Scientific Research Publishing

Journal of Information Security, 2020, 11, 149-160
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Towards Post-Quantum Cryptography Using Thermal Noise Theory and True Random Numbers Generation

Protais Ndagijimana[1], Fulgence Nahayo[2], Marc Kokou Assogba[3], Adoté François-Xavier Ametepe[4], Juma Shabani[1]

[1]Doctoral School and Faculty of Science, University of Burundi, Bujumbura, Burundi
[2]LURMISTA-ISTA; University of Burundi, Bujumbura, Burundi
[3]Laboratoire d'Electrotechnique, de Télécommunications et d'Informatique Appliquée LETIA, Ecole Polytechnique d'Abomey-Calavi, EPAC; Université d'Abomey-Calavi, Cotonou, Bénin
[4]Institut de Mathématiques et de Sciences physiques, IMSP; Université d'Abomey-Calavi, Cotonou, Bénin
Email: ndaprotais2000@yahoo.fr, juma.shabani@ub.edu.bi, fulgence.nahayo@ub.edu.bi, mkokouassogba@gmail.com, adote007@gmail.com

How to cite this paper: Ndagijimana, P., Nahayo, F., Assogba, M.K., Ametepe, A.F.-X. and Shabani, J. (2020) Towards Post-Quantum Cryptography Using Thermal Noise Theory and True Random Numbers Generation. *Journal of Information Security*, 11, 149-160.
https://doi.org/10.4236/jis.2020.113010

Received: May18, 2020
Accepted: July 12, 2020
Published: July 15, 2020

Abstract

The advent of quantum computers and algorithms challenges the semantic security of symmetric and asymmetric cryptosystems. Thus, the implementation of new cryptographic primitives is essential. They must follow the breakthroughs and properties of quantum calculators which make vulnerable existing cryptosystems. In this paper, we propose a random number generation model based on evaluation of the thermal noise power of the volume elements of an electronic system with a volume of 58.83 cm^3. We prove through the sampling of the temperature of each volume element that it is difficult for an attacker to carry out an exploit. In 12 seconds, we generate for 7 volume elements, a stream of randomly generated keys of 187 digits that will be transmitted from source to destination through the properties of quantum cryptography.

Keywords

Thermal Noise, True Random Numbers, Algorithm, Post-Quantum Cryptography

1. Introduction

The emergence of quantum computers exposes classical cryptosystems. These cryptosystems whose semantic security is based on difficult mathematical problems and algorithmic complexity become vulnerable. Shor's [1] and Grover's [2] algorithms are a perfect illustration. The first solves the problems of large numbers factorization and discrete logarithm in polynomial time [3] while the second [4] favors cryptanalysis of the AES for size keys of 128 and 192 bits [5]. This challenge to the fundamentals of symmetric and asymmetric cryptography worries the researchers. It leads to the rise of quantum and post-quantum cryptography [6]. However, post-quantum cryptography implemented through NP-complete problems [7] cannot guarantee perfect secrecy [8]. A promising related theory is the generation of random numbers associated to quantum physical phenomenon [9]. The aim is to exploit the laws of quantum physics associated to basic principle of cryptology for the implementation of new cryptographic primitives.

In this work, we propose a random number generation model using the thermal noise theory. This model is described as a sequence of concatenation of the integer and decimal parts of the thermal power of each volume element of an electronic system. The power is evaluated by sampling the temperature in non-equilibrium state according to Fourrier's law [10]. For a sampling period (*t*) with $t \in [0; +\infty[$, we prove that it is impossible for an attacker to determine exactly the variations of the temperature (ΔT_i), so the sequences of generated numbers.

We devote the first and second sections respectively to an exhaustive study of TRNG using the properties of quantum physics, and the description of the proposed mechanism. In third section, we carry out the experiments and performances analysis.

2. Related Works

In this section, we make an exhaustive study of the random numbers generators based on the properties of quantum physics.

