HARDWARE TROJAN ATTACKS ON RING OSCILLATOR TRNGS

Ring Oscillator TRNGs

1. Architecture
2. Principle
3. Possible attacks

under the guidance of

Prof. Rajat Subhra Chakraborty

Prof. Debdeep Mukhopadhyay

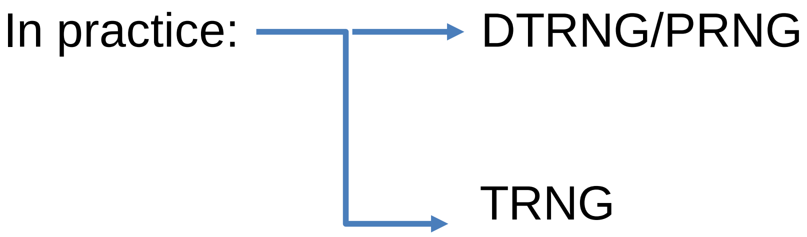
***By* Anju P. Johnson**

Research Scholar

SEAL, CSE, IIT Kharagpur

Context of this work

- Cryptography (confidential keys)
  - Unpredictable, non manipulable, good statistical properties
- Ideal RNG = generates independent and uniformly distributed random numbers



In practice:

DTRNG/PRNG

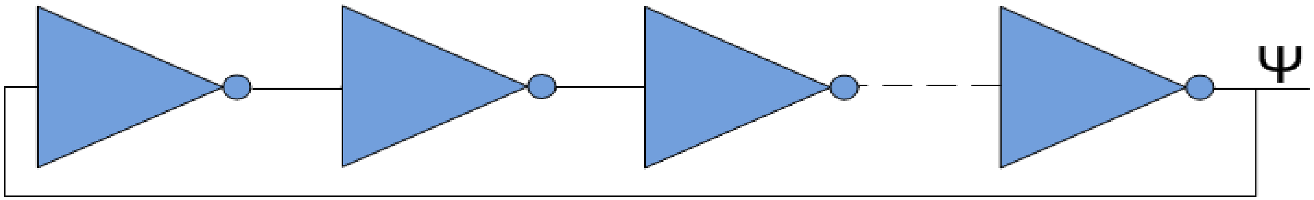
TRNG

- Good TRNG design rests on the quality of three components:
  - Entropy Source: thermal and shot noise in circuits, Brownian motion, nuclear decay etc.
  - Harvesting Mechanism
  - Post Processing
- We aim at analyzing the properties and weakness of TRNG design and point out the possible attacks on the TRNG considered.

(Combining and Sampling Ring Oscillator TRNG)

Architecture(Ring Oscillator TRNGs)

- Ring Oscillator: Chain of odd number of inverter gates in a ring configuration



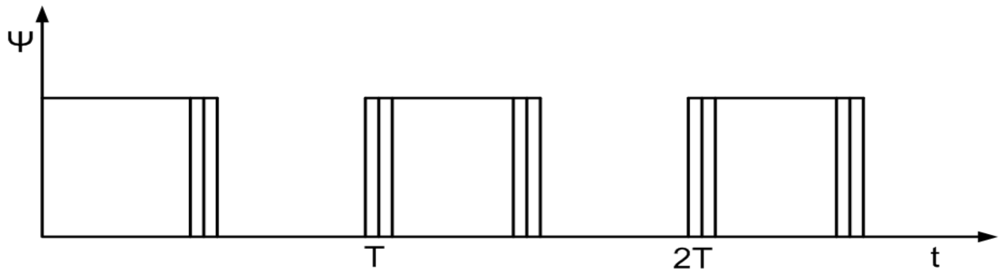
  - Output of any of the inverters will oscillate from a logic *1* to a logic *0* and back, due to the feed back.
  - A square wave is obtained by tapping into any point in the ring.

