International Journal of Cryptology Research 8(1): 54 - 76 (2018)

Evaluation Criteria on Ambience-Based True Random Number Generators

Nur Azman Abu[*1], **Shekh Faisal Abdul Latip**[1], and **Shahrin Sahib**[1]

[1]*Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia*

E-mail: nura@utem.edu.my
[*]*Corresponding author*

ABSTRACT

There is a need nowadays to ensure information security which is independent of the security mechanism of physical medium. Cryptography still remains an important science in daily life, be it for sovereignty use or the privacy of individuals. Ultimately, the security of the interoperating open cryptosystem must reside only in the key being used. It must be true random key. It is a challenging task to generate a true random key live on demand suitable for cryptographic applications. This paper shall formally propose an evaluation criteria on a true random number generator (TRNG). An evaluation has been done on various TRNG for cryptographic keys. This paper will also classify recent TRNGs into several groups. A new true random generator has been developed based on the air ambience for cryptographic application and evaluated against other TRNGs under the proposed evaluation criteria.

Keywords: True Random Numbers, Random Cryptographic Keys, Evaluation Criteria of Random Numbers

1 INTRODUCTION

In a modern cryptographic design, a chosen algorithm must provide a high level of security, completely specified in a clear easy manner for cryptographic community to understand, analyze and validate. The security of a cryptosystem should not depend on the secrecy of the algorithms nor apparatus being used. They shall be made public and available to all users.

For the purposes of interoperability, they must be efficient, exportable, economically implementable in electronic devices and adaptable for use in diverse future applications. The security of modern cryptosystem should be no longer based on the secrecy of the algorithm but rather on the secrecy of the key being used. However to maintain the secrecy of the key, one of several aspects that should be considered is that, the generation of the key should be indistinguishable from truly random sequence. Most of the cryptographic operations nowadays mandate a fresh random key as an input. Should the key generation processes not truly random, the cipher may be vulnerable to cryptanalysis such as related-key attacks (Biham, 1994), where the cipher can be analysed under several different unknown keys in which the mathematical relationship connecting the keys is known to the cryptanalyst. This is one of the reasons which explain why the use of true random number generator (TRNG) is critical in modern cryptography. However to generate a truly random number from a TRNG is very costly and time consuming. Thus in this paper we propose evaluation criteria for TRNG that may help to generate true random cryptographic keys efficiently and a new TRNG which has been developed and evaluated based on the proposed evaluation criteria.

The organization of this paper is as follows. In Section 2, we review several types of TRNG available in literature. Section 3, 4 and 5 contains the main contribution of this paper, where we provide a set of evaluation criteria, classification of TRNGs and a new TRNG called TERANG based on air ambience evaluated under the proposed evaluation criteria has been proposed. Section 6 discusses our work. Finally in Section 7 we conclude the paper.

2 TRUE RANDOM NUMBER GENERATORS

This section shall give an overview on several various types of true random number generators. Entropy is often used as a measure of the unpredictability of a cryptographic key. Most TRNGs make use of a natural phenomenon as an entropy source to produce random bits. They come in many types, ranging from Johnson noise in the case of Petrie and Connelly (2000) and ring oscillators by Sunar et. al. (2007) to a key generation scheme exploiting randomness of hyperchaos (Teh and et. al., 2016) and road surface plus driving behavior (Uz-Zaman et. al., 2017). Each TRNG captures and measures unpredictable natural processes by using a dedicated hardware device. The measurement usually follows certain principle of physics.

2.1 TRNGs around the Globe

There are various cryptographic research groups concentrating on TRNG around the globe. They have recently managed to produce their own random number generators. The selected research groups under review are listed in Table 1.

As the realm of cryptography has embarked on an open system, a cryptosystem will require a freshly minted key for each cryptographic operation. An entropy of a random variable is a mathematical measure (Barker and Roginsky, 2012). Recent research on cryptographic key generation based on physical biometrics is a popular topic(Dinca and Hancke, 2017). However, a key generator with a low entropy, such as using a fuzzy logic (Koeberl and et. al., 2014) and deterministic pilot signals from random fading gains (Fritschek and Wunder, 2017), is out of scope of this research project. Based on the literature survey on recent TRNGs above, every developer and country should have their own TRNG as the source of a secure random cryptographic key.