2.1. True Random Number Generator

A True Random Number Generator (TRNG) is a device able to produce a sequence of numbers for which there is no known deterministic link paradoxically to the pseudo-random number generator [9]. According to Stipcevic and Koç [11], it follows that a true random numbers is a sequence of numbers for which there is no deterministic algorithm.

In computer science, a hardware random number generator is a device that generates random numbers from a physical phenomenon rather than use of a computer program [12] [13] [14] [15]. These systems are in most cases based on laws of quantum physics and proven random phenomena. Several techniques exist for the generation of these random numbers whose properties are widely used in cryptography. These properties ensure the absolute information security. As example, we mention the techniques based on noise amplification, phase jitter in oscillators, the impact of noise on metastable behavior [16] and noise amplification based on chaos circuits [12]. These mechanisms are real entropy sources for random number generation.

However, they have the limits that require researchers to move towards other innovative primitives. For illustration purposes, research topics are oriented towards nano-devices, inverters, oxide distribution and random telegraph noise. Although these methods are efficient for producing true random numbers, their implementation proves to be complex for 14 nm processors and its derivatives [12].

2.2. Thermal Noise Study

Noise refers to all harmful signals that overlap with the useful signal at any point in a measurement chain or transmission system. The useful signal represents the information, while noise is a hindrance to understanding the information conveyed by the signal. In electronics, it presents interesting properties due to its randomness. According to Johnson-Nyquist work [17] [18], we define thermal noise as the noise generated by the thermal agitation of charge carriers. In other words, that is electrons at thermal equilibrium in electrical resistance. It is expressed:

- when we evaluate the noise across resistor [17] [18] by:

$$\bar{v}_b^2 = 4KTR\Delta F; \tag{1}$$

with:

$\bar{v}_b^2$: Voltage variance across the resistor,

K: Boltzmann constant, $K = 1.3806 \times 10^{-23}\,\mathrm{J \cdot K^{-1}}$,

T: resistor absolute temperature expressed in kelvin,

R: resistance expressed in Ohms,

ΔF : bandwidth expressed in Hertz.

This application enables to predict the minimum noise in electronic system and its detection limit:

- when we evaluate the power of thermal noise [17] [18] by:

$$\eta_0 = KT\Delta F; \tag{2}$$

with:

K: Boltzmann constant, $K = 1.3806 \times 10^{-23}\,\mathrm{J \cdot K^{-1}}$,

T: conductor temperature expressed in Kelvin,

ΔF : bandwidth in Hertz,

η_0 : thermal noise power, expressed in Watt.

Thermal noise is inevitable and unpredictable in electronic systems and has quite important characteristics when Shannon theory is associated it [19]. Indeed, by considering the noise as information source, it is possible to evaluate the quantity of derived information. In cryptography, this quantity of information is an entropic source for true random numbers generation. Through **Table 1**, we make a comparative study of mechanisms of which entropy describe good results for true random numbers generation [12] [16] [20].

Table 1. Comparative study of the mechanisms leading to true random numbers generation.

Classification		Technology	Advantages	Limits
AAmplify Noise		Analog	Simple structure	High energy consumption
Oscillator	Couple Oscillator	Digital	Easy integration	Vulnerable to frequency attacks
	Ring Oscillator	Digital	Good portability	Hermetic
	FIRO/GARO	Digital	More sensitive to jitter	Vulnerable to feedback connections leading to arbitrary output
Metastability		Digital	Easy integration	Sensitive to physical phenomena and vulnerable to symmetry of metastability
Chaos	Continuous Time	Analog	High rate	High energy consumption
	Discret Time	Digital	High rate	Finite computable precision with a pseudo-random output

