

Silicon-proven Intellectual Property (IP) for Random Number Generation

BENEFITS

- Highly reliable true random number generation
- Silicon-proven IP
- Fast and easy to integrate
- World-class support

Semiconductor designers require ready-to-use hardware designs that are silicon-proven and reliable. As part of our extensive IP product portfolio, AuthenTec provides SafeXcel™ IP True Random Number Generators (TRNGs) that address the unique needs of semiconductor OEMs and provide a reliable and cost-effective IP solution that is easy to integrate into System-on-Chip designs.

The SafeXcel IP True Random Number Generators are typically deployed in semiconductors that are utilized for secure data communications, secure electronic transactions, and secure data storage. They are, for example, used for generation of keys, initialization vectors, cookies, and nuances. They can also be used for statistical sampling, timers in communications protocols, as well as noise generation.

Silicon-proven Random Number Generator Solutions

The SafeXcel IP True Random Number Generators provide semiconductor designers with a silicon-proven solution that has been deployed in AuthenTec's leading VPN accelerator chips, as well as in several chips manufactured by AuthenTec semiconductor customers.

Ease of Integration

Years of experience in designing security products made AuthenTec the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly product interfaces. AuthenTec's global presence and expertise in security

IP design enables us to provide customers with 24/7 world-class support that is unmatched in the industry—ensuring the success of your project.

True Random Number Generation

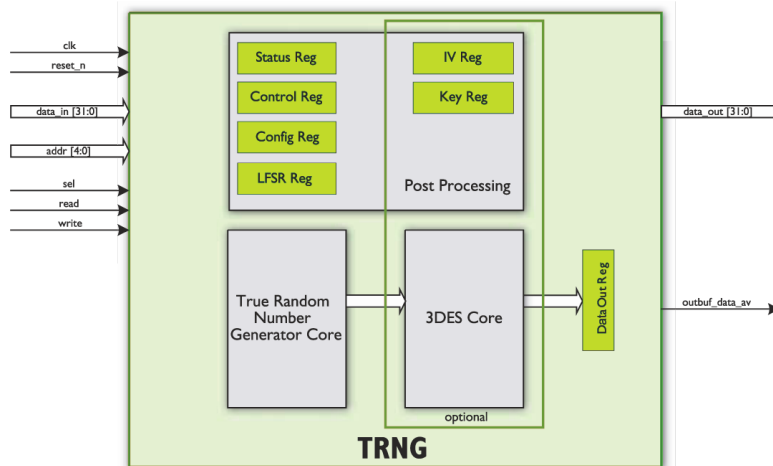
The TRNGs provide a hardware-based, nondeterministic noise source. The TRNGs are designed using dual shot noise generators that create unpredictable jittering output when asynchronously sampled by the system clock provided to the TRNGs. The outputs from the shot noise generators feed a complex, non-linear combinatorial circuit that produces the final TRNG output. Over 300 stages of Linear Feedback Shift Register (LFSR) are incorporated in the TRNG designs.

The random numbers are accessible to the application in a 32-bit read-only register. When the register is read, the random number generator immediately generates a new value, which is then shifted into the output register.

The TRNGs are designed for compliance with Federal Information Processing Standards (FIPS) Publication 140-2, facilitating system certification to this standard. An American National Standards Institute (ANSI) X9.17 Annex C / ANSI X9.31 Annex A post processor is available to meet the FIPS PUB 140-2 requirements.

Configuration flexibility

The SafeXcel IP True Random Number Generator is available in two configurations, as shown in the table.



SafeXcel IP True Random Number Generators Architecture

SafeXcel IP True Random Generator Configurations

CONFIGURATION	MAXIMUM CLOCK FREQUENCY ¹	TRNG THROUGHPUT		APPROXIMATE GATE COUNT ¹ AT SYNTHESIS FREQUENCY
		AT ANY CLOCK FREQUENCY	AT MAX. CLOCK FREQUENCY	
EIP-75a	433 MHz	0.19 bits/cycle	82.2 Mbit/s	5.3 kgates @200 MHz
EIP-75b (incl. 3DES post processor)	400 MHz	Post processing enabled: 0.33 bits/cycle	Post processing enabled: 132 Mbit/s	13.2 kgates @200 MHz
		Post processing disabled: 0.19 bits/cycle	Post processing disabled: 76 Mbit/s	

¹ Technology and synthesis dependent; based on the use of a basic design compiler and a high-speed 0.13 m technology.

SPECIFICATIONS

Features	Deliverables
• Generation of truly random numbers	• Synthesizable Verilog RTL source code
• Redundant fail-safe design with self-test circuits	• Self-checking RTL test bench
• Reliable shot noise oscillator implementation with self-adjustment	• Simulation script
• Designed for FIPS 140-2 compliance	• Synthesis script
• Optional 3DES post processor	• User's Manual with technical specifications, including the programmer's interface
	• Developer's Manual with step-by-step descriptions that allows developers to easily install, verify, and synthesize the design

HEADQUARTERS

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, FL 32901 USA
+1-321-308-1300

For more information
about Embedded Security
Solutions:
embedded@authentec.com

WORLDWIDE REPRESENTATIVES NETWORK

A complete listing of
AuthenTec's network of
representatives is
available at our web site.

www.authentec.com