

## Secure Advanced Encryption Standard

### Overview

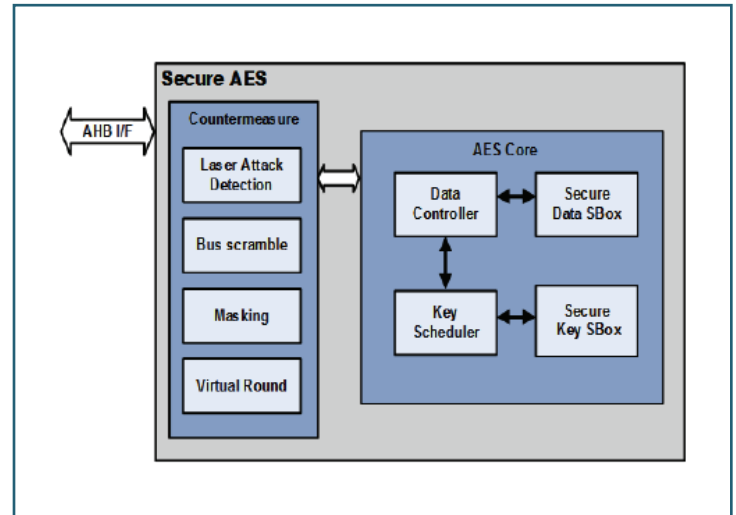
The Secure Advanced Encryption Standard (AES) IP is a representative block cipher engine (FIPS-197) and is resistant to side channel attack and fault attack. The Secure AES hardware can be easily configured for a customer's requirement such as target size, performance, or operation mode.

### Key Features

- FIPS Publication 197 Compliant
  - o ECB, CBC and XTS with CTS, CTR, CMAC, CCM, and GCM Mode
  - o 128/192/256 Bits Key
- Side Channel Attack (SCA) and Fault Attack Countermeasure
  - o Masking Method
  - o Secure SBox (Constant Power Consumption SBox)
  - o Fault Detection Logic
  - o Virtual Round and Optional Virtual AES

### Deliverables

- Encrypted RTL
- Data Sheet Document
- User Guide Document



### Target Applications

- Smart Card
- Digital Right Management (DRM)
- Any Field Required Side Channel Attack / Fault Attack Protection

# SAMSUNG Foundry

For more information, please contact us at [IP@silvaco.com](mailto: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](mailto:sales@silvaco.com)  
408-567-1000

MASSACHUSETTS

[masales@silvaco.com](mailto:masales@silvaco.com)  
978-323-7901

TEXAS

[txsales@silvaco.com](mailto:txsales@silvaco.com)  
512-418-2929

JAPAN

[jpsales@silvaco.com](mailto:jpsales@silvaco.com)

EUROPE

[eusales@silvaco.com](mailto:eusales@silvaco.com)

FRANCE

[eusales@silvaco.com](mailto:eusales@silvaco.com)

KOREA

[krsales@silvaco.com](mailto:krsales@silvaco.com)

TAIWAN

[twsales@silvaco.com](mailto:twsales@silvaco.com)

SINGAPORE

[sgsales@silvaco.com](mailto:sgsales@silvaco.com)

CHINA

[cnsales@silvaco.com](mailto:cnsales@silvaco.com)