QDI Circuits to Improve Smartcard Security

* Introduction
This presentation focuses on DPA attack sensitivity of an 8 bit QDI asynchronous microprocessor

* Objective
Our principal objective is to prove that quasi delay insensitive asynchronous logic can be a counter-measure against DPA attacks

The MICA 8-bit Micro-controller
* Technology: CMOS 0.25 µm
* Inputs/Outputs: 118 PADS
* Power Supply: 2.5 V
* Speed: 25

How...?

* DPA attack that allow to extract key information by statistical analysis of power consumption between the run of different data with the same cryptographic key. For implementing DPA attacks, we developed a specific board with the strict minimum of passive elements
**Results**

- Number of points: 100000
- 10000 computations

*Correlations*

- If curve1 and curve2 show an appreciable difference (not noise), we consider it is not good.
- If curve1 and curve2 do not show any substantial difference, we consider it is good.

**Results & Conclusion**

The analysis reveals that the processor resists to standard DPA attacks.

**Conclusion**

We showed on this result that QDI technology is a good candidate for resisting against DPA attacks using state-of-the-art power analysis equipment. QDI circuits is definitely a good solution to improve chip and cryptographic.