Tiempo

Charles GUILLEMET

Hardware Design Engineer

10 years Master SCCI

charles.guillemet@tiempo-ic.com

Plan

- Studies
- Tiempo presentation
- Internship: power attacks on DES
- Countermeasures design
- High speed AES implementation
- Cryptosystem Design

Studies

Master I Mathematics (2003-2007)
Montpellier

ENSIMAG (2008-2009)
UJF Master SCCI (2009)
Grenoble

Internship at Tiempo

TIEMPO overview

- Tiempo offers powerful asynchronous core IPs supported by an innovative design and synthesis flow for low power embedded electronics and secured devices

- Tiempo asynchronous design technology:
  - Is fully clockless (i.e. no local clocks)
  - Is delay insensitive = functionally correct regardless of any delay in gates and wires (no delay assumption)
  - Allow designs with both ultra-low power and high performances
  - Can be described with high-level models, in standard language

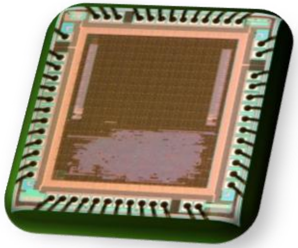
Tiempo

About Tiempo

- Created in 2007
- 21 people
- Located Near Grenoble, France

TIEMPO offers

- **Tiempo IP portfolio:**

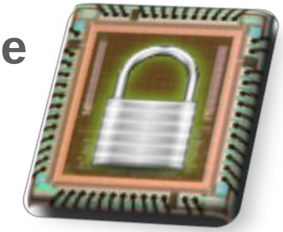


TAM16: ultra-low power 16-bit microcontroller

- < 50µA/MIPS
- fast wake-up
- Silicon Proved

TAK5: ultra-low power crypto-processor family

- **TDES**: DES/3DES IP core
- **TAES**: AES IP core
- **TPKA**: RSA/ECC co-processor IP



- **Target Applications:**

Contactless and other electronic transactions

Ultra-low power embedded electronics

Mobile consumer electronics

Automotive

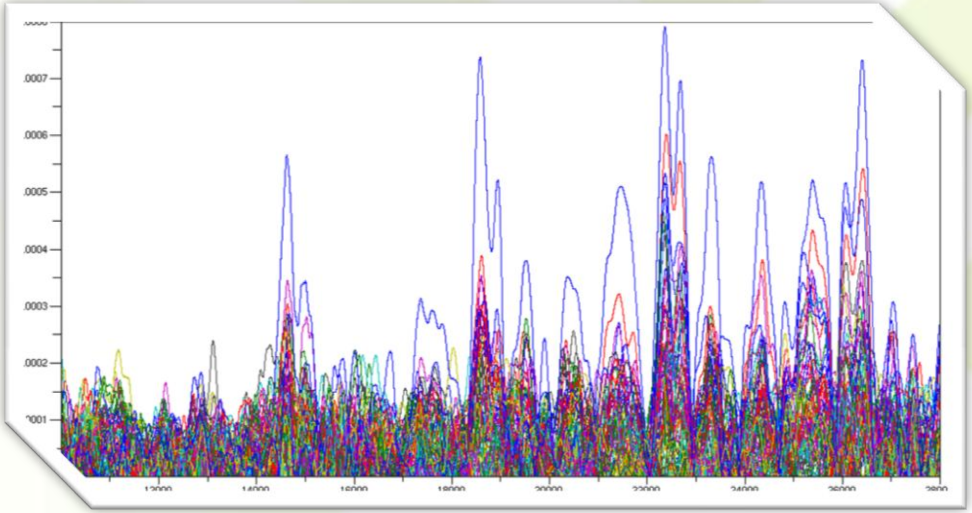
Aerospace

Internship - 2008

Security evaluation of asynchronous DES chips

Implementation of power attacks (DPA/CPA)

Vulnerabilities discovered



Countermeasures

Conception and implementation of innovative countermeasures against power & faults attacks

- AES crypto-processor
- DES crypto-processor
- TEAM16S cryptosystems

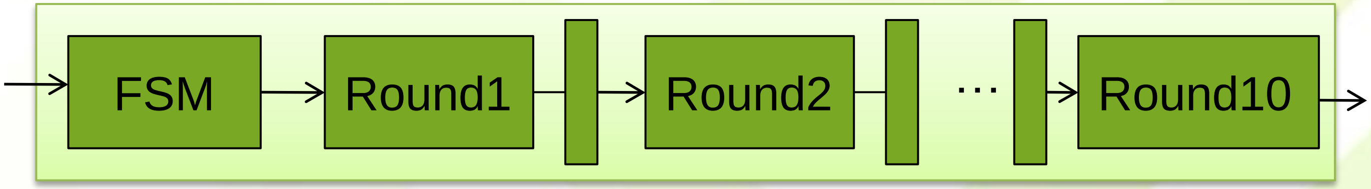
- Mathematics countermeasures (kind of masking)
- Hardware Countermeasures (delays insertion)

DES has been evaluated by external lab

=> did not succeed to attack DES with countermeasures

High speed AES

Evaluation of Tiempo asynchronous technology
Conception and implementation of an
High speed AES-GCM encryptor



Techno: 65nm GP
Throughput: 40 Gbit/s
Latency: ~12ns

Cryptosystem for Smartcard application

Conception of a fully asynchronous cryptosystem
Including AES/DES/PKA crypto IPs

In Charge of
- Validation
- Security Specification
- Crypto libs
- SW drivers

Contactless and other electronic transactions

Thanks for your attention

Questions ?