

Advanced Encryption Standard

Overview

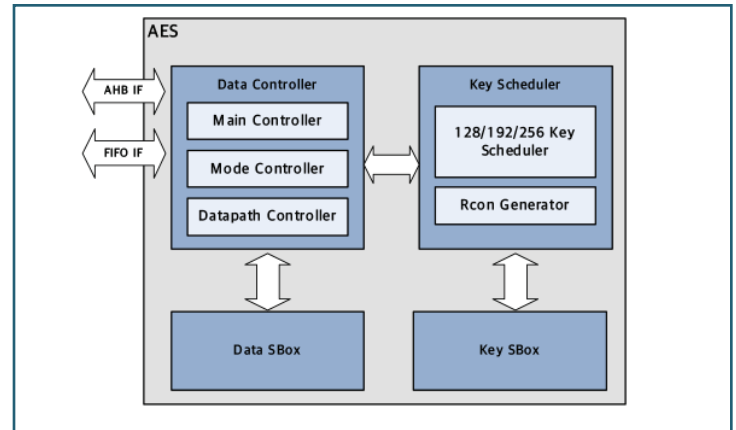
The Advanced Encryption Standard (AES) IP is a representative block cipher engine (FIPS-197). The AES hardware can be easily configured for a customer's requirement such as target size, performance, or operation mode.

Key Features

- FIPS Publication 197 Compliant
 - ECB, CBC and XTS with CTS, CTR, CMAC, CCM, and GCM Mode
 - 128/192/256 Bits Key
- AHB Slave Interface for SFR Setting or FIFO Interface for DMA Operation
- Optimization for High Performance, Small Gate Count and Low Power

Deliverables

- Encrypted RTL
- Data Sheet Document
- User Guide Document



Target Applications

- Digital Right Management (DRM)
- WLAN Application (IEEE 802.11)
- IPsec and SSL/TLS
- Full Disk Encryption (FDE)

SAMSUNG Foundry

For more information, please contact us at IP@silvaco.com.

©Copyright Silvaco, Inc. All rights reserved. Silvaco is a registered trademark of Silvaco, Inc. Samsung Foundry is a trademark of Samsung Electronics Co. Ltd. All other names mentioned herein are trademarks or registered trademark of their respective owners.

All information provided is for reference purposes only and may be changed without notice.

SILVACO

HEADQUARTERS

2811 Mission College Boulevard, 6th Floor

Santa Clara, CA 95054

Phone: 408-567-1000

Fax: 408-496-6080



CALIFORNIA

sales@silvaco.com
408-567-1000

MASSACHUSETTS

masales@silvaco.com
978-323-7901

TEXAS

txsales@silvaco.com
512-418-2929

JAPAN

jpsales@silvaco.com

EUROPE

eusales@silvaco.com

FRANCE

eusales@silvaco.com

KOREA

krsales@silvaco.com

TAIWAN

twsales@silvaco.com

SINGAPORE

sgsales@silvaco.com

CHINA

cnsales@silvaco.com

WWW.SILVACO.COM