Approach for High-Performance Random Number Generators for Critical Systems

Pascal Hammer, Veronika Krause, Tobias Probst, Jürgen Mottok

Approach for High-Performance Random Number Generators for Critical Systems

Pascal Hammer, Veronika Krause, Tobias Probst, Jürgen Mottok
Laboratory for Safe and Secure Systems (LaS³)
Technical University of Applied Sciences Regensburg
93053 Regensburg, Germany
{pascal.hammer, veronika1.krause, tobias.probst, juergen.mottok}@oth-regensburg.de

***Abstract*—In times of digitalization, the encryption and signing of sensitive data is becoming increasingly important. These cryptographic processes require large quantities of high-quality random numbers. Which is why a high-performance random number generator (RNG) is to be developed. For this purpose, existing concepts of RNGs and application standards are first analyzed. The proposed approach is to design a physical true random number generator (PTRNG) with a high output of random numbers. Based on this, the development begins with the analog part of the RNG, the noise signal source and a suitable amplifier for the analog noise signal. Therefore, a special noise diode from Noisecom and an amplifier from NXP were chosen and analyzed in different measurements. From the results of the measurements, it can be concluded that both components are suitable for use in the RNG.**

***Keywords*—RNG, Random Number Generation, Noise Source, Random Processes, Cryptography, Random Sequences**

I. Introduction

Due to the increasing demand of cryptography in communication and other domains, more attention falls to random numbers, which feature high entropy and are evenly distributed, and their generation. One distinguishes between true random processes like thermal noise, quantum mechanical effects or atomic decay processes on one hand and pseudo random numbers which seem genuine but are generated by a deterministic process on the other. True random numbers have a higher quality than pseudo random numbers, and are therefore mandatory for the proper function of many cryptographic processes. In cryptography, random numbers are used, for example, to generate keys for cryptographic procedures or non-deterministic padding. For the correct and secure functionality of these applications, it should not be possible to guess the random numbers or parts of them.

In enterprise environments on server, where many connections are established in a short time, exists a high demand for cryptographic keys. In fact, there are random numbers required in high frequency to seed the key generation. This point is in contrast with the fact that physical true random number generators (PTRNG) require more time to generate random numbers than deterministic random number generators (DRNG), which means they are too slow to meet the requirements of the cryptographic components. PTRNGs however generate random numbers with a higher rate, but have the disadvantage of being deterministic.

This is the main reason why the focus of this research is on the approach of developing a high-performance random number generator (RNG). The first idea of the approach is to evaluate whether a PTRNG can be realized with a suitable performance for these applications. The aim is to get as much performance as possible out of a PTRNG, and then combine it with a DRNG to cover applications that require even more throughput. The result is a hybrid RNG with a higher performance than a PTRNG and better random numbers than a DRNG. Regardless of the approach, determining the maximum achievable performance of a PTRNG is a suitable first step. Furthermore, the economic viability of the developed solutions has to be considered. This also means evaluating the use of cheaper or off-the-shelf components for the RNG. Irrespective thereof, the different RNGs should be a tradeoff between price and quality.

The Federal Office for Information Security (BSI) is the central authority for IT security in Germany. The objective of the BSI is to preventively promote cybersecurity to enable and support the secure use of information and communication technology in society. The BSI provides support to ensure the issue of IT security, and minimum standards and guidelines are developed and published to support users in avoiding risks or strengthening their systems. Regarding RNGs, there is the technical guideline TR-02102 [2] which contains recommendations for the key length in cryptographic systems but also includes information about the use of RNGs. For certification of RNGs in Germany, the AIS 20 (for deterministic RNGs) and the AIS 31 (for physical true RNGs) are mandatory [3]. These two application notes define the different classes of random number generators, PTG.1 to PTG.3 and DRG.1 to DRG.4, and their mathematical background. An overview of the RNG classes is depicted in Fig. 1. The nomenclature in this paper is based on the naming convention in the AIS20/31.

This paper aims to answer the following research questions:

- How can a high-speed noise signal source be realized?
- How and from which properties of the noise signal can conclusions be drawn about which properties of the raw random numbers (before post-processing)?

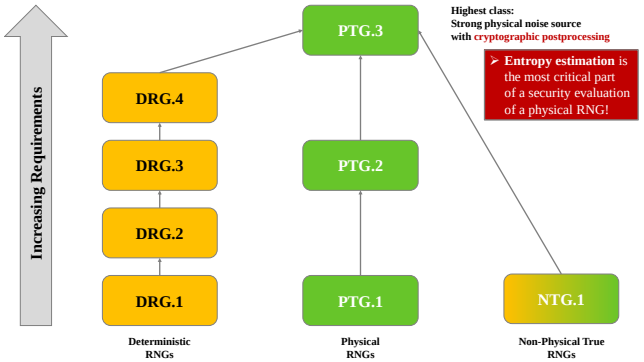

Fig. 1. Overview of the RNG classes [1]

- How must the analog noise signal be amplified so that good digitization is possible?

The paper is structured as follows: Section II shows the current state of the art regarding the RNGs, especially the application notes of the BSI. Chapter III provides a review of existing RNG concepts. Chapter IV gives an overview of the proposed approach of the research work. In Section V, the intermediate results are described. And Chapter VI concludes the paper and gives an outlook to the future work.

II. Current state of the art

Random number generators are divided into three types:

- The physical true RNGs (PTRNGs), which are based on physical phenomena like thermal noise or atomic decay processes, for example.
- The deterministic RNGs (DRNGs), which generate pseudo random bit sequences out of one initial random value called seed.
- Non-physical and non-deterministic RNGs, which are used if there is no certain cryptographic hardware available (beyond scope of this paper).

