MEAD Education S.A.

Cryptographic Engineering

EPFL, LAUSANNE, SWITZERLAND
JUNE 18-22, 2018

MONDAY, June 18

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

TUESDAY, June 19

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

WEDNESDAY, June 20

08:30 - 10:00 am	Trusted Computing Architectures, SSL and IPSec	P. Rohatgi
10:30 - 12:00 pm	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 21

08:30 - 10:00 am	ECC - Side Channel Attacks & Countermeasures	M. Joye
10:30 – 12:00 pm	Cryptocurrencies and Bitcoin Architecture	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 22

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