2016

Celestial sources for random number generation

Erin Chapman
Digital Forensics Research Laboratories, Institute for Radio Astronomy and Space Research, Auckland University of Technology, erinchapman@xtra.co.nz

Jerina Grewar
Digital Forensics Research Laboratories, Institute for Radio Astronomy and Space Research, Auckland University of Technology, jmgrewar@gmail.com

Tim Natusch
Digital Forensics Research Laboratories, Institute for Radio Astronomy and Space Research, Auckland University of Technology

DOI: 10.4225/75/58a6975133e06
Chapman, E., Grewar, J., & Natusch, T. (2016). Celestial sources for random number generation. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia.* (pp.5-13).

CELESTIAL SOURCES FOR RANDOM NUMBER GENERATION

Erin Chapman, Jerina Grewar, Tim Natusch
Digital Forensics Research Laboratories, Institute for Radio Astronomy and Space Research
Auckland University of Technology, Auckland, New Zealand
erinchapman@xtra.co.nz, jmgrewar@gmail.com

Abstract

In this paper, we present an alternative method of gathering seed data for random number generation (RNG) in cryptographic applications. Our proposed method utilises the inherent randomness of signal data from celestial sources in radio astronomy to provide seeds for RNG. The data sets were collected from two separate celestial sources, and run through the SHA-256 algorithm to deskew the data and produce random numbers with a uniform distribution. The resulting data sets pass all tests in the NIST Statistical Test Suite for random data, with a mean of 98.9% of the 512 total bitstreams from the two sources passing all tests in the NIST suite, as well as further testing in R. These results are on par with the control set generated using Java's SecureRandom function. An explanation of the sources, the data processing and detailed results of each of the tests are presented.

Keywords

Random number generation, RNG, random noise, NIST, seeds, cryptographic hash functions, SHA-256, secure hashing algorithm, radio astronomy, signal noise, data analysis, astronomy, analytics, random sequences

INTRODUCTION

The use of random number generators is a fundamental element of cryptographic systems. The creation of random initialisation vectors and keys are of utmost importance in security applications which utilise encryption on a day-to-day basis globally. The means by which these numbers are generated varies from application to application, however many are created through algorithmic processes, such as the Monte Carlo methods (Gentle, 2006). Many different options for producing truly random numbers through nature have been proposed, utilising the signal noise of lasers (Applegate et al., 2015), or implementing quantum chaotic generators (Akhshani, Akhavan, Mobaraki, Lim, & Hassan, 2014). In this paper we propose an alternative method for seeding RNGs which utilises the inherent randomness of the signal noise produced by radio telescopes, with a scheme which implements the Secure Hashing Algorithm (SHA) as a deskewing algorithm for randomness extraction. The output of this scheme passes statistical tests for randomness in both R and the NIST Statistical Test Suite (NIST STS), and offers a new method of collecting random numbers for use in seeding cryptographic applications. This research offers applications in the implementation of secure random number generators such as SHA-256 (Dang, 2015), which rely on irreproducible, statistically random seed data for security. The proposed scheme for gathering seed data could be utilised in the application of cryptographic protocols for secure systems, as our results show it presents a high-level of performance paired with rapid data collection.

The structure of this paper is as follows: in Part I relevant prior research is discussed briefly, and an overview of the area is given. In Part II the operation and theory of radio telescopes and the related signal noise is explained. Part III then offers our data sources and method for the collection of the output. Part IV enumerates the method by which the gathered data was processed using SHA-256 for deskewing purposes and our results based on the outcome of the statistical testing completed. Finally, Part V offers our conclusions and suggestions for further research.

RANDOM NUMBER GENERATION AND RANDOM SEEDS

The generation of random numbers for security applications is an ever-present concern. Utilising hardware to generate these numbers is a well-developed area, in which the main aim is to mitigate the statistical properties of the data, and to determine whether there is any way for an adversary to estimate the likely output of a particular system. As the algorithms used in these applications are themselves public knowledge, the security rests in the seed, for deterministic systems, and in the data source, for non-deterministic RNG.

Schemes such as the secure RNG developed by Lo Re, Milazzo, & Ortolani (2014) make use of the inherent properties of hardware components to collect data. In the system proposed by Lo Re et al. (2014) each node of the wireless sensor network is capable of generating random numbers, which are provided to the leader node.

Other systems have utilised the properties of quantum mechanics to implement RNGs. Lunghi et al. (2015) offered a quantum RNG which maintained consistent monitoring of the output to ensure continuing statistical randomness. Cicek, Pusan, & Dundar (2014) presented a method for True Random Number Generation (TRNG) through a chaos system, which gave excellent performance when tested by the NIST Statistical Test Suite, with the bitstream resulting from the scheme split into 1 Mbit blocks.

In generating random numbers for everyday use in cryptographic applications, most systems use pseudo-random number generators (PRNGs), which function through algorithmic means. This type of RNG requires a seed, which in itself should be statistically random and irreproducible, because if the seed is compromised, then the resulting random numbers are also compromised. Implementations such as the Java function call SecureRandom use a mixture of truly random and pseudorandom data, often starting with a TRN as the function seed. Other PRNGs use statistical methods such as Monte Carlo techniques, or Lorenz systems (Lynnyk, Sakamoto, & Celikovsky, 2015). In the case of Lynnyk, Nakamoto and Celikovsky (2015), a TRN was used to produce the seed for the algorithmic PRNG. In Barker and Kelsey (2015), the Secure Hash Algorithm (SHA) family is recommended for use in deterministic random number generation using irreproducible and statistically random seeds.

