Quantum Random Number Generation

Table of contents

1. Introduction

Cryptographic algorithms often require random numbers; these numbers may be used for the generation of cryptographic keys, initialisation vectors, nonces, seeds, salts, etc. Implementations of cryptographic algorithms therefore need access to a Random Number Generator (RNG) that provides random numbers of sufficient quality.

There are four main methods for generating random numbers:

1. classical computational methods

   Pseudo-Random Number Generators (PRNGs) are based on classical algorithms that automatically create long sequences of numbers with good random properties (but eventually the sequence repeats). The generated numbers are not really random but pre-determined as they can be reproduced when the state of the PRNG is known.

2. quantum computing methods

   Random number generation by quantum algorithms implemented on gate-based quantum computers.

3. physical methods

   True Random Number Generators (TRNGs) generate random numbers whereby each random number generation is a function of the momentaneous values of physical environment attributes that are constantly changing in an unpredictable fashion. Physical TRNGs can be subdivided into classical Hardware Random Number Generators (HRNGs) and Quantum Random Number Generators (QRNGs).

4. non-physical methods

   Non-physical methods generate random numbers based on the unpredictability of computer process runtimes and/or human-computer interactions. The unpredictability of computer process runtimes and human-computer interactions is questionable hence the quality of random numbers that are generated based on these methods cannot be guaranteed.

Several classical computational methods exist for PRNGs but many of them are unsuitable for use by cryptographic schemes. Cryptographically Secure PRNGs (CSPRNGs) are carefully designed PRNGs that are suitable for cryptographic purposes. Nonetheless, CSPRNGs must be properly initialised with seeds of sufficient high entropy (Box 1.1), for example obtained from TRNGs, otherwise the cryptographic schemes in which these keys are used for generating random cryptographic keys, will be vulnerable to cryptanalysis (Box 1.2).

Entropy is a scientific concept as well as a measurable physical property that is most commonly associated with a state of disorder, randomness or uncertainty.

Box 1.1: Entropy

Cryptanalysis is used to break cryptographic algorithms and obtain the cryptographic key that has been used, or gain access to the plaintext corresponding with encrypted data (ciphertext), even if the cryptographic key is not known. In addition to mathematical attacks on cryptographic algorithms (aka algorithmic attacks), cryptanalysis includes the study of attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their implementation and operation.

Box 1.2: Cryptanalysis

In many classical HRNGs, the dominant hardware noise source is a consequence of underlying quantum processes. Nonetheless, physical entropy sources do not typically produce a stream of bits that is immediately unbiased and uncorrelated, so the raw stream of bits has to go through a process of entropy extraction. Entropy extraction ideally produces a stream of bits that can be considered fully random and will pass statistical randomness tests. However, the quality of the generated random numbers is hard to determine in practice.

Using random numbers of insufficient quality for cryptographic purposes provides the opportunity to malicious parties to successfully attack cryptographic systems, even when state-of-the-art cryptographic mechanisms have been deployed. For example, cryptographic research groups from EPFL (led by Arjen Lenstra) and UCSD (led by Nadia Heninger) were able to factor a percentage of millions of public keys gathered from the internet (which were used in systems from more than 30 manufacturers) because these public keys were not sufficiently random.

2. Quantum random number generation

2.1. Quantum computing based quantum random number generation

The common practice for generating random numbers by means of gate-based quantum computers is to create entangled qubit states by combining Hadamard and CNOT quantum gates in a quantum circuit that implements a random number generating quantum algorithm. See the Boxes 2.1 through 2.9 for a brief explanation of gate-based quantum computation and underlying quantum mechanical concepts.

A gate-based quantum computer is a device that takes input data and transforms this input data according to a quantum circuit specification.

Box 2.1: Gate-based quantum computer

A quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a quantum system. Knowledge of the quantum state together with the rules for the quantum system's evolution in time exhausts all that can be predicted about the quantum system's behaviour.

