



## TDES: Asynchronous DES IP

Version 2.1 - Sept 2011

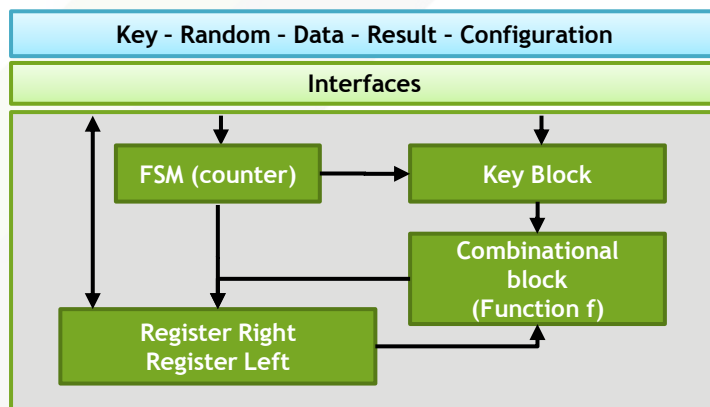
Tiempo clockless crypto-processor core - DES - is able to execute the standard encryption and decryption algorithms DES, DES-1, 3DES and 3DES-1. This IP is designed in Tiempo fully asynchronous and delay insensitive technology that allows ultra-low power consumption, ultra-low noise, ultra-low EMI, as 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



### TDES Block Diagram



### Key benefits

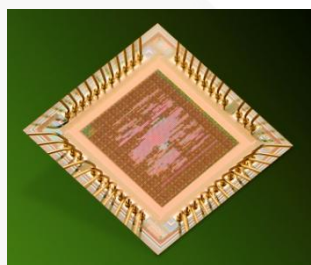
- Ultra low power consumption: low energy, low current peaks
- Ultra low electromagnetic emission (EMI/EMC)
- High speed (independent from any system clock)
- High robustness against any PVT (process, voltage, temperature) variation
- High robustness against attacks by power analysis and fault injections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

## Key features

- Executes standard encryption and decryption algorithms DES, DES<sup>-1</sup>, 3DES and 3DES<sup>-1</sup>
  - 64 Bits key and data
  - Triple DES supports two or three keys
  - ECB and CBC modes available
- 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<sup>1</sup> ready for P&R (silicon-proven netlist)
  - As an option: Verilog netlist<sup>1</sup> secured against attacks by power analysis and fault injection
  - As an option: Verilog netlist<sup>1</sup> strengthened for ultra low noise, ultra low EMI

<sup>1</sup> Please contact Tiempo for available libraries and technologies

Tiempo DES<sup>4</sup> chip



## Silicon Proven

Designed and processed in a general-purpose CMOS 130 nm technology, Tiempo DES<sup>4</sup> chip instantiates TDES Core IP.

## Characteristics

Figures below are based on electrical simulations on TSCM130LP 1.5V process after Place & Route. Simulations are run on the secured version of the IP.

These figures illustrate one instance of the IP and can be tuned to our customer needs (reduced power consumption or increased performance).

Supply voltage range	1.0V	1.5V
Encryption speed ( $\mu$ s)	2.03	0.71
Average current (mA)	0.31	1.38
Energy (nJ)	0.63	1.46

