

# Cryptography Research ECC Power Analysis Workshop

## Preliminary Agenda

**Monday, March 10, 2008**

**Day 1: Introduction to Power Analysis and DPA Workstation™ Tools**

*13:00 – 14:00*

**Lesson: Overview of CRI and Power Analysis (60 min)**

Introduction to Power Analysis attacks, Simple Power Analysis (SPA), Differential Power Analysis (DPA) and the DPA Workstation

*14:15 - 15:00*

**Lesson: Introduction to Simple Power Analysis (45 min)**

Introduction to simple power analysis (SPA) methods and attacks

*15:15 - 17:15*

**Tutorial: Introduction to SHOW.EXE and SPA (90 min)**

Introduction to SHOW.EXE, a DPA Workstation program for examining and interpreting data traces.

**Exercise: Introduction to SHOW.EXE and SPA: Using SHOW to perform SPA (30 min)**

Students will use SHOW.EXE to recover an RSA exponent using SPA.

*17:15 - 17:45*

**DPA Demonstration (30 min)**

Live demonstration of the DPA Workstation

*17:45 - 18:00*

**Discussion and Review (15 min)**

**Day 1 of the training is for those attendees who have not previously attended a general DPA Workstation™ training with CRI.**

# Tuesday, March 11, 2008

## Day 2

**09:00 - 9:15**

**Welcome / Introductions (15 min)**

**09:15 - 10:30**

**Lesson: Overview of ECC (75 min)**

Overview of the use of Elliptic Curves in Cryptography.

- Mathematical preliminaries
- The case for using Elliptic Curves
- Security margins and key sizes
- Standardization efforts

**10:30 - 11:00**

**Demonstration: Capturing and analyzing ECC and Simple Power Analysis (30 min)**

Demonstration of simple power analysis using the CRI DPA Workstation to evaluate a smart card performing ECC signature using the Nyberg-Reupel algorithm. The following topics will be covered:

- The DPA Workstation (smart cards, ECC algorithms, SPA)
- The steps of the Nyberg-Reupel signature algorithm
- Single-trace analysis by interpretation

**11:15 - 12:15**

**Lesson: Introduction to ECC Algorithms and Simple Power Analysis (60 min)**

Discussion of different of the EC algorithms EC-DSA, EC-NR, EC-DH, and EC-MQV. (Note: these are the algorithms supported by IEEE P1363.) Emphasis is on the ways that secret data is manipulated, the leaks that may be present, and attacks that exploit such leaks. The main attack strategies will be introduced:

- Attacks on modular arithmetic (EC-DSA / EC-NR, EC-MQV)
- SPA attacks on the curve multiplication step. Recovery of the full scalar breaks all algorithms (EC-DSA / EC-NR / EC-DH / EC-MVQ), partial recovery of the scalar breaks some (EC-DSA / EC-NR).
- LLL and partial nonce recovery attacks (EC-DSA / EC-NR)
- Algorithmic attacks on weak PRNG (EC-DSA / EC-NR)

**12:15 - 13:15**

**Lunch (60 min)**

**13:15 - 16:00**

**Tutorial: The MULT\_SORT attack on EC-NR (165 min)**

This tutorial will work through the process of breaking the example smart card as it performs signatures using the NR algorithm.

- Into to MULT\_SORT.EXE
- Attack on EC data set, collected previously
- Finally we'll need a discussion of harmonic peaks and how to determine which byte is which in the key.

**16:15 - 17:00**

**Demonstration: The BUMP\_SORT attack on EC-NR (45 min)**

This demonstration will attack the reduction step of the EC-NR algorithm to recover the key in a different way from the MULT\_SORT tutorial

# Wednesday, March 12, 2008

## Day 3

**9:00 -10:00**

**Lecture: Implementing Elliptic Curve Multiplication (60 min)**

This presentation will describe algorithms used for computing elliptic curve multiplication. A simple method will be presented first, followed by descriptions of optimizations and caching strategies. The presentation will build up to a description of the complicated algorithm deployed on the example card.

- Simple Double-and-Add
- Sliding Window algorithms
- Basic Lim-Lee algorithms with pre-computed points
- Extensions to simple Lim-Lee

**10:15 - 11:45**

**Tutorial: SPA attack on EC-NR (90 min)**

In this tutorial, students will use DPAWS software to implement partial nonce recovery attacks using the leak described in the preceding lecture

- Identifying the appropriate SPA leak.
- Collecting enough SPA data to do the analysis (10-20 bits per trace).

**11:45 - 12:45**

**Lunch (60 min)**

**12:45 -13:45**

**Lecture: LLL and Lattice based analysis (60 min)**

This presentation will introduce the LLL algorithm and Babai's algorithm and discuss their application to analysis of elliptic curve cryptosystems.

**14:00 - 15:30**

**Tutorial: Partial-Nonce recovery attacks on EC-NR (90 min)**

In this tutorial, students will use DPAWS software to implement partial nonce recovery attacks, including the steps of:

- Performing the analysis to recover the key using DPAWS/LLL software and Babai's algorithm
- Redoing the attack using just 6 bits per nonce.

**15:45 - 17:00**

**Discussion: Additional topics (75 min)**

In this time, students and instructors will have the opportunity to discuss some topics relating to ECC in greater depth:

- Implementing Elliptic Curve primitives (adding, doubling, halving)
- Reverse Engineering an unknown implementation
- Countermeasures