

# 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

© 2013–2017  
Lachlan J. Gunn  
All Rights Reserved



# Contents

<b>Contents</b>	<b>iii</b>
<b>Abstract</b>	<b>ix</b>
<b>Statement of Originality</b>	<b>xi</b>
<b>Acknowledgments</b>	<b>xiii</b>
<b>Conventions</b>	<b>xv</b>
<b>Publications</b>	<b>xvii</b>
<b>List of Figures</b>	<b>xix</b>
<b>List of Tables</b>	<b>xxv</b>
<b>Chapter 1. Introduction</b>	<b>1</b>
1.1 Introduction . . . . .	2
1.2 Thesis outline . . . . .	2
1.3 Motivation . . . . .	3
1.4 Background . . . . .	4
1.4.1 System identification . . . . .	4
1.4.2 Cryptography . . . . .	5
1.5 Original contributions . . . . .	12
<b>Chapter 2. Decisions, Failures, and Stochastic Systems</b>	<b>13</b>
2.1 Introduction . . . . .	14
2.2 Analysis of a biased coin . . . . .	15
2.3 A hypothetical Roman pot . . . . .	16
2.3.1 Formal model . . . . .	17

- 2.3.2 Analysis of the pot origin distribution . . . . . 17
- 2.4 The reliability of identity parades . . . . . 19
- 2.5 Ancient judicial procedure . . . . . 22
- 2.6 The reliability of cryptographic systems . . . . . 24
  - 2.6.1 Code changes caused by memory errors . . . . . 24
  - 2.6.2 The effect of memory errors on confidence . . . . . 26
- 2.7 Discussion . . . . . 28
- 2.8 Conclusion . . . . . 29
  - 2.8.1 Original contributions . . . . . 30

**Chapter 3. Nonlinear Sensing 31**

- 3.1 Introduction . . . . . 32
  - 3.1.1 Why sense in a nonlinear regime? . . . . . 32
- 3.2 Characterisation of nonlinearity in metrology . . . . . 32
  - 3.2.1 Direct response measurement . . . . . 33
  - 3.2.2 Histogram measurement . . . . . 33
- 3.3 Linearisation by noise measurement . . . . . 34
  - 3.3.1 Method . . . . . 34
  - 3.3.2 Estimation of the derivative . . . . . 35
  - 3.3.3 Harmonic distortion . . . . . 36
  - 3.3.4 Static error . . . . . 36
- 3.4 Optimisation for real-time use . . . . . 39
  - 3.4.1 Implementation . . . . . 41
- 3.5 Adaptation for resource-constrained environments . . . . . 46
  - 3.5.1 Results . . . . . 49
- 3.6 Conclusion . . . . . 51
  - 3.6.1 Original contributions . . . . . 51

**Chapter 4. Noise-based Communication 53**

- 4.1 Key establishment . . . . . 54
- 4.2 Security definitions . . . . . 54

4.3	Classical key establishment protocols . . . . .	56
4.3.1	Diffie-Hellman . . . . .	56
4.3.2	RSA public-key encryption . . . . .	57
4.3.3	Shamir’s three-pass protocol . . . . .	58
4.4	A physical implementation of the Shamir three-pass protocol . . . . .	60
4.4.1	The mutual information rate between endpoints . . . . .	61
4.4.2	Limitations . . . . .	62
4.4.3	Experimental Round-Trip Measurements . . . . .	63
4.4.4	Demonstration System . . . . .	64
4.5	The Kish key distribution system . . . . .	66
4.6	Attacking KKD with wave measurement . . . . .	68
4.6.1	Experimental apparatus . . . . .	70
4.6.2	Circuit analysis . . . . .	72
4.6.3	Statistical processing . . . . .	73
4.6.4	Experimental results . . . . .	75
4.6.5	Proposed countermeasures and alternative explanations . . . . .	75
4.6.6	Discussion . . . . .	82
4.7	Attacking KKD with propagation sensing . . . . .	82
4.7.1	Quantification of attack effectiveness . . . . .	82
4.7.2	Nonidealities in the lumped model . . . . .	87
4.7.3	Transient attacks . . . . .	88
4.7.4	Propagation delays and temperature mismatch . . . . .	89
4.7.5	Leak analysis . . . . .	91
4.7.6	Countermeasures to the transient attack . . . . .	93
4.8	Remarks on the proposed KKD proof of security . . . . .	94
4.8.1	Parametrisation of the design . . . . .	95
4.8.2	Continuity argument . . . . .	96
4.9	Conclusion . . . . .	97
4.9.1	Original contributions . . . . .	98

