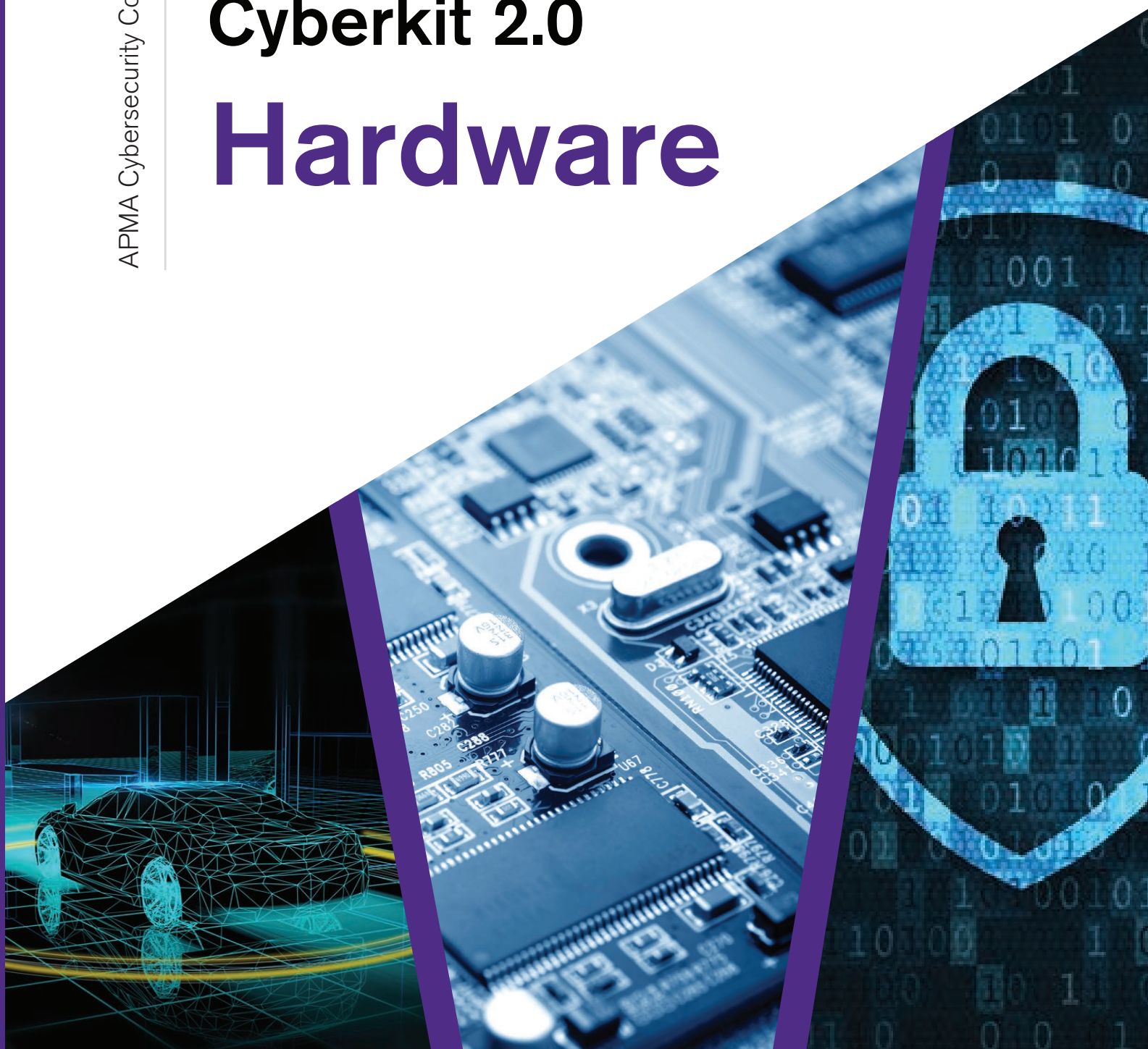
APMA
LEAD. REACH. CONNECT.

March 2021

APMA Cybersecurity Committee

Cyberkit 2.0

Hardware




600GB 10K
600GB 10K

CONTENTS

Introduction

The daily expansion of the employment of system-on-chips (SoC), and the general tendency towards automation, have raised many security concerns.

The multiple possible targets that an adversary can exploit to achieve malicious purposes are difficult to predict and model. The multiple possible targets that an adversary can exploit to achieve malicious purposes are difficult to predict and model.

Without a comprehensive understanding of the whole system, security assumptions made at each level may result in a system that fails to detect possible intrusions.

From the hardware security perspective, the hardware used in a system implementation may have unwanted components, resulting in a lack of reliability. On the other hand, an adversary can attack a pure, original system to exploit IP-valued data and system access keys. In fact, to increase the security of sensitive systems, cryptographic devices are employed to code the valued data.

It is possible for an adversary to simply examine the cryptographic devices to achieve a secured system's decryption codes. In this manuscript, we will briefly investigate these two types of hardware security fields.

An adversary can attack a pure, original system to exploit IP-valued data and system access keys.