ID	Recent TRNG	Institution	City/State/Country
1	Sunar *et. al.* (2007)	Worcester Polytechnic Institute	Worcester, Massachusetts
2	Stipcević and Rogina (2007)	Rudjer Bosković Institute	Zagreb, Croatia
3	Drutarovský and Galajda (2007)	Technical University of Košice	Slovak Republic
4	Tokunaga *et. al.* (2008)	University of Michigan	Ann Arbor, Michigan
5	Dynes *et. al.* (2008)	Cambridge Research Laboratory	Cambridge, United Kingdom
6	Ahmed and Naganathan (2008)	VLB Engineering College	Coimbatore, India
7	Ergün and Özoguz (2008)	Istanbul Technical University	Istanbul, Turkey
8	Thamrin *et. al.* (2008)	MIMOS	Malaysia
9	Blaszczyk and Guinee (2008)	Cork Institute of Technology	Bishopstown, Ireland
10	Wayne *et. al.* (2009)	University of Illinois	Urbana-Champaign, Illinois
11	Holcomb *et. al.* (2009)	University of Massachusetts	Amherst, Massachusetts
12	Kwon *et. al.* (2009)	Pohang University of Science and Technology	Pohang, South Korea
13	Danger *et. al.* (2009)	Telecom ParisTech	Paris, France
14	Wei and Guo (2009)	Peking University	Beijing, China
15	Bardis *et. al.* (2009)	University of Military Education	Vari, Greece
16	Hars (2009)	Seagate Technology	Longmont, Colorado
17	Hirano *et. al.* (2010)	Takushoku University	Tokyo, Japan
18	Pironio *et. al.* (2010)	Université Libre de Bruxelles	Bruxelles, Belgium,
19	Fürst *et. al.* (2010)	Ludwig-Maximilians Universität	München, Germany
20	Fechner and Osterloh (2010)	University of Hagen	Hagen, Germany
21	Argyris (2010)	University of Athens,	Panepistimiopolis, Ilisia, Greece
22	Abu and Sahib (2010)	Universiti Teknikal Malaysia Melaka (UTeM)	Melaka, Malaysia

Table 1: The institution, city, state or country of origin from TRNG's research group.

2.2 Special Devices of TRNG

Unlike the PRNG, a physical hardware random number generator has a greater advantage, since it can produce completely unpredictable and un-reproducible random sequences. Most of the true random number generators recently are designed based on special hardware devices such as a quantum detector device, an electronic flip-flop circuit and a chaos oscillator digital circuit. For instances, a quantum detector devices has been used by Stipcevi and Rogina (2007), Dynes et. al. (2008), Kwon et. al. (2009) and Frst et. al. (2010). An electronic flip-flop has been used by Sunar et. al. (2007), Thamrin et. al. (2008) and Fechner and Osterloh (2010). A chaos oscillator has been used by Ergn and zoguz (2008), Blaszczyk and Guinee (2008) and Danger et. al. (2009).

A literature survey has been done on the special hardware requirement in TRNGs. They are based on certain theoretical principles and special hardware to capture their source of randomness. In this research project, a systematic comparison on TRNGs has been hardly found. Some authors also have pointed out that to the best of their knowledge, no effective comparison of several TRNGs appears in the literature (Santoro et. al., 2009). Most research groups have proposed their techniques and reported their performances in terms of passing a random statistical test suite and output bitrates only. In order to achieve a viable TRNG, it should satisfy certain modern criteria as a competitive random cryptographic generator.

3 MODERN CRITERIA ON RANDOM CRYPTOGRAPHIC KEY GENERATION AND APPARATUS

In this paper, the authors shall propose a set of evaluation criteria to rate a TRNG according to Table 2. In general, the TRNG should only use minimum hardware and utilize only few basic computer algorithms. The users and owners of a cryptosystem are mostly nontechnical. It is important to have a generation process and apparatus which are physical, economics, convenient, efficient to use and secure. The measuring device should work automatically on demand from user's physical environment.

Index	Criterion
1	Minimum Hardware
2	Minimum Formula
3	Basic Algorithm
4	Efficiency
5	Economics
6	Mobility

Table 2: Modern Evaluation Criteria on TRNG for cryptographic keys.

The last criterion shall be referred to as mobility of the TRNG. This is the most critical criterion in this research project. It will determine whether the TRNG can and shall be used in generating the cryptographic key in each crypto operation independent of the developer preset RNG. It is common for the developer to use pseudo RNG instead of true RNG. In summary, this research project shall consider the six criteria listed in Table 2 to evaluate each TRNG. These criteria are critical factors in practical usage of embedding the TRNG in current modern cryptosystem.

Symbol	1.🟡	2.◐	3.◐	4.◐	5.🟢
Quality	Poor	Satisfactory	Good	Very Good	Outstanding

Table 3: Legend symbols for proxy qualitative variable for TRNG evaluation.

The symbolic scores shall be given according to the legend symbols which get the quantitative values from 1 to 5 as shown in Table 3. In the end, a proxy random variable will take an average qualitative score on each TRNG according to the modern criteria above. Every criterion shall be utilised to evaluate the chosen TRNG for cryptographic keys based on basic evaluation rules as prescribed in the following subsections. The objective of these criteria is partly to distinguish a practical TRNG from pseudo RNG for cryptographic keys.

3.1 Evaluation Rule on Minimum Hardware

The use of additional hardware in a TRNG shall be evaluated in this subsection according to the complexity and technology in use. The laser source quantum device in general shall been given qualitative score 1 or symbolic score 🟡 since it takes more complex hardware to control the environment during the random number generating process. Any TRNG using semi-conductor laser shall be given qualitative score 2 or symbolic score ◐ on minimum hardware requirement. The LED source QTRNG has been given qualitative score 2 or symbolic score ◐. Whereas since an oscillator are suitable for high-frequency and high-performance integrated circuit, such TRNG shall be given qualitative score 3 or symbolic score ◐ on minimum hardware requirement. Similarly, chaos system can be embedded as microcontroller, this TRNG system should be given a relatively balanced qualitative score 3 or symbolic score ◐. Any system which uses common computer component with certain requirement of specific brand or model shall be given almost full qualitative score 4 or symbolic score ◐ on minimum hardware requirement. Lastly, a TRNG utilising a common standard peripheral or computer component shall be given full qualitative score 5 or symbolic score 🟢 on this criterion.