- 5.1 Public-key distribution: the *status quo* . . . . . 102
  - 5.1.1 The public-key infrastructure . . . . . 102
  - 5.1.2 PKI failure modes . . . . . 103
  - 5.1.3 The Web of Trust . . . . . 105
  - 5.1.4 Identity-based cryptography . . . . . 106
- 5.2 Anonymous Auditing . . . . . 106
  - 5.2.1 Motivation . . . . . 108
  - 5.2.2 Related work . . . . . 108
  - 5.2.3 Verification protocol . . . . . 111
  - 5.2.4 Security Analysis . . . . . 112
  - 5.2.5 Anonymisation methods . . . . . 124
  - 5.2.6 Discussion . . . . . 130
  - 5.2.7 Implementation . . . . . 132
- 5.3 Distributed certificate issuance . . . . . 134
  - 5.3.1 Preliminaries . . . . . 137
  - 5.3.2 Random verification . . . . . 138
  - 5.3.3 Success over time in gaining false certificates . . . . . 141
  - 5.3.4 Avoidance of repeated requests . . . . . 142
  - 5.3.5 Implementation . . . . . 144
- 5.4 Conclusion . . . . . 146
  - 5.4.1 Original contributions . . . . . 146

**Chapter 6. Conclusions and Future Directions 147**

- 6.1 Conclusions and contributions . . . . . 148
- 6.2 Future work . . . . . 149
  - 6.2.1 Failure modes of stochastic systems . . . . . 150
  - 6.2.2 Nonlinear sensing . . . . . 150
  - 6.2.3 Noise-based communications . . . . . 151
  - 6.2.4 Stochastic approaches to identity management . . . . . 151

**Appendix A. KKD Attack Apparatus 153**

---

A.1	The hardware platform . . . . .	154
A.2	Theory of operation . . . . .	154
A.3	Design . . . . .	155
A.3.1	Analogue frontend . . . . .	155
A.3.2	ADC interface . . . . .	156
A.3.3	DSP Framework . . . . .	156
A.3.4	DSP . . . . .	157
A.3.5	Communications . . . . .	158
A.3.6	Noise generation . . . . .	158
A.4	Operation . . . . .	158
A.4.1	KKD experiment operation . . . . .	159
A.4.2	Testing . . . . .	162
A.5	SCPI command reference . . . . .	164
A.5.1	General commands . . . . .	164
A.5.2	:MEASure commands . . . . .	164
A.5.3	:SENSe commands . . . . .	165
A.5.4	:OUTPut commands . . . . .	166
A.6	Schematics . . . . .	166
A.7	Software build environment . . . . .	172

**Appendix B. Source Code** **173**

B.1	Nonlinear sensing . . . . .	174
B.1.1	Floating-point implementation . . . . .	174
B.2	Noise-based Communications . . . . .	181
B.2.1	Directional coupler . . . . .	181
B.2.2	Round-trip-time measurement engine . . . . .	190
B.2.3	Round-trip-time key establishment system . . . . .	192

**Appendix C. The Allison Mixture** **201**

C.1	Linear statistics of the Allison Mixture . . . . .	202
C.1.1	The Allison mixture . . . . .	202

## Contents

---

C.1.2	Numerical results . . . . .	206
C.2	Information-theoretic analysis of the Allison Mixture . . . . .	207
C.2.1	The Allison mixture . . . . .	207
C.2.2	Autoinformation of the Allison mixture sampling process . . . . .	209
C.2.3	Open questions . . . . .	211
<b>Bibliography</b>		<b>213</b>
<b>Acronyms</b>		<b>227</b>
<b>Index</b>		<b>229</b>
<b>Biography</b>		<b>233</b>



# Abstract

No measurement system is perfect, and two varieties of error compete to frustrate their designers and operators. Random errors produce measurement-to-measurement 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.

Signed

2017-09-05

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.

Above all, the greatest of thanks go to my supervisors, Derek Abbott and Andrew Allison, to whom I owe much of my academic development; *Primary Supervision* 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.

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

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. *Funding Sources*

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.

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 *Coauthors* 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 Lua $\text{T}_{\text{E}}\text{X}$  and  $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}2_{\text{e}}$  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 *T<sub>E</sub>X 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/e1.2013.2547
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 key servers trustworthy”. *10th Workshop on Hot Topics in Privacy Enhancing Technologies*. Minneapolis, USA<sup>1</sup>

---

<sup>1</sup>See Gunn et al. (2016a) for the full paper.

