An energy and area efficient, all digital entropy source compatible with modern standards based on jitter pipelining

2022 Conference on Cryptographic Hardware and Embedded Systems

Adriaan Peetermans    Ingrid Verbauwhede

imec-COSIC, KU Leuven, Leuven, Belgium

September 21, 2022
Random numbers

How are they used?

▶ Cryptography

▶ Statistical simulations

▶ Gambling/games
Random numbers

How are they generated?

- Pseudo Random Number Generator (PRNG)

- True Random Number Generator (TRNG)
RNG verification

Obsolete approach
- Statistical tests
- Parameter adjustment
- Pass/Fail

Modern approach
- Entropy requirement standard/application
- Entropy verification
- Entropy claim
- Design parameters

ES

Statistical tests

Experiments

Stochastic model

Design parameter optimization

Configuration

ES

Random bits

Prototype verification
Pass/Fail

Entropy requirement
Model assumptions
Platform parameters

Pass/Fail

Design parameters

TRNG architecture

- **Delay Chain (DC)**
  - Propagate start edge through two independent paths
  - Timing jitter accumulation
- **Time to Digital Converter (TDC)**
  - Resolve timing difference created by DCs
  - Timing jitter accumulation
- **Digitisation**
  - Convert resolved timing difference into digital format
  - Notifies controller output is valid
Throughput optimisation:
  • Reduced TDC resolution requires less jitter accumulation time
    ■ TDC frequency matching
  • Concurrent jitter accumulation both in DC and TDC
    ■ Jitter pipelining
Jitter pipeline

- Jitter pipeline with two stages
  - DC-stage
  - TDC-stage
- First bit is resolved while second one is already started
- Pipeline timing balance should be maintained
Stochastic model, overview

Delay Chain
DC0
DC1

Time to Digital Converter
TDC0
TDC1

Digitisation

Start

T_D = T_0^n - T_1^n

T_π

π

time

Random bit

0
1

R

DC0
DC1

TDC0
TDC1

Ready

Random Bit
Stochastic model, overview

Start
DC0
DC1

Delay Chain
DC0

Time to Digital Converter
TDC0

Digitisation
TDC1

Ready
Random
Bit

DC0
DC1
TDC0
TDC1

T^0_n
T^1_n
T^\Delta_n

n n n

n n n

E2L E2L

T
Q

Ready
Random

Bit

DC0
DC1
TDC0
TDC1

n n n

n n n

E2L E2L

T
Q

Ready
Random

Bit

DC0
DC1
TDC0
TDC1

n n n

n n n

E2L E2L

T
Q

Ready
Random

Bit
Stochastic model, overview
Stochastic model, overview

**Delay Chain**
- Start
- **DC0**
- **DC1**

**Time to Digital Converter**
- **TDC0**
- **TDC1**

**Digitisation**
- **Ready**
- **Random Bit**
Stochastic model, overview
Stochastic model, overview

- Delay Chain
  - DC0
  - DC1

- Time to Digital Converter
  - TDC0
  - TDC1

- Digitisation
  - TDC0
  - TDC1

- Random bit
  - 0
  - 1

- Start
- Ready
- E2L

- DC0
- DC1

- TDC0
- TDC1

- R

- Time

- Delay Chain:
  - Start
  - DC0
  - DC1

- Time to Digital Converter:
  - TDC0
  - TDC1

- Digitisation:
  - TDC0
  - TDC1

- Random Bit

- E2L

- DC0
- DC1
On-chip jitter measurement

- Experimentally determine platform dependent jitter parameter
- Conservative estimation method avoids overestimation
  - Overestimation could lead to false entropy claim
  - Measurement errors give positive bias
- On-chip and differential to avoid external influences
- Reuse existing TRNG hardware

\[ \text{delay} = T_0^n \]
\[ \text{delay} = T_1^n \]

\[ \text{DC}_0 \]
\[ \text{DC}_1 \]
\[ \text{TDC}_1 \]
On-chip jitter measurement, results

| DC0 period length [ns] | DC0 period variance [ns²] |
|------------------------|--------------------------|
| 0                      | 0.0                      |
| 20                     | 0.002                    |
| 40                     | 0.004                    |
| 60                     | 0.006                    |
| 80                     | 0.008                    |
| 100                    | 0.01                     |

- Chip 0
- Chip 1
- Chip 2
- Chip 3
- Chip 4
Four design parameters can be freely chosen: $\mu_{DC_0}$, $\mu_{DC_1}$, $\mu_{TDC_0}$ and $\mu_{TDC_1}$

- Represent DC, TDC oscillation frequencies

Selection criteria:
- Pipeline balance
- Entropy density
- Throughput
Resolution versus accumulation time bounded by:
- Entropy density (1)
- Pipeline balance (2)
- Throughput (colour gradient)

TRNG throughput improved by:
- Larger jitter strength (shifts (1))
- Faster TDC oscillation speed (shifts (2))
Experimental results

- **IID claim verification**
  - Correlation analysis
    - 4096 consecutively generated counter values
      - No correlation observed
  - NIST SP 800-90B IID test
    - 5 devices, 1 Mbit consecutively generated random bits per device
    - All devices pass
Experimental results

- Entropy validation
  - Standards require minimally 0.91 bit/bit min-entropy density
  - ES design parameters have been optimised to output at least the required entropy density
  - Higher entropy density levels possible at lower throughput
  - 5 devices, 1 Mbit consecutively generated random bits per device
  - All devices reach required entropy density

| Chip       | 0    | 1    | 2    | 3    | 4    |
|------------|------|------|------|------|------|
| Model estimate | 0.99988 | 0.99861 | 0.99811 | 0.99895 | 0.99963 |
| Test estimate   | 0.93341 | 0.94475 | 0.94722 | 0.95255 | 0.96221 |
| Minimum        | 0.93341 | 0.94475 | 0.94722 | 0.95255 | 0.96221 |
Experimental results

- Power and throughput

- All devices have a throughput higher than 250 Mbit/s (highest for jitter-based)
- Output min-entropy density above 0.91 bit/bit over all voltage levels tested
- Best energy efficiency at 0.8 V supply: 1.46 pJ/bit
Conclusion

- ES architecture design, verification, and fabrication in a 28 nm technology compatible with modern standards
- Jitter pipelining allows for efficient entropy generation
- All-digital structure benefits scaling and design integration
- Stochastic model estimating generated output entropy
- On-chip jitter measurements
- Optimisation scheme guides parameter selection
Thank you for your attention
Four design parameters can be freely chosen: $\mu_{DC_0}$, $\mu_{DC_1}$, $\mu_{TDC_0}$ and $\mu_{TDC_1}$.

- Represent DC, TDC oscillation frequencies

Selection criteria:

- Pipeline balance

$$\text{res} > \frac{P_{TDC_0} P_{TDC_1}}{2 \max(T_{0n}, T_{1n})}. \quad (1)$$

- Entropy density

$$\text{res} < \alpha \sqrt{F_{\text{noise}}} \max(T_{0n}, T_{1n}), \quad (2)$$

- Throughput

$$\text{throughput} = \frac{1}{\max(T_{0n}, T_{1n})}. \quad (3)$$