SYNOPSYS®

True Random Numbers for Every SoC

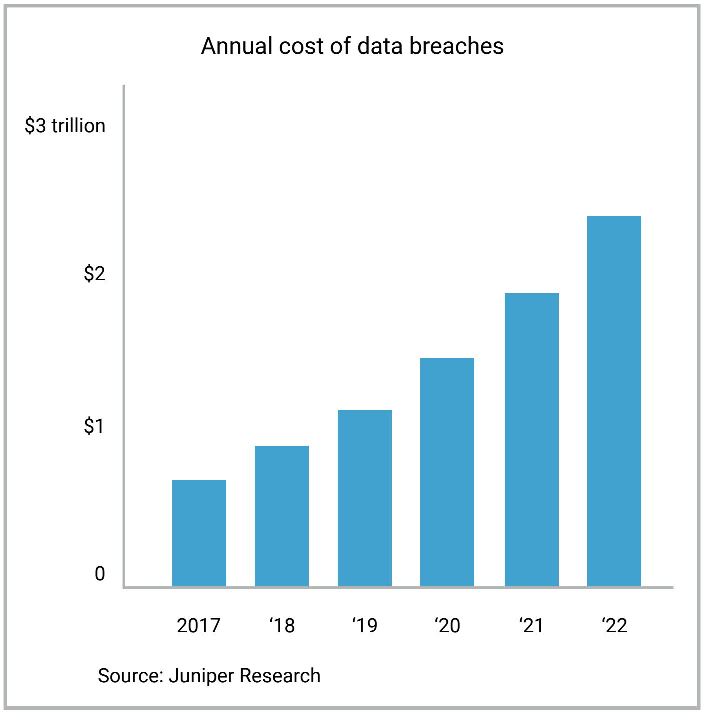
True Random Numbers for Every SoC

Connected devices are proliferating. The attacks, breaches, and malware are close behind. Protecting the data on your SoC is more important than ever, not just for your customer, but to help secure the full end product and ecosystem.

Cryptography, and specifically true random numbers, are at the heart of every secure system. The quality of random numbers contributes to the security strength of designs. True random numbers must be generated for cryptographic operations like the creation of cipher keys and initial values for counters and protocol parameters. If your random number generator is weak or predictable in any way, your chip can be open for attacks that can compromise keys, intercept data, and ultimately hack devices and their communication.

Preventing Data Breaches Starts with Really Random Numbers

Every consumer expects connected devices to operate correctly while protecting business and personal information. True Random Number Generators (TRNGs) are at the base of securing these devices. TRNGs are part of a "chain of trust" that needs to be established starting with the SoC, moving to the application layers and communication to the cloud.



Source: Juniper Research

> *"After evaluating four potential security IP providers, only Synopsys demonstrated sufficient technological expertise, product performance, and culture of flexibility to accommodate our specific functions and policies."*

Maurizio Paganini, Executive VP, MegaChips

A chain of trust is only as strong as its weakest link.

Using predictable random number generators can open doors to attacks that hack devices and compromise data. To be effective, random numbers must be unpredictable, statistically independent (unrelated to any previously generated random numbers), uniformly distributed (equal probability for any number to be generated) and undiscoverable.

Four Criteria for True Random Number Generators

- Unpredictable
- Independent
- Uniformly Distributed
- Undiscoverable

The Challenge of Generating Truly Random Numbers

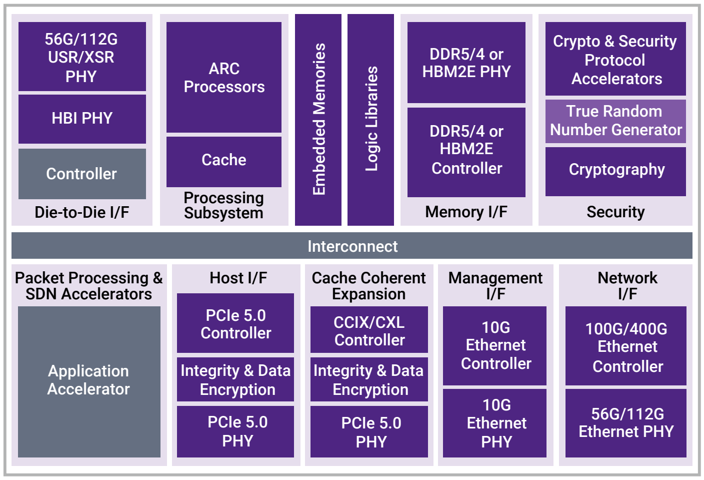
True randomness is very difficult to achieve. A TRNG is based on an unpredictable physical phenomenon, called an entropy source, that generates non-deterministic data (e.g., a succession of numbers) to seed security algorithms. The entropy source must use a random process, like the noise produced by current flowing in a transistor, or the time between radioactive decay events, or even the bubbles in a 1970s style lava lamp. A TRNG conditions the entropy signal to remove bias and whiten the spectrum of the resulting sequence of outputs.

