Entropy Evaluation for Oscillator-based True Random Number Generators

Yuan Ma

DCS Center
Institute of Information Engineering
Chinese Academy of Sciences

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

DCS CENTER
DATA ASSURANCE & COMMUNICATION SECURITY
EST 1980

Outline

- RNG
- Modeling method
- Experiment
- Entropy evaluation
- On the external perturbation

RNG

- RNGs (Random number generators) are used in cryptography to
  - initialize keys,
  - seed pseudo-random number generators,
  - help in generating digital signature
  - …
- RNG security is crucial for cryptographic systems

TRNG Security

- How to make sure a true (physical) RNG is secure?
  - Providing a reasonable mathematical model based on some physical assumptions
  - Figuring out the precise/minimum/maximum entropy
  - Confirming the sufficiency of the calculated entropy
- Not a easy work
  - Ideal physical assumption is not usually practical or is hard to be proved.
    - white noise vs. correlated noise
    - independent ring oscillators vs. coupled ring oscillators
  - Entropy estimation is complex though the design structure is simple
    - from noises to random bits, bit correlation

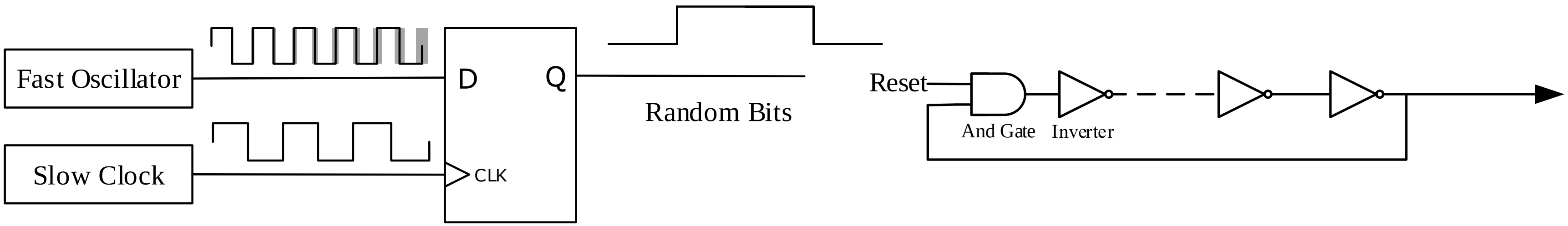
Our work

- Proposing a new modeling method to calculate a precise entropy for oscillator-based TRNGs

- Designing a jitter measuring circuit to acquire critical parameters and also verify the theoretical results

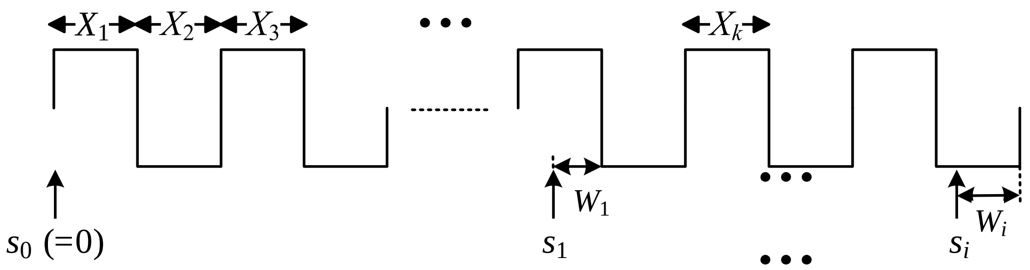
- Performing a comprehensive study on the effect of deterministic perturbations

Oscillator-based TRNG



- How a random bit is generated
  - Randomness is (accumulated) jitter. The cycle number of fast oscillator signal is random /unpredictable during the period of the slow clock
  - More precisely, how many half-cycles/edges
  - $B_i = B_{i-1} \oplus (R_i \bmod 2)$, R_i represents the number of edges
- The xor operation with the last bit has no impact on the information entropy, so we take $B_i = R_i \bmod 2$.

Model Setup



- Half-period: X_k, mean μ, variance σ^2
- Sampling interval: $s = v\mu$, $r = v \bmod 1$ (fractional part)

$$\mathrm{Prob}(R_i = k+1) = \mathrm{Prob}(T_k \le s) - \mathrm{Prob}(T_{k+1} \le s)$$

$$(T_k = X_1 + X_2 + \cdots + X_k)$$

$$\frac{T_k - k\mu}{\sigma\sqrt{k}} \to N(0,1), k \to \infty \ \ \text{(CLT)}$$

$$= \Phi\left((v-k)\cdot\frac{\mu}{\sigma\sqrt{k}}\right) - \Phi\left((v-k-1)\cdot\frac{\mu}{\sigma\sqrt{k+1}}\right)$$

$$\mathrm{Prob}(B_i = 1) = \sum_{j=1}^{\infty} \mathrm{Prob}(R_i = 2j-1)$$

From Killmann, et al. CHES 2008

One-time sampling: model approximation

- Physical assumption: small jitter

$$\mathrm{Prob}(R_i = k + 1)$$

$$\approx \Phi((v - k) \cdot \frac{\mu}{\sigma\sqrt{k}}) - \Phi((v - k - 1) \cdot \frac{\mu}{\sigma\sqrt{k + 1}})$$

