Security and bit rate for oscillator based TRNG

David Lubicz

University of Rennes 1

Introduction

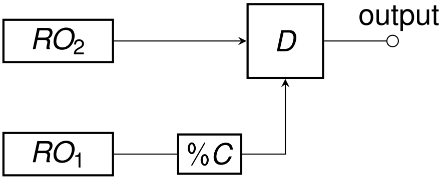
Random Number Generators (RNGs) are crucial components for the security of cryptographic systems. Typical usages include

- key generation,
- initialization vectors or
- counter measures against side-channel attacks.

But it is not easy to design hardware-based RNGs with a proved entropy rate.

A classical design

A classical design to produce random sequence of bits:

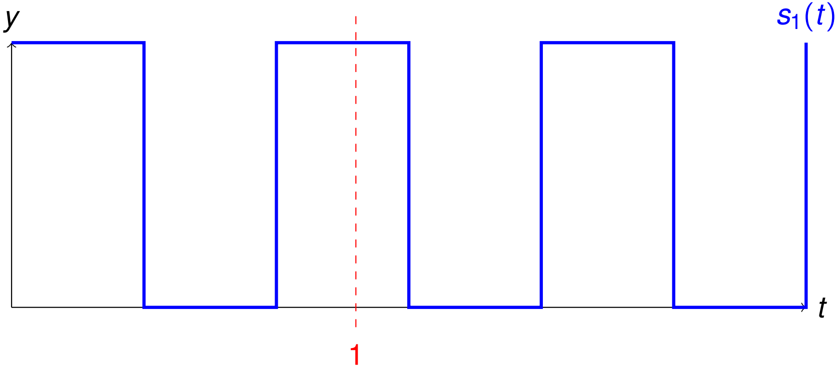


We call this simple structure an elementary TRNG in the following.

How does it work ?

For $i = 1, 2$, the signals of RO_i is:

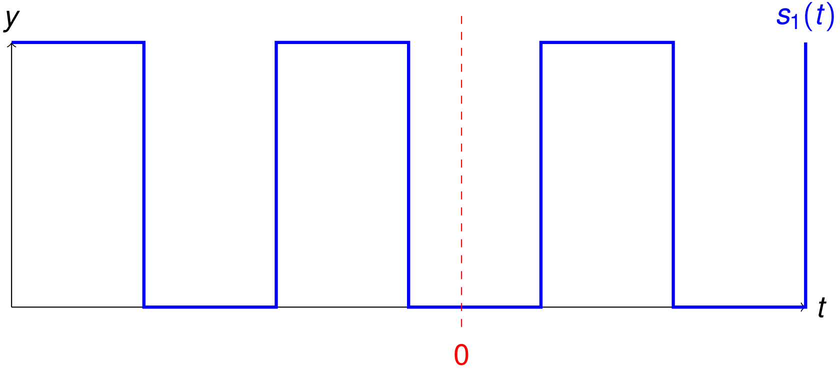
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

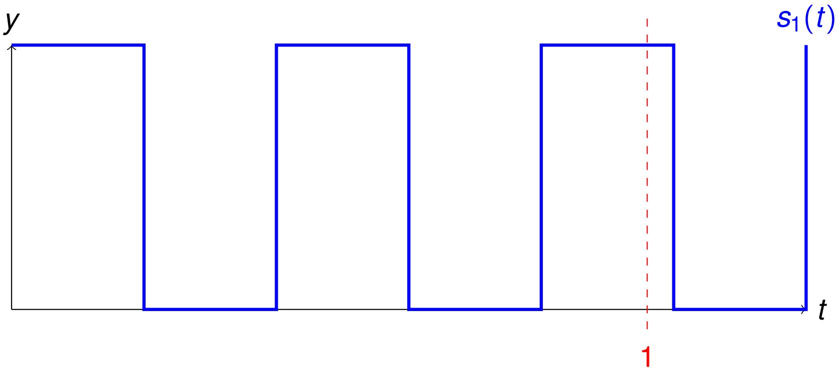
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

