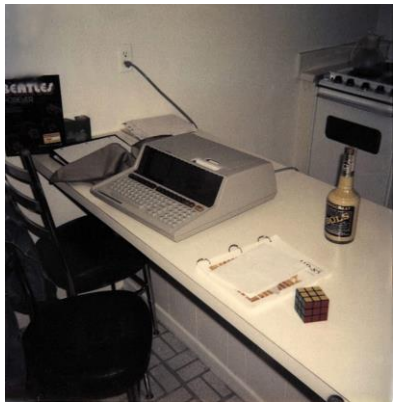
RANDAEMON®

Entropy is good

Testing RNGs
or
How PPC changed my life

Kuba Tatarkiewicz

- Got HP-25 as a wedding gift in 1976
  - Just graduated from physics department of Warsaw University
  - HP-25 cost $140 or roughly my yearly salary
- In 1978 joined PPC, member number **2865**
- Few contributions to PPC Journal but some were printed
- In 1981 worked for Gearhart Ind., Ft. Worth, TX
- From my first salary bought HP-41C
- Ordered PPC ROM – got #417
  - Sold it together with 41C and accessories in 1988 to friend in Poland
  - 2024 I bought on eBay #5150 and added to my collection of vintage HPs



Programming 41C

- Got several programs published in PPC Journal
  - Returned to Poland in 1982 (martial law)
  - Finished my PhD in 1983 – part of it on 41C
  - Did some programming just for fun
    - SIMAN – conversion of any units to SI (V12N2P30)
- Got Bronze Overlay from HP Users' Library Europe
- In 1986 effectively stopped using HP-41C because got first Macintosh and used it also for programming

RNGs in my life

- In 1976 programmed ERPEX, Monte Carlo code for simulating ranges of energetic protons in solids
- The code is still in RSICC Library at ORNL (FORTRAN)

  https://rsicc.ornl.gov/codes/ccc/ccc3/ccc-305.html
- RADDI was Monte Carlo simulation of radiation damages in solids, mainly in semiconductors
- Together with HP-41C code SDXRET for low energy ion damages it was enough to get PhD in 1983
- All these simulations were using PRNGs

Monte Carlo Integration V7N2P54

PPC CALCULATOR JOURNAL

FEBRUARY
MARCH
1980
VOL. 7
NO. 2

The Personal Programmers Club does Prolific and Productive Computing with Hewlett-Packard Personal Programmables from Corvallis.

PPC Calculator Journal is a monthly publication of PPC - a volunteer, non-profit, loosely organized, independent, world-wide group of Hewlett-Packard personal calculator and computer users. *PPC Calculator Journal* is the official Club calculator publication for PPC members to disseminate user information related to the selection, evaluation, care, and application of all Hewlett-Packard personal programmable calculators. PPC is not sponsored, nor in any way officially sanctioned, by Hewlett-Packard. Send all correspondence to: Richard Nelson, Editor/Publisher PPC Calculator Journal, 2541 W. Camden Place, Santa Ana, California 92704 USA. Telephone: (714) 754-6226.

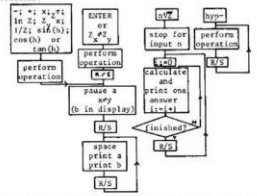
time. It is possible to increase or decrease the number of stack levels (see V6N1).
-the top five (shifted)functions can be replaced by 5 others by merging in a second card with 88 program steps. To do so: goto fA; g merge; read (one-sided) MERGE CARD. The now available functions are:

e^{Σ}	sin Σ	cos Σ	tan Σ	hyp-
ENTER	−	+	x	÷

To regain access to the original set: RTN; g merge; read both sides of MAIN CARD. These merging operations have no effect on program status and may even be executed during the evaluation of a long expression.
-the "hyp-" function is used as a prefix:

Problem	Keystrokes	Answer
tanh(1.3+5.7E)	1 . 3 ↑5 . 7 EE ED	0.93 − 0.13E

-to get rid of a complex number in the lowest stack level you can use the key sequence GTO D C.
-Program output: The program typically responds with 2 numbers. Please be sure that the program has stopped before keying in new data. The following partial flow-chart shows the program's output routines.