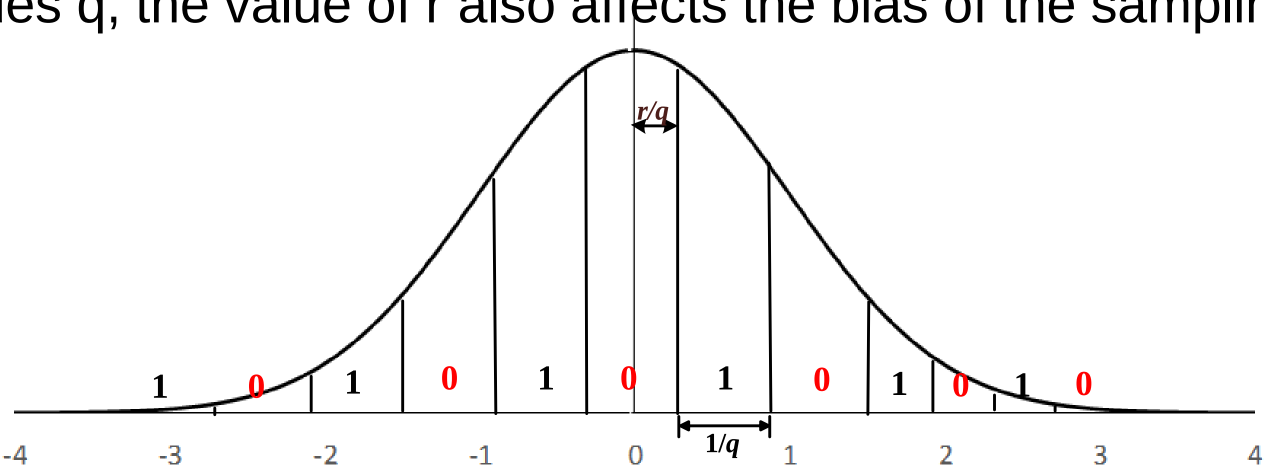
by defining $q = \frac{\sigma\sqrt{v}}{\mu}$ (Quality Factor)

$$\approx \Phi\left(\frac{v - k}{q}\right) - \Phi\left(\frac{v - k - 1}{q}\right)$$

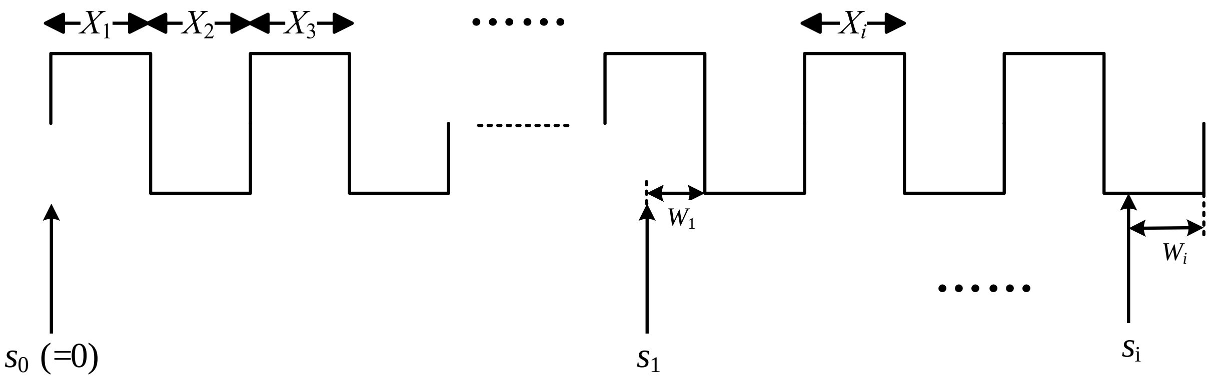
Understanding

$$\text{Prob}(R_i = k + 1) \approx \Phi\left(\frac{v - k}{q}\right) - \Phi\left(\frac{v - k - 1}{q}\right)$$

- In one-time sampling, the phase difference is set to 0.
- The area (equaling to 1) is divided at 1/q interval.
- The area of each column corresponds to the probability of R_i equaling to each k.
- The larger q is, the finer the column is divided, which means that the areas of '0' and '1' are closer.
- Besides q, the value of r also affects the bias of the sampling bit.



