SILEX INSIGHT

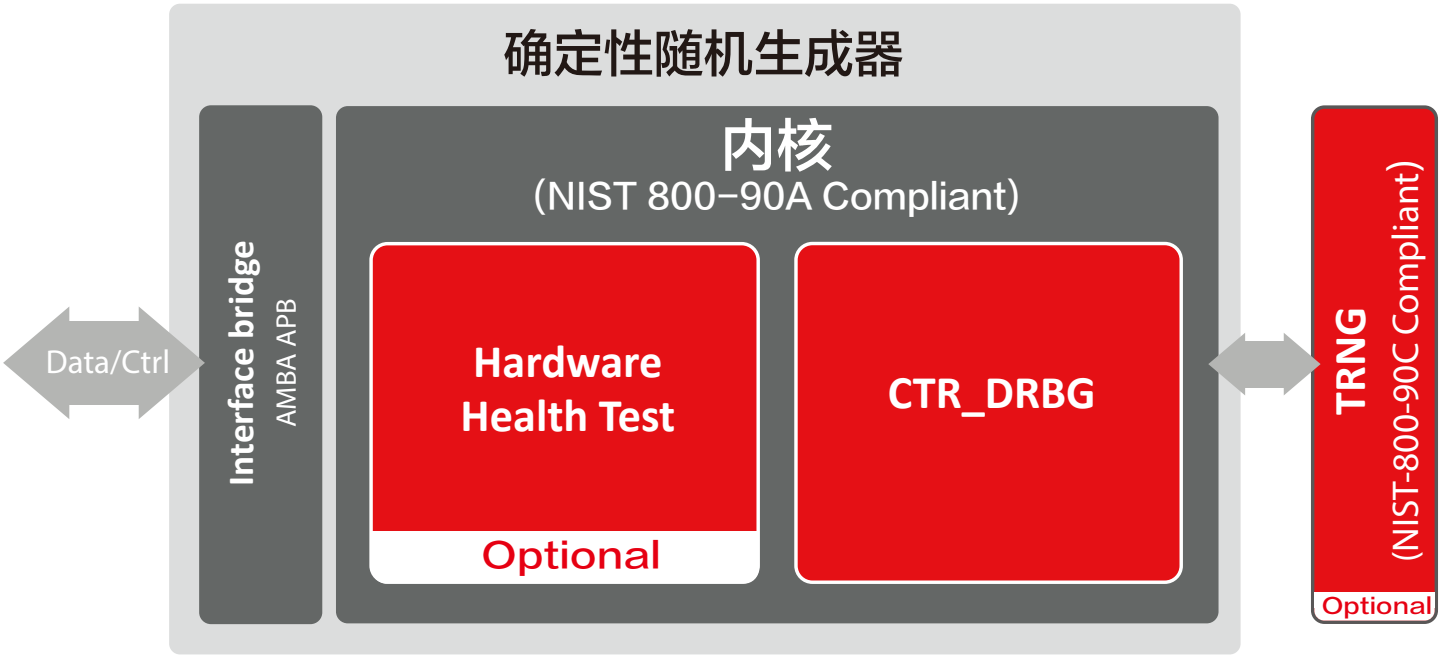
产品手册
BA433

确定性随机生成器 (DRBG)

确定性随机生成器可应用于需要加密保护的所有FPGA、ASIC和SoC设计，经过硅验证的数字IP内核，是符合NIST-800-90A Rev1的确定性算法， IP内核已成功通过NIST-800-90A Rev1测试套件，并且符合FIPS-140-2验证。

随机数的生成对于任何安全设备都至关重要，随机数用于密钥生成、密钥交换、数字签名、加密等，IPsec，MACsec，TLS / SSL或无线等典型的安全协议在身份验证/密钥交换和数据流阶段使用。

确定性随机生成器可以与真随机数发生器（TRNG）一起提供，形成具有完全符合FIPS 140-2的随机数发生器（NIST 800-90A / B / C），通用的AMBA APB接口可用于控制和数据传输。



特性

- 符合NIST 800-90A/B/C
- 健康测试
- 基于AES-CTR (CTR_DRBG)
- 符合FIPS 140-2
- 为 FIPS 140-3准备
- 技术可集成到 FPGA and ASIC
- AMBA APB 接口
- 纯数字

应用

- 防御
- IPSec (VPN)
- TLS/SSL
- 智能汽车
- IoT
- 可穿戴设备
- 嵌入式安全
- HSM

软件支持

Linux驱动程序可简化Linux OS中的集成， Linux驱动程序可通过“ / dev / random”直接访问真正的随机数生成器，还提供用于微控制器应用程序的软件驱动程序，以简化对随机发生器的控制。

技术

熵源是纯数字的，无需其他特殊技术的开发，可将其轻松集成到任何技术（所有ASIC节点，英特尔和赛灵思FPGA系列），随机发生器已用于许多ASIC和FPGA设计中，我们客户的产品还通过了FIPS 140-2的验证。

产品交付

- Netlist 或 RTL
- Synthesis & STA 脚本
- 基于 FIPS 的 elf-check 测试平台 vectors
- 文档

Silex Insight
上海市闵行区虹许路528号
2号楼208室（201103）

Tel: +86 21 6221 0867
E-mail: contact-cn@silexinsight.com
Web: www.silexinsight.com.cn