3.2 Evaluation Rule on Minimum Formula

A practical TRNG should be distinct from pseudo RNG for cryptographic keys which uses heavy mathematical formula to generate the random output. In general the minimum formula refers to the mathematical formula being used in capturing the candidate bits from the random source. The more complex mathematical formula being used shall be given the lower qualitative score.

For instance, Stipcević and Rogina (2007) basic idea of the method for extracting random bits is to consider a pair of non overlapping random time intervals. However, the time interval between subsequent random pulses is measured by counting periodic pulses from a continuous non-restartable quartz-controlled clock. Nevertheless, the statistics of time intervals between emission of subsequent photoelectrons is governed by convolution of exponential and differential binomial distributions. The probability density function (pdf) of measured time intervals between subsequent pulses has to be measured by the fast digital oscilloscope. Since the whole bit extraction process has been embedded in logic circuitry, this TRNG shall be given qualitative score 2 or symbolic score ◐ instead of 1. Similarly, Tokunaga et. al. (2008) makes use of statistical analysis in order to tune the system into metastability. A simpler mathematical formulas being utilized such as mapping equations by Drutarovský and Galajda (2007) shall be given the medium qualitative score 3 or symbolic score ◑.

In another instance, Sunar *et. al.* (2007) design uses jitter (or random vibration) in clock signals present in all digital clocked circuits as the random source. They harvest the jitter by sampling an output of coupled oscillators. The output of the XOR combines periodic transition zones contributed by each oscillator ring. Since the method uses more than a simple XOR and digital sampling, this TRNG has been given almost full qualitative score 4 or symbolic score ◑. In an ideal instance, Dynes *et. al.* (2008) captures the output bit by recording the time tagged count events. The time tagged events acquired were converted into random bits by assigning detection events in even clock cycles as a “1” and “0” for detection events in odd clock cycles. A direct capture of random output bit such as this TRNG shall be given full qualitative score 5 or symbolic score 🟢 on this criterion.

3.3 Evaluation Rule on Basic Algorithm

This evaluation rule on basic algorithm specifically pays attention to the computer algorithm in the generating process of random key. Special attention is given to the post-processing of the random bits being captured. Even though hashing algorithm is well known to secure the random number and make it irreversible, in this research project, the evaluation rule shall give it the lowest qualitative score 1 or symbolic score 🟡. A TRNG should stand on its own without relying on such a hashing algorithm. However, few TRNG uses some complex electronic algorithm without hashing function has been given a qualitative score 2 or symbolic score ◐ such as Tokunaga *et. al.* (2008). Similarly, Bardis *et. al.* (2009) utilises normalization transformation to create the packet of the uniformly distributed random variables.

A TRNG which uses the von Neumann method, in general shall be given the qualitative score 3 or symbolic score 🔵. A TRNG which uses the XOR corrector, in general, shall be given the qualitative score 4 or symbolic score ◐. An unbiased TRNG shall be given full qualitative score 5 or symbolic score 🟢 on this criterion such as Dynes *et. al.* (2008) without a need of any post-processing algorithm.

3.4 Evaluation Rule on Efficiency

Efficiency here specifically refers to the speed or potential capacity of TRNG. A qualitative score shall be based on the random output bit-rate such as few hundred bits per second, kilobits per second, few hundred kilobits per second, several megabits per second and in terms of gigabits per second and beyond. A TRNG which produces 500 random bits per second or less shall be given the lowest qualitative score 1 or symbolic score 🟡. Next, a TRNG which is capable of producing few thousand bits per second less than 50 Kbps shall be given the qualitative score 2 or symbolic score ◑. Third, a TRNG which has random output bitrate between 50 Kbps and 500 Kbps shall be given the medium qualitative score 3 or symbolic score 🔵. Fourth, a TRNG which has random output bitrate few megabits per second between 500 Kbps and 500 Mbps shall be given the almost full qualitative score 4 or symbolic score ◐.

Lastly, a TRNG which has random output bitrate in terms few gigabits per second specifically higher than 500 Mbps shall be given the full qualitative score 5 or symbolic score 🟢 on this criterion. Even though (Wei and Guo, 2009) has reported the process and apparatus to generate random keys at the rate of 500 Kbps, they have also shown a clear technique and modus operand on how to generate the random key in terms of gigabits per second. Thus, they are given the full qualitative score 5 or symbolic score 🟢 on this criterion.