Consecutive sampling: waiting time



- W_i: the distance of the ith sampling position to the following closest edge [Killmann et al. CHES 2008]
- In consecutive sampling, two adjacent sampling processes are dependent, as the waiting time W_i generated by the ith sampling affects the next one.
- $B_i \rightarrow W_i \rightarrow B_{i+1}$

W_i probability distribution

- Referring to renewal theory (i.i.d. assumption):

$$\mathrm{P}_W(y) = \mathrm{Prob}(W_i \le y) = \frac{1}{\mu}\int_0^y \big(1 - P_X(u)\big)du\ ,\quad s \to \infty$$

- Due to $\sigma \ll \mu$ (small jitter), $\mathrm{P}_W(y)$ approximates to a uniform distribution of [0,μ]

$$\mathrm{Prob}(W_i \le y) \approx \begin{cases} \frac{1}{\mu}\int_0^y 1du = \frac{y}{\mu}, 0 \le y \le \mu \\ 1, \qquad y > \mu \end{cases}$$

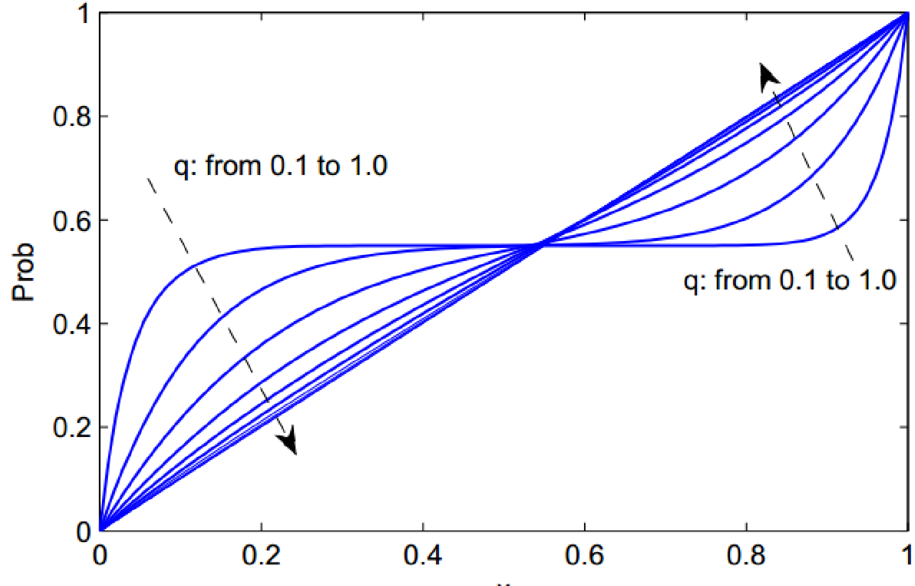
Independence Condition

- No matter what b_i is, W_i is always a uniform distribution.

$$\forall b_i \in \{0,1\}, \mathrm{Prob}(W_i \leq x | b_i) = \mathrm{Prob}(W_i \leq x) = \frac{x}{\mu}$$

$$\rightarrow q > 0.6$$

- Observation: when q is approximately larger than 0.6, the distribution becomes uniform and the correlation is almost eliminated.
- Only observation is not enough, precise entropy is needed.



Entropy Calculation

Bit-rate entropy $H = H_n / n$

$$H_n = \sum_{\mathbf{b_n} \in \{0,1\}^n} -p(\mathbf{b_n}) \log p(\mathbf{b_n})$$

$$p(\mathbf{b_n}) = \mathrm{Prob}(b_n, \dots, b_1) = \prod_{i=1}^{n} K(b_i)$$

$$K(b_i) = \mathrm{Prob}(b_i | b_{i-1}, \dots, b_1)$$

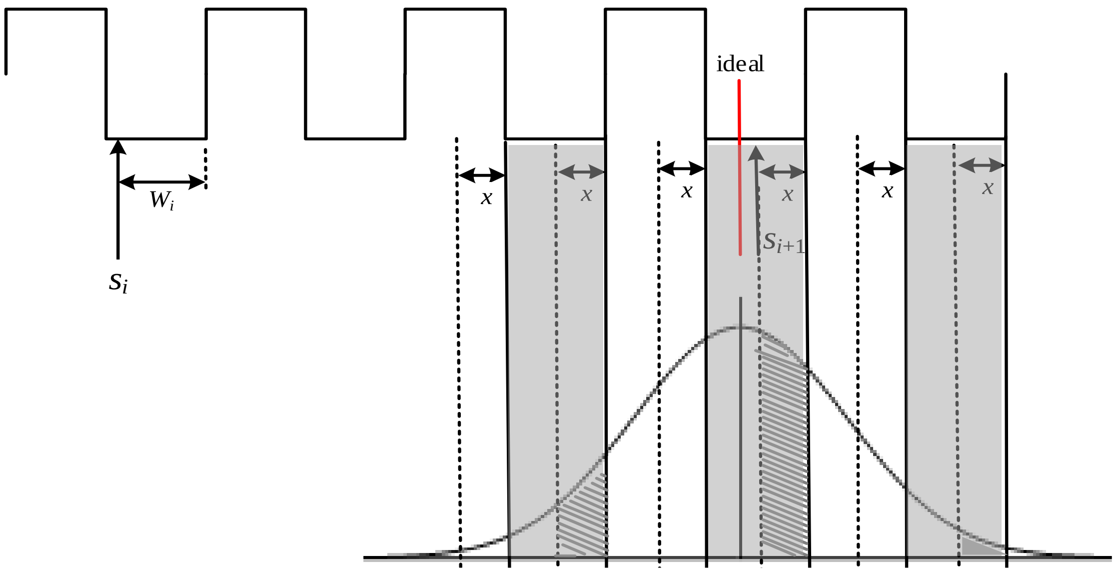
- The goal is calculating the probability of b_i in the condition of knowing the previous bits.
- Method: using the waiting time W_i to represent the relationship and then eliminating W_i