- Characteristics:
  - Ideally Ψ is a periodic square wave with period determined by the number of inverters(n) and the delay of an inverter(τ) $\boxed{T = n.\tau}$ $\boxed{\Psi(t) = \Psi(t+T)}$
  - In practice Ψ is not a perfect square wave
    - Period vibrates in a random manner $\boxed{T = T + \hat{T}}$ $\boxed{\hat{T} \in \mathbb{R}\,, {}^{-T}/_{2} < \hat{T} < {}^{T}/_{2}}$

The random variable $\hat{T}$ Commonly known as *jitter*, is the entropy to be harvested

Architecture cont…

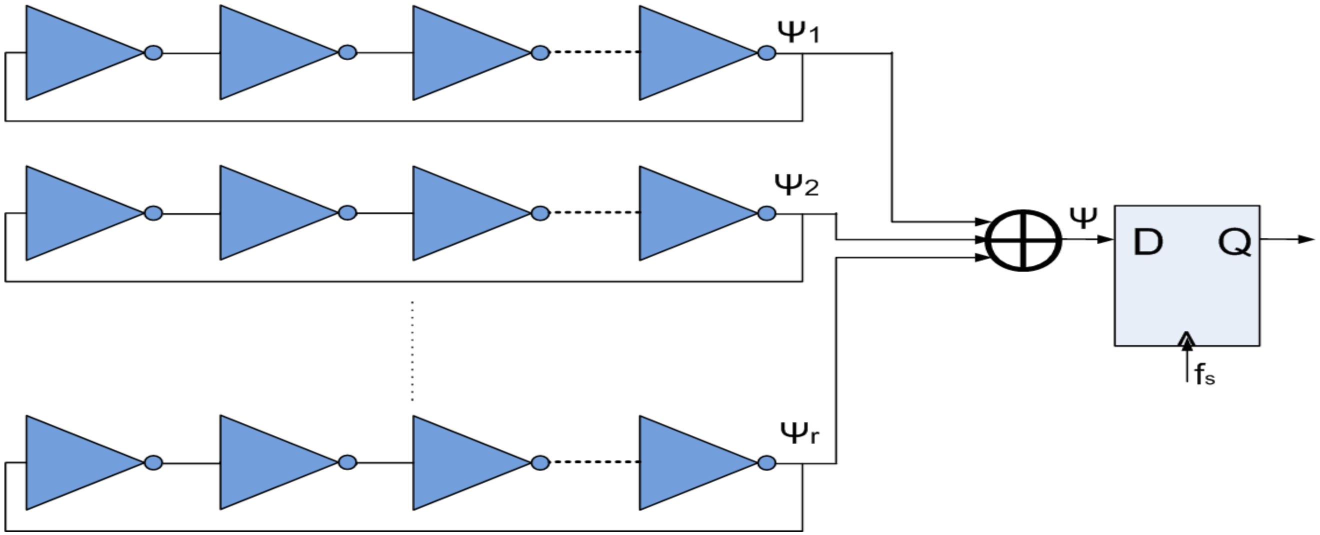
- A typical oscillator output is depicted in the figure
  - Jitter is represented by extra lines at each transition of the waveform



- Coupled Oscillator
  - Sampling the output of one ring oscillator using another
  - Requirement: The periods of the two oscillators should be well matched
    - Then, probability of sampling from the transition region will be high
    - Otherwise, sampling happens more in the deterministic part of the waveform
  - Difficulties:
    - Exactly matching the period of the two oscillators is difficult
    - Due to imperfections, the two signals may drift relative to one another, and this makes fragile TRNG designs