Each type consists of different classes, higher numbers indicate that an RNG provides better security capabilities, while the requirements to be met by the RNGs are consequently also increasing. According to the AIS20/31 workshop in June 2023, the classes DRG.1 and PTG.1 have been dropped because they are no longer sufficient for the required security features [1].

A. Physical true RNGs (PTRNGs)

One type is the physical true RNG based on specific hardware to generate true randomness, which means generating unpredictable random numbers. Calculating previous or subsequent random numbers based on known sequences and the physical environmental conditions at the time of generation must not be possible. The generation of random numbers is based on the unpredictable behavior of electronic circuits, like thermal noise etc. Reducing bias or dependencies between the random numbers can be achieved by a deterministic post-processing of the noise raw data (the digitized noise signals). But post-processing can also have different objectives like statistical inconspicuousness or entropy extraction, for example increasing the entropy per bit. [3]

A common deficit of PTRNGs is the slowness compared to other RNGs due to the fact that the generation of random numbers is more time-consuming due to the amplification and digitization of the raw analog noise signal. The bottleneck is therefore the more complex processing of the analog signals. Changes of the environmental conditions like temperature, electromagnetic fields etc. may impact the the generated random numbers. PTRNGs are also more difficult to evaluate in comparison to DRNGs because, due to the lack of standards of how an RNG should be set up, they can take on many different forms and utilize various physical phenomena as an underlying technology. [3]

The technical guideline TR-02102 recommends using a generator according to PTG.3, if a physical true RNG is required in an application. The recommendation applies in particular to generating keys for calculating signatures and to Diffie-Hellman based key exchange. For some applications, PTG.2 generators are sufficient, e.g. for the production of keys for symmetric encryption or seed generation for a deterministic RNG of class DRG.3 or DRG.4. Random numbers produced by PTG.2 RNGs feature high entropy but do not foreclose statistical dependencies. PTG.2 generator can be appropriate if it can be proven, that the potential advantage to an attacker caused by these dependencies is difficult to exploit. But nevertheless, it is not recommended to use a PTG.2 RNG directly. An RNG of class PTG.2 can be upgraded to a class PTG.3 generator using cryptographic post-processing, which is usually implemented as a software component. The following example of post-processing, shown in Fig. 2, is based on the Davies-Meyer compression function [4]. The raw random numbers from the RNG are divided into 128 bit blocks M_i where each block is XORed with 128 bit values (z_1 and z_2) from the digitized noise source and AES-128 encrypted afterwards. The results of the AES-128 encryption and the initial 16 byte block are XORed again to produce the final block of secure random numbers. The purpose of the post-processing is to increase the entropy of the random numbers and to eliminate statistic anomalies [5].

RNGs of classes PTG.2 and PTG.3 must comply with the following properties [2]:

- It is possible to describe the statistical properties of the random numbers with a stochastic model, capable of reliably entropy estimating.
- The average increase of entropy per random bit is above a defined minimum (near 1).
- Statistical weaknesses or deterioration must be detected within a reasonable time through statistical tests during operation.
- A total breakdown of the noise source or an unacceptable change of the random numbers must be detected immediately. In this situation, an alarm signal must be triggered. The generation of random numbers must be ceased after a breakdown occurs.
- This property is only relevant for PTG.3 generators: A strong cryptographic post-processing ensures a security level of a DRG.3 generator despite total breakdown of the noise source.

B. Deterministic RNGs (DRNGs)

The following section describes the second type of RNGs, the deterministic generators. DRNGs extend short random sequences, handed over as seed from an entropy source, to very long random bit sequences in a deterministic way. Although the bit sequences look random, the total entropy can never be larger than that of the seed. Depending on the generator, the seed can be renewed during its service life. [3]

The DRNGs have the advantage over PTRNGs to be less difficult to evaluate because the computational security can be evaluated independently of its implementation and there are also some approved standard DRNG mechanism. This is not possible for PTRNGs, where the same design may behave completely different with different hardware. [3]

The inner state of the generator is initialized with the seed value. Within every step, the inner state of the generator is updated, the random numbers are derived from this state and the values are issued as bit sequence with fixed length. Hybrid deterministic RNGs update their inner state in a process called reseed or seed update with true random values. This process can be cyclic or triggered by the application. The inner state of the RNG must always be protected against