Scott A. Wilber [13] proposes a mechanism for non-deterministic random numbers generation. It uses an electronic assembly of two oscillators producing output signals, of which one is multiplexed. The processor extracts the entropy resulting from the fluctuation during successive emission of signals by the two oscillators for true random numbers generation. The author mention that random number generators use physical sources of entropy evaluation. This value is then used as information source for true random numbers generation. Thus, it is possible to establish a hypothesis between the entropy and its evaluation sources. However, we estimate that Scott A. Wilber's approach inherits the limits of the oscillatory phenomena due to periodic properties of these phenomena. Indeed, study and determination of the frequencies of emitted signals by each oscillator influence the entropy. The device is therefore vulnerable to side channel attacks. Let's consider g, as the fluctuation between two signals according to time t and respectively frequencies f_1, f_2, if:

$$\lim_{t\to+\infty} g(t) = 0; \tag{3}$$

an attacker who studies behavior of the system, could compute the entropy accurate values. Therefore, they are many theories and implementation for true random numbers generation [21] [22]. Despite research efforts, the weaknesses persist and the semantic security still a great challenge due to advances in the implementation of quantum computers and side channel attacks. So, new theories need to be developed.

3. Architecture of Proposed Mechanism

In this section, we present logical structure of the proposed true random number generation mechanism. Also we perform the tests.

3.1. Logical Structure

Let's consider an embedded system in non-equilibrium state. Its density is given by:

$$\rho = \frac{m}{v}; \tag{4}$$

with:

ρ : density expressed in kg·m^{-3},

m: mass expressed in kg,

v: volume expressed in m^3.

According to Fourier's law [10] this non-equilibrium state generates a variation in temperature and creates a heatflow defined by:

$$F = I \times S \times GradT; \tag{5}$$

with:

F: heatflow in Watts,

S: plane area expressed in m^2,

I: thermal conductivity expressed in W·m^{-1}·K^{-1},

$GradT$: temperature gradient expressed in K·m^{-1}.

Let's consider:

a volume element of embedded system defined by:

$$v = \iiint_{\Sigma} \mathrm{d}x\mathrm{d}y\mathrm{d}z; \tag{6}$$

ΔT : the measured temperature according to time (*t*) and space (v). We evaluate it considering two parameters:

- time(*t*): it is sampling period of temperature;
- volume element (v): it is the volume element considered during temperature evaluation. The evaluation of thermal noise power in relation to its volume element is defined by:

$$Pv = K\Delta T\Delta F; \tag{7}$$

with:

K: Boltzmann constant, $K = 1.38 \times 10^{-23}\,\mathrm{J} \cdot \mathrm{K}^{-1}$,

ΔT : volume element temperature expressed in Kelvin,

ΔF : bandwidth expressed in Hertz,

Pv : thermal noise, expressed in Watt.

Let's consider:

$P_e v$ and $P_d v$ respectively as the integer part and the decimal part of the thermal noise power.

TRNG as the concatenation of $P_e v$ and $P_d v$ ($P_e v \,||\, P_d v$) such as :

$$TRNG_i = P_e v_i \,||\, P_d v_i; \tag{8}$$

where $TRNG_i$: the sequence of random numbers generated and $i \in [0; +\infty[$ the clock step of each temperature evaluation. Also, we describe through an algorithm, the proposed mechanism for true random numbers generation.

Algorithm 1 : True Random numbers generation

```
Input:
  $lenghtVariation\ dx$,
  $widthVariation\ dy$,
  $heighVariation\ dz$,
  $frequencyRange\ \Delta F$,
  $samplingTime\ t$
Output:
  $volumeElement\ \nu_i$,
  $temperatureVariation\ \Delta T_i$,
  $thermalPower\ P\nu_i$;
  $trueRandomNumberGeneration\ TRNG_i$,
  $integerPart\ P_e\nu_i$,
  $decimalPart\ P_d\nu_i$
Begin:
  $\nu_i \leftarrow 0$; //Volume element initialization
  $\Delta T_i \leftarrow 0$; //Temperature initialization
  $For\ t\, \varepsilon[0; +\infty[\ , i\, \varepsilon[0; n]i++$
      $\nu_i \leftarrow d_x\, d_y\, d_z$; //Volume element determination
      $While\ \nu_i > 0$
        $P\nu_i \leftarrow K\Delta T_i \Delta F$; //Thermal power evaluation
        $P_e\nu_i \leftarrow integer(P\nu_i)$; //retrieval of integer part
        $P_d\nu_i \leftarrow P\nu_i - P_e\nu_i$; //retrieval of decimal part
        $TRNG_i \leftarrow P_e\nu_i || P_d\nu_i$; //True random number generation
      $End\ while$
  $End\ for$
$End$
```

