (2017). DOI 10.1109/TVLSI.2017.2762398
84. Sengupta, A., Roy, D.: Antipiracy-aware ip chipset design for ce devices: A robust watermarking approach [hardware matters]. IEEE Consumer Electronics Magazine **6**(2), 118–124 (2017). DOI 10.1109/MCE.2016.2640622
85. Sengupta, A., Roy, D., Mohanty, S.P.: Triple-phase watermarking for reusable ip core protection during architecture synthesis. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **37**(4), 742–755 (2018). DOI 10.1109/TCAD.2017.2729341
86. Shen, H., Tan, H., Li, H., Zhang, F., Li, X.: LMDet: A "Naturalness" Statistical Method for Hardware Trojan Detection. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **26**(4), 720–732 (2018). DOI 10.1109/TVLSI.2017.2781423
87. Shepard, D.P., Bhatti, J.A., Humphreys, T.E., Fansler, A.A.: Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. In: ION GNSS Meeting, pp. 1–15 (2012)

88. Shepard, D.P., Humphreys, T.E.: Characterization of Receiver Response to Spoofing Attacks. In: ION GNSS Meeting, pp. 1–11 (2011)
89. Shila, D.M., Geng, P., Lovett, T.: I Can Detect You: Using Intrusion Checkers to Resist Malicious Firmware Attacks. In: IEEE Symposium on Technologies for Homeland Security (HST), pp. 1–6 (2016). DOI 10.1109/THS.2016.7568958
90. Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karliychuk, T.: Smart IoT Devices in the Home: Security and Privacy Implications. IEEE Technology and Society Magazine **37**(2), 71–79 (2018). DOI 10.1109/MTS.2018.2826079
91. Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karliychuk, T.: Smart IoT Devices in the Home: Security and Privacy Implications. IEEE Technology and Society Magazine **37**(2), 71–79 (2018). DOI 10.1109/MTS.2018.2826079
92. Soja, R.: Automotive Security: From Standards to Implementation. https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf
93. Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., Lung, C.H.: Smart Home: Integrating Internet of Things with Web Services and Cloud Computing. In: IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 2, pp. 317–320 (2013). DOI 10.1109/CloudCom.2013.155
94. c. Son, S., w. Kim, N., t. Lee, B., Cho, C.H., Chong, J.W.: A Time Synchronization Technique for Coap-Based Home Automation Systems. IEEE Transactions on Consumer Electronics **62**(1), 10–16 (2016). DOI 10.1109/TCE.2016.7448557
95. Storm, D.: Black Hat Europe: It's Easy to Hack Self-Driving Car Sensors (2015). https://www.computerworld.com
96. Sun, D.Z., Zhong, J.D.: A Hash-Based RFID Security Protocol for Strong Privacy Protection. IEEE Transactions on Consumer Electronics **58**(4), 1246–1252 (2012). DOI 10.1109/TCE.2012.6414992
97. Sundaravadivel, P., Mohanty, S.P., Kougianos, E., Albalawi, U.: An energy efficient sensor for thyroid monitoring through the iot. In: Proceedings of the 17th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE), pp. 1–4 (2016). DOI 10.1109/EuroSimE.2016.7463377
98. Surendran, S., Nassef, A., Beheshti, B.D.: A Survey of Cryptographic Algorithms for IoT Devices. In: 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1–8 (2018). DOI 10.1109/LISAT.2018.8378034
99. Thompson, D.R., Di, J., Daugherty, M.K.: Teaching RFID Information Systems Security. IEEE Transactions on Education **57**(1), 42–47 (2014). DOI 10.1109/TE.2013.2264289
100. UAV, T.: https://www.theuav.com/
101. Unwala, I., Taqvi, Z., Lu, J.: Iot security: Zwave and thread. In: 2018 IEEE Green Technologies Conference (GreenTech), pp. 176–182 (2018). DOI 10.1109/GreenTech.2018.00040
102. V. P. Yanambaka and S. P. Mohanty and E. Kougianos: Secure Multi-Key Generation Using Ring Oscillator based Physical Unclonable Function. In: Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 200–205 (2016)
103. Valea, E., Silva, M.D., Natale, G.D., Flottes, M.L., Dupuis, S., Rouzeyre, B.: SI ECCS: SECure Context Saving for IoT Devices. In: 2018 13th International Conference on Design Technology of Integrated Systems In Nanoscale Era (DTIS), pp. 1–2 (2018). DOI 10.1109/DTIS.2018.8368561
104. Vattem, S., Anjali, T.: Complete RFID Security Solution for Inventory Management Systems. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 179–183 (2017). DOI 10.1109/ICACCI.2017.8125837
105. Wang, J., Zhu, R., Liu, S.: A Differentially Private Unscented Kalman Filter for Streaming Data in IoT. IEEE Access **6**, 6487–6495 (2018). DOI 10.1109/ACCESS.2018.2797159
106. Wu, H.T., Horng, G.J.: Establishing an intelligent transportation system with a network security mechanism in an internet of vehicle environment. IEEE Access **5**, 19,239–19,247 (2017). DOI 10.1109/ACCESS.2017.2752420
107. Wu, J.H., Scholvin, J., del Alamo, J.A., Jenkins, K.A.: A Faraday Cage Isolation Structure for Substrate Crosstalk Suppression. IEEE Microwave and Wireless Components Letters **11**(10), 410–412 (2001). DOI 10.1109/7260.959312
108. Xiao, F., Miao, Q., Xie, X., Sun, L., Wang, R.: Indoor Anti-Collision Alarm System Based on Wearable Internet of Things for Smart Healthcare. IEEE Communications Magazine **56**(4), 53–59 (2018). DOI 10.1109/MCOM.2018.1700706
109. Xiao, J., Feng, H.: A Low-Cost Extendable Framework for Embedded Smart Car Security System. In: 2009 International Conference on Networking, Sensing and Control, pp. 829–833 (2009). DOI 10.1109/ICNSC.2009.4919387
110. Xue, H., Ren, S.: Self-Reference-Based Hardware Trojan Detection. IEEE Transactions on Semiconductor Manufacturing **31**(1), 2–11 (2018). DOI 10.1109/TSM.2017.2763088
111. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things. In: Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 172–177 (2016)
112. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things. In: Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 172–177 (2016)
113. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT. IEEE Potentials **93**(3), 429–441 (2017)
114. Yanambaka, V.P., Mohanty, S.P., Kougianos, E., Ghai, D.: Nanoscale high-κ/metal gate CMOS and FinFET based logic libraries, *Nano-CMOS and Post-CMOS Electronics: Devices and Modelling*, vol. 1, chap. 6, pp. 169–211. Institute of Engineering and Technology (2015). DOI 978-1-84919-997-1
115. Yang, T., Kong, L., Xin, W., Hu, J., Chen, Z.: Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems. In: 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, pp. 2232–2236 (2012). DOI 10.1109/FSKD.2012.6234155

Chapter 03

Trojan Security Aware DSP IP Core and Integrated Circuits

This chapter discusses different security approaches to design digital signal processing (DSP) cores that have detection capability against functional type Hardware Trojan in a global supply chain. In the current design and fabrication supply chain, design houses, circuits and system core vendors, and manufacturing houses are globally scattered. It is quite possible that Trojan can be inserted in this design and manufacturing supply chain by anyone involved at any phase. Such Trojans can give backdoors to hackers and affect the operation of the system that uses such as infected hardware. In a worst case, in critical applications such as aircrafts, medical devices etc can be completely stopped from functioning causing catastrophic consequences. The chapter is organized as follows: Section 2 discusses different features and threat model of hardware Trojan; Section 3 explains how a Trojan could be inserted in a 3PIP core and why it is difficult to detect; Section 4 discusses different hardware Trojan security approaches that are available in the literature with emphasis on DSP cores; Section 5 presents definition, goal and design evaluation models for Trojan security aware DSP IP core; Section 6 discusses design process of Trojan secured DSP IP core; Section 7 presents analysis and comparison of different Trojan security approach for DSP IP core; finally we conclude this chapter in Section 8.

3.1. Introduction

Use of heterogeneous System-on-Chip (SoC) architecture in modern Consumer Electronics (CE) devices such as smartphones, gaming consoles, tablets, digital cameras, etc. have become a common practice in the semiconductor industry. The in-house SoC designer or the system integrator mostly imports Intellectual Property (IP) cores from third party IP vendors to minimize the design

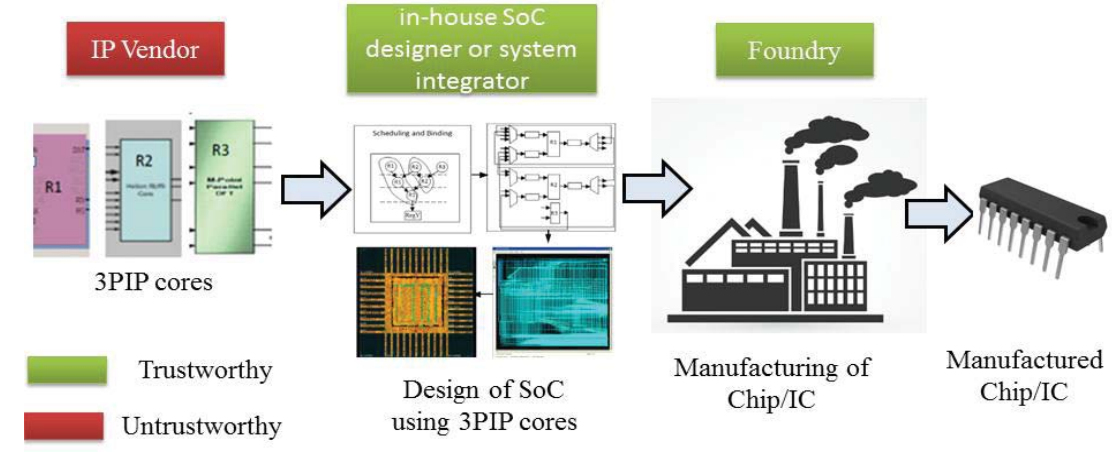

Fig.3.1. Design flow of a SoC

References

R. S. Chakraborty, S. Narasimhan, S. Bhunia (2009), 'Hardware Trojan: Threats and emerging solutions', *Proc. IEEE Int. High Level Design Validation Test Workshop*, pp. 166-171.

M. Tehranipoor, F. Koushanfar (2010), 'A survey of hardware Trojan taxonomy and detection', *IEEE Design Test Comput.*, vol. 27 (1), pp. 10-25.

R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, S. Bhunia (2009a), 'MERO: A statistical approach for hardware Trojan detection', *Proc. Workshop Cryptograph. Hardware Embedded Syst.*, pp. 396-410.

A. Sengupta (2017), 'Hardware Vulnerabilities and Their Effects on CE Devices: Design for Security Against Trojans,' in *IEEE Consumer Electronics Magazine*, vol. 6 (3), pp. 126-133.

A. Sengupta, S. Kundu (2017), 'Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions' in *IEEE Trans. on VLSI Systems*, vol. 25 (12), pp. 3265-3267.

F. Wolff et al. (2008), 'Towards Trojan-free trusted ICs: Problem analysis and detection scheme', *Design, Automation and Test in Europe*, pp. 1362-1365.

D. Agrawal et al (2007), 'Trojan detection using IC fingerprinting', *IEEE Symp. on Security and Privacy*, pp. 296-310.

M. Banga and M.S. Hsiao (2008), 'A region based approach for the identification of hardware Trojans', *IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 40-47.

R. Rad, J. Plusquellic and M. Tehranipoor (2010), 'A sensitivity analysis of power signal methods for detecting hardware Trojans under real process and environmental conditions', *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18 (12), pp. 1735-1744.

Y. Jin and Y. Makris (2008), 'Hardware Trojan detection using path delay fingerprint', *IEEE International Workshop on Hardware-Oriented Security and Trust,* pp. 51-57.

D. Rai and J. Lach (2009), 'Performance of delay-based Trojan detection techniques under parameter variations', *IEEE International Workshop on Hardware-Oriented Security and Trust,* pp. 58-65.

A. Sengupta and S. Bhadauria (2015), 'Untrusted Third Party Digital IP Cores: Power-Delay Trade-off Driven Exploration of Hardware Trojan Secured Datapath during High Level Synthesis' *In Proceedings of the 25th edition on Great Lakes Symposium on VLSI (GLSVLSI '15).* ACM, New York, NY, USA, pp. 167-172.

M. Banga and M. S. Hsiao (2009), 'A novel sustained vector technique for the detection of hardware Trojans,' in *Proc. 22nd Int. Conf. VLSI Design*, pp. 327–332.

S. Narasimhan et al. (2010), 'Multiple-parameter side-channel analysis: A noninvasive hardware Trojan detection approach,' in *IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 13–18.

C. Liu, J. Rajendran, C. Yang and R. Karri (2014), 'Shielding Heterogeneous MPSoCs From Untrustworthy 3PIPs Through Security- Driven Task Scheduling,' *IEEE Transactions on Emerging Topics in Computing*, vol. 2 (4), pp. 461-472.

S. Bhunia et al. (2013), 'Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution,' in *IEEE Design & Test*, vol. 30 (3), pp. 6-17.

A. Sengupta and R. Sedaghat (2011), 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, pp. 1-9.

A. Sengupta, and R. Sedaghat (2013), 'System and methodology for development of a system architecture using optimization parameters', *US Patent by United Sates Patent and Trademark Office (USPTO)*, Patent no. US 8,397,204.

F. Koushanfar and A. Mirhoseini (2011), 'A unified framework for multimodal submodular integrated circuits Trojan detection,' *IEEE Trans. Inf. Forensics Security*, vol. 6 (1), pp. 162–174.

J. Rajendran, H. Zhang, O. Sinanoglu and R. Karri (2013), 'High-level synthesis for security and trust,' *IEEE 19th International On-Line Testing Symposium (IOLTS)*, pp. 232-233.

A. Sengupta, S. Bhadauria and S. P. Mohanty (2017a), 'Low-cost security aware HLS methodology,' in *IET Computers & Digital Techniques*, vol. 11 (2), pp. 68-79.

A. Sengupta, S. Bhadauria, and S. P. Mohanty (2017b), 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 36 (4), pp. 655–668.

A. Sengupta, D. Roy, S. Bhadauria (2017c), 'Low cost optimized Trojan secured schedule at behavioral level for single & Nested loop control data flow graphs', *Integration, the VLSI Journal*, vol. 58, pp. 378-389.

O. Sinanoglu, N. Karimi, J. Rajendran, R. Karri, Y. Jin, K. Huang, Y. Makris (2013),'Reconciling the IC Test and Security Dichotomy', *18th IEEE European Test Symposium (ETS)*, pp. 176 – 181.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran (2018a), 'A Framework for Hardware Efficient Reusable IP Core for Grayscale Image CODEC,' in IEEE Access, vol. 6, pp. 871-882.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran (2018b), 'Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware,' in *IEEE Transactions on Consumer Electronics*, (accepted).

X. Cui, K. Ma, L. Shi and K. Wu (2014), 'High-level synthesis for run-time hardware Trojan detection and recovery,' *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, pp. 1-6.

A. J. Hu (1997), 'Formal hardware verification with BDDs: An introduction,' in *Proc. IEEE Pac. Rim Conf. Commun. Comput. Signal Process.* 10 Years PACRIM 1987-1997 Netw. Pac. Rim, vol. 2. Victoria, BC, Canada, pp. 677–682.

M. Bushnell and V. Agrawal (2013), 'Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits', New York, NY, USA: Springer, 2013.

H. Salmani, M. Tehranipoor, and J. Plusquellic (2009), 'New design strategy for improving hardware Trojan detection and reducing Trojan activation time,' in *Proc. IEEE Int. Workshop Hardware Oriented Security Trust (HOST)*, pp. 66–73.

X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic (2008), 'Hardware Trojan detection and isolation using current integration and localized current analysis,' in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Syst. (DFTVS)*, pp. 87–95.

A. Sengupta (2016), 'Intellectual Property Cores: Protection designs for CE products,' *IEEE Consumer Electronics Mag.*, vol. 5 (1), pp. 83– 88.

S. Salivahanan, A. Vallavaraj, C. Gnanapriya (2000), 'Digital signal processing' Tata McGraw-Hill, ISBN 007463996X , vol. xiii, pp. 808.

A. Obukhov and A. Kharlamov (2008) 'Discrete Cosine Transform for 8x8 Blocks with CUDA' Nvidia whitepaper document.

Chapter 04

IP Core and Integrated Circuit Protection using Robust Watermarking

This chapter discusses robust watermarking approaches for the ownership protection of hardware cores (aka IP cores). Watermarking ensures some additional attributes inserted in the hardware core such a way that it can be used to verify ownership of the hardware core when required. Robust watermarking approaches have been discussed as these are resilient to various attacks that happen in global supply chain for various reasons. The remaining chapter is structured as follows: Section 2 provides an overview on selected hardware/IP core watermarking approaches; Section 3 discusses design process of watermarked IP core; Section 4 analyses the hardware watermarking approaches on case studies/test cases; finally, Section 5 draws the conclusion.