RADIO ASTRONOMY

Radio Astronomy is the discipline of science using antennae or radio telescopes to detect the emission of celestial sources in the electromagnetic frequency range of 10^6 Hz to 10^9 Hz (Shuch, 2013). Radio telescopes allow astronomers to peer through not only the layers of our atmosphere but in frequencies beyond the human eye's capability into interstellar clouds of particles, thereby determining the chemistry and physics behind the astronomical phenomena of our universe (Dougherty, 2011).

At 30.48 metres in diameter, the Warkworth 2 antennae was licensed from Telecom and converted in 2010 by the Institute for Radio Astronomy and Space Research (IRASR) of Auckland University of Technology (AUT) (Murphy, 2010). This took it from an international telecommunications satellite dish to a radio telescope as part of the Warkworth Radio Astronomical Observatory (WRAO). The telescope is a reflector on a wheel and track with a beam waveguide feed (Woodburn et al., 2015). NEC Corporation of Japan originally built the dish for the Post Office (later Telecom) in 1984 as part of Warkworth Satellite Earth Station, which is located 5 km south of Warkworth and 60 km north of Auckland, in New Zealand's North Island (Ministry of Culture and Heritage, 2013).

The majority of astronomical objects give off radiation for astronomers to detect, but some have much greater emissions including pulsars, quasars, certain nebulae, and radio galaxies (The Editors of Encyclopædia Britannica, 2016). In 1931, Karl Jansky worked on improving the operation of transoceanic radio links for Bell Laboratories. The "steady hiss static" that he recorded became the origin of radio astronomy, and now the strength, or spectral flux density of a radio source is measured in Janskys (Jy), where 1 Jy = 10-26 Wm-2Hz-1 (Jansky, 1979).

Radio astronomy signals are inherently random, "a specific property of astronomical observations is that they cannot be repeated under the exact same conditions" (Junklewitz, 2014, p.13). The astrophysical source signal and the telescope system noise are both Gaussian distributed (Burke and Graham-Smith, 2002). The signal available at the output of a radio telescope consists of the combination of system noise (internally generated noise), a 2.73 Kelvin component from Cosmic Microwave Background Radiation, noise power from the celestial source of interest (the "signal") and typically interference signals picked up from the surrounding terrain (Campbell, 2002). The influence of the amplifier increases the amplitude of both "signal" and noise whilst a linear (frequency independent) response of the receiving system will preserve the statistical distribution of the input signal and result in a Gaussian output signal (Haykin, 2009).

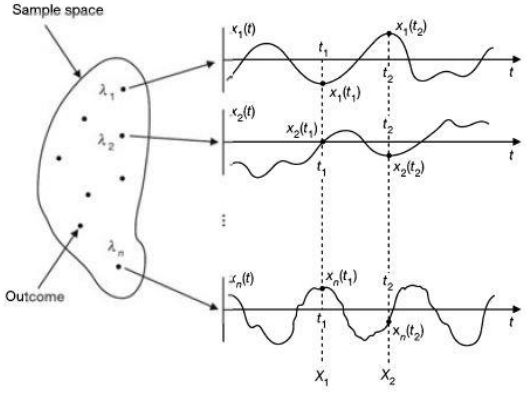

Figure a: Random Process (Hsu, 2013, p. 393)

Due to the random nature of all the processes contributing to the final receiver output signal it is not normally possible to distinguish between the various components from a study of the output signal. Using the sum of all these signals, and recognizing the implausibility of another party replicating the uniqueness of the system noise component(s) confers a distinct advantage for recording a unique source of randomly generated data (Burke and Graham-Smith, 2002). An illustrated example of how our recorded signal is a statistically random process is shown in *Figures A* and *B*.

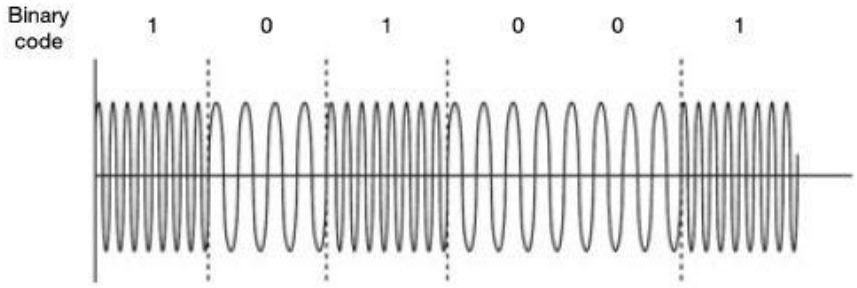

Figure b: Random sequence of data bits 1 or 0 produced by a Random Process (Hsu, 2013, p. 393)

