A NOVEL SIMPLE WAY TO GENERATE PSEUDO RANDOM NUMBERS

ITAMARACÁ

FRNS = ABS [N - (PN * XRN)]

DH PEREIRA

UNIVERSITY OF CAMBRIDGE

TechRxiv™ Powered by IEEE

UNDERSTANDING ITAMARACÁ

- Itamaracá or simply "Ita" is a novel, simple, fast and 'non-periodic' mathematical basis for PRNG that generates an "infinite" sequence of numbers within an interval [0,1] considering a uniform distribution.
- Its name is derived by the **Tupi-Guarani language in which means "Stone Shaker" or "Singing Stone"**, in this sense, a clear reference to something random or unexpected.

HOW ITA WORKS

Like all PRNGs algorithms, Ita have some distinctive features. Below we have some initial conditions:

- Firstly, choose N, that is, a maximum value within a range between 0 and N selected by a user criterion, where $N \in \mathbb{N}$.
- In this model, there are 3 seeds S_0, S_1 and S_2. For each of these seeds choose any number $\in \mathbb{N}$ belonging to the interval between 0 and N (already choose previously).

HOW ITA WORKS

After selected all the 3 seeds, S_0, S_1 and S_2, the calculation process is divided in two main and very simple steps:

- Pn (n Process)
- Final Calculation

HOW ITA WORKS

Pn (n Process) or Intermediate State

In this stage we need taking into account the absolute values considering the differences between the 2 seeds that must be moving in the sequence.

$$Pn = ABS\ (S2 - S0)$$

HOW ITA WORKS

Final Calculation or General Formula

In this step, we must multiply the "x" result obtained in the first step (in Pn) by the Xrn, that is, any value in which its founded value is desirable to be close to 2 (i.e. 1.97, 1.98, 1.99789...).

$$FRNS = ABS\,[N - (Pn * Xrn)]$$

APPLICATION EXAMPLE

Let's assume we want to generate numbers from 0 to 10,000:

N	10,000
Seed 0	8,777
Seed 1	11
Seed 2	8

APPLICATION EXAMPLE

We can generate the **first number** using the intermediate state (Pn) and then using the main formula, as we can see below:

P_1 = ABS (8 – 8,777) = 8,769

$FRNS_1$ = ABS [10,000 - (8,769*1.97) = 7,275

APPLICATION EXAMPLE

2nd number:

P_2 = ABS (7,275 – 11) = 7,264

$FRNS_2$ = ABS [10,000 - (7,264*1.97) = 4,310

3rd number:

P_3 = ABS (4,310 – 8) = 4,302

$FRNS_3$ = ABS [10,000 - (4,302*1.97) = 1,525

APPLICATION EXAMPLE

So, we have the first three numbers generated:

7,275 - 4,310 and 1,525...

The next sequences from now on follow the same calculation logic.

RESULTS OF SOME TOOLS AND STATISTICAL TESTS

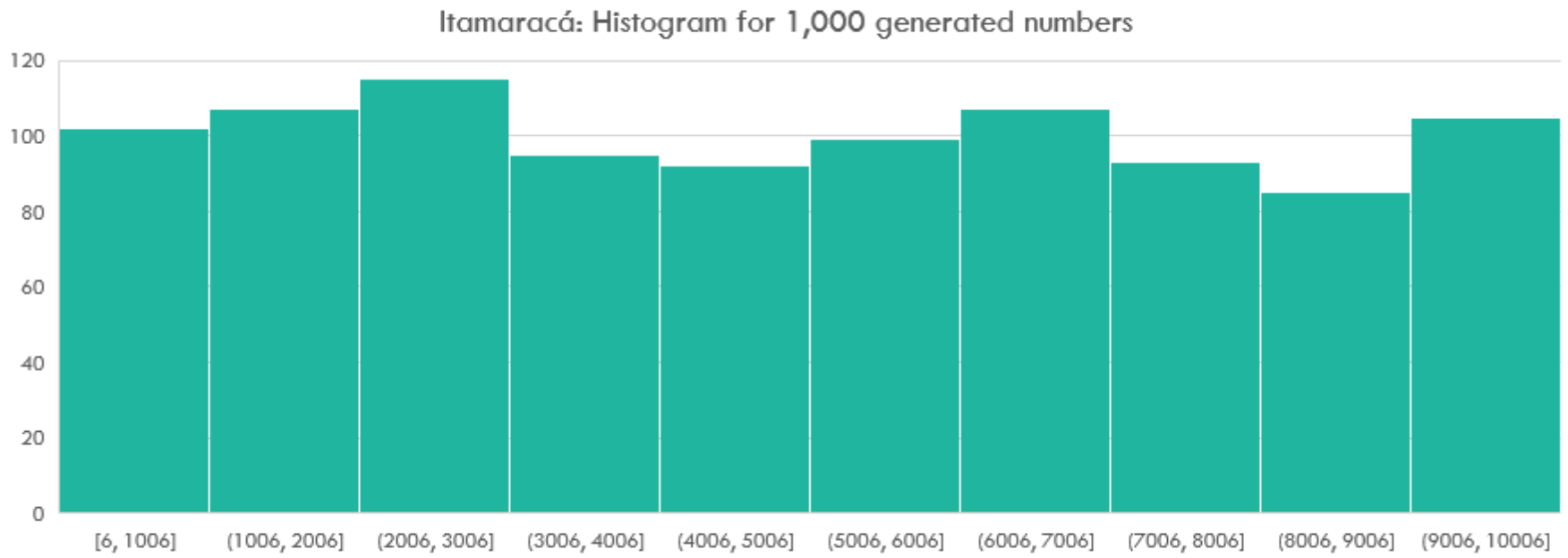
Comparing the results between Ita and TRNG by Random Org considering 10,000 numbers generated