-when recording the program on a magnetic card, don't forget flag status, etc.
- I'm not qualified to translate this program to the 41C myself (who?). The program can probably be made to fit in the basic 41C when one gets rid of the 10 unused registers R_{-1} (#11) through R_{-8} (#20). Some users may also want to shorten the program further by taking advantage of the 41C's improved flag tests, data transfer functions, etc. This space could be used for prompting, key assignments, etc. Note that the HP-67/97 will execute step 001 after step 224. I don't know if the 41C card reader will automatically simulate this with a "goto 67" instruction. If not, please add this yourself.
You can get additional documentation on this program by sending me a card.

Peter Van Den Hamer (3533)
Hendrimalaan 138, The Hague, HOLLAND

R/S

HP-25 MONTE CARLO INTEGRATION

MONTE CARLO INTEGRATION - HP-25 PROGRAM

I'd like to show you a less known application of Monte Carlo simulations: Monte Carlo integration. It is based on the limit:

$$\frac{(b-a)}{N} \sum_{i=1}^{N} f(x_i) \xrightarrow[N \to \infty]{} \int_a^b f(x)\,dx$$

where points x_i are distributed randomly and uniformly over [a,b]. This means that for large number of simulated points Monte Carlo integration results are very close to the accurate value of the integral. The variance of this approximation is:

$$\sigma^2(I) = \sigma_f^2 \; 1/N$$

$$\text{where } \sigma_f^2 = (b-a) \int_a^b f^2(x)\,dx - \left[\int_a^b f(x)dx\right]^2$$

More information about Monte Carlo integration errors can be found in specialistic books e.g., J.M. Hammersley and D.C. Handscomb "Monte Carlo Methods", Long-New York, Methuen, Wiley, 1961. My program for the HP-25 is written for all functions which can be expressed analytically, the random number generator described by R. Moore V6N2P20 is used to generate random points distributed uniformly over [a,b]. The program is:

01/	STO 3	23 03
02/	g 1/x	15 22
03/	STO + 3	23 51 03
04/	RCL 0	24 00
05/	g π	15 73
06/	+	51
07/	2	02
08/	1	01
09/	x	61
10/	g FRAC	15 01
11/	STO 0	23 00
12/	RCL 2	24 02
13/	x	61
14/	RCL 1	24 01
15/	+	51
16/	f sin	11 04
17/	g x²	15 02
18/	GTO 38	13 38

{the function to be integrated (in RAD mode)

.
.
.

38/	STO + 4	23 51 04	Registers
39/	1	01	R_0 - seed
40/	STO - 3	23 41 03	R_1 - a
41/	RCL 3	24 03	R_2 - (b - a)
42/	f INT	14 01	R_3 - N+1/N
43/	g x≠0	15 61	R_4 - Σ f (x_i)
44/	GTO 04	13 04	R_5, R_6, R_7: free for constants of the function
45/	RCL 4	24 04	
46/	RCL 2	24 02	
47/	x	61	
48/	RCL 3	24 03	
49/	x	61	

Instructions

1/ key in first 15 steps of program
2/ key in your function assuming that x is in X register and placing function's value in this register. Regs R_5 - R_7 are free for function's constants,
3/ end GTO 38, switch to RUN, GTO 37, switch to PRGM,
4/ Key in last 12 steps of prgm,
5/ switch to RUN, f PRGM,
6/ store seed: seed STO 0,
7/ store integral boundaries:
a STO 1
(b - a) STO 2
8/ to compute the integral key in number of points to be simulated:
N_0, R/S ⟶ I_0
9/ for another number of points:
0 STO 4, N_i R/S ⟶ I_i

This program is self-explanatory except perhaps the tip in reg 3. Because ↑25 has no DSZ this reg works as DSZ /1 is subtracted after each point has been simulated/ and also as storage reg for 1/N which is needed in the end part of the prgm.

