A Field RNG Experiment: Use of a Digital RNG at Movie Theaters

Takeshi Shimizu, Kitaro Yamamoto & Masato Ishikawa

ABSTRACT

Over the past two decades, field RNG studies have reported anomalous statistical biases when a coherent event evokes emotions from an audience. A hardware device must be dedicated to generate true random numbers. Recent Intel's Ivy Bridge CPU has an internal RNG, called a Digital RNG (Drng), which uses thermal noise. Using RdRand command, the present study involved a repeated-design field RNG experiment at theaters showing the movies Gekijo Rei (13 times), Star Wars Episode 7 (5 times), and Zang-e (8 times) to confirm this device's sensitivity to anomalies. The Drng chi-square results showed a positive bias eight times during Zang-e, whereas no bias was detected during the other movies. No differences or correlations were found among the other kinds of RNG devices, suggesting that RNGs behave independently from each other. Drng outputs could be a useful way to apply micro PK studies in the absence of access to a dedicated device.

Key Words: Ivy Bridge, RdRand, Japanese horror movies, and thermal noise.

DOI Number: 10.14704/nq.2017.15.1.964 **NeuroQuantology 2017; 1: 60-66**

Introduction

During the past two decades, to study anomalous phenomena such as micro-psychokinesis (PK) or field consciousness, almost studies have used a true random number generator (TRNG), and TRNG is becoming a methodological standard (Nelson, Jahn, Dunne, Dobyns, & Bradish, 1998; Nelson, 2001; Dobyns, Dunne, Jahn, & Nelson, 2004; Radin, 2006; Varvoglis & Bancel, 2015). Main reason why TRNG is required is that a pseudo-RNG (PRNG) is essentially deterministic due to its initial seed, and it is thus predictable. To assure nondeterministic number generation, an RNG must have its own physical source, such as thermal noise, nuclear decay, or quantum tunneling in a field-effect transistor. However, an environment must be created to provide dedicated hardware devices to users who conduct micro-PK studies. This might prevent prevalence of these studies.

Recently Intel Corporation released Digital RNG (Drng) with an open source c-language RdRand (read rand), which can generate nondeterministic numbers, by accessing entropy source (ES, or thermal noise) within the processor on the Ivy Bridge CPU. Although the RdRand command produces pseudo random numbers, its seed is true random created by the ES (Shrimpton, & Terashima, 2015). The Drng includes the reseeding procedures, resulting the outputs of the Drng become nondeterministic, actually. The randomness of the Drng outputs are evaluated

Corresponding author: Takeshi Shimizu
Address: School of Information and Communication, Meiji Univ. Japan
Phone: +090-8057-1928, **e-mail** ✉ shim1zu@hotmail.com
Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.
Received: 14 June 2016; **Accepted:** 3 November 2016

healthy (Hamburg, Kocher, & Marson, 2012), and the performance of the Drng ensure the robustness of its implementation and to provide transparency in its manner of operation (NIST SP800-90, FIPS-140-2, and ANSI X9.82.).

As almost all newer PC machines are equipped the Ivy Bridge CPU (or later series), many people do not have to obtain dedicated devices. Thus, it would be expected that the huge number of machines worldwide would increase the number of users, thereby generating further research.

However, questions about whether the Drng behaves like other TRNGs or if it is sensitive to coherent field events or micro-PK effects remain unanswered. Therefore, the purpose of this study was to examine Drng outputs in field RNG experiments. Field RNG experiments differ from worldwide-scale news-based field RNG studies, such as the "Global Consciousness Project" (Nelson et al., 1998), in that the experimenter designs, conducts, and repeats the experiment locally. Previous field RNG experiments, which were conducted at a movie theater (Shimizu & Ishikawa, 2010) or with short movies at classrooms (Shimizu & Ishikawa, 2012) and involved the local operation of a RNG, reported statistically biased output when the audience viewed a movie that evoked strong emotions. Although a non-biased movie experiment has been conducted (Shimizu & Ishikawa, 2013), the current study was designed to challenge the findings of field RNG experiments conducted at movie theaters.

This study explored the extent to which Drng behavior is similar to that of other kinds of RNGs during the same RNG experiment and compared the sensitivity of the RNGs with one another.