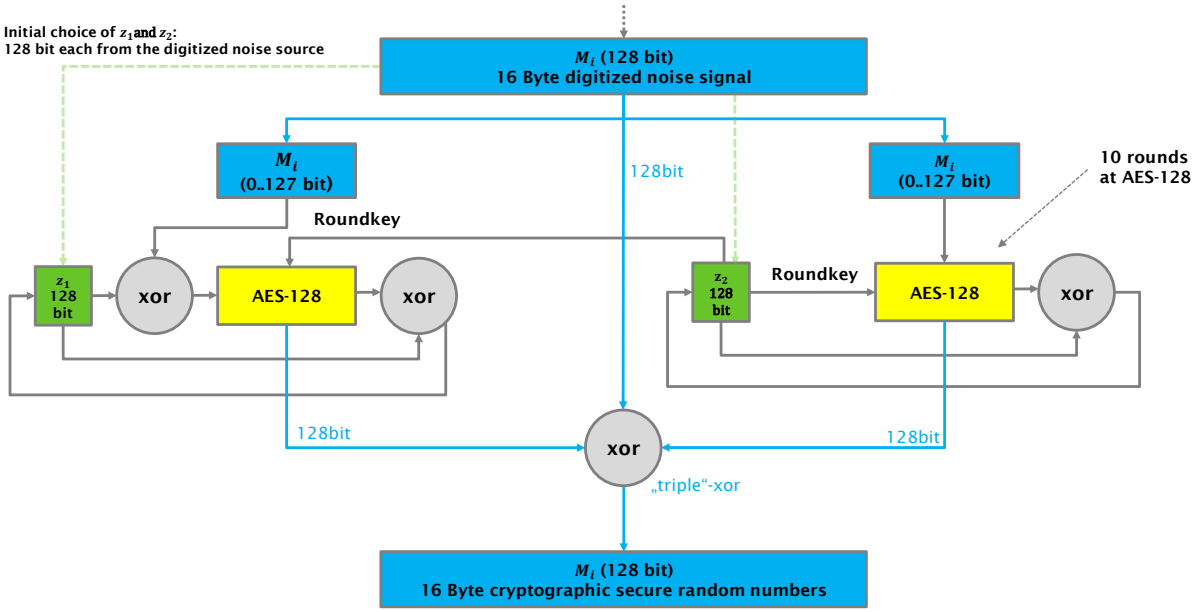

Fig. 2. Cryptographic post-processing based on the Davies-Meyer compression function [4]

access and manipulation, especially during reseed. If a deterministic RNG is required in an application, it is recommended to use a generator of class DRG.3 or DRG.4. For the DRG.3 class, a regular inflow of new entropy is required. However, this property is not sufficient to fulfill class DRG.4. For conformity with DRG.3 respectively DRG.4, the RNG must comply with the following requirements [2]:

- It is not possible for an attacker to calculate the predecessor or successor for a known subsequence of random numbers or to estimate one of them with a higher probability as without knowing the partial sequence.
- For an attacker with knowledge of the inner state, it is not possible to calculate previously issued random numbers or to estimate the numbers with higher probability as without knowing the inner state.
- If the RNG should be upgraded to DRG.4, there is another requirement to be met. Even with knowing the inner state of the generator, the attacker should not be able to calculate the random numbers which are generated after the next reseed/seed update or estimate them with higher probability as without knowing the state. [2]

Using inappropriate RNGs should be avoided because it can weaken strong cryptographic mechanisms. The most important property of the generators is the unpredictability and secrecy of the inner state at all times. For a good quality of the random numbers, they should be evenly distributed on $\{0, 1\}^n$. To achieve this, the individual bits of the random sequences must be independent of each other and the history. [2]

Basically, PTG.3 and DRG.4 generators have greater resistance against side channel attacks in comparison to PTG.2 and DRG.3. In side channel attacks, the principle is to observe the RNG and find correlations between observed data and generated random numbers. Characteristic information can be obtained, for example, by analyzing the runtime or energy consumption of the RNG. Attacks interfere with the device and provoke errors during execution. Due to the steady inflow of new entropy at PTG.3 and DRG.4 RNGs, side channel attacks regarding the cryptographic post-processing become more difficult. The attacker is not able to combine information about the inner state at consecutive points of time. Besides side channel attacks, there is a higher risk of long-term compromise of RNGs of class DRG.3 compared to DRG.4 and PTG.3 when the RNGs generate long random sequences from one single seed value. [2]

RNG class	Properties
DRG.3	calculation of predecessor or successor of known subsequence not possible, not even with knowledge of the inner state
DRG.4	calculation of predecessor or successor of known subsequence not possible, not even with knowledge of the inner state, calculation of random numbers after reseed not possible
PTG.2	statistical model to estimate entropy, statistical tests during operation, detection of breakdown and alarm signal, automatic deactivation of noise source
PTG.3	statistical model to estimate entropy, statistical tests during operation, detection of breakdown and alarm signal, automatic deactivation of noise source, cryptographic post-processing

C. Non-physical and non-deterministic RNGs

The third type of RNGs are the non-physical and non-deterministic generators (NTG). These are used in particular for cryptographic applications when neither a deterministic nor a physical RNG is available, as these applications are generally run on computers without certified cryptographic hardware. Typically, entropy is gained from system data (timing values, random access memory (RAM) data, etc.) or user's interaction (mouse movement, keystrokes, etc.). NTGs are beyond scope of this research because they are completely based on deterministic random numbers and therefore not suitable for cryptography. [2]

D. Hybrid RNGs

An RNG is called hybrid DRNG if it accepts additional input or if it is able to trigger a seeding/reseeding procedure. Hybrid RNGs use design elements from both DRNGs and PTRNGs. The combination aims to increase the computational complexity of the output sequence and also to increase the entropy per bit. A cryptographic post-processing applies additional security to the RNG in case the entropy per bit is smaller than assumed.

The security of a hybrid deterministic RNG of class DRG.4 is based on the complexity of the deterministic part of the RNG. Backward secrecy and forward secrecy should be ensured by the algorithmic properties of the DRNG alone and without relying on any entropy in the additional input data. Backward secrecy is the assurance that previous random numbers cannot be determined from the knowledge of current or subsequent random numbers, whereas forward secrecy means, it is not possible to determine subsequent random numbers from current or previous random numbers.

