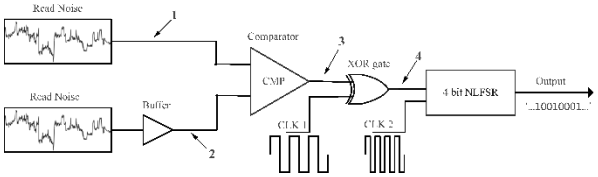
TO-197 • PT 1.3100
Peter Grünberg Institute
Electronic Materials (PGI-7)

ENDEAVOURS
science creating solutions

Advanced Random Number Generator for Secure Cryptographic Applications

Technology Description

Our new technology provides an innovative method for a random number generator (RNG) that can be used to generate cryptographically secure random numbers. As input signal for the current response of a memristive device to a square pule is used. The variation of the current response is called read noise. The length of the pulse can be chosen deliberately. It is suggested to use memristive devices with a large energy gap between oxygen vacancy level and conduction band to maximize the read noise. For the generation of random numbers the signal is split, one half is delayed and then both halves are compared. After comparison the signal already can be utilized as random number. Alternatively, the entropy and generation rate can be enhanced. For this purpose, the result of the comparison together with the clock signal CLK1 is fed into an XOR gate and subsequently used as a seed for a non-linear feedback shift register (NLFSR). The output of this circuit was demonstrated to meet the requirements for random numbers. The process is repeated to generate a sequence of bits until the desired length is reached. The use of memristors as a core component enables the hardware near generation of random numbers and ensure a high degree of randomness in the output.



Problem

In the field of cryptography, the generation of secure random numbers is of major importance. Conventional random number generators are often based on algorithms that are predictable, which makes them vulnerable to attack as malicious actors can replicate the random numbers. The generation of secure random numbers in novel computing system is thus of major interest to prevent side-attacks on the data transferred between components of the computer. Here, it is most convenient to utilize the variability of devices already cointegrated on-chip enabling the hardware-based generation of random numbers with scalable generation rate. There is an urgent need for new approaches that not only increases the unpredictability of the generated random numbers, but also improves the speed and reliability of the generation process.

IP
DE102024204563.2
Further patent filing is being pursued.

TRL
3

Contact
Scientific Contact
Kristoffer Schnieders

Innovation Manager
Dr. Jörg Bohnemann

Keywords
Memristor, Cryptographic Random Number, Signal Processing & Conversion, NIST Test, Valence Change Mechanism, VCM, Secure Encryption

More Information
go.fzj.de/to-197

As of 08/2024

Solution

Our random number generator significantly increases the unpredictability of the numbers generated, making them suitable for cryptographic applications where security is of primary importance. By using a combination of analogue signals and advanced processing techniques, the generator produces random numbers that pass rigorous testing standards such as the NIST test for randomness by the US National Institute of Science and Technology. Secondly, the invention improves the speed of random number generation, enabling the rapid production of large quantities of secure numbers, which is essential for high-demand applications. In addition, the technical requirements for implementing this generator are relatively low, making it accessible to various applications without the need for extensive hardware investment. This combination of efficiency, security and cost-effectiveness makes the new invention a superior alternative to existing cryptography technologies.

Potential Use

The new random number generator offers a wide range of applications. The RNG can be integrated in computing-in-memory units to allow for the encryption of data transfer within the computer. The random numbers can also be used for software applications that require random numbers for simulations, games or statistical sampling. The generator's ability to quickly generate high-quality random numbers makes it ideal for real-time applications such as secure communication and online transactions. In addition, the generator's low technical overhead makes it easy to integrate into existing systems, making it an attractive option for organisations looking to improve their security protocols without a large investment. Overall, this invention opens up new paths for secure data processing in an increasingly digital world.

Development Status and Next Steps

Forschungszentrum Jülich (FZJ) has extensive expertise in this field and holds several patents. Our technology described above is continuously being enhanced. Our Peter Grünberg Institute – Electronic Materials (PGI-7) both already cooperate with numerous national and international companies and scientific partners. Forschungszentrum Jülich focuses on energy and cost-efficient devices suitable for application in various emerging technologies. We are thus constantly seeking cooperation partners and/or licensees in this field and adjacent areas of research and applications.

IP
DE102024204563.2
Further patent filing is being pursued.

TRL
3

Contact
Scientific Contact
Kristoffer Schnieders

Innovation Manager
Dr. Jörg Bohnemann

Keywords
Memristor, Cryptographic Random Number, Signal Processing & Conversion, NIST Test, Valence Change Mechanism, VCM, Secure Encryption

More Information
go.fzj.de/to-197

As of 08/2024