FDTC 2006 Final Programme - Tuesday 10 October 2006

08:00-08:40. Registration + Coffee (Continental Breakfast)

08:40-08:50. Opening remarks

First Invited Talk

8:50-9:20. Fault attacks, an intuitive approach
Raphael Bauduin

Session I. Public key fault attacks
Chair Luca Breveglieri

09:25-09:45. Is it wise to publish your Public RSA Keys?
Shay Gueron, Jean-Pierre Seifert

09:45-10:05. Attacking right-to-left Modular Exponentiation with Timely Random Faults
Michele Boreale

10:05-10:25. Java Type Confusion and Fault Attacks
Olli Vertanen

10:25-11:10. Coffee break

Session II. Secret key fault attacks
Chair Shay Gueron

11:10-11:30. A Fault Attack Against the FOX Cipher Family
Luca Breveglieri, Israel Koren, Paolo Maistri

11:30-11:50. Fault Based Collision Attacks on AES
Johannes Blömer, Volker Krummel

11:50-12:10. Collision Fault Analysis of DPA-Resistant Algorithms
Frederic Amiel, Christophe Clavier, Michael Tunstall

12:10-14:00. Lunch

Second Invited Talk

14:00-14:30. Safe design methodologies against fault attacks
Bruno Robisson

Session III. Secret key fault protection
Chair Akashi Satoh

14:35-14:55. An Easily Testable and Reconfigurable Pipeline for Symmetric Block Ciphers
Myeong-Hyeon Lee, Yoon-Hwa Choi

14:55-15:15. Case Study of a Fault Attack on Asynchronous DES Crypto-Processors
Yannick Monnet, Marc Renaudin, Régis Leveugle, Christophe Clavier, Pascal Moitrel

15:15-15:50. Coffee break

Session IV. Public key fault attack protection
Chair Guido Bertoni

15:55-16:15. Wagner's Attack on a Secure CRT-RSA Algorithm Reconsidered
Johannes Blömer, Martin Otto

16:15-16:35. Blinded Fault Resistant Exponentiation
Guillaume Fumaroli, David Vigilant

16:35-16:55. Non-linear Residue Codes for Robust Public-Key Arithmetic
Gunnar Gaubatz, Mark G. Karpovsky, Berk Sunar

16:55-17:10. Closing remarks