Obtaining True-Random Binary Numbers from a Weak Radioactive Source*

Ammar Alkassar[1], Thomas Nicolay[2], and Markus Rohe[3]

[1] Sirrix AG security technologies,
Homburg, Germany
a.alkassar@sirrix.com

[2] Saarland University, Radio-Frequency Research Group,
Saarbrücken, Germany
th.nicolay@mx.uni-saarland.de

[3] Saarland University, Cryptography Research Group,
Saarbrücken, Germany
mail@markus-rohe.de

Abstract. In this paper, we present a physical random number generator (RNG) for cryptographic applications. The generator is based on alpha decay of Americium 241 that is often found in common household smoke detectors. A simple and low-cost implementation is shown to detect the decay events of a radioactive source. Furthermore, a speed-optimized random bit extraction method was chosen to gain a reasonable high data rate from a moderate radiation source (0.1 μCi). A first evaluation by applying common suits for analysis of statistical properties indicates a high quality of the data delivered by the device.

1 Introduction

Today, random numbers are well employed in numerical simulations and computations (e.g. Monte-Carlo simulations) as well as in cryptographic applications.

Many essential cryptographic primitives are are considered as probabilistic functions, or at least need a random input, e.g., the generation of challenges and session keys. Making random numbers available in deterministic environments as computers is a crucial task, hence, the security of the cryptographic systems highly depends on the quality of the employed random numbers. In this context, the main property is that the random sequence is *unpredictable*. Based on the source of randomness, we can distinguish between three classes of random generators:

* This work was partially funded by by the European Union in the Network of Excellence FIDIS and the German Federal Ministry of Education, Science, Research and Technology (BMBF) in the framework of the Verisoft project under grant 01 IS C38. The responsibility for this article lies with the authors.

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481, pp. 634–646, 2005.

Pseudo Random Numbers: A pseudo random number generator (PRNG) is a hard- or software instantiation of a deterministic algorithm that generates a long-periodic sequence of numbers from an initial value, called seed. Roughly speaking, a pseudorandom generator expands a short random seed into much longer random bit sequences that *appear* "random" (although they are not). In other words, the pseudorandom bit sequences have to be unpredictable, hence they are indistinguishable from true random sequences of the same length.

The notion of indistinguishability is strongly related to computational difficulty and the properties of these generators do not apply unconditionally, rather than for computationally restricted attackers. PRNG could be constructed from various intractability assumptions and good generators are proven under such assumptions.

Random Numbers Based on Complex Processes: Another possibility to obtain random numbers is given by relying on complex processes which are in principle physically deterministic but cannot be computed efficiently. For example, the random fluctuations caused by air turbulence within a disk drive or deriving randomness from a microphone/video camera signals [1]. Even "software-based" random generators rely on complex processes. Examples for random bases for such generators are the elapsed time between keystrokes or mouse movement, content of input/output buffers and operating system values such as system load and network statistics.

True Random Numbers: A true physical random number generator (TRNG) generates random numbers by observing a stationary physical phenomenon, like the elapsed time between the emission of particles during radioactive decay or the thermal noise from a semiconductor diode or resistor. The underlying phenomena are characterized by the fact that the basic quantity only could be described in a statistical manner. That is not because of inaccuracies in the used physical measurement methods, rather than because of the physical model of our world. A classic example is quantum theory, as it is intrinsically random. Hence, a quantum process like thermal noise in a semiconductor or the radioactive decay of an atomic nucleus provides an ideal base for a TRNG.

Devices based on those principles meet the definition of information-theoretic secrecy in cryptography: an attacker is unable to predetermine the bit sequence even with unbounded memory and time resources. Thus, an unconditionally secure system is only information-theoretic secure if its non-deterministic functions are founded on unpredictable random data.

Many TRNG devices for research and commercial purposes, based on quantum processes, have been constructed so far. Clipped white noise gained by thermal noise of resistors or semiconductors is used in the design of [2]. Another approach is to use noise from neon tubes [3]. The amplified noise is evaluated by a comparator, sampled and digitally de-skewed, i.e., processed to suppress correlations and statistical errors. Nevertheless these devices are very sensitive to high frequency electromagnetic disturbances. In an alternative approach [4] noise voltage modulates a voltage controlled oscillator (VCO). The output volt-