4.1. Introduction

A watermark is a secret mark implanted into an entity such as official documents, currency notes, postal stamps, audio/video files etc. to protect ownership right of an owner. Usually, a watermark embedded into an entity is expected to preserve its quality and functionality. However, for the domains in which watermarking is applied such as audio/video, documents etc., slight degradation of the quality is usually noticed. Given the advantages of a watermark, it may be considered an extremely useful tool for protecting hardware (e.g. DSP core) ownership as well. However, the prime difference from watermarking in other domains is zero tolerance towards modification of quality/functionality of the hardware design. This makes hardware watermarking challenging but extremely useful for protecting legal rights of an intellectual property (IP) vendor/owner. It is widely acknowledged that complex consumer electronics system design relies heavily on DSP IP cores realized as system-on-chip (SoC). Thus hardware watermarking plays an integral role in IP core protection of CE devices (Mohanty et al., 2017; Voyatzis et al., 1999; Cox et al., 2006; Roy et al., 2013; Sengupta, 2017).

In the modern era of consumer electronics (CE), use of DSP intellectual property cores in global supply chains become an inexorable part of complex SoC design process. IP cores not only speedup the design productivity massively but also decreases the design period immensely. Importing these IP cores from third-party IP vendors by the system integrator or SoC designer has become a common industry practise. Previously, IP vendors have mainly focused on IP performance and IP functionality but have neglected IP security. As evidence it can be observed that in a typical IP design flow, measurement of performance and functionality is only included in the IP specification. However, prevailing usage of IP cores in SoC design process increases the

References

S. P. Mohanty, A. Sengupta, P. Guturu and E. Kougianos (2017), 'Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection: From paper marks to hardware protection,' IEEE *Consumer Electronics Magazine*, vol. 6 (3), pp. 83-91.

A. Sengupta (2016), 'Intellectual Property Cores: Protection designs for CE products,' *IEEE Consumer Electronics Mag.*, vol. 5 (1), pp. 83– 88.

G. Voyatzis and I. Pitas (1999), "The use of watermarks in the protection of digital multimedia products," Proc. IEEE, vol. 87, no. 7, pp. 1197–1207.

J. Cox, G. Doërr, and T. Furon (2006), "Watermarking is not cryptography,"in Proc. Int. Workshop Digital Watermarkingpp 1–15.

S. D. Roy, X. Li, Y. Shoshan, A. Fish, and O. Yadid-Pecht (2013), "Hardware implementation of a digital watermarking system for video authentication," IEEE Trans. Circuits Syst. Video Technol., vol. 23, no. 2,pp. 289–301.

A. Sengupta, S. Bhadauria, and S. P. Mohanty (2017), 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 36 (4), pp. 655–668.

Y. Alkabani and F. Koushanfar (2008), ``Active control and digital rights management of integrated circuit IP cores," in Proc. Int. Conf. Compil., Archit. Synth. Embedded Syst. (CASES), pp. 227-234.

F. Koushanfar, I. Hong, and M. Potkonjak (2005), "Behavioral synthesis techniques for intellectual property protection", ACM Trans. Des. Autom. Electron. Syst., vol. 10 (3), pp. 523-545.

D. Ziener and J. Teich (2008), 'Power signature watermarking of IP cores for FPGAs,'' J. Signal Process. Syst., vol. 51 (1), pp. 123-136.

B. Le Gal and L. Bossuet (2012), 'Automatic low-cost IP watermarking technique based on output mark insertions,' Design Autom. Embedded Syst., vol. 16 (2), pp. 71–92.

A. Sengupta and S. Bhadauria (2016), 'Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis*,' IEEE Access*, 2016, vol. 4, pp. 2198–2215.

A. Sengupta, D. Roy and S. P. Mohanty (2018), 'Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis,' in *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. PP, pp. 1-1.

A. Sengupta and R. Sedaghat (2011), 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, pp. 1-9.

A. Sengupta et al (2013) "System and methodology for development of a system architecture using optimization parameters", *US Patent by United Sates Patent and Trademark Office (USPTO)*, Patent no. US 8,397,204.

J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls (2008), 'Brand and IP protection with physical unclonable functions,' in *Proc.IEEE Int. Sym. on Circuits and Systems*, pp. 3186–3189.

A. Sengupta and D. Roy (2017), 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach', in *IEEE Consumer Electronics Mag.*, April 2017, vol. 6 (2), pp. 118-124.

S. Salivahanan, A. Vallavaraj, C. Gnanapriya (2000), 'Digital signal processing' Tata McGraw-Hill, ISBN 007463996X , vol. xiii, pp. 808.

NanGate 15 nm open cell library. Available: http: //www.nangate.com/?pageid=2328, last accessed on 2018.

DSP benchmark suite. Available: http://www.ece.ucsb.edu/ EXPRESS/benchmark/, last accessed on 2018.

S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*. McGraw- Hill Education, 2015, no. 0071825711.

Altera Quartus, Available: https://dl.altera.com/13.0sp1, , last accessed on 2018.

Cyclone II FPGA, Available: https://www.altera.com/products/fpga/cyclone-series/cyclone-ii/overview.html, last accessed on 2018.

P. Coussy, D. D. Gajski, M. Meredith and A. Takach (2009), "An Introduction to High-Level Synthesis," in IEEE Design & Test of Computers, vol. 26, no. 4, pp. 8-17.

A. Sengupta (2017), 'Hardware Security of CE Devices,' *IEEE Consumer Electronics Mag.*, vol. 6 (1), pp. 130–133.

Chapter 05

Symmetrical Protection of DSP IP Core and Integrated Circuits using Fingerprinting and Watermarking

This chapter discusses the use of watermarking and fingerprinting for symmetrical protection of DSP IP cores and integrated circuits. Symmetrical IP core protection is a mechanism in which both seller and buyers of an IP can have signature for double-proof of ownership and whereas significantly reducing false ownership claims. The chapter is structured as follows: Section 2 discusses the fundamentals of IP core protection with emphasis on symmetrical IP core protection techniques for DSP cores; Section 3 discusses the low-cost DSP core IP core protection; Section 4 explained that methodology with a motivational example. Section 5 discusses the results of that approach. The conclusion of this chapter is provided in Section 6.

5.1. Introduction

The designs of integrated circuits have evolved into greater sophistication than ever before with the revolution of implementation and application technology in Consumer Electronics (CE) industry. The usage of digital signal processing (DSP) Intellectual Property (IP) cores [1] generated using architectural synthesis not only maintains a proper balance between time-to-market pressure and design productivity but additionally help in design cost reduction. HLS [2, 4] is an automated design process that transforms an algorithmic/behavioral description of a digital circuit or IP into its corresponding Register Transfer Level (RTL) digital hardware through numerous sub-processes like scheduling, hardware and register allocation and binding. In the process of manufacturing an IP core two entities are involved viz. seller and buyer. An IP seller also known as IP vendor is the creator of an IP, whereas an IP buyer also known as IP user is the purchaser of an IP. However, to maintain a viable application of IP cores in composite SoC-based designs, protection of both the entities against threats is extremely crucial. Let us now discuss on the protection aspect of IP buyer and IP seller: In a IP core, an IP buyer may claim buyer privilege as a buyer so that the same IP copy should not be usable/accessible to his competitors in the market. This is possible when customized specifications of an IP core are obtained by an IP seller from an IP buyer, thus creating an exclusive one-to-one mapping between both parties. Embedding a unique buyer's signature (known as buyer fingerprint) into an IP core design facilitates detection of unlawfully redistributed/resold duplicates of an IP core by a deceitful seller [3]. Likewise, an IP seller must protect his design from piracy and false claim of ownership before selling it to an IP buyer. Embedding a unique seller's signature (known as seller watermark) into an IP core design protects an IP core from ownership abuse [5-11] [35-38].

References

[1] E. Castillo, U. Meyer-Baese, A. Garca, L. Parrilla, A. Lloris, 'IPP@HDL: Efficient intellectual property protection scheme for IP cores', *IEEE Trans. Very large Scale Integr. (VLSI) Syst.*, 2007, vol. 15 (5), pp. 578–591.

[2] A. Sengupta and R. Sedaghat, 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, 2011, pp. 1-9.

[3] Q. Gang, M. Potkonjak, 'Intellectual Property Protection in VLSI Designs: Theory and Practice', *Springer Science & Business Media*, 2007.

[4] A. Sengupta, and R. Sedaghat, 'System and methodology for development of a system architecture using optimization parameters', Google Patents, 2013, https://www.google.com/patents/US8397204.

[5] Y. Alkabani, F. Koushanfar, M. Potkonjak, 'Remote activation of ICs for piracy prevention and digital right management', in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, Nov. 2007, pp. 674–677.

[6] A. Sengupta, S. Kundu, 'Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions' in *IEEE Trans. on VLSI Systems*, 2017, vol. 25 (12), , pp. 3265-3267.

[7] A. Sengupta, S. Bhadauria, and S. P. Mohanty, 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, April 2017, vol. 36 (4), pp. 655–668.

[8] E. Kougianos, S.P. Mohanty, R.N. Mahapatra, 'Hardware assisted watermarking for multimedia', *Comput. Elect. Eng.*, 2009, vol. 35 (2) pp. 339–358.

[9] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, 'Handbook of Fingerprint Recognition', *Springer, New York*, NY, USA, 2009.

[10] J.A. Roy, F. Koushanfar, I.L. Markov, 'EPIC: Ending piracy of integrated circuits', in *Proc. Design, Autom. Test Europe (DATE)*, Mar. 2008, pp. 1069–1074.

[11] Y. Alkabani, F. Koushanfar, 'Active control and digital rights management of integrated circuit IP cores', in *Proc. Int. Conf. Compil., Archit. Synth. Embedded Syst. (CASES)*, 2008, pp. 227–234.

[12] L. Yuan, G. Qu, L. Ghouti, A. Bouridane, 'VLSI design IP protection: Solutions, new challenges, and opportunities', in *Proc. 1st NASA/ESA Conf. Adapt. Hardw. Syst. (AHS)*, 2006, pp. 469–476.

[13] T. Yu, Y. Zhu, 'A new watermarking method for soft IP protection', in *Proc. Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2011, pp. 3839–3842.

[14] A. Sengupta, S. Bhadauria, 'Exploring low cost optimal watermark for reusable IP cores during high level synthesis', *IEEE Access J.*, 2016, vol. 4 (99) pp. 2198–2215.

[15] S.P. Mohanty, N. Ranganathan, V. Krishna, 'Datapath scheduling using dynamic frequency clocking', in *Proc. of the IEEE Computer Society Annual Symposium on VLSI*, 2002, pp. 58–63.

[16] S.P. Mohanty, M. Gomathisankaran, E. Kougianos, 'Variability- aware architecture level optimization techniques for robust nanoscale chip design', *Comput. Electr. Eng.*, 2014, vol. 40 (1) pp. 168–193.

[17] S.P. Mohanty, 'Nanoelectronic Mixed-Signal System Design', *McGraw- Hill Education*, 2015.

[18] F. Koushanfar, I. Hong, M. Potkonjak, 'Behavioral synthesis techniques for intellectual property protection', *ACM Trans. Design Autom. Electron. Syst.,* 2005, vol. 10 (3), pp. 523–545.

[19] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, 'Digital Watermarking and Steganography', *Morgan Kaufmann*, San Mateo, CA, USA, 2007.

[20] D. Ziener, J. Teich, 'FPGA core watermarking based on power signature analysis', in *Proc. IEEE Int. Conf. Field Program. Technol. (FPT)*, Dec. 2006, pp. 205–212.

[21] T. Nie, L. Zhou, Y. Li, 'Hierarchical watermarking method for FPGA IP protection', *IETE Tech. Rev.*, 2013, vol. 30 (5) pp. 367–374.

[22] D. Ziener, J. Teich, 'Power signature watermarking of IP cores for FPGAs', *J. Signal Process. Syst.*, 2008, vol. 51 (1), pp. 123–136.

[23] I. Hong, M. Potkonjak, 'Behavioral synthesis techniques for intellectual property protection', in *Proc. 36th Annu. ACM/IEEE Design Autom. Conf.*, Jun. 1999, pp. 849–854.

[24] B. Le Gal, L. Bossuet, 'Automatic low-cost IP watermarking technique based on output mark insertions', *Design Autom. Embedded Syst.*, 2012, vol. 16 (2), pp. 71–92.

[25] A. Sengupta, S. Bhadauria, S. Mohanty, 'Embedding low cost optimal watermark during high level synthesis for reusable IP core protection', in *Proc. of 48th IEEE Int'l Symposium on Circuits & Systems (ISCAS)*, Montreal, May 2016, pp. 974–977.

[26] J. Lach, W.H. Mangione-Smith, M. Potkonjak, 'Fingerprinting techniques for field-programmable gate array intellectual property protection', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2001, vol. 20 (10) pp. 1253–1261.

[27] S. Hada, 'Zero-knowledge and code obfuscation', in *Advances in Cryp- Tology, Springer*, Berlin, Germany, 2000, pp. 443–457.

[28] R.S. Chakraborty, S. Bhunia, 'HARPOON: An obfuscation based SoC design methodology for hardware protection', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2009, vol. 28 (10) pp. 1493–1502.

[29] J.L. Wong, D. Kirovski, M. Potkonjak, 'Computational forensic techniques for intellectual property protection', *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 2004, vol. 23 (6), pp. 987–994.

[30] A. Sengupta, D. Kachave, 'Forensic engineering for resolving ownership problem of reusable IP core generated during high level synthesis', in *Future Generation Computer Systems*, 2018, vol. 80, pp. 29-46,

[31] A. Sengupta, D. Roy, S. P. Mohanty, and P. Corcoran, 'DSP Design Protection in CE through Algorithmic Transformation Based Structural Obfuscation', *IEEE Transactions on Consumer Electronics* , 2017, vol. 63 (4), pp. 467-476.

[32] D. Roy, A. Sengupta, 'Low overhead symmetrical protection of reusable IP core using robust fingerprinting and watermarking during high level synthesis', *Future Generation Computer Systems*, 2017, vol. 71, pp. 89-101.

[33] NanGate 15 nm open cell library. [Online]. Available: http: //www.nangate.com/?pageid=2328, last accessed on June 2017.

[34] DSP benchmark suite. [Online]. Available: http://www.ece.ucsb.edu/ EXPRESS/benchmark/, last accessed on June 2017.

[35] A. Sengupta, 'Hardware Security of CE Devices,' *IEEE Consumer Electronics Mag.*, Jan 2017, vol. 6 (1), pp. 130–133.

[36] A. Sengupta, 'Intellectual Property Cores: Protection designs for CE products,' *IEEE Consumer Electronics Mag.*, Jan 2016, vol. 5 (1), pp. 83– 88.

[37] A. Sengupta and D. Roy, 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach', in *IEEE Consumer Electronics Mag.*, April 2017, vol. 6 (2), pp. 118-124.

[38] A. Sengupta, D. Roy and S. P. Mohanty, 'Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis,' in *IEEE Trans. on CAD of Integrated Circuits and Systems*, Volume 37, Issue 4, 2018, pp. 742--755.

Chapter 06

Computational Forensic Engineering for Resolving Ownership Conflict of DSP IP Core

The previous few chapters focused on watermarking and fingerprinting for ownership protection. This chapter will focus on another technique called forensic engineering for ownership protection. Forensic engineering extracts features of IP cores and matches to statistically suggest the original ownership. This section discusses various steps involved in forensic engineering of a hard IP core as well as presents specific details with case study examples.

6.1. Introduction

The rapid proliferation of electronic/system-on-chip (SoC) industry along with fierce competition has demanded ways to remain competent. To beat the competition, companies seek to reduce time-to-market and design cost. These goals can be easily met through utilisation of reusable IP core(s) [4],[9]. This is because reusable IP core(s) minimise design time by reducing man-hours required to reproduce an IP. Therefore, reusable IP core has become a mandatory component of generic SoC/IC design flow. Moreover, a design process at higher level of design abstraction such as High Level Synthesis (HLS) is always crucial for complex SoCs such as DSP/multimedia cores [29],[30]. This is because higher level of design abstraction reduces design complexity and identifies optimal (low cost) design architecture based on several orthogonal design objectives. Therefore, reusable IP core(s) such as DSP/multimedia core generated through HLS is an essential component for consumer electronics devices. However, an IP core is vulnerable to various threats such as IP piracy, Trojan insertion, IP overbuilding, false claim of ownership, etc [31], [32], [40]. An estimate based on report presented in [1] shows that electronics industry loose roughly minimum 1.5 trillion USD annually due to piracy and counterfeiting [2]. Therefore, it becomes mandatory to devise methodologies that can safeguard an IP core from these aforementioned threats. There are several IP protection mechanisms to overcome these threats, as shown in Fig.6.1.

Another technique that targets protection of IP core(s) is hardware obfuscation. Obfuscation targets protection against IP piracy and Trojan insertion [32]. Hardware obfuscation aims to obfuscate a design through either structural obfuscation [5],[38] or functional obfuscation [6]. The primary aim is to increase effort of an attacker to identify correct functionality of an IP [32], thus making it hard for an attacker to secretly insert Trojan that can go undetectable during testing phase of an IC design. Further, this also makes it difficult to re-sell or utilise an IP core because its correct functionality is unknown to an adversary. Obfuscation does not aim to provide protection against ownership conflict (since it does not insert a unique ID or signature). However, functional

References

[1] "Estimating the global economic and social impacts of counterfeiting and piracy," Int. Chamber Commerce, Paris, France,Tech. Rep., 2011.

[2] J. Zhang, "A Practical Logic Obfuscation Technique for Hardware Security," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 3, , March 2016 pp. 1193-1197.