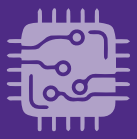
Hardware Trojans

The globalization of the integrated circuit (IC) design and fabrication process has emerged severe concerns related to the trustworthiness and security of manufactured ICs.

The complexity of the different steps in implementing integrated systems has pushed the semiconductor industry to form an IC supply chain, in which each step is accomplished in a different geographical site. These various site locations, usually in different continents, increase the risk of malicious chips. A dormant logic circuit, traditionally known as the hardware Trojan (HT), can be introduced to the original system by a culprit to affect the normal performance.

The HT circuit is usually implanted into the original circuit to achieve one or some of the following goals. First, an HT can be implemented to the original circuit to temporarily or permanently disrupt the system's functionality. In this scenario, the HT usually affects a sensitive building block of the target system. For instance, Trojan infested, off-the-shelf microprocessors used in implementing a Syrian radar system failed upcoming attack detection in 2008 [1]. As another example, a back-door in a processing chip used in Boing 787 was detected in 2012, allowing unauthorized navigation and flight control [2].

Another goal for an HT circuit is to leak data towards the HT designer. In this scenario, the HT does not affect the normal functionalities of the original circuit.



Trojan (HT), can be introduced to the original system by a culprit to affect the normal performance.

Still, the confidential data such as the decryption key for a cypher-text or data processing results of a microprocessor are transmitted to the adversary. For instance, in 2010, a hardware Trojan warning issued by Dell company for some of its server motherboards [2]. In [3], a wireless cryptographic IC was shown to be attacked by a simple yet extremely functional Trojan circuit, which was able to modulate the decryption keyword into frequency or amplitude.

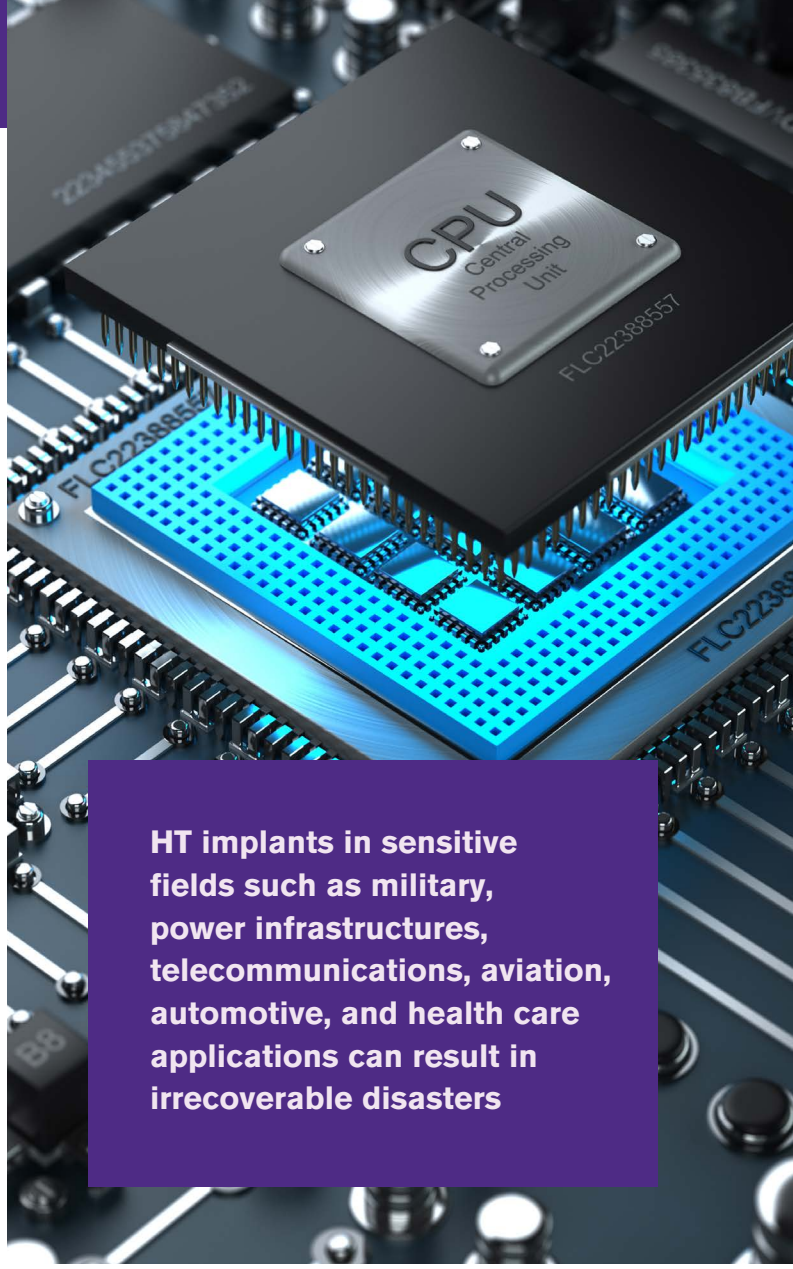
The modulated data was transmitted over a shared wireless channel and a normal data package and successfully received by an original and a rogue receiver. The original receiver could not find any significant

difference between the normal package and the received data. Nevertheless, the rogue receiver, which knew where to look precisely, could recover the desired code.

