# On the use of stochastic systems for sensing and security

*by*

Lachlan J. Gunn

Bachelor of Electrical and Electronic Engineering (Hons)
Bachelor of Mathematical and Computer Sciences (Pure)
*The University of Adelaide, 2012*

*Thesis submitted for the degree of*

**Doctor of Philosophy**
*in*
Electrical and Electronic Engineering

*The University of Adelaide*

*2017*

# Contents

# Abstract

No measurement system is perfect, and two varieties of error compete to frustrate their designers and operators. Random errors produce measurement-to-measurement to variation, while systematic errors result in consistently-incorrect results.

The interplay between these two phenomena has been the subject of research for many years, particularly within the area of *stochastic resonance*, which focusses upon cases where the signal-to-noise ratio of a nonlinear system can increase with the addition of noise to its input signal. While it has been demonstrated many times that noise can overcome systematic deficiencies in a measurement system, there remain open questions on how to take advantage of this in practical systems, what information can be extracted, and whether such 'randomised' systems are useful in other settings.

In this thesis, we consider this general theme in the context of two main settings: the adversarial, and the nonadversarial. In both cases, there is a significant advantage to be gained from the use of techniques that are adapted to the problem domain, in contrast to previous ad-hoc approaches that have failed to take advantage of the structures of the problems at hand.

The first part of this thesis considers the elimination of static nonlinearity from noisy measurements. We start with the phenomenon of 'classical' stochastic resonance, showing how input noise can be used to linearise the response of a nonlinear system. This phenomenon has been observed in the past, however we demonstrate that the use of nonlinear signal processing allows the linearisation to take place with far smaller levels of noise. We then investigate several approaches to the implementation of this technique, with the aim of supporting real-time operation in embedded systems and VLSI.

The remainder of the thesis concerns the use of randomness in measurements made as part of adversarial systems. This can be split into two situations: that where the operation of a system requires that measurement be difficult, and that where measurement must be straightforward. We first discuss the Kish key distribution system, a proposed classical alternative to quantum key distribution. This system claims to derive its security from the second law of thermodynamics, however these claims have been the subject of controversy. We examine the claims in detail, and show that the use of random signals does not render implausible the measurement of the system state.

Finally, we describe a number of approaches to the topical problems of key distribution and identity verification. We show how various forms of multi-path probing can be treated as a form of random sampling; much like in the first section, this randomness allows for the characterisation of systematic errors, in this case the consistent changes introduced by an attacker. We then compute bounds on the probability that an attacker achieves a deception against a user taking part in this sampling process.

The first approach that we consider uses an anonymising system such as Tor or a mix-net; if all users make anonymous requests to a service in lock-step, then a malicious service cannot guarantee a self-consistent set of responses to anyone without providing the malicious response to all users. This allows the development of a statistically guaranteed consensus, and thus permits auditors to assure themselves that they have examined the same data as has been provided to other users. This provides an attractive alternative to blockchain technology, avoiding the complexity of the proof-of-work and proof-of-stake-based systems that dominate the landscape today.

We have developed a second approach that allows the random-sampling approach to be used with the existing public-key infrastructure. By demonstrating that the entities chosen to carry out the verification of an identity holder are selected at random from a substantial number of independent entities, relying parties can be confident that small numbers of compromised verifiers cannot unilaterally issue certificates for identities that they do not hold. This provides a basis for the development of highly robust distributed certificate issuance systems that do not share the current 'weakest-link' nature of the existing public-key infrastructure.

Ultimately, these systems all hold in common the use of randomness in their measurement conditions in order to characterise systematic effects. While this phenomenon has been acknowledged, its potential to characterise real systems has until now not been realised. We demonstrate that randomness, whether natural and unavoidable or artificially introduced, can ironically render far more predictable the behaviour of many systems, and in more realistic situations than have been seen in the literature to date.

# Statement of Originality

I certify that this work contains no material which has been accepted for the award of any other degree or diploma in my name, in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. In addition, I certify that no part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of the University of Adelaide and where applicable, any partner institution responsible for the joint-award of this degree.

I give consent to this copy of my thesis when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

I acknowledge that copyright of published works contained within this thesis resides with the copyright holder(s) of those works.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

I acknowledge the support I have received for my research through the provision of an Australian Government Research Training Program Scholarship, and an Endeavour Research Fellowship.