Entropy Calculation

- Basic function 1:

$$\text{Prob}(b_{i+1}|w_i) = \sum_{i=-\infty}^{+\infty} \left(\Phi\left(\frac{2i+1-c_i}{q}\right) - \Phi\left(\frac{2i-c_i}{q}\right) \right)$$

$$:= J_{i+1}(w_i)$$

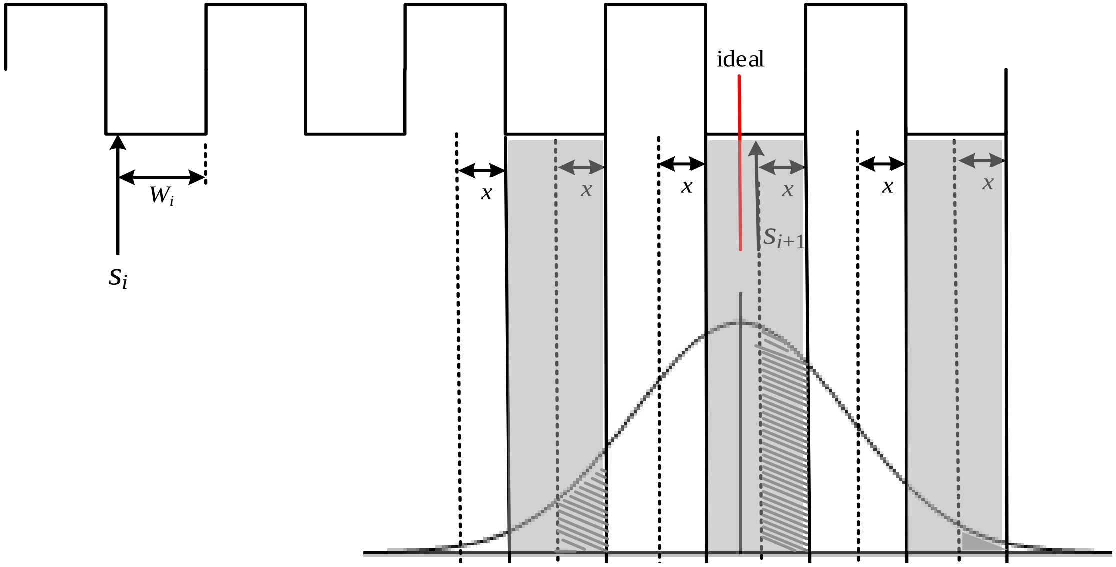


Entropy Calculation

- Basic function 2:

$$\text{Prob}(W_{i+1} \leq x, b_{i+1}|w_i) = \sum_{i=-\infty}^{+\infty}\left(\Phi\left(\frac{2i+1-c_i}{q}\right) - \Phi\left(\frac{2i-c_i+1-x}{q}\right)\right)$$

$$:= F_{i+1}(x, w_i)$$



Entropy Calculation

- The property of the Markov process

$$\text{Prob}\left(b_i \middle| w_{i-1}, b_{i-1,} w_{i-2}, b_{i-2,} \dots\right) = \text{Prob}(b_i | w_{i-1})$$