Finally, an HT circuit can be implemented into an original circuit for intellectual property (IP) piracy. In this scenario, different Trojan infested chips, which are used to implement an IP-valued system (on a PCB or an FPGA), leak their data to reveal the functionality of the whole system to the adversary [4].

Since HT implants in sensitive fields such as military, power infrastructures, telecommunications, aviation, automotive, and health care applications can result in irrecoverable disasters, it is required to design proper defence mechanisms to detect and disable an HT circuit in an IC. However, because of their stealthy nature, the size, topology, functionality, and location of HTs cannot be anticipated [5]. Moreover, different IC types face different threats from Trojan circuits. In other words, digital ICs, analogue and mixed-signal (AMS) ICs, and Radio Frequency (RF) ICs are targeted with different Trojan circuits for different malicious purposes. Additionally, an HT circuit is usually activated in rare conditions, and in some cases, is dormant most of the time. These features make the detection of HTs a challenging yet essential issue.

In addition to HT-based security concerns, cryptosystem designers and security system experts have always been worried about a possible adversary who is listening to the communication channel and wireless network for data and access keys. In this kind of attack, the adversary does not need to alter the hardware



HT implants in sensitive fields such as military, power infrastructures, telecommunications, aviation, automotive, and health care applications can result in irrecoverable disasters

which is used in the system. Instead, they just listen to communications over the channel to exploit confidential data.

In this section, we investigate the general structure of an HT circuit and study different available approaches for the detection of HTs in digital, AMS, and RF ICs. It should be mentioned that because the HT field has attracted researchers in recent years, it is hard to propose a single method for HT detection in different ICs. Moreover, some of the following approaches can be shared for Trojan detection in digital, AMS, and RF ICs.

A Trojan Circuits

Although numerous Trojan circuits can be used for malicious purposes, they usually share the typical structure shown in *Fig. 1*. As shown in this structure, the HT requires a trigger circuit, which activates the HT. To make HT hard to detect, the trigger condition is usually a rare condition in the host circuit.

The trigger signal activates the main HT circuit, which is responsible for performing the malicious action. The payload delivers the result of the HT circuit to the desired destination [5].

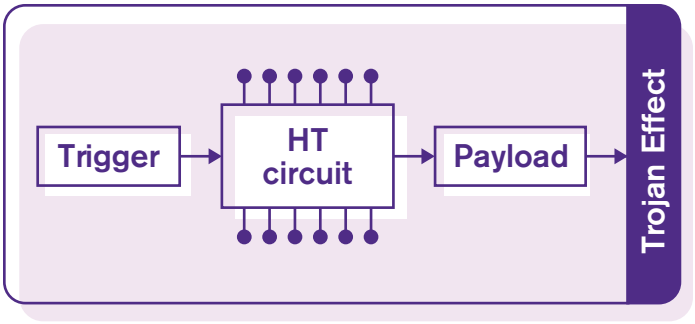


Figure 1. Typical Hardware Trojan Structure

A potential candidate for trigger circuits in digital ICs is the counter-based Trojan structure. In this structure, one or some of the most significant bits of an inserted or available counter in the host IC are used for HT activation [6].

In this scenario, the HT requires some digital gates implemented by MOS transistors, which in turn will affect the circuit configuration and its fingerprints, such as the power consumption and the path delay.

However, a capacitive based analogue HT was proposed in [7], which generally does not affect the fingerprints of the original circuit. The basic idea in [7] is to charge an invader capacitor using a clock in the circuit. With each pulse, some voltage is stored on the capacitor. If this voltage exceeds a threshold voltage, an attack to the host circuit is lunched.

Another possible Trojan in AMS ICs, known as Trojan State (TS), results from the fact that it is possible for an analogue circuit with positive feedback loops to have multiple stable DC operating points, one of them is the point in which the circuit shows normal performance.

This issue is usually addressed with start-up circuits, which guarantee that the circuit starts at the desired DC operating point. However, if there is no start-up circuit, or if the start-up circuit itself is under attack, the operation of the circuit can be disrupted. This issue is challenging in bias generators in AMS and RF ICs [8, 9].

B Trojan Prevention

The most obvious solution in dealing with HTs is to employ Trojan prevention mechanisms. In other words, design for hardware trust, which prevents HT insertion into the integrated circuits, has been investigated to achieve trustworthy chips. The first requirement for an adversary to insert an HT into an integrated circuit is to achieve a comprehensive understanding of the target chip.

