

RUHR-UNIVERSITÄT BOCHUM

Generating Secure Cryptographic Keys Derived from Channel Properties

Tobias Bock

Bachelor's Thesis – September 16, 2013.
Chair for Digital Communication Systems.

1st Supervisor: Prof. Dr.-Ing. Aydin Sezgin
2nd Supervisor: Prof. Dr.-Ing. Christof Paar
Advisors: M. Sc. Hendrik Vogt
M. Sc. Christian Zenger



Abstract

[...]

Eidesstattliche Erklärung

Ich erkläre, dass ich keine Arbeit in gleicher oder ähnlicher Fassung bereits für eine andere Prüfung an der Ruhr-Universität Bochum oder einer anderen Hochschule eingereicht habe. Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen, die anderen Quellen dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen kenntlich gemacht. Dies gilt sinngemäß auch für verwendete Zeichnungen, Skizzen, bildliche Darstellungen und dergleichen. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Ich erkläre mich damit einverstanden, dass die digitale Version dieser Arbeit zwecks Plagiatsprüfung verwendet wird.

Official Declaration

Hereby I declare that I have not submitted this thesis in this or similar form to any other examination at the Ruhr-Universität Bochum or any other institution or university. I officially ensure that this paper has been written solely on my own. I herewith officially ensure that I have not used any other sources but those stated by me. Any and every parts of the text which constitute quotes in original wording or in its essence have been explicitly referred by me by using official marking and proper quotation. This is also valid for used drafts, pictures and similar formats. I also officially ensure that the printed version as submitted by me fully confirms with my digital version. I agree that the digital version will be used to subject the paper to plagiarism examination. Not this English translation but only the official version in German is legally binding.

Datum/Date

Unterschrift/Signature

Contents

1	Introduction	1
1.1	Motivation	1
1.2	Related Work	1
1.3	Contribution	1
1.4	Outline	1
2	Theoretical Background	3
2.1	Fundamentals	3
2.1.1	Entropy	3
3	Simulation	5
3.1	Some Stuff	5
4	Evaluation	7
4.1	Comparing Signal Properties	7
5	Conclusion	9
5.1	Summary	9
5.2	Future Work	9
A	Appendix	11
B	Acronyms	15
	List of Figures	17
	List of Tables	19
	List of Algorithms	21
	List of Listings	23
	List of Formulas	25
	Bibliography	27

1 Introduction

[...]

1.1 Motivation

1.2 Related Work

1.3 Contribution

1.4 Outline

2 Theoretical Background

[...]

2.1 Fundamentals

For comparing different signals there exist several methods. We can either directly compare two (or more) different signals by, e. g., calculating the *mutual information*, *Bit Disagreement Probability (BDP)* or *cross-correlation function*, or we can compute the *entropy* of both signals and contrast them.

2.1.1 Entropy

Entropy measures the *uncertainty* of a random variable and was firstly described by Shannon in his fundamental paper in 1948 [36]. Let us assume we have a random variable X and its correspondent alphabet \mathcal{X} . Additionally, the probability for a random variable $x_i \in \mathcal{X}$ to occur is denoted as $p(x_i)$.

Definition 2.1 (Entropy) *The entropy $H(X)$ of a discrete random variable X is given as*

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log p(x). \quad (2.1)$$

Usually the logarithm is to base 2 and the unit of entropy is bits. We see that the content of x is completely irrelevant, whereas we only need know to the *probability* of that variable to occur.

