SILEX INSIGHT

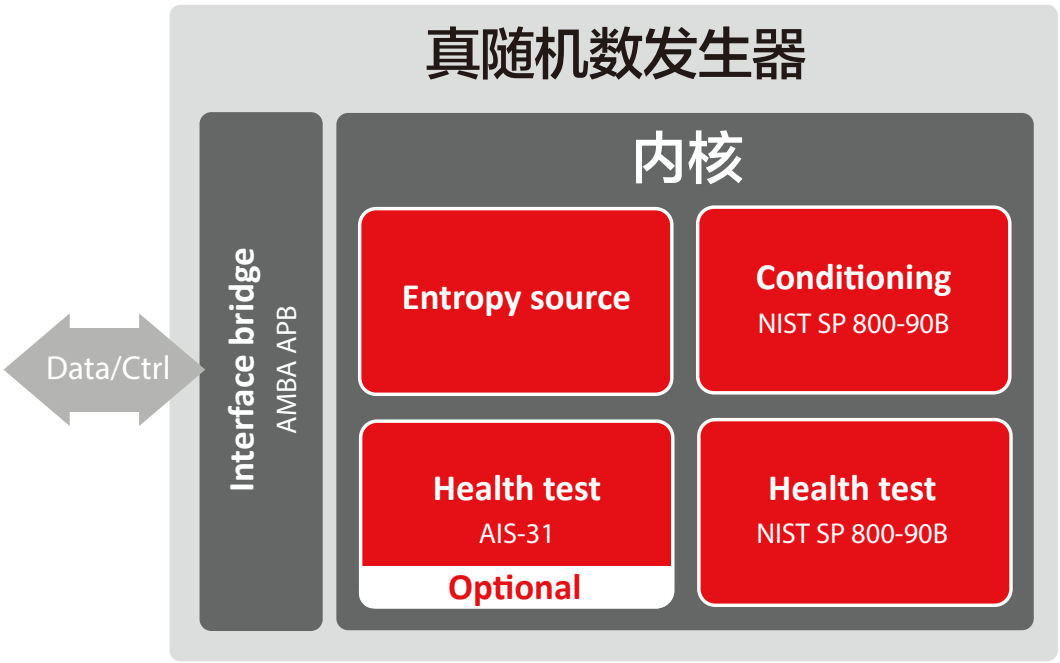
产品手册
BA431

真随机数发生器

真随机数发生器IP是一款经过硅验证的IP核,有基于FPGA,ASIC和SoC的各种实现方式,广泛应用在基于加解密的各种安全解决方案中,它是一种数字熵源,专为符合 NIST-800-90B和 AIS31而设计, IP核的熵源成功通过了 NIST-800-22、90B 和 AIS31 测试，并且符合FIPS-140-2验证。

随机数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，典型的安全协议，如IPsec、MACsec、TLS/SSL 或无线协议，在身份验证/密钥交换和数据传输阶段使用。

真随机数生成器包括NIST 800-90B 和AIS31中定义的校正功能和健康测试，AMBA APB 接口用于控制和数据传输。



特性

- 符合NIST 800-90B
- AIS-31 start-up and on-line tests (optional)
- 通过 NIST 800-22, 90B 和 AIS31 测试
- 符合FIPS 140-2
- 可以符合 FIPS 140-3
- FPGA 和 ASIC 便携技术
- Linux drivers (access from /dev/random)
- AMBA APB 接口
- 纯数字

应用

- 军用
- IPSec (VPN)
- TLS/SSL
- 汽车
- IIoT
- 可穿戴设备
- 嵌入式安全

软件支持

Linux驱动程序可用于简化 Linux操作系统中的集成， Linux驱动程序通过"/dev/random"提供对真随机数生成器的直接访问，微控制器应用的软件驱动程序也可用于简化随机生成器的控制。

技术

熵源是完全数字化的，无需依赖任何特定工艺，它便于将其移植到任何制程工艺（所有 ASIC 节点、英特尔和 Xilinx FPGA 系列），随机发生器已用于许多ASIC和FPGA设计。

我们客户的产品也通过了FIPS 140-2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

真随机数发生器也可选配在我们的**确定性随机数发生器（BA433）**及**加密处理器（BA450）**中。

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