Therefore, the first solution for Trojan prevention is to

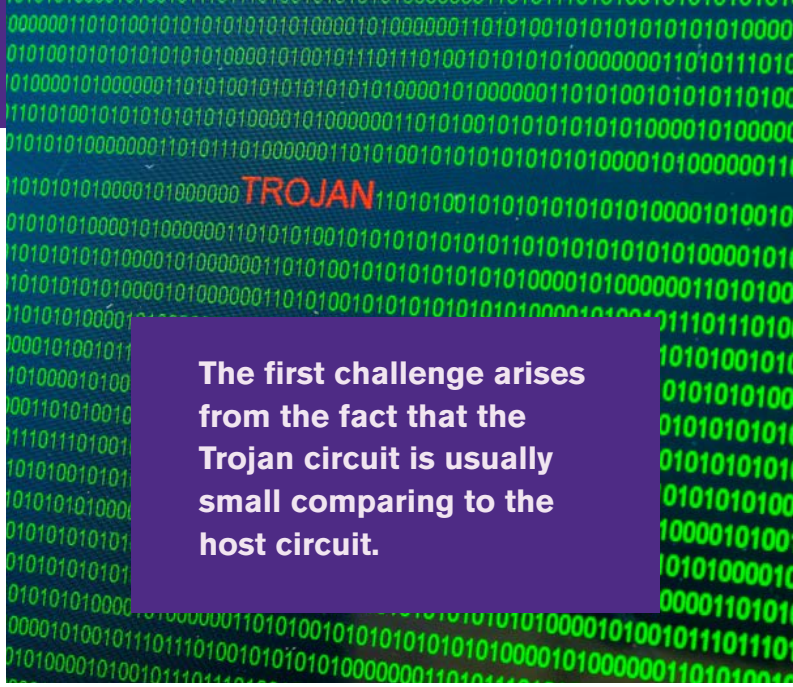
obscure the performance and functionality of the IC from adversaries. In [10], dummy contacts are used to mask functionality. Depending on the placement of the dummy contacts, a unique cell in layout can represent different gates. In [11], different threshold voltages are achieved using different doping patterns, which result in threshold dependent, disguised cells. However, the ultimate solution for Trojan prevention seems to arise from the fact that less HT insertion resources can decrease the probability of HT insertion. In other words, a layout fill approach can eliminate all of the available space for Trojan insertion [12].

C Trojan Detection

Although the detection of the Trojans in integrated circuits is extremely necessary, there are several challenges in this way.

The first challenge arises from the fact that the Trojan circuit is usually small comparing to the host circuit. Therefore, its chip area occupation is ignorable comparing to the host circuit, and physical comparison or imaging of the device under test (DUT) might not be so beneficial.

The other possible solution for HT detection is to use side-channel signal analysis. A side-channel signal is basically a signal which can be probed during the operation of a chip [6]. The most popular side-channel signals are the transient current, the power, and the delay of the circuit [6], [13] [14]. The general idea in HT detection using side-channel signal analysis relies on



The first challenge arises from the fact that the Trojan circuit is usually small comparing to the host circuit.

the fact that implanting the HT deviates the side channel signal of the infected chip form the normal expected value. Therefore, monitoring the side channel signals can result in HT detection. However, this approach faces several issues. First of all, the contribution of the HT circuit in the side channel signal of the circuit might be zero before activation (especially for power-based approaches). Since most of the HT circuits are dormant for most of their lifetime, HT detection using side-channel analysis might fail.

Secondly, the side channel signal based approaches usually require a golden reference IC, for comparison. Finding the golden chip fingerprints using a trusted fabrication run, or using the statistical investigation of random chips, is not so easy. Finally, even when the HT is activated and the golden chip is available, the HT side-channel effect can easily stay within the margins of noise and process variations effect [3].

In the following sub-sections, we briefly review the main available approaches for HT detection in digital, AMS and RF ICs. It should be mentioned that it is possible to use some of the available HT detection approaches (like side-channel signal analysis) on these three different types of ICs.

Trojan Detection in Digital ICs

Since off-the-shelf, commercially available digital processing chips like FPGAs and microprocessors are vastly used in the implementation of electronics and communication systems, several HT detection approaches are available for them in literature. The main obstacles in the detection of HTs in digital ICs arise from the fact that digital integrated circuits are usually composed of a very large number of MOS transistors. An HT circuit consisting of a few digital gates or flip flops (FFs) does not affect the characteristics of the infested chip.

A possible approach for HT detection in digital chips is to divide the chip into several clusters. Although the HT may not affect the side channel signals of the whole chip, it may deviate the side channel signals of the cluster under attack. The key point in cluster-based HT detection approaches is that during the investigation process for each cluster, all of the other clusters should be deactivated. Therefore, each cluster requires a virtual power and ground line for the investigation phase [6]. As another example, [15] used the clustering approach with dedicated sensors, which are embedded in the power grids of different voltage islands in FPGA, for hardware Trojan detection.

In addition to the above-mentioned side-channel signal analysis approach, several reports are available which investigate different aspects of security issues in FPGAs. The security of an FPGA includes the following aspects; 1) secure input bitstream delivery to FPGA, and 2) employment of FPGA as the attack target to breach FPGA-based systems [16]. In [17], a bitstream encryption approach is illustrated, which protects Xilinx Virtex FPGA chips. The security protocol for the encryption scheme protects the IP from being copied via restriction of access to the configuration file and key bits.

In [18], the authors proposed to monitor abnormalities in the physical layer of the FPGA by identifying the basic building block on the FPGA die that has different physical statistical characteristics with adjacent blocks. This golden-chip free technique employs the spatial correlation of intra-die process variations to detect HTs in the FPGA and evaluates each FPGA under investigation on its own characteristics. However, this

approach assumes that the HT is inserted sparsely in the FPGA fabric. If all or a large number of FPGA tiles are affected, this technique would not be functional.