2017-09-05

Signed

Date

# Acknowledgments

This thesis is the culmination of several years of work, but would not exist without the tremendous support of a great many people and organisations.

*Primary Supervision*

Above all, the greatest of thanks go to my supervisors, Derek Abbott and Andrew Allison, to whom I owe much of my academic development; it was they who bore the weighty responsibility of transforming a newly-graduated engineer into an academic, and without their endless toil and advice, I would not have reached this point.

*Supervision in Angers*

During my PhD, I was fortunate enough to spend six months at the University of Angers, under François Chapeau-Blondeau. His excellent supervision helped give me new perspective on my work, making my time in Angers some of the most productive of my Ph.D.

*Funding Sources*

Thanks are also due to the Australian Government for the award of an *Australian Postgraduate Award* in 2013 and an *Endeavour Research Fellowship* in 2015, as well as to the School of Electrical and Electronic Engineering of the University of Adelaide for providing travel funding.

I would also like to thank the Australian Mathematical Sciences Institute, who organised and supported my attendance at the *2014 AMSI Summer School*. As well as the courses presented at this event, the interesting discussions that I had with both fellow students and giants of the field, such as Daniel J. Bernstein and Tanja Lange, were most illuminating, and it is to this opportunity—giving me the chance to see the points of view of proponents of both conventional and alternative approaches to cryptography—more than anything else that I owe the perspective on cybersecurity that I have gained throughout the course of my research.

*Coauthors*

I owe also a great deal to those with whom I have collaborated over the last few years, both in Australia and abroad. In particular, I offer my thanks to Waddah Al-Ashwal, M. Ali Babar, François Chapeau-Blondeau, James Chappell, Bruce Davis, Alex Dinovitser, Samuel Drake, Fabing Duan, John Hartnett, Azhar Iqbal, Mark MacDonnell, Olaf Maennel, Heiki Pikker, Cameron Seidel, Tony Vladusich, and Liyan Xu.

*Talks and Visits*

I have been graciously hosted by and given talks to number of research groups. While space restricts me from listing all those with whom I have had so many most stimulating discussions, I would like to give credit to my hosts: Nigel Stocks, University of Warwick; Peter McClintock and Aneta Stefanovska, University of Lancaster; Jason Ralph, University of Liverpool; Raúl Toral, University of the Balearic Islands; Juan Parrondo, Complutense University of Madrid; François Chapeau-Blondeau, University of Angers; Luigi Fortuna, University of Catania; and Zoltan Gingl and Robert Mingesz, University of Szeged.

*Technical Discussions*

Beyond this, I owe much to those with whom I have had many technical discussions; this was especially so with Laszlo Kish, who introduced the system that occupies most of Chapter 4, and with whom I have had many stimulating discussions that have contributed greatly to the shape that my work has taken. Robert Bogner, Tobias Eggendorfer, and Matthew Sorell all deserve mention for useful discussions regarding various aspects of my research.

*Technical Staff*

Returning to home, there are many others at the University of Adelaide who have contributed to the research underlying this thesis in one way or another. The technical staff of the School of Electrical and Electronic Engineering are particularly notable; Danny Di Giacomo, Alban O'Brien, Ian Linke, Brandon Pullen, Pavel Simcik, and Aubrey Slater have aided me immeasurably in realising my constructions.

*Other Staff*

Much vital support was provided by the administrative staff of the School of Electrical and Electronic Engineering. None more so than Rose-Marie Descalzi, whose responsibility for travel and seminars resulted in a near-constant barrage of talk proposals and overly-complicated itineraries. But thanks are equally due to the others who keep the machine of the department running, and in particular to David Bowler, Franca Guest, Stephen Guest, Deb Koch, Mark Innes, Jodie Schluter, and Pavel Simcik.

*Personal Thanks*

In addition to these professional credits, thanks are also due to the family and friends who have supported me throughout these last few years. Without them, I would not have reached the beginning of my Ph.D, let alone the end.

# Conventions

This thesis is typeset using the LuaTEX and LATEX2e software. Harvard style is used for referencing and citation. Australian English spelling is adopted, as defined by the Macquarie English Dictionary (Delbridge 2001).

Acronyms are given in small caps—e.g. ADC, PDF—where this does not create ambiguity. Exceptions generally involve plurals, e.g. ADC/ADCs.

