



**Introduction to Side Channel Analysis (1-day)**  
**September 14, 2010**

*09:00 – 9:15*

**Introduction: Welcome & Overview of Workshop (15 min)**

*09:15 – 10:30*

**Session 1: Simple Power Analysis**

*09:15 - 10:00* Introduction to SPA (45 min)

*10:00 - 10:15* SPA waveform analysis exercise (15 min)

*10:15 - 10:30* Interactive PIN verify attack (15 min)

*10:30 – 10:45*

**Break**

*10:45 – 12:00*

**SPA Modular Exponentiation Exercise (75 min)**

*12:00 – 12:45*

**Lunch**

*12:45 – 14:15*

**Session 2: Differential Power Analysis**

*12:45 – 13:30* Introduction to DPA (45 min)

*13:30 – 14:15* Demo: DPA attack on FPGA (45 min)

*14:15 – 16:15*

**Session 3: Countermeasures & Certification Issues**

*14:15 – 15:30* Preventing DPA: Countermeasures (75 min)

*15:30 – 16:15* Testing and Certification (45 min)

*16:15 – 16:45*

**Advanced Topics in DPA (30 min)**

*16:45 – 17:00*

**Q&A/Wrap-up**