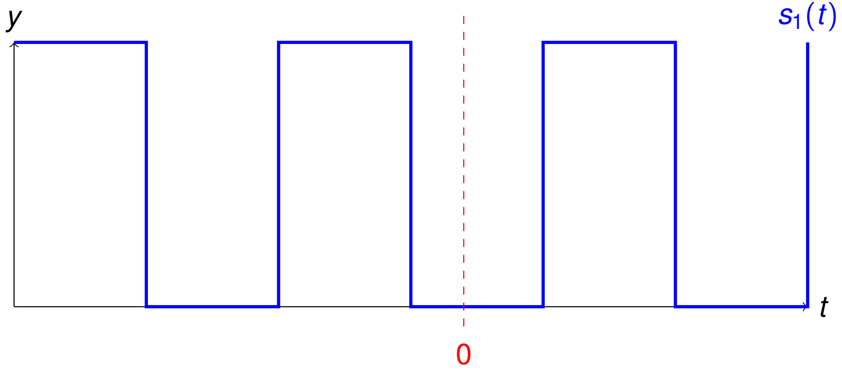
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

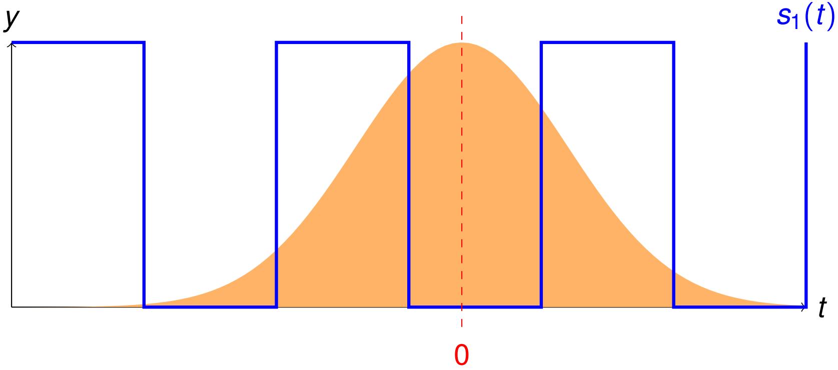
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

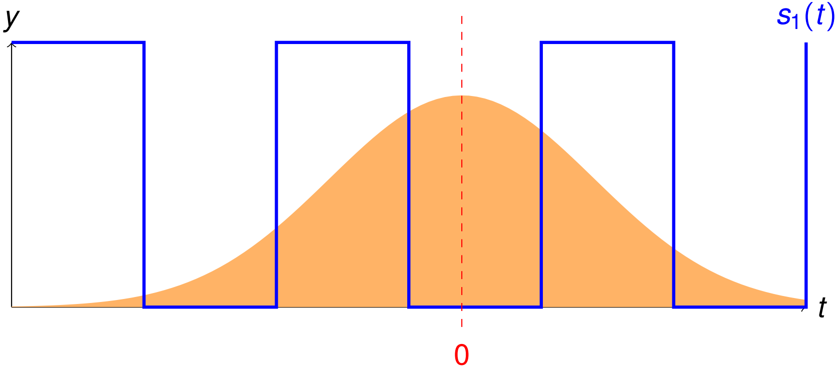
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

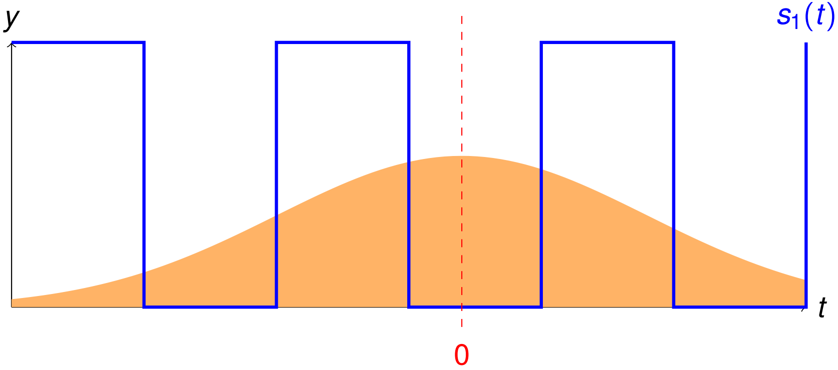
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