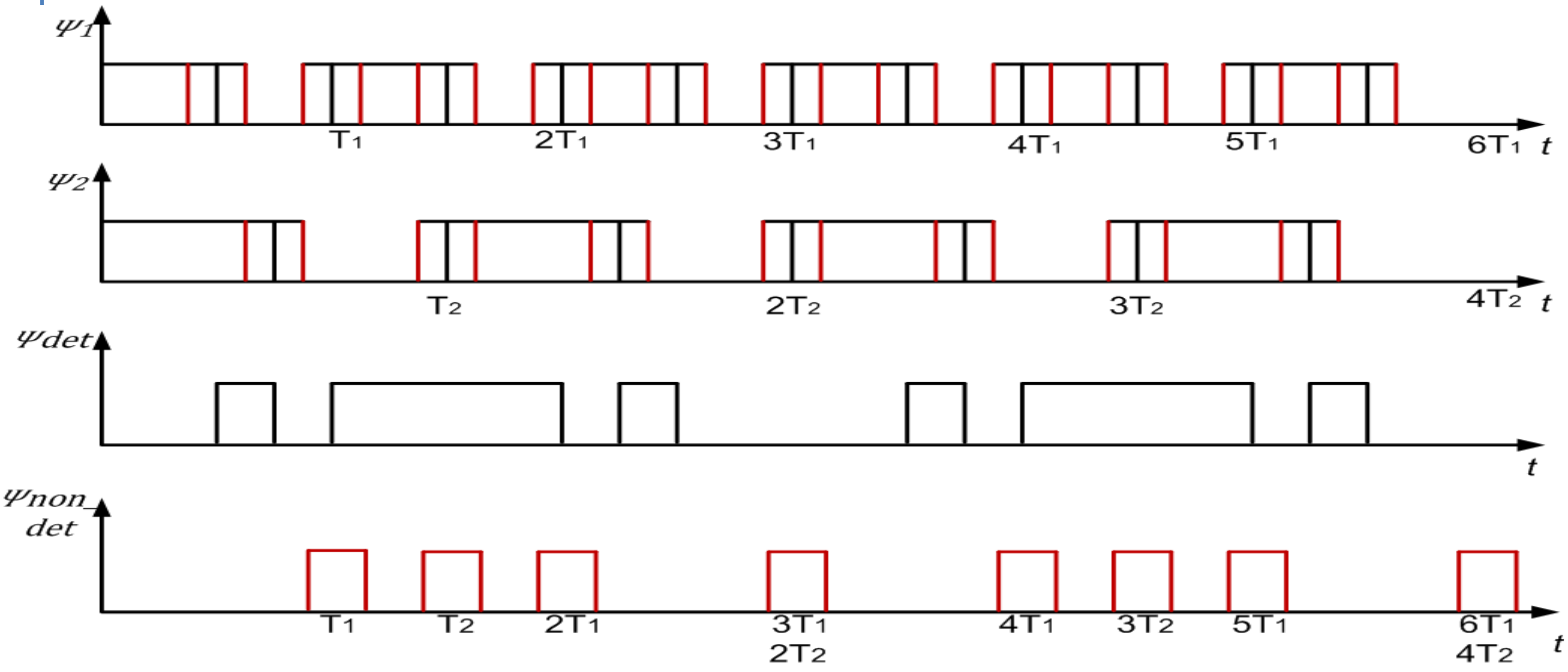
Architecture cont…

- Combining and Sampling Oscillator
  - r distinct oscillator rings
  - i-th ring consists of n_i inverters
  - The optimal values for r and ni needs to determined
  - All the output Ψ_j of r ROs are *XOR*-ed to generate the output signal Ψ
  - The *XOR* function is typically implemented as a binary *XOR*- tree
  - The output Ψ is sampled by a clock of frequency fs



B. Sunar, W.J. Martin and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," , *IEEE Transactions on Computers* , vol.56, no.1, pp.109,119, Jan. 2007

Architecture cont…



- Consider the output signal Ψ for two RO rings with clock period $2T_2= 3T_1$
- Consider the non deterministic transitions
  - The two oscillators contribute a transition zone at any even multiple of T_2
  - Due to such overlaps some entropy is lost