DATA COLLECTION

The data used in this research was collected at the WRAO. The two sources chosen for data collection were the bright Maser 309.92+0.47, hereafter referred to as "G309" (coordinates 13h 50mins 41.78s RA and -61º 35' 10.2" DEC) and M17 (18h 20mins 26s RA and -16º 10' 36" DEC) from the J2000 epoch. G309 is a methanol maser; an interstellar cloud of methanol (CH_3OH) molecules that emits at a frequency of approximately 6.7 GHz (in the laboratory/rest frame). Photons are released when these particular molecules change their angular momentum via a transition between allowed quantum rotational states. In the J/A+A/432/737 General Catalogue of 6.7GHz Methanol Masers, G309 has a flux of approximately 780 Jy (Pestalozzi and Chrysostomou, 2005). The methanol maser is 5.3 kiloparsecs (kpc) or 17.2 kilo-lightyears (kly) distant from Earth (Phillips, Norris, Ellingsen, & McCulloch, 1998). M17 is a nebula containing an open cluster of stars called NGC6618. The cluster is an HII star-forming region, an ionised cloud of Hydrogen that radiates by a thermal emission process. M17 is at 1.6 kpc distance and observed total flux is some 687 Jy (Povich et al., 2007).

Signal from the right hand circular polarisation (RCP) of the telescopes C band receiver was processed by a chain of backend electronics consisting of a "front end" Low Noise Amplifier (LNA), a down-converter that selected and mixed a 6.5-6.8 GHz "RF/Sky" band of signal down to a 300 MHz wide band centred on 825 MHz and finally to an RTL-SDR for further filtering, amplification and digitisation of the signal. Down conversion to the Intermediate Frequency (IF) band at 825 MHz is achieved by selecting the lower side band result of mixing the RF/Sky band with a 5.8 GHz signal from a Local Oscillator (LO) locked to the WRAO Hydrogen Maser (Woodburn et al., 2015):

$$f_{IF} = f_{SKY} - f_{LO} = 6.675\ GHz - 5.85\ GHz = 0.825\ GHz\ or\ 825\ MHz$$

The down converted band was conveyed by a short length (≈0.5 m) of coaxial cable that also converted from the type N output connector of the C band downconverter to the MCX input of the RTL-SDR. Equipped with a RTL2838U chipset the RTL-SDR Software Defined Radio (SDR) dongle was plugged into a USB 2.0 port of a Unix based laptop (provided by IRASR) The dongle was tuned to 825 MHz and set to a gain of 40 dB by constructing a simple GUI interface in the free GNU Radio Companion (GRC) software package (West, 2006). The digitized 8 bit data was interleaved into in-phase (I) and quadrature phase (Q) streams produced by the dongle. The raw data streams were processed by a Fast Fourier Transform (FFT) GRC block to produce a spectrum for visual monitoring of the recorded signal. The LO was turned on and off, the response assured a signal was being recorded from *fsky*. The actual recording of signals was initiated using appropriate commands from the rtl_sdr driver package (obtained from git clone git://git.osmocom.org/rtl-sdr.git). Approximately 400MB of raw data was recorded from each of our sources, for ≈ 1 min each, into 2 binary seed files. This data was then pre-processed using hex dump into text files each containing a 128 bit line of received data in hexadecimal format.

As part of the process of determining correct operation of the system the telescope was first pointed at Centaurus A (NGC5128), a Seyfert galaxy (13h25m27.6s RA, -43d01m09s DEC). A pointing observation was run, stepping through a grid of 9 points offset from the nominal position in both azimuth and elevation. The received power levels obtained for all offset positions where then subjected to a least squares fit (Gaussian peak on a straight line

background) to determine offsets of the flux peak. Offsets of 0.04º in azimuth and 0.03º in elevation where determined and then applied to subsequent source observations. With calibration of pointing offsets applied the telescope was then focused on G309 and M17 in sequence and data files recorded for analysis as described above.

RESULTS

The data collected from the sources G309 and M17 was processed for testing using Java. All processing and testing was completed on a Unix-based machine configured with 16GB 1867 MHz DDR3 RAM and a 3.1 GHz Intel Core i7 processor. The Java code stripped the index numbering from the lines in the hex dump file, and removed all excess white space. Each of the 128-bit lines of data were then individually used as a seed for hashing into random numbers. As per the NIST recommendations (Barker & Kelsey, 2015), we utilised the SHA family of algorithms for the purpose of randomness extraction, specifically the SHA-256 algorithm (Dang, 2015). The output of this process was then written to a binary file for testing purposes.

The first set of tests performed on our data were completed in R, version 3.3.1, which offers several libraries for the analysis of random data. The *randtests* package created by Mateus & Caeiro (2014) offer tests which examine the vector data read through a binary file and offer a p-value as the output. A p-value of greater than then significance level $a = 0.05$ gives the sequence a pass, while a p-value of less than $a = 0.05$ means the test has rejected the null hypothesis. The binary file for each source was read into a vector of integer elements, with 2 bytes to each integer value. The data was subjected to the Bartels Rank Test (Bartels, 1982), the Cox Stuart Test (Cox & Stuart, 1955), the Difference Sign Test (Moore & Wallis, 1943), and the Wald-Wolfowitz Runs Test (Wald & Wolfovitz, 1940) for continuous data. In all tests, the p-value result was greater than a, meaning the data passed the test. In comparing the two data sets, we found that the data gathered from M17 offered better results than that gathered from G309. We speculate that this may be due to the inherent nature of each of the sources, as M17 is a weaker and more generally dispersed source than G309. Further investigation is required for a definitive resolution to this speculation.