3.2. Security Proof

We evaluate the robustness of the proposed mechanism through the notion of entropy derived from Shannon [23] and Yamamoto [24] and the constraints to which the model is subjected:

- the numbers are generated following the measured temperature (ΔT_i) within each volume element (ν_i) of the proposed device;
- the measured value determines the power ($P\nu_i$) of the thermal noise.

Let's note respectively: X, Y, Z the random variables associated to the sources ($P\nu_i$), (ΔT_i), (ν_i) and $H(X)$, $H(Y)$, $H(Z)$, their entropies.

Let's consider the determination of the thermal noise power of a volume element as a source of information. Its probability and entropy follow respectively the relation:

$$P(X = x_i) = P(Y \mid Z); \tag{9}$$

$$\begin{aligned} H(X = x_i) &= -\sum_x P(X = x_i)\log\left(P(X = x_i)\right) \\ &= -\sum_x P(Y \mid Z)\log\left(P(Y \mid Z)\right) \end{aligned} \tag{10}$$

(By identification following to (10));

with: $P(Y \mid Z) = \dfrac{P(Y \cap Z)}{P(Z)}$.

For an infinity of volume elements (z), $z \to +\infty$:

1) $P(Z = z_i) \to 0$ (equiprobability);

2) $P(Y \cap Z) \to 0$ (nonequiprobable due to the source ($Y = y_i$);

3) $P(X = x_i) = P(Y \mid Z) \to 0$.

From 1), 2) and 3), we have:

$$\begin{aligned} H(X = x_i) &= -\sum_x P(X = x_i)\log\left(P(X = x_i)\right) \\ &= -\sum_x P(Y \mid Z)\log\left(P(Y \mid Z)\right) \to 0 \text{ bit.} \end{aligned} \tag{11}$$

Thus, an attacker has none information to determine the thermal power of each volume element.

We conclude that the proposed mechanism is efficient.

3.3. Description of Experimental Environment

We use an Arduino Uno ATMega 328p [25] as source of the thermal noise. It generates a solid (Σ) of space (ω).

We mention that the function which characterizes each volume element of the solid (Σ) is defined by:

$$\nu = \iiint_{\Sigma} \mathrm{d}x\mathrm{d}y\mathrm{d}z; \tag{12}$$

We define by framing in black (**Figure 1**) the considered volume elements during the temperature evaluation. They are referenced by numbering. We perform the tests on a set of 7 volume elements.

For each volume element of the electronic system, we deploy a temperature sensor type LM 35. Then, we determine the power for each volume element according to the temperature values measured.

We summarize through **Table 2** and **Table 3**, the obtained results following the experiments.

Table 2. Obtained results (Power computation).

Index	Volume (cm^3)	Constant J·K^{-1}	Temperature (K)	Frequency (Hz)	Time (s)	Power (w)
ν_1	1.35	1.3806×10^{-23}	305.25	16×10^3	0	$67{,}428{,}504 \times 10^{-24}$
ν_2	1.46	1.3806×10^{-23}	303.55	16×10^3	2	$670{,}529{,}808 \times 10^{-25}$
ν_3	1.08	1.3806×10^{-23}	305.85	16×10^3	4	$675{,}610{,}416 \times 10^{-25}$
ν_4	1.98	1.3806×10^{-23}	297.85	16×10^3	6	$657{,}938{,}736 \times 10^{-25}$
ν_5	22.2	1.3806×10^{-23}	304.75	16×10^3	8	$67{,}318{,}056 \times 10^{-24}$
ν_6	1.2	1.3806×10^{-23}	296.45	16×10^3	10	$654{,}846{,}192 \times 10^{-25}$
ν_7	5.4	1.3806×10^{-23}	296.95	16×10^3	12	$655{,}950{,}672 \times 10^{-25}$

Table 3. Obtained results (Retrieval of integer part and decimal part).