Results

Comparison with Simpson's rule (HP-25 Application programs, p.81) for the function $\sin^2 x$ over [0,π] :

Exact value: π/2 = 1.5709
Simpson's rule = 1.5708
/8 points/
Variances of Monte Carlo method for this function are:
σ^2 (I) = 1.234/N hence for:

100 points $\sigma^2 = (0.111)^2$
1000 points $\sigma^2 = (0.035)^2$
10000 points $\sigma^2 = (0.011)^2$

Simulated integral's values for unchanged seed of 10^8 were:

100 points 1.6 (4346), time ~ 3 min,
1000 points 1.55(709), time ~ 30 min,
10000 points 1.560(03), time ~ 5 h,

which is rather good results when very approximate method is considered. Another example (even better) is the SI(x) function. J.J. Davidson V5N2P29. Seed is 0.1

10 points → SI (1) = 0.9602
100 points → SI (1) = 0.9479
1000 points → SI (1) = 0.94715

where the exact value according to Jim Davidson is:

SI (1) = 0.9460803

The Monte Carlo accuracy is supposed to be due to the 'normalized' character of the function $\frac{\sin x}{x}$ which is integrated. I suggest that Monte Carlo method applied to calculators is fast enough in comparison with "Standard" integration method and gives results without preliminary calculations, tables etc. Besides it is fun to compute the integral using pure statistical method, isn't it?!

Jakub Tatarkiewicz (2965) Warszawa, Poland

R/S

Testing RNGs visually V10N9P22 (1983)

PPC® CALCULATOR JOURNAL

NOVEMBER 1983 V10N9

The Personal Programming Center is for People Programming Computers

APPLICATIONS

PROGRAMS

REGULAR COLUMNS

The PPC Calculator Journal is a monthly publication of PPC, a non-profit public benefit California Corporation dedicated to personal computing. A personal computer by PPC standards, is small, self-powered, and portable enough to be with the user. The user does not go to the computer to use it. PPC disseminates users information related to selection, evaluation, care, and application of personal computers. Send all correspondence to: PPC, 2545 W. Camden Place, Santa Ana, California 92704 USA. Telephone (714) 754-6226 P.M.

BEST RNG?

In V8N3P23 of PPC Calculator Journal John L. Baker (3726) presented his study on RNGs. From that time the only RNG I use is r_{i+1} = FRC(r_i+3579) which is my comparison the best (from the statistical point of view) as well as the fastest. Still many PPC members (notably Valentin Albiol V7N6P35 and V8N6P55 and Gary Chamberlain (V6N7P20 and others) prefer other RNGs. Having access to Sinclair Spectrum computer which easily generates color graphics (Oh, Mother HP, when will the 75 be capable of B/W graphics on a TV screen?) I decided to test as many as possible RNGs. Enclosed you will find the results of this job.

I am sorry, but color copies are very expensive here in Poland, hence I send you (for reproduction purposes) simple black and white enlargements, but if you like I can send you color slides as photographed from a TV screen. As you can see original RNG of Spectrum is bad, (picture #8). Also the RNG of Albillo (#4) looks non-random. Number 7 is totally wrong since accuracy of this RNG depends upon machine truncation which is different for HP calculators and for Spectrum.

Final Remark – This is marvelous how our brain performs the analysis of random patterns and sometimes (cf. photo #1) actually finds some simple correlations.

I hope that this last input to the PPC Calculator Journal (starting from the beginning of 1984 I will remain Computer activists only) will be of some interest to PPC members.

Jakub Tatarkiewicz (2865)
ul.Chocimska 35 m.10
00 791 Warszawa
Poland

CONTINUED ON NEXT PAGE

A CHRISTMAS POEM

'Twas the night before Christmas in my humble abode
I'm just burning an eprom with some micro code.
Two pills I just downed for a first class migrane
when I heard something banging on my window pane.
A red-suited fat man was standing out there
he was grousing and mumbling and clawing the air.
More than his presence I was astonished to see
one of his hands clutching a 41-C.

A large bag was sagging over his shoulder,
out from which dropped a magnetic card holder.
Extensions and peripherals hung out of his sack,
a printer, a plotter, and one finance pack.
I could see in his pockets some ROMs he included,
and, yes, from his sleeve a black wand had protruded.