Table 1 shows the results of the testing for both sources, as well as values generated through Java's SecureRandom function, used as our control group. The control data was similarly hashed with the SHA-256 algorithm, and read in to integer values 2 bytes at a time.

Table 1: Results of testing in R's randtests package (4 d.p.)

Test	*M17*	*G309*	*Control*
Bartel's rank test	0.5922	0.4317	0.5633
Cox Stuart test	0.7919	0.05636	0.138
Difference sign test	0.6885	0.4409	0.5945
Wald-Wolfowitz runs test	0.4372	0.2941	0.353

The hashed M17 data gave a better performance on the tests than the control group, of the hashed SecureRandom numbers, while G309 resulted in the worst performance of the test sets. Table 2 shows the entropy values of the data sets, both pre- and post-hashing, which were calculated using the Dirichlet-multinomial pseudo count model with Bayesian estimates using Laplace's prior (a=1) in the *entropy* R package (Hausser & Strimmer, 2009). The entropy value of the pre-hashed astronomical data in comparison with the control group of the data generated using the SecureRandom function suggests that the use of celestial sources provides data with a superior level of entropy for use in cryptographic functions.

Table 2: Data Entropy Values as per R's entropy package (5 d.p.)

Data set	*Entropy pre-processing*	*Entropy post-processing*
M17	16.11105	15.92491
G309	16.10822	15.92499
Control	15.89529	15.92493

The histograms for each of the data sets were also computed, both for the unprocessed stream received from the radio telescope, which presents a Gaussian distribution, and for the hashed data, which results in a visibly uniform distribution. *Figure C* shows the histogram for the unprocessed data gathered from M17, while *Figure D* shows the post-hashing data for M17 once it was fed through the SHA-256 algorithm. *Figure E* meanwhile displays the histogram for G309 pre-processing, and *Figure F* gives the histogram for G309 post-hashing.