Tests	Ita	Random Org
Chi-Square	11.26	3.65
Repeated Numbers / N	3,618	3,763
Average / Standard Deviation	4,941 / 2,884	4,925 / 2,905
Run Test (Even/Odd)	-0.914634	0.004101
Run Test (Median)	0.759184	0.603023
Autocorrelation (Average of the first 10 k-lags different from 0)	0.000103	0.000980
Shannon Entropy	3.45327	3.45284

Note: Methodology used for evaluating the results are exactly the same as those contained in the published version.

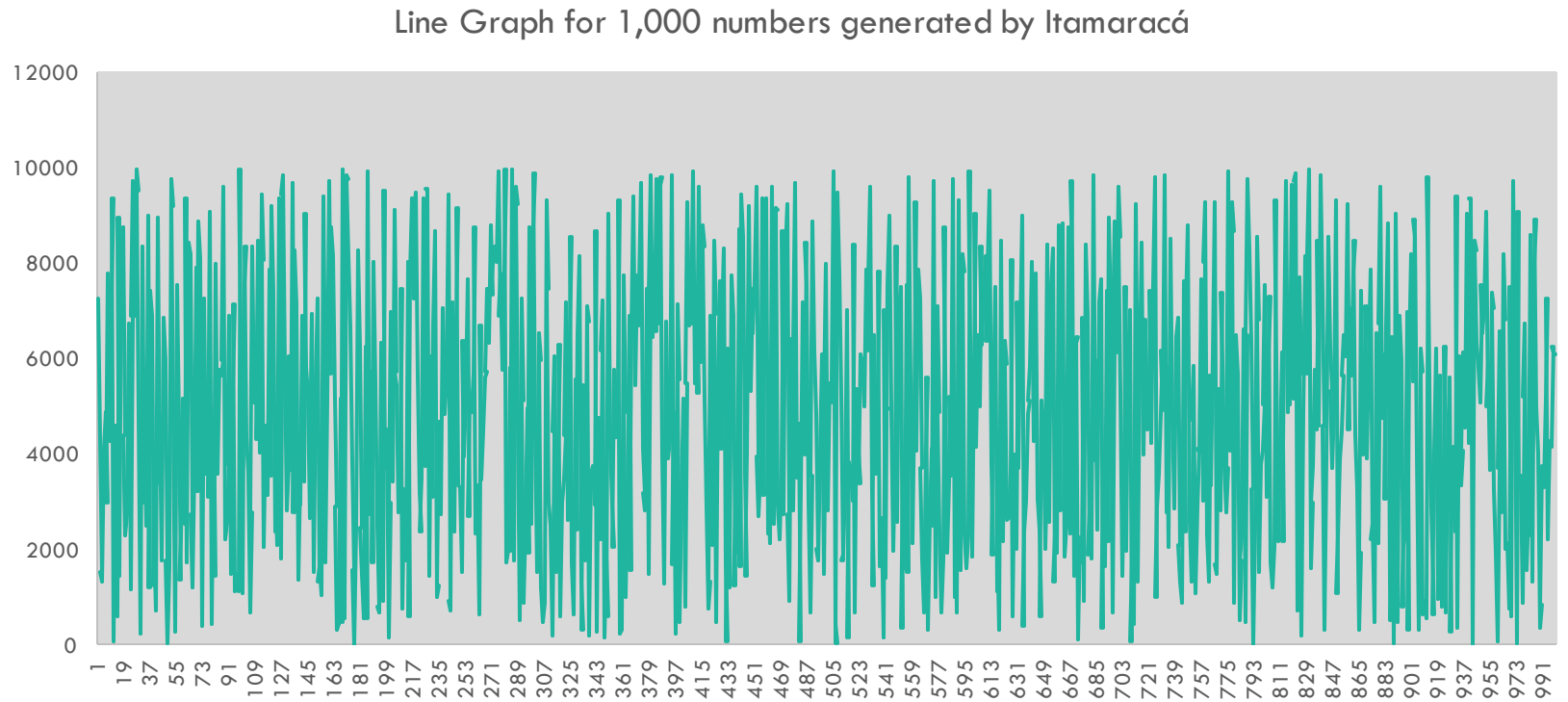
RESULTS OF SOME TOOLS AND STATISTICAL TESTS