The main text is typeset in *Minion Pro*, with the mathematics set in *TEX Gyre Pagella*. Figure captions and other sans-serif text are set in *Charlotte Sans*.

# Publications

*Papers marked ▸ are directly relevant to this thesis.*

## JOURNAL PAPERS


1. ▸ L. J. Gunn, A. Allison, and D. Abbott (2013). Identification of static distortion by noise measurement. *Electronics Letters* 49(21), pp. 1321–1323. DOI: 10.1049/el.2013.2547
2. L. J. Gunn, P. G. Catlow, W. A. Al-Ashwal, J. G. Hartnett, A. Allison, and D. Abbott. Simplified three-cornered-hat technique for frequency stability measurements. *IEEE Transactions on Instrumentation and Measurement* 63(4), pp. 889–895. DOI: 10.1109/tim.2013.2285796
3. J. M. Chappell, S. P. Drake, C. L. Seidel, L. J. Gunn, A. Iqbal, A. Allison, and D. Abbott (2014). Geometric algebra for electrical and electronic engineers. *Proceedings of the IEEE* 102(9), pp. 1340–1363. DOI: 10.1109/jproc.2014.2339299
4. ▸ L. J. Gunn, A. Allison, and D. Abbott (2014a). A directional wave measurement attack against the Kish key distribution system. *Scientific Reports* 4. Art. 6461. DOI: 10.1038/srep06461
5. A. Dinovitser, L. J. Gunn, and D. Abbott (2015). Towards quantitative atmospheric water vapor profiling with differential absorption lidar. *Optics Express* 23(17), pp. 22907–22921. DOI: 10.1364/OE.23.022907
6. L. Xu, T. Vladusich, F. Duan, L. J. Gunn, D. Abbott, and M. D. McDonnell (2015). Decoding suprathreshold stochastic resonance with optimal weights. *Physics Letters A* 379(38), pp. 2277–2283. DOI: 10.1016/j.physleta.2015.05.032
7. ▸ L. J. Gunn, A. Allison, and D. Abbott (2015b). A new transient attack on the Kish key distribution system. *IEEE Access* 3, pp. 1640–1648. DOI: 10.1109/access.2015.2480422
8. ▸ L. J. Gunn, F. Chapeau-Blondeau, M. D. McDonnell, B. R. Davis, A. Allison, and D. Abbott (2016d). Too good to be true: when overwhelming evidence fails to convince. *Proceedings of the Royal Society A* 472(2187). DOI: 10.1098/rspa.2015.0748

### CONFERENCE PAPERS

1. ► L. J. Gunn, J. M. Chappell, A. Allison, and D. Abbott (2014c). Physical-layer encryption on the public internet: a stochastic approach to the Kish-Sethuraman cipher. *International Journal of Modern Physics: Conference Series* 33. Presented at HotPI-2013. DOI: 10.1142/S2010194514603615
2. ► L. J. Gunn, A. Allison, and D. Abbott (2014b). Allison mixtures: where random digits obey thermodynamic principles. *International Journal of Modern Physics* 33. Presented at Hot Topics in Physical Informatics 2013. DOI: 10.1142/S2010194514603603
3. J. M. Chappell, L. J. Gunn, and D. Abbott (2013). The double-padlock problem: is secure classical information transmission possible without key exchange? Presented at Hot Topics in Physical Informatics. DOI: 10.1142/S201019451460355X
4. ► L. J. Gunn, A. Allison, and D. Abbott (2015a). "Real-time compensation of static distortion by measurement of differential noise gain". *Proc. IEEE Workshop on Signal Processing Systems*. Belfast, United Kingdom. DOI: 10.1109/SiPS.2014.6986079
5. ► L. J. Gunn, F. Chapeau-Blondeau, A. Allison, and D. Abbott (2016c). Towards an information-theoretic model of the allison mixture stochastic process. *Journal of Statistical Mechanics: Theory and Experiment* 2016(5). DOI: 10.1088/1742-5468/2016/05/054041
6. ► L. J. Gunn, A. Allison, and D. Abbott (2017). "Safety in numbers: anonymization makes keyservers trustworthy". *10th Workshop on Hot Topics in Privacy Enhancing Technologies*. Minneapolis, USA[1]

[1]See Gunn et al. (2016a) for the full paper.

# List of Figures

# List of Tables