Random Sources for Cryptographic Systems

G.B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario, Canada

Introduction

Random and pseudorandom sources have long been of interest in the study of statistical processes. Applications include the simulation of computer networks and communication channels. In these systems, pseudorandom sources (PRS) are preferred over true random sources (TRS) as repeatability (recreatability) of observations is important.

In cryptographic systems, true random sources are preferred in some instances to prevent penetration or influence of the system (some cryptographic systems in fact assume the availability of a true random source [1], [2]). It is observed that the strongest cryptographic system may be rendered insecure if an attacker can influence the generation of keys (presumably either by a PRS or TRS).

In this study we define a binary true random source (BTRS) as a device which generates an output pattern of 1's and 0's such that they are bitwise iid and all 2^n sequences of n bits are equally likely for any integer n. BTRS are generally based on measuring naturally occurring events such as sampling diode shot noise [3], time between radioactive particle decay, etc.. These devices are generally built external to the device using the random source. This is done for a number of reasons. First, the technology used to realize the random source is generally incompatible with the technology used for the cryptographic system (cryptodevice). Second, due to the nature of the process observed, temperature control or compensation is generally required. Third, shielding to prevent influence or observation may be required. Finally, if the random source is proven bias at a later date, it can be replaced by another source without redesign of the cryptodevice. We make the distinction at this point, between binary true random sources for general applications and sources for cryptographic purposes. In the former, the device operates in a 'friendly' environment, while in the latter, we must assume that an active attacker may try to observe or bias the output of the device.

There are several drawbacks in using an external random source. If the system is subject to observation or influence along the path from the source to the cryptodevice, then the system may be insecure (in some cryptographic systems, it may not be necessary or desirable to expose the outcome of the random source to the external environment, e.g., Diffie-Hellman key exchange protocol [2]). To provide a cryptographically strong BTRS for implementation on a cryptodevice, several criteria must be met:

i) Compatibility with device technology
ii) Immunity to observation or influence
iii) Stability of source output and freedom from bias.

By including the BTRS as part of the cryptodevice, most observation attacks can be avoided. Outside influence on the other hand, can take on several forms. A good BTRS should provide immunity from outside influence due to:

i)Modulation of grounds, power, input or output lines
ii) electromagnetic fields or radiation
iii) temperature manipulation
iv) forced resetting of the device to a known starting state.

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 77-81, 1988.

If we look carefully at the above requirements, we observe that requirements (i) and (ii) can be realized by a device exhibiting common mode rejection [4]. This can be explained in the following way: if we use two similar devices, both subject to the same environment (external stimulus), and measure the *difference* between them, any common effects will be reduced or nullified. This observation leads us to the design of a VLSI implementation of a BTRS as discussed in the next section.

A Metal Insulator Semiconductor Capacitor

A common structure in semiconductor systems is a metal insulator semiconductor capacitor (MISC). While a thorough discussion of the operation of such devices is beyond the scope of this paper, a brief explanation of the concepts involved will be given. Figure 1 shows the general physical structure of a MISC. It consists of a p-type semiconducting substrate material covered by insulating silicon oxide (S_iO_2) with a metalized pad placed over the insulation (the area covered by the metalization defines the area of the MISC). The p-type substrate material has, by nature of the impurities planted in it, a deficiency of free electrons. If a positive voltage V_g is applied to the metal pad, a *potential well* will be formed under the metalization. This potential well is the result of electrons being drawn to the positive charge. Since the p-type material is deficient in free electrons, there will not be enough free electrons to *fill the well* and a net shortage will exist. The depth of the well is determined by V_g and the size of the charge (number of electrons) required to fill the well is determined by ϕ_s. This is shown in Fig. 2a.

No physical system will support such an imbalance in charge for an indefinite period. Electrons will eventually migrate into the potential well and fill it up (see Fig. 2b). The period over which electrons are collected is referred to as the integration period. If we now remove the voltage V_g from the metalization, a net surplus of electrons will be present and this "charge" can be measured.

There are two major mechanisms by which free electrons can be generated to fill the potential well: i)by radiation or, ii) by dark current generation. If the top of the semiconductor device is left open and many cells are coupled together, light can be used to illuminate the cells and generate free electrons. In this case, the number of electrons generated is proportional to the intensity of the light. This forms the basis of today's imaging Charge Coupled Devices (CCDs) used to replace the old tube-type television cameras.

The second process involves electrons generated by thermal processes (noise). While this effect is small as compared to the radiation effect, if the device is sealed against light, this effect is considerable. This effect is highly sensitive to the temperature of the device. It is generally agreed by theory and experimental observation, that the number of electrons generated by dark current over the integration period follows a Poisson process (the variance equals the mean) [5]. It also appears that the dark current generation between devices even in close physical proximity, is uncorrelated. This leads us to a proposed structure for a BTRS.