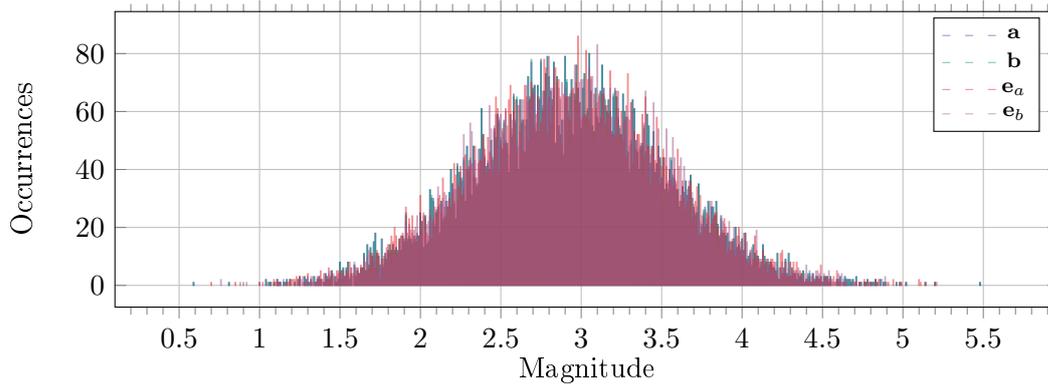
[...]

3 Simulation

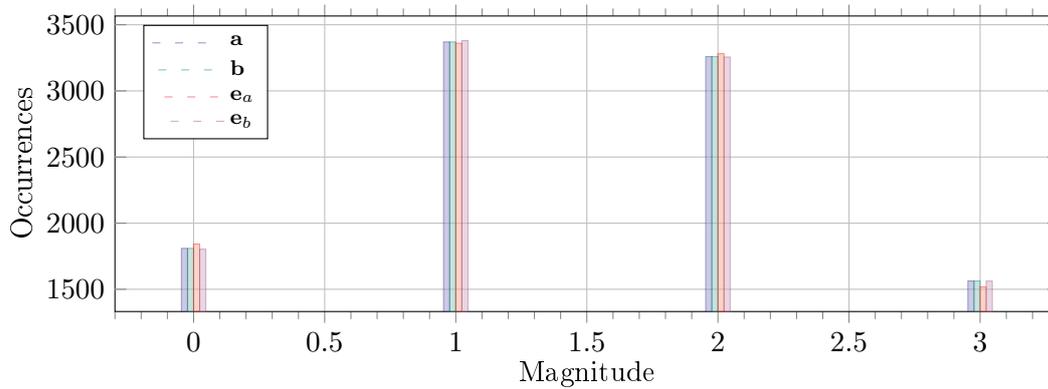
[...]

3.1 Some Stuff

[...]



(a) Signals produced by the source.



(b) Signal distribution after quantizing. Plots are shifted for readability reasons; the only symbols produced by the quantizer are 0, 1, 2, and 3.

Figure 4.1: Value distribution of each signal.

4 Evaluation

[...]

4.1 Comparing Signal Properties

[...]

Figure 4.1 shows the value distribution of the signals at the source and after quantization.

4 Evaluation

[...]

5 Conclusion

[...]

5.1 Summary

[...]

5.2 Future Work

[...]

A Appendix

SHA-512: Constants

Table A.1: Constants used during the calculation of a SHA-512 hash value.