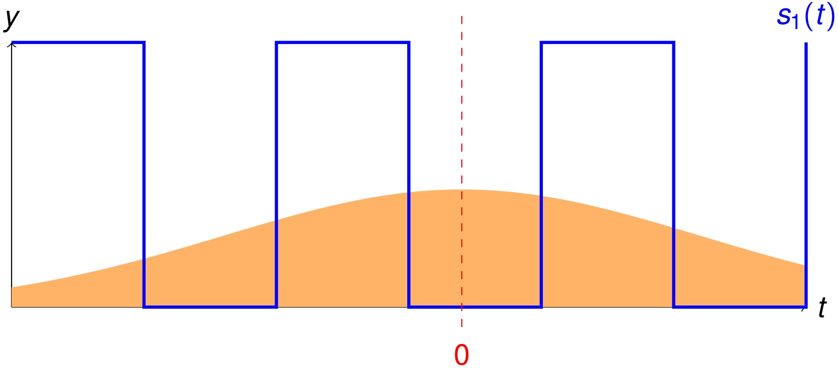
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

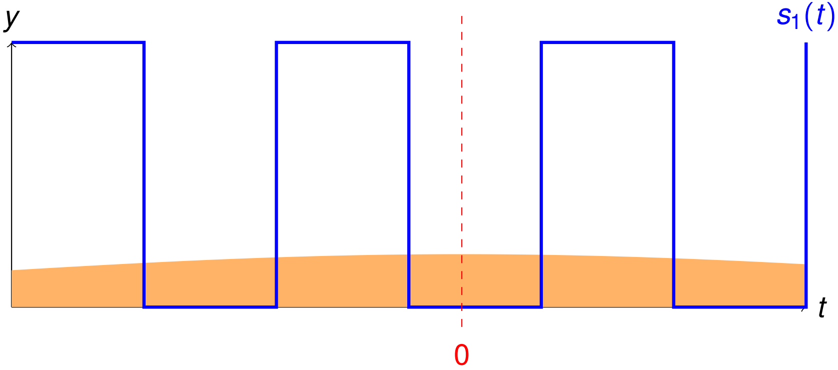
- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



How does it work ?

For $i = 1, 2$, the signals of RO_i is:

- $s_i = f(\omega_i t + \phi_i(t))$, $\omega_1 = \omega_2 = 1/T$ is the frequency of RO_i ;
- let $\phi(t) = \phi_1(t) - \phi_2(t)$ be the relative phase.



Conclusion

From our intuitive understanding, we deduce that:

- when D increases:
  - the bit rate per second decrease ;
  - the entropy rate per bit increase.
- In order to improve the entropy rate per bit we have to take D big.
- What to do in order to improve the entropy rate per second ?

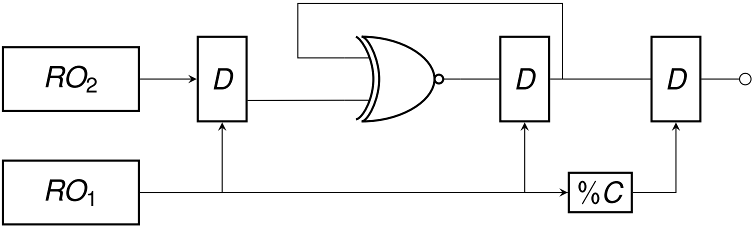
A related question

Is it more efficient

- to accumulate the entropy of a bit inside the TRNG (take D big), or
- to accumulate the entropy of a bit outside the TRNG (using a digital processing) ?

Another design

For instance, by using a xor and one bit memory:



We need a statistical model

Definition (informal)

A *statistical model* for a TRNG gives a probability distribution on output bit sequences depending on physical parameters of the TRNG.

Without a statistical model for the TRNG, it is not possible to compute the behavior of the xor with respect to output entropy.

