Domain specific high-level synthesis for cryptographic workloads

Khalid, Ayesha, author

Abstrak

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.