Histogram for Ita model



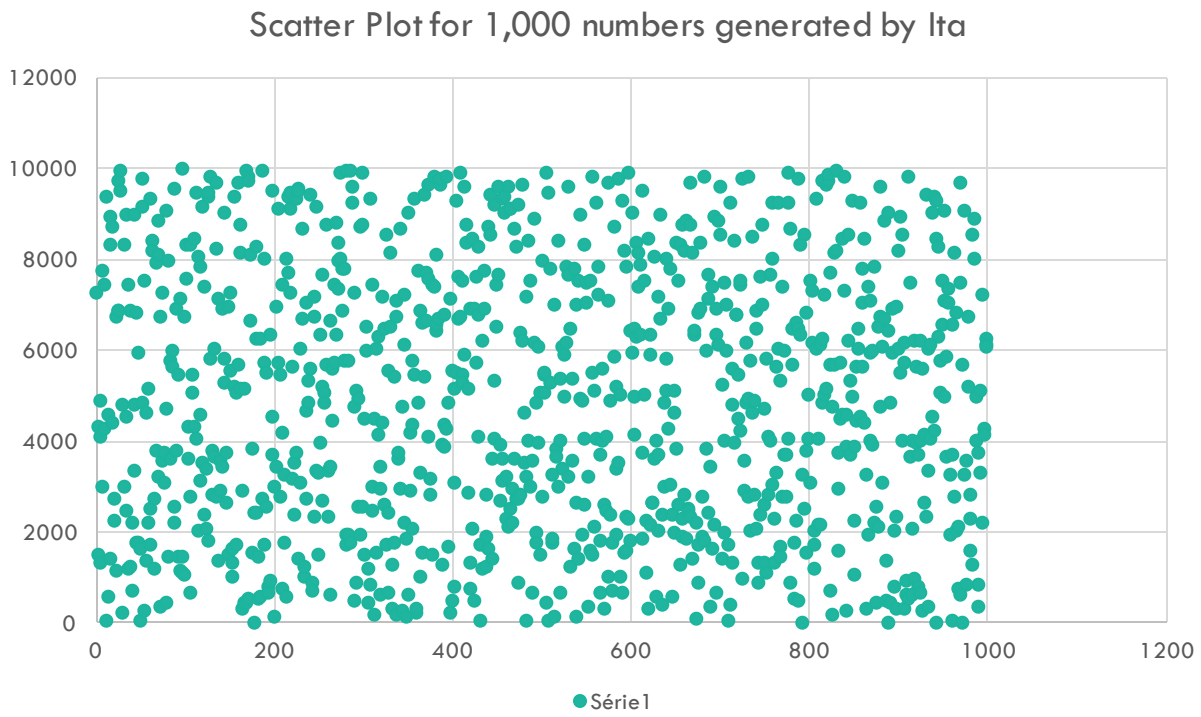
RESULTS OF SOME TOOLS AND STATISTICAL TESTS

Run Sequence for Ita model



RESULTS OF SOME TOOLS AND STATISTICAL TESTS

Scatter Plot for Ita model



SOME CONSIDERATIONS

- Ita model has proven to be a good random number generator, especially in the criteria that evaluate independence and uniformity. Despite being a recent study, there are good perspectives regarding the computational cost and its applicability for the cryptography area and becoming a CSPRNG.

- Another point to be highlighted is that it was not observed any rule of choice regarding the value of the seeds, it is enough they are chosen arbitrarily with values are within the range from 0 to N where $N \in \mathbb{N}$, their maximum value.

SOME CONSIDERATIONS

- Regardless of the initial seed values used, there is a strong tendency for the algorithm to pass basic statistical tests for uniformity and independence. However, although approved, some chosen values can cause the results of certain tests to be "better" or "worse" than when using other seeds.

SOME CONSIDERATIONS

- *Ita model as every PRNG also has some identified limitations. As an example, at some point probably after a large amount of generated numbers, the repetition of the same sequence of generated numbers only tends to repeat if and only if the values of the 3 initial seeds (S0, S1 and S2) appear in the middle of the generated sequence.*

- Despite this limitation, we can see it is very difficult for this sequence of numbers to be repeated itself completely, as we increase the value of N and considering an uniform distribution [0,1].

Well, we can infer it is a generator that generates "infinite" and 'non-periodic' psedourandom numbers.

CONCLUSION

The generation of random numbers is too important for several fields of study and practical applications for the development of mankind.

The present study, presented a new and simple proposal of a Pseudo Random Number Generator (PRNG) called "Itamaracá" (Ita in a abbreviated form). Ita model, like all PRNG algorithms, has some limitations, but in general, it showed good results in the statistical tests considered, and thus, as one more model in the portfolio, it is fully available for use and above all, for new studies, especially those applied to a specific objective and real problems.