Towards an oscillator based TRNG with a certified entropy rate

David Lubicz, Nathalie Bochard

Outline

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.

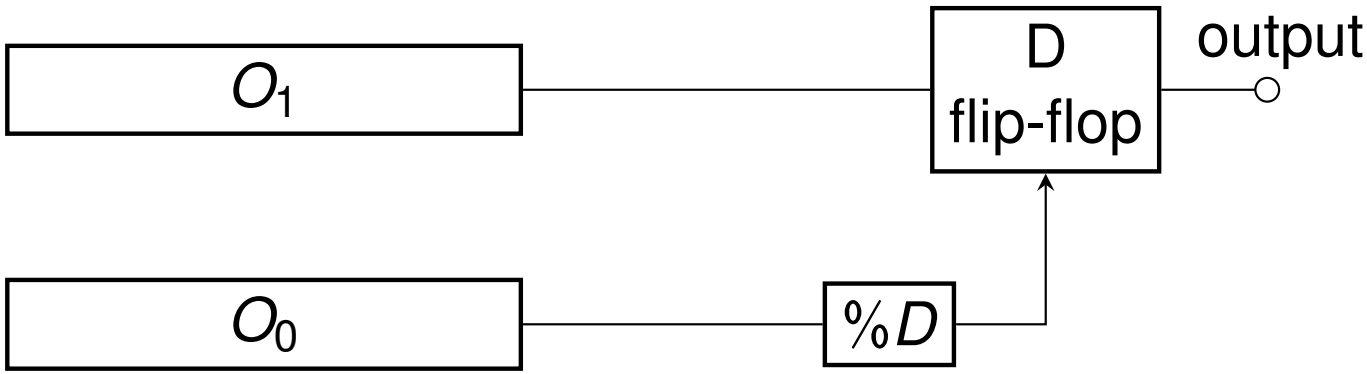
Ring oscillators I

A source of randomness commonly used in FPGA and ASIC implementations of TRNGs :

- instability of signal propagation time across logic gates;
- accumulated in so-called ring oscillators, consisting in a series of inverters or delay elements connected in a ring.

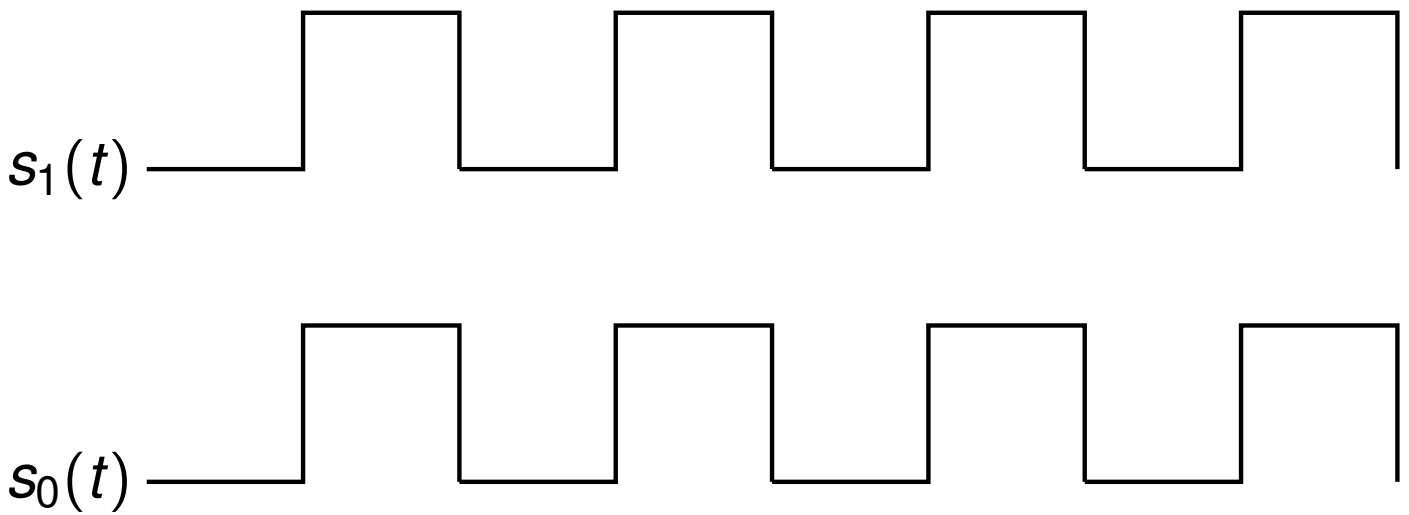
Ring oscillators II

The phase jitter of a ring oscillator is then extracted by means of a sampling unit.



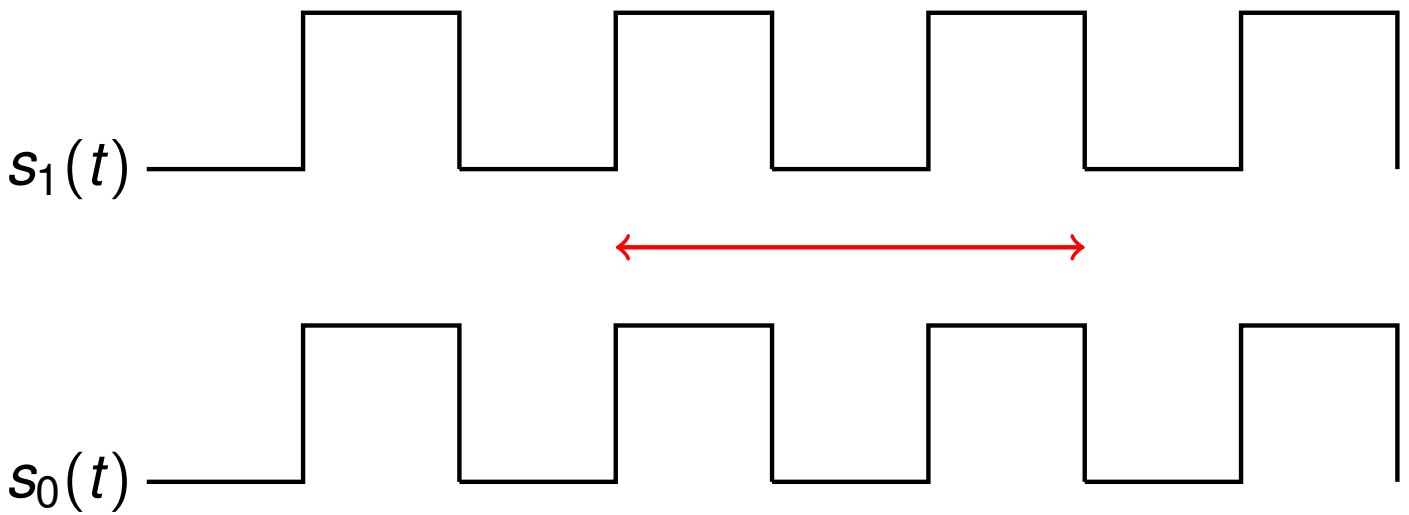
We call this simple structure an elementary TRNG in the following.

Phase jitter I



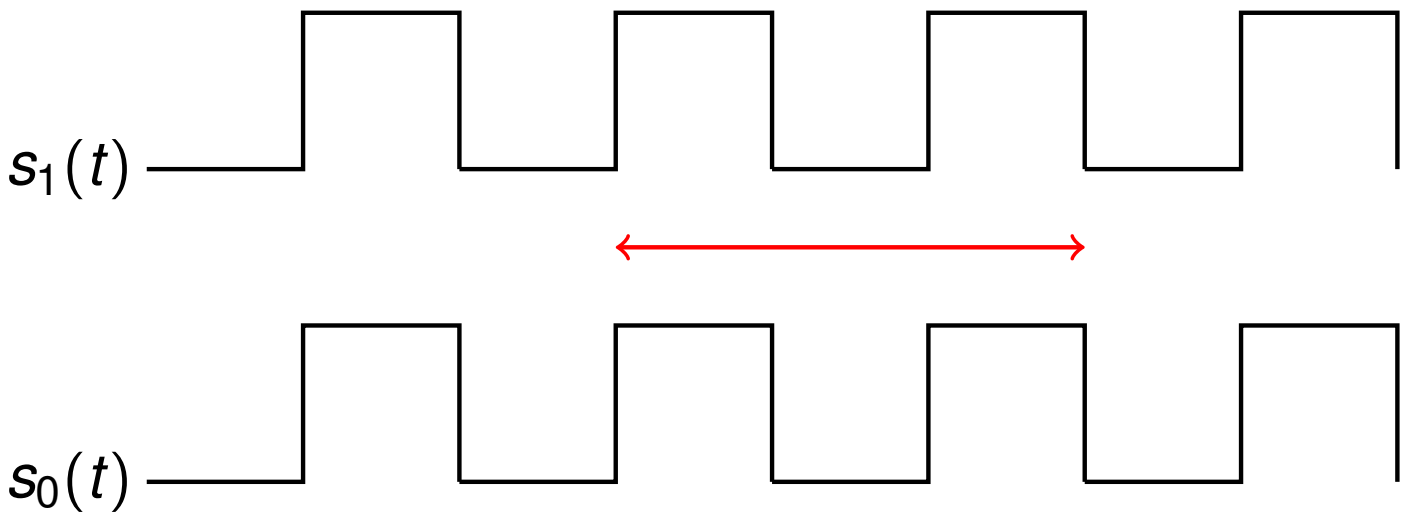
- $s_1(t) = f(\omega t + \phi_1(t))$ (sampled signal, mean period T_1),
  $s_0(t) = f(\omega t + \phi_0(t))$ (sampling signal, mean period T_0);
- $\phi_1(t)$ and $\phi_0(t)$ represent the phase jitter.