Constant	Value (hexadecimal)	Constant	Value (hexadecimal)
K_0	428a2f98d728ae22	K_{30}	06ca6351e003826f
K_1	7137449123ef65cd	K_{31}	142929670a0e6e70
K_2	b5c0fbcfec4d3b2f	K_{32}	27b70a8546d22ffc
K_3	e9b5dba58189dbbc	K_{33}	2e1b21385c26c926
K_4	3956c25bf348b538	K_{34}	4d2c6dfc5ac42aed
K_5	59f111f1b605d019	K_{35}	53380d139d95b3df
K_6	923f82a4af194f9b	K_{36}	650a73548baf63de
K_7	ab1c5ed5da6d8118	K_{37}	766a0abb3c77b2a8
K_8	d807aa98a3030242	K_{38}	81c2c92e47edae66
K_9	12835b0145706fbe	K_{39}	92722c851482353b
K_{10}	243185be4ee4b28c	K_{40}	a2bfe8a14cf10364
K_{11}	550c7dc3d5ffb4e2	K_{41}	a81a664bbc423001
K_{12}	72be5d74f27b896f	K_{42}	c24b8b70d0f89791
K_{13}	80deb1fe3b1696b1	K_{43}	c76c51a30654be30
K_{14}	9bdc06a725c71235	K_{44}	d192e819d6ef5218
K_{15}	c19bf174cf692694	K_{45}	d69906245565a910
K_{16}	e49b69c19ef14ad2	K_{46}	f40e35855771202a
K_{17}	efbe4786384f25e3	K_{47}	106aa07032bbd1b8
K_{18}	0fc19dc68b8cd5b5	K_{48}	19a4c116b8d2d0c8
K_{19}	240ca1cc77ac9c65	K_{49}	1e376c085141ab53
K_{20}	2de92c6f592b0275	K_{50}	2748774cdf8eeb99
K_{21}	4a7484aa6ea6e483	K_{51}	34b0bcb5e19b48a8
K_{22}	5cb0a9dc3d41fbd4	K_{52}	391c0cb3c5c95a63
K_{23}	76f988da831153b5	K_{53}	4ed8aa4ae3418acb
K_{24}	983e5152ee66dfab	K_{54}	5b9cca4f7763e373
K_{25}	a831c66d2db43210	K_{55}	682e6fff3d6b2b8a3
K_{26}	b00327c898fb213f	K_{56}	748f82ee5defb2fc
K_{27}	bf597fc7beef0ee4	K_{57}	78a5636f43172f60
K_{28}	c6e00bf33da88fc2	K_{58}	84c87814a1f0ab72
K_{29}	d5a79147930aa725	K_{59}	8cc702081a6439ec

Table A.2: Constants used during the calculation of a SHA–512 hash value. (Cont.)

Constant	Value (hexadecimal)	Constant	Value (hexadecimal)
K_{60}	90befffa23631e28	K_{70}	113f9804bef90dae
K_{61}	a4506cebde82bde9	K_{71}	1b710b35131c471b
K_{62}	bef9a3f7b2c67915	K_{72}	28db77f523047d84
K_{63}	c67178f2e372532b	K_{73}	32caab7b40c72493
K_{64}	ca273eceeaa26619c	K_{74}	3c9ebe0a15c9bebc
K_{65}	d186b8c721c0c207	K_{75}	431d67c49c100d4c
K_{66}	eada7dd6cde0eb1e	K_{76}	4cc5d4becb3e42b6
K_{67}	f57d4f7fee6ed178	K_{77}	597f299cfc657e2a
K_{68}	06f067aa72176fba	K_{78}	5fcb6fab3ad6faec
K_{69}	0a637dc5a2c898a6	K_{79}	6c44198c4a475817

SHA–512: Initial Hash $H^{(0)}$

Table A.3: Initial hash value for SHA–512.

$H_i^{(0)}$	Value (hexadecimal)
$H_0^{(0)}$	6a09e667f3bcc908
$H_1^{(0)}$	bb67ae8584caa73b
$H_2^{(0)}$	3c6ef372fe94f82b
$H_3^{(0)}$	a54ff53a5f1d36f1
$H_4^{(0)}$	510e527fade682d1
$H_5^{(0)}$	9b05688c2b3e6c1f
$H_6^{(0)}$	1f83d9abfb41bd6b
$H_7^{(0)}$	5be0cd19137e2179

SHA–512: Algorithm

Algorithm A.1 shows the complete algorithm for calculating the hash digest of a message that is split into $M^{(1)}, \dots, M^{(N)}$ blocks according to Section ??.

Algorithm A.1 SHA–512

Require: Message blocks $M^{(1)}$ to $M^{(N)} \in \mathcal{M}$

Ensure: SHA–512 hash value H of \mathcal{M}

- 1: **for** $i = 1$ to N **do**
- 2: Prepare message schedule W_t :

$$W_t = \begin{cases} M_t^{(i)}, & 0 \leq t \leq 15 \\ \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16}, & 16 \leq t \leq 79 \end{cases}$$

- 3: Initialize working variables a, b, c, d, e, f, g, h with $(i - 1)^{\text{st}}$ hash value:

$$\begin{aligned} a &= H_0^{(i-1)} \\ b &= H_1^{(i-1)} \\ c &= H_2^{(i-1)} \\ d &= H_3^{(i-1)} \\ e &= H_4^{(i-1)} \\ f &= H_5^{(i-1)} \\ g &= H_6^{(i-1)} \\ h &= H_7^{(i-1)} \end{aligned}$$

