



Cryptographic Engineering

EPFL, LAUSANNE, SWITZERLAND

JUNE 13-17, 2022

MONDAY, June 13

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 14

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 15

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

THURSDAY, June 16

08:30 - 10:00 am	ECC - Side Channel Attacks & Countermeasures	M. Joye
10:30 - 12:00 am	Implementations of Fully Homomorphic Encryption Methods	Çetin K. Koç
01:30 - 03:00 pm	Side Channel Attacks to Block Ciphers: DES & AES	F.-X. Standaert
03:30 - 05:00 pm	Countermeasures for Block Ciphers	F.-X. Standaert

FRIDAY, June 17

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