In [19], a specific taxonomy of FPGA-based HT attacks is presented, including models and instances of HTs which cause malfunction or structural damage. Also, the possibility of HTs which seek confidential data leakage from an operating FPGA is illustrated in [19]. Moreover, an adapted triple modular redundancy (ATMR) approach for HT detection on FPGAs is proposed for HT detection.

In [20], the normalized side-channel signals such as power and timing variation are weighted and used to generate a signature as a threat detectability metric. This signature is compared with a threshold for HT detection.

The authors in [20] believe that a single parameter is not sufficient to detect HTs with distinct features. Therefore, a combination of parameters monitoring various characteristics of the HT is required. Hence, a novel metric for hardware Trojan detection is proposed, as HT detectability metric (HDM) that employs a weighted combination of normalized parameters. HTs are identified by comparing the HDM with a threshold reference. If the HDM is more than the optimal threshold, the FPGA is considered to be infected.

As another solution, in [21], the unoccupied FPGA space is filled with dummy logics to eliminate potential HT insertion space on the FPGA. In fact, in [21] a low-level HT protection scheme by filling the unused resources of the FPGA with low-level dummy logic (LLDL) is proposed to reduce different sources available for HT insertion.

Trojan Detection in AMS and RF ICs

A possible approach for the detection of HTs in AMS ICs is to generate IC fingerprints based on side-channel parameters. These fingerprints can be statistically assessed to detect HTs in an AMS IC. Several previous methods have been proposed for HT detection based on the side-channel signal analysis approach.

In [6], a transient current sensing method is proposed for HT detection. During the design phase of the chip, the circuit is divided into several regions, and each region is equipped with a current sensor for transient current monitoring.

To increase the probability of HT detection, only one region is activated during the inspection, while other regions are kept in the sleep mode. In this way, a power signature is extracted for the device under test. Any significant difference between this signature and the power signature of the Trojan-Free IC (golden IC) indicates the Trojan infection [6]. Also, in [13], the DUT is divided into different regions.

By partial activation of the DUT, the capability of Trojan detection using power analysis is enhanced using localized switching activity. In [22], random patterns are applied, and the power is measured. The resulting power data includes power consumption of the original circuit, noise and process variations, and power contribution of the HT. The reference power signature is obtained by reverse engineering of a small number of the ICs. The

comparison of the power signature of any chip with the reference signature indicates HT implants [22].

In [14], the insertion of the HT into a chip is considered to alter the path delay of the chip. Therefore, high-coverage input patterns for a DUT produce high-dimension path delay data, which is used for the generation of a set of delay fingerprints. Then delay signature of the DUT is compared with the reference delay fingerprint for HT detection [14]. However, the HT Trojan can be implanted in such a way that the external delay is not affected [6]. Therefore, the delay based HT detection method will not do so well in the detection of such Trojans.

In [23], two practical instances of amplitude-modulating analogue/RF HTs are presented, and the performance of such malicious circuits in an IEEE 802.11a/g transmitter is analyzed. The results prove that an HT circuit is able to establish a stealthy channel in the analogue/RF front-end of a wireless device, which is hard to detect using conventional methods.

A wideband wireless network is frequency-selective and time-varying. Therefore, Wi-Fi transceivers use channel estimation algorithms for detection and decoding. These channel estimation algorithms employ training sequences in the packet preamble and the pilot symbols to frequently estimate the channel conditions. In conventional receivers, the effect of channel non-idealities and HT circuit are bundled together.

The authors in [23] address this issue by using the slow-fading characteristic of an indoor communication channel to differentiate the effect of channel non-idealities with the effect of the HT on the calculated coefficients for HT detection.

Side-Channel Attacks

In a world full of engineering and computing systems, the storage and processing of sensitive data are everywhere. Consider a laptop system in a company that contains corporate secrets and is an exciting target for corporate espionage.

Another example is the products of engineering industries, which are shipped around the world. These products contain IP-valued information like source codes and control parameters, which must be protected from unauthorized access and manipulation [24].

The primary problem in the above-mentioned examples is that usually, the adversary has unlimited time in physical access to the target system. To prevent confidential information leakage, memory encryption is used. However, unpredicted physical side-channel attacks can be used by an adversary to access secret key material used during encryption from various side channels. The most attractive side-channel attacks use power, timing, and Electromagnetic Emanation (EM) [24].

In power-based side-channel attacks, the dependency of the instantaneous power of a cryptographic device and its processed data and operation is used to reveal the sequence of the executed instructions or the processed data [25]. Its main advantages, such as being unapparent to users and not requiring expensive equipment, make it an interesting approach for attackers [25].

The simple power analysis (SPA) approach monitors one or a few power signals during cryptographic operations [26]. On the other hand, in differential power analysis

(DPA), a large number of power signals are statistically examined to extract confidential data [27]. The correlation power analysis (CPA), which can be considered as normalized DPA, examines the correlation between the power consumption of the cryptographic device and a reference model [28].