[3] Farinaz Koushanfar and Gang Qu. "Hardware metering." In Proceedings of the *38th annual design automation conference*, ACM 2001, pp. 490-493.

[4] A. Sengupta, "Intellectual Property Cores: Protection designs for CE products," in *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 83-88, Jan. 2016.

[5] A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran, "DSP design protection in CE through algorithmic transformation based structural obfuscation," in *IEEE Transactions on Consumer Electronics*, vol. 63, no. 4, pp. 467-476, November 2017.

[6] Y. Lao and K. K. Parhi, "Protecting DSP circuits through obfuscation," *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, Melbourne VIC, 2014, pp. 798-801.

[7] A. Sengupta, S. Bhadauria and S. P. Mohanty, "Embedding low cost optimal watermark during high level synthesis for reusable IP core protection," *2016 IEEE Int. Sym. on Circuits and Systems (ISCAS),* Montreal, QC, 2016, pp. 974-977.

[8] Franke K., Srihari S.N. (2008) Computational Forensics: An Overview. In: Srihari S.N., Franke K. (eds) Computational Forensics. IWCF 2008. Lecture Notes in Computer Science, vol 5158. Springer, Berlin, Heidelberg.

[9] Deepak Kachave, Anirban Sengupta "Protecting Ownership of Reusable IP Core Generated during High Level Synthesis', *Proc. IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Dec 2016, pp. 80 – 82.

[10] Anirban Sengupta, Deepak Kachave, "Forensic Engineering for Resolving Ownership Problem of Reusable IP Core generated during High Level Synthesis", *Elsevier Journal on Future Generation Computer Systems*, (Accepted). https://doi.org/10.1016/j.future.2017.08.001

[11] J. L. Wong, D. Kirovski and M. Potkonjak, "Computational forensic techniques for intellectual property protection," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 23, no. 6, pp. 987-994, June 2004.

[12] D. S. Harish Ram, M. C. Bhuvaneswari, and S. M. Logesh, (2011) "A novel evolutionary technique for multi-objective power, area and delay optimization in high level synthesis of datapaths," in *Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI '11),* pp. 290–295.

[13] T. Inoue, H. Henmi, Y. Yoshikawa and H. Ichihara (2011) "High-level synthesis for multi-cycle transient fault tolerant datapaths." *2011 IEEE 17th International On-Line Testing Symposium*, pp. 13 – 18.

[14] Sengupta, Anirban, and Reza Sedaghat (2015) "Swarm intelligence driven design space exploration of optimal k-cycle transient fault secured datapath during high level synthesis based on user power–delay budget." *Elsevier Journal on Microelectronics Reliability*, Vol 55, Issue 6, pp. 990-1004.

[15] Koushanfar F, I. Hong, and M. Potkonjak (2005) ‘‘Behavioral synthesis techniques for intellectual property protection,’’ *ACM Transactions on Design Automation of Electronic Syst*ems, vol. 10, no. 3, pp. 523–545.

[16] J. Rajendran, H. Zhang, O. Sinanoglu and R. Karri (2013) "High-level synthesis for security and trust," *IEEE 19th International On-Line Testing Symposium (IOLTS)*, Chania, pp. 232-233.

[17] Vipul Kumar Mishra, Anirban Sengupta (2014) “MO-PSE: Adaptive multi-objective particle swarm optimization based design space exploration in architectural synthesis for application specific processor design”, *Elsevier Journal on Advances in Engineering Software*, Volume 67, pp. 111-124.

[18] Sengupta, Anirban, and Saumya Bhadauria (2015) "Bacterial foraging driven exploration of multi cycle fault tolerant datapath based on power-performance tradeoff in high level synthesis." *Expert Systems with Applications*, Vol 42, Issue 10, pp. 4719-4732.

[19] Deepak Kachave, Anirban Sengupta "Forensic Engineering for resolving ownership conflict of reusable IP cores generated during High Level Synthesis", *IEEE VLSI Circuits & Systems Letter***,** Volume 2, Issue 2, 2017, pp. 15 – 18

[20] S. Nomura, et al., “Sampling + DMR: practical and low-overhead permanent fault detection”. In *Proceedings of the 38th annual international symposium on Computer architecture* (ISCA '11). ACM, New York, NY, USA, 201-212.

[21] Shu-Yi Yu and E. J. McCluskey, "Permanent fault repair for FPGAs with limited redundant area," *Proceedings 2001 IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, San Francisco, CA, 2001, pp. 125-133.

[22] S. D'Angelo, C. Metra and G. Sechi, "Transient and permanent fault diagnosis for FPGA-based TMR systems," *Defect and Fault Tolerance in VLSI Systems, 1999. DFT '99. International Symposium on*, Albuquerque, NM, 1999, pp. 330-338.

[23] A. Sengupta, D. Roy and S. P. Mohanty, "Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. PP, no. 99, pp. 1-1.

[24] P.G. Paulin, J.P. Knight, ‘Scheduling and Binding Algorithms for High-Level Synthesis’, *Proc. of 26th ACM/IEEE Design Automation Conference*, California, 1989, pp. 1 – 6.

[25] M. C. McFarland, ‘Tutorial on high-level synthesis’, *Proc. of 25th ACM/IEEE Design Automation Conference*, California, , 1988, pp. 330-336.

[26] S. Bhunia, M. Abramovici, D. Agrawal, P. Bradley, M. Hsiao, J Plusquellic, M Tehranipoor, 'Protection against hardware Trojan attacks: Towards a comprehensive solution', *Proc of IEEE Design & Test*, vol. 99, 2013, pp. 1–1.

[27] M. C. McFarland, 'The high-level synthesis of digital systems', *Proc. of IEEE*, 1990, vol.78 (2), pp. 301 – 318.

[28] X. Zhang, M. Tehranipoor, 'Case study: Detecting hardware Trojans in third-party digital IP cores'. *In Proc. of IEEE International Symposium on Hardware-Oriented Security and Trust*, California, 2011, pp. 67–70.

[29] A. Sengupta and R. Sedaghat, "Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration," *2011 12th International Symposium on Quality Electronic Design*, Santa Clara, CA, 2011, pp. 1-9.

[30] A. Sengupta, R. Sedaghat, "System and methodology for development of a system architecture using optimization parameters" U.S. patent US12974925, 21 December 2010.

[31] A. Sengupta, "Hardware Security of CE Devices [Hardware Matters]," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 130-133, Jan. 2017.

[32] 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* 35, no. 9 (2016): 1411-1424.

[33] A. Sengupta, S. Bhadauria and S. P. Mohanty, "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 4, pp. 655-668, April 2017.

[34] A. Sengupta and S. Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis," in *IEEE Access*, vol. 4, pp. 2198-2215, 2016.

[35] S. Gupta, 'Loop shifting and compaction for the high-level synthesis of designs with complex control flow', *Technical Report CECS-TR-03-14,* 2003, UC Irvine.

[36] N. K. S. Kurra, P.R. Panda, 'The impact of loop unrolling on controller delay in high level synthesis', Proc. *of IEEE Design, Automation and Test Europe (DATE)*, California, 2007, pp. 391-396.

[37] A. Sengupta and D. Roy, "Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach [Hardware Matters]," in *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 118-124, April 2017.

[38] L. Li and H. Zhou, "Structural transformation for best-possible obfuscation of sequential circuits," *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Austin, TX, 2013, pp. 55-60.

[39] Express benchmark suite, University of California San Diego, http://www.ece.ucsb.edu/EXPRESS/benchmark/.

[40] A. Sengupta and S. Kundu, "Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3265-3267, Dec. 2017.

Chapter 07

Structural Obfuscation of DSP Cores used in CE Devices

In the previous few chapters, watermarking, fingerprinting, and forensic engineering have been discussed for resolving various ownership related problems. This chapter discusses structural obfuscation approaches to thwart IP piracy and reverse engineering. This approach when effective can save billions of dollars of revenue losses to CE and semiconductor industry. Specifically, a multi –high level transformation based structural obfuscation process has been presented for DSP IP cores as hardware hardening technique. The chapter is structures as follows: Section 7.2 highlights the fundamentals of obfuscation with stress on structural obfuscation; Section 7.3 discusses different compiler transformation driven structural obfuscation methodology. Section 7.4 discusses low-cost structurally obfuscated design exploring technique. Section 7.5 demonstrates a multi-stage structural obfuscation technique through a motivational example. Section 7.6 presents the results of a case study.

7.1. Introduction

Today's Consumer Electronic (CE) devices, ranging from modern smart phone, smart TV, home appliance, set-top box, tablet, digicam to recent smart speaker, are designed using System-on-Chip (SoC) platforms (Thavalengal and Corcoran, 2016; Mohanty, 2015; Kim et al., 2015). These SoCs comprises of various system modules such as memory (SRAM, Flash), A-to-D converter, custom processor or co-processor, Digital Signal Processor (DSP) kernels, A/V codecs, wireless modems, etc. Among these modules, DSP kernels in the form of Intellectual Property (IP) cores are primarily responsible for data/power intensive computation at high speed, minimal silicon area and low power in a SoC (Li et al., 2015). Thus, DSP IP cores are the heart of every SoC based CE devices. For example, ConnX D2 DSP IP core used in telecom infrastructure of voice over internet protocol (VoIP) and wireless mobile device (ConnX, 2009). In a cellular telephone system, it is used in speech encoding/decoding process. Low-end

Fig. 7.1. A thematic representation of secured DSP IP core for CE devices that is resilient from adversary.

References

E. Castillo, U. Meyer-Baese, A. Garcia, L. Parrilla, A. Lloris, 'IPP@HDL: Efficient Intellectual Property Protection Scheme for IP Cores,' *IEEE Trans. Very Large Scale Integration Sys.*, 2007, vol. 15 (5), pp. 578–591.

H. Yang, N. Basutkar, P. Xue, K. Kim, and Y. H. Park, 'Software defined DVT-T2 demodulator using scalable DSP processors,' *IEEE Trans. on Consumer Electronics*, May 2013, vol. 59 (2), pp. 428–434.

M. Li, P. Zhang, C. Zhu, H. Jia, X. Xie, J. Cong, and W. Gao, 'High efficiency VLSI implementation of an edge-directed video up-scaler using high level synthesis,' in *Proc. IEEE Int. Conf. on Consumer Electronics (ICCE),* 2015, pp. 92–95.

A. Sengupta, 'Intellectual Property Cores: Protection designs for CE products,' *IEEE Consumer Electronics Mag.*, Jan 2016, vol. 5 (1), pp. 83– 88.

The Economic Impacts of Counterfeiting and Piracy, last modified: 02.03.2017. [Online]. Available: http://www.inta.org/Communications/ Documents/Forms/AllItems.aspx.

Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, 'Brand and IP protection with physical unclonable functions,' in *Proc. IEEE Int. Sym. on Circuits and Systems*, May 2008, pp. 3186–3189.

K. K. Parhi, 'Verifying equivalence of digital signal processing circuits,' in *Conf. Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2012, pp. 99–103.

Y. Lao and K. K. Parhi, 'Obfuscating DSP Circuits via High-Level Transformations,' *IEEE Trans. Very Large Scale Integration Sys.*, May 2015, vol. 23 (5), pp. 819–830.

S. Walz and Y. Schrder, 'A privacy-preserving system architecture for applications raising the energy efficiency,' in *Proc. IEEE Int. Conf. on Consumer Electronics (ICCE),* 2016, pp. 62–66.

A. Sengupta, 'Hardware Security of CE Devices,' *IEEE Consumer Electronics Mag.*, Jan 2017, vol. 6 (1), pp. 130–133.

S. P. Mohanty, *Nanoelectronic Mixed-Signal System Design*. McGraw- Hill Education, 2015, no. 0071825711.

J. Kim, E. s. Jung, Y. t. Lee, and W. Ryu, 'Home appliance control framework based on smart TV set-top box,' *IEEE Trans. on Consumer Electronics*, Aug 2015, vol. 61 (3), pp. 279–285.

S. Thavalengal and P. Corcoran, 'User Authentication on Smartphones: Focusing on iris biometrics,' *IEEE Consumer Electronics Mag.*, April 2016, vol. 5 (2), pp. 87–93.

A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, and S. Kundu, 'Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques,' *IEEE Trans. on Information Forensics and Security*, Jan 2017, vol. 12 (1), pp. 64–77.

M. Brzozowski and V. N. Yarmolik, 'Obfuscation as Intellectual Rights Protection in VHDL Language,' *in Computer Information Systems and Industrial Management Applications (CISIM),* June 2007, pp. 337–340.

C. Barria, D. Cordero, C. Cubillos, and R. Osses, 'Obfuscation procedure based in dead code insertion into crypter,' *in Int. Conf. on Computers Communications and Control (ICCCC),* May 2016, pp. 23–29.

J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, 'Security Analysis of Integrated Circuit Camouflaging,'*in Proc. ACM SIGSAC conference on Computer & communications security*, 2013, pp. 709–720.

R. S. Chakraborty and S. Bhunia, 'HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, Oct 2009, vol. 28 (10), pp. 1493–1502.

A.R. Desai, M.S. Hsiao, C. Wang, L. Nazhandali, S. Hall, 'Interlocking obfuscation for anti-tamper hardware,' in *Proceedings of Cyber Security and Information Intelligence Research Workshop (CSIIRW),* 2013, pp. 8:1–8:4.

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,' *IEEE Int.On-Line Testing Symposium (IOLTS)*, 2014, pp. 49-54.

Y. W. Lee and N. A. Touba, 'Improving logic obfuscation via logic cone analysis,' *Latin-American Test Symposium (LATS)*, 2015, pp. 1-6.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran, 'DSP design protection in CE through algorithmic transformation based structural obfuscation,' in *IEEE Transactions on Consumer Electronics*, November 2017, vol. 63 (4), pp. 467-476.

Y. M. Alkabani and F. Koushanfar, 'Active Hardware Metering for Intellectual Property Protection and Security,' *in Proc. USENIX Security Symposium,* 2007, pp. 20:1–20:16.

J. Zhang, 'A Practical Logic Obfuscation Technique for Hardware Security,' *IEEE Tran. Very Large Scale Integration Sys.*, March 2016, vol. 24 (3), pp. 1193–1197.

X. Wang, X. Jia, Q. Zhou, Y. Cai, J. Yang, M. Gao, and G. Qu, 'Secure and low-overhead circuit obfuscation technique with multiplexers,' *in GLSVLSI*, May 2016, pp. 133–136.

J. A. Roy, F. Koushanfar, and I. L. Markov, 'EPIC: Ending Piracy of Integrated Circuits,' *in DATE*, March 2008, pp. 1069–1074.

J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, 'Security analysis of logic obfuscation,' *in DAC, 2012*, June 2012, pp. 83–89.

J. Rajendran *et al*., 'Fault Analysis-Based Logic Encryption,' in *IEEE Transactions on Computers*, Feb. 2015, vol. 64 (2), pp. 410-424.

P. Subramanyan, S. Ray and S. Malik, 'Evaluating the security of logic encryption algorithms,' *IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST)*, 2015, pp. 137-143.

A. Baumgarten, A. Tyagi, and J. Zambreno, 'Preventing IC Piracy Using Reconfigurable Logic Barriers,' *IEEE Design Test of Computers*, Jan 2010, vol. 27 (1), pp. 66–75.

A. Sengupta and D. Roy, 'Protecting an intellectual property core during architectural synthesis using high-level transformation based obfuscation,' *IET Electronics Letters*, June 2017, vol. 53 (13), pp. 849 – 851.

D. Roy and A. Sengupta, 'Low Overhead Symmetrical Protection of Reusable IP Core Using Robust Fingerprinting and Watermarking During High Level Synthesis,' *Future Gener. Comput.* Syst., June 2017, vol. 71, pp. 89–101.

A. Sengupta and S. Bhadauria, 'Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis,' *IEEE Access*, 2016, vol. 4, pp. 2198–2215.

R. Torrance, D. James, 'The state-of-the-art in IC reverse engineering', in *Proceedings of Workshop on Cryptographic Hardware and Embedded Systems* (CHES) (Springer, Berlin, Heidelberg, 2009), pp. 363–381.

ExtremeTech, iphone 5 A6 SoC reverse engineered, reveals rare hand-made custom CPU, and tri-core GPU (2012).

J. L. Wong, D. Kirovski, and M. Potkonjak, 'Computational forensic techniques for intellectual property protection,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, June 2004, vol. 23 (6), pp. 987–994.

F. Koushanfar, '*Hardware Metering: A Survey'*, New York, NY: Springer New York, 2012, pp. 103–122.

A. Sengupta, S. Bhadauria, and S. P. Mohanty, 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, April 2017, vol. 36 (4), pp. 655–668.

Intel's 22-nm tri-gate transistors exposed (2012). [Online]. Available: http://www.chipworks.com/blog/technologyblog/ 2012/04/23/ intels-22-nm-tri-gate-transistors-exposed

NanGate 15 nm open cell library. [Online]. Available: http: //www.nangate.com/?pageid=2328, last accessed on June 2017.

DSP benchmark suite. [Online]. Available: http://www.ece.ucsb.edu/ EXPRESS/benchmark/, last accessed on June 2017.

