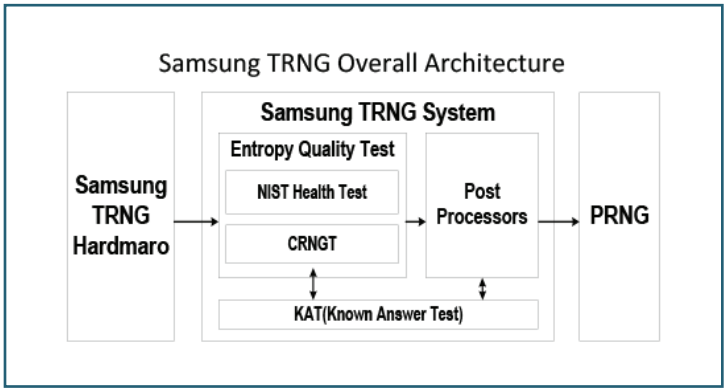
SILVACO

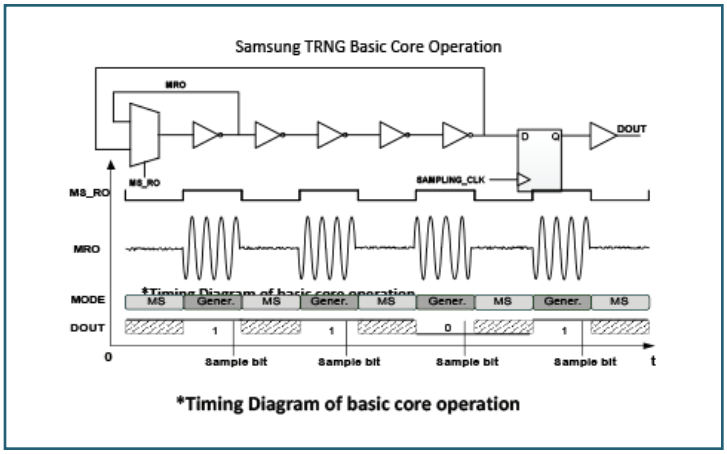
SIPware

True Random Number Generator

Overview

The True Random Number Generator (TRNG) is composed of three parts. The Samsung TRNG hard-macro generates the random seed, and the Samsung TRNG System (Softmacro) controls accumulation of random data, statistical verification, and processing. The PRNG generates the pseudo-random data, and it is optional depending on application. Samsung TRNG IPs are available in the latest Samsung processes.





*Timing Diagram of basic core operation

Key Features

- High Entropy Source based on thermal noise from Meta-stable Ring-OSC
- BSI AIS.31/PTG.2 Compliant Core
- Standard complicance
  - o NIST SP800-90A/B, FIPS140-2
- Embedded Post Processors
  - o LFSR32, Dichtl XOR, Von Neumann
- CRNGT (Continuous Random Number Generator Test) and KAT (Known Answer Test)
- Embedded BIST for Mass Production Test
- Throughput 0.500 Mbps

Deliverables

- Encrypted RTL
- Hardmacro DK / LEF / GDS
- User / Integration / Test Guide Documents

Target Applications

- Secret Key Generation
- Challenge-Response Protocol
- Unique Nonce Generation

SAMSUNG Foundry

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

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
71801