# List of Figures

1.1	Measurement bases for BB84. One of the four basis vectors is selected at random, and sent to the recipient, Bob, in the form of a single polarised photon. If the photon is measured with the wrong measurement basis, the measurement will be wrong 50% of the time. . . . .	7
<hr/>		
2.1	Prior and posterior distributions of the heads-probability of a biased coin. We suppose a prior distribution of $H \sim \mathcal{N}(0.5, 0.05)$ . Because the tails of the Gaussian distribution are not heavy, the posterior distribution moves only very slowly away from the unbiased value of 0.5. . . . .	15
2.2	Probability that the pot is of British origin given $n$ numbers of tests, all coming back positive, for a variety of contamination rates $p_c$ and a 30% error rate. In the case of the pot above, with $p_c = 10^{-2}$ , we see a peak at $n = 5$ , after which the level of certainty falls back to 0.5 as it becomes more likely that the pot originates at a contaminating factory. When $p_c = 0$ , this is the standard Bayesian analysis where failure states are not considered. We see therefore that even small contamination rates can have a large effect on the global behaviour of the testing methodology. . . . .	19
2.3	Probability of guilt given varying numbers of unanimous line-up identifications, assuming a 50% prior probability of guilt and identification accuracies given by Foster et al. (1994). Of note is that for the case that we have plotted here where the witnesses are unanimous, with a failure rate $p_c = 0.01$ it is impossible to reach 95% certainty in the guilt of the suspect, no matter how many witnesses have been found. . . . .	22

2.4	Probability of guilt as a function of judges in agreement out of 23—the number used by the Sanhedrin for most capital crimes—for various contamination rates $p_c$ . We assume as before that half of defendants are guilty, and use the estimated false-positive and false-negative rates of juries from Spencer (2007, model (2)), 0.14 and 0.25 respectively. We arbitrarily assume that a ‘contaminated’ trial will result in the a positive vote 95% of the time. The panel of judges numbers 23, with conviction requiring a majority of two and at least one dissenting opinion (Epstein 1961, Sanhedrin), thus requiring 13 to 22 votes inclusive in order to secure a conviction, as shown in the graph. . . . .	23
2.5	A function that tests for primality by attempting to factorise its input by brute force. . . . .	25
2.6	The acceptance rate as a function of time in memory and the number of Rabin-Miller iterations under the single-error fault model described in this thesis. An acceptance rate of $2^{-128}$ is normally chosen, however without error correction this cannot be achieved. The false-acceptance rate after $k$ iterations is given by $p_{fa}[k] = 4^{-k}(1 - p_f) + p_f$ , where $p_f$ is the probability that a fault has occurred that causes a false acceptance 100% of the time. We estimate $p_f$ to be equal to $10^{-19}T$ , where $T$ is the length of time in seconds that the code has been in memory. . . . .	27
—————		
3.1	Experimentally-noise-estimated amplifier voltage transfer function . . . . .	36
3.2	THD of amplified signal before and after naïvely-implemented nonlinear compensation . . . . .	37
3.3	Static error of the amplifier output before and after compensation, with quantisation noise included . . . . .	38
3.4	Static error of the amplifier output before and after compensation, with quantisation noise removed . . . . .	38
3.5	Basis functions used for differential gain approximation . . . . .	39
3.6	Block diagram of the adaptive real-time nonlinear compensator . . . . .	40
3.7	Distortion compensator experimental setup . . . . .	42
3.8	Real-time compensation of a distorted triangle wave . . . . .	42
3.9	INL and DNL of amplifier before and after real-time compensation . . . . .	44
3.10	Amplifier THD before and after compensation . . . . .	45