Originally, the functionality classes DRG.2 and DRG.3 were designed for pure DRNGs, but the AIS20/31 also covers hybrid DRNG designs. The functionality class DRG.4 defines requirements for all DRNGs, but these can only be fulfilled by hybrid DRNGs. Hybrid random number generators of class PTG.3 utilize a strong noise source and powerful cryptographic post-processing. [2] [3]

E. Test suites

The quality of random number generators can be determined with the help of statistical test suites. The following gives an overview of the NIST- [6] and Dieharder-Suite [7]. The NIST provides a test suite, which consists of 15 statistical tests, freely available on their website [6]. The suite was developed to test the randomness of arbitrarily long binary sequences produced by any type of RNG. Thereby, the tests focus on different types of non-randomness that could exist in a sequence. [8]

The Dieharder random number generator test suite is an open-source project developed and maintained by Robert G. Brown. This suite is the expansion and optimization of the original Diehard test suite introduced by George Marsaglia in 1995 [9]. It also includes tests of the NIST test suite and a variety of tests contributed by users, introduced by the Dieharder contributors or implemented from descriptions in literature. The test suite aims to provide a universal set of tests for random numbers. [10]

However, both test suites cannot definitively determine whether an RNG deliver true random numbers, they can only detect statistical correlations between the generated random numbers and mark the generators as weak in this case. [10]

F. General PTRNG structure and basic parts

In most cases, PTRNGs are designed and afterward evaluated for their security by independent institutions or companies. As only a limited number of laboratories are approved for certification, it is important and simplifies the process when the PTRNG designer and the certification institution use the same vocabulary and definitions.

Therefore, this section provides an overview of the general structure of a PTRNG and the main components that must be included. The main function of the PTRNG is to produce a series of unpredictable bits or binary numbers. The PTRNG is based on an unpredictable physical phenomenon, the output of which must be converted into a series of bits or numbers.

Since the majority of PTRNGs are based on analog physical effects, a component that performs the analog to digital conversion is an essential component of the PTRNG. For this reason, the following four basis blocks are required for PTRNGs [11]:

- Source(s) of randomness
- An analog-to-digital converter (ADC)
- A post-processor
- Embedded tests

An overview over the general structure is depicted in Fig. 3. The PTRNG usually contains one or more sources of randomness, each generating an analog signal. These analog signals are converted into a stream of bits with the help of an analog-to-digital converter. The ADC outputs a stream of random numbers in bits or multi-bit values, which may still be of poor statistical quality at this point. If necessary, this low statistical quality can be improved by an algorithmic post-processor to obtain a high-quality digital noise.

Using embedded tests according to predefined testing procedures, the quality of the generated random numbers is continuously monitored during the operation of the PTRNG. At least two tests should be carried out: one initial test at startup of the RNG for correct operation, and one function for continuous monitoring. [11]

This section described the different types of RNGs and also how the classification works for RNGs. PTRNGs have some advantages in comparison to DRNGs, but are therefore more complex. Hybrid RNGs combine the benefits of both types and thus offer a good intermediate solution. All RNGs can be tested with the help of statistic test suites. After this overview, the next section gives some examples of existing RNGs.

III. Related Work

This section describes and analyses existing RNG concepts and thus creates a basis for comparison for the newly developed RNG.

The first RNG to be analyzed is the Quantis QRNG engineered by the company ID Quantique [12]. This generator is a physical RNG based on a quantum optics process with a maximum rate of random data of 4 Mbit/s. The device functions by emitting photons one by one towards a semi-transparent mirror and their reflection or transmission events are detected and associated with the bit values 0 and 1. In comparison to other noise sources, quantum RNGs are less vulnerable to environmental perturbations, as the underlying

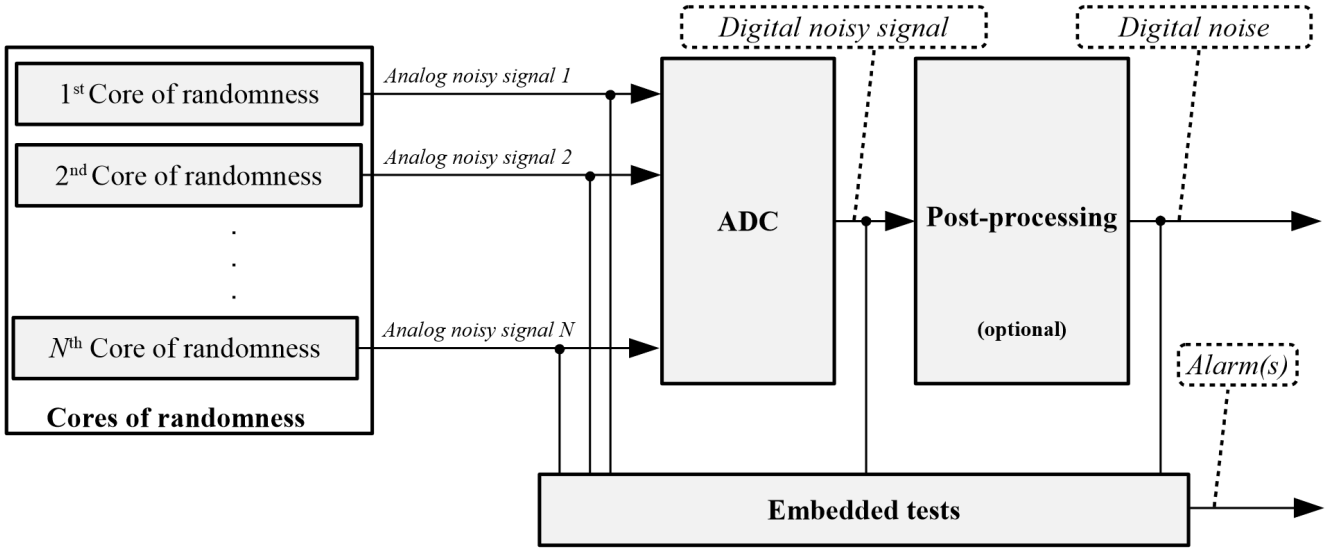

Fig. 3. General structure of PTRNG [11]

processes, for example light, have no dependencies to temperature or electromagnetic fields. On the other hand, as a manipulation attempt, laser light or the sending of photons onto just one of the detectors could compromise the produced noise signal. To avoid this, the hardware of the generator and the random numbers are continuously monitored and if a failure is detected, the random bit stream is immediately disabled.