Aim : Populate the entire spectrum with such nondeterministic transition

The URN Model

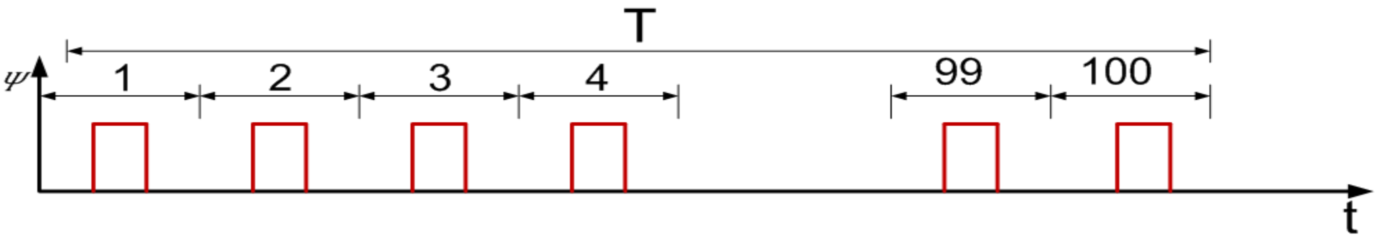
- Suppose *Rj* is a RO with time period *T=Tj*
  - *0, T, 2T, 3T…* → L to H transitions
  - *T/2, 3T/2, 5T/2…* → H to L transitions

Assumption: Jitter is harvested only from "up" transitions of the waveform

Assumption: In any open time interval (*mT-T/4, mT+T/4*) there is a unique point *t* where the signal crosses (*L+H*)/2 volts and this *t* behaves as a normally distributed random variable with mean *mT* and some variance $\sigma_j{}^2$

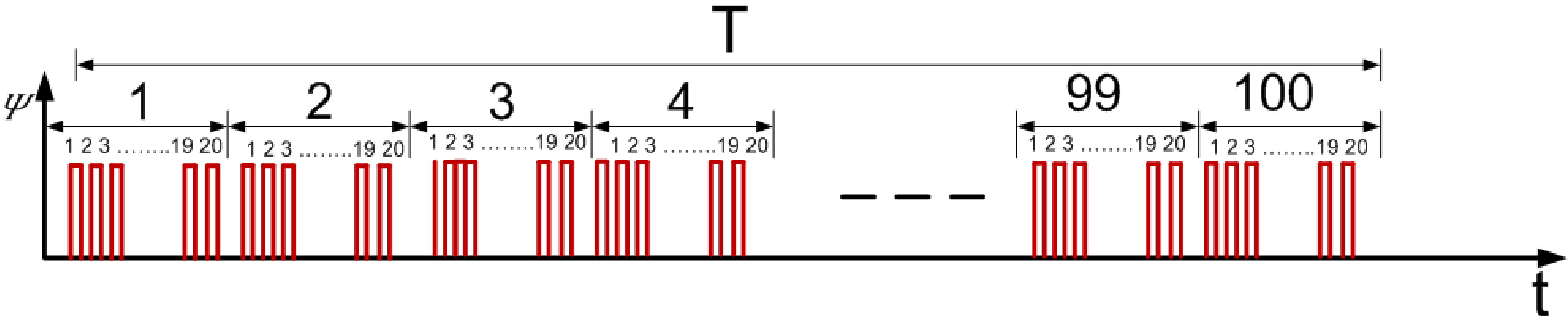
Approach:

- Consider a time interval I =[a,b], say I is divided into 100 time slots
- "Fill up this time interval with randomness" using the combined signal from *k* ROs
- At any point *t* in interval I, there exists some ring *Rj* such that $1/4 <(Prob[\Psi_j] < 2:5)<3/4$



The URN Model

- **Criterion A.** With t chosen uniformly at random from the interval I, the probability that there exist integers j and m with $|t - mT_j| < 0.6475\sigma_j$ is at least q.
- Each Time slot is subdivided into l subintervals $(J_1\ J_2\ J_3\ \ldots J_l)$
- In all the J subintervals at some point t\` some ring oscillator *Rj* is in transition.