Tensilica's ConnX D2 DSP Engine Wins EDN Top 100 Electronic Products Award for 2009. [Online]. Available: https://ip.cadence.com/news/310/330/Tensilica-s-ConnX-D2-DSP-Engine-Wins-EDN-Top-100-Electronic-Products-Award-for-2009.

A. Sengupta and D. Roy, 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach', in *IEEE Consumer Electronics Mag.*, April 2017, vol. 6 (2), pp. 118-124.

A. Sengupta, D. Roy and S. P. Mohanty, 'Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis,' in *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. PP, , pp. 1-1.

A. Sengupta and R. Sedaghat, 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, 2011, pp. 1-9.

A. Sengupta, and R. Sedaghat, 'System and methodology for development of a system architecture using optimization parameters', Google Patents, 2013, https://www.google.com/patents/US8397204.

A. Sengupta, S. Kundu, 'Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions' in *IEEE Trans. on VLSI Systems*, 2017, vol. 25 (12), pp. 3265-3267.

S. P. Mohanty, N. Ranganathan, E. Kougianos, and P. Patra, Low-Power High-Level Synthesis for Nanoscale CMOS Circuits, Springer, 2008, ISBN-10: 0387764739, ISBN-13: 978-0387764733.

A. Sengupta and S. P. Mohanty, "High-Level Synthesis of Digital Integrated Circuits in the Nanoscale Mobile Electronics Era", in Nano-CMOS and Post-CMOS Electronics: Circuits and Design, Edited by S. P. Mohanty and A. Srivastava, The Institute of Engineering and Technology (IET), 2016, ISBN-10: 184919999X, ISBN-13: 978-1849199995.

S. P. Mohanty, " Energy and Transient Power Minimization during Behavioral Synthesis", Doctoral Dissertation, Department of Computer Science and Engineering, University of South Florida, USA, 2003.

Chapter 08

Functional Obfuscation of DSP Cores used in CE Devices

The previous chapter detailed many approaches for structural obfuscation but we now move forward to another class of obfuscation called 'functional obfuscation'. Use of either of the techniques is the choice of design engineers. This chapter presents several methods to thwart IP piracy and RE attacks through functional obfuscation. More specifically, we will discuss IP functional locking blocks (ILBs) based logic obfuscation for DSP cores used in CE devices as hardware hardening technique (Sengupta et al., 2018). Moreover, a Particle Swarm Optimization (PSO) based Design Space Exploration (DSE) is performed to generate a low-overhead functionally obfuscated design solution for DSP cores (Sengupta and Sedaghat, 2011; Sengupta and Sedaghat, 2013). The rest of the chapter is organized as follows: Section 8.2 discusses different attack scenarios and threat model. Section 8.3 explains selected functional obfuscation techniques that are available in the literature. Section 8.4 discusses design process of functional obfuscation for DSP IP cores used in CE devices. Section 8.5 presents security analysis of functional obfuscation methodology for DSP IP core design. Section 8.6 discusses PSO-based optimization for functionally obfuscated design. Section 8.7 presents analysis on case studies/test cases.

8.1. Introduction

In the current Integrated Circuit (IC) supply chain model, multiple parties are involved to handle the increasing design complexity and cost. To avoid establishing and maintaining charge of a foundry with advanced fabrication facility, fabless semiconductor companies export their designed IC (such as DSP cores) to another company having fabrication facility. Additionally, sometimes system integrator while designing a System on chip (SoC), imports DSP Intellectual Property (IP) cores from third part IP (3PIP) vendors to meet the time-to-market requirement (Castillo et al., 2007). Thus, in this globalized business model for DSP cores, different countries and companies have different IP regulation policies and models. Therefore, in this scenario chip designing process is susceptible to many serious security threats, such as IP piracy, IP overbuilding, IP counterfeiting, reverse engineering, insertion of hardware Trojan, etc. (Sengupta and Kundu, 2017; Sengupta et al., 2018b; Wong et al., 2004; Alkabani et al., 2007). This necessitates improvement in the chip designing process to thwart these threats.

IP piracy is a process of illegal usage or selling of IP cores. An untrusted foundry, present in the design flow of an IP core can steal a design, illegally clone it and then resell it to other entity. Thus, it can bypass a substantial amount of research and development process, workforce, money and time invested by an original IP designer. Moreover, he/she can claim the ownership of

the PSO approach for generating low cost obfuscated netlist for DSP cores. In can also be noted that for very large size DSP IP cores such as JPEG IDCT and MESA (around 50K plus gates), the exploration time is not too large. Therefore, the optimization framework used in (Sengupta et al., 2018) does not suffer from scalability issue.

8.8. Conclusion

This chapter presents a low-cost, functional obfuscation mechanism for DSP IP core. This mechanism inserts reconfigured ILBs to lock a netlist of DSP IP core. Moreover, it integrates AES block to prevent SAT attack as a proactive countermeasure. Moreover, it was observed that (Sengupta et al., 2018) yielded power reduction, design cost reduction and SoO enhancement over other similar approaches. The research on functional obfuscation is still an open area and more research needs to be conducted for protection of other hardware circuits such as combinational/sequential circuit benchmarks against SAT attacks. There are new attacks such as approximate SAT and signal probability skew that are being launched to nullify the effect of Anti-SAT blocks used in conjunction with combinational/sequential circuit benchmarks. There is significant scope of work in the future, in this direction.

8.9. Exercises

1. What is functional obfuscation?
2. What is the difference between structural obfuscation and functional obfuscation in the context of DSP cores?
3. What are the Disadvantages of functional obfuscation?
4. What is Threat model of functional obfuscation?
5. How/ where is locking performed?
6. What are the properties of ILBs?
7. Why functional obfuscation is vulnerable to SAT attack for combinational/ sequential circuits?
8. Why functional obfuscation is not vulnerable to SAT attack for DSP core?
9. What is CNF?
10. How to find CNF for basic gates?
11. How to determine DIP?
12. How does AES protect against removal attacks of ILBs?
13. How is AES customized during insertion with obfuscation design?
14. How is AES removal attack prevented?
15. Design an obfuscated FFT (n=8).
16. What are the possible alternatives of AES for functional obfuscation?
17. What is key sensitization attack?
18. Design an ILB with AND, NAND, NOT, XOR, XNOR gates.
19. What is the difference between pairwise security and multi-pairwise security?
20. What is the role of random variable ‘μ’ in functional obfuscation?
21. What is run of key gates? How is it a drawback in the context of obfuscation?
22. Design a lightweight AES that uses less than 1 % FPGA resources.
23. How do you determine the design cost of an functionally obfuscated DSP design.

References

E. Castillo, U. Meyer-Baese, A. Garcia, L. Parrilla, A. Lloris (2007), 'IPP@HDL: Efficient Intellectual Property Protection Scheme for IP Cores,' *IEEE Trans. Very Large Scale Integration Sys.*, vol. 15 (5), pp. 578–591.

A. Sengupta (2016), 'Intellectual Property Cores: Protection designs for CE products,' *IEEE Consumer Electronics Mag.*, vol. 5 (1), pp. 83– 88.

The Economic Impacts of Counterfeiting and Piracy (2017), last modified: 02.03.2017. Available: http://www.inta.org/Communications/ Documents/Forms/AllItems.aspx.

J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls (2008), 'Brand and IP protection with physical unclonable functions,' in *Proc. IEEE Int. Sym. on Circuits and Systems,* pp. 3186–3189.

Y. Lao and K. K. Parhi (2015), 'Obfuscating DSP Circuits via High-Level Transformations,' *IEEE Trans. Very Large Scale Integration Sys.*, vol. 23 (5), pp. 819–830.

T. J. Biggerstaff (1989), 'Design recovery for maintenance and reuse,' *Computer*, vol. 22 (7), pp. 36–49.

A. Sengupta (2017), 'Hardware Security of CE Devices: Threat Models and Defence against IP Trojans and IP Piracy,' *IEEE Consumer Electronics Mag.*, vol. 6 (1), pp. 130–133.

S. P. Mohanty (2015), *Nanoelectronic Mixed-Signal System Design*. McGraw- Hill Education, no. 0071825711.

A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, and S. Kundu (2017), 'Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques,' *IEEE Trans. on Information Forensics and Security*, vol. 12 (1), pp. 64–77.

R. S. Chakraborty and S. Bhunia (2009), 'HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 28 (10), pp. 1493–1502.

A.R. Desai, M.S. Hsiao, C. Wang, L. Nazhandali, S. Hall (2013), 'Interlocking obfuscation for anti-tamper hardware,' in *Proceedings of Cyber Security and Information Intelligence Research Workshop (CSIIRW),* pp. 8:1–8:4.

S. Dupuis, P. S. Ba, G. Di Natale, M. L. Flottes and B. Rouzeyre (2014), 'A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans,' *IEEE Int.On-Line Testing Symposium (IOLTS)*, pp. 49-54.

Y. W. Lee and N. A. Touba (2015), 'Improving logic obfuscation via logic cone analysis,' *Latin-American Test Symposium (LATS)*, pp. 1-6.

R. Pappu, B. Recht, J. Taylor, N. Gershenfeld (2002), 'Physical one-way functions', *Science*, vol. 297 (5589), pp. 2026-2030.

M. C. Hansen, H. Yalcin and J. P. Hayes (1999), 'Unveiling the ISCAS-85 benchmarks: a case study in reverse engineering,' in *IEEE Design & Test of Computers*, vol. 16 (3), pp. 72-80.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran (2017a), 'DSP design protection in CE through algorithmic transformation based structural obfuscation,' in *IEEE Transactions on Consumer Electronics*, vol. 63 (4), pp. 467-476.

Y. M. Alkabani and F. Koushanfar (2007), 'Active Hardware Metering for Intellectual Property Protection and Security,' *in Proc. USENIX Security Symposium*, pp. 20:1–20:16.

J. Zhang (2016), 'A Practical Logic Obfuscation Technique for Hardware Security,' *IEEE Tran. Very Large Scale Integration Sys.*, vol. 24 (3), pp. 1193–1197.

X. Wang, X. Jia, Q. Zhou, Y. Cai, J. Yang, M. Gao, and G. Qu (2016), 'Secure and low-overhead circuit obfuscation technique with multiplexers,' *in GLSVLSI*, pp. 133–136.

J. A. Roy, F. Koushanfar, and I. L. Markov (2008), 'EPIC: Ending Piracy of Integrated Circuits,' *in DATE*, pp. 1069–1074.

J. Rajendran *et al*. (2015), 'Fault Analysis-Based Logic Encryption,' in *IEEE Transactions on Computers*, vol. 64 (2), pp. 410-424.

A. Sengupta, D. Kachave and D. Roy (2018), 'Low Cost Functional Obfuscation of Reusable IP Cores used in CE Hardware through Robust Locking,' in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. PP (99), pp. 1-1.

M. Yasin, J. J. Rajendran, O. Sinanoglu and R. Karri (2016), 'On Improving the Security of Logic Locking,' in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35 (9), pp. 1411-1424.

M. Yasin, B. Mazumdar, O. Sinanoglu and J. Rajendran (2017), 'Removal Attacks on Logic Locking and Camouflaging Techniques,' in *IEEE Transactions on Emerging Topics in Computing*, vol. PP (99), pp. 1-1.

P. Subramanyan, S. Ray and S. Malik (2015), 'Evaluating the security of logic encryption algorithms,' *IEEE Int. Symp. on Hardware Oriented Security and Trust (HOST)*, pp. 137-143.

Y. Xie and A. Srivastava, 'Anti-SAT: Mitigating SAT Attack on Logic Locking,' in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. PP (99), pp. 1-1.

A. Baumgarten, A. Tyagi, and J. Zambreno (2010), 'Preventing IC Piracy Using Reconfigurable Logic Barriers,' *IEEE Design Test of Computers*, vol. 27 (1), pp. 66–75.

D. Roy and A. Sengupta (2017), 'Low Overhead Symmetrical Protection of Reusable IP Core Using Robust Fingerprinting and Watermarking During High Level Synthesis,' *Future Gener. Comput*. Syst., vol. 71, pp. 89–101.

R. Torrance, D. James (2009), 'The state-of-the-art in IC reverse engineering', in *Proceedings of Workshop on Cryptographic Hardware and Embedded Systems* (CHES) (Springer, Berlin, Heidelberg), pp. 363–381.

J. L. Wong, D. Kirovski, and M. Potkonjak (2004), 'Computational forensic techniques for intellectual property protection,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 23 (6), pp. 987–994.

F. Koushanfar (2012), '*Hardware Metering: A Survey',* New York, NY: Springer New York, pp. 103–122.

A. Sengupta, S. Bhadauria, and S. P. Mohanty (2017b), 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 36 (4), pp. 655–668.

S. Kaveh et al. (2017), 'Appsat: Approximately deobfuscating integrated circuits' *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 95-100.

NanGate 15 nm open cell library, (2017). Available: http: //www.nangate.com/?pageid=2328, last accessed on June 2017.

DSP benchmark suite, (2017). Available: http://www.ece.ucsb.edu/ EXPRESS/benchmark/, last accessed on June 2017.

A. Sengupta and D. Roy (2017), 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach', in *IEEE Consumer Electronics Mag.*, vol. 6 (2), pp. 118-124.

A. Sengupta, D. Roy and S. P. Mohanty (2018b), 'Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis,' in *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. PP, , pp. 1-1.

M. Finke (2015), 'Equisatisfiable SAT Encodings of Arithmetical Operations', Available: http://www.martin-finke.de/documents/ Masterarbeit_bitblast_ Finke.pdf.

A. Sengupta and R. Sedaghat (2011), 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, pp. 1-9.

A. Sengupta, and R. Sedaghat (2013), 'System and methodology for development of a system architecture using optimization parameters', *US Patent by United Sates Patent and Trademark Office (USPTO)*, Patent no. US 8,397,204.

S. Chakraborty, A. Gupta, R. Jain "Matching Multiplications in Bit-Vector Formulas", Springer International Publishing, 2017, pp.131-150.

A. Sengupta, S. Kundu (2017), 'Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions' in *IEEE Trans. on VLSI Systems*, vol. 25 (12), pp. 3265-3267.

P. Hamalainen, T. Alho, M. Hannikainen, T.D. Hamalainen (2006), 'Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core', *IEEE 9th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools*, Washington, pp. 577-58.

S. Morioka, A. Satoh (2002), 'An Optimized S-Box Circuit Architecture for Low Power AES Design', *4th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 172-186.

Altera Quartus, Available: https://dl.altera.com/13.0sp1, , last accessed on 2018.

Cyclone II FPGA, Available: https://www.altera.com/products/fpga/cyclone-series/cyclone-ii/overview.html, last accessed on 2018.

Chapter 09

Obfuscation of JPEG CODEC IP Core for CE Devices

Joint Picture Export Group (JPEG) is the most commonly used image compression standard in the world. One can't comprehend a consumer electronic system that doesn't process a JPEG. Without JPEG there is no smart phone photography, no social media. So, authors feel strongly that this important multimedia core 'JPEG' needs to give well deserving credit in terms of securing it when security/protection of 'DSP core' has been a major focus of all the discussions in this book so far. The chapter is organized as follows: Section 9.2 provides an overview of DCT-based JPEG compression and decompression process. Section 9.3 explains design process of generating structurally obfuscated JPEG CODEC IP core; Section 9.4 provides a detailed insight on implementation process of obfuscated JPEG codec IP core in a CAD synthesis tool. Section 9.5 provides implementation and analysis of JPEG CODEC IP core as well as compressed images through the devised JPEG CODEC IP core.

9.1 Introduction

Currently most of the modern Consumer Electronics (CE) device comprises of a dedicated lens or camera to capture and/or display digital images, such as smartphone, tablets, scanner, laptop, smartwatch etc (Thavalengal and Corcoran, 2016; Kim et al., 2015; Corcoran and Andrae, 2014; Tang et al., 2016). Due to the enhancement of camera lenses, recording components and displaying components, current digital imaging systems are capable of capturing and displaying high-resolution images (Corcoran et al., 2001; Andorko et al., 2011). As high-resolution images contain too much detailed information, therefore, they are large in size. Storing or transmitting these large size images is a critical issue for storage space and transmission bandwidth respectively. Reducing the size of an image while storing and/or transferring it, is one of the popular and commercially successful techniques to address this crisis. Joint Photographic Experts Group (JPEG) standard formed in 1992 proposed Discrete Cosine Transformation (DCT) based image compression. Image compressions are of two types: (i) lossy and (ii) lossless. In lossy image compression, less important information of an image is discarded permanently (Mohanty 2003; Mohanty 1999). Camera (Corcoran et al., 2001; Andorko et al., 2011) in a smartphone, tablets, laptop, smartwatch etc. uses lossy image compression (Hnesh et al., 2016). In lossless image compression, no loss of information occurs. Camera in medical imaging (Bilgin et al., 1998), satellite imaging, forensic imaging etc. uses lossless image compression (Li et al., 2017; Scarmana et al., 2015).

DCT-based JPEG image compression is lossy by nature (Obukhov et al., 2008). DCT segregates an image into multiple sub-parts or blocks based on the visual quality of the image and then convert each block to the frequency domain from spatial domain. It discards small high-frequency components; therefore, DCT-based JPEG image compression method is lossy.

References

P. M. Corcoran and A. Andrae (2014), 'On Thin-Clients and The Cloud: Can Smartphones and Tablets Really Reduce Electricity Consumption?" in *Proc. IEEE International Conference on Consumer Electronics*, pp. 81–84.