The next RNG is the PRG310 developed by the IBB engineering office Bergmann [13]. This RNG is based on Z-diodes as thermal noise source for a continuous generation of random numbers for the classes PTG.2 and PTG.3 with a continuous random number bit rate of 300 kBit/s. A permanent monitoring of statistical properties of the digitized noise data verifies the quality of the random numbers.

The PRG700, also developed by the IBB engineering office Bergmann [14], is the third object of comparison. This RNG is designed on a small printed circuit board (PCB) for integration in other applications. It also uses thermal noise as an entropy source and continuously generates random numbers. But the RNG is not as fast as the PRG310, therefore it is only suitable for low bandwidth applications, because the maximum data rate for random numbers is 40 kBit/s for this RNG.

The last tested RNG is a smart card of the company Atos, which is classified as PTG.3 and includes cryptographic post-processing [15]. The smart card is based on the SLE78 security crypto controller developed by the semiconductor manufacturer Infineon [16]. This controller is recommended for applications like ID cards, passports or electronic signatures. For the smartcard, no data rate is specified for the output of the random numbers, but it is to be expected that it can output significantly less random data than the RNGs described above because typical smartcard applications only sporadically require random numbers for cryptographic applications.

The aim of this research approach is to achieve better performance than the RNGs described above. Performance describes in this case the maximum possible data rate in bit per second for random data.

IV. Proposed Approach

The subsequent section outlines the initial step in the development approach for a high-performance Random Number Generator (RNG). This includes the noise signal source and the amplification of the analog signal. A short preview of the further steps of the development process are presented at the end of the section, but they are part of future work.

Initially, this work focuses on the development of a PTRNG to assess its maximum performance as a standalone solution without integrating it into a hybridized approach. Performance is in this context defined as the number of generated random bits per second. In addition to performance, the quality of the generated random bits, the resilience against external interferences and the reproducible implementation has to be taken into consideration either. If this is not satisfactory, a hybrid RNG is to be developed as a second variant. The aim is to evaluate the impact of the hardware components on the quality of the generated random numbers. Atomic decay processes are not used as noise source in this research as these processes are too slow and radiation sources in RNGs are unsafe because, in this case, the RNG would have to be shielded against so that no radiation reaches the outside.

The initial step of the development process is the selection and analysis of adequate noise signal sources for a TRNG. During our research, the choice fell on the Noisecom NC302BL diode [17] which is to be investigated as a potential noise source for a first approach. The Noisecom diodes are suitable for broadband noise generation because they are optimized for this purpose. Theoretically, all Noisecom diodes have these properties, but to ensure the ideal performance, the best ones are hand-picked for performance characteristics from all those produced. According to the datasheet, the diodes deliver symmetrical white Gaussian noise and flat output power across the frequency band from 10 Hz to 3 GHz. In order to perform tests on the Noisecom diode, a PCB with the reference design as noise source according to the datasheet was developed. This PCB facilitates the investigation of the frequency spectrum of the noise source. The frequency response should be nearly horizontal because

the power should be as independent of the frequency as possible. [17]

The analog signal of the noise signal source only provides low output power. That is why a suitable amplifier is needed to amplify the signal for its digitization, otherwise the amplitude of the signal is too low for the hysteresis of the digitizing circuit. A relevant feature for the selection of the amplifier is the possible bandwidth. The amplifier is tested in combination with the noise source. Since the gain of the amplifier also has a certain dependence on the frequency, this characteristic can be used to improve the frequency response of the noise source. This means that the combination of noise source and amplifier offers a more horizontal frequency response than the individual components.

According to the required features, the NXP BGA2818 was selected as a suitable amplifier for the RNG. It is a wideband amplifier for frequencies up to 2 GHz with a maximum gain of +30 dB. The BGA2818 delivers a nearly constant gain over the complete frequency range. For the initial testing of the amplifier itself and in combination with the noise signal source, both parts are designed according to their reference circuits on individual PCBs. This simplifies the test process and offers the opportunity to use different components if one of them does not fulfil the expectations. The overview of these building blocks is depicted in Fig. 4. This figure also includes the digitization of the noise signal and the microcontroller, which are part of future work. After all components are tested on their individual PCBs, the complete circuit will be united on one PCB.

There are two options for the digitization of the amplified analog signal. Either using a comparator or with the aid of an analog to digital converter (ADC). The ADC needs to be fast enough so that the analog signal is sampled correctly.

The digitized noise signal is processed with the help of a microcontroller. The controller collects bits from the ADC and prepares the bit sequences for the cryptographic post-processing. This is the last step before the random numbers are ready for use in an application, which is done using a software component on the microcontroller. Via a defined interface, the random numbers are provided to the application demanding them. During the whole process, the controller needs to monitor the random bits in the event that errors occur in the process, such as the failure of the noise signal source or a deterioration in the quality of the random data due to external influences like temperature changes or electromagnetic fields.

The proposed approach is described in this section, starting with the analog part of the RNG, the noise signal source and the amplification of the analog signal. During the research, a special diode was chosen as noise signal source according to the characteristics described in the datasheet. To provide a analog signal for digitization, the analog signal of the noise sources needs to be amplified. Therefore, a suitable amplifier was also chosen. The intermediate results with both components are presented in the following section.

V. Intermediate Results

The following section describes the intermediate results achieved so far. Starting with the noise signal source and the amplifier up to the combination of both components.

A. Noise signal source (Noisecom NC302BL)

For the first approach, the Noisecom NC302BL is chosen as noise source to be evaluated because it is developed for this use case. To ensure a comparable test environment, a PCB with the reference circuit mentioned in the datasheet, is created for the Noisecom diode. In addition, the output signal is routed via a SMA connector to ensure a better connection to the measuring device. The operating point of the diode, that is defined by the current flowing through it, is adjustable via a potentiometer.

