An all-electronic true random number generator

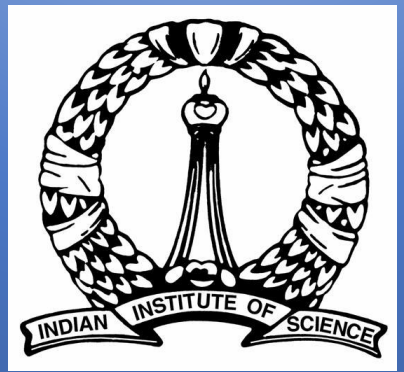
Kausik Majumdar

Electrical Communication Engineering

Indian Institute of Science

Email: kausikm@iisc.ac.in

27 March 2023



Quantum Electronics Laboratory @ ECE, IISc

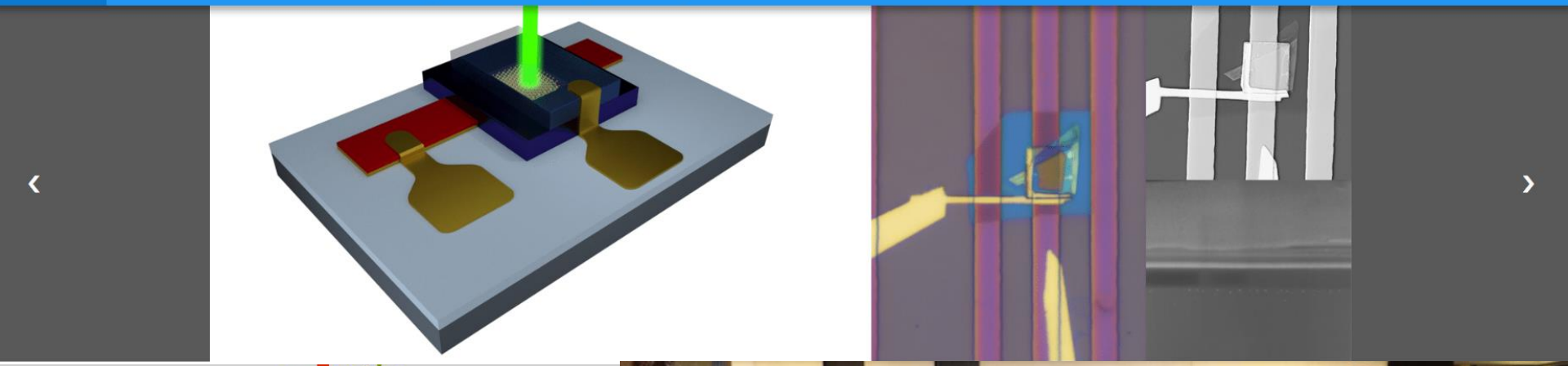
WWW: https://ece.iisc.ac.in/~kausikm

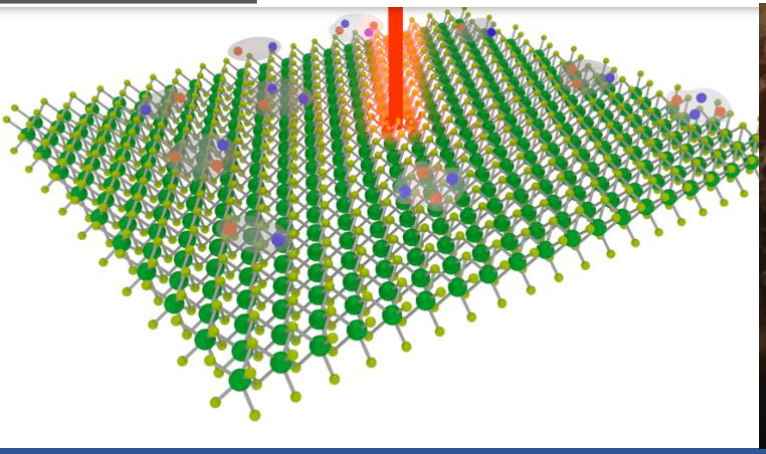
Kausik Majumdar's Group

Quantum Electronics Laboratory

Indian Institute of Science

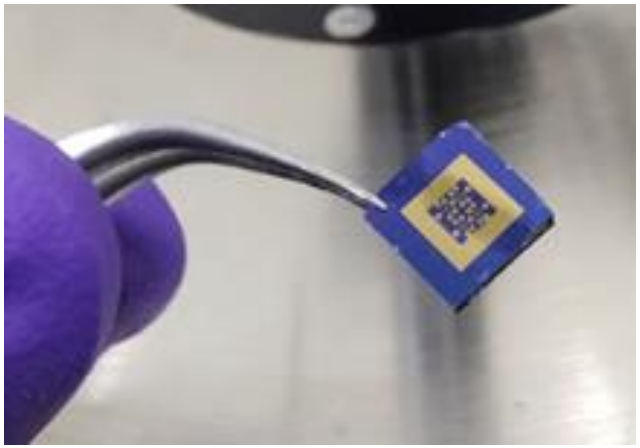
Home | Research | Publications | People | Teaching | Hiring | Contact Us





