ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available online at: https://www.ijergs.in

Volume - 5, Issue - 6, November – December - 2019, Page No. 13 - 18

Design and Analysis of Logic Locking in IoT System

[1]Dr. Alok Mishra, Research Supervisor, Sunrise University, Alwar, Rajasthan

[2]Ajay Saini, Research Scholar, Sunrise University, Alwar, Rajasthan

Abstract

The emergence of an ecosystem of increasingly connected, ubiquitous computing devices called the Internet of Things has contributed to considerable technical innovation (IoT). It is important to ensure the protection of these devices, considering the sensitive nature of the data gathered by IoT devices. By eliminating menial activities and improving the functionality of daily objects, the Internet of Things (IoT) holds a number of advantages for our lives. The internet-of-things can not be as secure as you assume because the devices used are limited by a variety of variables that may be used by criminals to obtain access to your data/device and everything they connect to, and as the internet-of-things is all about linking devices together, all it takes to achieve complete access may be a weak point. We look at the latest developments in IoT protection and the most powerful ways of securing IoT devices in this article. Logic encryption is a standard design-for-trust approach used for hardware IP theft, design counterfeiting, and hardware Trojan insertion security. The development of new strategies capable of thwarting the proposed attacks was motivated by the implementation of different attack methods that exploit flaws in existing logic encryption techniques.

In this essay, we discuss some of the most common methods of logic encryption and decryption proposed in the past decade. To determine their suitability for resource constrained devices, an overview of the area and power overhead of these logic encryption strategies using several common benchmark circuits is presented.

Keywords: Logic Encryption ,Internet of Things , Trust

Introduction

The Internet of Things is the interconnection of physical devices and consists of billions of devices that communicate through wireless technology. IoT operates by using sensors, processors and networking hardware to collect data from the real environment and then operate on the data. This devices are also called "smart" devices and may use connectivity protocols to communicate to other devices.

IOT Architecture

The IoT architecture can be split into three basic layers,

however they can change based on the use case's as some industry solutions may require further layers.

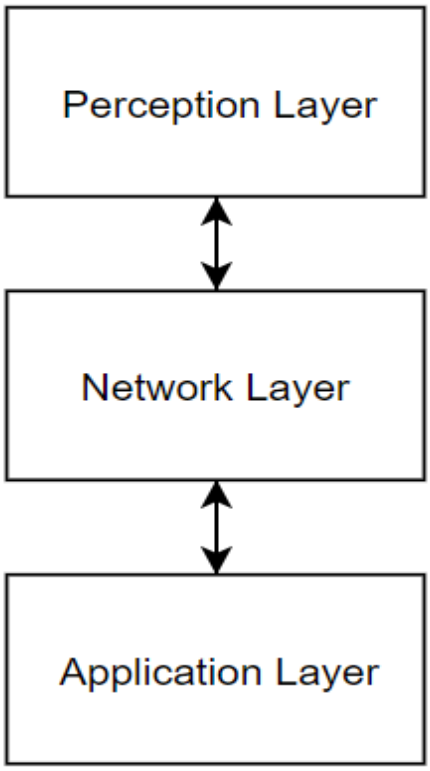

Fig.1 :Layer for IoT system

Usually, the design of conventional cryptographic algorithms that are successful against cyber attacks is not lightweight, a major requirement for IoT devices that are resource-constrained. Hardware-based authentication protocols such as logic encryption are acceptable alternatives to protect IoT devices from funder-based assaults such as reverse engineering, counterfeiting, and piracy. We will see many positives for both customers and organisations with this growth in IoT devices that streamline a number of processes, but they can still come with some drawbacks. Security & privacy is one of these drawbacks and having our personal data (banking information/location/activity) shared between devices comes with the risk of compromising a lot of our privacy.

Logic locking: defenses and attacks

Logic locking is a comparatively modern strategy that involves adding additional gates to the "Key gates" locking design that will change the performance and lock the right functionality of the gates affectively. This technique improves the level of protection over other less protected techniques such as IC Camouflaging, which is the method of inserting dummy contacts, so an attacker could extract an incorrect net list. Just in Fig. 2. Some XOR gates are used as main gates that need to be 0 for the operation to proceed, otherwise the original output will be hidden by k1 and k2.