With the help of this setup, the analog noise signal of this diode could be measured with an oscilloscope depicted in Fig. 5. The figure shows a section of the noise signal produced by the diode with a voltage level of 2 mV peak-to-peak. This voltage level is too low for direct digitization, which means an amplification is required to digitize the signal properly. No direct statement can be made about the quality of the signal on the basis of the chronological sequence. For this, the frequency spectrum of the signal must be analyzed.

The power density spectrum was also measured up to a frequency of 3 GHz with the PCB described before using a spectrum analyzer. The result of this measurement is the almost horizontal frequency response across the entire range depicted in Fig. 6. This is important for the frequency response because the power should be as independent of the frequency as possible, making predictions about the random numbers much more difficult. Otherwise, it would be possible to see at which frequencies more power is transmitted and thus draw conclusions about the noise signal. Since frequencies above 600 MHz are the mobile radio frequencies (which are recognizable in the spectrum) the RNG to be developed must either be shielded or suppress these frequencies using a filter.

To analyze the electromagnetic compatibility (EMC) resistance of the board, it was tested in an EMC laboratory under the influence of electromagnetic fields. The test board is irradiated with fields of different frequencies and field strengths to investigate the influence on the spectrum. The result is displayed in Fig. 7 where the yellow signal shows the maximum, the green one shows the average and the orange signal shows the minimum of the spectrum. The influence of the electromagnetic fields is clearly visible at the two peaks in the low frequency range. This means that the noise signal source can be influenced by electromagnetic radiation and must be shielded against EMC influence. Alternatively or additionally, other methods such as the use of a differential amplifier could be used. This requires two noise signal sources, whereby the difference between the two noise signals is first formed and then amplified. In this way, interference affecting both noise sources simultaneously can be eliminated.

B. Amplifier (NXP BGA2818)

Due to the fact that the amplitude of the noise signal is only 2 mV peak-to-peak, the signal needs to be amplified to be digitized properly and with a sufficient resolution. For this purpose, the NXP BGA2818 is selected as amplifier for the RNG. This component is a monolithic microwave integrated circuit (MMIC) wideband amplifier with an internal matching circuit to 50 Ω and a nearly constant gain of +30 dB over its complete frequency range. The special feature of this type of

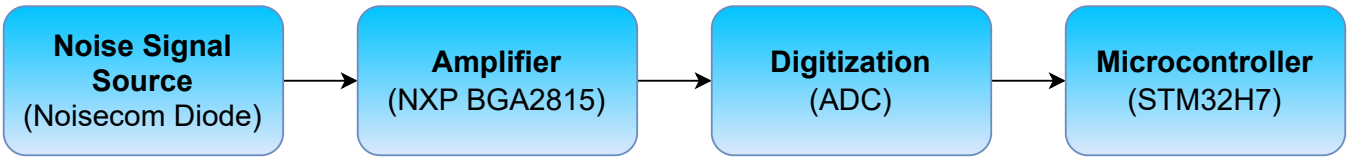

Fig. 4. Building blocks of the hardware development process

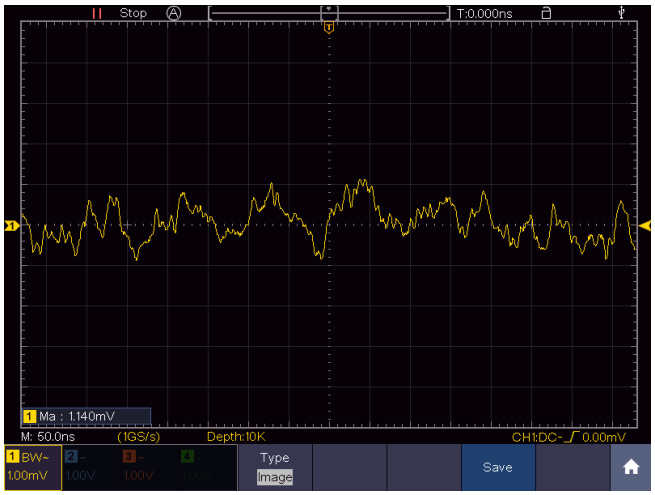

Fig. 5. Noise signal of the NC302BL

component is the integration of all active and passive components on a semiconductor substrate. This miniaturization enables the design of circuits down to the millimeter wave range.

However, since an amplification of +30 dB is not sufficient to generate a signal with adequate amplitude, an amplifier stage consisting of two BGA2818 in series was designed on a further test PCB. This corresponds to the procedure mentioned in the previous section of first realizing the individual components as building blocks. After each block is tested individually, they are combined on a common PCB.

To reduce the influence of the power supply to the amplifier and the analog noise signal, the LTM8080 from Analog Devices is chosen as a component for low noise voltage supply. At this stage of development, the LTM8080 is used with the help of a development board. Later on, this will also be integrated on a custom PCB with the other components of the RNG. The LTM8080 can be supplied with a voltage from 6 V to 40 V and generates from this a selectable output voltage from 0 V to 8 V with a ripple in the µV range. [18]