- From *i* = 1 to *n* for a pattern $\{b_n, \dots, b_1\}$, by iterating

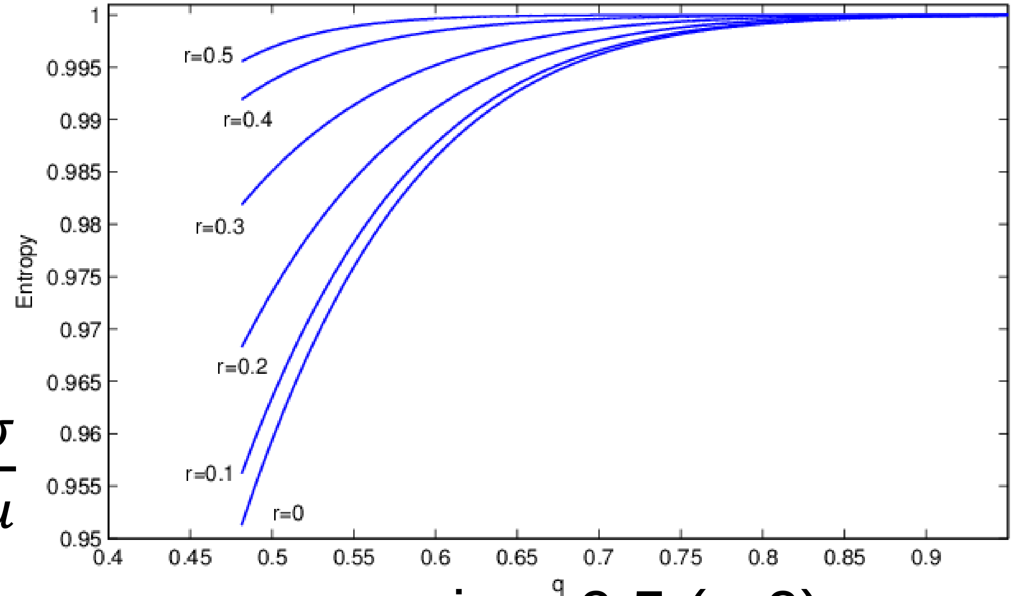
$$G_i(x) := \text{Prob}(W_i \leq x | b_i, \dots, b_1) = \int_0^1 \frac{F_i(x,y)}{K(b_i)} G_{i-1}(dy)$$

$$K(b_{i+1}) = \int_0^1 J_{i+1}(x) dG_i(x)$$

- Especially,

$$G_1(x) = \int_0^1 \frac{F_1(x, w_0)}{J_1(w_0)} dw_0$$

Entropy Evaluation

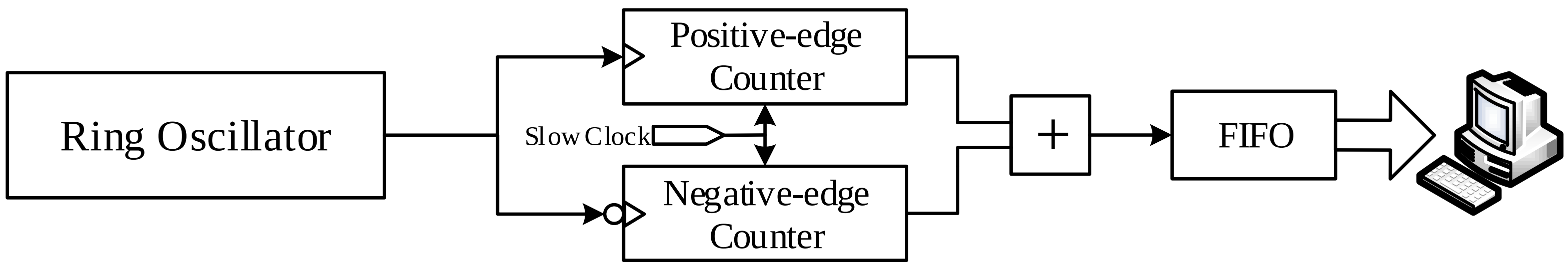


- For different $q = \sqrt{\frac{s}{\mu}} \cdot \frac{\sigma}{\mu}$
  - The best (worst) performance occurs in r=0.5 (r=0). r is the fractional part of s/μ
  - Maximum entropy and minimum entropy
  - The oscillator frequency is so high that r is hard to adjust.
  - A robust TRNG design should have sufficient entropy even in the worst (most unbiased) case.

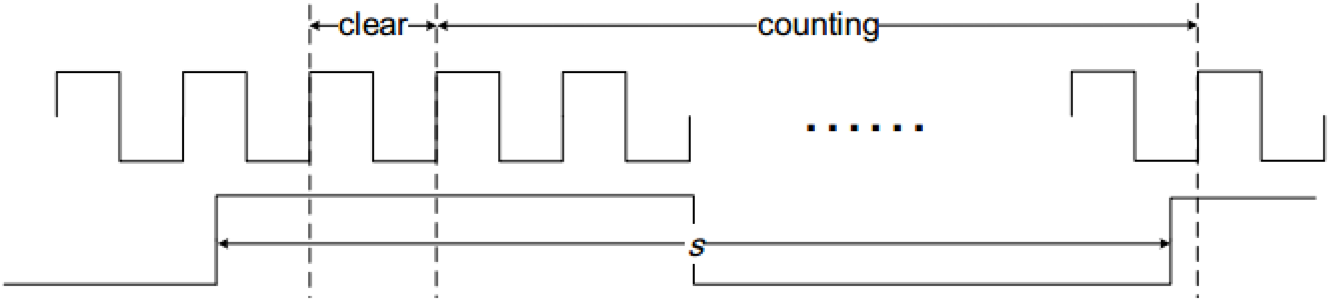
How to acquire *q*

- External measurement
  - needs high-precision oscilloscope to measure jitter
  - output circuit also causes jitter
- Inner measurement
  - convenient and reliable
  - can be embedded into hardware for online or inner test