Box 2.2: Quantum state

Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct quantum states. The principle of quantum superposition states that if a physical system may be in one of many configurations (arrangements of particles or fields) then the most general state is a combination of all of these possibilities. The principle applies to the states that are theoretically possible without mutual interference or contradiction. It requires us to assume that between these states there exist peculiar relationships such that whenever the system is definitely in one state, we can consider it as being partly in each of two or more other states. The original state must be regarded as the result of a kind of superposition of the two or more new states, in a way that cannot be conceived on classical ideas. Any state may be considered as the result of a superposition of two or more other states, and indeed in an infinite number of ways.

Box 2.3: Quantum superposition

Quantum entanglement is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the quantum state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical physics and quantum mechanics.

Box 2.4: Quantum entanglement

A quantum measurement is the testing or manipulation of a quantum system to yield a numerical result. The predictions that quantum mechanics makes about these measurements are in general probabilistic and depends on state of the system that is being measured. The main objective of quantum computing is to execute a quantum circuit to set up the system's quantum state in such a way that (the) desired measurement outcome(s) have a high probability of occurring.

Box 2.5: Quantum measurement

A qubit (quantum bit) is a basic unit of quantum information. It is the quantum version of the classic bit (binary bit) physically realised with a two-state quantum device. In classical computing the information is encoded in bits, where each bit can have the value zero or one. In quantum computing the information is encoded in qubits. A qubit is a two-level quantum system where the two basis qubit states are usually written as $|0\rangle$ and $|1\rangle$. A qubit can be in state $|0\rangle$, state $|1\rangle$ or (unlike a classical bit) in a linear combination of both states ($\alpha|0\rangle + \beta|1\rangle$). The name of this phenomenon is superposition.

Box 2.6: Quantum bit (qubit)

A quantum gate is an operation applied to a single qubit or to multiple that changes the quantum state(s) of the qubit(s).

Box 2.7: Quantum gate

A quantum circuit specifies a set of qubits and the sequence of operations to be performed on these qubits, i.e. preparation of qubits, quantum gate operations on the qubits and qubit measurements.

Box 2.8: Quantum circuit

A quantum algorithm is a step-by-step procedure, which is transformed into a quantum circuit that is executed by a quantum computer. Although classical algorithms can also be executed on a quantum computer, the term quantum algorithm usually designates algorithms that are inherently quantum (i.e. those that use some essential feature of quantum computation such as quantum superposition and quantum entanglement).

Box 2.9: Quantum algorithm

Whether or random numbers generated by the physical implementation of the quantum algorithm are genuinely random depends on the engineering of the quantum computer's qubit preparation and measurement hardware, which is non-quantum and may therefore jeopardise qubit quantum state indeterminism.

2.2. Physical quantum random number generators

A (physical) Quantum Random Number Generator (QRNG) exploits the probabilistic nature of quantum measurements to generate genuine random numbers. It relies on techniques based purely on quantum mechanics for its entropy. QRNGs do not provide any newmitigation against the threat from Cryptographically Relevant Quantum Computers (CRQCs)[1] to vulnerable classical public-key cryptography. However, they can generate truly unpredictable random numbers at very high speed because the processes used by QRNGs are simple compared to the classical physical processes used by HRNGs (which need to be complex enough to avoid predictability).

Most of the existing QRNGs are based on quantum optics technology. The inherent randomness in many parameters of the quantum states of photons (Box 2.10) allows for a choice of implementations using light generated by lasers (Box 2.11), LEDs (Box 2.12) or single photon sources.

The photon is an elementary subatomic particle. It is the quantum of the electromagnetic field, including electromagnetic radiation such as light and radio waves, and it is the force carrier for the electromagnetic force. Photons do not have electrical charge, they have zero mass and zero rest energy, and they only exist as moving particles. Photons move at 299,792,458 metres per second in a vacuum, the so-called "speed of light" denoted by *c* (from the Latin *celeritas*). The speed of photons in a medium depends upon the medium and is always slower than the speed in vacuum *c*.

Box 2.10: Photon

A laser emits light through a process of optical amplification based on the stimulated emission of electromagnetic radiation (hence the name). Stimulated emission is a quantum phenomenon where energy is extracted from a transition in an atom or molecule. Lasers emit highly coherent light beams (photons). Spatial (or transverse) coherence allows a laser to be focused to a very small spot and to stay narrow over great distances (collimation). Temporal (or longitudinal) coherence allows a laser to emit light with a very narrow frequency spectrum or to produce ultrashort pulses of light with a broad spectrum but with verry small durations (e.g. a femtosecond).