Experiments

Three movies, "Gekijo Rei" (Table 1), "Star Wars Episode 7" (Table 2), and "Zang-e" (Table 3) were selected for use in this experiment. The first is a light horror movie, the second is a well-known exciting and emotional science fiction film, and the third is a mystery/horror movie. All movies were expected to elicit strong emotions from and affect the mood of the audience. The second purpose of this study was to explore whether such arousing movies could bias RNG output.

Gekijo Rei, which was released on November 21, 2015, is 99 min in duration. Star Wars, which was released in Japan on December 19, 2015, is 134 min in duration. Zang-e, which was released on January 30, 2016, is 104 min in duration. We repeated field RNG experiments at the movie theaters from November 2015 to February 2016. The first author conducted the experiment in Tsukuba City, whereas the second author conducted the experiment three times in Yokohama City, and several students assisted with the experiment in Tokyo.

The VAIO Duo11, Panasonic Lets Note, and Surface Pro3 notebooks were used for all experiments, and all machines had the Ivy Bridge CPU enabled to use RdRand or access the Drng.

Table 1. Results for the movie Gekijo Rei for each random number generator (RNG) device and for all combined

Gekijo Rei		64 bps			
	Date start time	audience	χ^2	df	p-value
Psyleron	2015/11/21 9:33	11	6085.4	5940	0.092
	2015/11/21 14:08	25	5726.3		0.976
	2015/11/21 20:37	28	5988.6		0.326
	2015/11/22 9:33	10	5998.0		0.296
	2015/11/22 16:18	16	5797.6		0.905
	2015/11/22 20:37	29	5988.4		0.327
combined		119	35584.1	35640	0.582
Drng	2015/11/23 9:33	3	5821.9	5940	0.861
	2015/11/23 20:37	13	5960.9		0.422
	2015/11/29 19:47	30	5918.2		0.577
	2015/12/3 19:32	7	6011.8		0.254
	2015/12/11 22:11	5	5945.2		0.479
	2015/12/18 17:03	11	5795.6		0.908
	2015/12/22 15:27	4	5966.0		0.403
combined		73	41419.6	41580	0.710

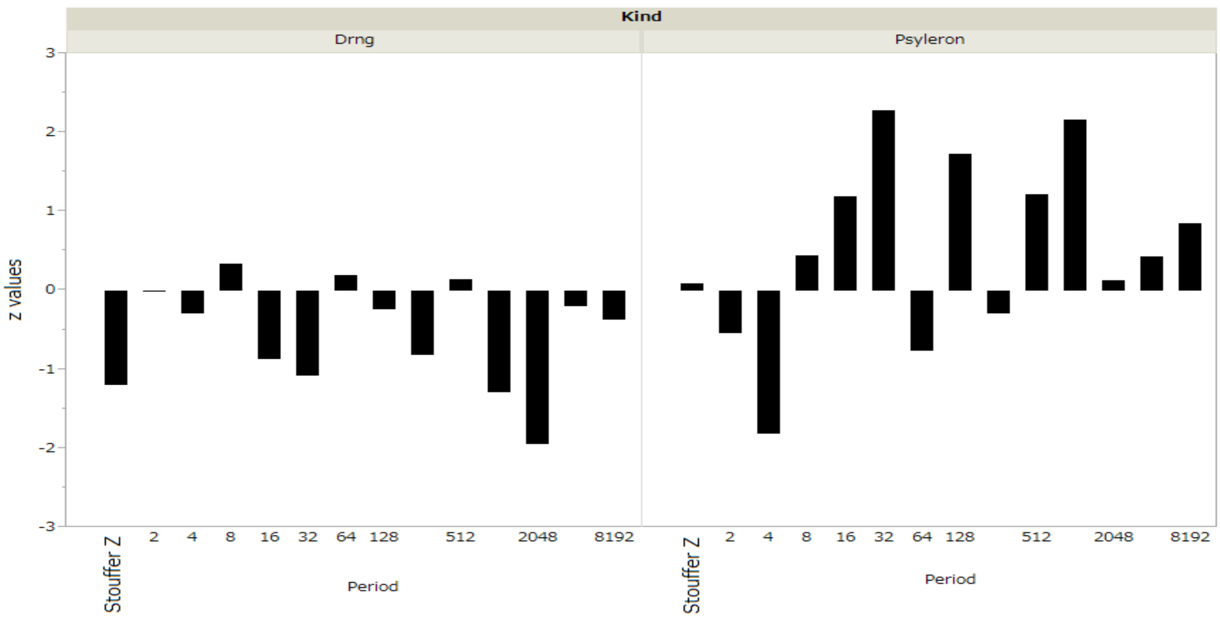
Table 2. Results for the movie Star Wars Episode 7 for each random number generator (RNG) device and for all combined