Fig. 6. Power density spectrum of the NC302BL

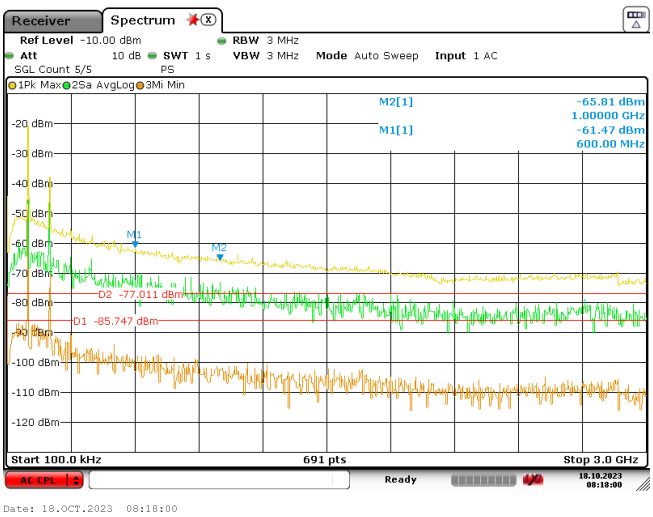

Fig. 7. Power density spectrum of the NC302BL under EMC influence

Fig. 8. Spectrum of the BGA2818

In Fig. 8 the spectrum of the BGA2818 with a constant reference signal over the frequency range from the spectrum analyzer is depicted. The reference level before amplification is at -60 dB (light blue horizontal line). There are placed four markers in the spectrum at different frequencies, showing the level at these points of the spectrum. Until marker 4 at 1 GHz, the figure shows a nearly horizontal spectrum, which means that the amplifier works as expected for this frequency range. According to the level at the markers, the gain is slightly below the ideal 60 dB that two amplifiers of this type can theoretically achieve when connected in series.

This means, the BGA2818 is suitable for use in this RNG development. The test PCB amplifies the noise signal up to about 2 V peak-to-peak so that the amplitude of the signal fits for the digitization. However, it must be taken into account that a direct current (DC) voltage offset needs to be added to the voltage signal for digitization. Without this DC offset, the voltage signal can also take on negative values, which can lead to problems during digitization. If digitization is carried

out using an ADC, for example, it could be damaged by the negative voltages because their operating range is between 0 V and typically 3.3 V.

C. Noise signal source and amplifier in series

After testing the noise signal source and the amplifier individually, the combination of them is to be tested as a next step. The aim is to exclude the possibility of interactions between the two PCBs.

The amplified noise signal has an amplitude of 2 V peak-to-peak. As the signal oscillates around the voltage level of 0 V after amplification, a DC offset of VCC/2 should be added to the signal. This means that the analog signal is exactly in the middle between 0 and VCC and can be digitized with an ADC, for example. To protect the digitization circuit, the voltage signal must be also limited to the maximum input voltage of the circuit.

Since the combination of the two boards provides an amplification gain of +60 dB, an emission measurement is then carried out, because interference frequencies are also amplified when they reach the high frequency signal line. This involves measuring whether the circuit boards emit electromagnetic fields and, if so, at what frequency they are located. This ensures that other parts of the RNG or other devices are not influenced or disturbed by the amplifier circuitry.

For this measurement, the structure consisting of the noise signal source and amplifier was placed under a stripline and the radiation of the two boards was measured with its help. The result of the measurement over the frequency range from 100 kHz to 6,25 GHz is depicted in Fig. 9. Up to a frequency range of around 2 GHz, the amplitudes of the signals at the various frequencies are below -80 dBm, which means that the emission of the PCBs in this range is very low. Only two peaks at about 2 GHz and 2,8 GHz attract attention, because the amplitudes at these frequencies are above -60 dBm and thus significantly higher than the remaining frequency spectrum. Although this is noticeable, it is not critical for the time being. The two peaks occur because the matching of the high frequency tracks on the two PCBs is not optimal. This is improved when the components are integrated onto a common circuit board at a later stage.

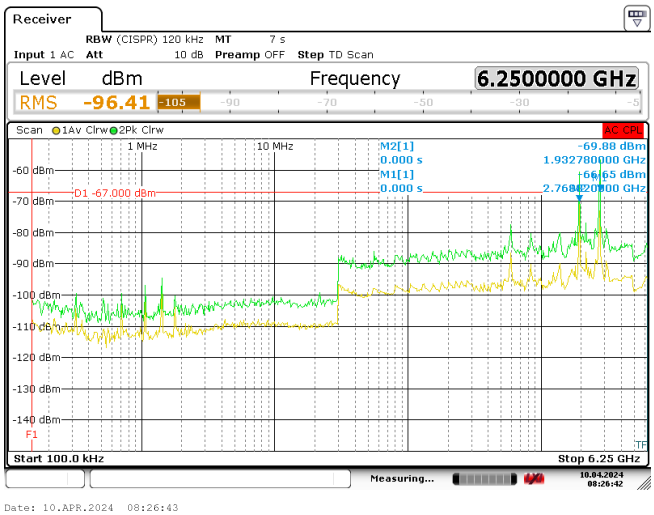

Fig. 9. Emission measurement of noise signal source and amplifier

VI. Conclusion and Outlook

In conclusion, the demand for high-quality random numbers is high due to the increasing use of cryptography. A distinction is made between deterministic RNGs, physical true random generators and non-deterministic RNGs, each consisting of different classes with special properties. For some applications, certain classes are recommended to meet the security requirements. Physical true RNGs are preferable to deterministic RNGs due to the fact that they use unpredictable behavior of specific hardware components like thermal noise as a base for the random numbers. The quality of the random number generators can be evaluated with the help of statistic test suites like the NIST test suite and the Dieharder suite.

The aim of this approach is the initial step in the development approach for a high-performance RNG. Therefore, first a suitable noise signal source is selected based on a frequency spectrum analysis and also a fitting amplifier to prepare the analog signal of the noise signal source for digitization.

For the tests of the first noise signal source, a PCB was developed, and the noise signal measured with an oscilloscope. Measuring the power density spectrum with a spectrum analyzer, the Noisecom diode shows a nearly horizontal frequency response, marking it as a promising candidate. Tests in the EMC laboratory for the influence of electromagnetic fields with different frequencies and field strengths show that the output signal is affected by those fields. Hence, a shielding of the noise source or the whole RNG is necessary.