Example

Let (x_i) be a perfectly random sequence. If we apply xor on the sequence (an even number of time) :

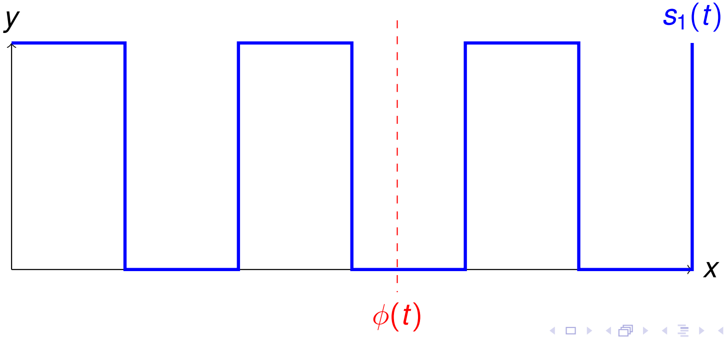
- $x_0 x_0 x_1 x_1 \dots$ we obtain 0 entropy rate;

Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t | X(t) = 1) = p(x, t).s_1(t)$.

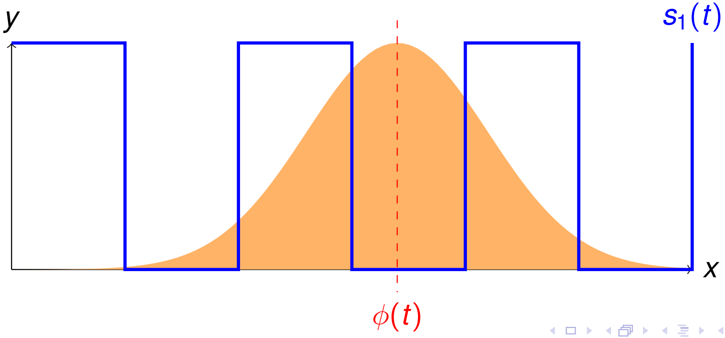


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t|X(t) = 1) = p(x, t).s_1(t)$.

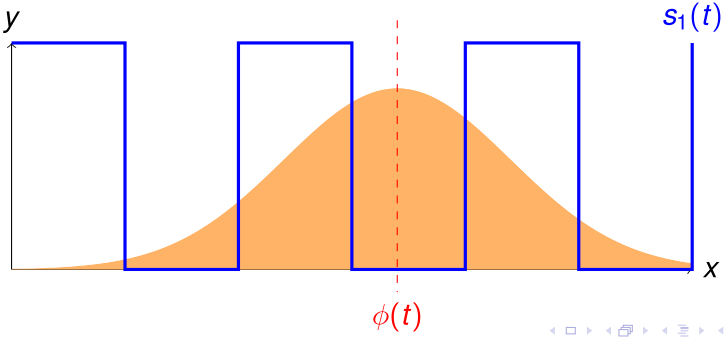


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t|X(t) = 1) = p(x, t).s_1(t)$.

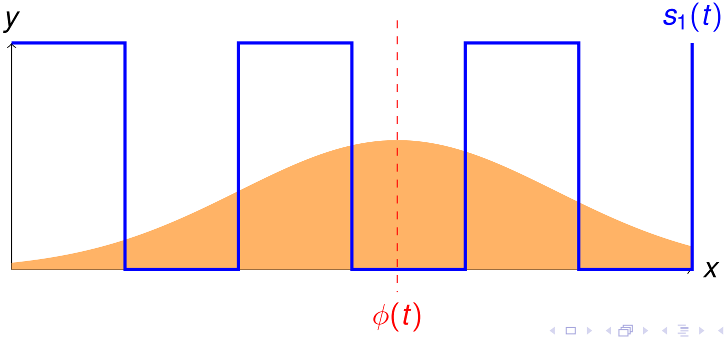


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t | X(t) = 1) = p(x, t).s_1(t)$.

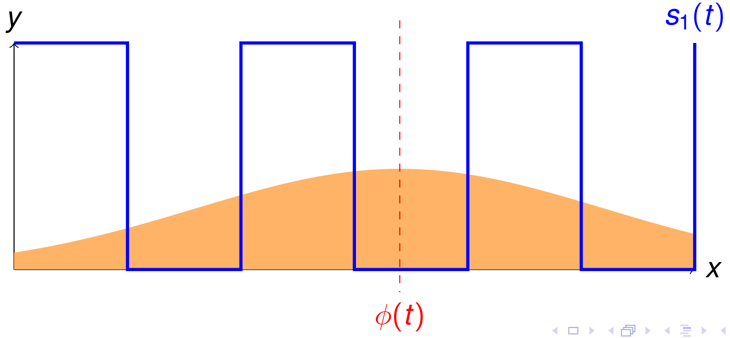


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t|X(t) = 1) = p(x, t).s_1(t)$.