This process must be controlled for factors such as operating temperature, aging, susceptibility to electronic noise and upset, voltage variation, and operating frequency range. Without controlling for these factors, the TRNG circuit could be modified by outsiders attempting to influence its operation.

To achieve true randomness, Synopsys DesignWare® True Random Number Generator IP contains an entropy source and whitening circuit that generates an **unpredictable** random sequence of bits that is statistically equivalent to a **uniformly distributed** noise. In addition, the TRNGs include a deterministic random bit generator which is securely seeded (**independent**) from this nonce to produce cryptographic quality (**undiscoverable**) random numbers.

> *“After evaluating multiple random number generator solutions, we selected the Synopsys DesignWare True Random Number Generator IP to protect our SoCs due to their proven, standards-compliant high-quality entropy and process portability.”*

Saleel Awsare, Senior VP & General Manager, IoT Division, Synaptics



Where are TRNGs Used in SoCs?

As part of the complete SoC security solution, TRNGs typically work with cryptographic cores for symmetric and asymmetric algorithms, or part of more complete secure systems with a Root of Trust.

Security Standards Help Ensure Quality of Random Number Generators

Designing TRNGs that provide consistently high-quality entropy across processes, temperature, voltage, and frequency variations is very complex. To help ensure the highest quality, international standards bodies have developed criteria to substantiate the truly random nature of TRNGs in a verifiable and statistically rigorous manner.

Several standards and certification associations, such as the US National Institute of Standards and Technology (NIST) agency, are driving specifications and validation methods for TRNGs to define the guidelines for design and certification of truly random solutions.

While these standards give some high-level architecture guidelines, they do not describe how to create a TRNG. The implementation details are left to the designers, and therefore permit many alternative approaches. In all cases though, certified TRNGs must meet the four criteria: they must be **unpredictable**, **uniform**, **independent**, and **undiscoverable**.

> *“The combination of Synopsys’ DesignWare Security and Foundation IP enabled us to implement the highest level of security while achieving the best combination of power, performance and area for our SoC.”*

Sky Shen, CEO, Starblaze Technology

DesignWare TRNGs Help Protect Your SoC Data

DesignWare TRNG IP is trusted to protect data in millions of SoCs worldwide. The standards-compliant and certification-ready DesignWare TRNGs are applicable to any digital semiconductor device and are highly portable across any ASIC and most FPGA process technologies. Synopsys TRNGs have been deployed in more than 150 designs down to 5nm processes, are customer configurable, and minimize impact on PPA while delivering the highest levels of security. They are compliant with the NIST SP800-90 A/B/c and BSI AIS 20/31 specifications, have been evaluated by third-party assessors, passed NIST CAVP validation and are certification ready for FIPS 140-2 / 140-3, Common Criteria (CC), and China's Commercial Cipher Administration (OSCCA).

DesignWare TRNG IP goes through rigorous internal validation, including silicon data collection and analysis to demonstrate its distribution of generated random numbers and its robustness across technologies and processes.

In addition to TRNGs, Synopsys provides a broad portfolio of highly integrated security IP solutions that use a common set of standards-based building blocks and security concepts to enable the most efficient silicon design and highest levels of security for a range of products in the mobile, automotive, digital home, IoT, and cloud computing markets. These integrated solutions enable the heart of many security standards, supporting confidentiality, data integrity, user/system authentication, non-repudiation, and positive authorization.

Synopsys' security IP helps protect your SoC against a wide range of evolving threats.

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors, and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits, and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enable designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit synopsys.com/designware.