To increase the immunity of the cryptographic device to power side-channel attacks, three main approaches are used. The basic idea in these three approaches is to change the encryption hardware device in such a way that its power consumption does not depend on the signal transitions. In the first approach, the signal to noise ratio (SNR) of the information is reduced using noise injection to power traces [29].

The second approach balances the power consumption at the rising and falling edges using dual-rail circuits [30] and wave dynamic differential logic [31]. The final solution is to isolate the power from the encryption engine, using switched capacitor circuits [32] or integrated voltage regulators [33].

In timing side-channel attacks, the time required for the execution of cryptographic algorithms is examined. The time that a particular operation needs to be executed depends on the inputs and the executed algorithm. Therefore, an adversary can use the measured execution time for specific inputs to achieve some information about the encryption system [34].

To remove the threat of timing attacks, one solution is to eliminate data-dependent timing information or to use constant-time algorithms. In [34], a dynamic delay management system is proposed to address the timing side-channel attacks in FPGAs. In order to reduce the dependency of the encrypted output delays to the internal values, a chain of several CMOS inverters is added into the design, which is activated according to the input data, to build a system with constant delay. In [35], a countermeasure with special masking techniques is presented to enhance the timing attack resistance by variegating virtualized hardware across physical FPGAs.

The most attractive side-channel attacks use power, timing, and Electromagnetic Emanation (EM)

While the power side-channel attacks use physical probing to monitor the power consumption of the cryptographic device, the basic idea in electromagnetic emanation attacks is to use electromagnetic analysis to retrieve data. A target chip is composed of numerous logic gates and metallic connections. During code execution, the flow of pulse currents generates weak electromagnetic waves.

These data-dependent radiations can be monitored to extract confidential data [36]. This kind of attacks has been recently addressed with inductive voltage regulators integrated with clock modulators [37]. The basic idea in this approach is to use the constant switching of the integrated inductive voltage regulator to alleviate the EM radiations issue.

Acknowledgements

Hardware module:

Flavio Volpe
President, APMA

Colin Dhillon
Chief Technical Officer, APMA

The Automotive Parts Manufacturers' Association (APMA) of Canada President and CTO would like to thank the cybersecurity committee members for their continued efforts to provide leadership and a global voice on the topic of automotive cybersecurity, privacy and cyber safety. The work you have all undertaken is having a positive impact in the complete auto ecosystem.

Dr. Mitra Mirhassani
Associate Professor,
University of Windsor

We would like to acknowledge Dr. Mitra Mirhassani, Associate Professor at the University of Windsor, for leading the development of the Hardware module for Cyberkit 2.0.

The APMA would also like to thank the members of its cybersecurity committee for their continued support and ongoing efforts.

Catherine Bertheau - Cyber Solutions Business Dev Lead - Aon
Sumit Bhatia – Director, Communications & Knowledge Mobilization -– Ryerson Cybersecure Catalyst
Todd Bielarczyk - Intelligence Officer - CSIS
Olivier Charron – Microsoft Canada
Sarah Chippure – Senior Policy Analyst - Transport Canada
Ali Dehghantanha – Director – Cyber Science Lab – University of Guelph
Trish Dyl – Director of Partnerships – Ryerson Cybersecure Catalyst
Peter Elliot – Global Information Security Officer – Magna International
John Esvelt – Chief Risk Officer - Dentons
Sebastian Fischmeister – Professor – University of Waterloo
John Heaton – Partner, Cybersecurity - KPMG
Ganesh Iyer - CIO & VP of Eng. - Martinrea
Marc Kneppers - Chief Security Architect – Telus Communications
Philip Lafrance – Standards Manager - Isara
Kevin Magee – Chief Security and Compliance Officer - Microsoft Canada
Siddhartha Parti -Global Director IT, Infrastructure & Ops – Woodbridge
Ken Schultz – General Manager - Escrypt
Jazz Singh – Cybersecurity, IT & Risk – TD Bank
Cara Wolf – Founder & CEO – Ammolite Analytx
John Wright – Founder & Chairman - JPOM

References:

[1] S. Adee, “The Hunt for The Kill Switch,” IEEE Spectrum, vol. 45, no. 5, pp. 34–39, May 2008.

[2] A. Antonopoulos, C. Kapatsori and Y. Makris, “Security and trust in the analog/mixed-signal/RF domain: A survey and a perspective,” 2017 22nd IEEE European Test Symposium (ETS), Limassol, 2017, pp. 1-10.

[3] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, “Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs,” IEEE Transactions on Very Large Scale Integration Systems, vol. 25, no. 4, pp. 1506–1519, 2017.

[4] M. M. Tehranipoor, U. Guin, and S. Bhunia, “Invasion of the hardware snatchers,” IEEE Spectr., vol. 54, no. 5, pp. 36–41, 2017.

[5] Mohammad Tehranipoor, A Survey of Hardware Trojan Taxonomy and Detection,2010

[6] Y. Cao, C.-H. Chang, and S. Chen, “A cluster-based distributed active current sensing circuit for hardware trojan detection,” IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2220–2231, 2014.

