iRNG

Intrinsic-ID's iRNG is a true random number generator developed on Intrinsic-IDs Hardware Intrinsic Security (HIS) technology. The generation of random data by iRNG is based on the use of memory: SRAM is used as the source of entropy. This uninitialized SRAM is used for the generation of a true random seed, which serves as input for a FIPS 140-3 compliant Deterministic Random Bit Generator (DRBG). It is designed to generate large amounts of random data at high speed, with a very short start-up time. iRNG is available both in hardware and software and can be integrated seamlessly into many of Microsemi's FPGAs, such as those in the ProASIC®3 family, or customizable system-on-chip devices (cSoCs), such as those in the SmartFusion® family.

Functionality

Random data generation

Advantages

- Quick start-up time, typically more than 10x faster than alternative technologies due to always ready SRAM
- Fast generation of large amounts of random data
- Based on true random seed
- Low implementation cost
- Usage of the SRAM makes the technology scalable, small and flexible towards process variations.

Applications

For a complete security solution, iRNG can be combined with other products by Intrinsic-ID, such as Quiddikey™. With this completely HIS-based security functionality, no secret information is stored in the device unprotected.

The generated random bit stream is approved to be used for the generation of strong key material, IVs, nonces and any other random data.

iRNG can be used in many kinds of applications, such as financial, automotive, government and military communication systems, content protection systems, routers or other network communication devices, Public Key Infrastructures, and modules for erasing sensitive data by overwriting with random data.

Hardware Specification Example

Number of ProASIC3 cells	2761
SRAM	2 Kbytes (four 4-Kbit SRAMs)
Performance	4 cycles per byte; 50 Mbps at 25 MHz
Start-up cycles	~20 Kcycles; 0.8 ms at 25 MHz
Maximum random bits before repowering	$<2^{64}$

Software Specification Example

Platform	SmartFusion cSoC with ARM® Cortex™-M3
SRAM	2 KBytes (four 4-Kbit SRAMs)
Performance	0.2 ms for 16 bytes 0.7 Mbps at 80 MHz
Start-up cycles	~3.7 Mcycles 47 ms at 80 MHz
Maximum random bits before repowering	$<2^{64}$

Notes:

1. Other trade-offs between area and performance are available on request.
2. Actual numbers are dependent on the specific FPGA or cSoC model selected.

Microsemi Corporate Headquarters
2381 Morse Avenue, Irvine, CA 92614
Phone; 949.221.7100 · Fax: 949.756.0308
www.microsemi.com