A VLSI Realization

The implementation consists of two identical structures, cells X and Y, in close physical proximity. We allow them to "charge" over the same integration period, then measure the difference in charge between them and assign either a 1 or 0 to the outcome. This amounts to the construction of a device with high common mode rejection since any attempt at influence will be common to both devices and removed in the comparison. In addition, the close physical proximity of the devices will result in consistent temperature affects in both cells.

To analyze the suitability of such a system as a BTRS, we will use some observed values from actual test CCDs (it should be noted that these devices were designed as "good" devices which exhibit low dark current characteristics, our purpose is opposite, to build cells which promote dark current effects). The dark current generated in the device is a function

of the size (area) of the cell and the dark current density (J_{gen}). The dark current density is highly dependent on the level of impurities in the p-type material and the temperature of the device. J_{gen} for a good device may range from 5 $nanoamps/cm^2$ to 1 $milliamp/cm^2$ at 20°C. For a cell with cross-sectional area of approximately 10^{-7} cm^2, the dark current generated is shown in Table 1 for various temperatures.

To create a random result, we must measure the difference in charge between the two cells. This will require the development of a differential sensing amplifier. Current sense amplifiers used in memory devices can resolve a difference down to about 100 electrons. If we model the Poisson distribution of the number of electrons arriving during the integration period as a normal distribution, then the characteristics of the process should be:

$$mean = \lambda_X - \lambda_Y \equiv 0$$
$$variance = \lambda_X + \lambda_Y \equiv 2\lambda$$

While the above would be the ideal case, it would be physically impossible to exactly match two cells even under the strictest control. In addition, we assume that if the difference in charge is too small for the differential amplifier to resolve, it will always be bias in one direction. Thus the generation of 1's and 0's will not be symmetric and we must put up with some bias. This bias will be inversely proportional to the number of electrons collected (i.e., the unresolved area of 100 electrons becomes less likely as the number of electrons collected increases). (Note: the simple lack of symmetry does not present a real problem in the generation of random sequences as the output of several such devices can be combined.)

In Table 2, we show the number of electrons which must be collected in order to provide various levels of accuracy (deviation from symmetry of 1's and 0's). In Table 3, we use the dark currents from Table 1 and calculate the integration period required to produce the various accuracies. These results can be interpreted in two ways: either the integration period must be increased at lower temperatures or, if the integration period is fixed, then the accuracy will decrease with temperature.

Summary

In this paper, we have presented a new approach to the generation of a random binary bit stream. This structure is compatible with current VLSI technology. We have shown that by using two cells subject to the same dark current generation process and taking the difference of charge between the two cells, a random result can be created. While much work remains to be done in this area, we feel the initial investigation shows great promise.

References

1. R. Rivest, A. Shamir, L. Adleman, 'On digital signatures and public key cryptosystems', Comm. of ACM, Vol. 21, Feb. 1978, pp.120-126

2. W. Diffie, M. Hellman, 'Privacy and authentication : An introduction to cryptography', Proc. of the IEEE, Vol. 67, March 1979, pp. 397-427.

3. D. Kahn, 'Cryptography and the origin of spread spectrum', IEEE Spectrum, Vol. 21, no. 9, Sept. 1984, pp. 70-80.

4. IEEE Standard Dictonary on Electrical and Electronic Terms, IEEE Inc., New York, 1984.

5. G. Hobson, 'Charge Transfer Devices', Edward Arnold, London, 1978.

Table 1

Dark Current for Typical Cell

TEMP	I_{gen}
20°C	100 pA
-10°C	10 pA
-30°C	1 pA

Table 2

Number of Electrons Required During Integration

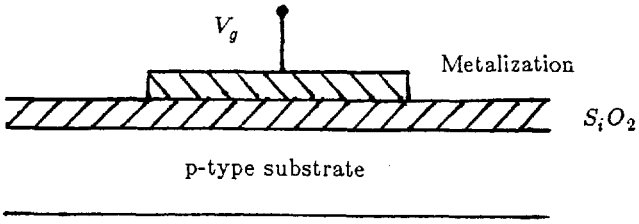
Accuracy	Number of Electrons λ
1%	10^7
5%	$5 * 10^5$
10%	10^5

Table 3

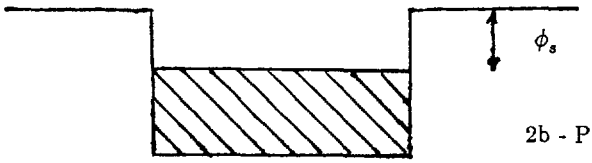
Integration Time

TEMP	1%	5%	10%
20°C	10 msec	0.3 msec	60 μsec
-10°C	100 msec	3 msec	600 μsec
-30°C	1 sec	30 msec	6 msec

Figure 1 - Metal Insulator Semiconductor Capacitor



2a - Empty Potential Well



2b - Partially Full Potential Well

Figure 2 - Potential Well