Q. Tang, . M. Groba, E. Juarez, C. Sanz, and F. Pescador (2016), 'Real-Time Power-Consumption Control System for Multimedia Mobile Devices,' IEEE Trans. on CE, vol. 62 (4), pp. 362– 370.

A. Sengupta, S. Bhadauria, and S. P. Mohanty (2017a), 'TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling With Optimal Loop Unrolling Factor During High Level Synthesis,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 36 (4), pp. 655–668.

A. Sengupta and D. Roy (2017a), 'Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach', in *IEEE Consumer Electronics Mag.*, April 2017, vol. 6 (2), pp. 118-124.

G. Scarmana and K. McDougall (2015), 'Exploring the application of some common raster scanning paths on lossless compression of elevation images,' in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Milan, Italy, pp. 4514-4517.

P. M. Corcoran, P. Bigioi, and E. Steinberg (2001), 'Wireless transfer of images from a digital camera to the Internet via a standard GSM mobile phone,' *IEEE Trans. Consumer. Electronics*, vol. 47 (3), pp. 542-547.

A. Sengupta and D. Roy (2017b), 'Protecting an intellectual property core during architectural synthesis using high-level transformation based obfuscation,' *IET Electronics Letters*, vol. 53 (13), pp. 849 – 851.

A. Bilgin and M.W. Marcellin (1998), 'Applications of reversible integer wavelet transforms to lossless compression of medical image volumes,'' in Proc. IEEE Int. Symp. Inf. Theory, Cambridge, MA, USA, pp. 411

S. Li, H. Yin, X. Fang, and H. Lu (2017), 'Lossless image compression algorithm and hardware architecture for bandwidth reduction of external memory,' IET Image Process., vol. 11 (6), pp. 379-388.

A. Sengupta and R. Sedaghat (2011), 'Integrated scheduling, allocation and binding in High Level Synthesis using multi structure genetic algorithm based design space exploration,' *International Symposium on Quality Electronic Design*, pp. 1-9.

P. Coussy, D. D. Gajski, M. Meredith and A. Takach (2009), 'An Introduction to High-Level Synthesis,' in *IEEE Design & Test of Computers*, vol. 26, no. 4, pp. 8-17.

D. Roy and A. Sengupta (2018), 'Obfuscated JPEG Image Decompression IP Core for Protecting Against Reverse Engineering,' *IEEE Consumer Electronics Mag.,* Volume: 7, Issue: 3, May 2018, pp. 104 - 109.

I. Andorko, P. Corcoran, and P. Bigioi (2011), 'A dual image processing pipeline camera with CE applications,'' in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, pp. 737-738.

A. M. G. Hnesh and H. Demirel (2016), 'DWT-DCT-SVD based hybrid lossy image compression technique,'' in Proc. Int. Image Process., Appl. Syst. (IPAS), Hammamet, Tunisia, Nov. 2016, pp. 1-5.

N. Ahmed, T. Natarajan and K. R. Rao (1974), 'Discrete Cosine Transform,' in IEEE Transactions on Computers, vol. C-23 (1), pp. 90-93.

A. Sengupta (2017), 'Hardware Security of CE Devices,' *IEEE Consumer Electronics Mag.*, vol. 6 (1), pp. 130–133.

D. Roy and A. Sengupta (2017), 'Low Overhead Symmetrical Protection of Reusable IP Core Using Robust Fingerprinting and Watermarking During High Level Synthesis,' *Future Gener. Comput*. Syst., vol. 71, pp. 89–101.

J. L. Wong, D. Kirovski, and M. Potkonjak (2004), 'Computational forensic techniques for intellectual property protection,' *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. 23 (6), pp. 987–994.

Y. M. Alkabani and F. Koushanfar (2007), 'Active Hardware Metering for Intellectual Property Protection and Security,' *in Proc. USENIX Security Symposium*, pp. 20:1–20:16.

Y. Lao and K. K. Parhi (2015), 'Obfuscating DSP Circuits via High-Level Transformations,' *IEEE Trans. Very Large Scale Integration Sys.*, vol. 23 (5), pp. 819–830.

A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar, and S. Kundu (2017), 'Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques,' *IEEE Trans. on Information Forensics and Security*, vol. 12 (1), pp. 64–77.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran (2017b), 'DSP design protection in CE through algorithmic transformation based structural obfuscation,' in *IEEE Transactions on Consumer Electronics*, vol. 63 (4), pp. 467-476.

A. Sengupta, D. Roy and S. P. Mohanty (2018a), 'Triple-Phase Watermarking for Reusable IP Core Protection during Architecture Synthesis,' in *IEEE Trans. on CAD of Integrated Circuits and Systems*, vol. PP, pp. 1-1.

J. Kim, E. s. Jung, Y. t. Lee, and W. Ryu (2015), 'Home appliance control framework based on smart TV set-top box,' *IEEE Trans. on Consumer Electronics*, vol. 61 (3), pp. 279–285.

S. Thavalengal and P. Corcoran (2016), 'User Authentication on Smartphones: Focusing on iris biometrics,' *IEEE Consumer Electronics Mag.*, vol. 5 (2), pp. 87–93.

A. Sengupta, D. Roy, S. P. Mohanty and P. Corcoran (2018b), 'Low-Cost Obfuscated JPEG CODEC IP Core for Secure CE Hardware,' in *IEEE Transactions on Consumer Electronics*, (accepted).

A. Obukhov and A. Kharlamov (2008) 'Discrete Cosine Transform for 8x8 Blocks with CUDA' Nvidia whitepaper document.

‘DCT matrix’, Available: http://www.engr.colostate.edu/ECE513/SP09/lectures/lectures11_12.pdf, last accessed on 2018.

‘Dataset of standard 512x512 grayscale test images,’ Available: http://decsai.ugr.es/cvg/CG/base.htm, last accessed on 2018.

‘Nasa image and video library,’ Available: https://images.nasa.gov/n#/, last accessed on 2018.

‘NanGate 15 nm open cell library.’ Available: http: //www.nangate.com/?pageid=2328, last accessed on 2018.

Intel Quartus, Available: https://dl.altera.com/13.0sp1, , last accessed on 2018.

Cyclone II FPGA, Available: https://www.altera.com/products/fpga/cyclone-series/cyclone-ii/overview.html, last accessed on 2018.

S. P. Mohanty, " Watermarking of Digital Images”, Masters Thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999.

S. P. Mohanty, N. Ranganathan, and R. K. Namballa, "VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Development of a Secure JPEG Encoder", in *Proceedings of the IEEE Workshop on Signal Processing System (SIPS)*, pp. 183-188, 2003.

E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel, “Design of a High-Performance System for Secure Image Communication in the Internet of Things (Invited Paper)”, *IEEE Access Journal*, Volume 4, 2016, pp. 1222--1242.

Chapter 10

Advanced Encryption Standard (AES) and its Hardware Watermarking for Ownership Protection

In this era of consumer electronics cyberscecutity is one of key challenges. Any security, privacy, or protecton methods that is deployed relies on cryptography. Advance Encryption Standard (AES) is one of heavily used cryptogrpahy algorithmms for its advantages. This chapter is dedicated to the process of AES and its hardware design in the form of IP core. Several hardware security techniques rely on AES IP core as an important block. Additionally, since this is such an important core its self protection againts foregery/piracy is also crucial. This chapter also discusses AES IP core protection using watermarking.

10.1 Introduction

Cryptography is widely used in everyday life, ranging from established applications such as wireless local area network, procuring items with a credit or debit card, installing a software update, smart cards, banking application, voice of internet protocol (VOIP) to emergent domains such as electronic health system, Internet of Things (IoT) security, smart city security and hardware security [(Paar & Pelzl), (Tehranipoor & Bhunia 2018), (Sengupta 2017), (Sengupta 2015), (Sengupta, Bhadauria & Mohanty 2017), (Sengupta & Bhadauria 2016), (Sengupta & Sedaghat 2011), (Mishra, Bhunia and Tehranipoor 2017), (Sengupta & Sedaghat 2013), (Sengupta & Roy 2017), (Sengupta, Roy, Mohanty & Corcoran 2017)]. Cryptography comprises of cryptographic algorithms which are symmetrical by nature. There is tremendous usage of symmetric ciphers, especially for encryption of data and integrity check of messages. Further, cryptographic protocol deals with the application of cryptographic algorithms. An example of cryptographic protocol is Transport Layer Security (TLS) scheme, widely employed in browser Advanced Encryption Standard (AES) is a very popular symmetric cipher used today. The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data recognized by the U.S. National Institute of Standards and Technology (NIST) (). In the context of AES (Rijndael family), three members were designated by NIST, each with a block size of 128 bits, but dissimilar key lengths: 128, 192 and 256 bits. It is a mandatory standard in several industry/commercial systems and US government applications such as Wi-Fi encryption standard IEEE 802.11i, TLS, VOIP [(Paar & Pelzl, 2009)].

In this chapter, we focus on the following aspects (a) AES algorithm – description of each step and its flow diagram (b) corresponding hardware mapping of AES block cipher – overview of how each step can be mapped to a specific hardware sub-block (c) key scheduler – description of each step (d) corresponding hardware mapping of key scheduler used in AES (e)

References

Christof Paar, Jan Pelzl “Understanding Cryptography - A Textbook for Students and Practitioners”, Springer-Verlag, eBook ISBN 978-3-642-04101-3, Number of Pages: XVIII, 372, Nov 2009.

Swarup Bhunia and Mark M. Tehranipoor “Hardware Security: A Hands-on Learning Approach”, Morgan Kaufmann imprint , USA, 2017.

Anirban Sengupta, "Hardware Security of CE Devices: Threat Models and Defence against IP Trojans and IP Piracy", IEEE Consumer Electronics Magazine, Jan 2017, Volume: 6, Issue: 1, pp. 130 – 133

Anirban Sengupta "Protection of IP-Core Designs for CE Products", *IEEE Consumer Electronics Magazine*, Vol 5, pp. 83- 89, Dec 2015.

Anirban Sengupta, Saumya Bhadauria, Saraju P Mohanty "TL-HLS: Methodology for Low Cost Hardware Trojan Security Aware Scheduling with Optimal Loop Unrolling Factor during High Level Synthesis", IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems (TCAD), Volume: 36, Issue: 4, April 2017, pp. 655 – 668.

Prabhat Mishra, Swarup Bhunia, and Mark Tehranipoor “Hardware IP Security and Trust”, Springer , New York, USA, January 2017.

Anirban Sengupta, Saumya Bhadauria, "Exploring Low Cost Optimal Watermark for Reusable IP Cores during High Level Synthesis", *IEEE Access Journal*, Invited paper, Volume:4, Issue: 99, pp. 2198 - 2215, May 2016.

Anirban Sengupta, Reza Sedaghat, "Integrated Scheduling, Allocation and Binding in High Level Synthesis using Multi Structure Genetic Algorithm based Design Space Exploration System", *Proceedings of 12th IEEE/ACM International Symposium on Quality Electronic Design (ISQED)*, Silicon Valley, California, USA, 2011, pp. 486-494.

Anirban Sengupta (co-inventor: Reza Sedaghat),"System and methodology for development of a system architecture using optimization parameters", US Patent by United Sates Patent and Trademark Office (USPTO), Patent no. US 8,397,204, March 12, 2013.

N. M. Kosaraju, M. Varanasi, and S. P. Mohanty, "A High-Performance VLSI Architecture for Advanced Encryption Standard (AES) Algorithm", in Proceedings of the 19th International Conference on VLSI Design (VLSID), pp. 481-484, 2006.

S. P. Mohanty, R. Sheth, A. Pinto, and M. Chandy, "CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images", in Proceedings of the 11th IEEE International Symposium on Consumer Electronics (ISCE), 2007, pp. 1-6.

Chapter 11

Hardware Approaches for Media and Information Protection and Authentication

Technology scaling has allowed us to design high performance devices with a low power consumption. The advent of Internet of Things has increased the versatility of data collection and there are many different ways of collecting and transferring data over the internet. The data that is being collected is also in different forms, text, images, videos and audio. When they are shared, for a legit use, attackers can break the security and use them for illegible purposes or claim ownership to sell them commercially. This has been the trend lately where many counterfeit products are appearing in the market. This section discusses the digital watermarking, different schemes of digital watermarking and how a media object can be secured using a watermark. They are also not completely resistant to attacks and measures need to be taken to secure the content that is being watermarked. The chapter also presents different issues with the watermark implementations, attacks and countermeasures to those attacks on watermarking. Section 1 presents a broad overview of the intellectual property (IP) protection. Section 2 discusses the generic overview and components of any watermark system. Section 3 summarizes the various types of watermarks. Various applications of watermarking are discussed in Section 4. Desired characteristics of watermarks are presented in Section 5. Sections 6 discusses the technical challenges of the watermarking. Hardware based watermarking systems available in the current literature are discussed in Section 7. Section 8 discusses about watermarking in smart vehicles. Section 9 discusses about medical signal authentication. Section 10 highlights side channel information leakage and its countermeasures. Section 11 outlines various forms of attacks on watermarks and watermarking systems. Section 12 presents the difficulties involved in making use of them in practice.

1 Intellectual Property (IP) Protection - A Broad Overview

With the advent of new technology, new devices are being introduced into the world and high performance applications are being designed. With better systems coming out every-day, there is also a problem that they are used for various malicious applications like counterfeiting. This is a major problem in hardware and also media. Many people now-a-days are producing content and sharing it with the world [68, 47]. But the content that they own is being illegally used by many commercially without paying royalties to the owner and in some cases, misusing the content. This raises many problems pertaining to the Intellectual Property Rights and their protection. Fig. 1 gives a broad overview on the area of counterfeiting. An image can be produced by the owner and watermarked but an attacker can attack the watermark, tamper or remove it from the image and claim ownership. This creates many issues on the copyrights and ownership Rights.

1.1 Digital Rights Management (DRM)

Fig. 2 shows the different media and the threat levels that they are vulnerable to attacks. A cinema will have a high privacy where-as a broadcast content will have low security. This has become a major issue lately where the content of the owner is being reproduced without paying a royalties ot he owner.

In such cases, the owner will have copyrights violated and misses out on the royalties that are entitled legally. When a content media like a digital video disc (DVD) or BluRay is produced with a video content, it is considered to be secure with the watermarks embedded in it. But there are also many attacks that are available that can remove or tamper the watermark on the content. Fig. 3 shows the different types of multimedia that are available on the internet. Many of the audio services provide audio to the user at a monthly cost. But tampering with the audio that is broadcast over the internet is not difficult with the technological advancements that are

