Master Security, Cryptography and Coding of Information Systems

-----

10th Birthday !!!

Alexandre BERZATI (SCCI 2007)
Grenoble, 12/09/11

My career at a glance

- 2007: Master Thesis
  - Morpho (previously SAGEM Sécurité)
  - *« Side-Channel Attacks on Cryptographic Implementations »*
- 2007 – 2010: PhD Thesis
  - CEA-Leti CESTI | UVSQ
  - *« Cryptographic Analysis of Algorithm Corruptions »*
- 2010 – ????
  - INVIA – Secure Semiconductor IP
  - Embedded Software Engineer

2007 – 2010 | PhD Thesis

- Introduction
  - Title: *« Cryptographic Analysis of Algorithm Corruptions »*
  - Advisors: Cécile Dumas (CEA) and Louis Goubin (UVSQ)
- Context
  - CESTI: Centre d'Evaluation de la Sécurité des Systèmes d'Information
  - Part of certification for secured products
  - Resistance to Fault Attack is evaluated
- Motivations
  - Up-to-date knowledge on Fault Attacks
  - Develop new attacks

2008 – Fault Attacks on RSA Pub. Keys

- Main Result: CHES 2008 (Washington DC)

2009 – Fault Attacks on Stream Ciphers

- Main Result: Indocrypt 2009 (New Delhi)

2010 – Fault Attacks on Secured RSA

- Main Result: CHES 2010 (Santa Barbara)

2010 – ???? | About INVIA

- Founded in 2006 by smart card industry veterans
  - Independent, private company headquartered in France
- Strong expertise in secure platforms
  - R&D headcount : 18 including 6 PhD
  - System level expertise : architecture, hardware, firmware, software
  - Strong Patent Portfolio
- Silicon proven IPs with volume production track record
  - From 350 nm to 65 nm
- End Markets
  - Military Communications, SIM, PayTV, EMV Payment, ID and Access, Automotive

Product Portfolio

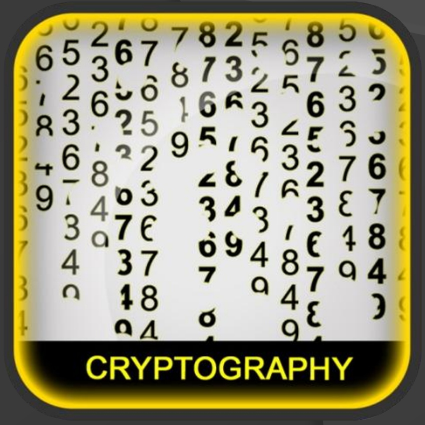
Triple DES
AES
Modular Exp.
Embedded Software Library

Glitch Detector
Active Shield
Re-routing Detector
Temperature Sensor

InterChip USB
ISO 7816-3
ISO 14443

True RNG
Voltage Regulator
Clock Management

Crypto engines IP

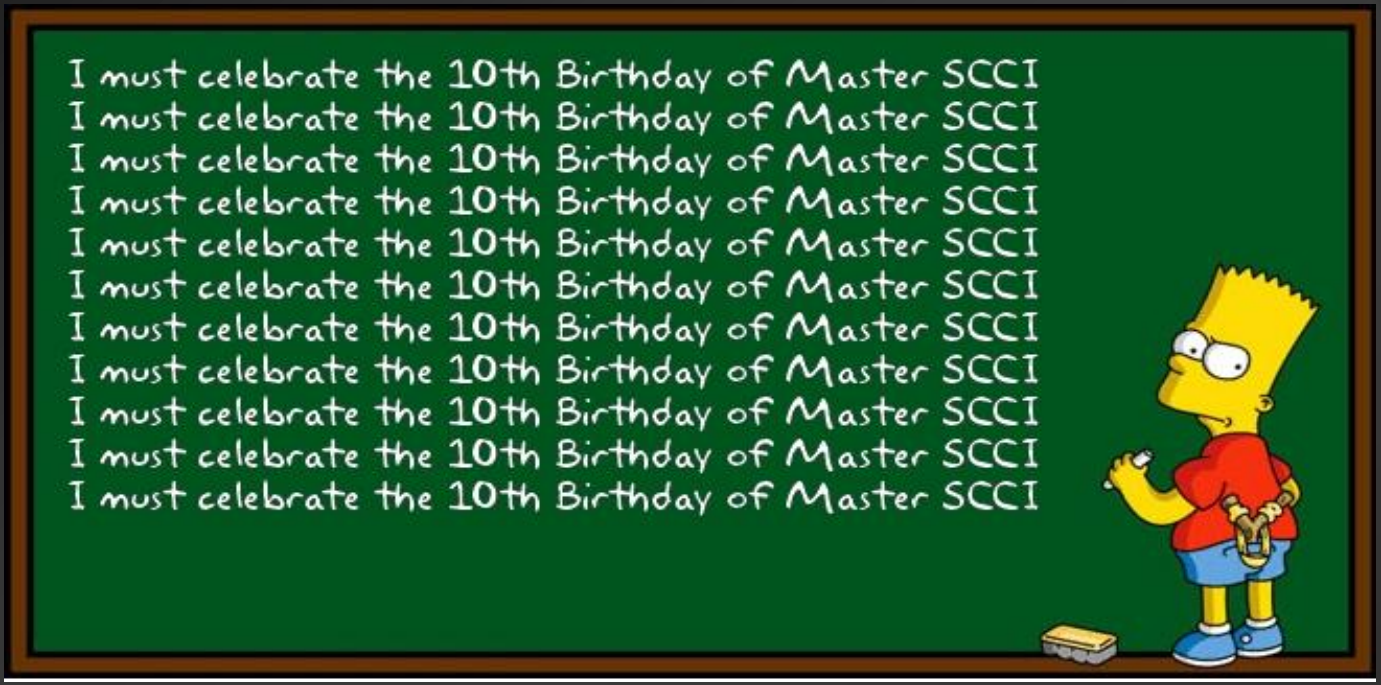


- Digital IP
  - RTL source code
- 3DES / AES / RSA / Elliptic Curves
- AMBA APB Interface
- Very Low Area
  - DES : 2700 gates – 305 Mb/s @ 300 MHz (90 nm)
  - AES 256 bits : 6110 gates –685 Mb/s @ 300 MHz (90 nm)
  - RSA 2048 bit : 10 000 gates – 5 ops/s @ 100 MHz (65 nm)
- Low power
  - Derived from smart card implementations
- Protected against transient fault injection
  - 10% area increase

Embedded Software library

- Libraries for AES and RSA
- Secured Bootloader/Embedded Systems
- Delivered in assembly source code or source code binary
- Optimized for embedded processors
  - ARM CORTEX M3
  - LEON 3 (SPARC)
- Protected against side channel attack and fault-injection
- Code re-routing protections
- Interface with hardware accelerated AES or Modular Exponentiation for RSA

Thank you ;-)



I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI
I must celebrate the 10th Birthday of Master SCCI

INVIA
Arteparc – Bat.D
Route de la Cote d'Azur
13590 Meyreuil
alexandre.berzati@invia.fr
Jobs: jean-roch.coulon@invia.fr