S.A.B.E.R. Encryptor (ASCON)

Product Guide

Murilo MULLER

2025-08-21

Overview

encryptor_system is a self-contained, single-clock hardware pipeline that encrypts a byte stream using **ASCON-128** and outputs a **1792-bit** framed packet suitable for downstream transmission (e.g., Wi-Fi). The frame contains: *23 ciphertext blocks (23 × 64 b), TAG (128 b), Associated Data AD (64 b), and NONCE (128 b).*

Internally, the design integrates: a byte → 64 b packer (`data_reg`), control FSMs (`fsm_SABER` and `drive_ascon`), the `ascon` core, static `ad_reg`/`key_reg`, a `nonce_gen`+`nonce_reg` path, and a 1792-bit frame packer (`cipher_reg`).

Key Features

- ASCON-128 authenticated encryption flow (init, AD absorption, plaintext encryption, finalisation, tag).
- Fixed payload: 23 plaintext blocks (64 b each) per frame.
- Framed output: 56 words × 32 b (total 1792 b) + 1-cycle `data_valid_o` pulse.
- Single clock domain, active-high asynchronous reset.
- Embedded constants: `KEY_CONST` (128 b) and `AD_CONST` (64 b).
- Internally generated 128-bit NONCE for each frame.

Ports

Name	Dir	Width	Description
`data_i`	in	8	Incoming ECG byte stream (sampled internally).
`go_i`	in	1	Start trigger for the system controller.
`reset_i`	in	1	Asynchronous reset, active-high.
`clock_i`	in	1	System clock (see "Clock/Reset").
`data_o`	out	1792	Flattened frame (56 × 32 b), layout below.
`data_valid_o`	out	1	1-cycle pulse when `data_o` is valid/complete.
`send_data_o`	out	1	Strobe to request downstream send (from `fsm_SABER`).

Clock / Reset

- **Clock:** single clock on `clock_i`. Typical configuration: `FREQ_HZ = 100 MHz`.[1]
- **Reset:** `reset_i` is asynchronous, active-high.

[1] The IP metadata sets `ASSOCIATED_RESET=reset_i` and `ASSOCIATED_BUSIF=frame_if` for packaging.

Operation Sequence (Simplified)

1. Assert `reset_i` to clear internal state; deassert to start idle.
2. Pulse or assert `go_i`. The controller (`fsm_SABER`) begins one frame cycle:
   - Generates NONCE, loads AD/KEY/NONCE regs.
   - Feeds AD then plaintext blocks into the ASCON core via `drive_ascon`.
3. When the frame is complete, `data_valid_o` pulses for 1 cycle; `data_o` holds the 1792-bit packet.
4. `send_data_o` strobes for external transmission logic. The packer keeps the frame stable until internally cleared for the next cycle.

Frame Layout (1792 b)

`data_o` is arranged as 56 little-endian 32-bit words (word 0 is `data_o[31:0]`). Mapping:
- Ciphertext blocks (23 × 64 b): words **0..45**, two words per block: *LSW first* then *MSW*.
- TAG (128 b): words **46..49**.
- AD (64 b): words **50..51**.
- NONCE (128 b): words **52..55**.

Note: `data_o` remains stable after `data_valid_o` until the internal clear for the next frame.

Plaintext Byte Intake

- `data_reg` collects incoming bytes on `data_i` and emits 64-bit words every 8 bytes.
- After 181 bytes, it emits a final 64-bit word formed by the last 5 bytes plus padding `0x80_00_00`.

Parameters & Constants

- `KEY_CONST` (128 b): device key embedded at top level.
- `AD_CONST` (64 b): associated data embedded at top level (keep the trailing padding `0x8000` if modified).
- Total plaintext blocks per frame: **23**.

Interfaces (IP Packaging Hints)

For IP Packager compliance:
- Mark `clock_i` as `xilinx.com:signal:clock:1.0` with `FREQ_HZ` and `ASSOCIATED_RESET=reset_i`.
- Optionally associate `data_o` to a simple data interface, e.g., `xilinx.com:signal:data:1.0` named `frame_if`, and set `ASSOCIATED_BUSIF=frame_if`.

Versioning & License

- Module: `encryptor_system`, Version: **v1.1**.
- License: **MIT**. This work was produced for the AMD Open Hardware University Design Competition 2025.

Contact

Author: Murilo MULLER.
Email: murimattosmuller@gmail.com
Linkedin: www.linkedin.com/in/murilomuller7
Project: **S.A.B.E.R. — Secure AI-Based Encrypted ECG Rhythm-Monitoring**.