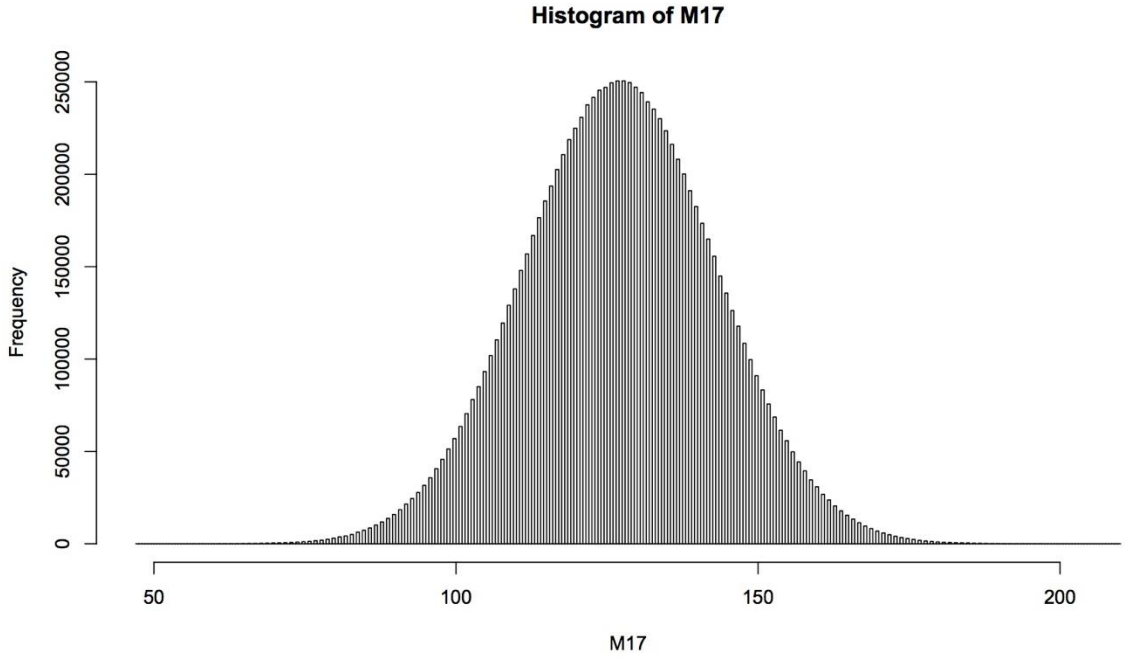

Figure c: M17 data distribution frequencies, per one million bits

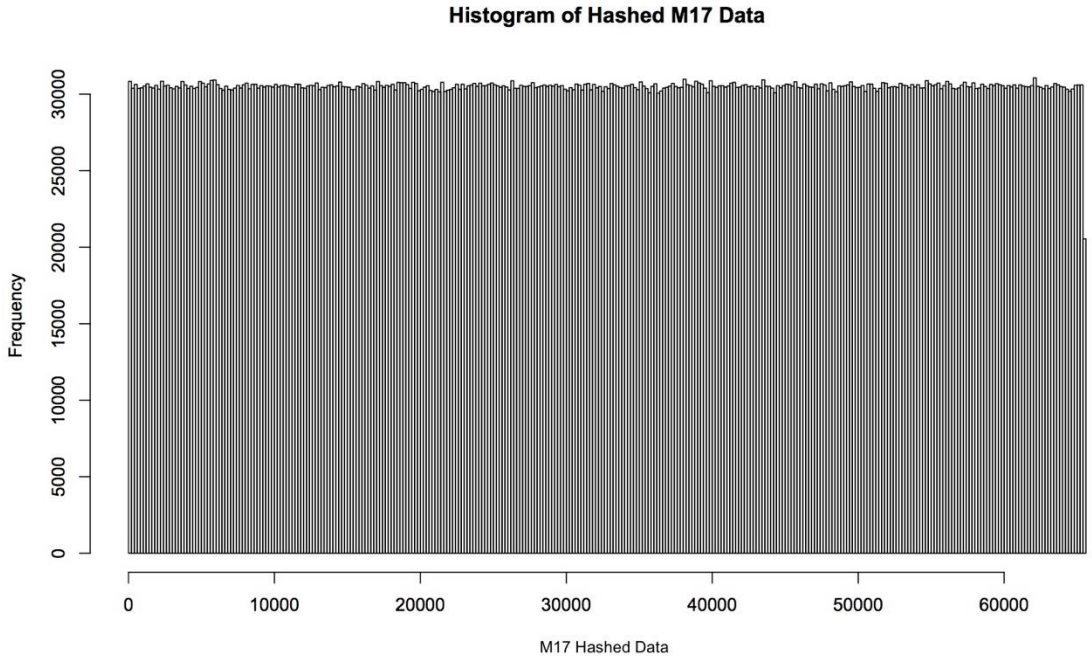

Figure d: Hashed M17 data distribution frequencies, per one million bits.

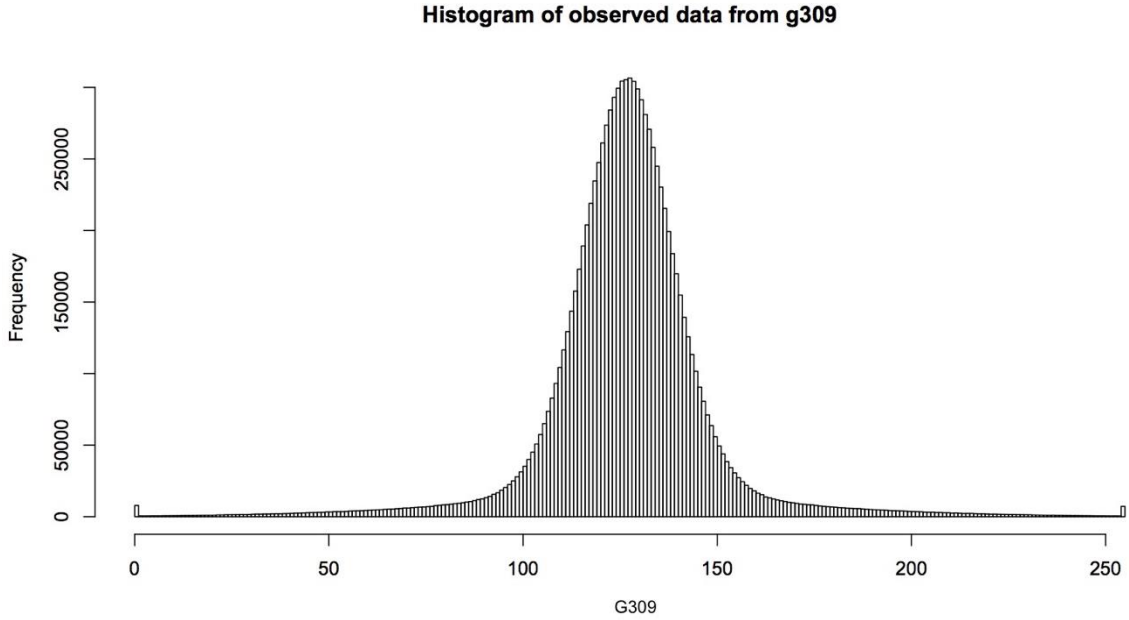

Figure e: G309 data distribution frequencies, per one million bits.