Phase jitter I



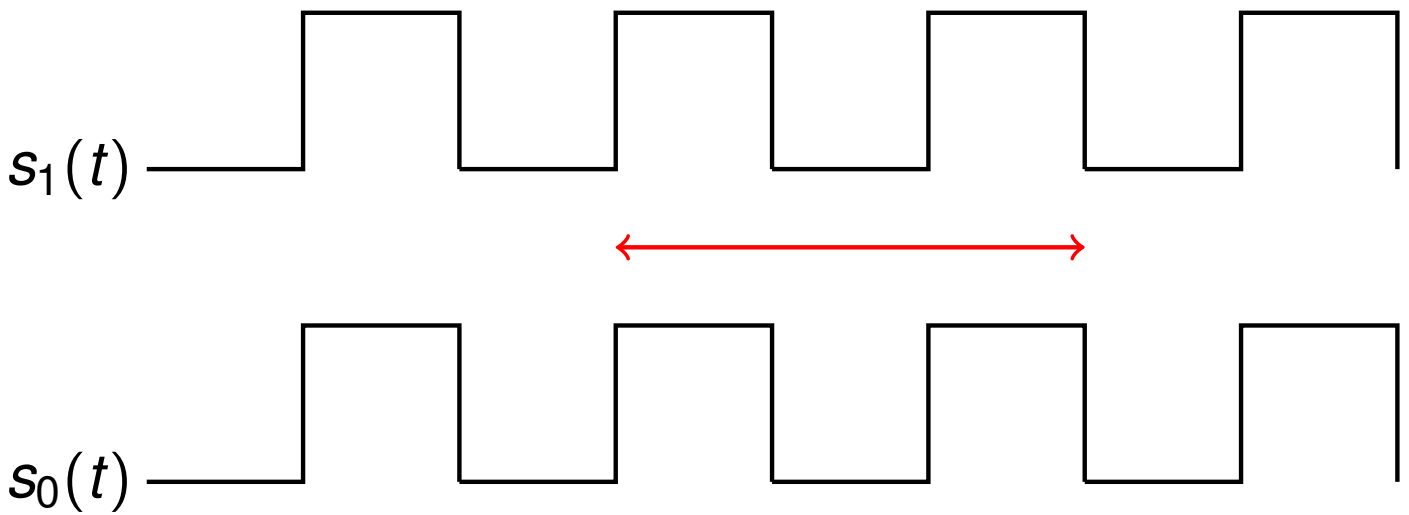
- $s_1(t) = f(\omega t + \phi_1(t))$ (sampled signal, mean period T_1),
  $s_0(t) = f(\omega t + \phi_0(t))$ (sampling signal, mean period T_0);
- $\phi_1(t)$ and $\phi_0(t)$ represent the phase jitter.

Phase jitter I



- $s_1(t) = f(\omega t + \phi_1(t))$ (sampled signal, mean period T_1),
  $s_0(t) = f(\omega t + \phi_0(t))$ (sampling signal, mean period T_0);
- $\phi_1(t)$ and $\phi_0(t)$ represent the phase jitter.

Phase jitter I



- $s_1(t) = f(\omega t + \phi_1(t))$ (sampled signal, mean period T_1),
  $s_0(t) = f(\omega t + \phi_0(t))$ (sampling signal, mean period T_0);
- $\phi_1(t)$ and $\phi_0(t)$ represent the phase jitter.

Phase jitter II

The phase jitter is made of the superimposition of different noise sources:

- important to distinguish the local component of the phase jitter from the global deterministic noises $\Rightarrow$ differential measure ;
- even the local component of the phase jitter is made of a combination of different type of noises with different statistical properties.

For instance, the random walk component of the phase jitter: its variance is linear function of the time.

Classical approach

The classical approach goes through the following steps:

- design a source of randomness;
- test it using a general purpose test suite (NIST for instance);
- tune the parameters of the GDA so that it passes the statistical tests.

Not a satisfying approach since it does not guaranty the entropy rate of the generator.

Model of a TRNG

Definition

A statistical model of a TRNG gives a distribution of probability on output bit patterns depending on physical parameters.

In a previous paper, we have described:

- a statistical modele based on a Wieiner process for the random walk component of the phase jitter;
- from which we can deduce a lower bound for the entropy rate of an elementary TRNG.

Parameters of the statistical modele

For an elementary TRNG there are two parameters which describe the random walk component of the phase jitter:

- $T_0 \mod T_1 \Rightarrow$ governs the pseudo-random behavior of the TRNG;
- the standard deviation of the distribution of the random walk component of the phase jitter accumulated during a unity of time $\Rightarrow$ governs the true random behavior of the TRNG.

Question: how to evaluate these parameters ?

Oscilloscope method

The usual method: output the signal $s_1(t)$ and analyse it with an oscilloscope. Limitations of this method:

- not precise (distortion coming from the acquisition chain);
- not practical to test each chip on a production line ;
- can not be used to check the proper operation of the device.

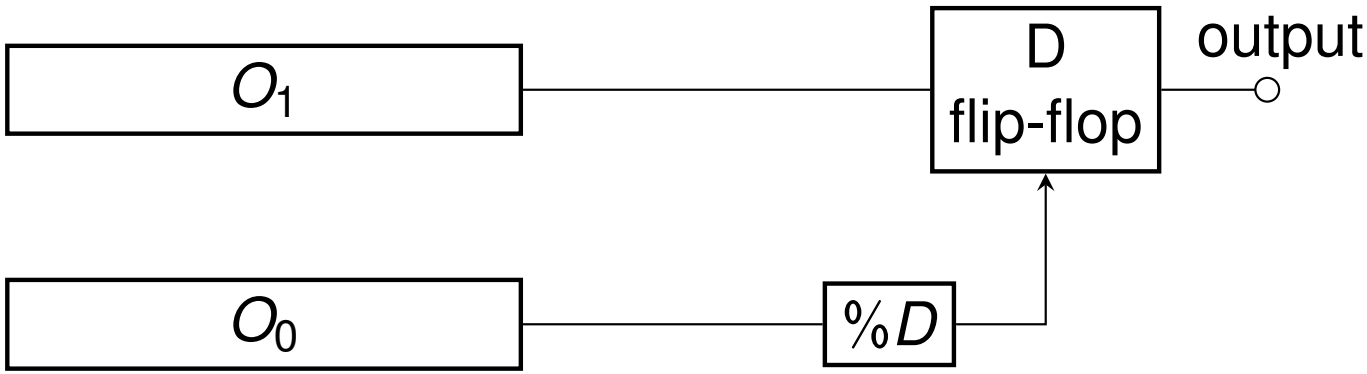
We would like an algorithm that can be embedded inside the chip.

Problem

In order to filter out the flicker noise, we have to measure the phase jitter accumulated for a short period of time:

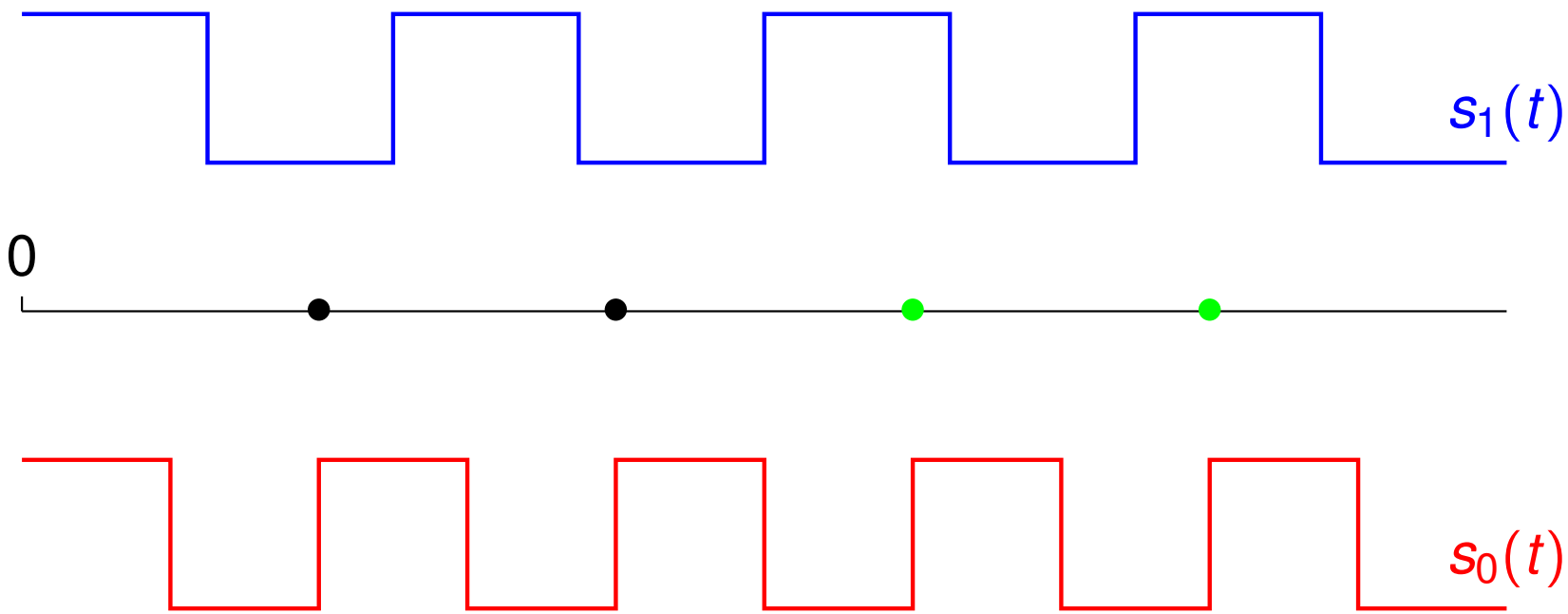
- Our experiments show that the flicker noise becomes dominant after a few hundred periods of $s_0(t)$;
- The standard deviation of the distribution of the accumulated phase jitter is much smaller than any clock signal inside the chip.