Box 2.11: Laser

A Light-Emitting Diode (LED) is a semiconductor light source that emits light when an electrical current flows through it. This is caused by electrons in the semiconductor that recombine with electron holes, releasing energy in the form of photons. The colour of the light emitted by the LED (which corresponds to the energy of the photons) is determined by the energy required for electrons to cross the band gap of the semiconductor (i.e. the minimum energy required to excite an electron from its bound state into a free state, where it can participate in conduction). White light is obtained by using multiple semiconductors or by applying a layer of light-emitting phosphor on the semiconductor's surface.

Box 2.12: Light-Emitting Diode (LED)

[1] The term Cryptographically Relevant Quantum Computer (CRQC) is used to specifically describe powerful future quantum computers that are capable of actually attacking real world cryptographic schemes that would be infeasible to attack with a classical computer.

QRNGs based on quantum optics technology include:

- branching-path generators: based on the randomness of the measurement of photons in a superposition of two or more light travelling paths;
- time-of-arrival generators: based on the randomness of the arrival time of successive single photons;
- photon-counting generators: based on the randomness of the number of photons detected during a fixed time interval;
- quantum-vacuum-fluctuation generators: based on the randomness of the balanced homodyne measurements (Box 2.13), by two amplitude detectors, of the vacuum fluctuations of the electromagnetic field contained in the radiofrequency sidebands of a single-mode laser diode;

> Homodyne detection is a method of extracting information encoded as modulation of the phase and/or frequency of an oscillating signal, by comparing that signal with a standard oscillation that would be identical to the signal if it carried null information. "Homodyne" relates to the use of a single frequency, in contrast to the dual frequencies employed in heterodyne detection.

Box 2.13: Homodyne detection

- phase-noise generators: based on the randomness of the output field of a laser that is caused by spontaneous emission;
- amplified-spontaneous-emission generators: based on the randomness of spontaneously emitted photons from a light source.

Non-optical QRNG techniques include for example:

- tunnelling QRNGs which are based on measuring unpredictable quantum tunnelling variations (noise) in the current flow through a forward-based tunnel diode junction;
- radioactive decay QRNGs which are based on the random timing of decay of radioactive atoms and the detection of these decay events by a Geiger-Müller counter;
- skyrmion-based QRNGs (Box 2.14).

> The skyrmion is a topological quasiparticle which has the remarkable property of being able to model, with reasonable accuracy, multiple low-energy properties of the nucleus of an atom, simply by fixing its radius.

Box 2.14: Skyrmion

Despite claims made by the vendors (and also occasionally by the media), the true unpredictability that QRNGs provide in theory is hard to realise in practice. QRNGs are typically based on the property that a quantum system can exist in a superposition or entanglement state. While the preparation of the quantum system into superposition or entanglement and the measurement of it are relatively simple processes, the engineering of the preparation and the measurement hardware has to be trusted. Furthermore, QRNGs will necessarily be embedded in classical electronic components and these add noise to the measurement of the QRNG's quantum state.

The embedding within classical hardware also implies that QRNGs are potentially subject to a similar range of implementation-level attacks as classical HRNGs, as well as those specific to quantum technology. This leads to several challenges, which must be overcome when designing and implementing a QRNG solution.

3. Device-independent quantum random number generation

An interesting research area is the so-called device-independent quantum cryptography. A quantum cryptographic mechanism is device-independent if its security does not rely on trusting that the device used to implement the mechanism is truthful. The security analysis of these quantum cryptographic mechanisms includes scenarios of imperfect or even malicious devices. Device-independent quantum cryptography is based on "self-testing" devices, the internal operations of which can be uniquely determined by their input-output statistics. This is typically done by means of Bell inequality testing (Box 3.1).

Bell's theorem is used to prove that quantum mechanics is incompatible with ‘local hidden-variable’ theories. It was introduced by physicist John Stewart Bell in a 1964 in response to the EPR paradox. The EPR paradox refers to a thought experiment that Albert Einstein, Boris Podolsky and Nathan Rosen formulated in 1935, in order to argue that quantum mechanics was an incomplete theory. In their view (shared by many other leading physicists at the time), quantum particles carry physical attributes (later called ‘local hidden-variables’) not included in the quantum mechanics theory, and the uncertainties in quantum mechanics theory's predictions are due to ignorance of these attributes.