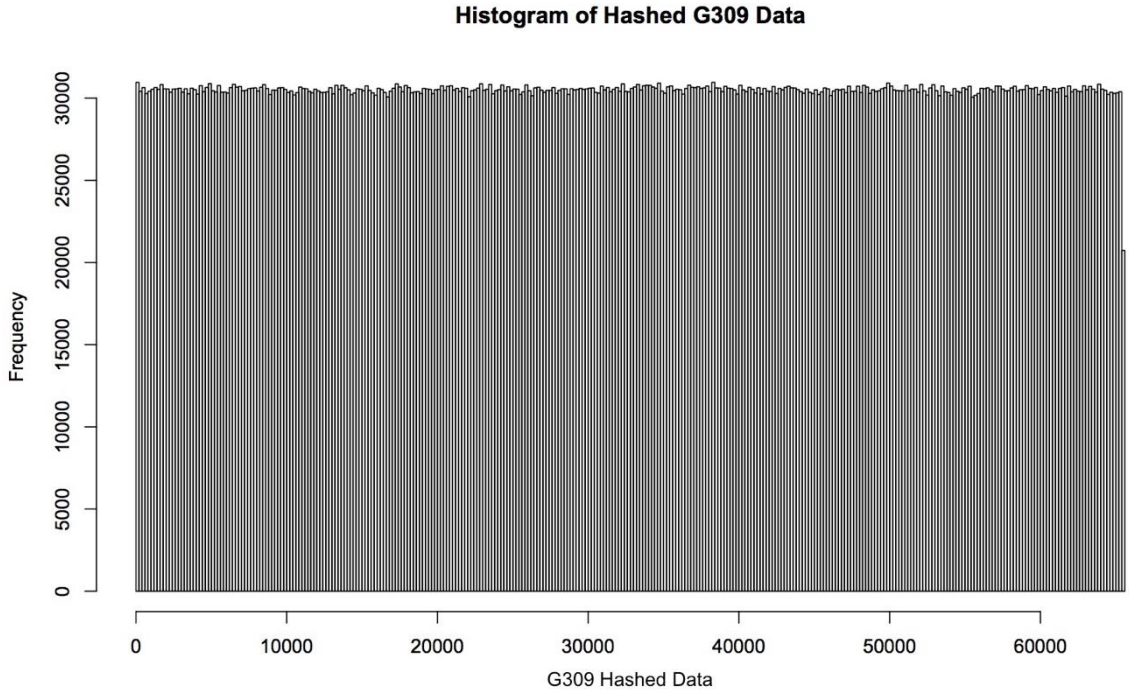

Figure f: Hashed G309 data distribution frequencies, per one million bits.

Based on the results of testing in the *randtests* suite, a second set of testing was conducted using the NIST Statistical Test Suite (Rukhin et al., 2010), which conducts 15 tests for randomness in binary data. The binary files input to this program were the same ones used for the testing in R, and the bitstream length was set to $n = 6{\times}10^6$ for 256 streams of data.

Table 3 gives the results of testing in the NIST STS. All data sets passed all 15 of the tests for randomness, with 97% or more of the streams passing each. For all data sets the results are within a few percentage points of one another, suggesting highly comparable values. For tests such as the non-periodic template matching test, which returned multiple results for each data set, the mean value was calculated from all returned values for that test.

Table 3: Results from testing in the NIST Statistical Test Suite (4 d.p.)

Test	*M17*		*G309*		*Control*	
	p-val	*%*	*p-val*	*%*	*p-val*	*%*
Frequency	0.7637	99.6094	0.6828	98.8281	0.0835	99.6093
Block Frequency	0.3012	98.0469	0.4484	98.4375	0.8237	98.8281
Cumulative Sums	0.7455	100	0.7065	99.2188	0.5834	99.4141
Runs	0.4711	98.8281	0.6993	98.4375	0.6993	98.8281
Longest Run of 1s	0.5022	97.2656	0.7637	99.2188	0.4559	100
Rank	0.9769	99.2188	0.5667	98.8281	0.1167	99.6093
DFT	0.1681	98.4375	0.2954	99.6094	0.0989	99.2188
Non-periodic Template Matching	0.4805	98.9627	0.4974	98.9390	0.5262	98.9733
Overlapping Template Matching	0.1038	98.0469	0.4788	99.2188	0.5194	98.0469
Universal Statistical	0.0815	99.2188	0.9114	99.2188	0.2320	98.4375
Approximate Entropy	0.3191	98.4375	0.5914	100	0.9114	97.6563
Random Excursions	0.5232	99.0783	0.5166	99.2477	0.4923	98.2981
Random Excursions Variant	0.4301	99.2832	0.6290	98.9712	0.4117	98.9306
Serial	0.3169	99.2188	0.6696	99.2188	0.4541	99.2188
Linear Complexity	0.5667	98.0469	0.8092	98.8281	0.2272	99.2188

Figure G gives the graphed percentages of the NIST STS results for each of the data sources. The overall mean of the percentage of bitstreams which pass the tests for the two celestial sources is within 0.02% of the control group, with 98.9% of the 512 bitstreams passing the tests.

