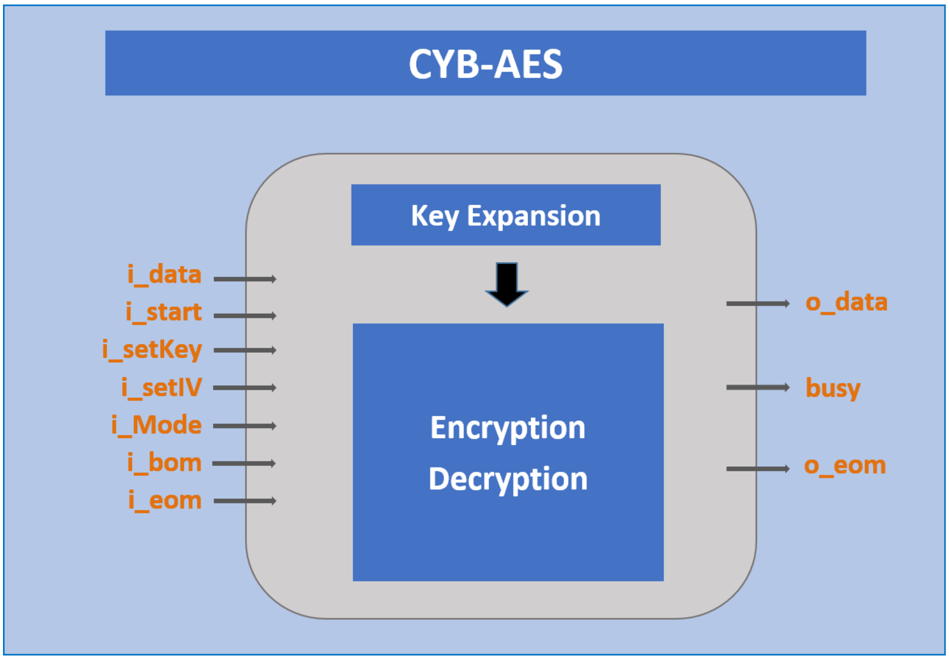
Overview of AES



CYB-AES implements Rijndael cipher encoding and decoding in compliance with the NIST Advanced Encryption Standard. It supports all of the available key-sizes (128, 192, 256-bit) to be integrated into any AES design requirement. Basic core is designed only for encryption. Enhanced versions are available that support encryption and decryption for various NIST cipher modes (ECB, CBC, OFB, CFB, CTR), as well as different datapath widths for size/performance tradeoff. It also includes the key expansion logic.

CYB-AES is an ideal solution for Wi-Fi products, sensor networks, wireless communications and surveillance systems. It is designed with high performance and fast integration into ASIC and FPGA applications.

Feature

- Encrypts using the AES Rijndael Block Cipher Algorithm
- Employs key sizes of 128, 192, or 256 bits
- Key expansion function
- Simple external interface
- Highly optimised for use in Xilinx and Altera FPGA technologies

Deliverable

- Flexible licensing
- Documentation
- Netlist
- Verilog or VHDL
- Testbench
- Technical support

Application

- Wi-Fi / Zigbee
- Sensor networks
- Cipher for wireless communications
- Surveillance systems
- Electronic transactions