Star Wars Epsode7		64 bps				
			Psyleron		Drng	
date	audience	df	χ^2	p-value	χ^2	p-value
2015/12/19 11:48	67	8040	7972.1	0.702	7859.1	0.924
2015/12/19 20:48	200		8074.0	0.392	7819.1	0.960
2015/12/22 20:17	20		8185.1	0.127	8032.2	0.522
2016/1/3 20:48	16		8268.1	0.037	7879.4	0.898
2016/2/7 20:46	14		8134.9	0.226	8224.2	0.074
combined	317	40200	40634.3	0.063	39814.0	0.914

Table3. Results for the movie Zang-e for each random number generator (RNG) device and for all combined

Zang-e	256 bps											
			Drng		Psyleron		Quantis		Random*		RngCrypto*	
date	audience	df	χ^2	p-value	χ^2	p-value	χ^2	p-value	Chi sq	p-value	Chi sq	p-value
2016/1/30 9:35	16	6360	6508.8	0.094	6309.1	0.672	6251.8	0.831	6540.1	0.056	6437.6	0.245
2016/1/30 11:55	26		6549.4	0.048	6256.3	0.821	6259.1	0.814	6584.2	0.024	6227.2	0.881
2016/1/30 18:45	34		6489.5	0.126	6411.0	0.324	6347.6	0.542	6391.4	0.388	6281.5	0.756
2016/1/31 11:55	49		6389.3	0.395	6355.4	0.514	6405.3	0.342	6219.8	0.894	6487.3	0.130
2016/1/31 18:40	42		6326.2	0.616	6230.2	0.875	6522.3	0.076	6305.2	0.685	6151.2	0.969
2016/2/2 21:09	19		6501.1	0.106	6447.9	0.217	6282.7	0.753	6614.5	0.013	6428.8	0.270
2016/2/5 19:54	23		6354.6	0.517	6445.5	0.223	6265.7	0.798	6560.4	0.039	6446.0	0.222
2016/2/6 12:22	84		6359.7	0.499	6513.6	0.087	6367.6	0.471	6347.3	0.543	6412.7	0.318
combined	293	50880	51478.6	0.031	50969.0	0.389	50701.9	0.711	51562.8	0.016	50872.4	0.509

*:PRNG by software random numbers



All dZ values were standardized from the wavelet variance for each period. Period '2' was the main component for the conventional chi-square.
Figure 1.DZ and Stouffer Z value differences between the digital random number generator (Drng) and Psyleron REG1 during the movie Gekijo Rei

A software application was developed using Visual Studio 2013 and the Intel Parallel C++ compiler to control RdRand. In addition, we used .Net wrapper produced by JebTek, although its original source was partially changed to optimize our application.

The experimenters ran the software and determined the audience size at the exit after the movie ended.

The Psyleron (REG-1) and several other RNGs were added to the experimental protocol to compare their performance with that the Drng. Table 1 presents the details of the experimental conditions. During the first movie, Gekijo Rei, both the Drng and the Psyleron generated 64 bps. The between-screen design was repeated seven times with the Drng and six times with the Psyleron. Unexpectedly, the film attracted a small audience and closed earlier than expected. During Star Wars Episode 7, the Drng and Psyleron devices generated 64 bps simultaneously during five repetitions of the within-screen design (Table 2). During Zang-e, we used the Psyleron and IDQ Quantis as TRNG hardware devices and added the pseudo-RNGs from .Net framework and RngCrypto and Random to the protocol. All five RNGs generated 256 bps using the within-screen design (Table 3). Unexpectedly, the second author failed to generate random numbers four times during the third movie due to unspecified software problems.

