Workshop IV: Special purpose hardware for cryptography: Attacks and Applications

Monday December 4, 2006

8:00–9:30 *Check-In/Light Breakfast (Hosted by IPAM)*

9:30–9:45 *Welcome and Opening Remarks*

9:45–10:30 **Keith Mayes** (Royal Holloway and Bedford New College)
Smart Card Platform Fingerprinting

10:30–10:45 *Break*

10:45–11:15 **Ari Juels** (RSA Laboratories)
The Quirks and Conundrums of RFID Security

11:15–12:00 **Christof Paar** (Ruhr-Universität Bochum)
Light-Weight Cryptography for Ubiquitous Computing

12:00–1:30 *Lunch (on your own)*

1:30–2:15 **Bart Preneel** (Katholieke Universiteit Leuven)

2:15–2:30 *Break*

2:30–3:15 **Marc Joye** (Thomson R&D France)
Elliptic Curve Cryptosystems in the Presence of Faults

3:15–4:00 **Chien Siang Yu** (Singapore Ministry of Home Affairs)
Securing the Intelligent Nation

4:00–4:45 **Shenglin Yang** (Beijing (Peking) University)

5:00–6:30 *Wine/Cheese Reception (Hosted by IPAM)*

Tuesday December 5, 2006

8:00–9:45 *Continental Breakfast*

9:45–10:30 **Luca Breveglieri** (Politecnico di Milano)
Parallel Hardware Architectures for the Computation of the Tate Pairing

10:30–10:45 *Break*

(Tuesday schedule continued on next page)

(Tuesday schedule continued from previous page)

10:45–11:30 **Sharon Goldberg** (Princeton University)
Encryption at the Speed of Light? Cryptanalysis of an optical CDMA encryption scheme

11:30–12:15 **Ingrid Verbauwhede** (Katholieke Universiteit Leuven)
Security for embedded devices

12:15–1:30 *Lunch (on your own)*

1:30–2:15 **Cetin Koc** (Oregon State University)
Spectral Modular Arithmetic

2:15–2:30 *Break*

2:30–3:15 **Erkay Savas** (Sabanci University)
Unified Architectures for Efficient and Compact Crypto-Processing

3:15–4:00 **M. Hasan** (University of Waterloo)
A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields

Wednesday December 6, 2006

8:00–9:45 *Continental Breakfast*

9:45–10:30 **Martin Simka** (Sentivision / Technical University of Košice)
Random numbers in cryptography

10:30–10:45 *Break*

10:45–11:30 **Berk Sunar** (Worcester Polytechnic Institute)
State of the Art in Cryptographic True Random Number Generation

11:30–12:15 **Jan Pelzl** (Ruhr-Universität Bochum)
Cryptanalysis with a Cost-Optimized FPGA Cluster

12:15–1:30 *Lunch (on your own)*

1:30–2:15 **Willi Geiselmann** (Universität Fridericiana (TH) Karlsruhe)
Another Attempt To Sieve With Small Chips — Part I: Collecting Relations

2:15–2:30 *Break*

2:30–3:15 **Rainer Steinwandt** (Florida Atlantic University)
Another Attempt To Sieve With Small Chips—Part II: Norm Factorization

3:15–4:00 **François-Xavier Standaert** (Laboratoire de microélectronique de l'Université catholique de Louvain)
A Formal Practice-Oriented Model for the Analysis of Side-Channel Attacks (or How to Evaluate Side-Channel Attacks?)

4:00–4:45 **Israel Koren** (University of Massachusetts Amherst)
Using Error Detection Codes to detect fault attacks on symmetric key ciphers

Thursday December 7, 2006

8:00–9:45 *Continental Breakfast*

9:45–10:30 **Christine Priplata** (Edizone)
Hardware Cracker for Integer Factorization - Designs, Costs and Feasibility

10:30–10:45 *Break*

10:45–11:30 **Christine Priplata** (Edizone)
Sieving Hardware for Factoring and ECM Support

11:30–12:15 **Thorsten Kleinjung** (Rheinische Friedrich-Wilhelms-Universität Bonn)
Estimates for factoring 1024-bit integers

12:15–1:30 *Lunch (on your own)*

1:30–2:15 **Ricardo Dahab** (State University of Campinas (UNICAMP))
A few ECC arithmetic results for hardware and software implementations

2:15–2:30 *Break*

2:30–3:15 **Amit Sahai** (UCLA)
Private Circuits: Can you keep a secret while your brain is being tampered with?

Friday December 8, 2006

8:00–9:45 *Continental Breakfast*

9:45–10:30 **Kris Gaj** (George Mason University)
Implementation of the rho, p-1 and the Elliptic Curve Methods of Factoring in Reconfigurable Hardware

10:30–10:45 *Break*

10:45–11:30 **Elisabeth Oswald** (University of Bristol)
Power Analysis Attacks

11:30–12:15 **Sergei Skorobogatov** (University of Cambridge)
Semi-Invasive Extension to Physical Attacks