Universitas Indonesia Library >> eBooks

On the Physical Security of Physically Unclonable Functions

Tajik, Shahin, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920529788&lokasi=lokal

---

Abstrak

This book investigates the susceptibility of intrinsic physically unclonable function (PUF) implementations on reconfigurable hardware to optical semi-invasive attacks from the chip backside. It explores different classes of optical attacks, particularly photonic emission analysis, laser fault injection, and optical contactless probing. By applying these techniques, the book demonstrates that the secrets generated by a PUF can be predicted, manipulated or directly probed without affecting the behavior of the PUF. It subsequently discusses the cost and feasibility of launching such attacks against the very latest hardware technologies in a real scenario. The author discusses why PUFs are not tamper-evident in their current configuration, and therefore, PUFs alone cannot raise the security level of key storage. The author then reviews the potential and already implemented countermeasures, which can remedy PUFs’ security-related shortcomings and make them resistant to optical side-channel and optical fault attacks. Lastly, by making selected modifications to the functionality of an existing PUF architecture, the book presents a prototype tamper-evident sensor for detecting optical contactless probing attempts.