Appendix 06
TRNGs: True Random Number Generators

1 Definition and Security-Critical Requirements

There are two types of devices:

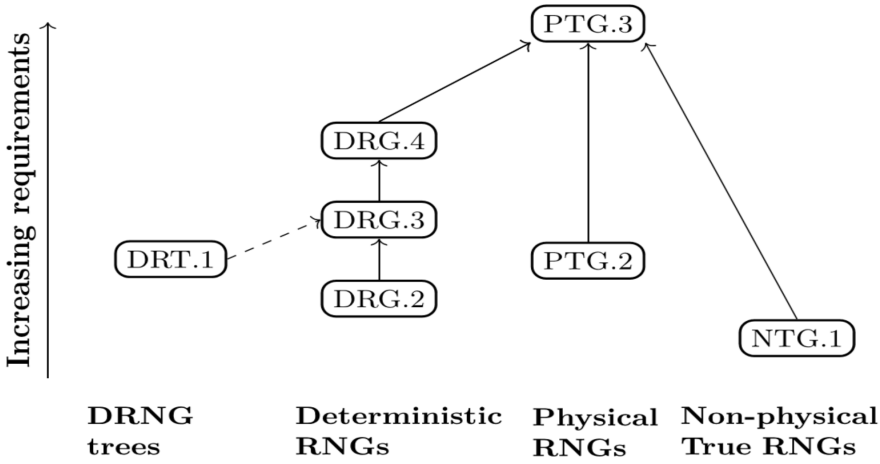
- A random bit sequence generator (RBSG) generates a sequence of bits (0 and 1) in an unpredictable order.
- A random number generator (RNG) generates a sequence of rational numbers in an unpredictable order.

This book does not distinguish between these two types because any RNG can also be used as a PRNG, and vice versa. Therefore, it will be referred to simply as a random number generator hereafter.

In cryptographic applications, random number generators are essential because their bit sequences can be used as key material.

The German Federal Office for Information Security (BSI) does not explicitly mention RBSG, but defines several different security levels for RNG in accordance with AIS 31, including the following:

- PTG.2 and PTG.3: Generators that use physical processes and produce non-predictable number sequences in three different quality grades. These generators are referred to in the book as non-deterministic random number generators.
- DRG.2 to DRG.4: Generators that use mathematical algorithms and produce number sequences that are, in principle, predictable. These generators are referred to in the book as deterministic random number generators.



For QKD and MKD, only random number generators with security levels PTG.2 through PTG.3 are suitable.

Devices of the highest security level PTG.3 ...

- ... use a physical entropy source (e.g., quantum processes),
- ... subject the raw data to cryptographic post-processing,
- ... provide an algorithmically generated bit sequence that meets at least the security level of DRG.3 in the event of a failure of the physical source.

In doing so, the BSI prioritizes continuous availability over the highest possible randomness quality. This prioritization makes sense in many applications (e.g., in a PC's operating system). For random number generators that must ensure randomness during quantum key exchange and when generating key bits for MKD, however, the quality of the randomness is more important than constant availability.

Non-deterministic random number generators (PTG.2 to PTG.3) can lose quality over time or become faulty—possibly due to a deliberate external attack—or a weakness may have already been introduced by the manufacturer or during the delivery process. Therefore, in non-entangled QKD and in MKD, at least two different random number generators—if possible from different manufacturers—must always be used, and the random numbers from the generators must then be XORed bit by bit.

Namely, if two random numbers A and B are XORed bit-by-bit, i.e.,

C = A XOR B, then the following holds for the entropy of the resulting random number C

$H(C) \geq \max (H(A), H(B))$

This means that it can be mathematically proven that the entropy of C is at least as large as the entropy of the strongest random number, provided that A and B are stochastically independent.

2 Attack scenario involving manipulated random number generators

An attacker could replace a legitimate random number generator with a deterministic generator (DRG.2 – DRG.4) (e.g., during manufacturing or in the supply chain).

- Since the bit sequences produced in this way pass every randomness test, the manipulation cannot be detected by analyzing the bit sequences.
- Once the attacker has obtained a sufficient number of bits through eavesdropping, they can predict the entire future sequence without error.
- In a QKD system, they could analyze the classical communication channel and fully compute the key without having to directly attack the quantum part of the protocol.