Bell carried out an analysis of quantum entanglement and deduced that if measurements are performed independently on the two separated halves of a pair of entangled particles, then the assumption that the outcomes depend upon ‘local hidden-variables’ within each half implies a constraint on how the outcomes on the two halves are correlated. This constraint would later be named the ‘Bell inequality’. Quantum mechanics predicts correlations that violate this inequality and multiple variations on Bell's theorem have been tested experimentally in physics laboratories many times. All these ‘Bell tests’ have found that the hypothesis of ‘local hidden-variables’ is inconsistent with the way that quantum entanglement works. While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Box 3.1: Bell inequality testing

Device-independent quantum random number generation by means of Noisy Intermediate-Scale Quantum (NISQ) quantum computers (Box 3.2) with a limited number of “imperfect” (aka “noisy”) physical qubits is based on reasonable computational hardness assumptions, but does not need that the NISQ quantum computer is a trusted device. Future availability of quantum computers with large numbers of “perfect” logical qubits could remove the dependence on computational hardness assumptions.

Noisy Intermediate-Scale Quantum (NISQ) applies to current state-of-the-art quantum computers. The term 'noisy' refers to the fact that these quantum computers are very sensitive to the environment and may lose their quantum state due to quantum decoherence because they are not sophisticated enough to implement quantum error correction. Quantum decoherence is the loss of quantum coherence and represents a challenge for the practical realisation of quantum computers, since such machines are expected to rely heavily on the undisturbed evolution of quantum coherences. The term 'intermediate-scale' refers to the not-so-large number of qubits.

Box 3.2: Noisy Intermediate-Scale Quantum (NISQ)

Device-Independent physical QRNGs (DI-QRNGs) produce unpredictable genuine randomness without any assumption whatsoever about the device being used. DI-QRNGs are “self-testing" devices that use quantum entanglement mechanisms, making it possible for its internal operations to be uniquely determined by performing Bell inequality testing based on device input-output statistics.

DI-QRNG is very difficult to implement. In Semi-Device-Independent QRNG (SDI-QRNG) some components of the QRNG implementation are subjected to Bell inequality testing, while other components are trusted in the traditional sense.

Appendix A - References

[arXiv 2022]
A Comprehensive Review of QRNGs: Concepts, Classification and the Origin of Randomness

[BSI AIS-20 1999]
Functionality classes and evaluation methodology for deterministic random number generators

[BSI AIS-31 2001]
Functionality Classes and Evaluation Methodology for Physical Random Number Generators

[evolutionQ 2021]
Quantum Random-Number Generators: Practical Considerations and Use Cases

[ISO/IEC 20543 2019]
Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

[NIST SP 800-90B 2018]
Recommendation for the Entropy Sources Used for Random Bit Generation

[NOREA 2024] Quantum Computing Explained

[Wikipedia 2022] Diehard tests

Appendix B - Acronyms and abbreviations

AIS	Anwendungshinweise und Interpretationen im Schema
aka	also known as
bit	binary digit
BSI	Bundesamt für Sicherheit in der Informationstechnik
c	celeritas
CNOT	Controlled NOT gate
CRQC	Cryptographically Relevant Quantum Computer
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DI-QRNG	Device-Independent Quantum Random Number Generator
e.g.	exempli gratia
EPFL	École Polytechnique Fédérale de Lausanne
EPR	Einstein-Podolsky-Rosen
etc.	et cetera
HRNG	Hardware Random Number Generator
i.e.	id est
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
laser	light amplification by stimulated emission of radiation
LED	Light-Emitting Diode
NISQ	Noisy Intermediate-Scale Quantum
NIST	National Institute of Standards and Technology
nonce	number used once

PRNG	Pseudo-Random Number Generator
QRNG	Quantum Random Number Generator
qubit	quantum bit
RNG	Random Number Generator
SDI-QRNG	Semi-Device-Independent QRNG
SP	Special Publication
TRNG	True Random Number Generator
UCSD	University of California at San Diego