Clock step	Time (s)	Volume (cm^3)	Power (w)	Integer part	Decimal part
1	0	1.35	$67{,}428{,}504 \times 10^{-24}$	0	$67{,}428{,}504 \times 10^{-24}$
2	2	1.46	$670{,}529{,}808 \times 10^{-25}$	0	$670{,}529{,}808 \times 10^{-25}$
3	4	1.08	$675{,}610{,}416 \times 10^{-25}$	0	$675{,}610{,}416 \times 10^{-25}$
4	6	1.98	$657{,}938{,}736 \times 10^{-25}$	0	$657{,}938{,}736 \times 10^{-25}$
5	8	22.2	$67{,}318{,}056 \times 10^{-24}$	0	$67{,}318{,}056 \times 10^{-24}$
6	10	1.2	$654{,}846{,}192 \times 10^{-25}$	0	$654{,}846{,}192 \times 10^{-25}$
7	12	5.4	$655{,}950{,}672 \times 10^{-25}$	0	$655{,}950{,}672 \times 10^{-25}$

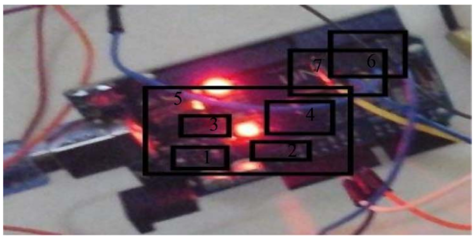

Figure 1. Volume elements [25].

4. Analysis and Discussions

We devote this section to the analysis of the results obtained during the tests. Thus, **Figures 2-4** represent graphs relating to the achieved results during the experiments. It is constant to note that the thermal noise power varies for each volume element at **Figure 4**. This variation happened due to changes of the temperature for each volume element over a time. Thus, the thermal noise power in a volume element means the determination of the following parameters: Temperature (T), time (t), and volume element (v). We conclude that the power varies according to temperature, volume element and time. As a result, the generated numbers vary in time and space and do not follow any deterministic approach. Therefore, they are deemed to be true and random.

We generate a number by concatenation of the integer and decimal parts of the thermal noise power obtained per volume element ignoring the decimal point. A sequence of generated numbers is equivalent to a sequence of concatenation of integer and decimal parts of the power of each volume element according to its assignment index j. So:

$$\text{for}\quad j \in [1;7] \Rightarrow v_j \in \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$$

$$\Rightarrow Pv_j \in \{Pv_1, Pv_2, Pv_3, Pv_4, Pv_5, Pv_6, Pv_7\}$$

$$\Rightarrow TRNG = \{P_e v_1 \| P_d v_1 \| P_e v_2 \| P_d v_2 \| P_e v_3 \| P_d v_3 \| P_e v_4 \| P_d v_4 \\ \| P_e v_5 \| P_d v_5 \| P_e v_6 \| P_d v_6 \| P_e v_7 \| P_d v_7\}$$

For 7 volume elements, we get a sequence of random numbers of 187 digits distributed as follows:

Let's note:

nv_i: number of digits for each volume element,

$nP_e v_i$: number of digits enumerated for the integer part of each volume v_i,

$nP_d v_i$: number of digits enumerated for the decimal part of each volume element v_i. The results are represented in **Table 4**.