- Each J_h is called as an *URN*
- An *urn* is said to be full if there is some *Rj* in the circuit whose signal satisfies the threshold value (i.e., *(L+H)/2)* at any real time t\` in *J*.
- Otherwise, the *urn* is empty

The URN Model Cont…

- Criterion A is satisfied provided
  - at least *ql* of the urns are filled and
  - $l > (b\text{-}a)/0.6475\sigma_j$ for all $j = 1 \ldots k$
- Ignoring phase drift, ring *Rj* will fill roughly one out of every $\pi_j = l * T_j/(\text{b-a})$ urns.
- π_j is the ***combinatorial period*** of the ring *Rj*

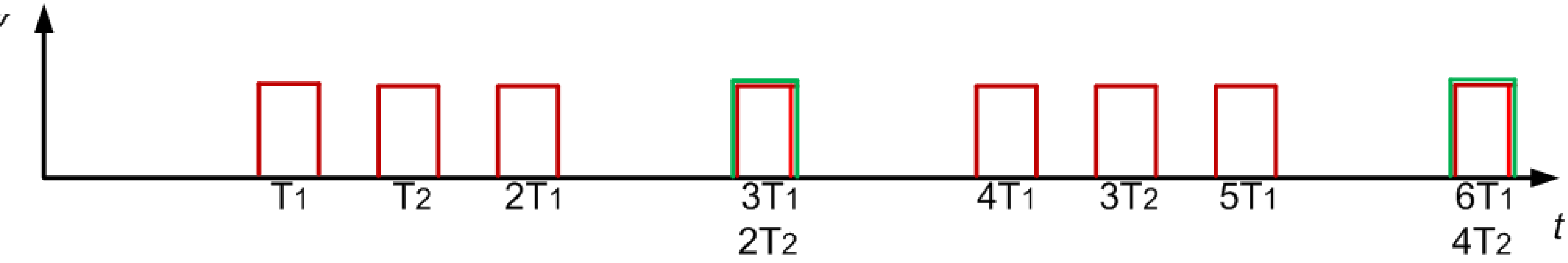
We require at least *ql* of the urns to be filled to avoid biasing
→ Requires large number of *RO*s and known phase drifts

Ex: T=1000
I=[1:100]
$l = 10$
$\pi_j =$
*10*1000/99=*
101.010101

Relatively Prime Ring Lengths

How do we efficiently populate an interval *I* with jitter events?

- When two rings are in transition at the same point in time there is wastage of entropy



In order to fill as many urns as possible and in order to make the behavior of the *r* rings as independent as possible, the ring lengths $n_1\ n_2\ n_3\ \ldots n_r$ *should be pairwise relatively prime* *

* B. Sunar, W.J. Martin and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," , *IEEE Transactions on Computers* , vol.56, no.1, pp.109,119, Jan. 2007

Identical Ring Lengths

- Ideally, two rings with equal number of inverters will exhibit a great deal of overlap in their transition zones

- Practically, Not
  - Random delays and phase drifts ensures non overlap in their contributions to the jitter.

- *Urn Width*: Parameters
  - Number of inverters (*n*) determines the period of the ring(*T*)
  - Specifics of the hardware determines the jitter width (*w*)
    - The standard deviation of the associated random variable
  - Desired entropy per bit

Identical Ring Lengths

- *Phase Drift*: can only improve randomness of the of identical ring length model
  - The combinatorial period of *Rj*: $\pi_j = l * T_j$/(b-a)
    - Ring *Rj* will fill roughly one out of every π_j urns (ignoring phase drift)
  - In each sequence of π consecutive urns each ring fills one randomly chosen urn
    - Urn with index congruent to d_j modulo π (considering phase drift)

  (Assumption)