Chip-scale solution of quantum hardware components

Single Photon Source	Single Photon Detector	Random Number Generator
• Coulomb blockade • High rate (several MHz) • High purity [$g^{(2)}(0)$ ~0.1]	• Operates @1550 nm • Room-temperature • Efficiency: 21% (42% for polarized light)	• All-electronic • High quality (near-ideal min-entropy)



Miniaturization is important!

Why do we need random numbers?

- Increasing demand for hardware security
  - secure communication, digital money, cryptocurrency
- Quantum technology applications
  - quantum communication
- Large scale simulations (Biology, Chemistry, Monte Carlo)
- Gaming, gambling

How do we measure randomness?

Shannon entropy: $$H_1 = -\sum_{i=1}^{n} p_i \log_2 p_i$$

[Average information content]

Min-entropy: $$H_\infty = \min_{i=1}^{n}(-\log_2 p_i)$$

[Chance of predicting with a single guess]

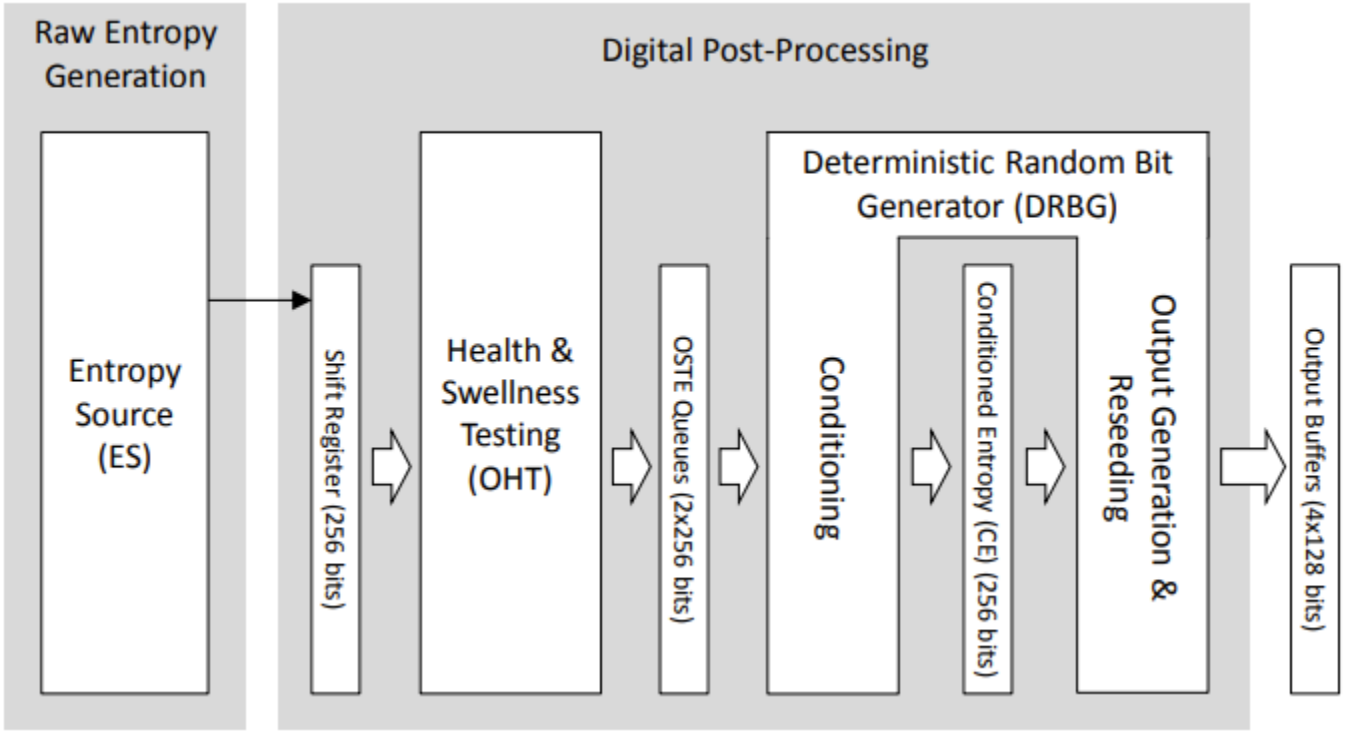
A good random sequence should

- have independent and identically distributed symbols
- **maximize** its entropy content – uniformly distributed symbols