3.5 Evaluation Rule on Economics

The economic issue here refers to the cost or relative price of certain TRNG. The cost includes the cost deployment of a TRNG as a cryptographic key generator for nontechnical user applications. For instance, in Dynes *et. al.* (2008), the avalanche photodiode (APD) is held at a temperature of -30^{o}C. This requirement is certainly very costly for deployment in general cryptographic environment. In general, the quantum TRNG shall be given qualitative score 1 or symbolic score 🟡. Simpler setup on the quantum TRNG shall be given a qualitative score 2 or symbolic score ◐.

A quantum photonic TRNG comprises an optical system and extremely compact circuitry which can be implemented on any advance crypto hardware devices. For instance, Argyris (2010) make use of a photonic integrated circuit as its bit extraction controller. A photonic TRNG are mostly given a qualitative score 3 or symbolic score 🔵 on economic criterion. Even better, an oscillator TRNG is suitable for high-frequency and high-performance integrated circuit. An oscillator TRNG without any requirement of specific hardware brand or model shall be given almost full qualitative score 4 or symbolic score ◑.

Lastly, a simple TRNG without any special circuit which makes use of only common computer component shall be given full qualitative score 5 or symbolic score 🟢 on this criterion. It is a popular idea to generate the random bit based on nature collected using the common computer peripherals. These types of TRNGs shall be discussed in the second half of the next section.

3.6 Evaluation Rule on Mobility

A score on mobility of any TRNG shall be evaluated here according to its size and portability. The laser source quantum device in general shall been given qualitative score 1 or symbolic score 🟡 since it takes more complex hardware to control the environment during the random number generating process. Any TRNG using semi-conductor laser shall be given qualitative score 2 or symbolic score ◐ on minimum hardware requirement. The LED source QTRNG has been given qualitative score 2 or symbolic score ◐.

Chaos system, however, can be embedded as microcontroller. So, this TRNG system should be given a relatively balanced qualitative score 3 or symbolic score 🔵. Since an oscillator are suitable for high-frequency and high-performance integrated circuit, they TRNGs are mostly given qualitative score

3 or 4 on mobility criterion. Similarly, any system which uses common computer component with certain requirement of specific brand or model shall be given almost full qualitative score 4 or symbolic score ◐ on mobility criterion since it is not ever ready to generate a random cryptographic key generation live on demand. Lastly, a TRNG utilising a common standard peripheral or computer component shall be given full qualitative score 5 or symbolic score 🟢 on this criterion.

4 CLASSIFICATION OF RECENT TRNGS

A TRNG shall always be an important primitive in a cryptosystem. This literature review shall be miniturized by classifying recent TRNGs into several groups. The security of every cryptographic operation primarily relies on the unpredictability of the random key being used. The source of randomness in every TRNG is the real world phenomenon. Some kind physical hardware device is needed to detect and record a continuous event. This section shall pay a particular attention to the minimum hardware and mobility criteria on classifying recent TRNGs under review.

4.1 Quantum TRNG

A quantum TRNG relies upon a physical process, extracting randomness from the inherent uncertainty in quantum mechanics. Notably, it relies on a photon detector as its special apparatus. It also requires another hardware as a source of light. There are 2 main sources of lights. First, it is using a light emitting diode (LED) such as in Stipcević and Rogina (2007), Wayne *et. al.* (2009) and Fürst *et. al.* (2010). Second, it is using a laser diode such as in Dynes *et. al.* (2008), Kwon *et. al.* (2009), Wei and Guo (2009) and Pironio *et. al.* (2010).

At the same time, it requires another set of tools to control the light source and the environment of the random bit generating process. Stipcević and Rogina (2007) makes use of a photo-multiplier with photocathode. Wayne *et. al.* (2009) utilises an optical laser diode attenuator. Fürst *et. al.* (2010) uses a photomultiplier tube. Whereas Dynes *et. al.* (2008) uses an avalanche photodiode (APD). Kwon *et. al.* (2009) requires a pair of interference filters, a fiber beam splitter and polarization controllers. Wei and Guo (2009) uses a flexible attenuator and an avalanche photodiode. Pironio *et. al.* (2010) requires a pair of independent vacuum chambers placed in the magnetic field and photomultiplier tubes.

The LED source QTRNG has been given qualitative score 2 or symbolic score ◑. Whereas the laser source QTRNG has been given qualitative score 1 or symbolic score 🟡 since it takes more hardware to control the environment during the random number generating process.

4.2 Photonic TRNG

A quantum photonic TRNG relies on a photo detector/receiver as its special apparatus. The design comprises an optical system and extremely compact and digitally random bit extraction circuitry which can be implemented on any advance crypto hardware devices.

Thamrin *et. al.* (2008) use T-shape optical system and a bit extraction controller. The optical setup consists of an optical source, attenuators, a half-wave plate, a polarize beam splitter and two detectors. The bit extraction microcontroller consists of D flip-flop circuit. Argyris (2010) uses a photonic integrated circuit, a photo receiver/detector and a real-time oscilloscope as part of bit extraction controller.