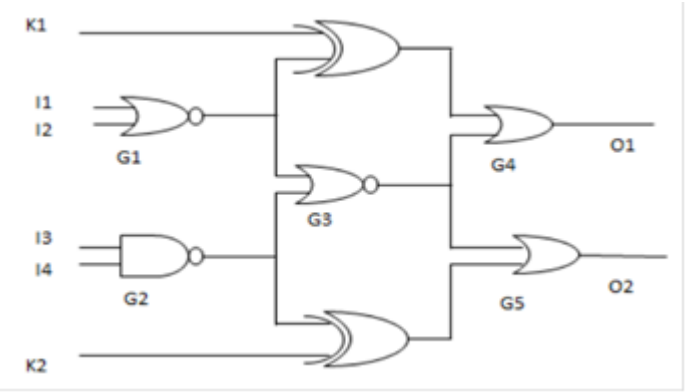

Fig.2: Logic Locking

There was a drastic reduction in the latency without losing protection when compared logic locking to an older system (OC Cell). Logic encryption is a security strategy for hardware that uses a series of newly implemented inputs called key inputs to lock the design features. Figure 2 provides an outline of logic encryption. The design acts as planned if the right logic value (chosen by the designer) is added to the main inputs. An inaccurate key value produces distortion of the circuit's input-output relationship. A basic encryption scheme as seen in Figure 2. Original schemes to encrypt logic.

Logic Encryption Techniques

The introduction of the SAT-based assault resulted in numerous SAT-resilient methods being proposed. These tactics ensured that the attack was unable to delete more than a small amount of incorrect keys per iteration by adding SAT-hard blocks, leading to incredibly long, unfeasible attack times. Through incorporating key controlled feedback loops into the architecture, other SAT-resilient strategies centred on stopping the SAT attack from modelling the circuit. We identify many methods of logic encryption suggested over the past decade. We begin by addressing conventional encryption mechanisms, which are susceptible to the SAT attack, followed by the SAT-resilient methods. Finally, the methods of sequential encryption and some of their significant characteristics are detailed.

By incorporating key-controlled XOR/ XNOR gates coupled with inverters into the circuit, EPIC is used to lock the design. These gates are positioned in the circuit on randomly selected nets while avoiding vital paths. If an incorrect key value is added to some key gate, it will invert its performance. As the attacker does not know if the inverter is part of the original configuration or part of the locking mechanism incorporated, it could be ineffective to use a straightforward reverse engineering attack to infer the key values.

As a strategy to design a well-obfuscated hardware Trojan, the Logic Cone Size dependent scheme was suggested. To stop graph isomorphism-based equivalence attacks, the insertion of main gates on networks with large fan-in and fan-out cones is advocated. Suitable positions for main gate insertion may be selected using a weighted normalised metric[2] for all gates in the architecture.

Through measuring two significant metrics - pair protection and supremacy, Good Logic Locking focuses on intelligent insertion of key regulated gates. If the key value on any one of these key gates can not be sensitised to a primary output without knowing the correct key value on the other key gate, two key gates are called pairwise stable. Meanwhile, the other key gate is said to be dominated by a key gate lying on some path from another key gate to any primary output. The key gates are inserted such that, with at least one other key gate, each key gate is pairwise safe. Additionally, with a

subset of the in-memory key serving as its input, a one-way random function like AES is used while its output is fed to each of the key gates.

In order to thwart the introduction of hardware Trojans into the architecture, a lightweight logic encryption system called Hardware Enlightening was proposed. Nets with low controllability/observability values are chosen as trigger signals for the Trojan to prevent detection during the testing process. The encryption algorithm starts by identifying nets with low values of probability. A key-controlled XOR/XNOR gate with the lowest probability value and ample slack time is applied to the fan-in signal for both of these signals. The probability values of all nets in the circuit are re-calculated after the insertion of a main gate and the procedure is repeated for the next low probability signal. A gate-level sequential logic encryption technique, Encrypt Flip-Flop proposes to add key-controlled MUXes on the outputs of scan-chain accessible flip-flops, to prevent direct reverse engineering attacks, an inverter is inserted at the output of the key gate based on a hidden signature (generated by the designer).

