Cryptographic Engineering

EPFL, LAUSANNE, SWITZERLAND
JUNE 24-28, 2024

MONDAY, June 24

08:30 - 10:00 am	Introduction to Block Ciphers; DES and AES	C. Paar
10:30 - 12:00 am	Lightweight Block Ciphers for RFIDs	C. Paar
01:30 - 03:00 pm	Public-Key Cryptography: Algorithms and Protocols	Ç. K. Koç
03:30 - 05:00 pm	Integer Arithmetic Algorithms and Architectures	Ç. K. Koç

TUESDAY, June 25

08:30 - 10:00 am	Specialized Hardware for Secret-Key Algorithms	I. Verbauwhede
10:30 - 12:00 am	Introduction to PUFs (Physically Unclonable Functions)	I. Verbauwhede
01:30 - 03:00 pm	Finite Field Arithmetic Algorithms and Architectures	Ç. K. Koç
03:30 - 05:00 pm	Public-Key Cryptographic Hardware and Embedded Systems	Ç. K. Koç

WEDNESDAY, June 26

08:30 - 10:00 am	Introduction to Side-Channel Analysis	M. Joye
10:30 - 12:00 am	Block Ciphers: Attacks & Countermeasures	M. Joye
01:30 - 03:00 pm	Trusted Computing Architectures, SSL and IPSec	P. Rohatgi
03:30 - 05:00 pm	Electromagnetic Attacks, Countermeasures and Advanced Analysis Techniques	P. Rohatgi

THURSDAY, June 27

08:30 - 10:00 am	RSA/ECC: Attacks & Countermeasures	M. Joye
10:30 - 12:00 am	Fully Homomorphic Encryption	M. Joye
01:30 - 03:00 pm	Post-Quantum Cryptography Algorithms	F. Rodrìguez-Henrìquez
03:30 - 05:00 pm	Post-Quantum Cryptography Implementations	F. Rodrìguez-Henrìquez

FRIDAY, June 28

08:30 - 10:00 am	Random Number Generators for Cryptographic Applications	W. Schindler
10:30 - 12:00 am	Evaluation Criteria Non-Deterministic Random Number Generators	W. Schindler
01:30 - 03:00 pm	Random Number Generator Design Constraints and Challenges	V. Fischer