- 4: **for** $t = 0$ to 79 **do**
- 5: Calculate, whereas T_1, T_2 are temporary words:

$$\begin{aligned} T_1 &= h + \Sigma_1(e) + \chi(e, f, g) + K_t + W_t, \\ T_2 &= \Sigma_0(a) + \Upsilon(a, b, c) \\ h &= g \\ g &= f \\ f &= e \\ e &= d + T_1 \\ d &= c \\ c &= b \\ b &= a \\ a &= T_1 + T_2 \end{aligned}$$

- 6: **end for**

7: Compute the i^{th} *intermediate* hash value $H^{(i)}$:

$$H_0^{(i)} = a + H_0^{(i-1)}$$

$$H_1^{(i)} = b + H_1^{(i-1)}$$

$$H_2^{(i)} = c + H_2^{(i-1)}$$

$$H_3^{(i)} = d + H_3^{(i-1)}$$

$$H_4^{(i)} = e + H_4^{(i-1)}$$

$$H_5^{(i)} = f + H_5^{(i-1)}$$

$$H_6^{(i)} = g + H_6^{(i-1)}$$

$$H_7^{(i)} = h + H_7^{(i-1)}$$

8: **end for**

9: Concatenate the intermediate hash values of the N^{th} round to the output hash:

$$H \leftarrow H_0^{(N)} \parallel H_1^{(N)} \parallel H_2^{(N)} \parallel H_3^{(N)} \parallel H_4^{(N)} \parallel H_5^{(N)} \parallel H_6^{(N)} \parallel H_7^{(N)}$$

B Acronyms

BDP Bit Disagreement Probability

List of Figures

4.1 Value distribution of each signal.	7
--	---

List of Tables

A.1	Constants used during the calculation of a SHA-512 hash value. . . .	11
A.2	Constants used during the calculation of a SHA-512 hash value. (Cont.)	12
A.3	Initial hash value for SHA-512.	12

List of Algorithms

A.1 SHA-512	12
-----------------------	----

List of Listings

List of Formulas

2.1	Definition: Entropy	3
-----	-------------------------------	---

Bibliography

- [1] AHLWEDE, Rudolf ; CSISZÁR, Imre: Common Randomness in Information Theory and Cryptography. Part I: Secret Sharing. In: *IEEE Transactions on Information Theory* 39 (1993), Nr. 4, S. 1121–1132. – ISSN 0018-9448
- [2] AONO, Tomoyuki ; HIGUCHI, Keisuke ; OHIRA, Takashi ; KOMIYAMA, Bokuji ; SASAOKA, Hideichi: Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels. In: *Antennas and Propagation, IEEE Transactions on* 53 (2005), S. 3776 – 3784. – URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1528749
- [3] BESSENRODT, Christine: RSA-Algorithmus. In: *Verfahren in der Kryptographie* (2001). – URL <http://fma2.math.uni-magdeburg.de/~bessen/krypto/krypto8.htm>
- [4] BEUCHER, Ottmar: *MATLAB und Simulink (Scientific Computing)*. Pearson Studium, 08 2006. – ISBN 3827372062
- [5] BOHDANOWICZ, Adrian: *On Efficient BER Evaluation of Digital Communication Systems via Importance Sampling*. – URL <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.2785&rep=rep1&type=pdf>
- [6] BURR, William E. ; DODSON, Donna F. ; POLK, W. T. ; EVANS, Donald L.: Electronic Authentication Guideline. In: *NIST Special Publication*, 2004
- [7] BUSSGANG, J.J.: *Crosscorrelation Functions of Amplitude-distorted Gaussian Signals*. Research Laboratory of Electronics, Massachusetts Institute of Technology, 1952 (Technical report (Massachusetts Institute of Technology. Research Laboratory of Electronics)). – URL <http://books.google.com/books?id=IWGLGwAACAAJ>
- [8] CHEN, Po-Ning: *Continuous Sources and Channels*. – URL <http://shannon.cm.nctu.edu.tw/it/c1-6s04.pdf>
- [9] CHIKKATUR, A.P. ; SHIN, Y. ; LEANHARDT, A.E. ; KIELPINSKI, D. ; TSUKATA, E. ; GUSTAVSON, T.L. ; PRITCHARD, D.E. ; KETTERLE, W.: A continuous source of Bose-Einstein condensed atoms. In: *Science* 296 (2002), Nr. 5576, S. 2193–5
- [10] COVER, Thomas M. ; THOMAS, Joy A.: *Elements of Information Theory*. New York, NY, USA : Wiley-Interscience, 1991. – ISBN 0-471-06259-6

