

Cryptographic Engineering

**EPFL PREMISES, LAUSANNE, SWITZERLAND
AUGUST 30 - SEPTEMBER 3, 2010**

MONDAY, AUGUST 30

8:30 - 12:00 am	Efficient Software Implementations of DES and AES	Christof Paar
10:30 - 12:00 am	Lightweight Block Ciphers for RFIDs	Christof Paar
1:30 - 3:00 pm	Random Number Generators for Cryptographic Applications	Werner Schindler
3:30 - 5:00 pm	Evaluation Criteria Non-Deterministic Random Number Generators	Werner Schindler

TUESDAY, AUGUST 31

8:30 - 12:00 am	Specialized Hardware for Secret Key Algorithms, Part 1	Ingrid Verbauwhede
10:30 - 12:00 am	Specialized Hardware for Secret Key algorithms, Part 2	Ingrid Verbauwhede
1:30 - 3:00 pm	Introduction to Modular Arithmetic & Finite Fields for Cryptography	Cetin K. Koc
3:30 - 5:00 pm	Software & Hardware Realization of Modular Arithmetic and Finite Fields	Cetin K. Koc

WEDNESDAY, SEPTEMBER 1

8:30 - 12:00 am	Fundamentals and Algorithms for Public-Key Cryptography	Cetin K. Koc
10:30 - 12:00 am	RSA, Diffie-Hellman, and Elliptic Curve Cryptography and Discrete Logarithms	Cetin K. Koc
1:30 - 3:00 pm	Pairing-Based Cryptograph	Colin Walter
3:30 - 5:00 pm	Modular Arithmetic and Side Channels	Colin Walter

THURSDAY, SEPTEMBER 2

8:30 - 12:00 am	Side-Channel Attacks on Cryptographic Tokens	Marc Joye
10:30 - 12:00 am	Countermeasures for Preventing Side-Channel Attacks	Marc Joye
1:30 - 3:00 pm	Electromagnetic Attacks and Countermeasures	Pankaj Rohatgi
3:30 - 5:00 pm	Improved Techniques for Side-Channel Analysis	Pankaj Rohatgi

FRIDAY, SEPTEMBER 3

8:30 - 12:00 am	Trusted Computing Architectures	Pankaj Rohatgi
10:30 - 12:00 am	Efficient Implementations of Symmetric Cryptographic Primitives in Reconfigurable Hardware Devices	François-X. Standaert
1:30 - 3:00 pm	Secure Implementations of Symmetric Cryptographic Primitives in Reconfigurable Hardware Devices Generators	François-X. Standaert