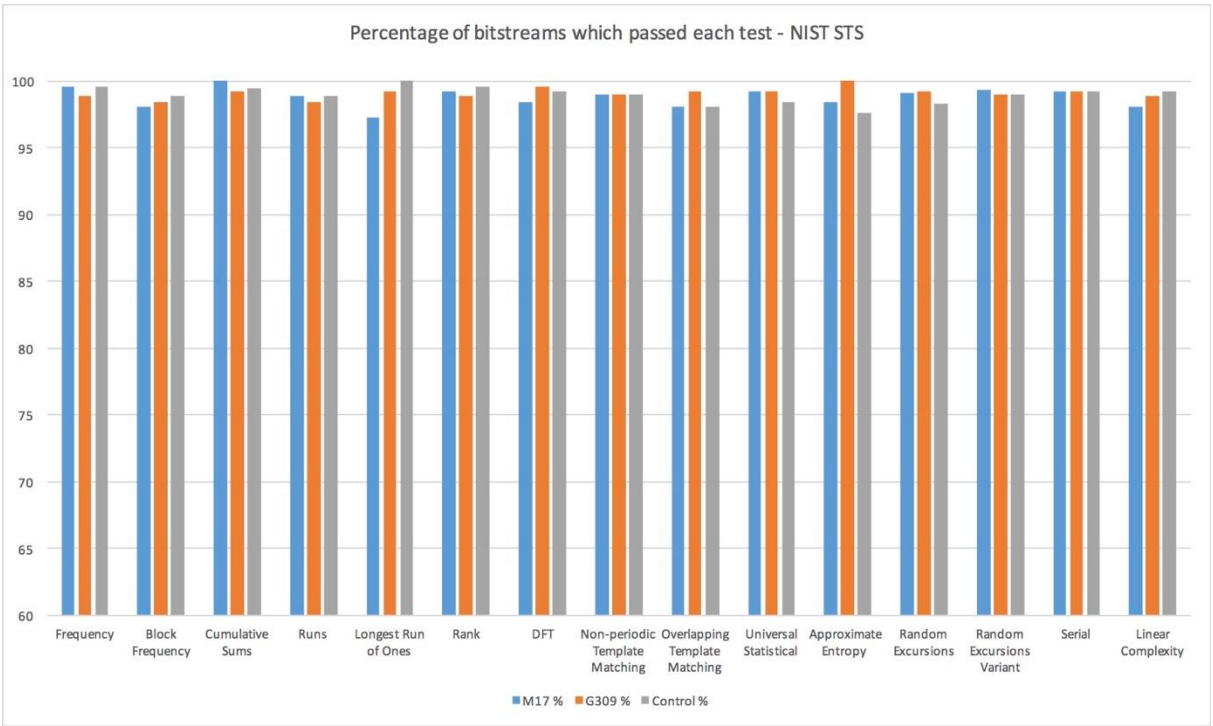

Figure g: Percentage of bitstreams which passed the NIST testing for each data source.

The results of the testing suggest that data gathered through radio astronomy may present a viable option for use as seeds for cryptographic application. The wide variety in data due to fluctuations in machinery, inconsistent

radiation from sources, and interference from satellites and other space junk offers a continuous stream of irreproducible random bits. The time taken to gather the data used in the testing, approximately 400MB worth for each source, was approximately one minute per source. The resulting performance of the data with the SHA-256 algorithm shows it may be a viable option for security applications. As such, it offers a new, rapid and efficient method of gathering irreproducible seeding for random number generation.

CONCLUSION

In this paper we have presented an alternative method for the collection of seed data for random number generators. Utilising the inherent randomness and irreproducibility of radio signal data from celestial sources presents what our results appear to show is a viable method for collecting vast amounts of seed data for use in RNG. The data sets tested all offered high performance levels in the statistical tests for randomness, over long period bitstreams. This suggests that astronomical data retrieved from celestial sources presents a viable option for use in implementing secure systems, and cryptographic functions such as SHA-256. With the ever increasing demand for secure systems, the need for seed data for random numbers is growing rapidly and our results suggest the large volume of data that is available through radio astronomy offers a scheme for addressing this growing demand.

Further research is necessary to determine the most effective use of this type of astronomical data in cryptographic applications. Examination of other sources to examine the best types of celestial events to collect seed data from, as well as collecting and comparing data from other radio telescopes, would be a prudent next step, as would testing the astronomical data with multiple different RNGs for performance. However, the data presented in this paper offers a feasible beginning to such research.

Acknowledgements

We would like to thank the Institute for Radio Astronomy and Space Research at Auckland University of Technology, for the use of the 30m Warkworth Radio Telescope for the collection of the data used in this research.

REFERENCES

Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S. ., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, *19*(1), 101–111. doi:10.1016/j.cnsns.2013.06.017

Applegate, M. J., Thomas, O., Dynes, J. F., Yuan, Z. L., Ritchie, D. A., & Shields, A. J. (2015). Efficient and robust quantum random number generation by photon number detection. *Applied Physics Letters*, *107*(7), 071106. doi:10.1063/1.4928732

Bartels, R. (1982). The rank version of von Neumann's ratio test for randomness. *Journal of the American Statistical Association*, *77*(377), 40-46.

Burke, B. F., & Graham-Smith, F. (2002). *An introduction to radio astronomy 2ed* (2nd ed.). Cambridge, UK: Cambridge University Press.

Barker, E. B., & Kelsey, J. M. (2015). *Recommendation for random number generation using deterministic random bit generators, (NIST 800-90A rev1)*. Retrieved September 3, 2016, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

Campbell, D. B. (2002). Measurement in Radio Astronomy. *Single-Dish Radio Astronomy: Techniques and Applications*, *278*, 84–85. Retrieved September 17, 2016 from http://adsabs.harvard.edu/full/2002ASPC..278...81C

Cicek, I., Pusane, A. E., & Dundar, G. (2014). A novel design method for discrete time chaos based true random number generators. *Integration, the VLSI Journal*, *47*(1), 38–47. doi:10.1016/j.vlsi.2013.06.003

Cox, D. R., & Stuart, A. (1955). Some quick sign tests for trend in location and dispersion. *Biometrika*, *42*(1/2), 80-95.