Hirano *et. al.* (2010) have constructed by far a complex setup to reach high random output. They uses two distributed-feedback (DFB) semi-conductor lasers, a temperature controller, a fiber coupler, a variable fiber reflector, polarization maintaining fibers and AC photo detectors. The readings go through electronic amplifiers and a digital oscilloscope a radio-frequency (RF) spectrum analyzer. For this reason Photonic RNG has been typically given qualitative score 2 or symbolic score ◑ on minimum hardware requirement.

4.3 Oscillator TRNG

Oscillators provide a simple and effective method to build TRNGs. They are suitable for high-frequency and high-performance integrated circuit. Typically, an oscillator TRNG is build upon chaotic system.

Sunar *et. al.* (2007) have made use of oscillator rings, XOR gates and a D flip-flop sampler. This particular Oscillator TRNG is based on sampling phase jitter in oscillator rings or random vibration in clock signals present in a typical digital clock circuit. Ergün and Özoguz (2008) use a continuous-time chaotic oscillators, a voltage-controlled oscillator (VCO) and CMOS transistor arrays. Blaszczyk and Guinee (2008) use a double-scroll attractor from a chaotic oscillator based on Chua's circuit for a nonlinear operation leading to its chaotic behaviour. The circuit has been modified to obtain TRNG's performance using a simple temperature dependent control resistor in the oscillator circuit and optimal voltage threshold settings. To achieve optimal voltage, three current feedback operational amplifiers are used along with a voltage comparator. Danger *et. al.* (2009) have presented a new method to build a very high speed TRNG based on an open loop structure. This principle can be implemented in an FPGA. They also need to use an external adjustable potentiometer RC delay and a Peltier sensor.

Since Oscillator TRNGs are suitable for high-frequency and high-performance integrated circuit, they are mostly given qualitative score 3 or symbolic score ◐ on minimum hardware requirement. For the same reason, they are mostly given a qualitative score 4 or symbolic score ◐ on mobility.

4.4 Chaos TRNG

Drutarovský and Galajda (2007) has proposed a new robust chaos-based TRNG embedded in a true PSoC integrating configurable analog and digital peripheral functions, memory and a microcontroller on a single chip. The system requires a powerful Harvard CPU architecture. A the same time , the system uses advanced peripherals, namely, four rail-to-rail continuous analog PSoC blocks, eight Switched Capacitor (SC) analog blocks, eight digital PSoC blocks and a mixed-signal PSoC hardware which includes also an embedded microcontroller. Even though chaos system is popular within the cryptosystem, this system is given a relatively balanced qualitative score 3 or symbolic score ◑ on minimum hardware requirement and mobility.

4.5 User Interaction TRNG

Ahmed and Naganathan (2008) have proposed a user interaction model consisting of the time-stamp of mouse movements, character input pressed on the keyboard, hard disk reading time and operating system states. This interaction system is certainly an ideal TRNG for this research project in term of cryptographic key generation live on demand at the user physical location. This system has been given full qualitative score 5 or symbolic score 🟢 on minimum hardware requirement, economically and mobility. Unfortunately, it is not efficient and relies strongly on the hashing algorithm being used.

4.6 CMOS TRNG

Tokunaga *et. al.* (2008) have proposed a meta-stable system to generate individual bits that result from the effect of thermal noise. The system also comes with meta-stable latch, completion detector and a time-to-digital converter (TDC) and fabricated chips on 8-metal-layer bulk CMOS. The dynamic control module that tunes the latch into the meta-stable region responds to both process and temperature variations, as well as external noise sources.Holcomb *et. al.* (2009) use a 64-bit SRAM logical device consists of cross-coupled CMOS inverters and access transistors. The system generates random numbers from the power-up of SRAM and existing volatile CMOS memory without requiring any dedicated circuitry. The system relies on the large number of cells to ensure that some cells will be influenced by noise when the chip is powered-up. The primary limitation of this TRNG is that entropy is only generated during power-up which makes it unpractical for random cryptographic key generation to be done live on demand.

Since both systems use common computer component, they are given almost full qualitative score 4 or symbolic score ◐ on minimum hardware requirement. Holcomb *et. al.* (2009) should get a slightly lower score on mobility criterion since it is not ever ready to generate random cryptographic key generation live on demand.

4.7 Disk Drive TRNG

Hars (2009) specifically uses a Seagate Momentus FDE disk drive and a diagnostic interface between the main control ASIC and the channel signal processor to access the coefficients of an adaptive channel-filter. Since a disk drive is considered as a common computer component, this system is given almost full qualitative score 4 or symbolic score ◐ on minimum hardware requirement. A full score may be given if the system may utilise any standard disk drive without referring to any specific brand or model. Nevertheless, the system is given full qualitative score 5 or symbolic score ● on mobility.

4.8 SRAM TRNG

Although SRAM has been used in earlier TRNGs such as in Holcomb *et. al.* (2009), it has not been used as the main hardware or the principle source of random extraction. Fechner and Osterloh (2010) use a six-transistor SRAM in 26 nm process technology and meta-stable flip-flops. Since SRAM is considered as common computer component, this system is given almost full qualitative score 4 or symbolic score ◐ on minimum hardware requirement.

