Tiempo

TAES: Asynchronous AES IP

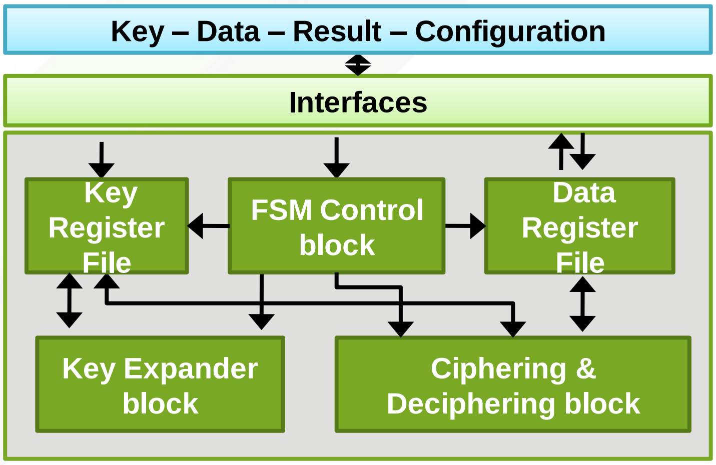
Version 2.3 - Nov 2012

Tiempo clockless crypto-processor core - TAES - is able to execute the standard AES encryption and decryption algorithms. This IP is designed in Tiempo fully asynchronous and delay insensitive technology that allows ultra-low power consumption, ultra-low noise, ultra-low EMI, as well as robustness against attacks by power analysis & fault injection.

Applications

Targeted applications are chips for smart cards (with or without contact), RFID tags, sensor networks, systems embedding NFC technology and other secured applications

TAES Block Diagram



Key benefits

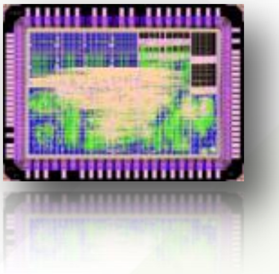
- Ultra low power consumption: low energy, low current peaks
- Ultra low electromagnetic emission (EMI/EMC)
- High speed under low/variable power (independently from system clock)
- High robustness against any PVT (process, voltage, temperature) variation
- High robustness against attacks by power analysis and fault injections (for secured applications)

Key features

- Executes AES standard encryption and decryption algorithms
  - Data: 128 bits
  - Key: 128, 192 or 256 bits
  - ECB mode supported
- Fully asynchronous (no clock) and delay insensitive (correctness of encryption / decryption is guaranteed regardless of any actual delay in internal gates and wires)
- Available as Verilog netlist ready for P&R (silicon-proven netlist) or as a GDSII hard-IP block (verified layout description) [1]
- Option: IP *secured* against attacks by power analysis and fault injection

[1] Please contact Tiempo for available libraries and technologies

Tiempo TESIC chip



Silicon Proven

Designed and processed on TSMC CMOS 130 nm LP technology.

Characteristics

Figures below are electrical measurements made on Tiempo prototype chip TESIC fabricated on a TSCM130LP 1.5V process. Figures are valid for the *secured* version of the IP with a 128-bit key.
These figures illustrate one instance of the IP and can be tuned to our customer needs (reduced power consumption or increased performance).

Supply voltage	1.0V	1.5V
Encryption speed (µs)	15.40	5.60
Average current (mA)	0.34	1.25
Energy (nJ)	5.5	10.4
Decryption speed (µs)	22.52	8.30
Average current (mA)	0.31	1.17
Energy (nJ)	9.9	19.6