



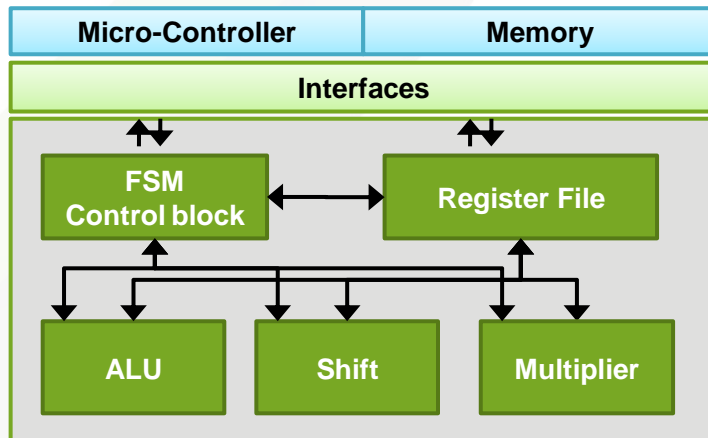
Tiempo clockless crypto-processor core - TPKA - is a public key encryption and decryption accelerator. It is able to execute the standard RSA encryption and decryption algorithms with CRT computation. It can also be used as an accelerator for ECC computations. This IP is designed in Tiempo fully asynchronous 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



TPKA 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 RSA standard encryption and decryption algorithms
 - Key and data: up to 2048 bits + 128 bits for security
 - Full hardware RSA-CRT computation
- ECC - GF(p) - encryption and decryption algorithms primitives 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 netlist¹ ready for P&R (silicon-proven netlist)
 - As an option: Verilog netlist¹ secured against attacks by power analysis and fault injection
 - As an option: Verilog netlist¹ strengthened for ultra low noise, ultra low EMI

¹ Please contact Tiempo for available libraries and technologies

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
RSA CRT 1024 speed (ms)	36.3	12.7
Average current (mA)	1.89	8.5
Energy (μJ)	68.6	162