Properties of a good random number generator

- Quantum mechanical processes are excellent sources of entropy
  - process complexity and/or ignorance (classical) versus Intrinsic randomness (quantum)
  - Device independence
  - Provably random
  - bias
- Need a way to capture such events through elegant, compact read-out

How random numbers are generated today?



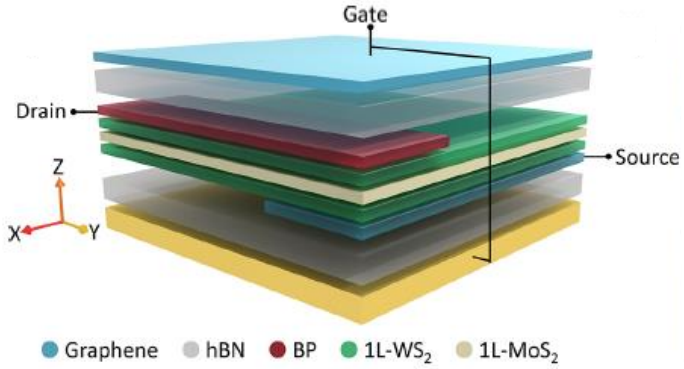
Source: https://www.rambus.com/wp-content/uploads/2015/08/Intel_TRNG_Report_20120312.pdf

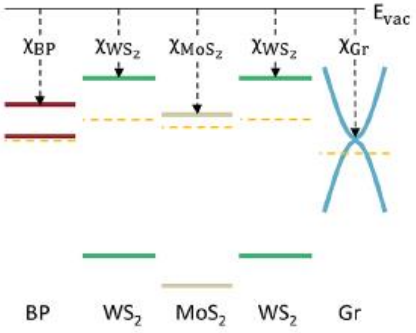
Repeated attacks!!

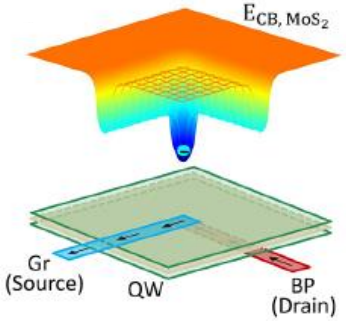
Our approach

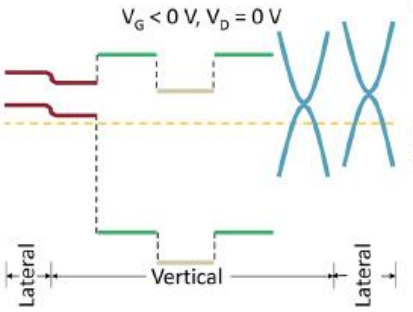
- **Discrete electron fluctuation** in van der Waals tunnel junction
- Extract entropy from the **timing** information - **uniformly** distributed
- **All-electronic** approach
- We demonstrate near-ideal **min-entropy of 0.995 bits/bit**

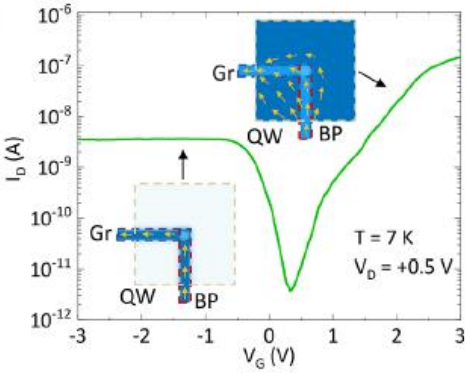
Measuring **discrete** electron fluctuation