[7] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, “A2: Analog malicious hardware,” in Proc. IEEE Symp. Secur. Privacy, 2016, pp. 18–37.

[8] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, “A hardware Trojan embedded in the Inverse Widlar reference generator,” in Proc. IEEE Int. Midwest Symp. Circuits Syst., 2015, pp. 1–4.

[9] Z. Liu, Y. Li, Y. Duan, R. L. Geiger, and D. Chen, “Identification and break of positive feedback loops in Trojan states vulnerable circuits,” in Proc. IEEE Int. Symp. Circuits Syst., 2014, pp. 289–292.

[10] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, “Security analysis of integrated circuit camouflaging,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Berlin, Germany, 2013, pp. 709–720.

[11] M. I. M. Collantes, M. E. Massad, and S. Garg, “Threshold-dependent camouflaged cells to secure circuits against reverse engineering attacks,” in Proc. IEEE Comput. Soci. Annu. Symp. VLSI, Pittsburgh, PA, USA, 2016, pp. 443–448.

[12] P.-S. Ba, M. Palanichamy, S. Dupuis, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, “Hardware Trojan prevention using layout-level design approach,” in Proc. Eur. Conf. Circuit Theory Des., Trondheim, Norway, 2015, pp. 1–4.

[13] H. Salmani and M. Tehranipoor, “Layout-aware switching activity localization to enhance hardware trojan detection,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 76–87, 2011.

[14] Y. Jin and Y. Makris, “Hardware trojan detection using path delay fingerprint,” in 2008 IEEE International workshop on hardware-oriented security and trust. IEEE, 2008, pp. 51–57.

[15] Y. Cao, C.-H. Chang, and S. Chen, “Cluster-based distributed active current timer for hardware Trojan detection,” in Proc. IEEE Int. Symp.
Circuits Syst. (ISCAS), vol. 1, May 2013, pp. 1_4.

[16] Z. Zhang, L. Njilla, C. A. Kamhoua and Q. Yu, “Thwarting Security Threats From Malicious FPGA Tools With Novel FPGA-Oriented Moving Target Defense,” in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 3, pp. 665-678, March 2019

[17] S. Trimberger, “Trusted design in FPGAs,” in Proc. DAC, Jun. 2007, pp. 5–8.

[18] Y. Pino, V. Jyothi, and M. French, “Intra-die process variation aware anomaly detection in FPGAs,” in Proc. ITC, Oct. 2014, pp. 1–6.

[19] S. Mal-Sarkar, A. Krishna, A. Ghosh, and S. Bhunia, “Hardware trojan attacks in FPGA devices: Threat analysis and effective counter measures,” in Proc. GLSVLSI, May 2014, pp. 287–292.

[20] D. M. Shila and V. Venugopal, “Design, implementation and security analysis of hardware trojan threats in FPGA,” in Proc. IEEE ICC, Jun. 2014, pp. 719–724.

[21] B. Khaleghi, A. Ahari, H. Asadi, and S. Bayat-Sarmadi, “FPGA based protection scheme against hardware trojan horse insertion using dummy logic,” IEEE Embedded Syst. Lett., vol. 7, no. 2, pp. 46–50, Jun. 2015.

[22] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, “Trojan detection using ic fingerprinting,” in 2007 IEEE Symposium on Security and Privacy (SP’07). IEEE, 2007, pp. 296–310.

[23] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia and Y. Makris, “Amplitude-Modulating Analog/RF Hardware Trojans in Wireless Networks: Risks and Remedies,” in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3497-3510, 2020,

[24] Unterluggauer, T & Mangard, S 2016, Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption. in Constructive Side-Channel Analysis and Secure Design - COSADE 2016. LNCS, vol. 9689, Springer International Publishing AG, pp. 3-18, International Workshop on Constructive Side-Channel Analysis and Secure Design, Graz, Austria.

[25] Le, T.H., Canovas, C. and Clédiere, J., 2008, March. An overview of side channel analysis attacks. In Proceedings of the 2008 ACM symposium on information, computer and communications security (pp. 33-43)

[26] P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis”, In proceedings of CRYPTO 1999, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[27] R. Bevan and E. Knudsen, “Ways to Enhance DPA”, In proceedings of ICISC 2002, LNCS 2587, pp. 327-342, Springer-Verlag, 2003.

[28] T.H. Le, J. Clediere, C. Canovas, C.Serviµere, J.L. Lacoume and B. Robisson, “A proposition for Correlation Power Analysis enhancement”, In Proceedings of CHES 2006, LNCS 4249,

[29] T. Güneysu et.al. “Generic Side-Channel Countermeasures for Reconfigurable Devices,” in SpringerLink, Springer Berlin Heidelberg.

[30] D. Sokolov et.al. “Design and analysis of dual-rail circuits for security applications,” IEEE Trans. Comp., vol.54, no.4, pp.449–460

[31] D. D. Hwang et al., “AES-Based Security Coprocessor IC in 0.18- CMOS with Resistance to Differential Power Analysis Side-Channel Attacks”, JSSC vol.41, no.4, pp.781–792, Apr. 2006.