4.9 Ambience TRNG

Bardis *et. al.* (2009) proposal use a basic peripheral of a personal computer, namely, a microphone. This device is a standard part of modern personal computers, laptop computers, PDAs and of course mobile phones. Bardis *et. al.* (2009) have investigated several environmental sounds captured under four different scenarios *id est* single person speaking in an office environment, almost silent office noise, cocktail party noise and mixed noise (office noise, multimedia sounds and human conversations).

Since microphone is just a common computing device, this system is given full qualitative score 5 or symbolic score 🟢 on minimum hardware requirement and mobility criteria. On the practical application of the idea, this research project shall follow and broaden this strategy in moving forward.

5 TRUE ENVIRONMENTAL RANDOM AMBIENCE NUMBER GENERATOR

In this research project, a true environmental random ambience number generator (TERANG) has been proposed. TERANG utilises only a common standard peripheral or computer component such as web camera (Abu and Sahib, 2011) and regular microphone (Abu and Sahib, 2010a). On the case of one-megabit random number generation, it uses high fidelity digital camera which can be purchased over the shelves (Abu and Sahib, 2010b). TERANG shall be given full qualitative score 5 or symbolic score 🟢 on the first criterion, Minimum Hardware requirement. The random output bit has been captured directly from an image pixel or an audio signal. TERANG uses only basic minimum formula to do the direct capture of random output bit. TERANG shall be given full qualitative score 5 or symbolic score 🟢 on the second criterion, Minimum Formula being used prior to post-processing.

For the post-processing stage, however, TERANG uses the XOR operation among output bit being captured in the colour digital image. It shall be given the qualitative score 4 or symbolic score ◐ on the third criterion, Basic Algorithm. In the case of the fourth criterion, Efficiency here specifically refers to the speed or potential capacity of TRNG. TERANG's the random output bit-rate in the current form is categorised and fall within several megabits per second. It shall be given the qualitative score 4 or symbolic score ◐.

Random ambience follows the basic principle to generate the random bit from natural phenomena collected using the common computer peripherals. They carry minimum cost and widely available without any special circuit to operate on. TERANG shall be given full qualitative score 5 or symbolic score 🟢 on the fifth criterion, Economics. At the same time, utilising a common standard peripheral or computer component, they are ready to be deployed anywhere and certainly very mobile. TERANG shall be given full qualitative score 5 or symbolic score 🟢 on this last criterion, Mobility.

Following the proxy qualitative variable on the evaluation criteria, every TRNG has been evaluated and ranked in ascending order by their average scores as shown in the Table 4. TERANG has achieved the highest score compared to the rest.

0	Min Hardware	Min Formula	Basic Algorithm	Efficiency	Economic	Mobility	Average
18	1.🟡	3.◐	4.◐	2.◐	1.🟡	1.🟡	2.00
12	1.🟡	3.◐	3.◐	3.◐	1.🟡	2.◐	2.17
10	2.◐	3.◐	1.🟡	4.◐	2.◐	2.◐	2.33
2	2.◐	2.◐	5.🟢	4.◐	2.◐	2.◐	2.83
5	1.🟡	5.🟢	5.🟢	4.◐	1.🟡	1.🟡	2.83
14	1.🟡	3.◐	3.◐	5.🟢	1.🟡	4.◐	2.83
9	3.◐	3.◐	3.◐	2.◐	4.◐	3.◐	3.00
4	3.◐	2.◐	2.◐	4.◐	5.🟢	3.◐	3.17
8	2.◐	3.◐	4.◐	5.🟢	3.◐	2.◐	3.17
3	3.◐	3.◐	4.◐	3.◐	4.◐	3.◐	3.33
16	4.◐	3.◐	1.🟡	2.◐	5.🟢	5.🟢	3.33
17	2.◐	4.◐	4.◐	5.🟢	3.◐	2.◐	3.33
19	2.◐	3.◐	5.🟢	4.◐	2.◐	4.◐	3.33
20	4.◐	3.◐	3.◐	2.◐	5.🟢	3.◐	3.33
13	3.◐	3.◐	3.◐	4.◐	4.◐	4.◐	3.50

1	3.🔵	4.◐	3.🔵	4.◐	4.◐	4.◐	3.67
6	5.🟢	5.🟢	1.🟡	1.🟡	5.🟢	5.🟢	3.67
7	3.🔵	3.🔵	3.🔵	5.🟢	4.◐	4.◐	3.67
11	4.◐	4.◐	4.◐	2.◑	5.🟢	3.🔵	3.67
15	5.🟢	3.🔵	2.◑	2.◑	5.🟢	5.🟢	3.67
21	2.◑	4.◐	5.🟢	5.🟢	3.🔵	4.◐	3.83
22	5.🟢	5.🟢	4.◐	4.◐	5.🟢	5.🟢	4.67

Table 4: Evaluation scores of the random ambience as a source of randomness among the recent TRNGs for cryptographic keys.

This concept of random ambience is certainly by far the most practical, convenient and robust TRNG suitable for cryptographic applications. The proposed TRNG method in this project is not only capable of generating random cryptographic keys efficiently but also tested in real time live on demand.