3.11	Distorted sinusoid before and after real-time compensation . . . . .	45
3.12	Compensating function construction for high-speed evaluation . . . . .	47
3.13	Feedback-based algorithm for nonlinear compensator . . . . .	48
3.14	Test setup for feedback-based nonlinear compensator . . . . .	50
3.15	THDs before and after feedback-based compensation of distorted sinusoid .	51
—————		
4.1	The basic Diffie-Hellman key-establishment protocol. In this diagram, $\$$ denotes the selection of a random element from the set to the right, $(G, \cdot)$ is a finite cyclic group of order $p$ , and $g$ a generator for the group. . . . .	57
4.2	Timestamping events for round-trip-time measurements . . . . .	60
4.3	Round-trip time distribution . . . . .	61
4.4	Server locations in round-trip-time measurement system . . . . .	64
4.5	Bit-error-rates of timing-based protocol after information reconciliation . .	65
4.6	The KKD system under analysis. . . . .	66
4.7	The four possible resistor states. Each time the protocol is run, the two switches are set at random, placing the system into one of the four states shown; at the bottom of each square is the mean-square line voltage for $R_a = 1\ \Omega$ , $R_b = 2\ \Omega$ , and $4kTB = 2$ ; this is only for illustrative purposes, and in practice the resistors will be of the order of several kilo-ohms. Two of the states are indistinguishable by an eavesdropper measuring only $\langle V^2 \rangle$ , while Alice and Bob, who know their own selected resistor values, and so which row and column respectively the true state is in, can distinguish all four states. When running the protocol, Alice and Bob simply agree to drop any insecure bits from the generated random key. . . . .	67
4.8	Directional measurement analog frontend . . . . .	69
4.9	DSP block diagram of directional wave measurement device . . . . .	71
4.10	An $s$ -parameter model of the KKD system. . . . .	72
4.11	Log likelihood-ratio test statistics for the KKD attack measurements . . . . .	76
4.12	Simulated eavesdropper error rates for the KKD system with attenuation . .	77
4.13	Directional coupler as constructed . . . . .	78
4.14	Coupler apparatus frequency response . . . . .	79
4.15	Measured eavesdropper BER for attenuation attack . . . . .	80

## List of Figures

---

4.16	KKD schematic with component values . . . . .	86
4.17	Secrecy rate of simulated KKD system with finite line resistance . . . . .	88
4.18	Secrecy rate of ideal KKD system with voltage mismatch . . . . .	89
4.19	Apparent kkd noise temperatures as a function of time . . . . .	90
4.20	Mismatch of apparent temperatures in KKD system at startup . . . . .	91
4.21	Error rates of KKD resistor estimation via apparent temperature mismatch .	93
4.22	KKD secrecy rate with an eavesdropper using the transient attack . . . . .	94
4.23	A resistive circuit containing two secret DC voltage sources $V_1$ and $V_2$ , each with a series resistance of $1\ \Omega$ . An eavesdropper can measure the voltage at two points on the line, yielding voltages $V_x$ and $V_y$ , which determine $V_1$ and $V_2$ if and only if $R \neq 0$ . . . . .	96
<hr/>		
5.1	Failure modes for a certificate or registration authority. The cases are split according to whether or not the authority's systems were bypassed in producing the certificate, whether, if not, the operators knowingly issued a false certificate, and whether, if the authority systems were bypassed, it was because the attacker gained control of the issuance systems or because of a cryptographic failure. The observed probabilities of various failure modes are estimated by categorising thirteen known incidents that resulted in attackers fraudulently obtaining a certificate. We denote the observed probability of an event $p$ , and the number of occurrences of an event $N$ . . . . .	103
5.2	Interpretation of the results obtained from the protocol. Clients that have not received consistent responses from the server reject the response from the server, which they know to be faulty. Clients that have consistently received the same response accept it as unequivocated. In this figure, the server has equivocated, with the third and fourth clients being unaware of the fact and the others detecting the misbehavior of the service. . . . .	112

---

5.3	A model of an anonymously-accessed service, where $\mathcal{A}$ is the potentially-malicious service, and $\mathcal{L}$ is a leakage function that captures the information leaked to the adversary. In the case of Tor, for example, $\mathcal{L}$ is the user-to-request mapping $R_I$ with its domain restricted to users whose entry guards are surveilled by the attacker. The service accepts a set of users, and selects a random mapping from users to request identifiers. The adversary is given system-dependent partial information on the source of each request, and invited to provide a response to each request. . . . .	113
5.4	Security experiment for sender-anonymity. An anonymity system, defined by its leakage function $\mathcal{L}$ , is used to make requests to an adversary who aims provide particular messages to particular users. The adversary is asked to determine the users to whom each of its responses were sent; it wins if it correctly identifies all of the recipients. . . . .	115
5.5	Connecting to a public keyserver via Tor and via a mix-net. The user randomly selects several relays, then adds a layer of encryption for each relay. After receiving a message, the relays strip their layer of encryption, revealing the address of the next relay. Eventually, the message reaches an <i>exit node</i> , which passes it to the open internet. Anyone can contribute nodes to the network—including adversaries—however as the routing path is selected by the user, an attacker cannot gain access to the encrypted messages with probability better than chance. Mix-nets are composed of a chain of <i>mixes</i> , which take batches of messages, remove a layer of encryption, shuffle the messages, then pass them to a new mix. If at least one mix in the chain is honest, then an attacker cannot connect messages to their senders with probability better than chance. . . . .	125
5.6	Waiting-time necessary to achieve various levels of security. We show the hypothesized Certificate Transparency system modelled on the Chrome auto-update mechanism (top), our proposed keyserver-auditing system (middle), and our conception of how a keyserver built on something like Continuous Identity and Key Management System (CONIKS) might look (bottom). We see that very small probabilities of equivocation are achieved within only a few hours, such that deanonymisation and endpoint compromise quickly become far more likely than chance success by a malicious service. . . . .	133
5.7	Certificate issuance protocol . . . . .	139
5.8	Probability of selecting colluding verifiers at random . . . . .	140