Coupon Collecting

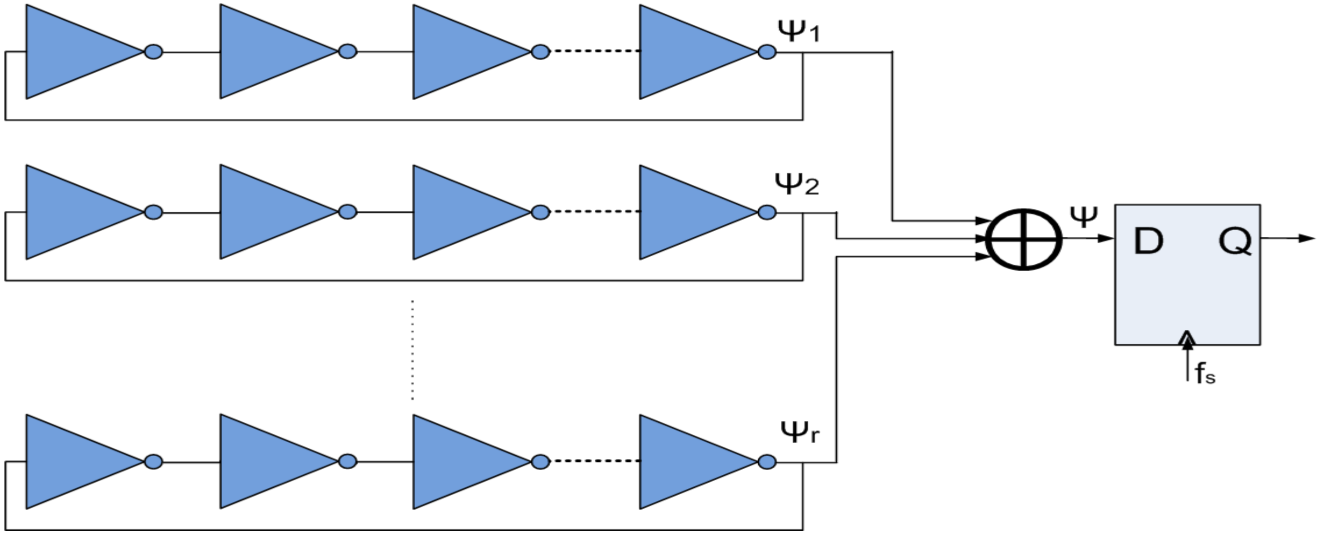
- Problem: Select one urn from a set of *N* uniformly at random until each urn has been filled or selected at least once.
- Expected number of rings needed to fill all *N* urns is *N log N*

- *So the aim is to reduce the fill rate and to compensate for the resulting fraction of non randomness*

- Resulting samples hence might have deterministic and non deterministic components
- *Resilient functions* can be used to eliminate these nonrandom components

Possible attacks

- Modify Sampling Clock



- Glitches
- Increase/Decrease Sampling Clock, until a bias is observed

Possible attacks

- On ROs
  - Insert/ Remove Rings
    - This may reduce the fill rate
    - Determine the number of rings to be removed to get the desired biasing
  - On Combined Signal before sampling

Criticisms

- Unrealistic Probabilistic Model of Jitter
- Interaction of Ring Oscillators
- Unrealistic Speed
- Violation of Operating Conditions for sampling Flip-Flop