We have to be able to measure time shifts much smaller than any period of clock signal achievable inside a chip.



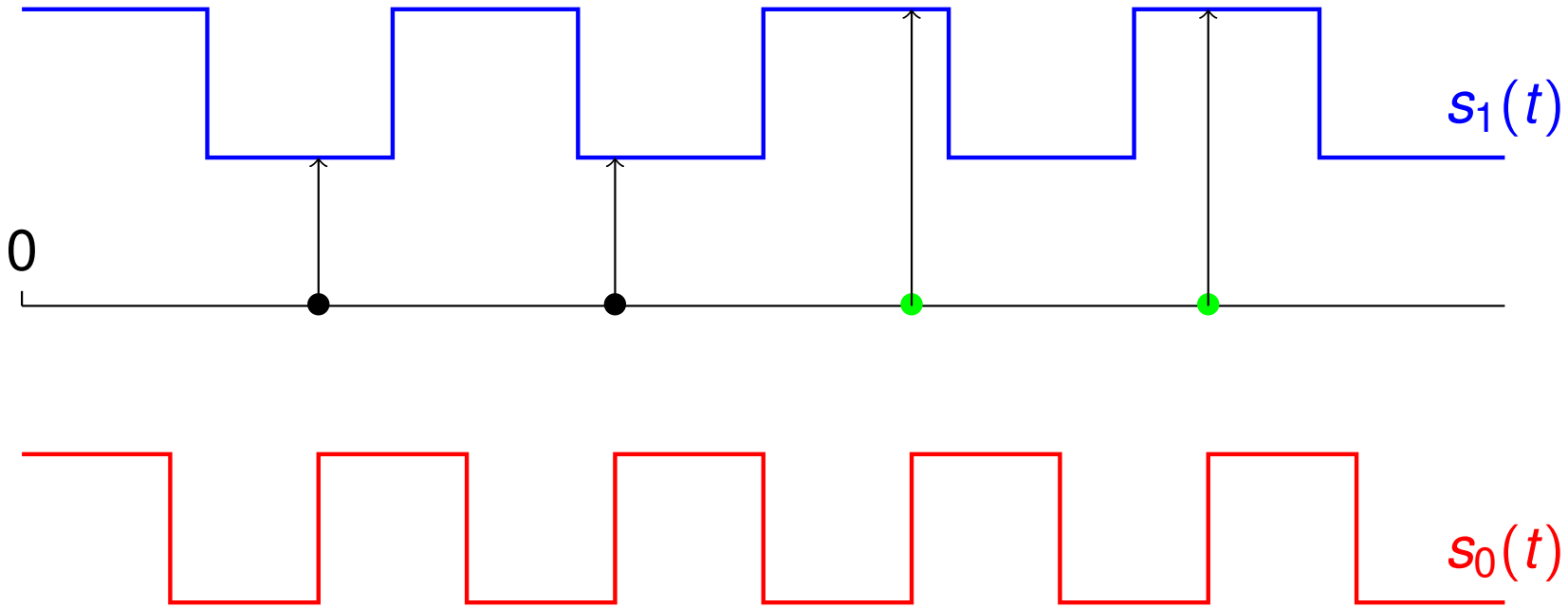
Principle: set $D = 1$ and analyse the output bit sequence.

Measure phase shift with patterns



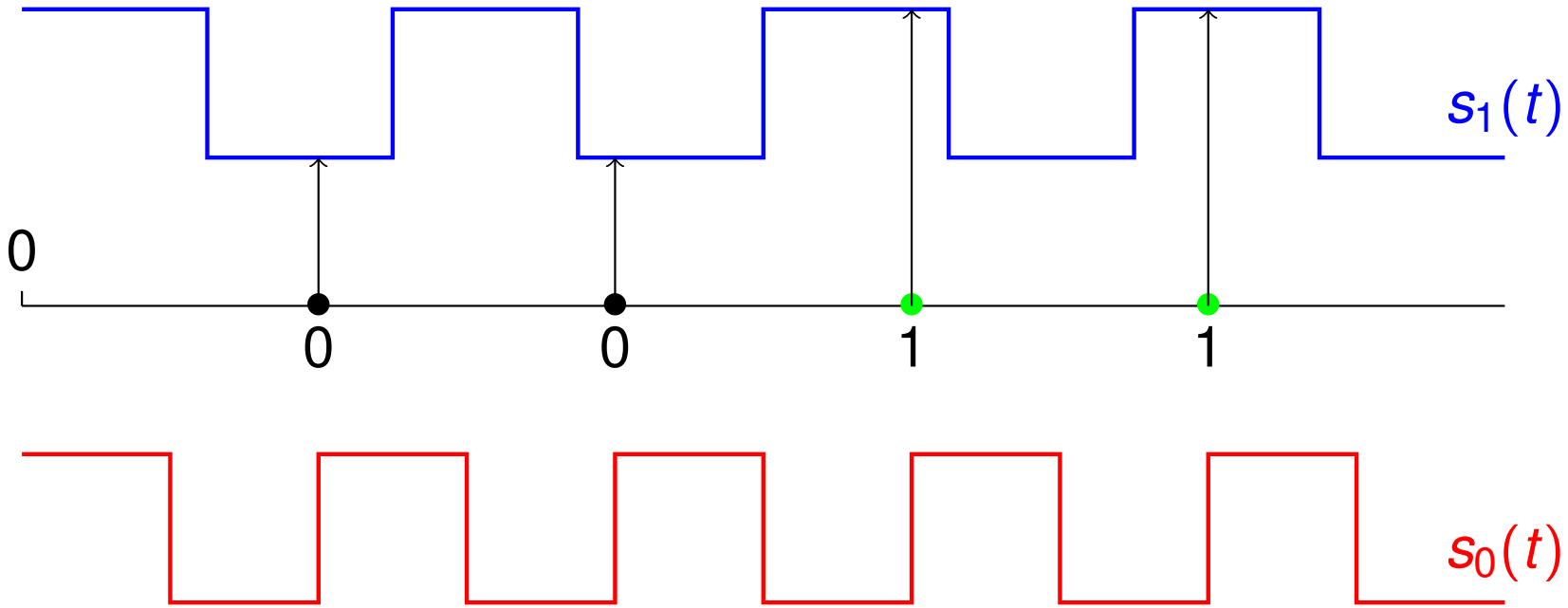
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



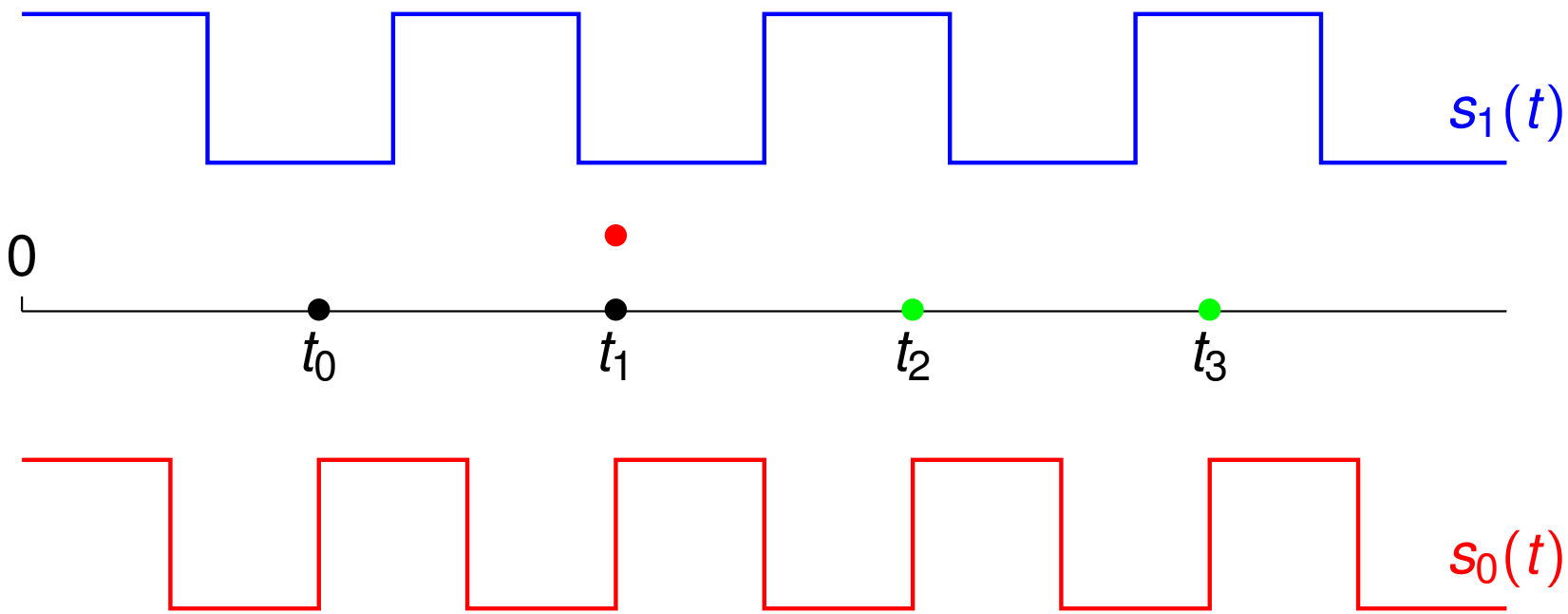
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



