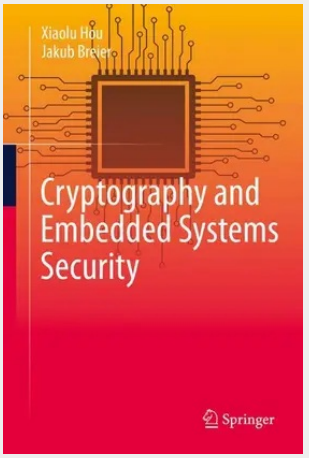
Hou / Breier

Cryptography and Embedded Systems Security

This textbook provides an all-in-one approach for learning about hardware security of cryptographic systems. It gives the necessary background on mathematics that is used for the construction of symmetric and public-key cryptosystems. Then, it introduces the most commonly used encryption algorithms that can be found on a wide variety of embedded devices to provide confidentiality, integrity, and authenticity of the messages/data. Finally, it provides theoretical and practical details on the two most common attack methods in hardware security – side-channel attacks, and fault injection attacks, together with the protection methods used against both.

This textbook provides an all-in-one approach for learning about hardware security of cryptographic systems. It gives the necessary background on mathematics that is used for the construction of symmetric and public-key cryptosystems. Then, it introduces the most commonly used encryption algorithms that can be found on a wide variety of embedded devices to provide confidentiality, integrity, and authenticity of the messages/data. Finally, it provides theoretical and practical details on the two most common attack methods in hardware security ¿ side-channel attacks, and fault injection attacks, together with the protection methods used against both.



106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783031622045
Medium: Buch
ISBN: 978-3-031-62204-5
Verlag: Springer
Erscheinungstermin: 09.08.2024
Sprache(n): Englisch
Auflage: 2024
Produktform: Gebunden
Gewicht: 951 g
Seiten: 489
Format (B x H): 160 x 241 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)