Experiment Design



- Dual-counter measurement circuit: counting the number of edges of fast oscillator signal
- Clear mechanism



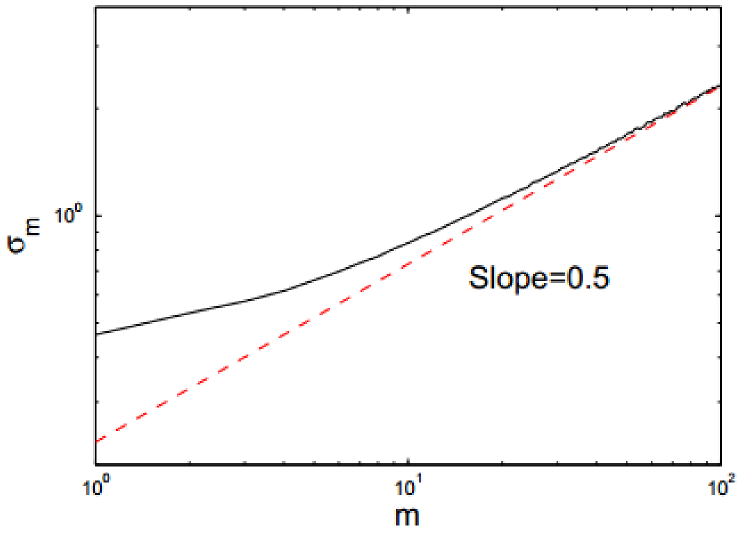
Calculating *q*

- Counting is a (delayed) renewal process. The variance of counting results is

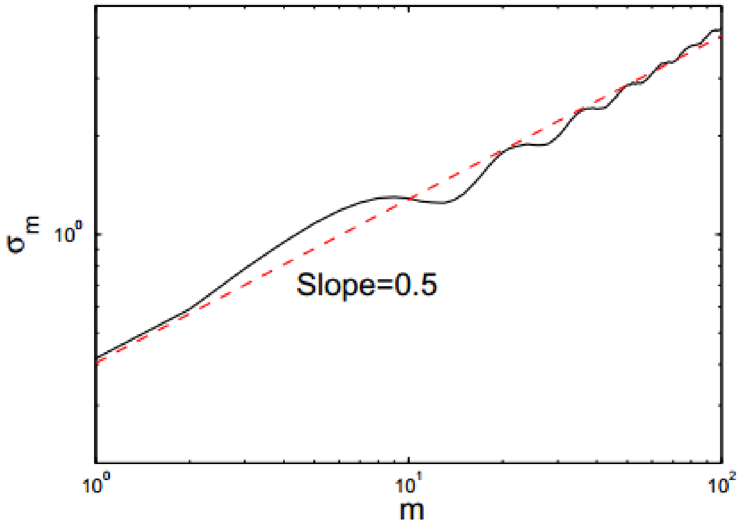
$$s(\sigma^2/\mu^3) + o(s) = q^2 + o(s), o(s) \to 0 \text{ when } s \to \infty$$

- The clear mechanism guarantees
  - after getting numbers of count results in the duration of s, we sum the m non-overlapping results to obtain the number of edges in the duration of m*s
  - only one-time counting is needed for acquire the (approximated) *q* values under different sampling intervals

Measurement Results



(a) Simulation results with white noises

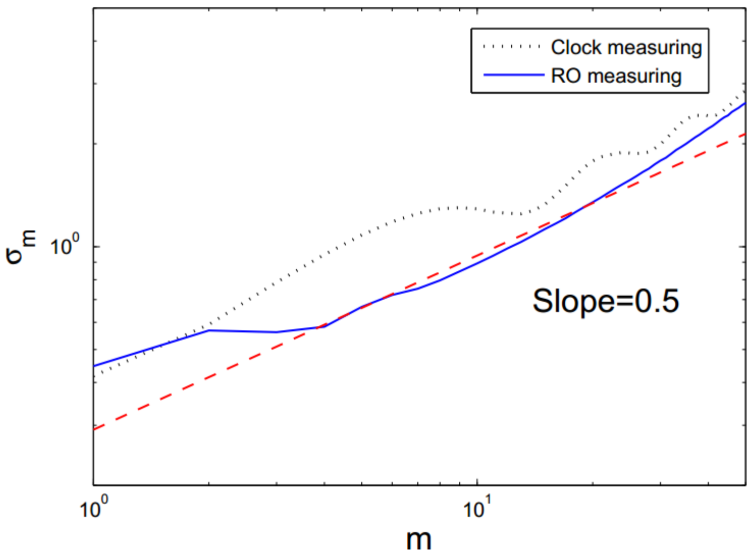


(b) Practical measuring results in FPGA

- The overestimation decreases with the sampling interval increasing.
- Deterministic jitter exists!