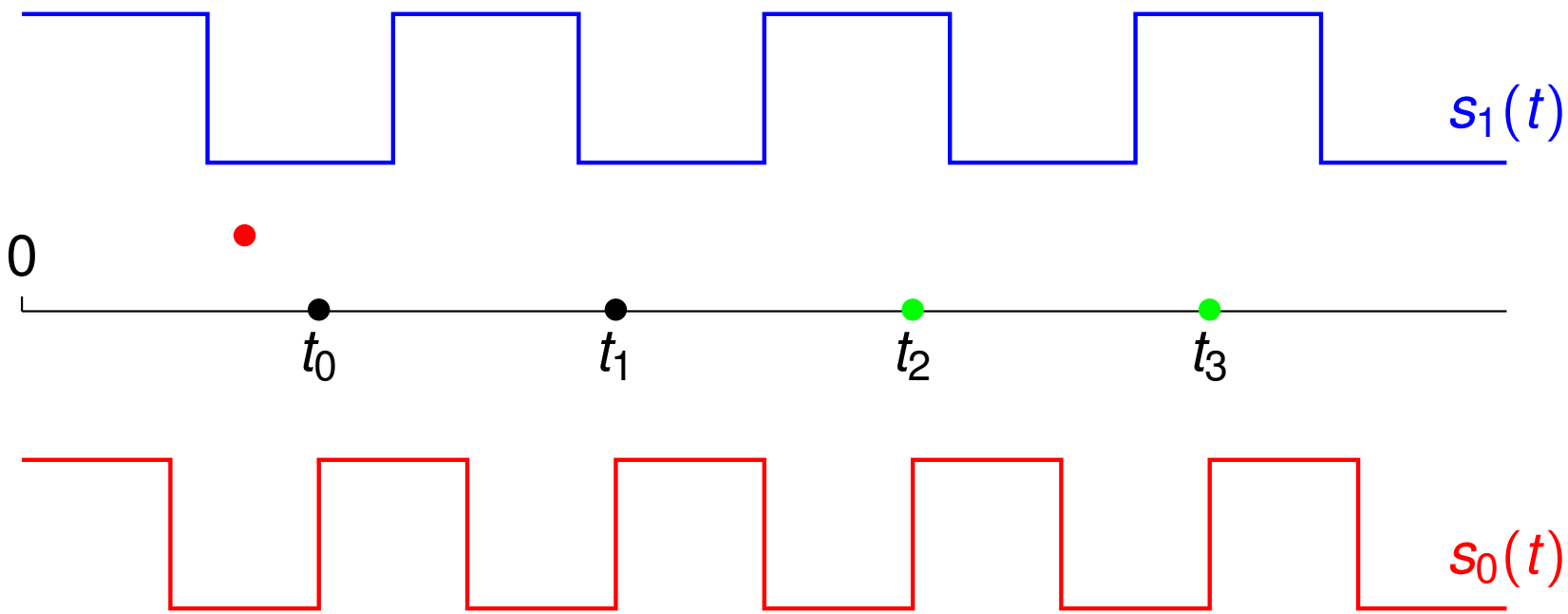
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



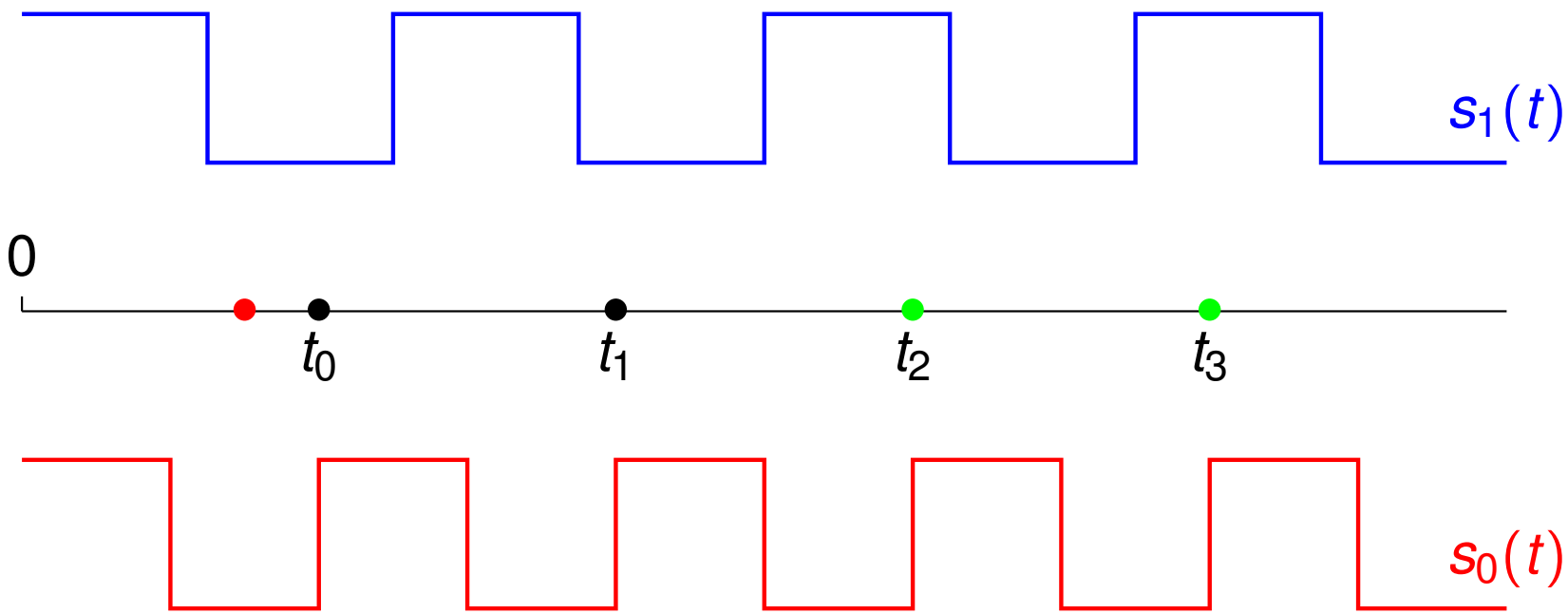
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



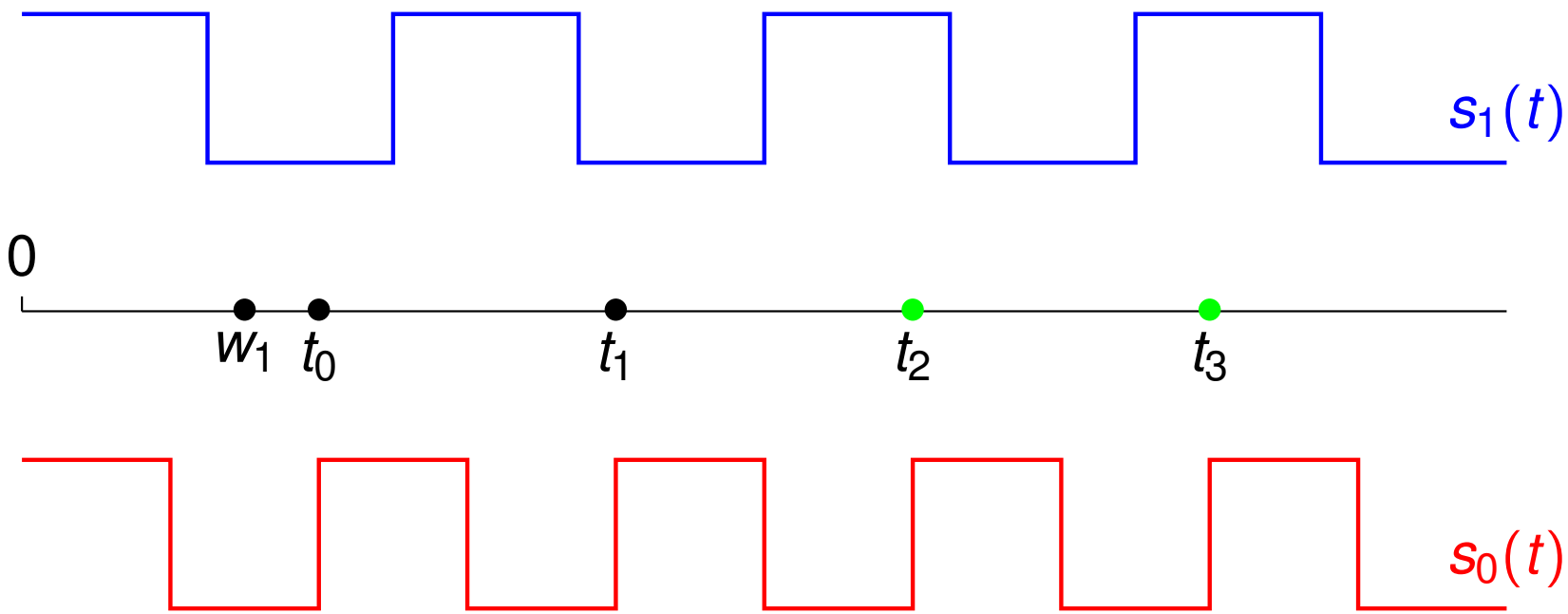
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