- [11] DOMPIERRE, Julien: *The Pigeonhole Principle*. 2008. – URL http://www.cs.laurentian.ca/jdompierre/html/MATH1056E_F2009/cours/s5.2_pigeonhole_principle_BW.pdf
- [12] DÖTTLING, Nico ; LAZICH, Dejan ; MÜLLER-QUADE, Jörn ; ALMEIDA, Antonio S. de: Vulnerabilities of Wireless Key Exchange Based on Channel Reciprocity. In: *Proceedings of the 11th international conference on Information security applications*. Berlin, Heidelberg : Springer-Verlag, 2011 (WISA'10), S. 206–220. – URL <http://dl.acm.org/citation.cfm?id=1949945.1949964>. – ISBN 3-642-17954-1, 978-3-642-17954-9
- [13] EDELSON, R. A. ; KROLIK, J. H.: The Discrete Correlation Function: A New Method for Analyzing Unevenly Sampled Variability Data. In: *The Astrophysical Journal* 333 (1988), Oct., S. 646–659
- [14] FREY, Thomas ; BOSSERT, Martin: *Signal- und Systemtheorie*. Vieweg+Teubner Verlag / GWV Fachverlage GmbH, Wiesbaden, 2009. – URL <http://link.springer.com/book/10.1007/978-3-8348-9292-8/page/1>
- [15] GIROD, Bernd: *Image and Video Compression*. – URL <http://www.stanford.edu/class/ee368b/Handouts/01-Introduction.pdf>
- [16] JANA, Suman ; PREMNATH, Sriram N. ; CLARK, Mike ; KASERA, Sneha K. ; PATWARI, Neal ; KRISHNAMURTHY, Srikanth V.: On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments. In: *Proceedings of the 15th annual international conference on Mobile computing and networking*. New York, NY, USA : ACM, 2009 (MobiCom '09), S. 321–332. – URL <http://doi.acm.org/10.1145/1614320.1614356>. – ISBN 978-1-60558-702-8
- [17] JERUCHIM, M.: Techniques for Estimating the Bit Error Rate in the Simulation of Digital Communication Systems. In: *Selected Areas in Communications, IEEE Journal on* 2 (1984), Nr. 1, S. 153–170. – URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1146031
- [18] JURAFSKY, Daniel ; MARTIN, James H.: *Speech and Language Processing (2nd Edition) (Prentice Hall Series in Artificial Intelligence)*. 2. Prentice Hall, 2008. – URL <http://www.amazon.com/Language-Processing-Prentice-Artificial-Intelligence/dp/0131873210%3FSubscriptionId%3D13CT5CVB80YFWJEPWS02%26tag%3Dws%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D0131873210>. – ISBN 0131873210
- [19] LIANG, Y. ; POOR, H.V. ; SHAMAI, S.: *Information Theoretic Security*. Now Publishers, 2009 (Foundations and trends in communications and information theory). – URL <http://books.google.ca/books?id=YSH3Rm5fd70C>. – ISBN 9781601982407