"Whats wrong?" I inquired as his voice got more hoarse.
"This thing in my hand has me way, way off course."
"I was using this tool at my kind elves insistance
to plot where I've been and determine the distance.
It worked really well when I got up today
but started to crash when I rode in the sleigh.
Now what do I do when the kids are in slumber?
Call up HP with their 800 number?

"Why Santa, it's frozen," I said with a sigh
you can't press those buttons when you travel so high.
Also you'll know, sooner or later,
The "Low Bat" signs on in the annunicator.

"Machines I don't need, as the old legend goes
I'll cruise by my instinct and Rudolph's red nose.
If I want a computer to guide me over the trees,
I'll tie to my reins eight Corvallis E.E.'s"
"But Santa," I said, "there is help, here, you'll see
A map! to a place where it says PPC.

"Oh really!" He shouted as he went to his coat
and like a conjurer he flashed out a note.
In Neanderthal scribbling here's what it said:
"Dear PPC members I've gone home to bed
there's a bug going around -- Herpes I'm told
I've developed a fever, some chills and a cold
so I'm closing up shop; I sure hope you don't mind
If you call on the phone a recording you'll find.

He kicked the computer a few feet my way
started laughing insanely and then he did say
"So now what's it good for? A beep, or a tone?
and made a street gesture internationally known.
He smiled rather darkly and pointed up to the roof
then snapped both his fingers and was gone in a poof.

And the last words I heard as he took to the sky
"Will I have better luck if I go to T.I.?"

Barry Price (4146)
2833 N. Bristol #588
Santa Ana, CA 92706

USERS REVIEW

USERS REVIEW is a column for members to provide their reviews of other publications covering topics of interest to calculator users.

Instrument Engineering Programs by Stanley W. Thrift. ISBN 0-87201-387-1.

This is a compilation of instrument engineering programs for use on the HP-41C and the TI-59.
The programs cover Control Valves for liquid, gas or vapour, steam, and two phase flow. That is sizing of valves. Line pressure drop across control valves. Sizing of flow elements (orifice plates, venturi and flow nozzles) for liquid and gas or vapour flow. Sizing of restriction orifices for liquid and gas or vapour flow. Pressure relief valve sizing for various conditions. Tank vent sizing and some other related areas.

The programs for the HP-41C require a quad memory module or a 41CV. Each program has a set of user instructions, a print out for an example, a listing of the memory register from 000 to 079 and a program listing with rough headings of what the individual routines do. Also after the program listing there is a sequence of calculations which gives the calculations used in order and gives any limits. Following this is a nomenclature of symbols used and references.

I found the programs easy to use but a pain to put into the calculator. Thrift recommends using a card reader and a printer and I agree with him. The 80 registers of memory, 200 to 300 program steps, and long alpha string prompting necessitate this. In most cases all the data needed to input properties of vapours, gases and liquids are available in the text.

I do, however have some negative comments to make with regard to the data register listings and the program listings. In some programs the logic is incorrect but I only found two cases of this and using the calculation listings and limitations these were easily fixed. In some cases the data printed listings is in the fix 4 mode and unfortunately the data is actually in fix 6. However as the data in question only gives the prompting routine the register in which the alpha components for string formation are it is reasonably easy to compare the prompt with the example and obtain what is missing. I also found an example where the alpha data was incorrect and I had to use the same technique.

In summary if you want a set of programs for instrument engineering and do not have the time available to write them your self this may be what you are looking for.

The book was published in 1982 by Gulf Publishing Company, Book Division, P.O. Box 2608, Houston, Texas 77001. and in their 1983 catalog is priced at $65.00.

Bar code is to follow, at an estimated $50.00.

Regards,

Terence H. Bartlett (9596),
C/- New Plymouth Power Station,
Private Bag,
New Plymouth,
New Zealand.

TELEPHONE BULLETINS

8.8.8.8.8.8 Richard Nelson with your PPC Bulletin Number 8, September 22nd, 1983. Orlando Conference: Proceedings for PPC Conference No. 7 are available for $6.00 plus shipping – $1.56 first class in the US. The 108 pages makes this the biggest proceedings to date. MCODE, HP-75 FORTH and VisiCALC,

Continued on page 24.