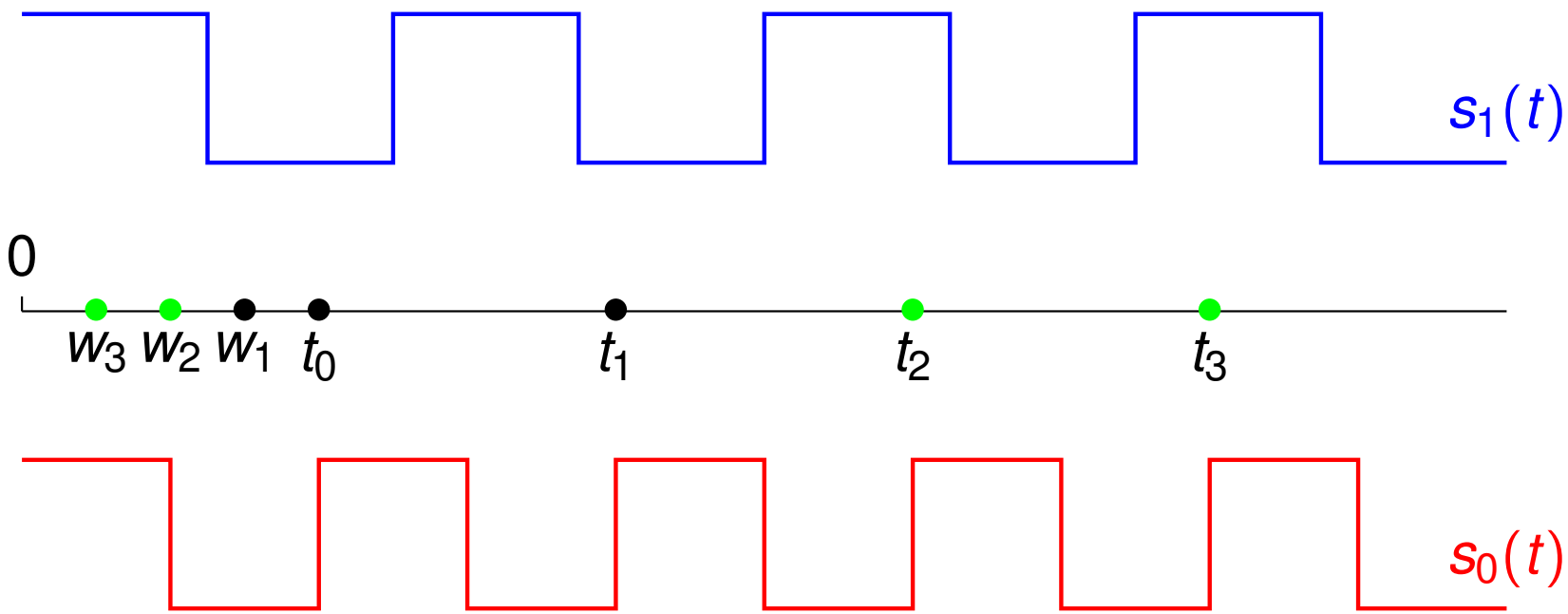
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



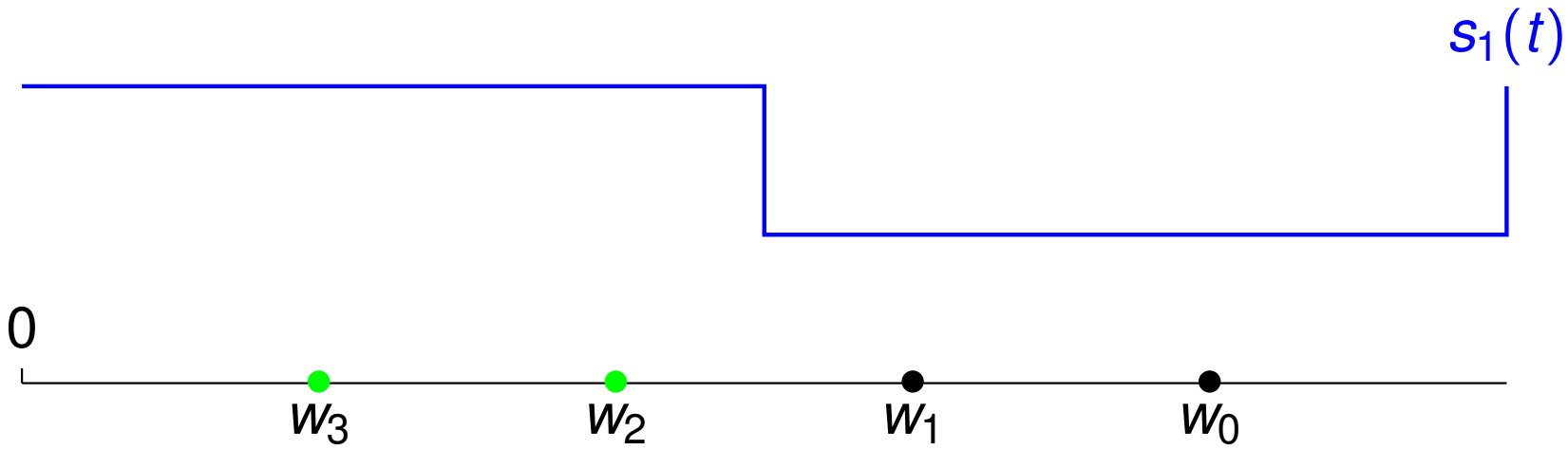
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

Measure phase shift with patterns



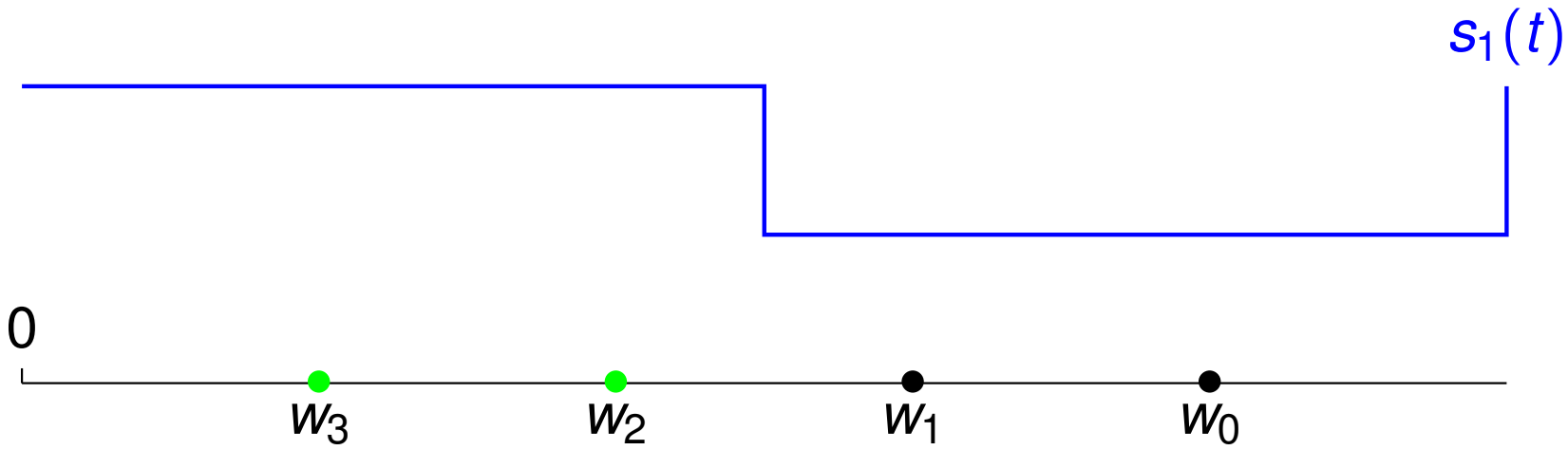
- $w_i = t_i \mod T_1$, T_1 is the mean period of $s_1(t)$.

A zoom over one period



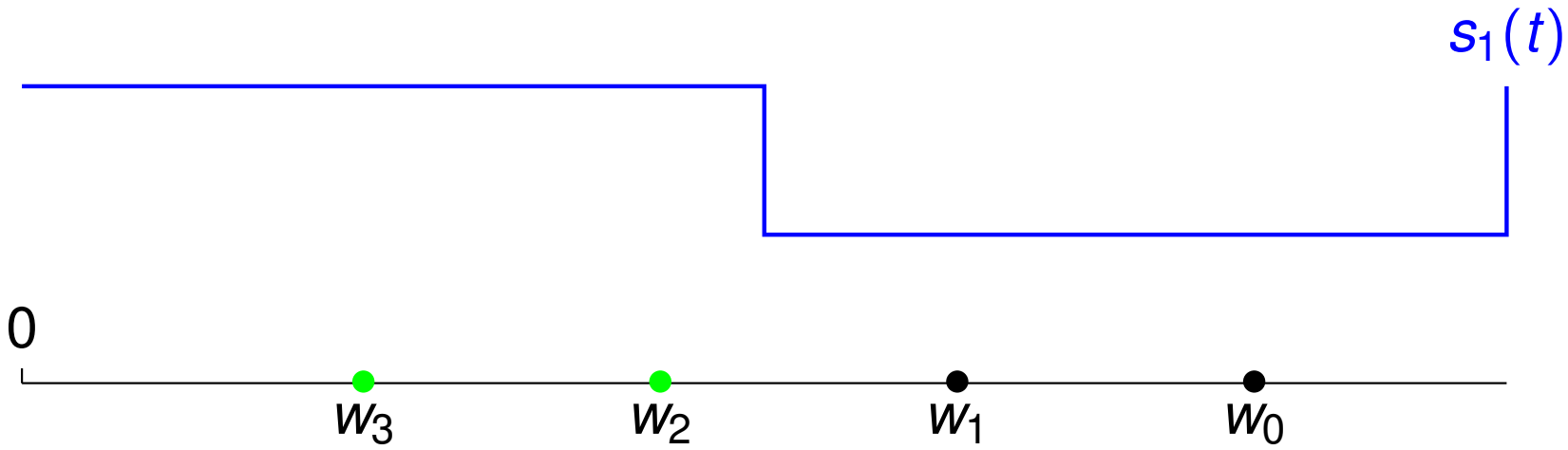
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