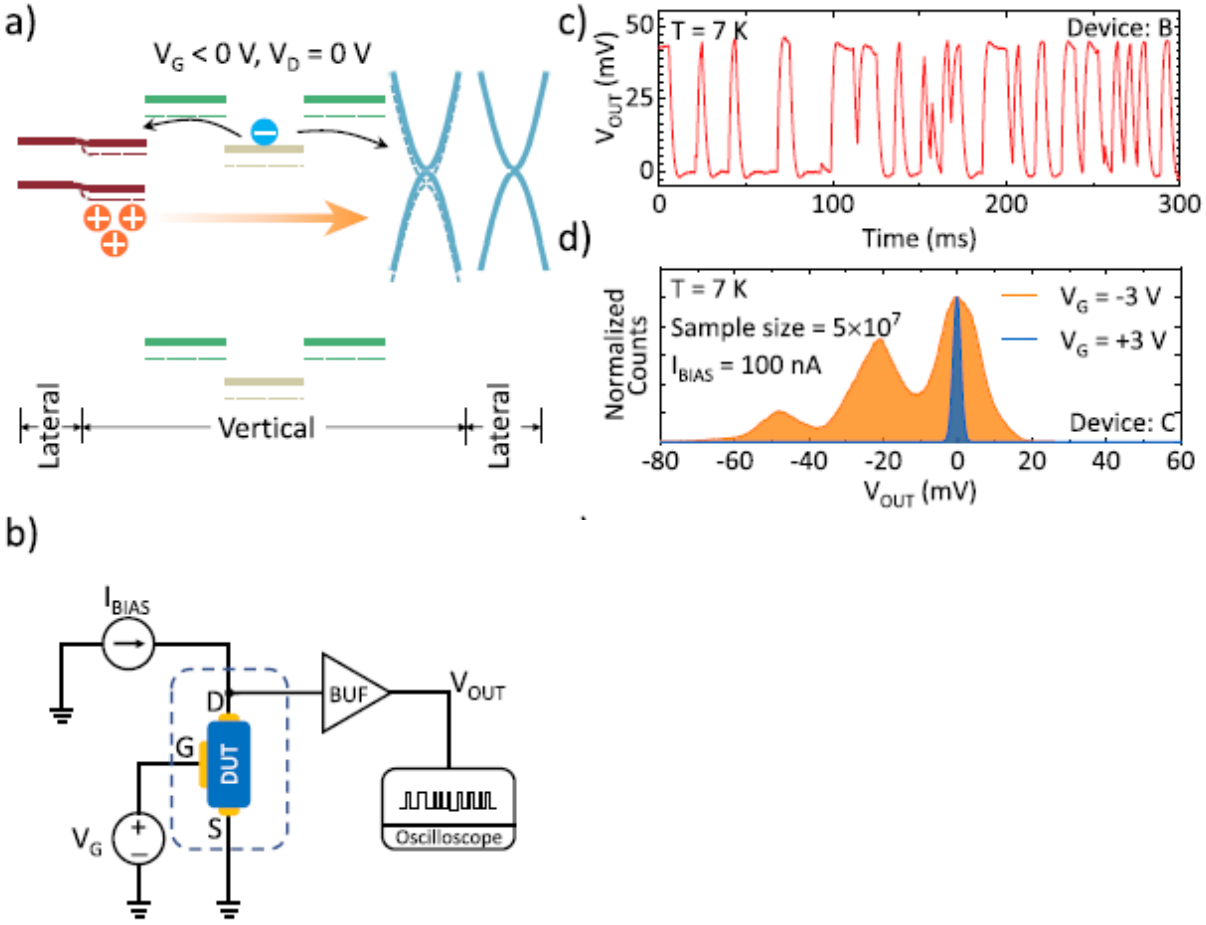


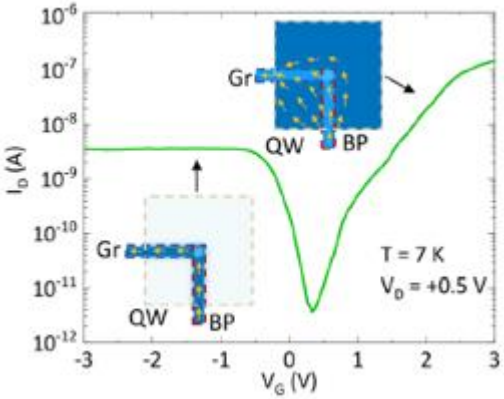






Measuring **discrete** electron fluctuation

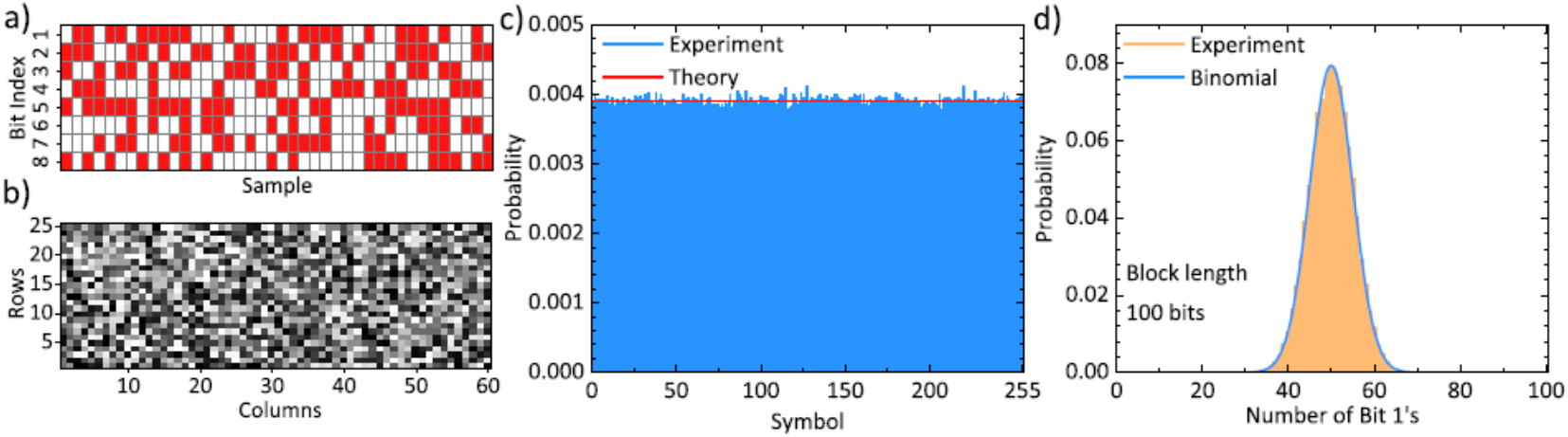




Randomness embedded in electron capture timing

Encoding into digital bits

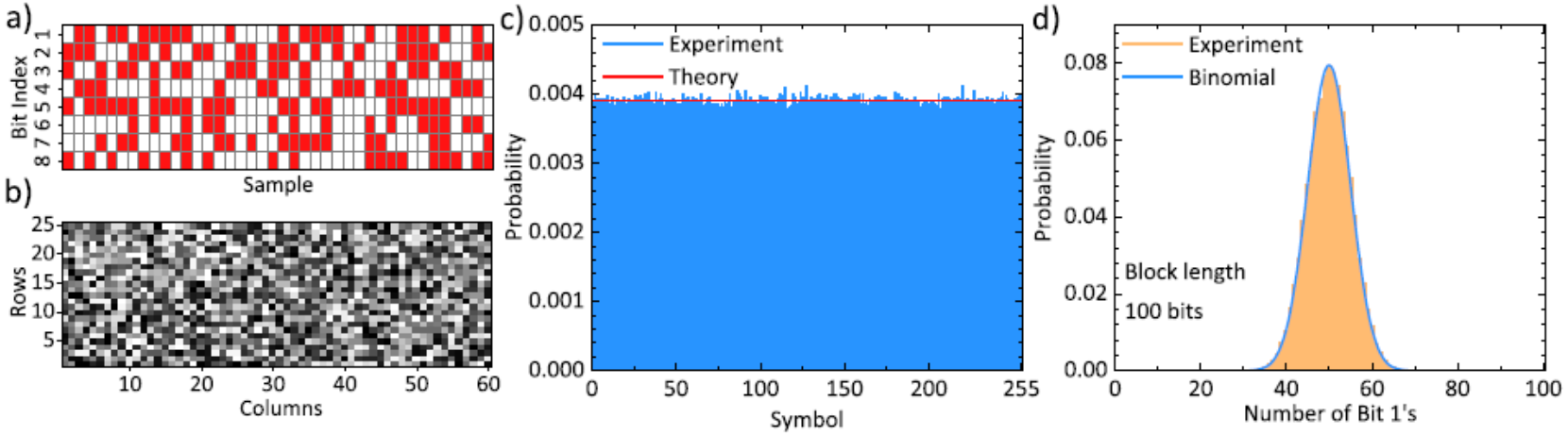
T = 7 K



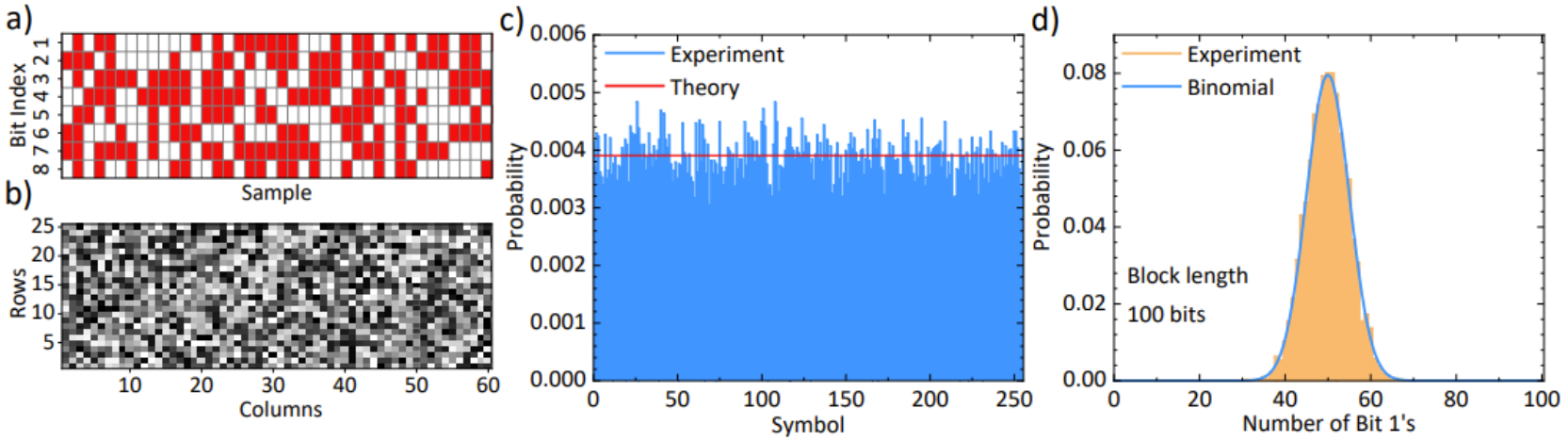
Unbiased distribution of symbols

Temperature independence, but enhanced throughput

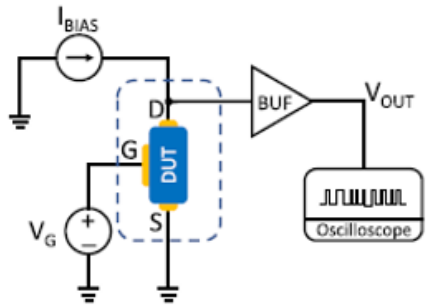
T = 7 K

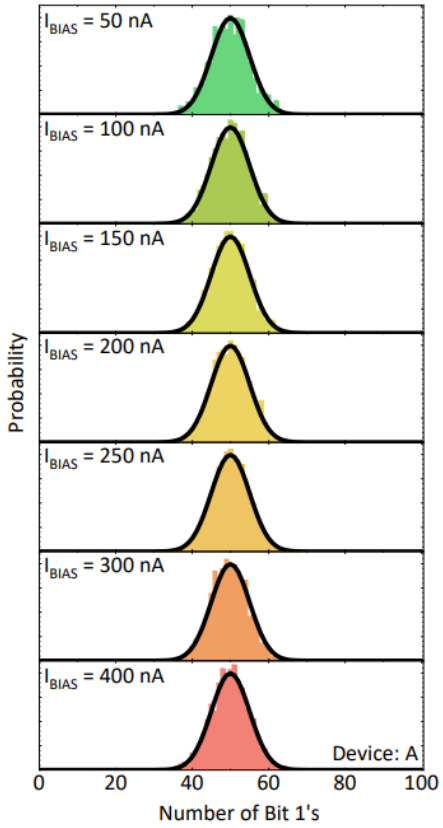


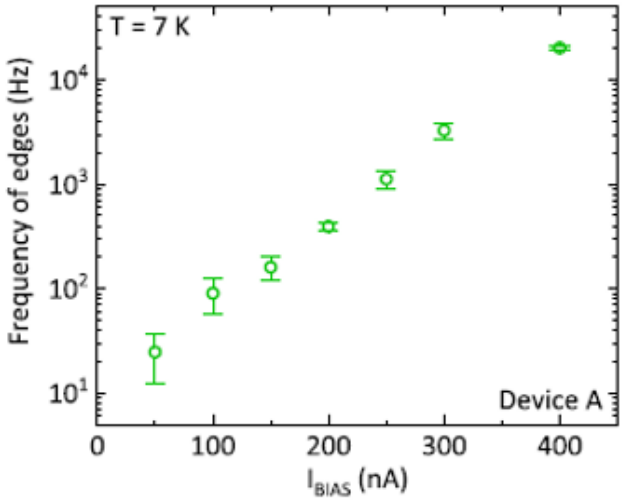
T = 295 K

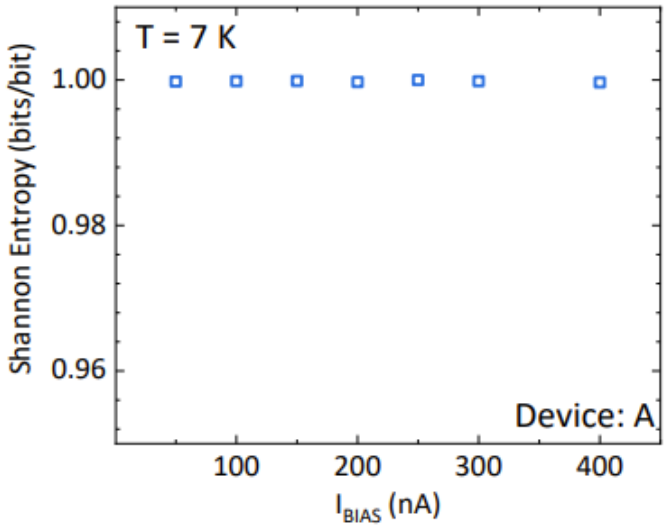


Variation of random nature with bias current









Enhanced throughput without degradation of quality

NIST test for IID - SP 800-90B

test	sequential	Restart	