6 DISCUSSION

A secure communication is meant to be used by many users. For a large number of applications, especially for those intended for use on mobile devices, the use of dedicated, specialized hardware for RNG is not feasible, due to the cost, volume and power consumption limitations. A large number of applications may significantly benefit by the availability of independent random number inputs. Therefore, development of an innovative and efficient TRNG is an urgent prerequisite for current information security system.

In this research project, however, the true random number generator does not depend on a special device. This research project shall make use of already available devices on the shelf or common peripherals. It is the environment which becomes the source of randomness. Even the vacuum was once thought to be just an empty dark silent space. In fact, vacuum is an extent of space that has virtual sub-atomic particles spontaneously appearing and disappearing. It is the presence of these virtual particles that give rise to random noise. This ’vacuum noise’ is omnipresent and may be exploited and used to generate random numbers (Symul *et. al.*, 2011).

7 CONCLUSION

True random key generator is the most crucial components of modern cryptosystem. For cryptographic use, however, it is important that the numbers used to generate any cryptographic keys are not just seemingly random; they must be truly unpredictable. In fact, each operation in cryptography requires a new fresh random key. A set of evaluation criteria of modern TRNG for cryptographic keys has been proposed in this paper. In this research project, a true environmental random ambience number generator has been developed upon which the recent TRNGs have been evaluated against. Air ambience is the natural choice here. A TRNG based on air ambience has a strong potential to perform well according to the quantitative evaluation criteria proposed in this paper.

8 ACKNOWLEDGMENT

The authors would like to express sincere appreciation to Universiti Teknikal Malaysia Melaka and Fundamental Research Grant Scheme FRGS/1/2015/ ICT05/FTMK/02/F00293 funded by the Ministry of Higher Education, Malaysia for giving full technical and financial supports in this research.

REFERENCES

Abu, N.A. and Sahib, S. (2010a). *Random Ambience Key Generation Live on Demand*, 2nd IEEE International Conference on Signal Processing Systems, Vol. 1, pp. 110-114. 5-7 July 2010, Dalian.

Abu, N.A. and Sahib, S. (2010b). *One Megabit Random Ambience*, International Journal of Cryptology Research, Vol. 2, No. 1, pp. 073-087.

Abu, N.A. and Sahib, S. (2011). *Random Ambience Using High Fidelity Images*, 3^{rd} International Conference on Digital Image Processing, 15-17 April 2011, Proc. of SPIE (International Society for Optical Engineering), Volume 8009, 80092H, Chengdu.

Ahmed, M. S. I. and Naganathan, E. R. (2008). *A Secured Key Generation Scheme Using Enhanced Entropy*, International Journal of Computer Science and Network Security, Vol. 8, No. 2, pp. 236-240, February 2008.

Argyris, A., Deligiannidis, S., Pikasis, E., Bogris, A. and Syvridis, D. (2010). *Implementation of 140 Gb/S True Random Bit Generator based on A Chaotic Photonic Integrated Circuit*, Optics Express, Vol. 18, Issue 18, pp. 18763-18768, 18 August 2010.

Bardis, N. G., Markovskyi, A. P., Doukas, N. and Karadimas, N. V. (2009). *True Random Number Generation based on Environmental Noise Measurements for Military Applications*, Proceedings of the 8^{th} WSEAS International Conference On Signal Processing, Robotics and Automation, 21-23 February 2009, pp. 68-73, Cambridge.

Barker, E. and Roginsky A.(2012). Recommendation for Cryptographic Key Generation, NIST Special Publication 800-133, December 2012.

Biham, E. (1994). *New Type of Cryptanalytic Attacks Using Related Keys*, Journal of Cryptology, Vol. 7, No. 4, pp. 229-246, December 1994.

Blaszczyk, M. and Guinee, R. A. (2008). *A True Random Binary Sequence Generator based on Chaotic Circuit*, Signals and Systems Conference, 18-19 June 2008, pp. 294 – 299, Galway.

Danger, J. L., Guilley, S. and Hoogvorst, P. (2009). *High Speed True Random Number Generator based on Open Loop Structures in FPGAs*, Microelectronics Journal, Vol. 40, No. 11, November 2009, pp. 1650-1656.

Dinca, L. M. and Hancke, G.(2017). User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks, Special Issue on

Entropy-Based Applied Cryptography and Enhanced Security for Ubiquitous Computing, Vol. 19, pp. 70-91, 21 February 2017.

Drutarovský, M. and Galajda, P. (2007). *A Robust Chaos-Based True Random Number Generator Embedded in Reconfigurable Switched-Capacitor Hardware*, Radio Engineering, Vol. 16, No. 3, pp. 120-127, September 2007.

Dynes, J. F., Yuan, Z. L., Sharpe, A. W. and Shields, A. J. (2008). *A High Speed, Post-processing Free, Quantum Random Number Generator*, Applied Physics Letters, Vol. 93, No. 3, Article ID. 031109(3 pages), 25 July 2008.

Ergün, S. and Özoguz, S. (2008). *Truly Random Number Generators Based On Non-Autonomous Continuous-Time Chaos*, International Journal of Circuit Theory and Applications, Vol. 38, No. 1, 31 July 2008, pp. 1–24.

