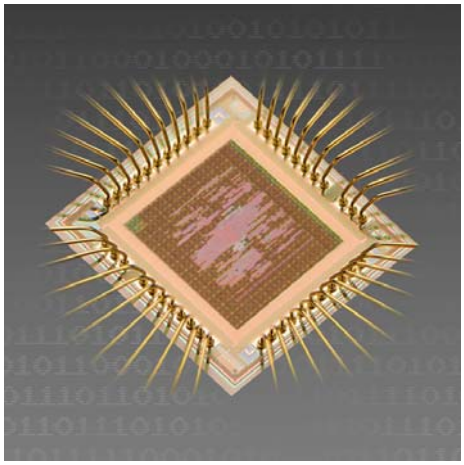
Montbonnot, June 10th, 2008

GRENOBLE, France – June 2008 – Tiempo, specialist in the design of asynchronous ICs, announces a fully-asynchronous delay insensitive DES crypto-processor chip.

Tiempo released in May 2008 a clock-less crypto-processor chip - **DES^4** - including four different DES cores *available as IP* and able to execute standard ciphering algorithms DES, DES^{-1}, 3DES & 3DES^{-1}.



Tiempo DES^4 crypto-processor chip

The DES^4 chip is *fully asynchronous* and *fully delay insensitive*, meaning that a correct execution of the ciphering algorithms is guaranteed regardless of the environmental variations ("PVT" for process, voltage, temperature).

Each core (IP) is designed with a different level of security (none, with temporal and/or spatial jitters against power analysis, with protection against fault injections).

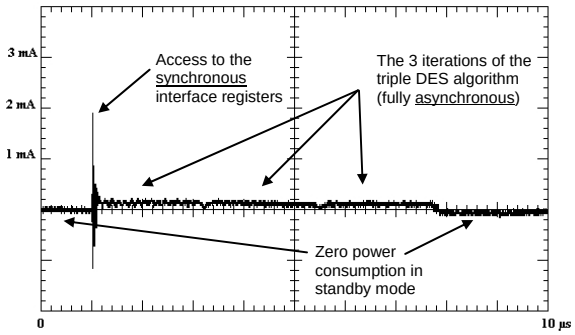
The DES^4 chip demonstrates the outstanding performances of Tiempo asynchronous delay insensitive design technology on processing speed and power consumption, as well as its robustness against attacks by power analysis and fault injections (with different levels of counter-measures).

Targeted applications are smart cards (with/without contact), RFID tags, sensor networks, systems with NFC technology…

Electrical characteristics

The chip was designed and processed in a general-purpose CMOS 130 nm technology in March 2008. It is fully operational at first run (with all options) and has exceptional performances: high speed (independent from any system clock) & low power consumption.

Supply voltage range	0.6 V	1.2 V
Max. current peaks	250 µA	800 µA
Power consumption	200 µA	1 mA
DES execution time	2,3 µs	250 ns



Average current profile on 20 runs of the 3DES algorithm (measures on circuit operating at 0.6V)

About Tiempo

Tiempo, located in Montbonnot St-Martin, near Grenoble (France), develops and commercializes a complete solution – IP, EDA and services – for the design of innovative clock-less integrated ICs. Tiempo technology is fully asynchronous and delay insensitive. It allows designing chips that are ultra-low power (energy and current peaks), ultra-low noise, functionally robust against PVT variations and secured against attacks by power analysis and fault injections. Tiempo portfolio of IPs includes asynchronous cores of microcontrollers, microprocessors, crypto-processors and peripherals.

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
Web: www.tiempo-ic.com