References

1. Acharya, U.R., Acharya, D., Bhat, P.S., Niranjan, U.C.: Compact Storage of Medical Images with Patient Information. IEEE Transactions on Information Technology in Biomedicine **5**(4), 320–323 (2001). DOI 10.1109/4233.966107
2. Ahmaderaghi, B., Kurugollu, F., Rincon, J.M.D., Bouridane, A.: Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory. IEEE Transactions on Computational Imaging **4**(1), 46–59 (2018). DOI 10.1109/TCI.2018.2794065
3. Ambrose, J.A., Ragel, R.G., Jayasinghe, D., Li, T., Parameswaran, S.: Side Channel Attacks in Embedded Systems: A Tale of Hostilities and Deterrence. In: Proceedings of the Sixteenth International Symposium on Quality Electronic Design, pp. 452–459 (2015)
4. American Society of Composers, Authors and Publishers (ASCAP): URL `https://www.ascap.com/`. Last Accessed: 06-20-2018
5. Annadurai, K., Pavithra, K., Subharani, S.: Double Watermarking of Dicom Medical Images using Wavelet Decomposition Technique **1** (2012)
6. Bender, W., Gruhl, D., Morimoto, N.: Techniques for Data Hiding. IBM Systems Journal **35**(3), 313–336 (1996)
7. Bi, W., Zhang, W., He, W., Li, C.: A Modified Decoding Algorithm Involving Priori Characteristics Bits for LDPC. In: 6th IEEE/International Conference on Advanced Infocomm Technology (ICAIT), pp. 245–246 (2013). DOI 10.1109/ICAIT.2013.6621574
8. Braudaway, G.W., Magerlein, K.A., Mintzer, F.: Protecting Publicly Available Images with a Visible Image Watermark. In: Proceedings of the SPIE Conference on Optical Security and Counterfiet Deterrence Technique (Vol. SPIE-2659), pp. 126–132 (1996)
9. Busch, C., Funk, W., Wolthusen, S.: Digital Watermarking: from Concepts to Real-Time Video Applications. IEEE Computer Graphics and Applications **19**(1), 25–35 (1999)
10. Cai, W.: FPGA Prototyping of A Watermarking Algorithm . Master's thesis, Department of Electrical Engineering Technology, University of North Texas, Denton, TX (2006)
11. Chan, H.T., Hwang, W.J., Cheng, C.J.: Digital Hologram Authentication Using a Hadamard-Based Reversible Fragile Watermarking Algorithm. Journal of Display Technology **11**(2), 193–203 (2015). DOI 10.1109/JDT.2014.2367528
12. Chen, S.T., Hsu, C.Y., Huang, H.N.: Wavelet-Domain Audio Watermarking Using Optimal Modification on Low-Frequency Amplitude. IET Signal Processing **9**(2), 166–176 (2015). DOI 10.1049/iet-spr.2013.0399
13. Cheng, C.J., Hwang, W.J., Zeng, H.Y., Lin, Y.C.: A Fragile Watermarking Algorithm for Hologram Authentication. Journal of Display Technology **10**(4), 263–271 (2014). DOI 10.1109/JDT.2013.2295619
14. Coatrieux, G., Lecornu, L., Sankur, B., Roux, C.: A Review of Image Watermarking Applications in Healthcare. In: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 4691–4694 (2006). DOI 10.1109/IEMBS.2006.259305
15. Copy Protection Technical Working Group (CPTWG): URL `http://www.cptwg.org/`. Last Accessed: 06-20-2018
16. Cox, I.J., Linnartz, J.P.M.G.: Some General Methods for Tampering with Watermarks. IEEE Journal on Selected Areas in Communications **16**(4), 587–593 (1998)
17. Cox, I.J., Miller, M.: A Review of Watermarking and Importance of Perceptual Modelling. In: Proceedings of SPIE Human Vision and Imaging, vol. 3016, pp. 92–99 (1997)
18. Cox, I.J., Miller, M.L.: Electronic Watermarking : The First 50 Years. EURASIP Journal of Applied Signal Processing **2002**(2), 126–132 (2002)
19. Craver, S., Memon, N., Yeo, B.L., Yeung, M.: Can Invisible Watermarks Resolve Rightful Ownerships? Tech. rep., IBM Research Report, RC 20509 (1996)
20. Craver, S., Memon, N., Yeo, B.L., Yeung, M.M.: Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications. IEEE Journal on Selected Areas in Communications **16**(4), 573–586 (1998)
21. Delaigle, J.F., Devleeschouwer, C., Macq, B., Langendijk, I.: Human Visual Systems Features Enabling Watermarking. In: Proceedings of the IEEE International Conference Multimedia and Expo, pp. 489–492 (2002)
22. Depovere, G., Kalker, T., Haitsma, J., Maes, M., Strycker, L.D., Termont, P., Vandewege, J., Langell, A., Alm, C., Norman, P., O'Reilly, G., Howes, B., Vaanholt, H., Hintzen, R., Donnelly, P., Hudson, A.: The VIVA Project : Digital Watermarking for Broadcast Monitoring. In: Proceedings of the IEEE International Conference on Image Precessing (Vol. 2), pp. 202–205 (1999)
23. Devillier, N.: Aging, Well-Being, and Technology: From Quality of Life Improvement to Digital Rights Management - A French and European Perspective. IEEE Communications Standards Magazine **1**(3), 46–49 (2017)
24. Fallahpour, M., Shirmohammadi, S., Semsarzadeh, M., Zhao, J.: Tampering Detection in Compressed Digital Video Using Watermarking. IEEE Transactions on Instrumentation and Measurement **63**(5), 1057–1072 (2014). DOI 10.1109/TIM.2014.2299371
25. Fan, Y.C., Van, L.D., Huang, C.M., Tsao, H.W.: Hardware-Efficient Architecture Design of Wavelet-based Adaptive Visible Watermarking. In: Proceedings of 9th IEEE International Symposium on Consumer Electronics, pp. 399–403 (2005)
26. Fatima, N., Tuptewar, D.J.: Comparison of Hybrid Watermarking Technique on Different Color Spaces. In: Conference on Advances in Signal Processing (CASP), pp. 13–17 (2016). DOI 10.1109/CASP.2016.7746129
27. Frattolillo, F.: Watermarking Protocols: Problems, Challenges and a Possible Solution. The Computer Journal **58**(4), 944–960 (2015). DOI 10.1093/comjnl/bxu015
28. Fridrich, J., Goljan, M., Baldoza, A.C.: New Fragile Authentication Watermark for Images. In: Proceedings 2000 International Conference on Image Processing, vol. 1, pp. 446–449 vol.1 (2000). DOI 10.1109/ICIP.2000.900991

29. Gafsi, M., Ajili, S., Hajjaji, M.A., Mtibaa, A.: XSG for Hardware Implementation of a Robust Watermarking System. In: 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), pp. 117–122 (2016). DOI 10.1109/STA.2016.7952031
30. Garimella, A., Satyanarayan, M.V.V., Kumar, R.S., Murugesh, P.S., Niranjan, U.C.: VLSI Impementation of Online Digital Watermarking Techniques with Difference Encoding for the 8-bit Gray Scale Images. In: Proceedings of the International Conference on VLSI Design, pp. 283–288 (2003)
31. Garimella, A., Satyanarayana, M.V.V., Murugesh, P.S., Niranjan, U.C.: ASIC for Digital Color Image Watermarking. In: Proceedings of 11th IEEE Digital Signal Processing Workshop, pp. 292–295 (2004)
32. Hsiao, S.F., Tai, Y.C., Chang, K.H.: VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking. In: Proceedings of the IEEE International Conference on Consumer Electronics, pp. 186–187 (2000)
33. Hsiao, S.F., Tai, Y.C., Chang, K.H.: VLSI Design of an Efficient Embedded Zerotree Wavelet Coder with Function of Digital Watermarking. IEEE Transactions on Consumer Electronics **46**(3), 628–636 (2000)
34. Hua, X.S., Feng, J.F., Shi, Q.Y.: Public Multiple Watermarking Resistant to Cropping. In: Proceedings of the 6th international conference on pattern recognition and information processing, pp. 263–268 (2001)
35. I.J.Cox, Kilian, J., Shamoon, T., Leighton, T.: Secure Spread Spectrum Watermarking of Images, Audio and Video. In: Proc IEEE International Conf on Image Processing, vol. 3, pp. 243–246 (1996)
36. Jayasinghe, D., Ignjatovic, A., Ambrose, J.A., Ragel, R., Parameswaran, S.: QuadSeal: Quadruple Algorithmic Symmetrizing Countermeasure Against Power based Side-Channel Attacks. In: Proceedings of the International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), pp. 21–30 (2015)
37. J.F.Delaigle, Vleeschouwer, C.D., Macq, B.: Watermarking Algorithm based on Human Visual Model. Signal Processing **66**(3), 319–335 (1998)
38. J.Zhao, Koch, E., O'Ruanaidh, J., Yeung, M.: Digital watermarking : What will it do for me? and what it won't! In: Proceedings of SIGGRAPH Conference, pp. 153–155 (1999)
39. Kahn, D.: The History of Steganography. In: Proceedings of First International Workshop on Information Hiding, vol. 1174, pp. 1–7 (1996)
40. Kamaruddin, N.S., Kamsin, A., Por, L.Y., Rahman, H.: A Review of Text Watermarking: Theory, Methods, and Applications. IEEE Access **6**, 8011–8028 (2018). DOI 10.1109/ACCESS.2018.2796585
41. Kankanhalli, M.S., Rajmohan, Ramakrishnan, K.R.: Content based watermarking for images. In: Proceedings of the 6th ACM International Multimedia Conference, pp. 61–70 (1998)
42. Kaur, R., Kalra, G.S., Kansal, M.: A User Friendly GUI Based Benchmark for Image Watermarking. In: International Conference on Computing Sciences, pp. 70–76 (2012). DOI 10.1109/ICCS.2012.8
43. Khan, M.I., Jeoti, V., Malik, A.S.: Designing a Joint Perceptual Encryption and Blind Watermarking Scheme Compliant with JPEG Compression Standard. In: International Conference on Computer Applications and Industrial Electronics, pp. 688–691 (2010). DOI 10.1109/ICCAIE.2010.5735022
44. Kirovski, D., Malvar, H.: Spread-Spectrum Audio Watermarking: Requirements, Applications, and Limitations. In: IEEE Fourth Workshop on Multimedia Signal Processing, pp. 219–224 (2001). DOI 10.1109/MMSP.2001.962737
45. Koubaa, M., Amar, C.B., Nicolas, H.: Adaptive Video Watermarking using Mosaic Images. In: IEEE International Conference on Signal Processing and Communications, pp. 1143–1146 (2007). DOI 10.1109/ICSPC.2007.4728526
46. Kougianos, E., P.Mohantya, S., N.Mahapatra, R.: Hardware Assisted Watermarking for Multimedia. Computers & Electrical Engineering **35**(2), 339–358 (2009)
47. Krishnamurthy, R.K., Humble, T., Cheung, S.C., Lyke, J., Mohanty, S.P., Casto, M.: Energy and Cybersecurity Constraints on Consumer Electronics. `http://www.icce.org/expert-panels/` (January 13, 2018). Last visited on 20th Nov 2017
48. Lah, U., Lewis, J.R.: How Expertise Affects a Digital-Rights-Management-Sharing Application's Usability. IEEE Software **33**(3), 76–82 (2016). DOI 10.1109/MS.2015.104
49. Li, R., Xu, S., Yang, H.: Spread Spectrum Audio Watermarking Based on Perceptual Characteristic Aware Extraction. IET Signal Processing **10**(3), 266–273 (2016). DOI 10.1049/iet-spr.2014.0388
50. Liu, S., Pan, Z., Song, H.: Digital Image Watermarking Method Based on DCT and Fractal Encoding. IET Image Processing **11**(10), 815–821 (2017). DOI 10.1049/iet-ipr.2016.0862
51. Loan, N.A., Hurrah, N.N., Parah, S.A., Lee, J.W., Sheikh, J.A., Bhat, G.M.: Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption. IEEE Access **6**, 19,876–19,897 (2018). DOI 10.1109/ACCESS.2018.2808172
52. Ma, Z.: Digital Rights Management: Model, Technology and Application. China Communications **14**(6), 156–167 (2017). DOI 10.1109/CC.2017.7961371
53. Ma, Z., Huang, J., Jiang, M., Niu, X.: A Novel Image Digital Rights Management Scheme with High-Level Security, Usage Control and Traceability. Chinese Journal of Electronics **25**(3), 481–494 (2016). DOI 10.1049/cje.2016.05.014
54. Maes, M., Kalker, T., Linnartz, J.P.M.G., Talstra, J., Depovere, G.F.G., Haitsma, J.: Digital Watamarking for DVD Video Copyright Protection. IEEE Signal Processing Magazine **17**(5), 47–57 (2000)
55. Makbol, N.M., Khoo, B.E., Rassem, T.H.: Block-Based Discrete Wavelet Transform-Singular Value Decomposition Image Watermarking Scheme using Human Visual System Characteristics. IET Image Processing **10**(1), 34–52 (2016). DOI 10.1049/iet-ipr.2014.0965
56. Marcinak, M.P., Mobasseri, B.G.: Digital Video Watermarking for Metadata Embedding in UAV Video. In: MILCOM 2005 - 2005 IEEE Military Communications Conference, pp. 1637 Vol. 3–5 (2005). DOI 10.1109/MILCOM.2005.1605909
57. Mathai, N.J., Kundur, D., Sheikholeslami, A.: Hardware Implementation Perspectives of Digital Video Watermarking Algortithms. IEEE Transanctions on Signal Processing **51**(4), 925–938 (2003)

58. Mathai, N.J., Sheikholeslami, A., Kundur, D.: VLSI Implementation of a Real-Time Video Watermark Embedder and Detector. In: Proceedings of the IEEE International Symposisum on Circuits and Systems (Vol. 2), pp. 772–775 (2003)
59. Mathivanan, P., Ganesh, A.B.: Colour Image Steganography Using XOR Multi-Bit Embedding Process. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp. 1980–1988 (2017). DOI 10.1109/ICECDS.2017.8389797
60. Memon, N., Wong, P.W.: Protecting Digital Media Content. Communications of the ACM **41**(7), 35–43 (1998)
61. Mintzer, F., Braudaway, G., Yeung, M.: Effective and Ineffective Digital Watermarks. In: IEEE International Conference on Image Processing (ICIP-97), vol. 3, pp. 9–12 (1997)
62. Mintzer, F., Braudaway, G.W., Bell, A.E.: Opportunities for Watermarking Standards. Communications of the ACM **41**(7), 57–64 (1998)
63. Mintzer, F.C., Boyle, L.E., Cazes, A.N., Christian, B.S., Cox, S.C., Giordano, F.P., Gladney, H.M., Lee, J.C., Kelmanson, M.L., Lirani, A.C., Magerlein, K.A., Pavani, A.M.B., Schiattarella, F.: Towards online Worldwide Access to Vatican Library Materials. IBM Journal of Research and Development **40**(2), 139–162 (1996)
64. M.M.Yeung: Digital Watermarking. Communications of the ACM **41**(7), 31–33 (1998)
65. Mohanty, S.P.: Everything you Wanted to Know about Internet of Things (IoT). `https://cesoc.ieee.org/images/files/pdf/Mohanty\_IEEE-DL\_IoT.PDF` (16th November, 2017). Last visited on 20th Nov 2017
66. Mohanty, S.P.: Digital Watamerking of Images. Master's thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India (1999)
67. Mohanty, S.P.: A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management. Journal of Systems Architecture - Embedded Systems Design **55**(10-12), 468–480 (2009)
68. Mohanty, S.P.: Nanoelectronic Mixed-Signal System Design. 9780071825719. McGraw-Hill Education (2015)
69. Mohanty, S.P., C., R.K., Nayak, S.: FPGA Based Implementation of an Invisible-Robust Image Watermarking Encoder. In: Lecture Notes in Computer Science, vol. 3356, pp. 344–353 (2004)
70. Mohanty, S.P., Kougianos, E.: Real-Time Perceptual Watermarking Architectures for Video Broadcasting. Journal of Systems and Software **84**(5), 724–738 (2011)
71. Mohanty, S.P., Kougianos, E., Cai, W., Ratnani, M.: VLSI architectures of perceptual based video watermarking for real-time copyright protection. In: Proceedings of the 10th International Symposium on Quality of Electronic Design (ISQED), pp. 527–534 (2009)
72. Mohanty, S.P., Kougianos, E., Guturu, P.: SBPG: Secure Better Portable Graphics for Trustworthy Media Communications in the IoT. IEEE Access **6**, 5939–5953 (2018)
73. Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.S.: A Dual Watermarking Technique for Images. In: Proceedings of the 7th ACM International Multimedia Conference (Vol. 2), pp. 49–51 (1999)
74. Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.S.: A DCT Domain Visible Watermarking Technique for Images. In: Proceedings of the IEEE International Conference on Multimedia and Expo, pp. 1029–1032 (2000)
75. Mohanty, S.P., Ramakrishnan, K.R., Kankanhalli, M.S.: An Adaptive DCT Domain Visible Watermarking Technique for Protection of Publicly Available Images. In: Proceedings of the International Conference on Multimedia Processing and Systems, pp. 195–198 (2000)
76. Mohanty, S.P., Ranganathan, N.: A Framework for Energy and Transient Power Reduction during Behavioral Synthesis. IEEE Transactions on Very Large Scale Integration Systems **12**(6), 562–572 (2004)
77. Mohanty, S.P., Ranganathan, N.: Energy Efficient Datapath Scheduling using Multiple Voltages and Dynamic Clocking. ACM Transactions on Design Automation of Electronic Systems **10**(2), 330–353 (2005)
78. Mohanty, S.P., Ranganathan, N., Balakrishnan, K.: Design of a Low Power Image Watermarking Encoder using Dual Voltage and Frequency. In: Proceedings of 18th IEEE International Conference on VLSI Design, pp. 153–158 (2005)
79. Mohanty, S.P., Ranganathan, N., Namballa, R.K.: VLSI Implementation of Invisible Digital Watermarking Algorithms Towards the Developement of a Secure JPEG Encoder. In: Proceedings of the IEEE Workshop on Signal Processing Systems, pp. 183–188 (2003)
80. Mohanty, S.P., Ranganathan, N., Namballa, R.K.: A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^2DC) Design. IEEE Transactions on Very Large Scale Integration Systems **13**(8), 1002–1012 (2005)
81. Mohanty, S.P., Rangnathan, N., Namballa, R.K.: VLSI Implementation of Visible Watermarking for a Secure Digital Still Camera Design. In: Proceedings of the 17th International Conference on VLSI Design, pp. 1063–1068 (2004)
82. Mohanty, S.P., Sengupta, A., Guturu, P., Kougianos, E.: Everything You Want to Know About Watermarking. IEEE Consumer Electronics Magazine **6**(3), 83–91 (2017)
83. Parameswaran, S.: QUADSEAL : A Hardware Countermeasure against Side channel Attacks on AES. IEEE International Symposium on Nanoelectronic and Information Systems, Bhopal, India (19th December, 2017). Last visited on 29th June 2018
84. Peng, H., Wang, J., Wang, W.: Image Watermarking Method in Multiwavelet Domain Based on Support Vector Machines. Journal of Systems and Software **83**(8), 1470 – 1477 (2010). DOI https://doi.org/10.1016/j.jss.2010.03.006. URL `http://www.sciencedirect.com/science/article/pii/S0164121210000701`
85. Pereira, S., Voloshynovskiy, S., Madueo, M., Marchand-Maillet, S., Pun, T.: Second Generation Benchmarking and Application Oriented Evaluation. In: Proceedings of 3rd International Workshop on Information Hiding (2001)
86. Petitjean, G., Dugelay, J.L., Gabriele, S., Rey, C., Nicolai, J.: Towards Real-time Video Watermarking for Systems-On-Chip. In: Proceedings of the IEEE International Conference on Multimedia and Expo (Vol. 1), pp. 597–600 (2002)
87. Pexaras, K., Tsiourakis, C., Karybali, I.G., Kalligeros, E.: Optimization and Hardware Implementation of Image Watermarking for Low Cost Applications. In: 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 347–350 (2017). DOI 10.1109/ICECS.2017.8292014