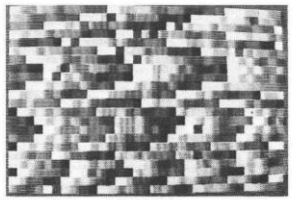


Photo 1: RNG: r_{i+1} = FRC IEXP(PI*r_i)]
HP-25 Games, Slow

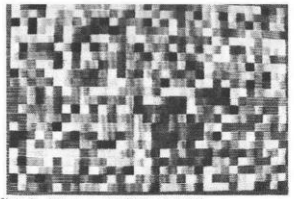


Photo 2: RNG: r_{i+1} = FRC (9821r_i+0.211327)
PPC ROM

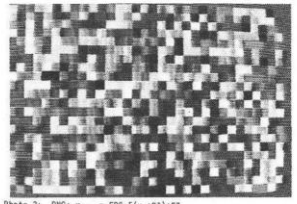


Photo 3: RNG: r_{i+1} = FRC [(r_i+PI)+5]
Original HP-25 Slow

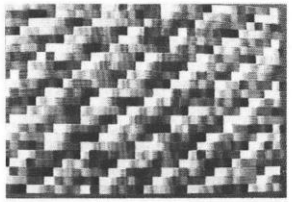


Photo 4: RNG: r_{i+1} = FRC (180/PI r_i)
Albillo V7N6P35

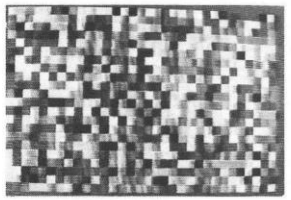


Photo 5: RNG: r_{i+1} = FRC (3579r_i)
Marsaglia V8N3P23

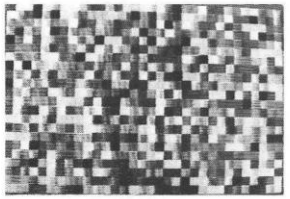


Photo 6: RNG: r_{i+1} = FRC (997r_i)
HP38

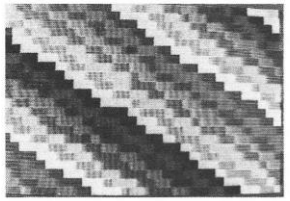


Photo 7: RNG: r_{i+1} = FRC [21(v_i+PI)]
R. Moore V6N2P20

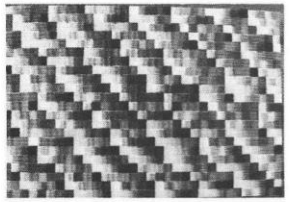


Photo 8: RND: (SINCLAIR)

Fast forward to 2024

- In 1996 moved to USA; in 2008 became US citizen
  - Worked at MIT, UCSD, founded startup MANTA Inc.
- In 2020 founded startup RANDAEMON in Poland
- We develop true quantum random number generators based on beta decay (tritium, nickel-63)
- RANDAEMON got 11 US patents allowed
- Some of our patents used Monte Carlo simulations
- Testing tQRNGs is purely statistical process after random numbers are produced – only probability if they are OK
- We can only test finite number of random bits - time

Random numbers are produced

"Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, ***there is no such thing as a random number - there are only methods to produce random numbers****, and a strict arithmetic procedure of course is not such a method."*

