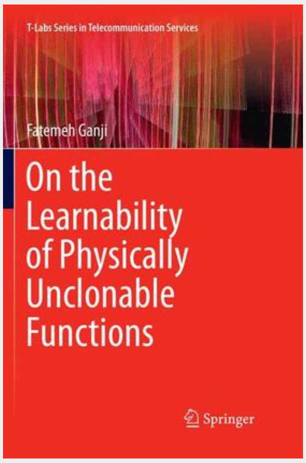
Ganji

On the Learnability of Physically Unclonable Functions

This book addresses the issue of Machine Learning (ML) attacks on Integrated Circuits through Physical Unclonable Functions (PUFs). It provides the mathematical proofs of the vulnerability of various PUF families, including Arbiter, XOR Arbiter, ring-oscillator, and bistable ring PUFs, to ML attacks. To achieve this goal, it develops a generic framework for the assessment of these PUFs based on two main approaches. First, with regard to the inherent physical characteristics, it establishes fit-for-purpose mathematical representations of the PUFs mentioned above, which adequately reflect the physical behavior of these primitives. To this end, notions and formalizations that are already familiar to the ML theory world are reintroduced in order to give a better understanding of why, how, and to what extent ML attacks against PUFs can be feasible in practice. Second, the book explores polynomial time ML algorithms, which can learn the PUFs under the appropriate representation. More importantly, in contrast to previous ML approaches, the framework presented here ensures not only the accuracy of the model mimicking the behavior of the PUF, but also the delivery of such a model. Besides off-the-shelf ML algorithms, the book applies a set of algorithms hailing from the field of property testing, which can help to evaluate the security of PUFs. They serve as a “toolbox”, from which PUF designers and manufacturers can choose the indicators most relevant for their requirements. Last but not least, on the basis of learning theory concepts, the book explicitly states that the PUF families cannot be considered as an ultimate solution to the problem of insecure ICs. As such, it provides essential insights into both academic research on and the design and manufacturing of PUFs.

This book addresses the issue of Machine Learning (ML) attacks on Integrated Circuits through Physical Unclonable Functions (PUFs). It provides the mathematical proofs of the vulnerability of various PUF families, including Arbiter, XOR Arbiter, ring-oscillator, and bistable ring PUFs, to ML attacks. To achieve this goal, it develops a generic framework for the assessment of these PUFs based on two main approaches. First, with regard to the inherent physical characteristics, it establishes fit-for-purpose mathematical representations of the PUFs mentioned above, which adequately reflect the physical behavior of these primitives. To this end, notions and formalizations that are already familiar to the ML theory world are reintroduced in order to give a better understanding of why, how, and to what extent ML attacks against PUFs can be feasible in practice. Second, the book explores polynomial time ML algorithms, which can learn the PUFs under the appropriate representation. More importantly, in contrast to previous ML approaches, the framework presented here ensures not only the accuracy of the model mimicking the behavior of the PUF, but also the delivery of such a model. Besides off-the-shelf ML algorithms, the book applies a set of algorithms hailing from the field of property testing, which can help to evaluate the security of PUFs. They serve as a “toolbox”, from which PUF designers and manufacturers can choose the indicators most relevant for their requirements. Last but not least, on the basis of learning theory concepts, the book explicitly states that the PUF families cannot be considered as an ultimate solution to the problem of insecure ICs. As such, it provides essential insights into both academic research on and the design and manufacturing of PUFs.


T-Labs Series in Telecommunication Services
Fatemeh Ganji
On the Learnability of Physically Unclonable Functions
Springer

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030095635
Medium: Buch
ISBN: 978-3-030-09563-5
Verlag: Springer International Publishing
Erscheinungstermin: 19.12.2018
Sprache(n): Englisch
Auflage: Softcover Nachdruck of the original 1. Auflage 2018
Serie: T-Labs Series in Telecommunication Services
Produktform: Kartoniert
Gewicht: 184 g
Seiten: 86
Format (B x H): 155 x 235 mm