Dang, Q. H. (2015). *Secure hash standard (FIPS 180)* (4). Retrieved August 18, 2016, from http://csrc.nist.gov/publications/ fips/fips180-4/fips-180-4.pdf

Dougherty, S. (2011). *Fundamentals of radio astronomy*. Retrieved September 17, 2016, from http://chime.phas.ubc.ca/workshop_penticton/dougherty_Fundementals_2011.pdf

The Editors of Encyclopædia Britannica (2016). Radio source | astronomy. In *Encyclopædia Britannica*. Retrieved September 17, 2016, from https://www.britannica.com/topic/radio-source

Gentle, J. E. (2006). *Random number generation and Monte Carlo methods*.

Haykin, S. (2009). *Communication systems* (4th ed.). New York: John Wiley & Sons.

Hausser, J., & Strimmer, K. (2009). Entropy inference and the James-Stein Estimator, with application to Nonlinear Gene Association networks. *Journal of Machine Learning Research*, *10*(Jul), 1469–1484. Retrieved September 18, 2016, from http://www.jmlr.org/papers/v10/hausser09a.html

Hsu, H. P. (2013). *Schaum's outline of signals and systems, 3rd edition* (Third ed.). United States: McGraw-Hill Professional.

Jansky, C. M., Jr. (1979). My Brother Karl Jansky and his Discovery of Radio Waves from Beyond the Earth. *Cosmic Search*, *1*(4), 12. Retrieved September 16, 2016, from http://www.bigear.org/CSMO/HTML/CS04/cs04p12.htm

Junklewitz, H. (2014). *Statistical inference in Radio Astronomy*. Retrieved September 18, 2016, from https://edoc.ub.uni-muenchen.de/17745/1/Junklewitz_Henrik.pdf

Lo Re, G., Milazzo, F., & Ortolani, M. (2014). Secure random number generation in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *27*(15), 3842–3862. doi:10.1002/cpe.3311

Lunghi, T., Brask, J. B., Lim, C. C. W., Lavigne, Q., Bowles, J., Martin, A., … Brunner, N. (2015). Self-testing quantum random number generator. *Physical Review Letters*, *114*(15), doi:10.1103/physrevlett.114.150501

Lynnyk, V., Sakamoto, N., & Čelikovský, S. (2015). Pseudo random number generator based on the generalized Lorenz chaotic system. *4th IFAC Conference on Analysis and Control of Chaotic Systems CHAOS 2015*, *48*(18), 257–261. doi:10.1016/j.ifacol.2015.11.046

Mateus, A., & Caeiro, F. (2014). An R implementation of several Randomness Tests. *AIP Conf. Proc*, *1618*, 531–534.

McLean, G., & Ministry of Culture and Heritage. (2013, September 3). Warkworth Satellite Earth Station. Retrieved September 18, 2016, from NZ History, http://www.nzhistory.net.nz/media/photo/warkworth-satellite-earth-station

Moore, G. H., & Wallis, W. A. (1943). Time series significance tests based on signs of differences. *Journal of the American Statistical Association*, *38*(222), 153-164.

Murphy, K. (2010, November 19). New Recipe for Famous Dish. Retrieved September 18, 2016, from Telecom NZ Media Releases, https://archive.is/oYVP

Pestalozzi, A. M. R., & Chrysostomou. (2005). *The General Catalogue of 6.7 GHz Methanol Masers in the Galaxy*. Retrieved September 18, 2016, from http://www.lpi.usra.edu/meetings/ppv2005/pdf/8130.pdf

Phillips, C. J., Norris, R. P., Ellingsen, S. P., & McCulloch, P. M. (1998). Methanol masers and their environment at high resolution. *Monthly Notices of the Royal Astronomical Society*, *300*(4), 1131–1157. doi:10.1046/j.1365-8711.1998.t01-1-01979.x

Povich, M. S., Stone, J. M., Churchwell, E., Zweibel, E. G., Wolfire, M. G., Babler, B. L., … Whitney, B. A. (2007). A Multiwavelength study of M17: The spectral energy distribution and PAH emission morphology of a massive Star Formation region. *The Astrophysical Journal*, *660*(1), 346–362. doi:10.1086/513073

Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., … Vo, S. (2010, April). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (1a). Retrieved August 10, 2016, from http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Shuch, P. H. (2013, August 9). Significant radio astronomy frequencies. Retrieved September 20, 2016, from http://www.setileague.org/articles/protectd.htm

Wald, A., & Wolfowitz, J. (1940). On a test whether two samples are from the same population. *The Annals of Mathematical Statistics*, *11*(2), 147-162.

West, N. (2006). GNU Radio Companion (GRC). Retrieved August 8, 2016, from http://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioCompanion

Woodburn, L., Natusch, T., Weston, S., Thomasson, P., Godwin, M., Granet, C., & Gulyaev, S. (2015). Conversion of a New Zealand 30-Metre telecommunications antenna into a radio telescope | Cambridge core. *Publications of the Astronomical Society of Australia*, *32*, doi:10.1017/pasa.2015.13