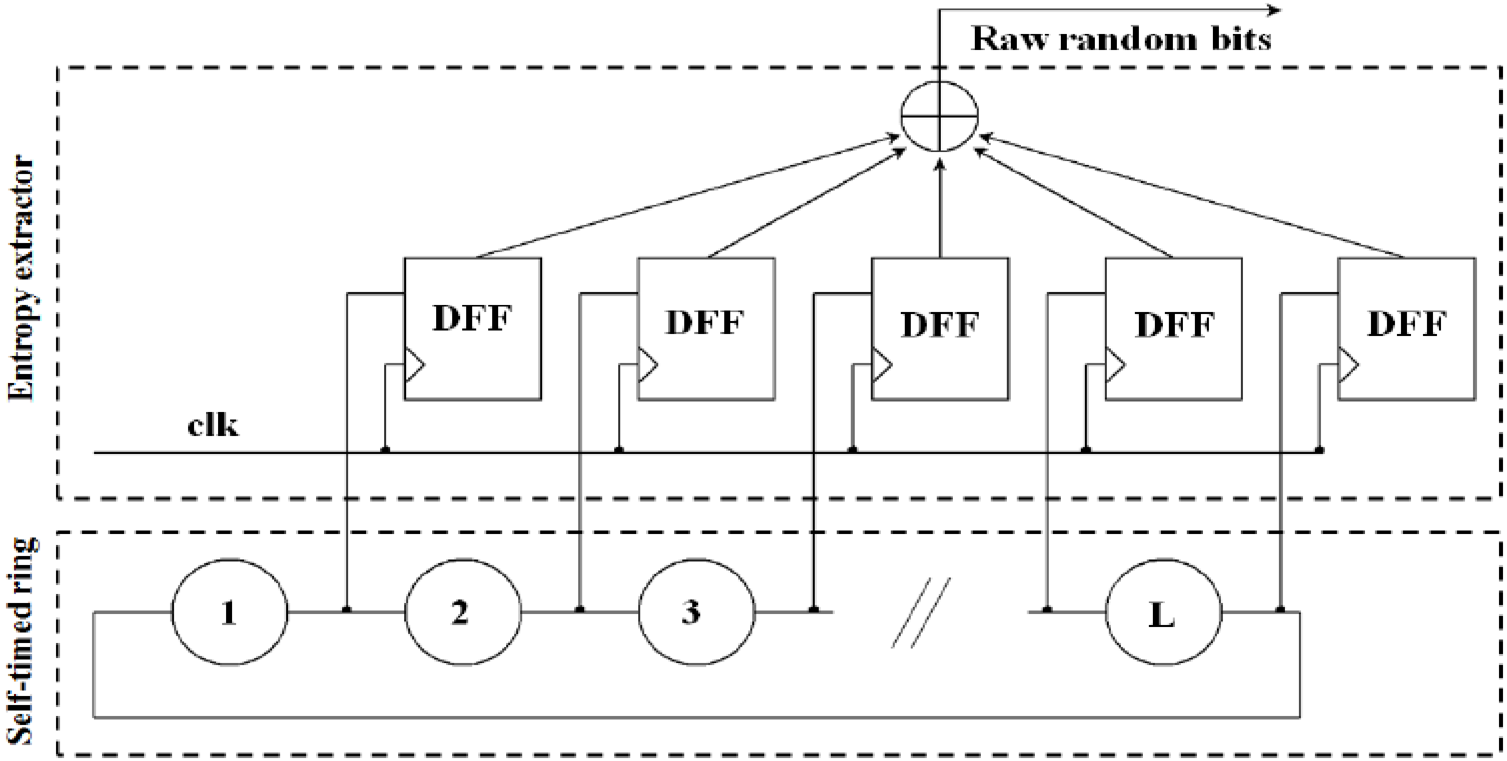
M. Dichtl and J. Dj. Goli´c, “High-Speed True Random Number Generation with Logic Gates Only” , *CHES 2007,* LNCS vol. 4727, pp. 45-62, Springer Verlag, 2007.

Remedies

- Sampling rate may be easily reduced
- Difficult to verify the independence of the ring oscillators when a large number of rings are used.
  - For a smaller number of rings, careful place and routing may sufficiently isolate the rings from interacting with each other.
- Collect only one sample from one oscillation period.
  - In this case, ring independence is not required.
  - It suffices to check against phase interlock which would reduce the fill-rate.

2: Sunar, "True Random Number Generators for Cryptography" *Cryptographic Engineering, Springer US*, **2009**, 55-73

