The ESP-RNG Says: "YES"

J.M. Birkett[1], M-J. O. Saarinen[1] and D. Page[2]

June 21, 2007

[1] Information Security Group,
Royal Holloway, University of London,
Egham, TW20 0EX, UK.
{j.m.birkett,m.saarinen}@rhul.ac.uk

[2] Department of Computer Science,
University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol, BS8 1UB, UK.
page@cs.bris.ac.uk

Abstract

High quality, high performance random number generators are a vital component in modern cryptographic systems. While traditional LFSR designs have some advantages they can only be operated in one mode, namely the generation of random numbers. We present the ESP-RNG, a new design that is additionally capable of executing in a powerful predictification mode. In this mode the design is able to reliably ascertain the validity of arbitrary statements, potentially even those that relate to future events. We show the ESP-RNG is efficiently implementable in hardware and passes known statistical randomness tests; we posit that inclusion in standards such as those by IEEE, ISO and ANSI is a natural next step.

1 Introduction

It is a tradition at major cryptographic conferences, and presumably a major burden to the General Chairs of said conferences, that delegates are provided with a gift as part of their registration package. This gift commonly takes the form of a localised item intended to remind the owner of great memories spent listening to impenetrable presentations and killing brain cells with the local brew. Focusing on Eurocrypt as an example, gifts presented over the last few years have been

Eurocrypt 2002, Amsterdam Travel umbrella.

Eurocrypt 2003, Warsaw ???

Eurocrypt 2004, Interlaken Photograph of delegate with cow.

Eurocrypt 2005, Aarhus USB key-drive.

Eurocrypt 2006, St. Petersburg Ornamental globe.

Some cynics have noted that the quality of conference gift is usually inversely proportional to the quality of the conference food. This view neglects the potential usefulness of such gifts however; given the changeable weather, few delegates in Amsterdam would have swapped their umbrella for a second helping of rijstebrij.

High quality, high performance random number generators are a vital component in modern cryptographic systems. Random number generators can be separated into two main classes: those that produce so-called real random results and those that produce pseudo-random results. Real random number generators are typically based on some physical phenomena such as radioactive decay, metastability in circuits or complex fluid dynamics. Pseudo-random number generators are deterministic algorithms that are iterated to generate a sequence using some starting seed state. Uses for such generators include production of keys and system parameters and, as a result, lack of quality in the result can significantly reduce the security of the encompassing system. To ensure this potential problem is limited, it is common to include random number generators as part of cryptographic standards.

Our focus in this paper is the gift from St. Petersburg, a small ornamental globe which implements a similar functionality to the so-called magic 8-ball. Our theory is that the device, far from being a toy to prevent terminal boredom during the main conference program, is a sophisticated random number generator. Adopting the nomenclature of Naccache [1], we name this device the Eurocrypt Spinning Predictificator and Random Number Generator (ESP-RNG). Unlike traditional generators that simply produce random outputs, the ESP-RNG is additionally capable of executing in a powerful predictification mode. In this mode the ESP-RNG is able to reliably ascertain the validity of arbitrary statements, potentially even those that relate to future events.

The paper is organised as follows. We start by offering a description of the ESP-RNG hardware platform in Section 2 before presenting our experiments on device in Section 3. We present some concluding remarks in Section 4.

2 ESP-RNG Hardware Definition

Definition 1 *The spinner is defined as the (unique) person operating the ESP-RNG device.*

Definition 2 *The spinee is defined as the (unique) ESP-RNG hardware being used.*

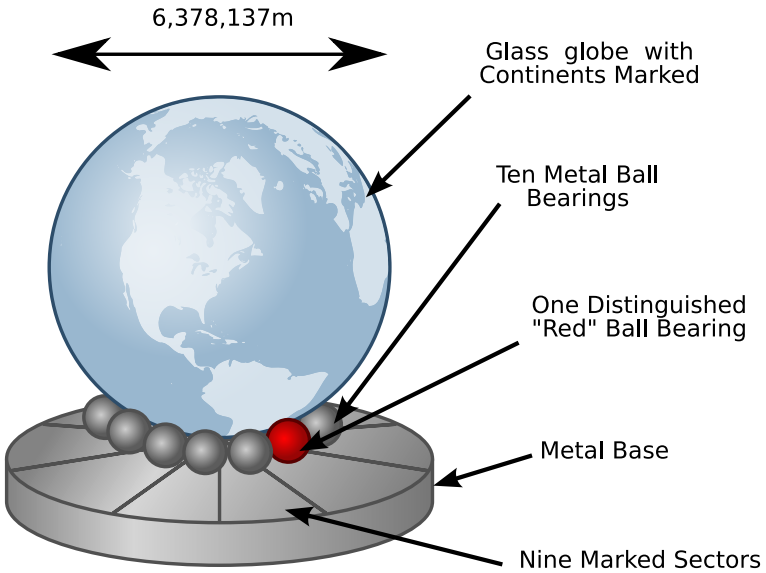

Figure 1: Abstract ESP-RNG hardware definition.

Combining Definition 1 and Definition 2 we define an ESP-RNG implementation as the combination of spinner and spinee. The hardware is realised as a glass globe that is mounted, via an axle that connects it to the weighted and ornate base, on a bed of ball barrings. The ball barrings are all coloured silver apart from one, termed the distinguished ball barring, which is red. The ball barrings allow the globe to be spun smoothly and are themselves stimulated by the spinnage; the ball barrings rotate with the spin until the kinetic energy of the globe is exhausted. Figure 1 describes the ESP-RNG hardware diagrammatically: one can see that it is ideal for use in mobile and ubiquitous computing and also doubles as an attractive centre-piece to coffee tables and fire places alike.