Dual-RO Measuring

- The deterministic perturbation is global.
- Using another RO to measure the fast RO signal to filter deterministic jitter. [Fischer, et al., FPL 2008]
- The existence of correlated noise
  - dominant in low frequency, but sight in the concerned region (*q* around 1)
  - does not degrade sampling bit quality when accumulated independent jitter is sufficient
- Basic experimental data for verification



Parameters for Sufficient Entropy

- Simulation for required q
  - Theoretical entropy: H>0.9999 (stricter)
  - Sampling sequence: passing FIPS 140-2
- The required q values are close
- The variation tendencies for q values are consistent

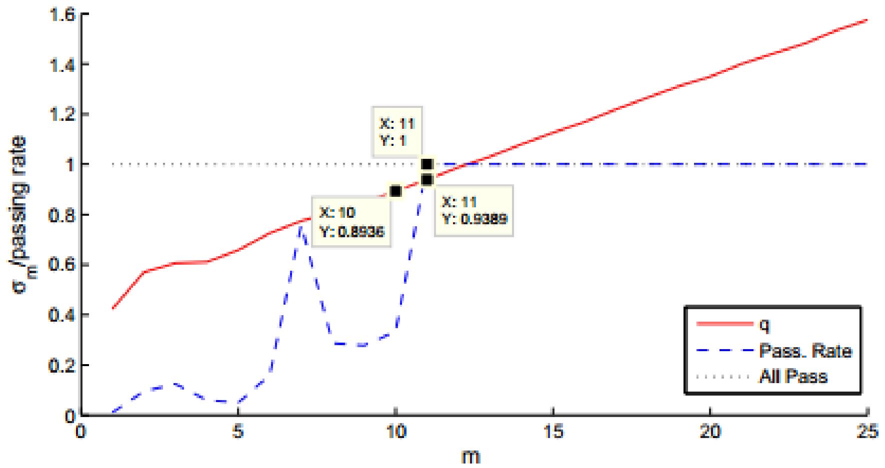
Table 1. The required q to achieve sufficient entropy for different r

r / Req. q	r=0	r=0.1 (0.9)	r=0.2 (0.8)	r=0.3 (0.7)	r=0.4 (0.6)	r=0.5	Remark
Theory	0.9264	0.9209	0.9029	0.8673	0.7895	0.6511	$H > 0.9999$
Sim. Measured	0.9778	0.9392	0.9198	0.8759	0.7928	0.7002	passing FIPS 140-2

- When r=0.5 the balance is always satisfied, so, once the independence condition is achieved, the entropy is sufficient and the sequence can pass the test.

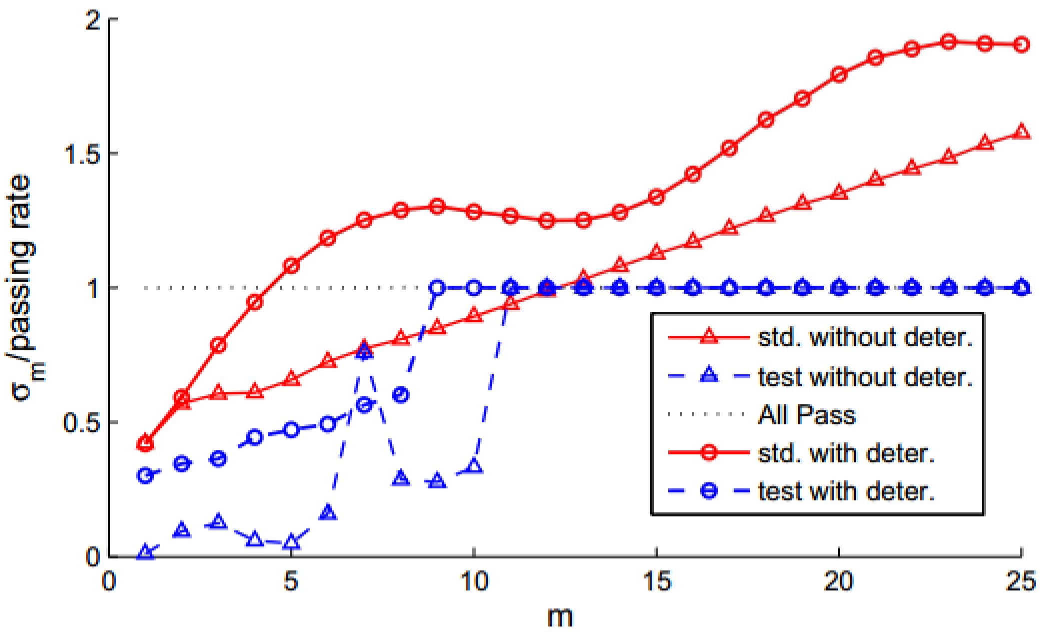
Parameters for Sufficient Entropy

- FPGA
  - passing ratio vs. standard variance: $q \in [0.8936, 0.9389]$
  - It seems infeasible to measure the right r at this point to do a further verification.
  - A tiny measuring error will make the measured r totally different in such a high frequency of the fast oscillator signal.
  - Correlated noise makes an overestimation for independent jitter, especially when m is large.