J. von Neumann, **Various techniques used in connection with random digits**

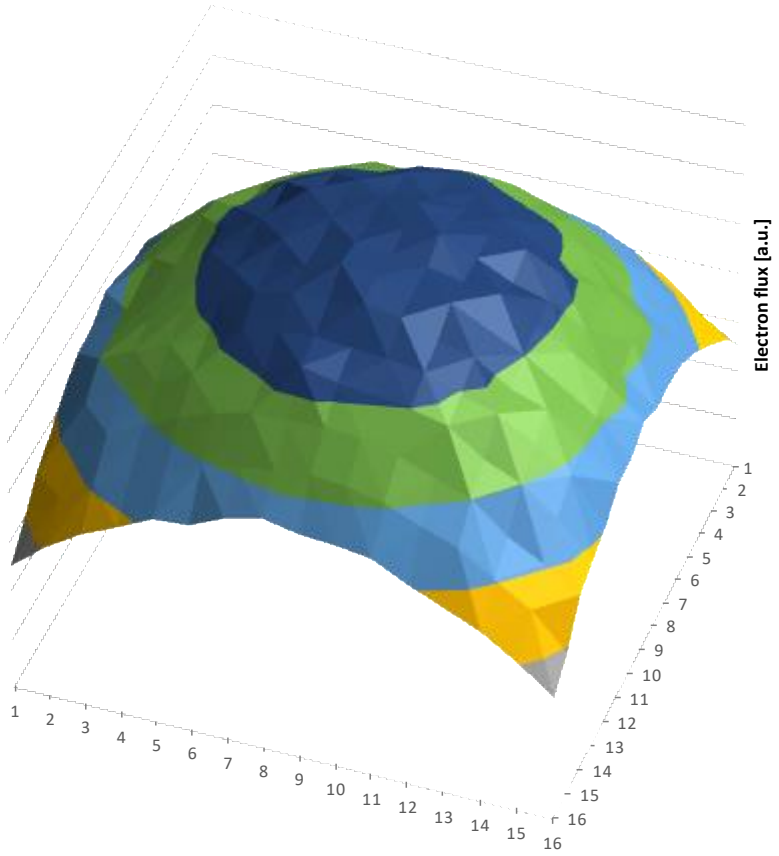
vol. **Monte Carlo Method**, eds. A.S. Householder, G.E. Forsythe and H.H. Germond, **1951**

Simulation in Excel using Visual Basic

N = 256 (matrix 16 x 16)
a = 2 mm (distance between source and detectors)
b = 1.6 mm (side of the square matrix)
c = 1 mm (overhang of the source over matrix)
d = 0.1 mm (single detector diameter)

Monte Carlo simulation involved generation of $8 \cdot 10^9$ electrons*
☞ only 1.4 % reached the matrix

** VB function Rnd() has a period of about $2 \cdot 10^7$ numbers; we used RndM() based on Wichmann-Hill algorithm with a cycle of about $7 \cdot 10^{12}$ different numbers possible*



BARN – new class of ciphers

- Cryptography is all about maximizing entropy
- Bury Among Random Numbers
  - Bits of any digital message are inserted into the stream of random bits from tQRNG
  - Insertion is following a key or some random pattern
  - US patent 12,034,834
- The BARN method is easy to program (low power) but hard to crack by brute force only
  - 256-bit octal key creates about $4 \cdot 10^{62}$ permutations

How BARN works

bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	…
bits	0	0	0	1	1	0	1	0	0	0	0	0	1	0	1	1	1	0	1	0	0	…

stream of random bits

bit#	1	2	3	4	5	6	7	8	9	10
bits	1	1	1	0	0	0	1	1	0	1

message

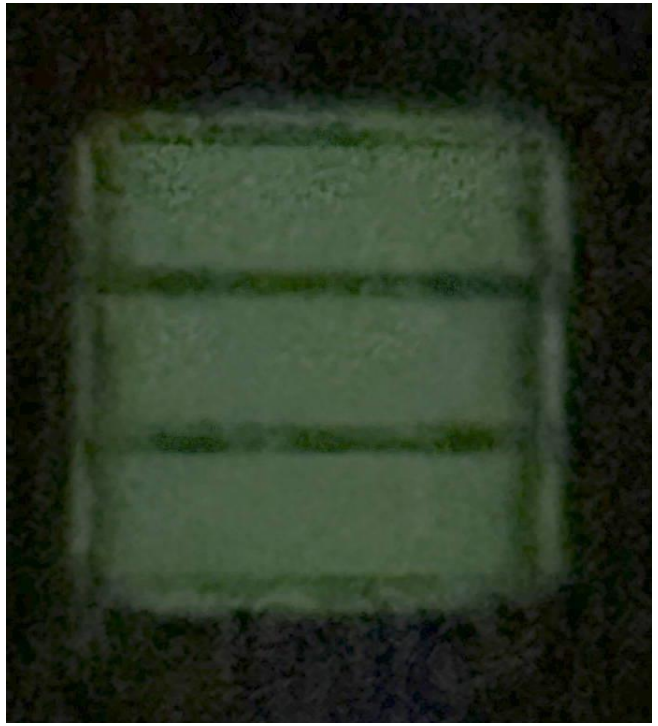
bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
bits	**1**	0	0	**1**	1	**1**	**0**	**0**	0	0	**0**	0	**1**	**1**	**0**	1	1	**1**	1
shift	*1*			*3*		*2*	*1*	*1*			*3*		*2*	*1*	*1*			*3*	