Analysis

Previous field RNG studies have produced anomalous chi-square statistics. Each trial bit is described by x, which is standardized based on a binomial distribution given by $z = (x - np) / \sqrt{np(1-p)}$, where n is the size of bits generated for a trial (e.g., 200, 512 etc.) and p is .50 when the device has been calibrated precisely; bits 0 and 1 have an equal probability of being generated. Our first analysis examined whether the Drng produced anomalies after computing the chi-square for an event given by $\chi^2 = \Sigma_{t=1}^{T} z_t^2$, where t is the time index and T is the length of the event. The chi-square values reflect the variance between trials in an event. If the Drng were sensitive to field consciousness and psychologically aroused states, the chi-square value would reflect anomalistic biases.

The current study decomposed and analyzed all variances from the RNG outputs as follows. First, a wavelet analysis was used to decompose the RNG output into multiple period lengths. Second, analysis of covariance (ANCOVA) was used to test the effects of RNG period type and audience size. Third, an intraclass correlation coefficient (ICC; Shrout, 1979) analysis was performed to detect any associations among RNG devices.

Haar wavelet decomposition

This approach was chosen because its time duration is conventionally intuitive. However, as no actual evidence indicates that a 1-sec interval is optimal to detect signals from field consciousness, an alternative method that does not rely on this length was applied (Shimizu & Ishikawa, 2016). A discrete wavelet analysis using Haar filter would decompose variances into multiple levels. Not concerned about details for wavelet, two aspects should be mentioned here. The Haar filter creates a scaling (approximation) coefficient expressed as follows:

$$c_{j+1,k} = (c_{j,2k-1} + c_{j,2k}) / \sqrt{2}, \quad (1)$$

where j is the depth of a level and k is the index at the j-th sequence of the level. This approach smooths the sequences, and the filter creates the coefficient

$$d_{j+1,k} = (c_{j,2k-1} - c_{j,2k}) / \sqrt{2}, \quad (2)$$

and the sum of squares becomes the wavelet variance.

The Haar filter is restricted for event length to a power of 2 (e.g., 256, 8,192 sec), which has little practical value. To mitigate this issue, the data set took zero padding for the surplus length (e.g., 8,192 sec toward the actual 6,240 sec), and the degrees of freedom were not counted for padded zeros. This procedure helped adjust the wavelet variance and the *Stouffer Z* value. Notably, the wavelet variance is related to the chi-square values as follows:

$$\chi^2 = \Sigma d_j^2 \; + Stouffer\, Z^2. \quad (3)$$

Thus, the sum of d^2 (over 2-sec periods) equals the chi-square value based on a 1-sec trial calculation.

Stepwise construction of the ANCOVA model

The dependent variables in the following analysis of variance (ANOVA) were standardized wavelet variances (dZ). Standardization was determined according to $dZ_j = (\sum d_j^2 \; - df) / \sqrt{2df}$, where j is depth and $df = T / 2^j$. Instead, the current study computed (1) the probability of d^2 according to the chi-square distribution, and (2) the z-score was determined from the probability (e.g., $d^2 = 34.1, df = 23.2, p - value \; = \; .936$, converting $z \; = 1.524$, which is defined as dZ).

The outputs of all movies were analyzed by ANCOVA after stepwise factor selections which were performed based on Akaike's Information Criterion (AIC) using direction to increase variables. Candidate factors were the 'kinds' of

RNG (Drng or Psyleron was the between-screen factor for Gekijo Rei or the within-screen factor for Star Wars). Drng, Psyleron, Quantis, Random, and RngCrypto were the RNG within-screen factors for Zang-e, with 'periods' (14 levels of the Stouffer Z and 13 levels created by film length) and 'audience size' added to the model as covariates and first-order interaction terms, respectively.