88. Pfitzmann, B.: Information Hiding Terminology. In: Proceedings of First International Workshop on Information Hiding, vol. 1174, pp. 347–350 (1996)
89. Ramkumar, M.: Data Hiding in Multimedia - Theory and Applications. Ph.D. thesis, Department of Electrical and Computer Engineering, New Jersy i Institute of Technology, Newwark, NJ, USA (2000)
90. Ramkumar, M., Akansu, A.N.: Capacity Estimates for Data Hiding in Compressed Images. IEEE Transactions on Image Processing **10**(8), 1252–1263 (2001)
91. R.Barnett: Digital Watermarking : Application, Techniques, and Challengs. IEE Electronics and Communication Engineering Journal pp. 173–183 (1999)
92. Ross, P.E.: Commandments. IEEE Spectrum **40**(12), 30–35 (2003)
93. Roy, S.D., Li, X., Shoshan, Y., Fish, A., Yadid-Pecht, O.: Hardware Implementation of a Digital Watermarking System for Video Authentication. IEEE Transactions on Circuits and Systems for Video Technology **23**(2), 289–301 (2013). DOI 10.1109/TCSVT.2012.2203738
94. Roy, S.D., Yadid-Pecht, O.: Design and Implementation of Hardware Based Watermarking Solutions for CMOS Image Sensors. In: IEEE International NEWCAS Conference, pp. 341–344 (2012). DOI 10.1109/NEWCAS.2012.6329026
95. Sang, J., Alam, M.S.: Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking. IEEE Transactions on Instrumentation and Measurement **57**(3), 595–606 (2008). DOI 10.1109/TIM.2007.911585
96. Sarreshtedari, S., Akhaee, M.A., Abbasfar, A.: A Watermarking Method for Digital Speech Self-Recovery. IEEE/ACM Transactions on Audio, Speech, and Language Processing **23**(11), 1917–1925 (2015). DOI 10.1109/TASLP.2015.2456431
97. Sengupta, A., Roy, D.: Antipiracy-Aware IP Chipset Design for CE Devices: A Robust Watermarking Approach [Hardware Matters]. IEEE Consumer Electronics Magazine **6**(2), 118–124 (2017). DOI 10.1109/MCE.2016.2640622
98. Seo, Y.H., Kim, D.W.: Real-Time Blind Watermarking Algorithm and its Hardware Implementation for Motion JPEG2000 Image Codec. In: Proceedings of the 1st Workshop on Embedded Systems for Real-Time Multimedia, pp. 88–93 (2003)
99. Sequeira, A., Kundur, D.: Communications and information theory in watermarking : A survey. In: Proceedings of SPIE Multimedia Systems and Application IV, vol. 4518, pp. 216–227 (2001)
100. Servette, S.D., Podilchuk, C., Ramchandran, K.: Capacity Issues in Digital Watermarking. In: IEEE International Conference on Image Processing, ICIP-98, vol. 1, pp. 445–449 (1998)
101. Singh, A., Kumar, B., Dave, M., Mohan, A.: Multiple Watermarking On Medical Images Using Selective DWT Coefficients **5**, 1–8 (2015)
102. Singh, A.K., Kumar, B., Singh, G., Mohan, A. (eds.): Medical Image Watermarking. Springer International Publishing (2017)
103. Strycker, L.D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M., Depovere, G.: An Implementation of a Real-time Digital Watermarking Process for Broadcast Monitoring on a Trimedia VLIW Processor. In: Proceedings of the IEE International Conference on Image Precessing and Its Applications (Vol. 2), pp. 775–779 (1999)
104. Strycker, L.D., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M., Depovere, G.: Implementation of a Real-Time Digital Watermarking Process for Broadcast Monitoring on Trimedia VLIW Processor. IEE Proceedings on Vision, Image and Signal Processing **147**(4), 371–376 (2000)
105. Su, P.C., Wu, C.S., Chen, I.F., Wu, C.Y., Wu, Y.C.: A Practical Design of Digital Video Watermarking in H.264/AVC for Content Authentication. Image Communication **26**(8-9), 413–426 (2011). DOI 10.1016/j.image.2011.07.004. URL `http://dx.doi.org/10.1016/j.image.2011.07.004`
106. Sugihara, R.: Practical Capacity of Digital Watermark as Constrained by Reliability. In: Proceedings of the International Conference on Information Technology: Coding and Computing, pp. 85–59 (2001)
107. Swanson, M., Kobayashi, M., Tewfik, A.: Multimedia Data Embedding and Watermarking Technologies. Proceedings of the IEEE **86**(6), 1064–1087 (1998)
108. Tefas, A., Pitas, I.: Robust Spatial Image Watermarking Using Progressive Detection. In: Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (Vol. 3), pp. 1973–1976 (2001)
109. Termont, P., Strycker, L.D., Vandewege, J., Haitsma, J., Kalker, T., Maes, M., Depovere, G., Langell, A., Alm, C., Norman, P.: Performance Measurements of a Real-time Digital Watermarking System for Broadcast Monitoring. In: Proceedings of the IEEE International Conference on Multimedia Computing and Systems (Vol. 2), pp. 220–224 (1999)
110. The Broadcast Music Inc.: URL `https://www.bmi.com/`. Last Accessed: 06-20-2018
111. The Motion Picture Licensing Corporation: URL `https://www.mplc.org/`. Last Accessed: 06-20-2018
112. Tsai, T.H., Lu, C.Y.: A Systems Level Design for Embedded Watermark Technique using DSC Systems. In: Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems (2001)
113. Tsai, T.H., Wu, C.Y.: An Implementation of Configurable Digital Watermarking Systems in MPEG Video Encoder. In: Proceedings of the IEEE International Conference on Consumer Electronics, pp. 216–217 (2003)
114. Vellaisamy, S., Ramesh, V.: Inversion Attack Resilient Zero-Watermarking Scheme for Medical Image Authentication. IET Image Processing **8**(12), 718–727 (2014). DOI 10.1049/iet-ipr.2013.0558
115. Vijayan, R., Sreedivya, R.S.: Cryptographic-Steganography Network Communication. In: IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 694–697 (2017). DOI 10.1109/ICPCSI.2017.8391802
116. Vo, P.H., Nguyen, T.S., Huynh, V.T., Do, T.N.: A Robust Hybrid Watermarking Scheme Based on DCT and SVD for Copyright Protection of Stereo Images. In: 4th NAFOSTED Conference on Information and Computer Science, pp. 331–335 (2017). DOI 10.1109/NAFOSTED.2017.8108087
117. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., Su, J.: Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks. IEEE Communications Magazine **39**(9), 118–126 (2001)
118. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J.J., Su, J.K.: Attacks on Digital Watermarks: Classification, Estimation Based Attacks, and Benchmarks. IEEE Communications Magazine **39**(8), 118–126 (2001). DOI 10.1109/35.940053

119. Voyatzis, G., Pitas, I.: The Use of Watermarks in the Protection of Digital Multimedia Products. Proceedings of the IEEE **87**(7), 1197–1207 (1999)
120. Wang, H., Peng, D., Wang, W., Sharif, H., Chen, H.H.: Energy-Aware Adaptive Watermarking for Real-Time Image Delivery in Wireless Sensor Networks. In: IEEE International Conference on Communications, pp. 1479–1483 (2008). DOI 10.1109/ICC.2008.286
121. p. Wang, J., f. Sun, S., Jiang, M., g. Xie, D., j. Lei, B.: Anti-protocol Attacks Digital Watermarking Based on Media-Hash and SVD. In: Fifth International Conference on Information Assurance and Security, vol. 1, pp. 364–367 (2009). DOI 10.1109/IAS.2009.206
122. Wang, S., Cui, C., Niu, X.: A Novel DIBR 3D Image Watermarking Algorithm Resist to Geometrical Attacks. Chinese Journal of Electronics **26**(6), 1184–1193 (2017). DOI 10.1049/cje.2017.09.025
123. Wang, Y., Liu, J., Yang, Y., Ma, D., Liu, R.: 3D Model Watermarking Algorithm Robust to Geometric Attacks. IET Image Processing **11**(10), 822–832 (2017). DOI 10.1049/iet-ipr.2016.0927
124. Wang, Y.G., Xie, D., Gupta, B.B.: A Study on the Collusion Security of LUT-Based Client-Side Watermark Embedding. IEEE Access **6**, 15,816–15,822 (2018). DOI 10.1109/ACCESS.2018.2802928
125. Winkler, T., Rinner, B.: TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera Based on Trusted Computing. In: 7th IEEE International Conference on Advanced Video and Signal Based Surveillance, pp. 593–600 (2010). DOI 10.1109/AVSS.2010.38
126. Xiang, Y., Natgunanathan, I., Guo, S., Zhou, W., Nahavandi, S.: Patchwork-Based Audio Watermarking Method Robust to De-synchronization Attacks. IEEE/ACM Transactions on Audio, Speech, and Language Processing **22**(9), 1413–1423 (2014). DOI 10.1109/TASLP.2014.2328175
127. Zhang, F., Shi, Z.J.: Differential and Correlation Power Analysis Attacks on HMAC-Whirlpool. In: Eighth International Conference on Information Technology: New Generations, pp. 359–365 (2011). DOI 10.1109/ITNG.2011.70
128. Zhang, J., Liu, L.: Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **25**(4), 1520–1527 (2017). DOI 10.1109/TVLSI.2016.2619682
129. Zhang, Y., Xu, Z., Huang, B.: Channel Capacity Analysis of the Generalized Spread Spectrum Watermarking in Audio Signals. IEEE Signal Processing Letters **22**(5), 519–523 (2015). DOI 10.1109/LSP.2014.2363655
130. Zhao, J., Zhang, N., Jia, J., Wang, H.: Digital Watermarking Algorithm Based on Scale-Invariant Feature Regions in Non-Subsampled Contourlet Transform Domain. Journal of Systems Engineering and Electronics **26**(6), 1309–1314 (2015). DOI 10.1109/JSEE.2015.00143

Chapter 12

Physical Unclonable Functions (PUFs)

It has been the practice to store information under lock and key for safeguarding it. Even today, we use cryptographic primitives to store information securely under lock and key, encryption and decryption. For the process of cryptography, keys are necessary for any operation. But these keys should be stored in the memory so that they can be used whenever necessary. When a key is stored in the memory, it can be stolen by the adversary using various methods. So storing it in a non-volatile memory is not an option in this age of security threats. Physical Unclonable Functions are the promising security primitives that are used for generating the keys instead of storing them in the memory. These modules use the naturally occurring manufacturing variations in the fabrication process for generating the keys for cryptographic purposes. This chapter discusses different types of PUFs. Section 1 gives a brief introduction of Physical Unclonable Functions (PUF). Section 2 discusses working principles of Physical Unclonable Functions (PUF). Section 3 discusses different characteristics of a PUF design, Section 4 presents different classifications of PUFs. Various designs of PUF based on ring oscillators is presented in Section 5, based on multiplexers and reconfigurability are presented in Section 6. Static Random Access Memory (SRAM) based PUFs are presented in Section 7, Memristor-based PUFs are presented in Section 8 and Diode based PUFs are presented in Section 9. There are also Non-Silicon based PUF designs like Carbon PUFs are presented in Section 10. Microprocessors can also be used for implementing the PUF designs which are presented in Section 11. Magnetic material based PUFs are presented in Section 12 and the Field Programmable Gate Array (FPGA) implementations of PUF and security measures for FPGA are presented in Section 13. Some case study applications are presented in Section 14. Further the issues and challenges that are faced during the design of PUF modules are presented in Section 15. The conclusions and future directions are presented in Section 16.

1 Introduction

The first transistor was invented in 1948. With the introduction of the transistor, vacuum tubes occupying huge space disappeared and led to the invention of the Integrated Circuit (IC) in 1958 [30]. Along came the Moore's Law which states that the number of transistors on an Integrated Circuit will double every two years. This came true until recently and the number of transistors on a single chip has exponentially increased since its first introduction. With the introduction of the new 10nm technology, each square millimeter of the IC can be packed with 100 million transistors [13]. With technology improving at such a drastic pace, it has penetrated into almost every sphere of human life. Day-to-day activities such as communications, business, financial transactions and so on depend on technology. Digital footprint of human being has become an inevitable parameter and unavoidable [18]. Internet of Things (IoT) has become an integral part of our lives. In an IoT environment, every device is connected to the network and will have a unique Internet Protocol (IP) address [56]. Smart Cities, Smart Grid, Smart Healthcare and so on are various forms of IoT.

With so many devices connected to each-other, there are security concerns that are raised. The data that is being collected by various applications, sensors and other devices should be stored securely. There are many attacks reported recently where security needs to be given the highest importance [8, 9]. To secure the data that is being generated, cryptography is being used. It has been around for a very long time. Cryptography is the process of concealing a message or information by converting it into unreadable text and only the end user will be able to extract the original information from the text. It was found that Egyptians used such techniques in the year 1900 B.C. [2]. Various algorithms are available currently for encryption and decryption which can transfer the data securely. National Bureau of Standards proposed data encryption standard (DES) algorithm which lasted for 20 years. Then came advanced encryption standard (AES) algorithm which is very popular now but there have been reports of AES being successfully broken [49]. $7.5 Billion is estimated to be lost by the US semiconductor industry because of IC counterfeiting [61]. Besides all of this, in the case of many devices, sensors or applications, the device itself will not be monitored all the time. It will be in a remote

References

1. http://www.eecs.mit.edu/news-events/media/mit-spinoff-verayo-developed-srini-devadas-gains-increase
2. Steganography: Past, Present, Future. SANS Institute InfoSec Reading Room (2001). URL http://www.sans.org/reading-room/whitepapers/stenganography/steganography-past-present-future-552
3. AMD: AMD Ryzen (2018). URL https://www.amd.com/en/products/cpu/amd-ryzen-7-2700x. Last Accessed: 7-1-2018
4. Bai, C., Zou, X., Dai, K.: A Novel Thyristor-Based Silicon Physical Unclonable Function. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **24**(1), 290–300 (2016). DOI 10.1109/TVLSI.2015.2398454
5. Barker, E.B., Kelsey, J.M.: Recommendation for Random Number Generation Using Deterministic Random Bit Generators. National Institute of Standards and Technology, NIST (2015)
6. Bhm, C.: Physical Unclonable Functions in Theory and Practice (2013)
7. Chang, C.H., Zheng, Y., Zhang, L.: A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement. IEEE Circuits and Systems Magazine **17**(3), 32–62 (2017). DOI 10.1109/MCAS.2017.2713305
8. Charette, R.: 2017 was a record year for id theft in the u.s. IEEE Spectrum (2018)
9. Charette, R.: Healthcare it systems: Tempting targets for ransomware. IEEE Spectrum (2018)
10. Chatterjee, U., Chakraborty, R.S., Mathew, J., Pradhan, D.K.: Memristor Based Arbiter PUF: Cryptanalysis Threat and Its Mitigation. In: 29th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID), pp. 535–540 (2016). DOI 10.1109/VLSID.2016.57
11. Chatterjee, U., Chakraborty, R.S., Mukhopadhyay, D.: A PUF-Based Secure Communication Protocol for IoT. ACM Trans. Embed. Comput. Syst. **16**(3), 67:1–67:25 (2017)
12. Chowdhury, S., Xu, X., Tehranipoor, M., Forte, D.: Aging Resilient RO PUF with Increased Reliability in FPGA. In: 2017 International Conference on ReConFigurable Computing and FPGAs (ReConFig), pp. 1–7 (2017). DOI 10.1109/RECONFIG.2017.8279773
13. Courtland, R.: Intel Now Packs 100 Million Transistors in Each Square Millimeter. IEEE Spectrum (2017)
14. Dimitrakopoulos, C.D., Pfeiffer, D., Smith, J.T.: Authentication using Graphene based devices as physical unclonable functions (2012)
15. Ganta, D., Nazhandali, L.: Study of IC Aging on Ring Oscillator Physical Unclonable Functions. 15th International Symposium on Quality Electronic Design (ISQED) pp. 461–466 (2014)
16. Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O., Abbott, D.: Emerging Physical Unclonable Functions With Nanotechnology. IEEE Access **4**, 61–80 (2016). DOI 10.1109/ACCESS.2015.2503432
17. Gassend, B., Clarke, D., Dijk, M.V., Devada, S.: Controlled Physical random Functions. 18th Annual Computer Security Applications Conference pp. 149–160 (2002)
18. Gencoglu, O., Simil, H., Honko, H., Isomursu, M.: Collecting a Citizen's Digital Footprint for Health Data Mining. In: 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 7626–7629 (2015). DOI 10.1109/EMBC.2015.7320158
19. Giterman, R., Weizman, Y., Teman, A.: Gain-Cell Embedded DRAM-Based Physical Unclonable Function. IEEE Transactions on Circuits and Systems I: Regular Papers pp. 1–11 (2018). DOI 10.1109/TCSI.2018.2838331
20. Gunlu, O., Iscan, O.: DCT based ring oscillator Physical Unclonable Functions. IEEE International Conference o Acoustics, Speech and Signal Processing (ICASSP) pp. 8198–8201 (2014)
21. Haider, I., Hoberl, M., Rinner, B.: Trusted Sensors for Participatory Sensing and IoT Applications based on Physically Unclonable Functions. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 14–21 (2016)
22. Hashemian, M.S., Singh, B., Wolff, F., Weyer, D., Clay, S., Papachristou, C.: A Robust Authentication Methodology using Physically Unclonable Functions in DRAM Arrays. In: Design, Automation Test in Europe Conference Exhibition (DATE), pp. 647–652 (2015). DOI 10.7873/DATE.2015.0308
23. Herder, C., Yu, M.D., Koushanfar, F., Devadas, S.: Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE **102**(8), 1126–1141 (2014). DOI 10.1109/JPROC.2014.2320516
24. Huai, Y.: Spin-Transfer Torque MRAM (STT-MRAM) : Challenges and Prospects. AAPPS Bulliten **18**(6) (2010)
25. Ikezaki, Y., Nozaki, Y., Nagata, H., Yoshikawa, M.: FPGA Implementation Technique for Power Consumption Aware Tamper Resistance Accelerator of Lightweight PUF. In: 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), pp. 1–2 (2017). DOI 10.1109/GCCE.2017.8229397
26. Jeloka, S., Yang, K., Orshansky, M., Sylvester, D., Blaauw, D.: A Sequence Dependent Challenge-Response PUF Using 28nm SRAM 6T Bit Cell. In: Symposium on VLSI Circuits, pp. C270–C271 (2017). DOI 10.23919/VLSIC.2017.8008504
27. Johnson, A.P., Chakraborty, R.S., Mukhopadhyay, D.: A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications. IEEE Transactions on Multi-Scale Computing Systems **1**(2), 110–122 (2015). DOI 10.1109/TMSCS.2015.2494014
28. Joshi, S., Mohanty, S.P., Kougianos, E.: Everything You Wanted to Know About PUFs. IEEE Potentials **36**(6), 38–46 (2017)
29. Khan, M.A., Mohanty, S.P., Kougianos, E.: Statistical Process Variation Analysis of a Graphene FET based LC-VCO for WLAN Applications. In: Proceedings of the 15th IEEE International Symposium on Quality Electronic Design (ISQED), pp. 569–574 (2014)
30. Kilby, J.S.: Invention of the Integrated Circuit. IEEE, TRANSACTIONS ON ELECTRON DEVICES **23**(7), 648–654 (1976)
31. Kim, G.H., Kim, K.M., Seok, J.Y., Lee, H.J., Cho, D.Y., Han, J.H., Hwang, C.S.: A theoretical model for Schottky diodes for excluding the sneak current in cross bar array resistive memory. In: Preceedings of IOP Science on Nanotechnology, pp. 1–7 (2010)