Each MUX's non-select inputs are related to the Q and Q ⁇ outputs of the previous flip-flop. If an incorrect key value is added to the MUX, the incorrect flip-flop output is moved on to the next clock-edge stage. To maximise the overlap in the output cone of dependence of the main gates, a positioning approach similar to the one employed in the Key Interdependency technique is adopted.

Each MUX's non-select inputs are related to the Q and Q ⁇ outputs of the previous flip-flop. If an incorrect key value is added to the MUX, the incorrect flip-flop output is moved on to the next clock-edge stage. To maximise the overlap in the output cone of dependence of the main gates, a positioning approach similar to the one employed in the Key Interdependency technique is adopted.

Similar to TTLock, the logic cone is modified in Stripped-Functionality Logic Locking (SFLL-HD), and restore logic is used to restore the output of the modified cone when the right key value is added. However, unlike TTLock, for multiple PIPs, SFLL-HDh inverts the logic cone output, where the Hamming distance is h between each PIP and the k-bit secret key. The restore block tests if the Hamming distance is equal to h between the value on the logic cone input and the key added and, if this condition is met, inverts the output of the modified logic cone. As many as k,h input patterns can be covered by this approach.

Logic Decryption Strategies

Many groundbreaking decryption methods have been proposed against logic encryption during the past decade. We address the extraordinary properties of some of the more frequently cited methods of attack in this chapter.

The purpose of the Key Sensitization attack[12] is to decode the right key assignment by sensitising incorrect key bits to primary outputs for observation, one of the first oracle driven attacks. This is analogous to the ATPG technique of sensitising the primary output to a stuck-at-fault on a net. The output pattern from the encrypted circuit is compared with the output from an oracle circuit (acquired from the market) after seeking an appropriate input pattern to sensitise the necessary key bit to avoid an incorrect value on the key bit. In order to derive the right key assignment, all incorrect values are found iteratively.

Attack Resiliency of Encryption Schemes

The durability of the logic encryption schemes discussed in this paper against the attack strategies from the previous section is tested in this section. The resiliency review provided in this section is outlined.

EPIC (Random): EPIC is vulnerable to the main sensitization attack and all SAT-based attacks because of the random key gate location.

LCB: Although the insertion of key gates on networks with large fan-in and fan-out cones will thwart attacks based on graph equivalence, this device is prone to sensitization attacks because there is no requirement for interaction between the key gates. In comparison, the lack of hard SAT cases renders it prone to SAT-based attacks.

SLL: The sensitization attack is unable to spread an incorrect key value to a primary output without understanding the right assignment on all intervening key gates, because the key gate location technique in SLL ensures maximal interference between each pair of key gates. It is also argued that SAT-based attacks do not evaluate the in-memory key (AES input) by evaluating the value at the inputs of the key gates because of the existence of the AES block (AES output). It has been said, however, that AES blocks are highly visible and therefore vulnerable to elimination.

SFLL-HD: Similar to TTLock, deleting input patterns from the logic cone increases SFLL-resistance HD's to the removal attack since, after removing the restore logic, a corrupt logic cone is obtained. Increasing the number of PIPs, however, reduces resistance to SAT attacks, which can now remove more than one key per DIP. New Assault

Methods such as FALL and Gaussian exclusion were able to beat SFLL-HD without an oracle being used.

Cost Analysis - Area and Power

Typical IoT systems run under the limitation of restricted capital. During the design process to which the added logic encryption blocks must also conform, harsh areas and power restrictions are imposed on these machines. Wide blocks of logic coding are also unacceptable. In this chapter, we analyse the area and power overhead of the logic encryption techniques mentioned.

Conclusion

We also explored many logic encryption and decryption techniques in this work. To measure the cost incurred (area occupied and energy consumed) by these strategies, circuits encrypted by these schemes are used. Traditional methods of logic encryption are light with minimal overhead, but are vulnerable to SAT-based attacks. Huge overheads are imposed by efficient SAT-resilient systems and are thus unacceptable for applications where resources are limited. While sequential logic encryption strategies exhibit comparatively lower overhead costs, newly pro-posed decryption methods are still attackable. A new lightweight, robust logic encryption framework is therefore needed for IoT device protection applications.