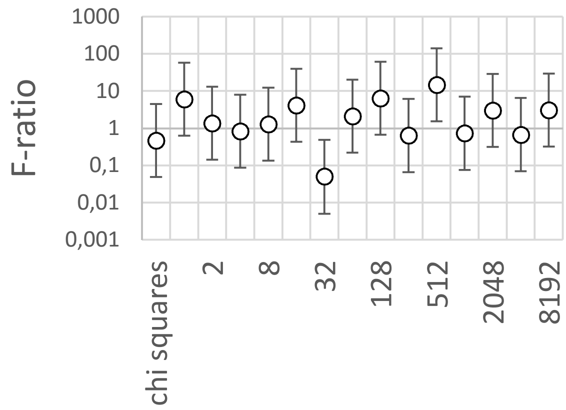
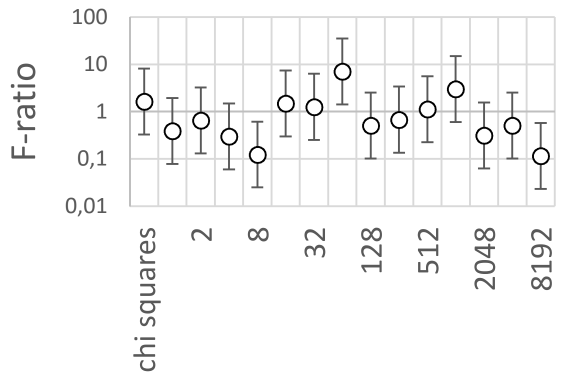
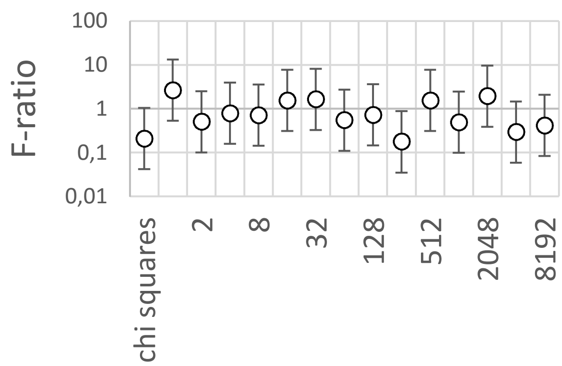


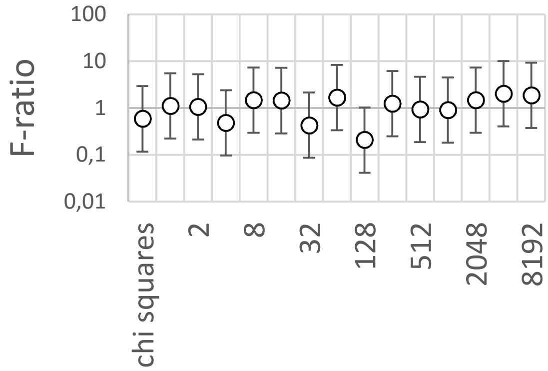
Figure 2. Each number is the period length in the wavelet variance. Bars correspond to the 95% confidence intervals (CIs) for the expected F ratios of 1.0.F-ratios from the intraclass correlation coefficients (ICC2) between the digital random number generator (Drng) and Psyleron REG1 for dZ values after five repetitions of Star Wars.



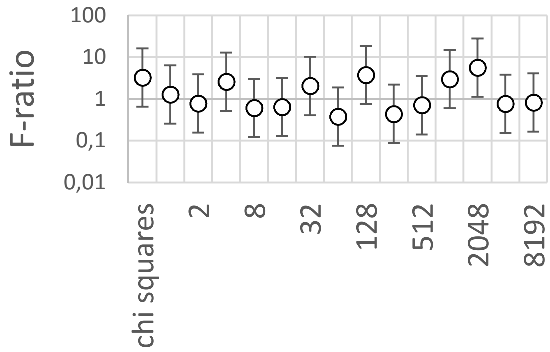
Psyleron



Quantis



Random



RngCrypto

Figure 3.F-ratios from intraclass correlation coefficients (ICC2s) between the digital random number generator (Drng) and other RNG devices for dZ values after eight repetitions during the movie Zang-e

F-ratio confidence interval (CI) from the ICC

Intra Class Correlation, ICC2 was computed among RNGs. The computing is essentially equal to an ANOVA model. As ICC values can range from negative infinity to 1.0, we used 95% CI of the F-ratio, which has the same meaning as the ICC, rather than the ICC itself (e.g., $F > 1$ positive and $F < 1$ negative). Since the F-ratio is equal between ICC (2, 1) and ICC (2, k), we describe ICC2.