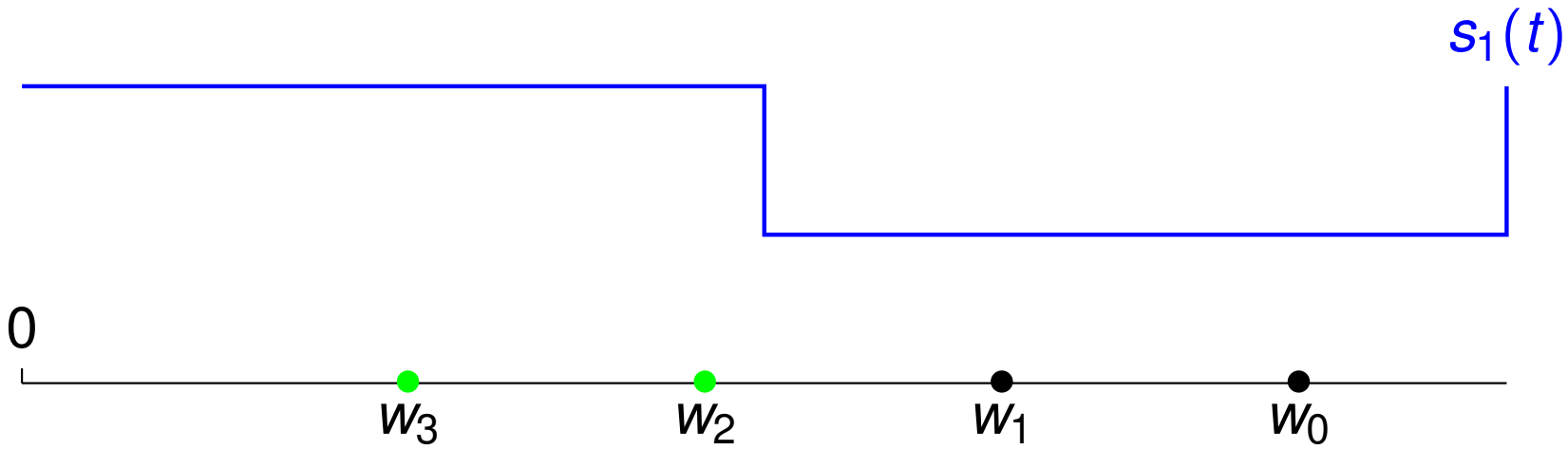
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



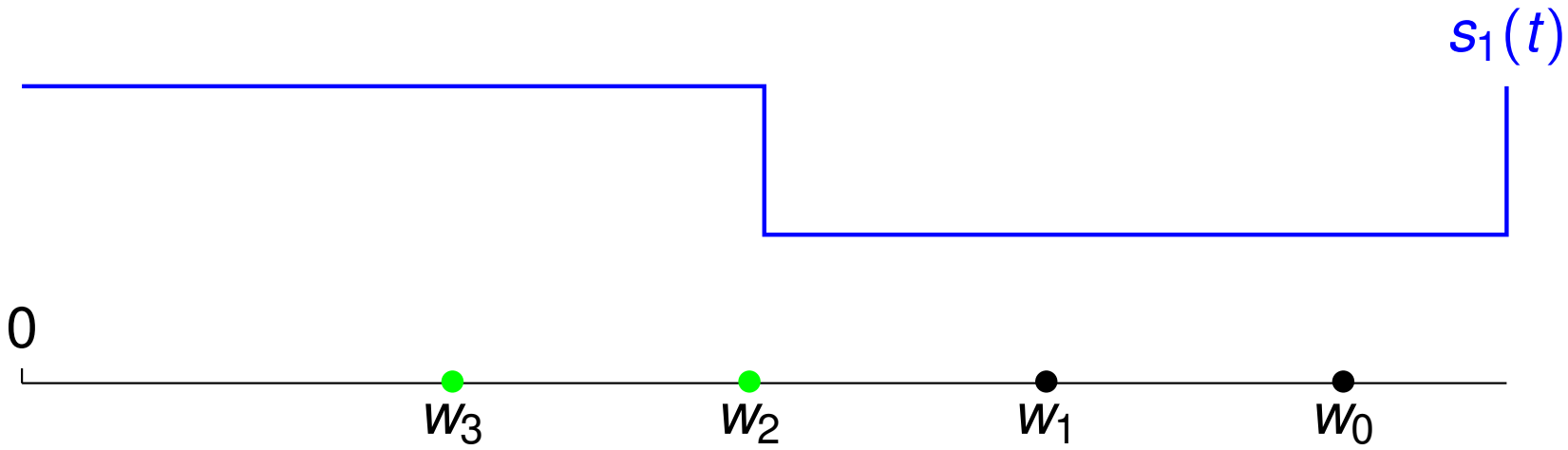
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



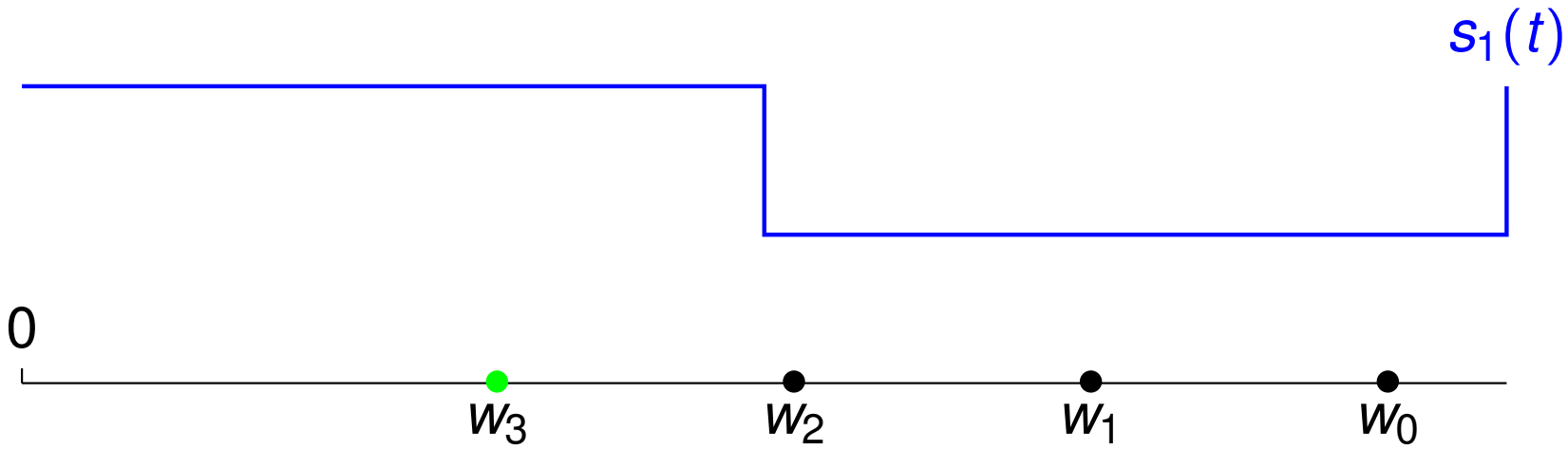
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



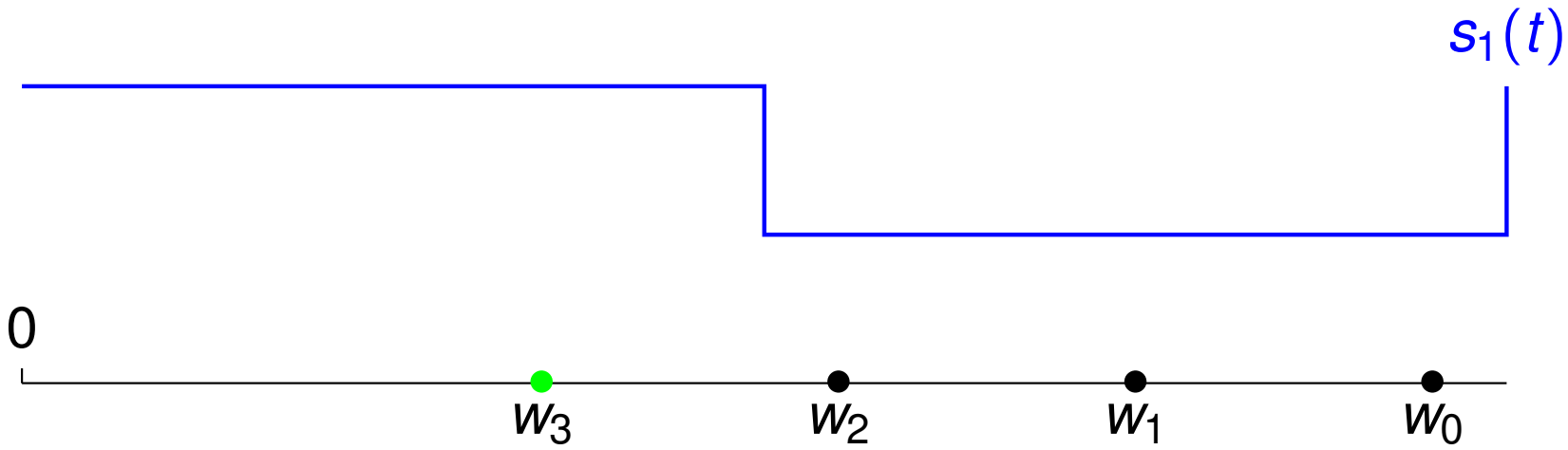
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