Since the noise signal has only low power, it needs to be amplified for later digitization. Therefore, the NXP BGA2818 was chosen as an amplifier for the analog noise signal. This amplifier is a MMIC wideband amplifier with a nearly constant gain of +30 dB over its complete frequency range. Due to the low amplitude of the analog signal, two BGA2818 in series are designed on another PCB to test the amplifier individually and in combination with the noise signal source. With this two-stage amplifier circuit, a suitable signal for digitization can be achieved.

This paper focuses on the analog part of the high-performance RNG, thus the noise source and the amplification of the noise signal are of interest. Initially starting with the Noisecom diode and a suitable amplifier, in a later step, other noise sources should be tested and compared.

The next step after amplifying the noise signal is the digitization of the noise data and the statistical evaluation with an associated model. An important aspect is the cryptographic post-processing of the generated random numbers to meet class PTG.3 of the RNGs. In addition, the RNG must also provide online-tests to monitor the correct functioning and quality of the random data during the runtime. The digitization, statistical evaluation, cryptographic post-processing and the online-tests are part of future work.

Acknowledgment

The presented work is part of the research project *KRITIS Scalable Safe and Secure Modules* (KRITIS³M), which is funded by the Project Management Jülich (PtJ) and the German Federal Ministry for Economic Affairs and Climate Action (BMWK) under funding code 03EI6089A.

REFERENCES

[1] Peter, Matthias and Schindler, Werner. (2023, June) Deterministic RNGs (DRNGs). Publication. Accessed: May 5th, 2024. [Online]. Available: https://www.nist.gov/system/files/documents/2021/05/28/BSI%20Update-Schindler.pdf

[2] Bundesamt für Sicherheit in der Informationstechnik. (2023, January) Technische Richtlinie TR-02102 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Publication.

[3] ——. (2023) A Proposal for Functionality Classes for Random Number Generators. BSI. Accessed: May 5th, 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=7

[4] Frank Bergmann. (2023) Welche Anforderungen werden an kryptografisch sichere Zufallsgeneratoren gestellt? IBB Ingenieurbüro Bergmann. Accessed: May 5th, 2024. [Online]. Available: https://www.ibbergmann.org/GRUNDLAGEN/

[5] A. M. Garipcan and E. Erdem, "A gigabit TRNG with novel lightweight post-processing method for cryptographic applications," *The European Physical Journal Plus*, 2022, Firat University.

[6] National Institute of Standards and Technology. (2023) NIST SP 800-22: Download Documentation and Software. National Institute of Standards and Technology. Accessed: May 5th, 2024. [Online]. Available: https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software

[7] Brown, Robert G. (2023) Dieharder: A Random Number Test Suite. Duke University. Accessed: May 5th, 2024. [Online]. Available: https://webhome.phy.duke.edu/~rgb/General/dieharder.php

[8] National Institute for Standards and Technology. (2010, April) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Publication.

[9] Marsaglia, George. (2023) Diehard Battery of Tests of Randomness. Florida State University. Accessed: May 5th, 2024. [Online]. Available: https://web.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/

[10] Brown, Robert. (2006) DieHarder: A Gnu Public License Random Number Tester. Publication.

[11] D. Lubicz and V. Fischer, "Recommendations for the design and validation of a physical true random number generator integrated in an electronic device," Cryptology ePrint Archive, Paper 2024/301, 2024, https://eprint.iacr.org/2024/301. [Online]. Available: https://eprint.iacr.org/2024/301

[12] ID Quantique. (2023) Standard certified USB Quantum Random Number Generation module. ID Quantique. Accessed: May 5th, 2024. [Online]. Available: https://www.idquantique.com/random-number-generation/products/quantis-random-number-generator/

[13] Frank Bergmann. (2023) Professionelle Zufallsgeneratoren für kryptografisch sichere Zufallszahlen. IBB Ingenieurbüro Bergmann. Accessed: May 5th, 2024. [Online]. Available: https://www.ibbergmann.org/ZUFALLSGENERATOREN/Mit-Kommando-Interface/PRG310/

[14] ——. (2023) Professionelle Zufallsgeneratoren für kryptografisch sichere Zufallszahlen. IBB Ingenieurbüro Bergmann. Accessed: May 5th, 2024. [Online]. Available: https://www.ibbergmann.org/ZUFALLSGENERATOREN/Ohne-Kommando-Interface/PRG600/

[15] Atos SE. (2015, November) CardOS DI V5.3 - The multifunctional smart card operating system with dual interface for the highest demands. Publication.

[16] Infineon Technologies AG. (2023) SLE 78 SOLID FLASH™ dual-interface and contactless security cryptocontroller Certification to Common Criteria EAL 6+ (high). Infineon Technologies AG. Accessed: May 5th, 2024. [Online]. Available: https://www.infineon.com/cms/en/product/security-smart-card-solutions/security-controllers/contactless-and-dual-interface-security-controllers/sle-78clfx1m10ph/

[17] Wireless Telecom Group. (2023) NC100/200/300/400 Series Chips and Diodes. Wireless Telecom Group. Accessed: May 5th, 2024. [Online]. Available: https://noisecom.com/products/components/nc100-200-300-400-series-chips-and-diodes

[18] Analog Devices. (2024) LTM8080 - 40VIN, Dual 500mA or Single 1A Ultralow Noise, Ultrahigh PSRR Module Regulator. Analog Devices. Accessed: May 5th, 2024. [Online]. Available: https://www.analog.com/en/products/ltm8080.html