An ESP-RNG can be operated in one of two modes: as a pure random number generator or as a predictification method. In either case, when it is invoked an ESP-RNG device produces a number supposedly uniformly at random

$$ESP - RNG =_R \{1, 2, \ldots 9\}.$$

This output can be read from the ESP-RNG when the globe is settled in a resting state: one simply observes the location of the distinguished ball barring.

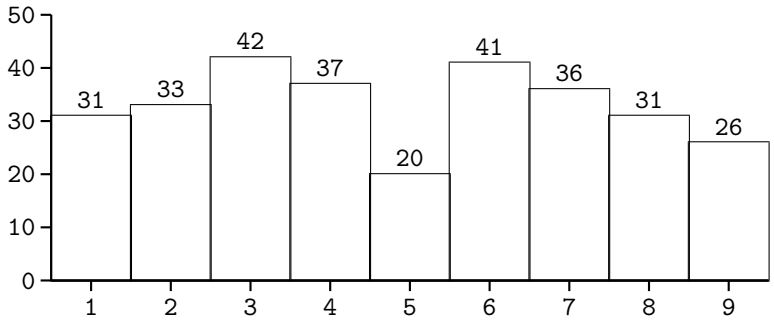

Figure 2: Frequency of ESP-RNG output over three spinner-spinee pairings.

To realise the predictification functionality, one uses the random output x as input to the map Φ

$$\Phi(x) = \begin{cases} \textit{“Ask mom”} & \text{if x=1} \\ \textit{“Buy”} & \text{if x=2} \\ \textit{“Sell”} & \text{if x=3} \\ \textit{“Go for it”} & \text{if x=4} \\ \textit{“No”} & \text{if x=5} \\ \textit{“Pray”} & \text{if x=6} \\ \textit{“Yes”} & \text{if x=7} \\ \textit{“Maybe”} & \text{if x=8} \\ \textit{“Fire someone”} & \text{if x=9} \end{cases}$$

Interpretation of the predictification is a subtle art since the results are valid on a strictly per-user basis. Further, the results of predictification are only meaningful if a question is posed to the ESP-RNG before spinnage takes place; questioning while spinnage is underway or after it has finished can result in a confused outcome.

3 Experimental Results

Our experimental aims were to verify two claims relating to the ESP-RNG. Firstly, we instrumented rigorous statistical testing of the randomness properties; we hoped this might assist standardised use of the device. Secondly, we investigated the accuracy of predictification.

3.1 Random Number Generation

In order to analyse the ESP-RNG in a rigorous, statistical manner we procured three spinee devices and randomly paired them with three spinners. Through a series of over 200 trials, we produced the result distribution detailed in Figure 2.

These results clearly highlight two key features. Firstly, note that the entropy of the ESP-RNG is roughly 2.1-bits: the device can produce random bits

at roughly twice the rate of the previous best result, namely the Coin-Flip Random Number Generator (CF-RNG). Although the ESP-RNG is able to produce random bits twice as fast as a £1 coin, it is worth almost exactly half as much in terms of scrap value. This produces a ratio of roughly $4 : 1$ in favour of ESP-RNG in terms of the standard randomness-per-pound measure as used in the UK since 1978.

Secondly, option five (where $\Phi(5) =$ "No") is substantially less likely to occur than any other. In particularly, one should note that "No" is a far less likely outcome than "Yes". This bias hints at potential subversion of the design, perhaps by naturally optimistic designers or governmental organisations keen to provide back doors in ESP-RNG based cryptosystems.

3.2 Predictification Accuracy

To investigate the supposed supernatural question answering powers of the ESP-RNG, we first calibrate our experimental implementations using a control question or ground truth. We asked the question

Q : Will obtaining Russian visa be easy ?
A : No.

As many Eurocrypt 2006 attendees will attest, this is the correct answer and calibration was thus adjudged to be successful. Following this early success we initiated a more complete program of hypothesis testing. Unfortunately the sample size of ESP-RNG implementations is small, and preliminary indications are somewhat ambiguous. We started with the question

Q : Will our expenses claim be accepted by the finance department ?
A : Pray.

Although this was perhaps to be expected (given our extensive research into ESP-RNG was paid for as part of said expenses), this did not seem positive. We decided to ask the ESP-RNG about some more important issues

Q : Is AES secure ?
A : Fire someone.

There is an ancient proverb that states "nobody ever got fired for buying IBM". Until now one could easily have rephrased this as "nobody ever got fired for deploying AES", the ESP-RNG has predicted otherwise and we expect the cryptographic community in Belgium to go into hiding as a result. Fed up with the trivialities of cryptography, we decided to use the ESP-RNG to assess the stock market

Q : What should I do with my NTRU stock options ?
A : Sell.

Cryptanalysts working on lattice based attacks on the various NTRU primitives would no doubt agree but we decided to balance this negative result by investigating the future for quantum computing, one source of attacks NTRU apparently can repel

Q : What is the future for quantum cryptography ?
A : Ask mom.

We asked all our mothers and not one of them had heard of quantum cryptography. Ironically this is exactly the same number of people who have developed even marginally practical applications of said technology; we interpreted this as a negative result although now we have seen it, it might have changed.

4 Conclusions

Through rigorous experiments we have shown that the ESP-RNG, a portable and visually appealing random number generator, is biased: the result "yes" is far a more likely outcome than "no". Despite this, we have also shown that the device can accurately predict the future, a feature which improves significant value to previous designs.

References

[1] V. Gratzer and D. Naccache. Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt. In *Advances in Cryptology (EUROCRYPT)*, Springer-Verlag LNCS 4004, 48–58, 2006.