The Gekijo Rei results did not yield an ICC, as the experiment was conducted using a between-screen design. The Star Wars experiment produced ICCs for the Drng and Psyleron after five repetitions for each period condition, whereas the Zang-e experiment produced ICCs between two physical RNGs (Psyleron and Quantis) and two PRNGs (RngCrypto and Random). A lower bound of 95% CI > 1.0 for the F-ratio indicates a significantly positive association between devices during a period. On the other hand, an upper limit of < 1.0 indicates the devices canceled each other out.

Results

Gekijo Rei Table 1 shows the Gekijo Rei results for the two RNGs. The chi-square test did not detect any bias. The ANCOVA included only factor type after the stepwise model selections, and the Drng dZ values were lower than those of the Psyleron (F (1,180) $= 6.53, p = .011$; Figure 1). A post hoc test focusing only on the Drng showed significantly small variances, ($\sum dZ_j \,/\, \sqrt{14} = -2.06, p = .039$. two-tailed). The Drng outputs during the film failed to detect large variances.

Star Wars Table 2 shows the results for Star Wars Episode 7. Two devices were used with a within-screen design. The combined chi-squares ($df = 40{,}200\ = 8{,}040\ \times 5\, times$) for the Psyleron devices were marginally significant ($\chi^2(40200) = 40634.3, p = .063$) suggesting the experiment would detect anomalies, whereas those for the Drng were not. The stepwise ANCOVA model only selected the main effect of audience size, but it unexpectedly detected a marginally significant negative coefficient −.002, F (1,138) = 2.98, p = .087. This result was related to the small variance when 200 people viewed the film (Table 2).

The ranges of the 95% CIs for the F-ratios from ICC2 were compared between the Drng and Psyleron after five repetitions to explore whether they behaved similarly. Figure 2 shows the logarithm of the 95% CI for the F-ratios (4, 4). These two devices seemed independent, showing a slight negative correlation at the 32-sec period and a positive one at the 512-sec period.

Table 3 shows the Zang-e results. Both the Drng and Random (PRNG) showed significantly high chi-squares, whereas the Psyleron and Quantis did not show any bias. The ANCOVA revealed no effects from the wavelet variances after stepwise model selection. The F-ratio (7, 7) results from the ICC2 for each period after eight repetitions were used to determine whether the Drng was more similar to a TRNG or to a pseudo-RNG. The F-ratios between Psyleron devices showed positive correlations at the 8- and 64-sec periods, which differed from the results for Star Wars. The F-ratios between Quantis devices were independent from each other, except a negative effect was found at the 256-sec period. No correlations were found between the pseudo-RNGs. A positive correlation was found for the RngCrypto at 2,048 sec.

Discussion

The current study involved a repeated-design field RNG experiment using the Drng inside the Intel Ivy Bridge CPU at three movie theaters as an audience viewed a film. The three movies used (Gekijo Rei, Star Wars Episode 7, and Zang-e) were categorized as light horror, exciting science fiction, and mystery/horror, respectively. Two of the movies were Japanese horror movie, and all were chosen to evoke thrills or fear from the audience. Unexpectedly, Gekijo Rei was not experienced by the audience as serious but was experienced as light-hearted, and Zang-e was experienced as more a mystery movie than a horror film. The outputs of Psyleron device during Star Wars showed marginally high chi-squares, suggesting that the local field RNG experiment could detect anomalies from field consciousness, although those of the Drng didn't show biases.

On the other, the Drng outputs during Zang-e reflected a positive bias in the chi-square analysis, suggesting that (1) the Drng (RdRand command) can detect field consciousness, and that (2) fear affected the anomalous RNG output. As the other physical RNGs did not show anomalies, further study is needed. On the other hand, the wavelet variances for the Drng were significantly small for all periods during Gekijo Rei (Figure 1), which may be related to the small audience sizes. In general, biases in the RNG output seemed to be associated with the strength of the emotional reactions evoked by the film.

Correlation between other RNG devices

The results of ICC2 F-ratio showed that the Drng was not correlated with the other pseudo-RNGs, whereas the Drng may have been correlated with Psyleron device. Whereas no differences were detected during Star Wars or Zang-e, the bit rate (generation speed) differed between them, as Star Wars had 64 bps, whereas Zang-e had 256 bps.