3 Recommendations for maximum security

- QKD schemes using entangled photons and RKD schemes offer the highest level of security because they do not require a random number generator (the random number generator is inherent to the scheme).
- If key exchange protocols require a separate random number generator—which is the case with Prepare-and-Measure QKD schemes and MKD—it must come from a trusted source and meet a quality standard that corresponds to at least security level PTG.2 according to BSI.
- At least two different random number generators from different manufacturers must be used, and the random numbers from the generators must be XORed bit-by-bit

4 Non-deterministic random number generators

Random number generators can be deterministic, generating random numbers via an algorithm, or non-deterministic, utilizing physical processes such as thermal noise,

radioactive decay, or quantum-optical processes[1] . Non-deterministic random number generators produce truly random numbers (bit sequences). However, they are slower than deterministic ones because they rely on real physical processes. This is, however, merely a matter of the technology used, as random processes such as thermal noise have cutoff frequencies of many terahertz. Furthermore, reproducibility of the results is not possible in principle, since the generated random numbers are unpredictably random. They are aperiodic, i.e., the non-repeating sequence of random numbers is infinite if the generator runs long enough. With non-deterministic physical random number generators, however, there is the problem of aging.

Deterministic and non-deterministic random number generators can also be combined, for example, by deriving the parameters of deterministic random number generators from non-deterministic ones and generating only a few random numbers (e.g., varying from 20 to 50) at a time using a random parameter set. These random number generators are called hybrid generators and can be used when the number of random bits per second required for a one-time pad needs to be increased. This slightly reduces the quality of the random numbers.

Non-deterministic random number generators (True Random Number Generators, TRNGs) exhibit technical differences, such as:

1. Physical basis: TRNGs utilize natural phenomena such as thermal noise, radioactive decay, or quantum-optical processes
2. Key generation speed in bits per second: the speed of the various technologies and products varies greatly. Currently, it typically ranges from 350 kbit/sec to 240 Mbit/sec
3. External interface: USB interface, PCIe (Peripheral Component Interconnect Express)
4. Standalone device or integrated into a CPU or other unit (e.g., PC TPM chip, smart card)

5 Functionality of TRNGs

TRNGs are true random number generators (TRNGs) and they utilize **non-deterministic physical phenomena** to generate random numbers. A simple approach for TRNGs utilizes classical electronic noise phenomena. These include Johnson-Nyquist noise (thermal noise) in resistors, which arises from the random thermal motion of charge carriers, as well as avalanche breakdown in semiconductors. However, electronic noise sources are susceptible to external

[1] https://en.wikipedia.org/wiki/Random_number_generation

environmental influences (temperature, supply voltage, electromagnetic interference). A targeted attack (e.g., frequency injection) can significantly reduce the entropy of the source.

In general, all natural sources based on physical effects that provide a fairly high quality can be used. Common methods include:

- Voltage fluctuations across a Zener diode, avalanche noise across a pn diode
- Analysis of clock edge variations (oscillator jitter) in integrated circuits
- **Radioactive decay** – The time intervals between the decays of a radioactive isotope are random
- **Photonics interference** – Light waves generate random patterns that serve as a basis

Particularly secure and fast TRNGs, which is especially important for MKD, utilize quantum effects such as the beam splitter experiment with single photons, the phase noise of lasers, or the measurement of vacuum fluctuations. In the beam splitter experiment, a single photon is directed onto a 50:50 beam splitter. According to quantum mechanics, the outcome (reflection or transmission) is fundamentally indeterminate. Unlike classical noise, there is no hidden variable here that determines the result. The randomness is physically provable and independent of incomplete knowledge about the system.

6 Hardware Interfaces

- **USB** – Many TRNGs offer a USB interface. However, USB is of limited use for very high bit rates, which are usually required for MKD.
- **PCIe** – The speed limitation of USB does not apply to PCIe. Therefore, PCIe is ideal for MKD. The issue with PCIe is connectivity with laptops, though this is not a practical problem (see below).
- **GPIO** – Some microcontrollers and embedded systems use **General Purpose Input/Output (GPIO)** pins to communicate with TRNGs.
- **I²C / SPI** – In embedded systems, TRNGs are often connected via I²C or SPI.

7 Speed (Bit Rates) of TRNGs

The speed of non-deterministic random number generators depends on several factors:

- **Physical source:** Some sources, such as radioactive decay, are relatively slow, while others, such as thermal noise, can achieve high key rates.
- **Measurement method:** The acquisition and processing of random values influence the speed.

