1. Record Nr. UNINA9910337635503321

Autore	Khalid Ayesha
Titolo	Domain Specific High-Level Synthesis for Cryptographic Workloads / / by Ayesha Khalid, Goutam Paul, Anupam Chattopadhyay
Pubbl/distr/stampa	Singapore : , : Springer Singapore : , : Imprint : Springer, , 2019
ISBN	981-10-1070-6
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (254 pages)
Collana	Computer Architecture and Design Methodologies, , 2367-3478
Disciplina	652.8
Soggetti	Electronic circuits Data encryption (Computer science) System safety Circuits and Systems Cryptology Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Background -- Dwarfs of Cryptography -- High Level Synthesis for Symmetric Key Cryptography -- Manual Optimizations for Efficient Designs -- Study of Flexibility -- Study of Scalability -- Efficient Cryptanalytic Hardware -- Conclusion and Future Work.
Sommario/riassunto	This book offers an in-depth study of the design and challenges addressed by a high-level synthesis tool targeting a specific class of cryptographic kernels, i.e. symmetric key cryptography. With the aid of detailed case studies, it also discusses optimization strategies that cannot be automatically undertaken by CRYKET (Cryptographic kernels toolkit. The dynamic nature of cryptography, where newer cryptographic functions and attacks frequently surface, means that such a tool can help cryptographers expedite the very large scale integration (VLSI) design cycle by rapidly exploring various design alternatives before reaching an optimal design option. Features include flexibility in cryptographic processors to support emerging cryptanalytic schemes; area-efficient multinational designs supporting various cryptographic functions; and design scalability on modern graphics processing units (GPUs). These case studies serve as a guide

to cryptographers exploring the design of efficient cryptographic implementations.