The trough at the 32-sec period in Star Wars (Figure 2) may correspond to that at 8 sec in Zang-e (Figure 3), both of which generated 2,048 bits (= 32 sec × 64 bits and 8 sec × 256 bits). Peaks were detected at 512 sec in Star Wars and at 64 sec in Zang-e, which converted to 32,786 (= 512 sec × 64) bits and 16,384 (= 64 sec × 256) bits, respectively. The different bit sizes may have been caused by the coarseness of the Haar filter. Further study is needed to compare the devices. The entropy source for the Drng is thermal noise, whereas that for the Psyleron REG-1 is quantum tunneling in a field-effect transistor. The current behaviors of the RNGs seemed to be independent of one another. Our results suggest that these RNG devices cannot be regarded as sensors for detecting field consciousness signals. Thus, we must address questions about how a reliable RNG device senses anomalous signals from field consciousness.

Future tasks

The Drng is only at the beginning of its application as a new technology using the Ivy Bridge. If the Drng becomes available as a physical RNG resource, it would expand RNG study designs. The current GCP has more than 60 EGGs worldwide, whereas the Drng may operate on a scale of a billion bits worldwide if fully activated. About 300 billion new PCs have been manufactured each year over the past 10 years. Therefore, a huge number of machines is equipped with the Ivy Bridge CPU.

Near future, we can be available new generation CPU of Intel Broadwell series, which can control Drng outputs by RdSeed (read seed) command directly instead of RdRand. The outputs from RdSeed is purely true random numbers, although the outputs would be assumed to provide seeds for pseudo random number generation. Anyway, the Drng will expand to cover entire micro-PK studies, and the development of appropriate software technology will contribute to these studies.

References

Daubechies, I. Ten lectures on wavelets (Vol. 61, pp. 198–202. Philadelphia: Society for industrial and applied mathematics., 1992.

Dobyns YH, Dunne BJ, Jahn RG & Nelson RD. The MegaREG Experiment: Replication and Interpretation. Journal of Scientific Exploration 2004; 18: 369–397.

Hamburg M, Kocher P & Marson ME. (2012). Analysis of Intel's Ivy Bridge digital random number generator. Online: http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf.

Nelson RD, Jahn RG, Dunne BJ, Dobyns YH & Bradish GJ. Field REG II: Consciousness field effects: Replications and explorations. Journal of Scientific Exploration 1998; 12: 425–454.

Nelson RD. Correlation of global events with REG data: An Internet-based, nonlocal anomalies experiment. Journal of Parapsychology 2001; 65: 247–271.

Radin DI. Entangled Minds: Extrasensory experiences in a quantum reality. Paraview Pocket Book, Simon & Schuster: New York., 2006.

Shimizu T & Ishikawa M. Field RNG data analysis, based on viewing the Japanese movie Departures (Okuribito). Journal of Scientific Exploration 2010; 637–654.

Shimizu T & Ishikawa M. Field RNG Experiments Using Short Movies: An Examination of the Focused-attention and Emotion Hypotheses. Journal of the International Society of Life Information Science 2012; 30: 17–30.

Shimizu T & Ishikawa M. Exploration of Field Consciousness Signal Wavelength: Field RNG Experiment at a Movie Theater. Journal of the International Society of Life Information Science 2013; 31: 17–29.

Shimizu T & Ishikawa M. Optimal length exploration for field RNG outputs using a Haar wavelet filter: TV Audience Ratings for New Year 2012 in Japan. Journal of Parapsychology 2016; 80(1): 87-98.

Shrimpton T & Terashim RS. A Provable-Security Analysis of Intel's Secure Key RNG. In Advances in Cryptology EUROCRYPT Springer Berlin Heidelberg. 2015; pp.77-100.

Shrout PE & Fleiss JL. Intraclass correlations: uses in assessing rater reliability. Psychological bulletin 1979; 86(2): 420-428.

Varvoglis M & Bancel PA. Micro-psychokinesis. Parapsychology: A Handbook for the 21st Century, 2015; pp.266–281.

eISSN 1303-5150