		rows	columns
excursion test statistic	pass	pass	pass
number of directional runs	pass	pass	pass
length of directional runs	pass	pass	pass
number of increases and decreases	pass	pass	pass
number of runs based on the median	pass	pass	pass
length of runs based on median	pass	pass	pass
average collision test statistic	pass	pass	pass
maximum collision test statistic	pass	pass	pass
periodicity test statistic (lag = 1)	pass	pass	pass
periodicity test statistic (lag = 2)	pass	pass	pass
periodicity test statistic (lag = 8)	pass	pass	pass
periodicity test statistic (lag = 16)	pass	pass	pass
periodicity test statistic (lag = 32)	pass	pass	pass
covariance test statistic (lag = 1)	pass	pass	pass
covariance test statistic (lag = 2)	pass	pass	pass
covariance test statistic (lag = 8)	pass	pass	pass
covariance test statistic (lag = 16)	pass	pass	pass
covariance test statistic (lag = 32)	pass	pass	pass
compression test statistic	pass	pass	pass
chi-square independence	pass	pass	pass
chi-square goodness of fit	pass	pass	pass
length of the longest repeated substring	pass	pass	pass

NIST test for IID - SP 800-90B

test	sequential	Restart	
		rows	columns
excursion test statistic	pass	pass	pass
number of directional runs	pass	pass	pass
length of directional runs	pass	pass	pass
number of increases and decreases	pass	pass	pass
number of runs based on the median	pass	pass	pass
length of runs based on median	pass	pass	pass
average collision test statistic	pass	pass	pass
maximum collision test statistic	pass	pass	pass
periodicity test statistic (lag = 1)	pass	pass	pass
periodicity test statistic (lag = 2)	pass	pass	pass
periodicity test statistic (lag = 8)	pass	pass	pass
periodicity test statistic (lag = 16)	pass	pass	pass
periodicity test statistic (lag = 32)	pass	pass	pass
covariance test statistic (lag = 1)	pass	pass	pass
covariance test statistic (lag = 2)	pass	pass	pass
covariance test statistic (lag = 8)	pass	pass	pass
covariance test statistic (lag = 16)	pass	pass	pass
covariance test statistic (lag = 32)	pass	pass	pass
compression test statistic	pass	pass	pass
chi-square independence	pass	pass	pass
chi-square goodness of fit	pass	pass	pass
length of the longest repeated substring	pass	pass	pass

data set	sanity check	entropy estimate
sequential	NA	7.8644
restart rows	pass	7.8640
restart columns	pass	7.8640