Therefore, for z volume elements, $z \in [0; +\infty[$, it is very difficult for an attacker to determine exactly the different temperatures within each volume element and:

$$TRNG_z = P_e v_1 \| P_d v_1 \| P_e v_2 \| P_d v_2 \| P_e v_3 \| P_d v_3 \| P_e v_4 \| P_d v_4 \\ \| P_e v_5 \| P_d v_5 \| P_e v_6 \| P_d v_6 \| P_e v_7 \| P_d v_7 \| \cdots \\ \| P_e v_{z-4} \| P_d v_{z-4} \| \cdots \| P_e v_{z-1} \| P_d v_{z-1} \| P_e v_z \| P_d v_z.$$

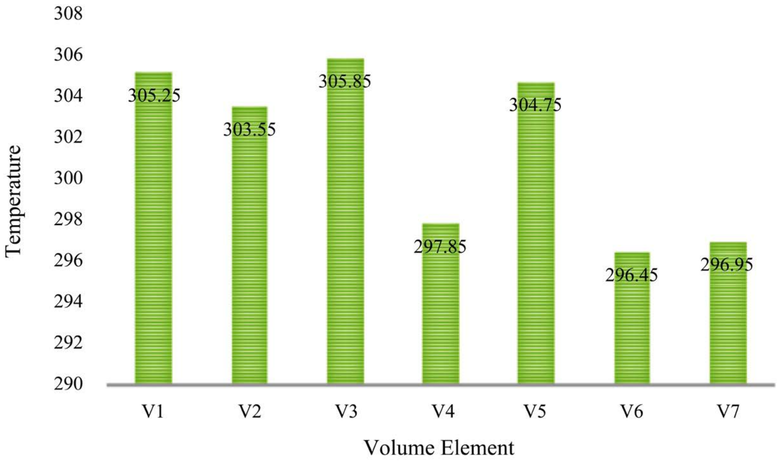

Figure 2. Variation of temperature depending on volume elements.

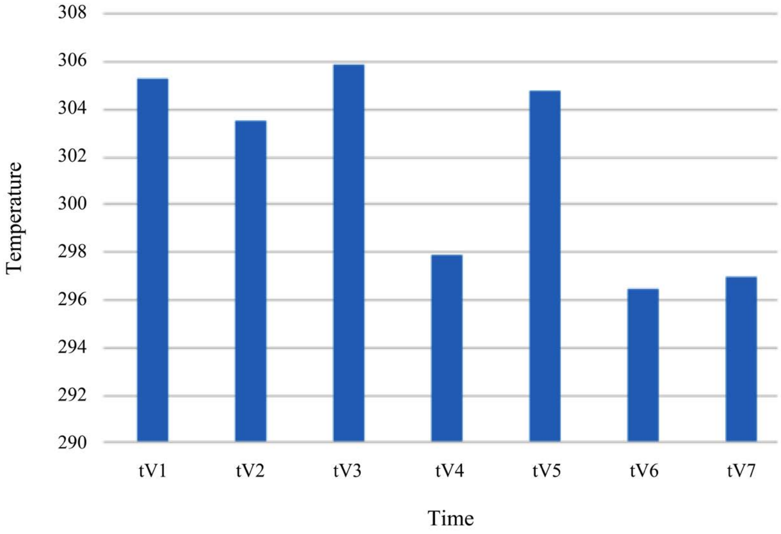

Figure 3. Sampling the temperature for each volume element.

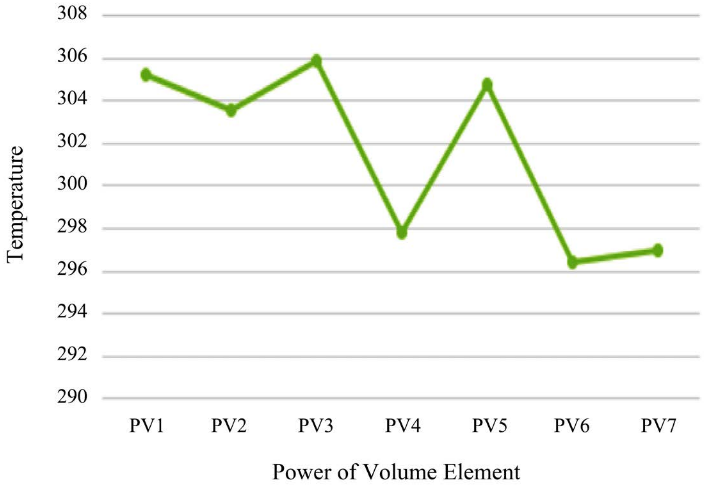

Figure 4. Variation of temperature depending on the power of thermal noise.