---

5.9	Probability of obtaining a false certificate with imperfect verifiers . . . . .	141
5.10	Architecture of distributed CA prototype . . . . .	144
-----		
A.1	Status LEDs on STM32F4DISCOVERY board. . . . .	159
A.2	Measured log-likelihood ratios from KKD test system, as in (4.41), vs. sample number. The red dots represent a single test with the system configured with a key bit of '1', and the blue dots with a key bit of zero. The clear separation demonstrates the distinguishability of the two cases. . . . .	161
-----		
-----		
C.1	The Markov chain defining the sampling process $S_t$ of the Allison mixture. It is parametrised by the probabilities $\alpha_0$ and $\alpha_1$ of leaving states 0 and 1 respectively. When in state one, its value is equal to that of the first process $U$ , and when in state two to that of the second $V$ . . . . .	203
C.2	The autocorrelation coefficient of the Allison mixture of $N(-10, 1)$ and $N(10, 1)$ for various values of $\alpha_1$ and $\alpha_2$ . The thick line shows the case $\alpha_1 + \alpha_2 = 1$ in which the autocorrelation coefficient is zero. . . . .	206
C.3	The Allison mixture of $N(-10, 1)$ and $N(10, 1)$ with varying parameters $\alpha_i$ . In (a) the low probability of switching causes the process to stay with its current input for long periods of time. The autocorrelation coefficient is large and positive. Conversely, in (a) the probability of switching is high, causing the sampling operation to flit between the two processes almost every cycle. The autocovariance is large and negative. . . . .	207
C.4	Single-step autoinformation $I_{SS}[1]$ of the Allison mixture sampling process $S_t$ as a function of the transition probabilities $\alpha_0$ and $\alpha_1$ , calculated according to Equation C.47. Note the lines of zero autoinformation along $\alpha_0 = 0$ , $\alpha_1 = 0$ , and $\alpha_0 + \alpha_1 = 1$ . . . . .	211
C.5	The exponentially-decaying autoinformation $I_{SS}[k]$ and autocovariance $R_{SS}[k]$ of an Allison mixture sampling process with $\alpha_0 = 0.1, \alpha_1 = 0.1$ . The slope of the autoinformation line is approximately double that of the autocorrelation line; the results of Chapeau-Blondeau (2007) hint that this may be exactly so asymptotically. . . . .	212



# List of Tables

2.1	The model parameters for the case of the pot for use in (2.3) with a contamination rate $p_c = 10^{-2}$ . The <i>a priori</i> distribution of the origin is identically 50% for both Britain and Italy, whether or not the pot's manufacturing process has contaminated the results. As a result, the two columns of $P[F, H_i]$ are identical. The columns of the measurement distribution, shown right, differ from one another, thereby giving the test discriminatory power. When the pot has been contaminated, the probability of a positive result is identical for both samples, rendering the test ineffective. . . . .	18
2.2	The model parameters for the hypothetical identity parade. In a similar fashion to the first example, we assume <i>a priori</i> a 50% probability of guilt. In this case, the measurement distributions are substantially assymmetric with respect to innocence and guilt, unlike Table 2.1. . . . .	21
2.3	The model parameters for the Sanhedrin trial. Again, we assume an <i>a priori</i> 50% probability of guilt. However, the measurement distributions are the results of Spencer (2007, model (2)) for juries; in contrast to the case of the identity parade, the false negative rate is far lower. Despite the trial being conducted by judges, we choose to use the jury results, as the judges tendency towards conviction is not reflected in the highly risk-averse rabbinic legal tradition. . . . .	23
2.4	Model parameters for the Rabin-Miller test on random 2000-bit numbers. However, we have no choice but to assume the lower bound on the composite-number rejection rate, and so this model is inappropriate. Furthermore, in an adversarial setting the attacker may intentionally choose a difficult-to-detect composite number, rendering the prior distribution optimistic. . . . .	26
4.1	Values of $1 - \Gamma^2$ for various choices of resistor. A characteristic impedance of $50 \Omega$ is assumed. . . . .	92
5.1	Costs and security of the proposed protocol for literal-data and Merkle Tree systems. . . . .	131