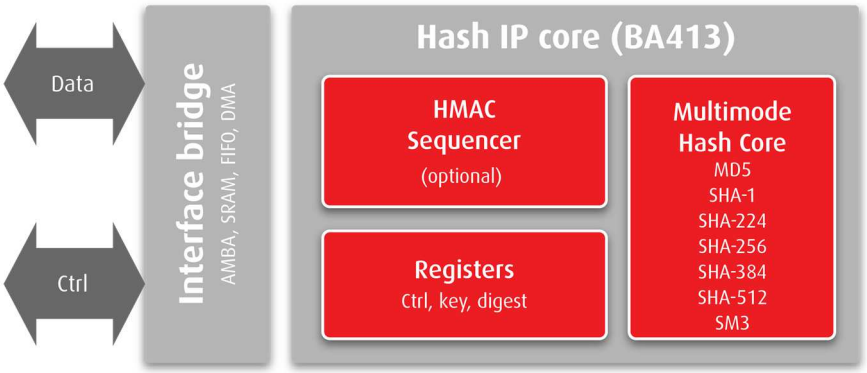
Hash crypto Engine

BA413
Product sheet

The BA413 is a flexible and optimized hash IP core developed, validated and licensed by Silex Insight.

With a flexible wrapper supporting a wide selection of programmable hashing modes (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SM3 and MD-5) with HMAC and several options of data interface, the BA413 is an easy-to-use solution with predictable resources and performances on ASIC and FPGA.



Implementation aspects

The BA413 core is easily portable to ASIC and FPGA (Altera, Xilinx, Microsemi). It supports a wide range of applications on various technologies. The unique architecture enables a high level of flexibility. The throughput and features required by a specific application can be taken into account in order to select the most optimal and compact configuration.

Deliverables

- Netlist or RTL
- Scripts for synthesis & STA
- Self-checking test-bench based on referenced vectors
- Documentation

Features

- Supports SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SM3 and MD-5
- Supports HMAC
- 66 or 83 cycles per 512- or 1024-bit chunks depending on the algorithm
- Low power feature
- Compact solution (<30KG for SHA-256)
- Data interface: AMBA (AHB/AXI) with optional DMA
- Control interface: APB or AXI4-lite

Applications

- Message digest calculation
- Required by most security protocols