Table 4. Number of digits counted per volume element.

v_i	$np_e v_i$	$np_d v_i$	nv_i
v_1	1	25	26
v_2	1	26	27
v_3	1	26	27
v_4	1	26	27
v_5	1	25	26
v_6	1	26	27
v_7	1	26	27
	Total number of digits		187

The obtained TRN is converted into binary and recovered as a keystream. This keystream will be transmitted from the transmitter to the receiver through quantum cryptography properties. We will associate it on-time pad cryptographic method to secure the transmitted data.

5. Conclusion

In this paper, we have proposed a mechanism for true random number generation which can resist to an attacker with quantum computers. This mechanism uses the fundamentals of thermal noise theory which is a random phenomenon. For tests and experiments, we used an ATMega microcontroller as a solid space that generates volume elements. We sample the temperature of these volume elements to determine the power of thermal noise for each volume element. Thus, we have obtained for 7 volume elements, a series of random numbers of 187 digits which conversion into binary represents the cryptographic key. Our analysis shows that it is not possible for an attacker to determine the generated sequence numbers for infinity of volume elements. In future work, we will propose a quantum cryptography mechanism to exchange the generated keystream and associate it the One-Time Pad cryptographic method.

Acknowledgements

The authors would like to thank the reviewers for their constructive comments. Many thanks to the Doctoral School of University of Burundi, IMSP-UAC of Benin and Antenne Afrique des Grands lacs de l'AUF-Burundi for their support.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Shor, P. (1994) Algorithm for Quantum Computation: Discrete Logarithms and Factoring. In: *Proc.* 35*th Annual Symposium on Foundations of Computer Science*,

IEEE Press, Santa Fe, New Mexico, USA, 124-134.

[2] Grover, L.K. (1996) Fast Quantum Mechanical Algorithm for Database Search. *STOC-96: Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, Philadelphia, Pennsylvania, USA, July 1996, 212-219. https://doi.org/10.1145/237814.237866

[3] Shor, P. (1997) Polynomial-Time Algorithms for Prime Factorization and Discret Logarithms on a Quantum Computer. *SIAM Journal on Computing*, **26**, 1484-1509. https://doi.org/10.1137/S0097539795293172

[4] Grassl, M., Langenberg, B., Roetteler, M. and Steinwandt, R. (2016) Applying Grover's Algorithm to AES: Quantum Resource Estimates. *Proceedings of the 7th International Conference on Post-Quantum Cryptography*, Vol. 9606, 29-43. https://doi.org/10.1007/978-3-319-29360-8_3

[5] Rao, S., Mahto, D., Yadav, D.K. and Khan, D.A. (2017) The AES-256 Cryptosystem Resists Quantum Attacks. *International Journal of Advanced Computer Research*, **8**, 404-408.

[6] Moody, D., Jordan, S.P., Chen, L. and Li, Y.-K. (2016) NIST Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal Report 8105, 15 p.