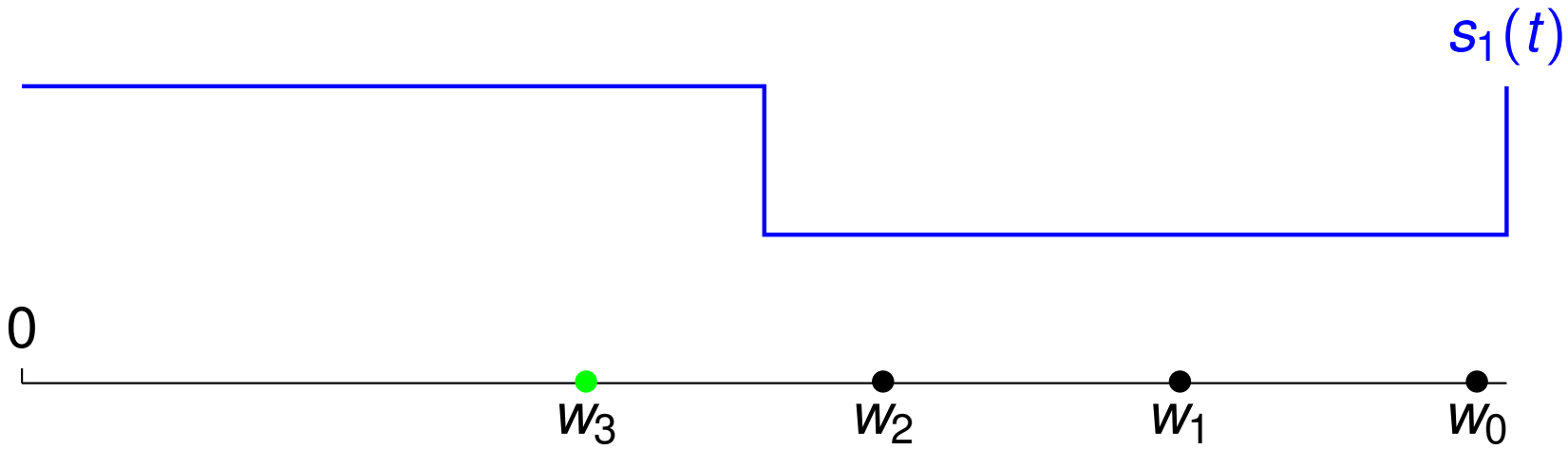
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



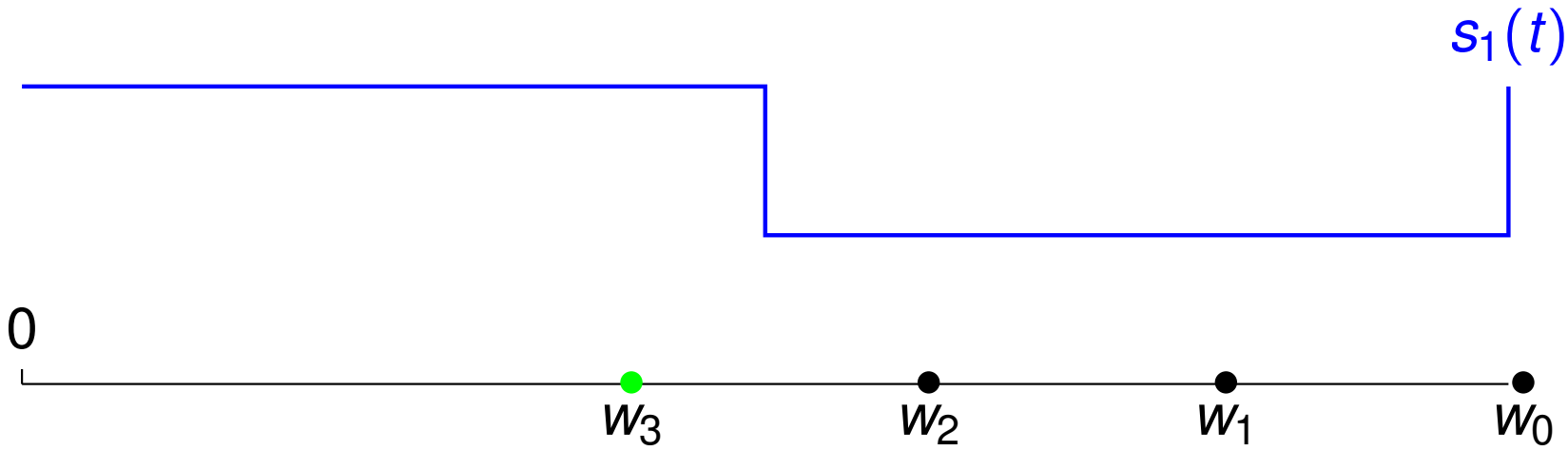
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



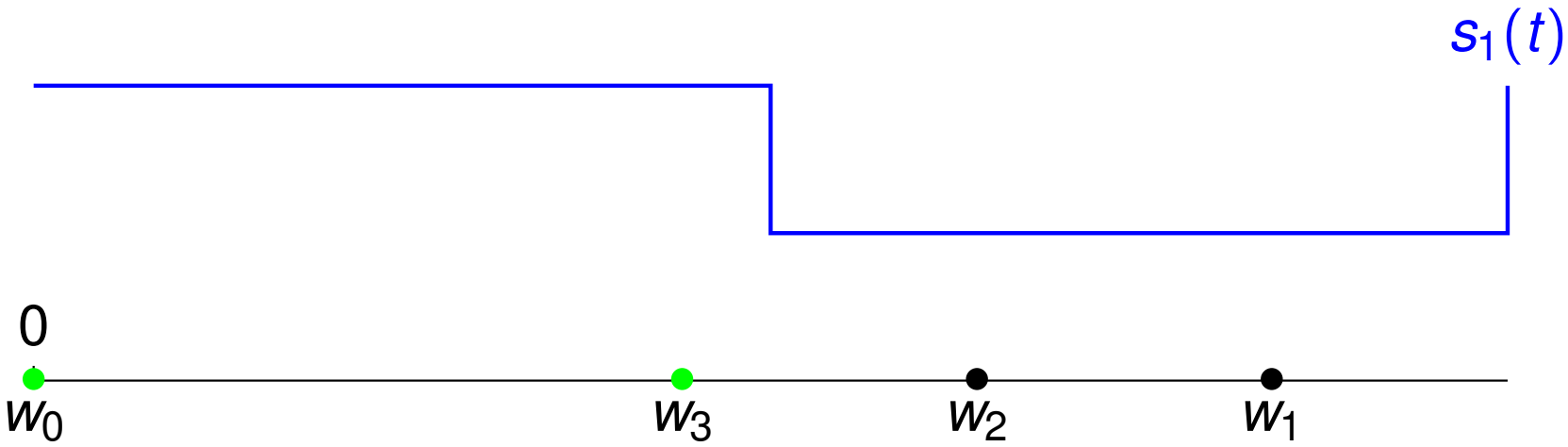
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



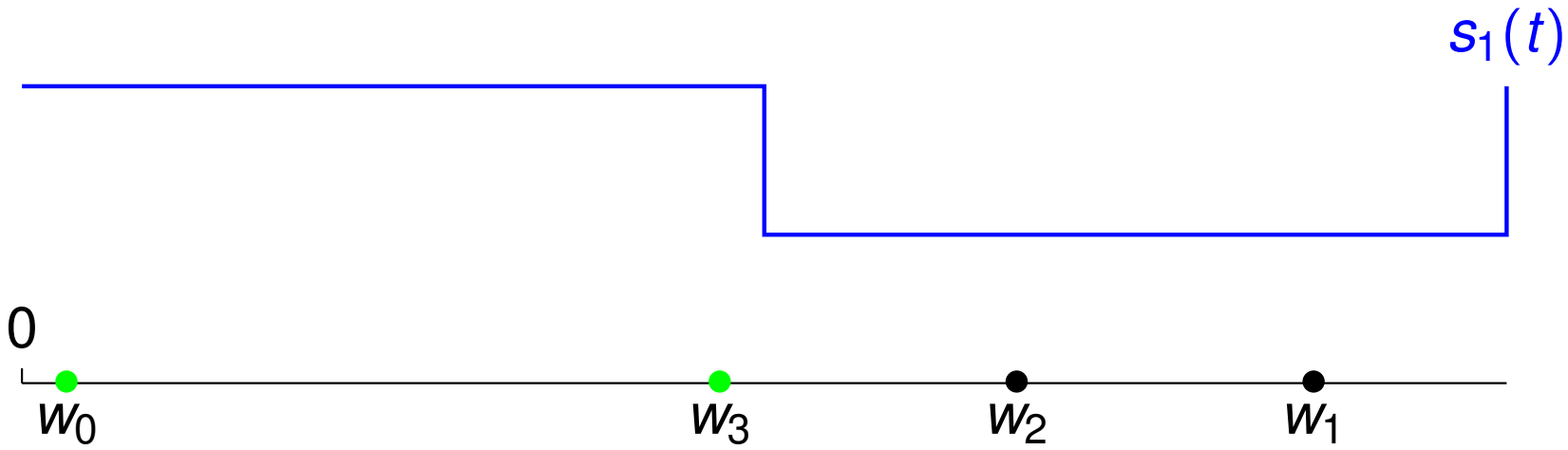
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