Technique	Cost	Security
Random	A	D
LCB	A	D
SLL	A	C

Table 1: Encryption Scheme Rankings - Cost and Security

References

1. Alasad, Q., Bi, Y., Yuan, J.S.: E2LEMI: Energy-e_cient logic encryption usingmultiplexer insertion. Electronics 6(1), 16 (2017).
2. Amir, S., Shakya, B., Xu, X., Jin, Y., Bhunia, S., Tehranipoor, M., Forte, D.: Devel-opment and evaluation of hardware obfuscation benchmarks. Journal of Hardwareand Systems Security 2(2), (2018).
3. Chakraborty, R.S., Bhunia, S.: HARPOON: an obfuscation-based soc designmethodology for hardware protection. IEEE Transactions on Computer-Aided De-sign of Integrated Circuits and Systems 28(10), 1493{1502 (2009)
4. El Massad, M., Garg, S., Tripunitara, M.: Reverse engineering camouaged sequential circuits without scan access. In: 2017 IEEE/ACM International Conference onComputer-Aided Design (ICCAD). pp. 33{40. IEEE (2017).
5. Karmakar, R., Chatopadhyay, S., Kapur, R.: Encrypt Flip-Flop: A novel logic encryption technique for sequential circuits. arXiv preprint arXiv:1801.04961 (2018).
6. Karmakar, R., Kumar, H., Chattopadhyay, S.: On _nding suitable key-gate locations in logic encryption. In: 2018 IEEE International Symposium on Circuits andSystems (ISCAS). pp. 1{5. IEEE (2018).
7. Kasarabada, Y., Thulasi Raman, S.R., Vemuri, R.: Deep state encryption for sequential logic circuits. In: 2019 IEEE Computer Society Annual Symposium onVLSI (ISVLSI). pp. 338{343 (July 2019).
8. Lee, Y.W., Touba, N.A.: Improving logic obfuscation via logic cone analysis. In:2015 16th Latin-American Test Symposium (LATS), IEEE (2015)
9. Li, M., Shamsi, K., Meade, T., Zhao, Z., Yu, B., Jin, Y., Pan, D.Z.: Provably secure camouaging strategy for IC protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2017).
10. Narasimhan, S., Chakraborty, R.S., Chakraborty, S.: Hardware ip protection during evaluation using embedded sequential trojan. IEEE Design & Test of Computers 29(3), 70-79 (2012).
11. Rajendran, J., Pino, Y., Sinanoglu, O., Karri, R.: Security analysis of logic obfuscation. In: Proceedings of the 49th Annual Design Automation Conference. pp.83-89. ACM (2012).
12. Roshanisefat, S., Mardani Kamali, H., Sasan, A.: SRClock: Sat-resistant cycliclogic locking for protecting the hardware. In: Proceedings of the 2018 on GreatLakes Symposium on VLSI. pp. 153-158. ACM (2018).
13. Roy, J.A., Koushanfar, F., Markov, I.L.: Ending piracy of integrated circuits. Computer 43(10), pp-30-38 (2010).
14. Samimi, M.S., Aerabi, E., Kazemi, Z., Fazeli, M., Patooghy, A.: Hardware enlightening: Nowhere to hide your hardware trojans! In: 2016 IEEE 22nd InternationalSymposium on On-Line Testing and Robust System Design (IOLTS). pp. 251-256.IEEE (2016)
15. Shamsi, K., Li, M., Meade, T., Zhao, Z., Pan, D.Z., Jin, Y.: AppSAT: Approximately defecating integrated circuits. In: Hardware Oriented Security and Trust(HOST), 2017 IEEE International Symposium on. pp. 95-100. IEEE (2017).
16. Shamsi, K., Li, M., Meade, T., Zhao, Z., Pan, D.Z., Jin, Y.: Cyclic obfuscation forcreating SAT-irresolvable circuits. In: Proceedings of the on Great Lakes Symposium on VLSI 2017. pp. 173-178, ACM (2017)