

HMAC IP for Integrity Check

Overview

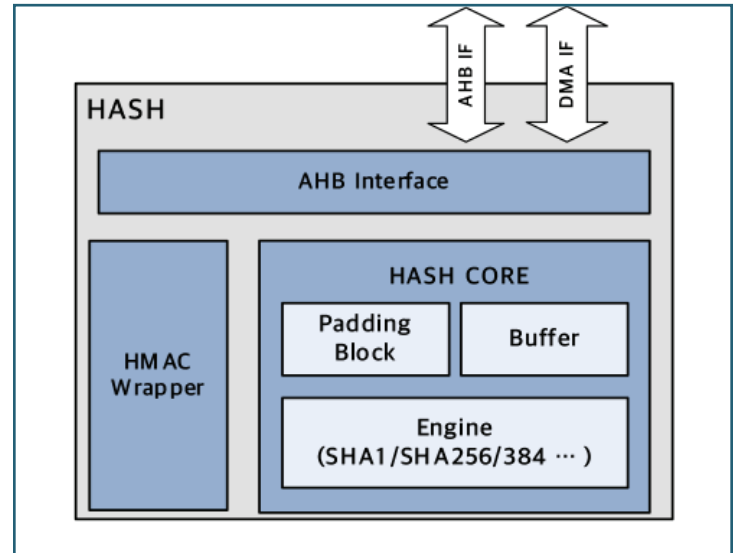
This IP is a cryptographic engine to digest messages for digital signature, integrity check, and so on. The corresponding standards are FIPS180-2 (SHA1/SHA256/384/512) and FIPS 202 (SHA3-224/256/384/512, SHAKE128/256) as published by NIST. Hash hardware can be easily configured for a customer's requirement such as target size, performance and supporting algorithm.

Key Features

- Configurable SHA1, SHA256/384/512, SHA3-224/256/384/512 with Keyed-Hash Message Authentication code (HMAC)
- Partial Hash/HMAC Operation with User IV
- Hash/HMAC Operation for Zero-length Message

Deliverables

- Encrypted RTL
- Data Sheet Document
- User Guide Document



Target Applications

- Integrity Check with Symmetric Key
- Message Digest for Fixed Size

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

Rev 080619_01
71811