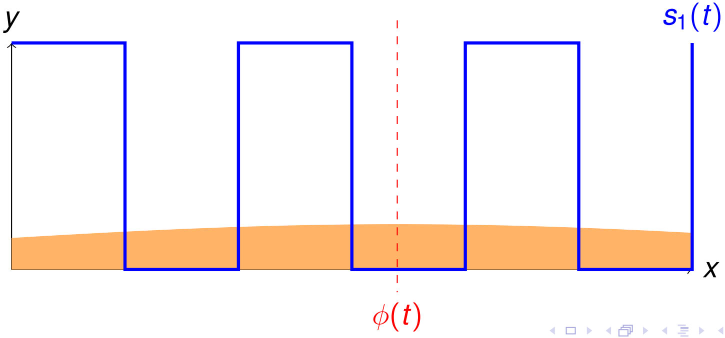


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t | X(t) = 1) = p(x, t).s_1(t)$.

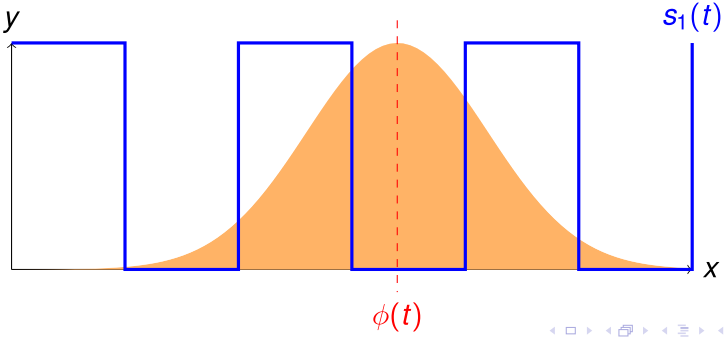


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x, t)$.

The distribution $p(x, t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x, t|X(t) = 1) = p(x, t).s_1(t)$.

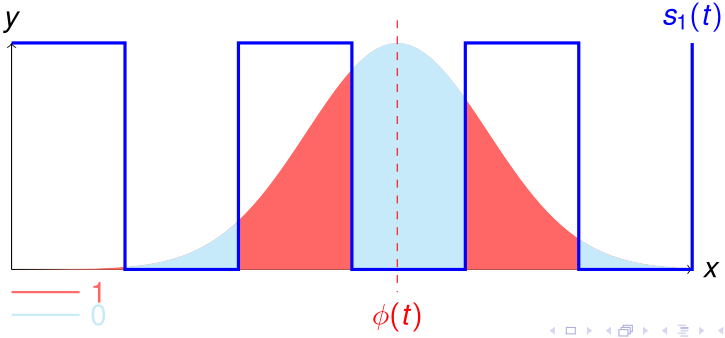


Principle of known statistical models

- The state of the TRNG is given by the relative phase $\phi(t)$.
- The knowledge of the attacker is represented by a strochastic process given by a distribution law $p(x,t)$.

The distribution $p(x,t)$ evolves following:

- a law of evolution with the time (describing the effect of the noise) ;
- the effect of sampling : $p(x,t|X(t)=1) = p(x,t).s_1(t)$.



But existing statistical models are not sufficient

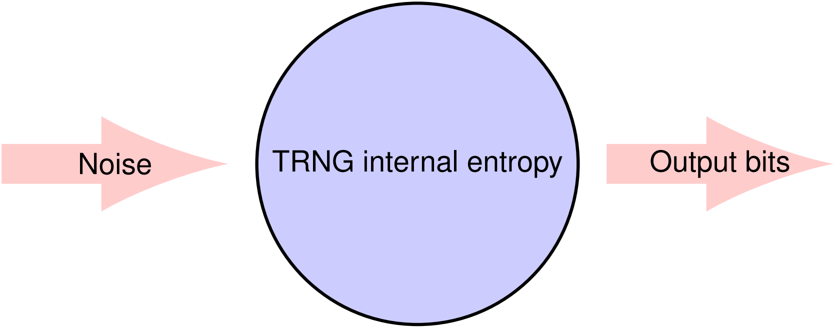
Existing statistical models are not well suited to understand:

- what's happening when the frequency of the sampling oscillator is high;
- or when the noise is very small.