32. Koeberl, P., Li, J., Rajan, A., Wu, W.: Entropy Loss in PUF-Based Key Generation Schemes: The Repetition Code Pitfall. In: IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 44–49 (2014). DOI 10.1109/HST.2014.6855566
33. Konigsmark, S.T.C., Hwang, L.K., Chen, D., Wong, M.D.F.: CNPUF: A Carbon Nanotube-based Physically Unclonable Function for secure low-energy hardware design. 19th Asia and South Pacific Design Automation Conference (ASP-DAC) pp. 73–78 (2014)
34. k. Kumar, S., Sahoo, S., Mahapatra, A., Swain, A.K., Mahapatra, K.K.: Microprocessor Based Physical Unclonable Function. In: IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pp. 246–251 (2017). DOI 10.1109/iNIS.2017.59
35. Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P.: Extended abstract: The butterfly PUF protecting IP on every FPGA. IEEE International Workshop on Hardware-Oriented Security and Trust, HOST (11), 67–70 (2008)
36. Lao, Y., Parhi, K.K.: Reconfigurable Architecture for Silicon Physical Unclonable Function. IEEE International Conference on Electro/Information Technology (EIT) pp. 1–7 (2011)
37. Lao, Y., Parhi, K.K.: Statistical Analysis of MUX-Based Physical Unclonable Functions. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **33**(5), 649–662 (2014). DOI 10.1109/TCAD.2013.2296525
38. Lee, J., Lim, D., Gassend, B., Suh, G.E., van Dijk, M., Devadas, S.: A technique to build a secret key in integrated circuits with identification and authentication applications. Digest of Technical Papers. 2004 Symposium on VLSI Circuits pp. 176–179 (2004)
39. Leest, V.V.D., Jan, S.G., Helena, H., Pim, T.: Hardware Intrinsic Security from D Flip-Flops. In: Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing, STC '10, pp. 53–62. ACM, New York, NY, USA (2010). DOI 10.1145/1867635.1867644
40. Liu, H., Liu, W., Lu, Z., Tong, Q., Liu, Z.: Methods for Estimating the Convergence of Inter-Chip Min-Entropy of SRAM PUFs. IEEE Transactions on Circuits and Systems I: Regular Papers **65**(2), 593–605 (2018). DOI 10.1109/TCSI.2017.2733582
41. Lugli, P., Mahmoud, A., Csaba, G., Algasinger, M., Stutzmann, M., Ruhrmair, U.: Physical unclonable functions based on crossbar arrays for cryptographic applications. In: Proceedings of the International Journal of Circuit Theory and Applications, pp. 619–633 (2013)
42. Ma, Q., Gu, C., Hanley, N., Wang, C., Liu, W., O'Neill, M.: A Machine Learning Attack Resistant Multi-PUF Design on FPGA. In: 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 97–104 (2018). DOI 10.1109/ASPDAC.2018.8297289
43. Maes, R., Van Herrewege, A., Verbauwhede, I.: PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. In: E. Prouff, P. Schaumont (eds.) Cryptographic Hardware and Embedded Systems – CHES, pp. 302–319. Springer Berlin Heidelberg (2012)
44. Maiti, A., Casarona, J., McHale, L., Schaumont, P.: A Large Scale Characterization of RO-PUF. In: IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 94–99 (2010)
45. Maiti, A., Gunreddy, V., Schaumont, P.: A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions, pp. 245–267. Springer New York, New York, NY (2013). DOI 10.1007/978-1-4614-1362-2_11
46. Maiti, A., Schaumont, P.: Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive. Journal of Cryptology **24**(2), 375–397 (2011). DOI 10.1007/s00145-010-9088-4
47. Maiti, A., Schaumont, P.: The Impact of Aging on a Physical Unclonable Function. IEEE Transactions on Very Large Scale Integration (VLSI) Systems **22**(9), 1854–1864 (2014). DOI 10.1109/TVLSI.2013.2279875
48. Majzoobi, M., Koushanfar, F., Potkonjak, M.: Lightweight secure PUFs. IEEE/ACM International Conference on Computer-Aided Design pp. 670–673 (2008)
49. Mangard, S., Pramstaller, N., Oswald, E.: Successful Attacking Masked AES Hardware Implementations. In: Proceedings of the Cryptographic Hardware and Embedded Systems CHES, pp. 157–171 (2005)
50. Marukame, T., Tanamoto, T., Mitani, Y.: Extracting Physically Unclonable Function From Spin Transfer Switching Characteristics in Magnetic Tunnel Junctions. IEEE Transactions on Magnetics **50**(11), 1–4 (2014). DOI 10.1109/TMAG.2014.2325646
51. McDonald, N., Bishop, S., Briggs, B.D., Nostrand, J.E.V., Cady, N.C.: Influence of the plasma oxidation power on the switching properties of Al/CuxO/Cu memristive devices. International Semiconductor Device Research Symposium (ISDRS) pp. 1–2 (2011)
52. McDonald, N., Bishop, S., Cady, N.C.: Experimentally Demonstrated Filamnet-based Switching Mechanism for Al/CuxO/Cu Memristive Devices. IEEE International Integrated Reliability Workshop Final Report (IRW) pp. 195–198 (2012)
53. Meguerdichian, S., Potkonja, M.: Device aging-based physically unclonable functions. 48th ACM/EDAC/IEEE Design Automation Conference (DAC) pp. 288–289 (2011)
54. Mispan, M.S., Su, H., Zwolinski, M., Halak, B.: Cost-Efficient Design for Modeling Attacks Resistant PUFs. In: Design, Automation Test in Europe Conference Exhibition (DATE), pp. 467–472 (2018). DOI 10.23919/DATE.2018.8342054
55. Mohanty, S.P.: Nanoelectronic Mixed-Signal System Design. 9780071825719. McGraw-Hill Education (2015)
56. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything You wanted to Know about Smart Cities. IEEE Consumer Electronics Magazine **5**(3), 60–70 (2016)
57. O'Donnell, C.W., Suh, G.E., Devadas, S.: PUF-Based random Number Generation. MIT CSAIL CSG Technical Memo (2004)
58. Rahman, M.T., Forte, D., Fahmy, J., Tehranipoor, M.: ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design. Design, Automation and Test in Europe Conference and Exhibition (DATE) pp. 1–6 (2014)
59. Rahman, M.T., Forte, D., Rahman, F., Tehranipoor, M.: A Pair Selection Algorithm for Robust RO-PUF Against Environmental Variations and Aging. In: 2015 33rd IEEE International Conference on Computer Design (ICCD), pp. 415–418 (2015). DOI 10.1109/ICCD.2015.7357137

60. Rahman, M.T., Rahman, F., Forte, D., Tehranipoor, M.: An Aging-Resistant RO-PUF for Reliable Key Generation. IEEE Transactions on Emerging Topics in Computing **4**(3), 335–348 (2016). DOI 10.1109/TETC.2015.2474741
61. Rose, G.S., McDonald, N., Yong, L.K.W., Wysocki, B., Xu, K.: Foundations of Memristor Based PUF Architectures. IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH) pp. 52–57 (2013)
62. Rosenblatt, S., Fainstein, D., Cestero, A., Safran, J., Robson, N., Kirihata, T., Iyer, S.S.: Field Tolerant Dynamic Intrinsic Chip ID Using 32 nm High-K/Metal Gate SOI Embedded DRAM. IEEE Journal of Solid-State Circuits **48**(4), 940–947 (2013). DOI 10.1109/JSSC.2013.2239134
63. Ruhrmair, U., Jaeger, C., Bator, M., Stutzmann, M., Lugli, P., Csaba, G.: Applications of High-Capacity Crossbar Memories in Cryptography. In: Proceedings of the IEEE Transactions on Nanotechnology, pp. 489–498 (2011)
64. Ruhrmair, U., Jaeger, C., Hilgers, C., Algasinger, M., Csaba, G., Stutzmann, M.: Security Applications of Diodes with Unique Current-Voltage Characteristics. Financial Cryptography and Data Security pp. 328–335 (2010)
65. Sahoo, S.R., Kumar, S., Mahapatra, K.: A Modified Configurable RO PUF with Improved Security Metrics. In: Proceedings of the 2nd IEEE International Symposium on Nanoelectronic and Information Systems, pp. 320–324 (2016). DOI 10.1109/iNIS.2015.37
66. Sahoo, S.R., Kumar, S., Mahapatra, K.: A Novel Configurable Ring Oscillator PUF with Improved Reliability Using Reduced Supply Voltage. Microprocessors and Microsystems **60**, 40 – 52 (2018). DOI https://doi.org/10.1016/j.micpro.2018.03.012
67. Schrijen, G.J., Leest, V.V.D.: Comparative analysis of SRAM memories used as PUF primitives. Design, Automation & Test in Europe Conference & Exhibition (DATE) pp. 1319–1324 (2012)
68. Škorić, B., Tuyls, P., Ophey, W.: Robust Key Extraction from Physical Uncloneable Functions. In: J. Ioannidis, A. Keromytis, M. Yung (eds.) Applied Cryptography and Network Security, pp. 407–422. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
69. Su, Y., Holleman, J., Otis, B.P.: A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations. IEEE Journal of Solid-State Circuits **43**(1), 69–77 (2008). DOI 10.1109/JSSC.2007.910961
70. Suh, G.E., Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation. 44th ACM/IEEE Design Automation Conference pp. 9–14 (2007)
71. Suh, G.E., O'Donnell, C.W., Sachdev, I., Devadas, S.: Design and Implementation of the AEGIS Single-Chip Secure PrProcess Using Physical Random Functions. In: Proceedings of the 32nd International Symposium on Computer Architecture (ISCA), pp. 1–12 (2005)
72. Tanaka, Y., Bian, S., Hiromoto, M., Sato, T.: Coin Flipping PUF: A Novel PUF With Improved Resistance Against Machine Learning Attacks. IEEE Transactions on Circuits and Systems II: Express Briefs **65**(5), 602–606 (2018). DOI 10.1109/TCSII.2018.2821267
73. Wan, M., He, Z., Han, S., Dai, K., Zou, X.: An Invasive-Attack-Resistant PUF Based On Switched-Capacitor Circuit. IEEE Transactions on Circuits and Systems I: Regular Papers **62**(8), 2024–2034 (2015). DOI 10.1109/TCSI.2015.2440739
74. Wang, X., Tehranipoor, M.: Novel Physical Unclonable Function with Process and Environmental Variations. Design, Automation & Test in Europe Conference & Exhibition (DATE) pp. 1065–1070 (2010)
75. Wen, Y., Lao, Y.: PUF Modeling Attack using Active Learning. In: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–5 (2018). DOI 10.1109/ISCAS.2018.8351302
76. Wong, H.S.P., Raoux, S., Kim, S., Liang, J., Reifenberg, J.P., Rajendran, B., Asheghi, M., Goodson, K.E.: Phase Change Memory. Proceedings of the IEEE **98**(12), 2201–2227 (2010). DOI 10.1109/JPROC.2010.2070050
77. Yan, W., Tehranipoor, F., Chandy, J.A.: PUF-Based Fuzzy Authentication Without Error Correcting Codes. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **36**(9), 1445–1457 (2017). DOI 10.1109/TCAD.2016.2638445
78. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Making Use of Semiconductor Manufacturing Process Variations: FinFET-based Physical Unclonable Functions for Efficient Security Integration in the IoT. IEEE Potentials **93**(3), 429–441 (2017)
79. Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security. IEEE Transactions on Semiconductor Manufacturing **PP**(99), 1–1 (2018). DOI 10.1109/TSM.2018.2818180
80. Ye, J., Gong, Y., Hu, Y., Li, X.: Polymorphic PUF: Exploiting Reconfigurability of CPU + FPGA SoC to Resist Modeling Attack. In: IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 205–206 (2017). DOI 10.1109/IOLTS.2017.8046220
81. Ye, J., Guo, Q., Hu, Y., Li, H., Li, X.: Modeling Attacks on Strong Physical Unclonable Functions Strengthened by Random Number and Weak PUF. In: IEEE 36th VLSI Test Symposium (VTS), pp. 1–6 (2018). DOI 10.1109/VTS.2018.8368627
82. Yu, L., Wang, X., Rahman, F., Tehranipoor, M.: iPUF: Interconnect PUF with Self-Masking Circuit for Performance Enhancement. In: 18th International Workshop on Microprocessor and SOC Test and Verification (MTV), pp. 45–50 (2017). DOI 10.1109/MTV.2017.14
83. Yu, M.D., Devadas, S.: Secure and Robust Error Correction for Physical Unclonable Functions. In: Proceedings of the IEEE Design & Test of Computers, pp. 48–65 (2010)

IP Core Protection and Hardware-Assisted Security for Consumer Electronics

IP Core Protection and Hardware-Assisted Security for Consumer Electronics presents established and novel solutions for security and protection problems related to IP cores (especially those based on DSP/multimedia applications) in consumer electronics. The topic is important to researchers in various areas of specialization, encompassing overlapping topics such as EDA-CAD, hardware design security, VLSI design, IP core protection, optimization using evolutionary computing, system-on-chip design and application specific processor/hardware accelerator design.

The book begins by introducing the concepts of security, privacy and IP protection in information systems. Later chapters focus specifically on hardware-assisted IP security in consumer electronics, with coverage including essential topics such as hardware Trojan security, robust watermarking, fingerprinting, structural and functional obfuscation, encryption, IoT security, forensic engineering based protection, JPEG obfuscation design, hardware assisted media protection, PUF and side-channel attack resistance.

About the Authors

Anirban Sengupta is an Associate Professor in Computer Science and Engineering at Indian Institute of Technology (IIT) Indore. He is the author of 172 peer-reviewed publications. He is a recipient of honors such as IEEE Distinguished Lecturer by CESoc in 2017, IEEE Computer Society TCVLSI Editor Award in 2017 and IEEE Computer Society TCVLSI Best Paper Award in iNIS 2017. He holds around 12 Editorial positions. He is the Editor-in-Chief of IEEE VCAL (IEEE CS- TCVLSI) and General Chair of 37th IEEE International Conference on Consumer Electronics 2019, Las Vegas.

Saraju P. Mohanty is a tenured full Professor at the University of North Texas (UNT). He has authored 280 research articles, 3 books, and invented 4 US patents. He has received various awards and honors, including the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, IEEE Distinguished Lecturer by the Consumer Electronics Society (CESoc) in 2017, and the PROSE Award for best Textbook in Physical Sciences & Mathematics in 2016. He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine (CEM). He has received 4 best paper awards and has delivered multiple keynotes.

ISBN 978-1-78561-799-7

9 781785 617997 >

Materials, Circuits & Devices
Security

The Institution of Engineering and Technology • www.theiet.org
978-1-78561-799-7