message embedded into the random bit stream, key {1, 3, 2, 1}

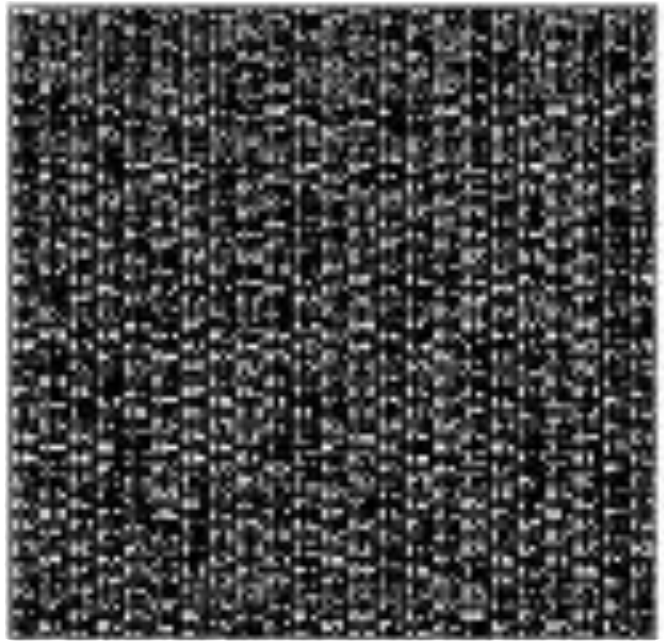
bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
bits	1	**0**	**0**	1	**1**	**1**	0	**0**	**0**	0	**0**	**0**	1	**1**	**0**	1	**1**	**1**	1
shift		*2*	*1*		*2*	*1*		*2*	*1*		*2*	*1*		*2*	*1*		*2*	*1*	

failed attempt to decode a message, key {2, 1, 2, 1}

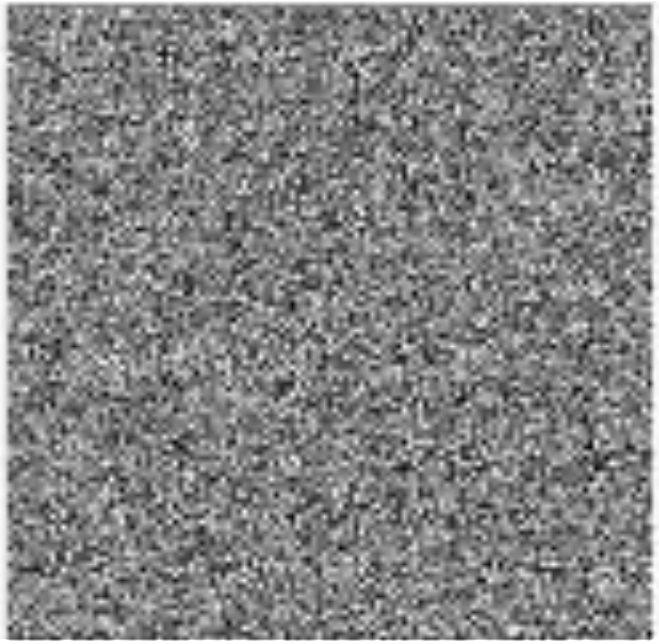
Testing tQRNG and BARN visually



Trigalights®



Text



Cipher

To remember

- Good random numbers are produced, not generated by some arithmetical formula
- AI can analyze sequences of PRNGs and eventually find the formula used to generate random numbers
- Only physical quantum sources of entropy can be trusted
- Even such sources require proof (typically there are based on Poisson or Gaussian distributions of events)
- When running simulations, do not trust PRNGs as most have very short sequences compared to billions of points