[32] C. Tokunaga et.al. “Securing Encryption Systems with a Switched Capacitor Current Equalizer,” IEEE JSSC, vol. 45, no. 1, Jan. 2010.

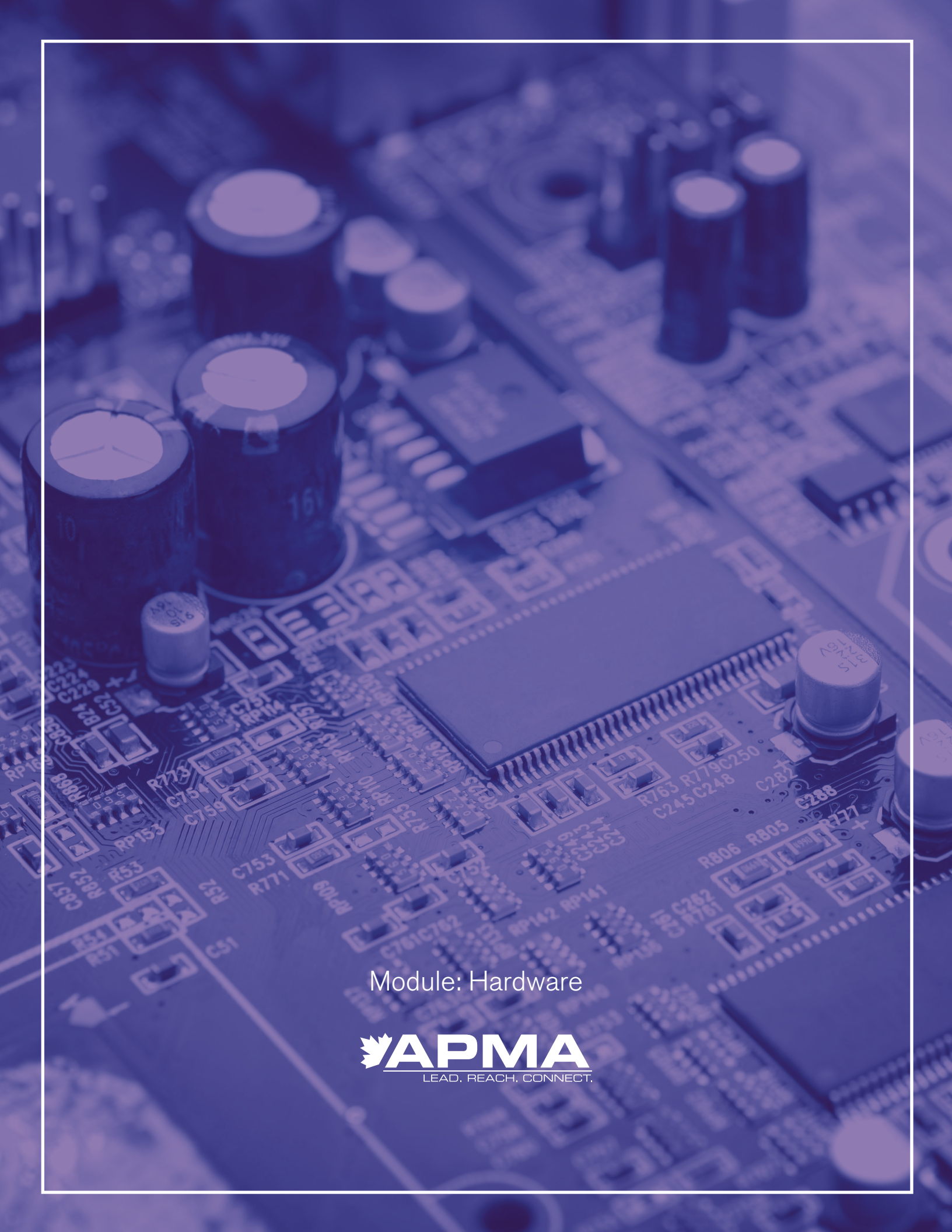
[33] M. Kar, et.al. “Exploiting Fully Integrated Inductive Voltage Regulators to Improve Side Channel Resistance of Encryption Engines,” in ISLPED 2016 New York, USA, 2016, pp. 130–135.

[34] P. Bayat-Makou, A. Jahanian and M. Reshadi, “Security Improvement of FPGA Design Against Timing Side Channel Attack Using Dynamic Delay Management,” 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), Quebec City, QC, 2018, pp. 1-4.

[35] K. Yang, J. Park, M. Tehranipoor and S. Bhunia, “Robust Timing Attack Countermeasure on Virtual Hardware,” 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Hong Kong, 2018, pp. 148-153, doi: 10.1109/ISVLSI.2018.00036.

[36] M. Prvulovic, A. Zajić, R. L. Callan and C. J. Wang, “A Method for Finding Frequency-Modulated and Amplitude-Modulated Electromagnetic Emanations in Computer Systems,” in IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 1, pp. 34-42, Feb. 2017, doi: 10.1109/TEMC.2016.2603847.

[37] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, “Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering,” IEEE J. Solid-State Circuits, vol. 54, no. 2, pp. 569–583, Feb. 2019.



Module: Hardware

APMA

LEAD. REACH. CONNECT.