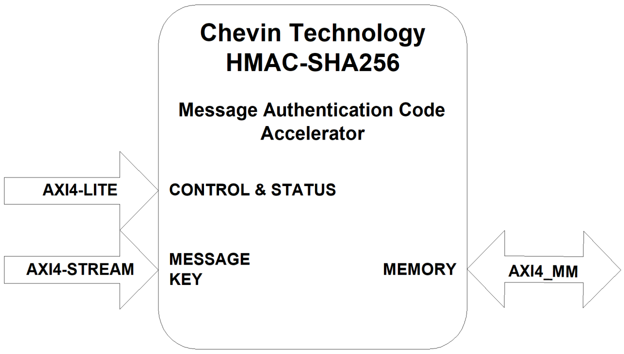
HMAC-SHA256 Accelerator

Overview

Chevin Technology's HMAC-SHA256 cryptographic accelerator function is used to securely generate and verify message authentication codes. The all-RTL solution provides a fast and secure way to calculate a SHA256 hash for any message of any length. When combined with a secret key, it can also construct a HMAC keyed-hash message authentication code, which can be used when protect messages that are sent and verify those that are received. The accelerator accepts multiple independent streaming messages/channels, and support any number of arbitrary length messages. Number of channels is limited only by the memory resources provided, embedded Block RAM or external DDR. Typical use cases include highly secure RTL solutions where a CPU is unable to meet the required throughput and security performance.

Applications

- *Hardware Root of Trust*
- *Widely used password hash algorithm*
- *Security Critical HTTP, SSL, TLS*
- *Securely generate & verify keyed-hash MAC*
- *Reduce Risk of cyber hacks, copying, cloning*



Key Features

- *HMAC-SHA256 Message Authentication*
- *All-RTL security solution in Hardware*
- *Key storage in Private memory*
- *Multi-channel operation with AXI4_STREAM*
- *High Throughput >1M hashes /second @156MHz*
- *Compact 554Mbps - 2700 LUTs / 2BRAM*
- *Performance 4.4Gbps - 21k LUTs / 20BRAM*
- *Seamless integration with AXI4_ST / AXI4_MM*
- *NIST FIPS 180-4 Secure Hash Standard*
- *RFC6234 SHA256 Secure Hash Algorithm*
- *NIST FIPS 198-1 HMAC Keyed-Hash MAC*

Performance Figures

Logic consumption	
LUTs	2700 / 21k
BRAMs	2/ 20
Clock Rate (FPGA)	400MHz
Clock cycles per Hash	232Mbps / 4.4Gbps

Interface	
Message & Key	AXI4-Stream 32bit
Hash & HMAC	AXI4-MM 32bit
Message max length	2^61 bytes
HMAC # of channels	
Using BRAM (internal)	32 to 256
Using DDR (external)	64k

Message Authentication

Many applications today require message authentication to verify the integrity of a message and preventing any part of it being changed. SHA256 is a widely used message authentication code, MAC or a one-way hash, that was developed by United States National Security Agency (NSA) and published by NIST as FIPS 180-2. It offers greater protection than the popular previous hash methods MD5 and SHA-1, and is currently being used for applications such as TLS, SSL, IPSec and Bitcoin.

Fast and Efficient Hashing Logic

The hash algorithm SHA256 logic splits the message into an integer number of 512bit blocks. Arbitrary length messages are extended with padding logic taking the messages nearest multiple before going through a series of shift , rotate, xor and add operations which have an "avalanche" effect and cause a great deal of change in output from even a single bit difference input. The RTL in this block has been designed to take advantage of the high performance available in FPGAs and ASICs, and deliver high throughput in a compact logic footprint.

Multiple Channels — Streaming and Memory Mapped Interfaces

The streaming input TID identifies input channels by number 0..N-1, which supports the calculation of hashes on independent data sources concurrently rather than sequentially. This is particularly useful when working with data of different sizes, as there is no need for coordination to avoid smaller blocks being held up by large blocks being hashed.

The memory mapped interface fetches messages from memory, using DMAs. This too works on channels that allow concurrent hashing on independent sources.

HMAC-SHA256 Accelerator

The HMAC-SHA256 accelerator protects both the integrity and authenticity of the original message by combining a key and message with a cryptographic HMAC, keyed-hash message authentication code. A message is provided over the streaming or memory mapped interface along with the key, and the HMAC result is stored in memory. The accelerator works on multiple channels concurrently, which supports multiple arbitrary length messages HMAC calculations without causing head-of-line blocking or other scheduling constraints.

Easy Integration with IP-XACT

The HMAC-SHA256 accelerator is delivered as source code for ASIC or a targeted netlist for FPGA with an IP-XACT package that is recognised by FPGA vendor EDA tools making integration quick and accurate. Software drivers and examples are included to shorten the development time and effort

Deliverables

- Encrypted compiled netlist
- Datasheet & User Guide
- Reference Designs
- Simulation Test bench
- Build scripts for Vivado
- Support for integration into FPGA