

## Public Key Engine

### Overview

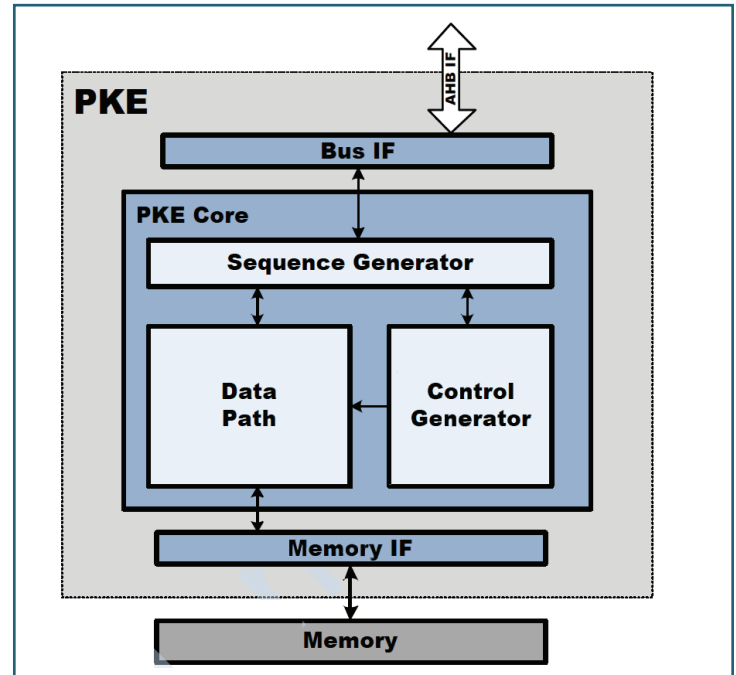
The Public Key Engine (PKE) accelerates RSA and Elliptic Curve Cryptography (ECC) operations by supporting modular operations and elliptic curve based operation for public key cryptosystems. It provides high performance for application processors, smartcards and consumer applications.

### Key Features

- Various Arithmetic Operations
  - o Modular Addition/Subtraction (up to 4,128 bits)
  - o Montgomery Multiplication (up to 4,128 bits)
  - o Modular Exponentiation/Inversion (up to 4,128 bits)
  - o EC Operation (Point Addition/Doubling, Scalar Multiplication) over GF(p) (up to 544 bits)
- Optional Security Features
  - o Power Analysis and Fault Attack Countermeasures
  - o SRAM Management for Secure and Non-Secure Regions
- Requirement
  - o Dedicated SRAM for PKE (Minimum 1.8KB for RSA-2048)

### Deliverables

- Encrypted RTL source
- Data Sheet Document
- User Guide Document



### Target Applications

- User/Device Authentication
- Secure Booting & Key Exchange
- Digital Signature

# 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)

[WWW.SILVACO.COM](http://WWW.SILVACO.COM)

Rev 080619\_01

71812