[7] Ohya, M. and Masuda, N. (2000) Np Problems in Quantum Algorithm. *Open Systems and Information Dynamics*, **7**, 33-39. https://doi.org/10.1023/A:1009651417615

[8] Furer, M. (2008) Solving NP-Complete Problems with Quantum Search. *Theoretical Informatics, 8th Latin American Symposium*, Buzios, 7-11 April 2008, 784-792. https://doi.org/10.1007/978-3-540-78773-0_67

[9] Fechner, B. and Osterloh, A. (2010) A Meta-Level True Random Number Generator. *International Journal of Critical Computer-Based Systems*, **1**, 267-279. https://doi.org/10.1504/IJCCBS.2010.031719

[10] Liu, S. (1990) On Fourier's Law of Heat Conduction. *Continuum Mechanics and Thermodynamics*, **2**, 301-305. https://doi.org/10.1007/BF01129123

[11] Stipcevic, M. and Koç, Ç.K. (2014) True Random Number Generators. In: Koç, Ç.K., Ed., *Open Problem in Mathematics and Computational Science*, Springer, Berlin, 275-315. https://doi.org/10.1007/978-3-319-10683-0_12

[12] Gong, L.S., Zhang, J.G., Liu, H.F., Sang, L.X. and Wang, Y.C. (2019) True Random Numbers Generators Using Electrical Noise. *IEEE Access*, **7**, 125796-125805. https://doi.org/10.1109/ACCESS.2019.2939027

[13] Wilber, S.A. (2005) True Random Number Generator and Entropy Calculation Device and Method. US 6,862,605B2.

[14] Yu, F., Li, L.X., Tang, Q., Quai, S., Song, Y. and Xu, Q. (2019) A Survey on True Random Number Generators Based on Chaos. *Discrete Dynamics in Nature and Society*, **2019**, Article ID: 2545123. https://doi.org/10.1155/2019/2545123

[15] Bagini, V. and Bucci, M. (1999) A Design of Reliable True Random Number Generator for Cryptographic Applications. *1st International Workshop on Cryptographic Hardware and Embedded Systems*, Worcester, 12-13 August 1999, 204-218. https://doi.org/10.1007/3-540-48059-5_18

[16] Walker, S. and Foo, S.Y. (2001) Evaluating Metastability in Electronic Circuits for Random Number Generation. *Proceedings IEEE Computer Society Workshop on VLSI*, Orlando, 19-20 April 2001, 99-101.

[17] Schurr, J., Moser, H., Pierz, K. and Ramm, G. (2011) Johnson-Nyquist Noise of the

Quantized Hall Resistance. *IEEE Transactions on Instrumentation and Measurement*, **60**, 2280-2285. https://doi.org/10.1109/TIM.2010.2088050

[18] Nyquist, H. (1928) Thermal Agitation of Electric Charge in Conductors. *Physical Review*, **32**, 110-113. https://doi.org/10.1103/PhysRev.32.110

[19] Shannon, C.E. (1948) A Mathematical Theory of Communication. *Bell System Technical Journal*, **27**, 379-423, and 623-656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x

[20] Maurer, U.M. (1992) A Universal Statistical Test for Random Bit Generators. *Journal of Cryptology*, **5**, 89-105. https://doi.org/10.1007/BF00193563

[21] Parisi, G. and Rapuano, F. (1985) Effects of the Random Number Generator on Computer Simulations. *Physic Letters B*, **157**, 301-302. https://doi.org/10.1016/0370-2693(85)90670-7

[22] Sunar, B., Martins, W.J. and Stinson, D.R. (2007) A Provable Secure True Random Number Generator with Build in Tolerance to Active Attacks. *IEEE Transaction on Computer*, **56**, 109-119. https://doi.org/10.1109/TC.2007.250627

[23] Shannon, C.E. (1979) Communication Theory of Secrecy Systems. *Bell System Technical Journal*, **28**, 656-715.

[24] Yamamoto, H. (1994) Coding Theorems for Shannon's Cipher System with Correlated Source Outputs and Common Information. *IEEE Transaction on Information Theory*, **40**, 85-95. https://doi.org/10.1109/18.272457

[25] Ametepe, A.F.-X., Ahouandjinou, S.A.R.M. and Ezin, E.C. (2019) Secure Encryption by Combining Asymmetric and Symmetric Cryptographic Method for Data Collection WSN in Smart Agriculture. *IEEE ISC2*, Casablanca, 14-17 October 2019, 93-99.