



# Asynchronous DES Core IP

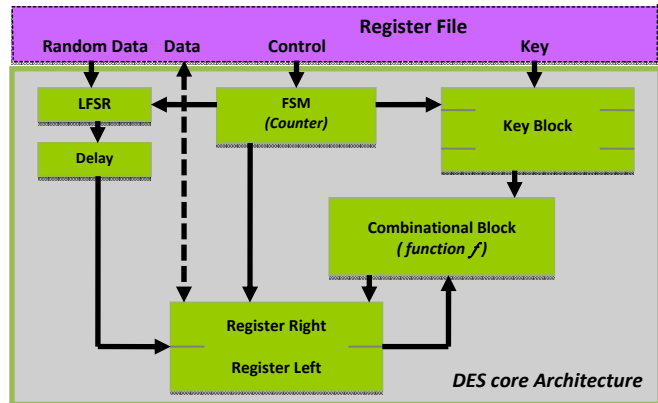
Tiempo clockless crypto-processor core - **DES** – is able to execute the standard ciphering and deciphering algorithms DES, DES<sup>-1</sup>, 3DES and 3DES<sup>-1</sup>. This IP is designed in Tiempo fully asynchronous and delay insensitive technology that allows ultra-low power consumption, ultra-low noise, ultra-low EMI, as well as robustness against attacks by power analysis & fault injections.

## Applications

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

## Key features

- Executes standard ciphering and deciphering algorithms DES, DES<sup>-1</sup>, 3DES and 3DES<sup>-1</sup>
- Fully asynchronous (no clock) and delay insensitive (correctness of ciphering/deciphering 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



Tiempo DES architecture

## Key benefits

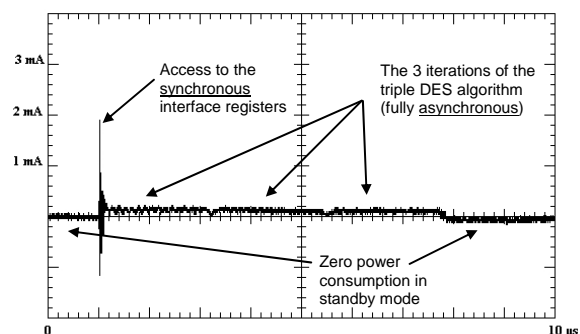
- Ultra low power consumption: low energy, low current peaks
- Ultra low electromagnetic emission (EMI/EMC)
- High speed (independent from any system clock)
- High robustness against any PVT (process, voltage, temperature) variation
- High robustness against attacks by power analysis and fault injections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

## Electrical characteristics

Measurements below were performed on the DES<sup>4</sup> chip designed and processed in a general-purpose CMOS 130 nm technology.

|                          |             |             |
|--------------------------|-------------|-------------|
| Supply voltage range     | 0.6 V       | 1.2 V       |
| Max current peaks        | 250 $\mu$ A | 800 $\mu$ A |
| Aver current consumption | 200 $\mu$ A | 1 mA        |
| DES execution time       | 2,3 $\mu$ s | 250 ns      |

Note: the DES<sup>4</sup> chip includes synchronous interface registers for test purposes.



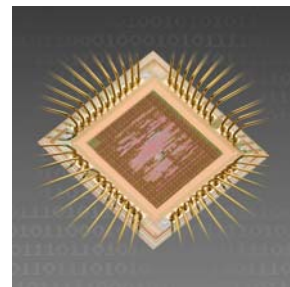
Average 3DES current profile  
(measures on circuit operating at 0.6V)

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

## Silicon-proven

Designed and processed in a general-purpose CMOS 130 nm technology in March 2008, Tiempo **DES<sup>4</sup>** chip instantiates four DES cores, each core being functionally equivalent but designed with a different level of security (none, with different counter-measures against power analysis and/or fault injections).

This chip was fully operational at first run (with all options) and with expected performances (high speed, low power consumption).



**Tiempo DES<sup>4</sup> chip**

---

## For more information

### **TIEMPO SAS**

110 rue Blaise Pascal, Inovallée, 38330 Montbonnot St-Martin, France

Tel: +33 4 76 61 10 00

Email: [sales@tiempo-ic.com](mailto:sales@tiempo-ic.com)

Web: [www.tiempo-ic.com](http://www.tiempo-ic.com)