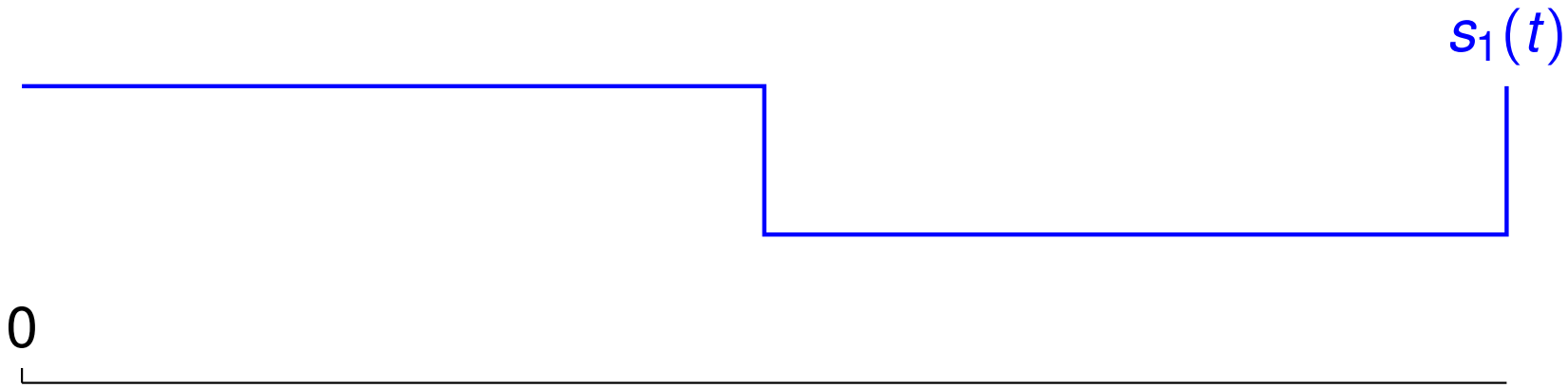
- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A zoom over one period



- the effect of phase jitter is to translate the w_i;
- a pattern of length N allows to measure the relative phase with precision $1/N.T_1$.

A fact

We can recover $T_0/T_1 \mod 1$ by computing a probability on the output sequence (b_i).

Fact

If the two half periods of $s_1(t)$ are equal (simplifying hypothesis), we have

$$1/2.\mathbb{P}\{b_i \neq b_{i+1}\} = \min(T_0/T_1, 1 - T_0/T_1).$$

Experiments

We have thoroughly tested the method with simulations and in hardware.
We give a step by step execution in the case of an Altera implementation of the elementary TRNG:

- O_1 with mean period $T_1 = 11.335\,ns$;
- O_0 with mean period $T_0 = 8.712\,ns$;
- we obtained $(b_i)_{i \in I}$ of 819200 bits from the output of the elementary TRNG with $D = 1$.

Computing the ratio of mean frequencies

We compute

$$1/2.\mathbb{P}\{b_i \neq b_{i+1}\} = 0.23144. \quad (1)$$

By Fact 2, we have
$\zeta = 1/2.\mathbb{P}\{b_i \neq b_{i+1}\} = 1 - T_0/T_1 = 0.23140$ which agrees with (1) with an error of $1/\sqrt{\sharp I}$.

Recovering the edges from patterns

The first 64 bits of the sequence $(b_i)_{i \in I}$ are:

0011001100011001 1001100111001100
0011001100011001 1001100111001100

If we reorder this pattern according, we obtain:

0000000000000000 0000011111111111
1111111111111111 1111000000000000

Accumulated distribution function of the phase jitter

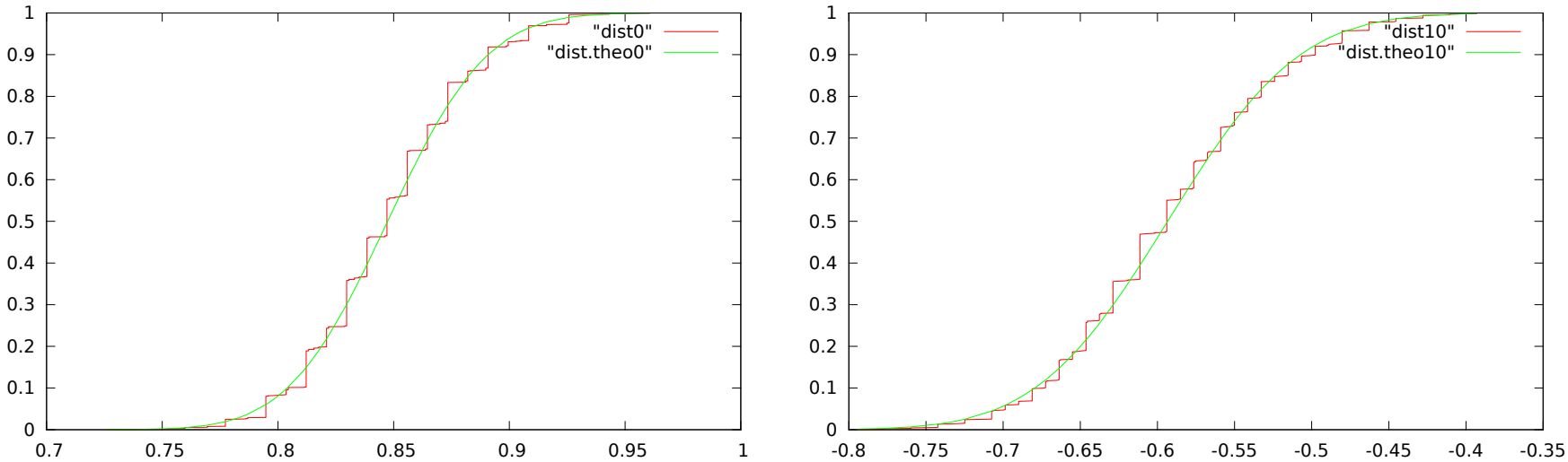
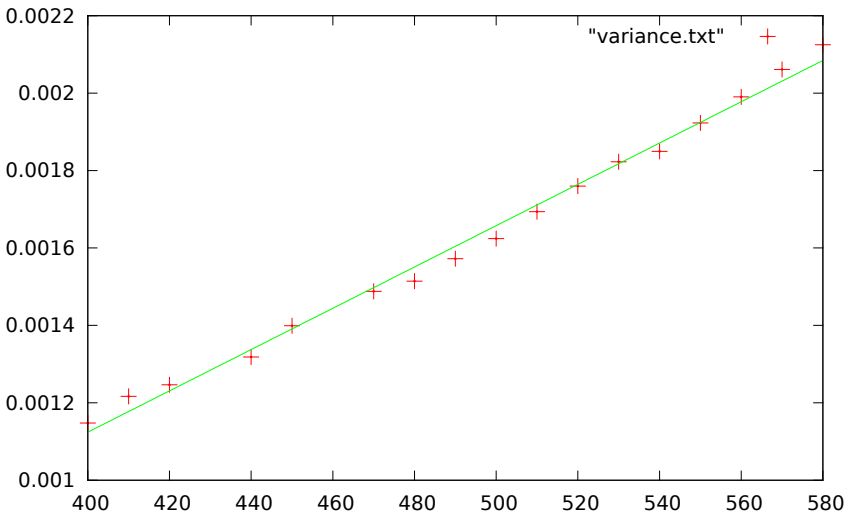


Figure: *Accumulated distribution function for* $M = 400$ *(left) and* $M = 900$ *(right); the horizontal time scale is such that* 1 *corresponds to* $1/2\ T_1$.

Accumulated variance



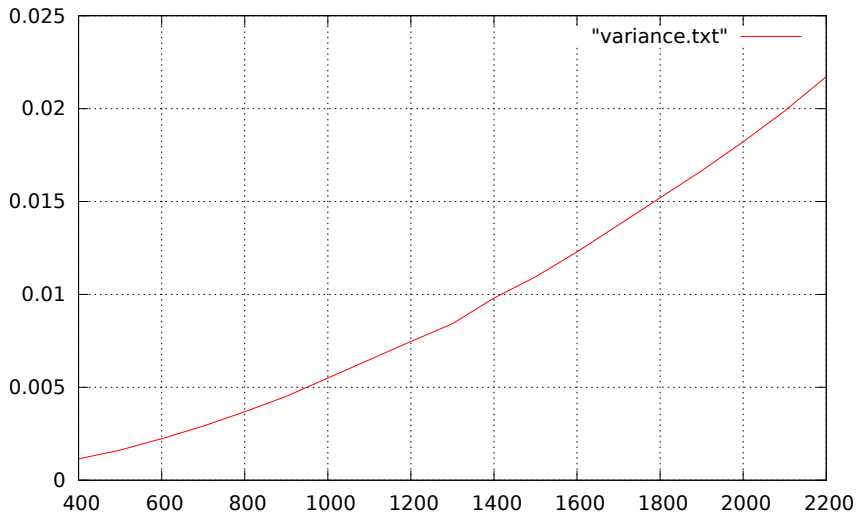


Figure: *V*(*M*) *as a function of M.*

Result of simulations

σ_c	a	$\sqrt{2}\sigma / T_1$	$\sqrt{a}$	Error percetage
$10\,ps$	$6.82494\,10^{-6}$	0.00156	0.00155	6%
$15\,ps$	$1.45836\,10^{-5}$	0.00234	0.00227	3%

Table: Results of the simulations

Results and further work

Some readings:

- *Toward an oscillator based TRNG with a certified entropy rate* with N. Bochard.

Further applications:

- lock protection ;
- detection of failure while in operation.

Questions ?