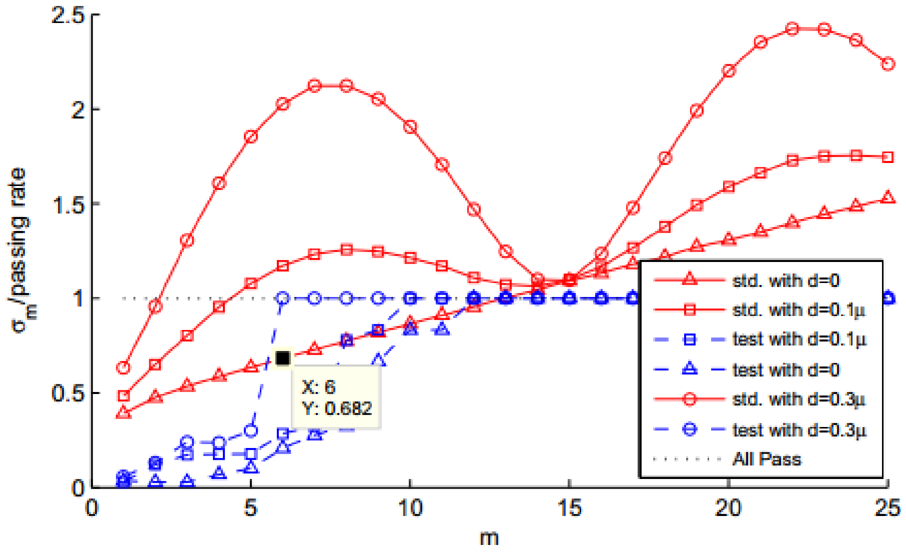
Effect of Deterministic Perturbations

- making it easier to pass statistical tests
  - from m=11 to m=9
- enlarging the amount of estimated randomness jitter



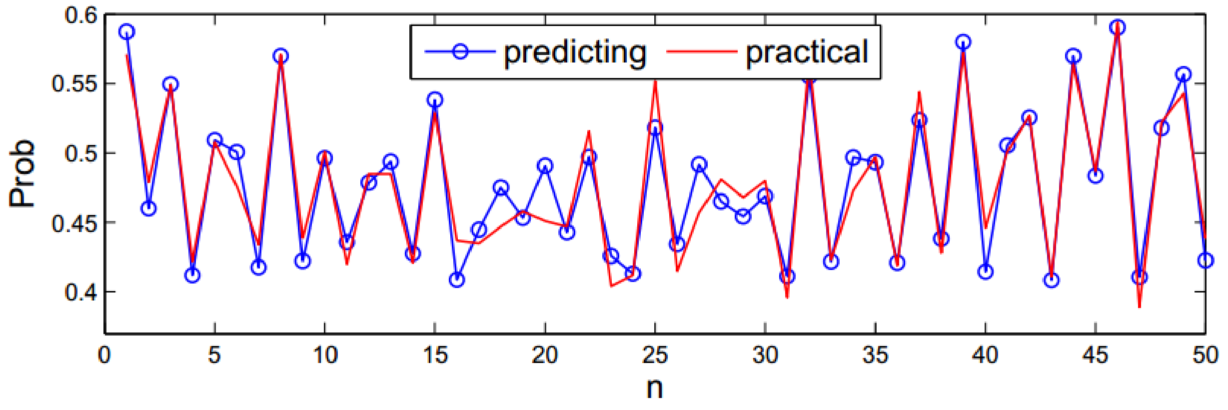
Bound for Randomness Improvement

- With the strength of the perturbation increasing , the passing position does not move up any more after m = 6 (q = 0.68), consistent with the independence condition.
- Perturbation causes little impact on the correlation but improve the balance of random bits



Predicting the “Random” Bits

- Under deterministic perturbations
  - for a sequence, the statistical property is satisfied
  - but, for each bit, the entropy might be insufficient
  - making the prediction of each bit probability possible
- Simulation: by previously knowing the precise design parameters and the function of the deterministic perturbation



Conclusion

- An entropy estimation method is provided, which is well consistent with experiment.
  - helpful for designers to determine the theoretical fastest sampling frequency (r=0.5) and secure frequency (r=0).
  - helpful for verifiers to calculate the entropy of given TRNG parameters.
- A simple quality factor extraction circuit is designed.
  - Embedded into hardware for online tests
  - A higher precision can be obtained by “filtering” correlated jitter and deriving from the result with long interval.
  - Detection of deterministic perturbations or even attacks.
- The accumulated independent jitter should be sufficient.

Entropy Evaluation for Oscillator-based True Random Number Generators

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

DCS CENTER
DATA ASSURANCE & COMMUNICATION SECURITY
EST 1980

Thanks!