Intuitive explanation : the function $p(x, t)$ becomes more and more difficult of approximate in the time or frequency domain when it converges towards a Dirac distribution.

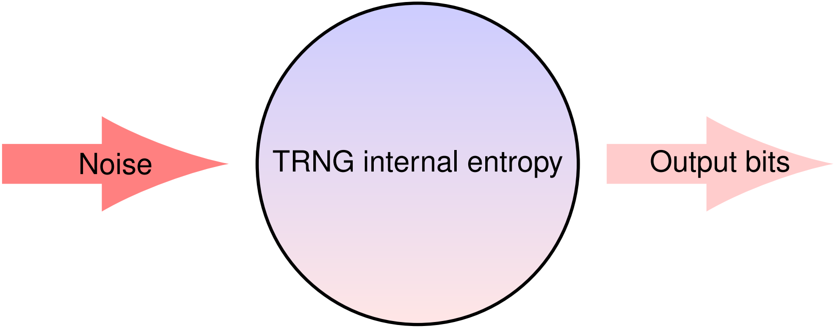
A general approach

We propose an approach based on information theory:



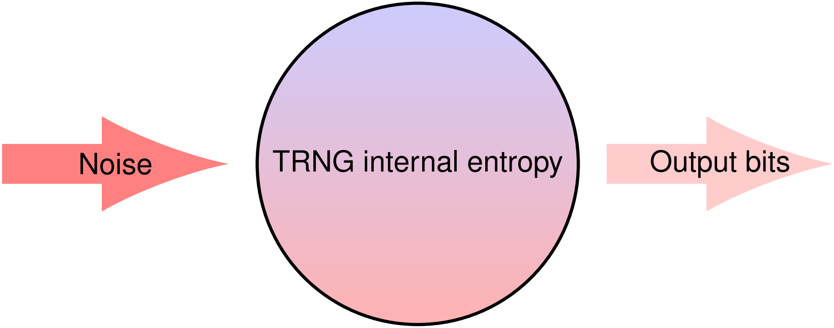
A general approach

We propose an approach based on information theory:



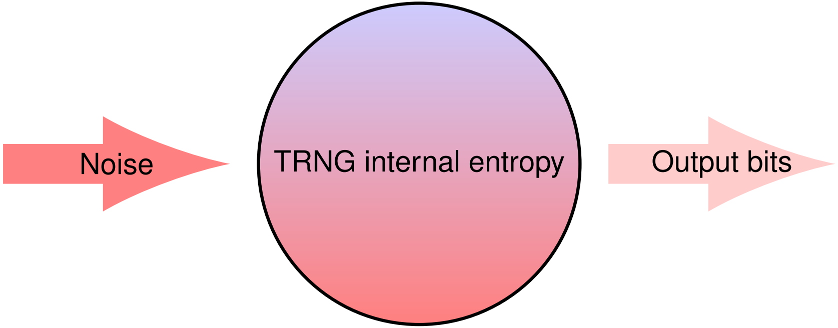
A general approach

We propose an approach based on information theory:



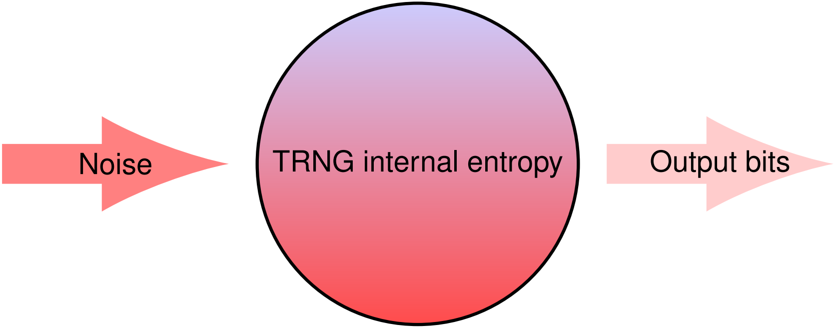
A general approach

We propose an approach based on information theory:



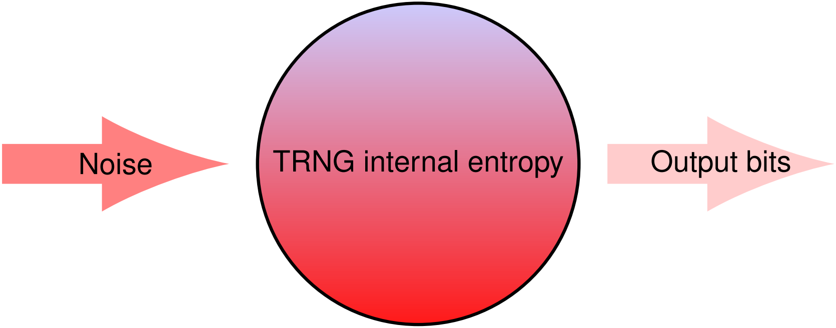
A general approach

We propose an approach based on information theory:



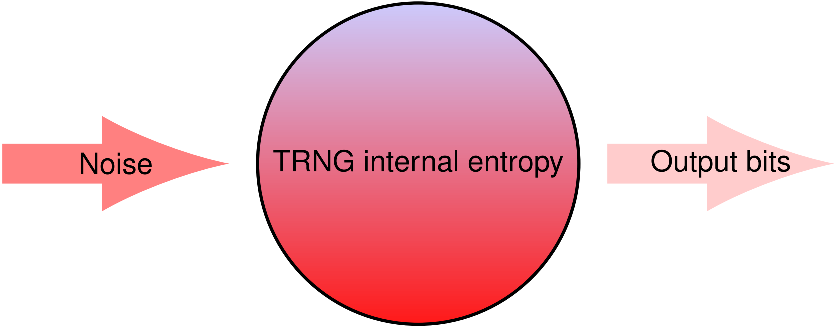
A general approach

We propose an approach based on information theory:



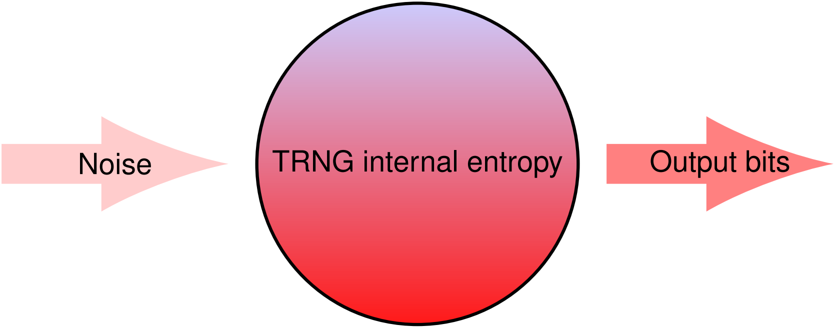
A general approach

We propose an approach based on information theory:



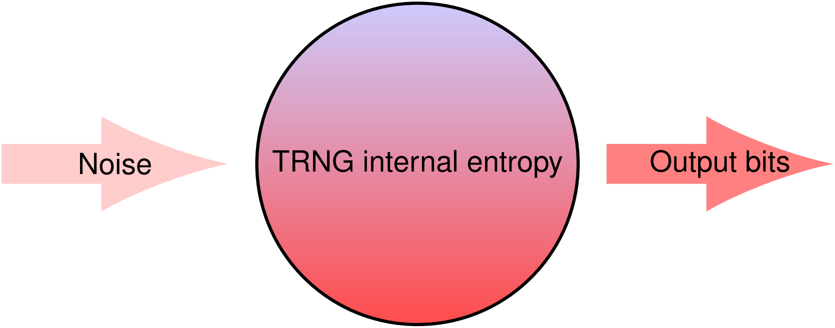
A general approach

We propose an approach based on information theory:



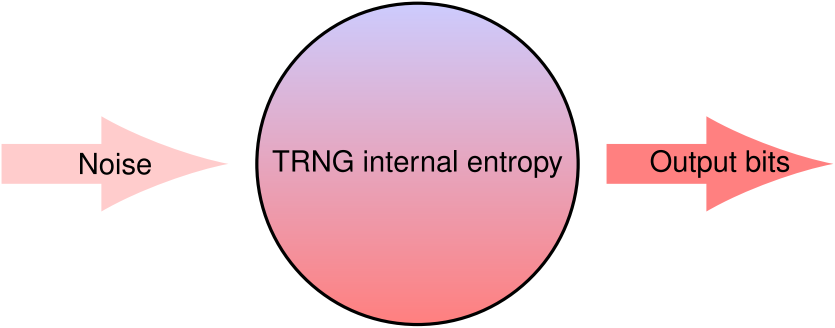
A general approach

We propose an approach based on information theory:



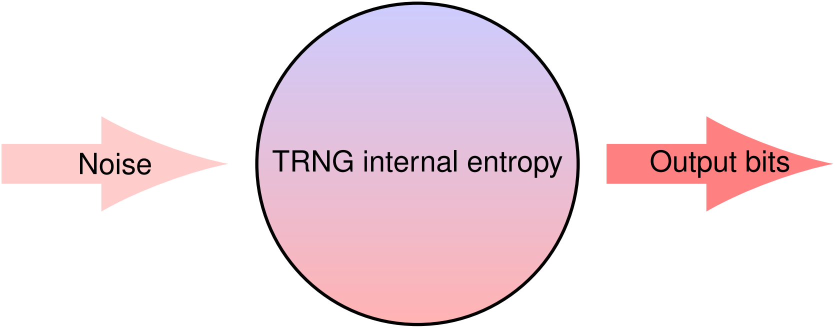
A general approach

We propose an approach based on information theory:



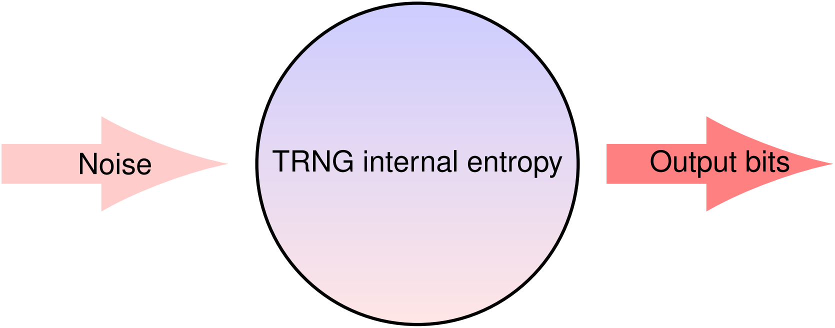
A general approach

We propose an approach based on information theory:



A general approach

We propose an approach based on information theory:



Kullback-Lieber entropy

One can give a meaning to the entropy accumulated inside a TRNG:

Definition

Let $p(x,t)$ the distribution of the phase of a TRNG, its *Kullback-Leibler entropy* is given by:

$$\mathcal{H}(p(x,t)) = \int_I p(x,t) \log\left(\frac{p(x,t)}{\mu(x)}\right) dx$$

where μ is is uniform distribution on $I = [0, T]$.

Some good properties

It verifies the following "good" properties:

Proposition

- $\mathcal{H}(p(x,t)) \in]-\infty, 0]$;
- $\mathcal{H}(p(x,t)) = 0 \Leftrightarrow p(x,t) = \mu(x)$;
- Let $X(t)$ be the binary random variable representing the distribution of the output bit at time t of the TRNG, we have:

$$\mathcal{H}(p(x,t|X(t)) = \mathcal{H}(p(x,t)) + H(X(t)),$$

where H is the usual Shannon entropy.

Effect of the $1/f^2$ noise

The evolution of the internal entropy taking into account $1/f^2$ noise, if we know the phase of the TRNG at time t is given by:

Proposition

Suppose $p(x, t|\phi(0) = x)$ evolves following $1/f^2$ type noises, the internal entropy of the TRNG is given by:

$$\mathcal{H}(p(x, t|\phi(0) = x)) = \log_2(\sigma_0\sqrt{t}),$$

where σ_0 is a parameter depending on the noise.

Remark

The quantity of information produced by the TRNG is bigger when the internal entropy is small.

Some qualitative results

Using Kullback-Leiber entropy, one can show that:

- if the bit rate increase ;
- the entropy rate per bit decrease ;
- but the entropy rate per second increase.

So in order to increase the entropy rate per second one have take D as small as possible.

Questions ?