CRYPTOEXPERTS
WE INNOVATE TO SECURE YOUR BUSINESS

WISE 2015 (Workshop on Implementation Security and Evaluation)

Program

9:00 - 9:10	**Reception**
9:10 - 11:00	**Session 1: Evaluation methodology**
	9:10 - Emmanuel Prouff (ANSSI) - *Security assessment for designers and evaluators*
	10:05 - Tobias Schneider (Ruhr-University Bochum) - *Leakage assessment methodology - a clear roadmap for side-channel evaluations*
11:00 - 11:15	**Coffee break**
11:15 - 12:45	**Session 2: Certification & standardization**
	11:15 - Hugues Thiebeauld (eShard) - *Walking through the attack rating methodology to manage the trust*
	12:10 - Sylvain Guilley (Telecom ParisTech & SecureIC) - *State-of-the-art of international standardisation of side-channel analysis test methodologies and calibration of acquisition tools*
12:45 - 2:00	**Lunch**
2:00 - 3:50	**Session 3: Profiling & automated proofs**
	2:00 - Elisabeth Oswald (University of Bristol) - *Making the most of leakage*
	2:55 - François Dupressoir (IMDEA) - *Computer-aided cryptographic proofs for low-level implementations*
3:50 - 4:00	**Coffee break**
4:00 - 5:30	**Discussion panel: What shall the future hold?**
	Hosted by Pascal Paillier (CryptoExperts) Sylvain Guilley (Telecom ParisTech & SecureIC) Elisabeth Oswald (University of Bristol) Emmanuel Prouff (ANSSI) François-Xavier Standaert (UCL) Hugues Thiebeauld (eShard)