Chapter 7
Masked Transient Effect Ring Oscillator Physical Unclonable Function Against Machine Learning Attacks

Sivasankari Narasimhan
Mepco Schlenk Engineering College, India

ABSTRACT

Many types of physical unclonable function (PUF) structures have been proposed in the last decade. The responses generated from the conventional PUF are vulnerable to attack. In this chapter, the transient effect of ring oscillator structure has been used. This works on two loops with complex loops containing NOT gates and NAND gates. Response prediction of these loops is a very difficult task for the adversary. Many machine learning algorithms may produce the responses with higher accuracies. This study provides new masked PUF architectures that are more secure and invulnerable to modeling attacks. Hence, in this chapter, masking-based configurability design on various PUF structures is introduced. This will be helpful for resource-constrained machines. For different sizes of challenge-response pair, machine learning techniques need to be changed, but prediction accuracy by the attacker should be low. By using this kind of masked PUF structure, 54.7% uniqueness can be obtained, and 97.5% reliability can be achieved. Machine learning accuracy is 70.7% with SVM and 63.67% accuracy in LR.

DOI: 10.4018/978-1-7998-9430-8.ch007

INTRODUCTION

The evolvement of the Machine Learning (ML) combined with advances in computational and storage capacities creates a lot of fruitful things. For example, ML-based algorithms altered the practice of disease findings, stock market analysis and cricket score prediction. But the ML techniques also capture the security domain, by monitoring bait machines, and extracting actionable information that in the past would have been impossible. Hence some vulnerabilities inherent with ML techniques are included with the security set-up. Currently, there are more advanced techniques to mitigate the ML attacks protecting the security set-ups. Such techniques may be smelled by hackers. Effort has been made to rectify the errors in security set-up. Several research sectors are developed for this, still this domain is in vulnerable position. These loopholes also create another focus for research and produce the new solutions for security threats. In this chapter, a unified hardware/ software approach is developed as a solution for security issues.

In security and privacy domain, maintaining confidentiality, integrity, and authentication are more essential. Hence, after 2000s, there is a proposal to introduce hardware security modules. Attacks on confidentiality attempt to expose the model structure or parameters (which may be highly valuable intellectual property) or the data used to train it, e.g., patient data, stock market data, continuously monitored information. But when a hardware entity is used, its unclonability nature avoids the data hacking problem and provides confidentiality to both communicating parties. On the other side, the main advantage of a PUF compared to the current classical cryptographic solutions is its compatibility with IoT devices with limited computational resources. Each node can be leveraged as an authentication mechanism to detect tamper. Several papers and works were developed in the last two decades. One simple category of PUF is shown in Figure 1.

Despite the several advantages that PUF brings for safety, there are several concerns and issues which need to be solved before it is incorporated in cyber physical devices. First, in PUF the devices are noisy (i.e., the device response is not the same in all environments). Due to temperature or fluctuations in it, the responses may get 5% deviations. It is quite natural that monitoring and maintenance of every PUF CRP pair is not a simple task. Second, the threshold level introduced for allowing the authorized user may also permit the wrong intruders. Third, when it is implemented in IoT devices, the centralized server may become a fraudulent one. The details from one device may be shifted to another device if they convince the server / trusted third party. Fourth, the details may be modelled by a clever intruder. This work focuses on how to reduce the fourth threat and find the solution.

Multi-Objective Materialized View Selection Using Improved Strength Pareto Evolutionary Algorithm

Jay Prakashand T. V. Vijay Kumar (2019). *International Journal of Artificial Intelligence and Machine Learning (pp. 1-21).*
www.irma-international.org/article/multi-objective-materialized-view-selection-using-improved-strength-pareto-evolutionary-algorithm/238125