min-entropy = 7.8640 bits/8 bits

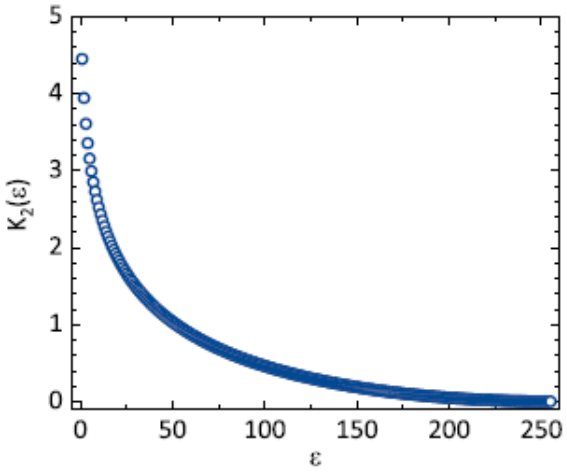
Near-ideal min-entropy: 0.983 bits/bit

Suitability for cryptographic applications – NIST SP 800-22

Test	Pass rate	Result
The Frequency (Monobit) Test	100/100	Pass
Frequency Test within a Block	100/100	Pass
The Runs Test	99/100	Pass
Tests for the Longest-Run-of-Ones in a Block	100/100	Pass
The Binary Matrix Rank Test	100/100	Pass
The Discrete Fourier Transform (Spectral) Test	99/100	Pass
The Non-overlapping Template Matching Test	Pass	Pass
The Overlapping Template Matching Test	8/8	Pass
Maurer's "Universal Statistical" Test	20/20	Pass
The Linear Complexity Test	8/8	Pass
The Serial Test	Pass	Pass
The Approximate Entropy Test	98/100	Pass
The Cumulative Sums (Cusums) Test	100/100	Pass
The Random Excursions Test	4/4	Pass
The Random Excursions Variant Test	4/4	Pass

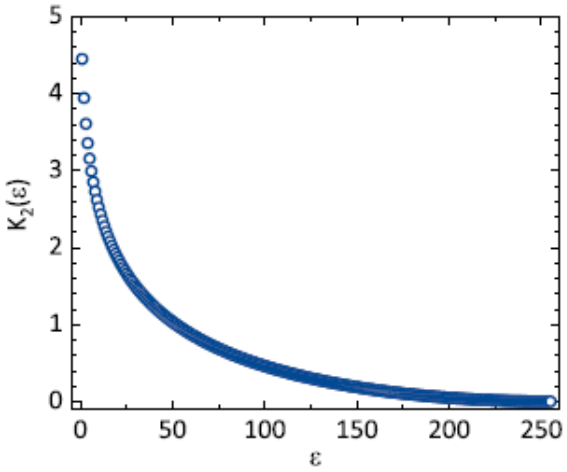
No post-processing needed for cryptographic application!

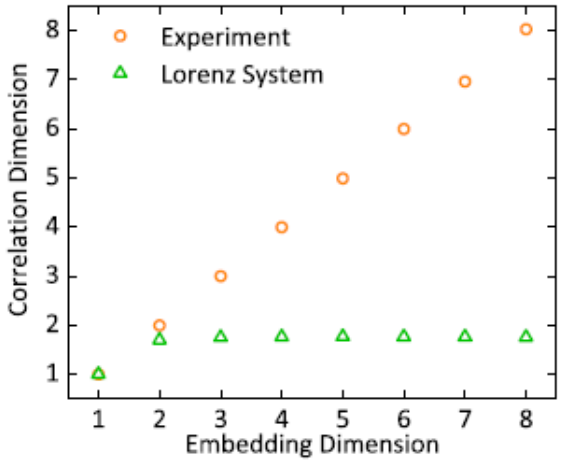
Statistical tests for random nature



- Divergence of K_2 entropy with distance threshold

Statistical tests for random nature





- Divergence of K_2 entropy with distance threshold
- No higher dimensional hidden periodicity (up to 8 dimensions)

Benchmarking with existing RNGs

Ref	Platform	IID	SP 800-22	SP 800-90B	Min-Entropy (bits/bit)
(3)	Optical	No		Pass	0.22
(4)	Electronic	No	Pass	Pass	0.893
(5)	Optical	Yes	Yes		
(6)	Electronic	Yes	Yes		
(9)	Optical	Yes	Yes		
(11)	Super-paramagnetic	Yes	Yes		
(23)	Electronic	Yes	Yes		
(30)	Electronic	No	Pass	Pass	0.889
(31)	Electronic	No	Pass	Pass	0.721
(32)	Optical	No		Pass	0.219
(33)	Electronic	Yes	Yes		
(34)	Electronic	Yes	Yes		
This Work	**Electronic**	**Yes**	**Pass**	**Pass**	**0.983**

More details

ACSNANO Vol.16, No. 5898, 2022

www.acsnano.org

ARTICLE

A High-Quality Entropy Source Using van der Waals Heterojunction for True Random Number Generation

Nithin Abraham, Kenji Watanabe, Takashi Taniguchi, and Kausik Majumdar*

Acknowledgements

Collaborators:
K. Watanabe, T. Taniguchi (NIMS, Japan)

Funding:
DST, MHRD, ISRO