CRYPTOGRAPHY ENGINEERING

ON-LINE CLASS

SEPTEMBER 7 - 18, 2020

WEEK 1		**SEPT 7-11**	10 Modules (1:30hr each), 2 Modules per day		
WEEK 2		**SEPT 14-18**	10 Modules (1:30hr each), 2 Modules per day		
		Central European Time	Eastern Standard Time	Pacific Standard Time	Singapore Time Zone
DAILY		**CET (Lausanne)**	**EST (New York)**	**PST (California)**	**SGT (Singapore)**
Module 1		3:00-4:30 pm	9:00-10:30 am	6:00-7:30 am	9:00-10:30 pm
Module 2		5:00-6:30 pm	11:00 am -12:30 pm	8:00-9:30 am	11:00 pm - 00:30+ am
WEEK 1	Module				
Monday, Sept 7	1	Introduction to Block Ciphers; DES and AES			Christof Paar
	2	Lightweight Block Ciphers for RFIDs			Christof Paar
Tuesday, Sept 8	1	Specialized Hardware for Secret-Key Algorithms			Ingrid Verbauwhede
	2	Introduction to PUFs (Physically Unclonable Functions)			Ingrid Verbauwhede
Wednesday, Sept 9	1	Integer Arithmetic Algorithms and Architectures			Cetin Koç
	2	Finite Field Arithmetic Algorithms and Architectures			Cetin Koç
Thursday, Sept 10	1	Public-Key Cryptography: Algorithms and Protocols			Cetin Koç
	2	Public-Key Cryptographic Hardware and Embedded Systems			Cetin Koç
Friday, Sept 11	1	Trusted Computing Architectures, SSL and IPSec			Pankaj Rohatgi
	2	Introduction to Side-Channel Analysis			Marc Joye
WEEK 2					
Monday, Sept 14	1	RSA - Side Channel Attacks & Countermeasures			Marc Joye
	2	Electromagnetic Attacks, Countermeasures and Advanced Analysis Techniques			Pankaj Rohatgi
Tuesday, Sept 15	1	ECC - Side Channel Attacks & Countermeasures			Marc Joye
	2	Cryptographic Engineering in a Post-Quantum World			Cetin Koç
Wednesday, Sept 16	1	Side Channel Attacks to Block Ciphers: DES & AES			François-Xavier Standaert
	2	Countermeasures for Block Ciphers			François-Xavier Standaert
Thursday, Sept 17	1	Random Number Generators for Cryptographic Applications			Werner Schindler
	2	Evaluation Criteria Non-Deterministic Random Number Generators			Werner Schindler
Friday, Sept 18	1	Random Number Generator Design Constraints and Challenges			Viktor Fischer