Examples of microprocessors with non-deterministic TRNGs

- Intel SGX: Intel integrates non-deterministic TRNGs directly into its CPU platforms. Processor-generated thermal and electronic noise is used for continuous high-entropy bit generation
- AMD Ryzen processors
- ARM TrustZone

8 Market Overview

Overview of non-deterministic random number generators (TRNGs) currently available from four manufacturers:

1. Quantis by ID Quantique: They use quantum effects to generate true random numbers
2. TrueRNG by Ubld.it: These are based on electromagnetic noise and include a USB interface
3. Avalanche by BitBabbler: They use avalanche noise in semiconductors to generate true random numbers
4. Intel Secure Key (RDRAND & RDSEED): Here, hardware-based random number generation is integrated directly into Intel microprocessors

Features of TrueRNG by Ubld.it

- Physical random source: Uses avalanche noise to generate true random numbers
- Speed: Over 350 kbit/sec
- USB connection

Features of the Quantis QRNG from ID Quantique

- Physical random source: Uses quantum-optical processes for true random numbers
- Speed: Up to 240 Mbit/sec entropy data rate
- Certifications: Complies with NIST SP800-22, SP800-90B, and Dieharder tests
- Live monitoring: Detects errors immediately and disables the random stream
- USB or PCIe interface

Some TRNGs, such as those from ID Quantique, utilize **quantum effects**, such as **electron tunneling** or spontaneous emissions in optical systems. Since quantum mechanics enables **true randomness**, these methods are particularly reliable.

Features of the Avalanche TRNG from BitBabbler

- Physical random source: Uses avalanche noise to generate true random numbers.
- Speed: 2.5 Mbit/s
- Two variants:
    - BitBabbler White – Premium version with four independent entropy sources
    - BitBabbler Black – More cost-effective version with reduced hardware

Table of certified non-deterministic random number generators. Selection of three providers: ID Quantique (Switzerland), BitBabbler (Australia), and TrueRNG (Ireland):

Manufacturer	Product	Speed	Approx. Price	Technology
BitBabbler	Avalanche TRNG White	2.5 Mbit/s	120	Avalanche noise in semiconductors
BitBabbler	Avalanche TRNG Black		60	Avalanche Noise in Semiconductors
ID Quantique	QRNG USB	4 Mbit/s	$1,000	Quantum Mechanics
ID Quantique	QRNG PCIe 40	40 Mbit/s	$1,400	Quantum Mechanics
ID Quantique	QRNG PCIe 240	240 Mbit/s	$3,100	Quantum Mechanics
TrueRNG	TrueRNG	350 kbit/s	60	Avalanche noise in semiconductors
Intel	Secure Key on Intel Processor	6.4 Gbit/s	Integrated	unknown

When implementing MKD on PCs (desktop PCs, laptops, etc.), the internal non-deterministic random number generator can also be used if one is available on the processor and is sufficiently fast. The advantages are that there are no additional costs, no additional external device is required or needs to be connected to the PC (thus also saving on an external connection), and that no illegal replacement can take place in the user's absence.

9 Speed Estimate

Assuming one terabyte of cryptographic key bits—which is a realistic figure for MKD and the use of a one-time pad for data encryption—the Quantis QRNG USB at 4 Mbit/s requires approximately 12 full days for generation, and the Quantis QRNG at 240 Mbit/s requires approximately 9 hours. The INTEL processor integrated into PCs manages this in 21 minutes, although the quality of the random numbers could not be precisely determined.

In practice, this means that random number generators for keys of this length require a speed in the megabit range at a minimum. In the table above, this applies only to products from ID Quantique. In a laptop environment, only random number generators with a USB interface can be used.

However, the fastest currently available model with a USB interface, the Quantis QRNG USB at 4 Mbit/s, takes approximately 12 days to generate a 1 TB portable storage medium. The Quantis QRNG PCIe 240 requires only 9 hours for this, but the PC needs a PCIe interface or a PCIe adapter.

Because the keys—and thus the random numbers—need to be generated only at longer intervals, and because data storage in the data storage application is handled not by users but by role administrators, the PCIe interface can also be used in MKD, even if encryption then takes place on laptops. In the telecommunications application as well, key generation and data encryption can be completely separated.

10 Market size

The non-deterministic random number generators listed above are of interest for QKD and MKD, but they represent only a small fraction of the market. The global market is very large, both in terms of the number of suppliers and the volume of units.

The global market size for non-deterministic random number generators was estimated at $3.3 billion in 2024 and is projected to grow to $11.6 billion by 2034 at

a CAGR of 13.4%. Global manufacturers of random number generators include, among others (in alphabetical order):

- Advanced Micro Devices
- ID Quantique
- IBM
- Infineon Technologies
- Intel
- Microchip Technology
- Quside Technologies
- QuintessenceLabs
- Silicon Laboratories
- STMicroelectronics
- Texas Instruments
- Toshiba
- Xiphera