Fechner, B. and Osterloh, A. (2010). *A Meta-Level True Random Number Generator*, International Journal of Critical Computer-Based Systems, Vol. 1, No. 1-3, 2010, pp. 267-279.

Fritschek R. and Wunder, G.(2017). On-the-Fly Secure Key Generation with Deterministic Models, IEEE International Conference on Communications (ICC), 21-25 May 2017, Paris, pp. 1-6.

Fürst, M., Weier, H., Nauerth, S., Marangon, D. G., Kurtsiefer, C. and Weinfurter, H. (2010). *High Speed Optical Quantum Random Number Generation*, Optics Express, Vol. 18, No. 12, pp. 13029-13037, 2 June 2010.

Hars, L. (2009). *Random Number Generators in Secure Disk Drives*, EURASIP Journal on Embedded Systems, Vol. 2009, Article ID 598246(10 pages), 9 June 2009.

Hirano, K., Yamazaki, T., Morikatsu, S., Okumura, H., Aida, H., Uchida, A., Yoshimori, S., Yoshimura, K., Harayama, T. and Davis, P. (2010). *Fast Random Bit Generation with Bandwidth-Enhanced Chaos in Semiconductor Lasers*, Optics Express, Vol. 18, No. 6, pp. 5512-5524, 15 March 2010.

Holcomb, D. E., Burleson, W. P. and Fu, K. (2009). *Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers*, IEEE Transactions on Computers, Vol. 58, No. 9, September 2009, pp. 1198-1210.

Koeberl, P., Li, J., Rajan A. and Wu W.(2014). Entropy loss in PUF-based key generation schemes: The repetition code pitfall, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 6-7 May 2014, Arlington, pp. 44-49.

Kwon, O., Cho, Y. W. and Kim, Y. H. (2009). *Quantum Random Number Generator Using Photon-Number Path Entanglement*, Applied Optics, Vol. 48, No. 9, pp. 1774-1778, 19 March 2009.

Petrie, C. and Connelly, J. (2000). *A Noise-Based IC Random Number Generator for Applications in Cryptography*, IEEE Transaction on Circuits Syst. I: Fundamental Theory and Applications, Vol. 47, pp. 615–621.

Pironio, S., Acín, A., Massar, S., de la Giroday, A. B., Matsukevich, D. N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T. A. and Monroe, C. (2010). *Random Numbers Certified by Bell's Theorem*, Nature, Vol. 464, pp. 1021-1024, 15 April 2010.

Santoro, R., Sentieys, O. and Roy, S. (2009). *On-the-Fly Evaluation of FPGA-Based True Random Number Generator*, Proceedings IEEE Computer Society Annual Symposium on VLSI ISVLS 2009, pp. 055-060.

Stipcević, M. and Rogina, B. M. (2007). *Quantum Random Number Generator based on Photonic Emission in Semiconductors*, Review of Scientific Instruments, 9 April 2007, Vol. 78 No. 4, 045104, pp. 001-007.

Sunar, B., Martin, W. J. and Stinson, D. R. (2007). *A Provable Secure True Random Number Generator with Build-In Tolerance to Active Attacks*, IEEE Transactions on Computers, Vol. 56, No. 1, January 2007, pp. 109-119.

Symul, T., Assad, S. M. and Lam P. K. (2011). *Real Time Demonstration of High Bitrate Quantum Random Number Generation with Coherent Laser Light*, Applied Physics Letters: Lasers, Optics and Optoelectronics, Vol. 98, No. 23, 17 May 2011.

Teh, J. S., Teng, W. J. and Azman Samsudin, A. (2016) A True Random Number Generator based on Hyperchaos and Digital Sound, 3rd International Conference on Computer and Information Sciences, pp. 246-269, 15-17 August 2016, Kuala Lumpur.

Thamrin, N. M., Witjaksono, G., Nuruddin, A. and Abdullah, M.S., (2008). *A Photonic-based Random Number Generator for Cryptographic Application*, 9^{th} ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 6-8 August 2008, pp. 356-361.

Tokunaga, C., Blaauw, D. and Mudge, T. (2008). *True Random Number Generator with a Metastability-Based Quality Control*, IEEE Journal of Solid-State Circuits, Vol. 43, No. 1, January 2008, pp. 078-085.

Uz-Zaman, I., Lopez, A. B., Al Faruque, M. A. and Boyraz, O.(2017). *A Physical Layer Security Key Generation Technique for Inter-Vehicular Visible Light Communication*, Signal Processing in Photonic Communications, Article SpTu1F.3, New Orleans, 24–27 July 2017

Wayne, M. A., Jeffrey, E. R., Akselrod, G. M. and Kwiat, P. G. (2009). *Photon Arrival Time Quantum Random Number Generation*, Journal of Modern Optics, Vol. 56, No. 4, pp. 516-522, February 2009.

Wei, W. and Guo, H. (2009). *Bias-Free True Random-Number Generator*, Optics Letters, Vol. 34, No. 12, 11 June 2009, pp. 1876-1878.