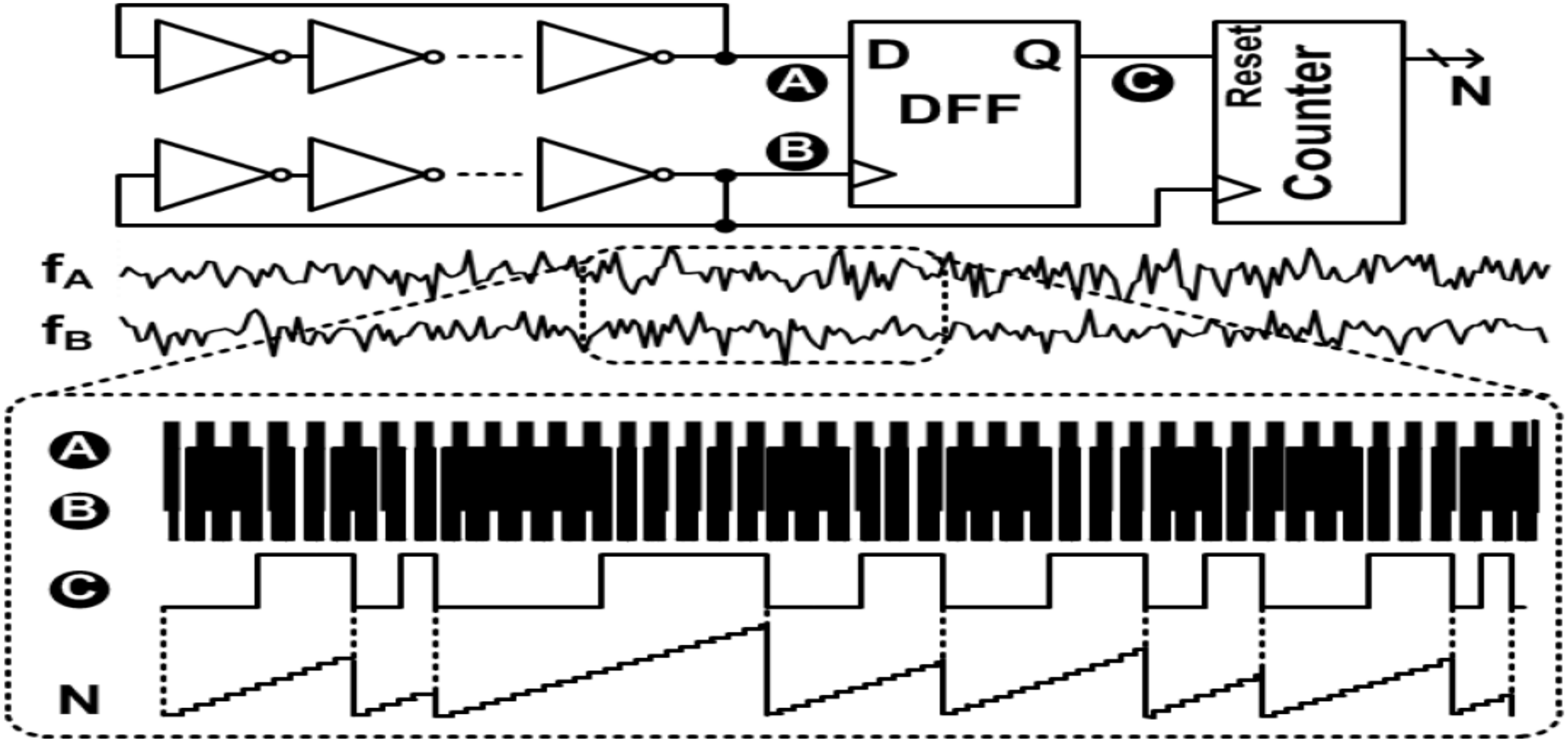
Self Timed Ring Based TRNG



1: Abdelkarim Cherkaoui, Viktor Fischer, Laurent Fesquet, Alain Aubert: A Very High Speed True Random Number Generator with Entropy Assessment. CHES 2013: 179-196

2. Martin, H.; Korak, T.; San Millan, E.; Hutter, M., "Fault Attacks on STRNGs: Impact of Glitches, Temperature, and Underpowering on Randomness," *Information Forensics and Security, IEEE Transactions on* , vol.10, no.2, pp.266,277, Feb. 2015

TRNG Circuits Based on Beat Frequency Detection



Qianying Tang; Bongjin Kim; Yingjie Lao; Parhi, K.K.; Kim, C.H., "True Random Number Generator circuits based on single- and multi-phase beat frequency detection," *Custom Integrated Circuits Conference (CICC), 2014 IEEE Proceedings of the* , vol., no., pp.1,4, 15-17 Sept. 2014

THANK YOU