- [20] LU, D. ; YAO, K.: Improved Importance Sampling Technique for Efficient Simulation of Digital Communication Systems. In: *IEEE J.Sel. A. Commun.* 6 (2006), September, Nr. 1, S. 67–75. – URL <http://dx.doi.org/10.1109/49.192731>. – ISSN 0733-8716
- [21] LUNZE, J.: *Ereignisdiskrete Systeme: Modellierung und Analyse dynamischer Systeme mit Automaten, Markovketten und Petrinetzen*. Oldenbourg, 2006. – URL <http://books.google.ca/books?id=12c7x3Z1h9cC>. – ISBN 9783486580716
- [22] MATHWORKS, The: *Matlab Optimization Toolbox User's Guide*. – URL http://www.mathworks.co.uk/access/helpdesk/help/pdf_doc/optim/optim_tb.pdf
- [23] MATHWORKS, The: *Simulink: Dynamic System Simulation for MATLAB. Writing S-functions : version 5*. URL <http://books.google.ca/books?id=eozkygAACAAJ>, 2002 (Modeling, simulation, implementation Bd. 2)
- [24] MAURER, Ueli ; WOLF, Stefan: Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free. In: *Proceedings of the 19th international conference on Theory and application of cryptographic techniques*. Berlin, Heidelberg : Springer-Verlag, 2000 (EUROCRYPT'00), S. 351–368. – ISBN 3-540-67517-5
- [25] MAURER, Ueli M.: Secret Key Agreement by Public Discussion from Common Information. In: *IEEE Transactions on Information Theory* 39 (1993), Nr. 3, S. 733–742. – URL <https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=256484>
- [26] MAURER, Ueli M. ; WOLF, Stefan: Secret-Key Agreement over Unauthenticated Public Channels – Part I: Definitions and a Completeness Result. In: *IEEE Transactions on Information Theory* 49 (2003), Nr. 4, S. 822–831. – URL <https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1193793>
- [27] MCEVOY, Robert P. ; CROWE, Francis M. ; MURPHY, Colin C. ; MARNANE, William P.: Optimisation of the SHA-2 Family of Hash Functions on FPGAs. In: *Proceedings of the IEEE Computer Society Annual Symposium on Emerging VLSI Technologies and Architectures*. Washington, DC, USA : IEEE Computer Society, 2006 (ISVLSI '06), S. 317ff. – URL <http://dx.doi.org/10.1109/ISVLSI.2006.70>. – ISBN 0-7695-2533-4
- [28] NIST: *FIPS 180-2, Secure Hash Standard, Federal Information Processing Standard (FIPS), Publication 180-2*. August 2002. – URL <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf>
- [29] PAAR, C. ; PELZL, J.: *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2009. – URL <http://books.google.ca/books?id=f24wFELSzkoC>. – ISBN 9783642041013

- [30] PIERROT, Alex J. ; CHOU, Rémi A. ; BLOCH, Matthieu R.: *Experimental Aspects of Secret-Key Generation in Indoor Wireless Environments*. Accepted to IEEE Workshop on Signal Processing Advances in Wireless Communications. April 2013
- [31] PRATAP, Rudra: *Getting Started with MATLAB*. New York : Oxford University Press, 2002
- [32] PROAKIS, John: *Digital Communications*. 4. McGraw-Hill Science/Engineering/Math, August 2000. – URL <http://www.amazon.com/exec/obidos/redirect?tag=citeulike07-20&path=ASIN/0072321113>. – ISBN 0072321113
- [33] RIDGWAY, Ged: *Rician Probability Density Function*. 2008. – URL <https://bitbucket.org/tuomov/dticode/raw/0fb38dc4f755a9a2e6c31e1bac4b6e3dd06a5158/matlab/rician/ricpdf.m>
- [34] ROUX, Philippe ; SABRA, Karim G. ; KUPERMAN, W. A. ; ROUX, Andre: Ambient noise cross correlation in free space: Theoretical approach. In: *The Journal of the Acoustical Society of America* 117 (2005), Nr. 1, S. 79–84. – URL <http://dx.doi.org/10.1121/1.1830673>
- [35] SHANBHAG, D.N. ; RAO, C.R.M.: *Stochastic Processes: Theory and Methods*. North-Holland, 2001 (Developments in Cell Biology). – URL <http://books.google.com/books?id=UENGL9bXSQC>. – ISBN 9780444500144
- [36] SHANNON, Claude E.: A Mathematical Theory of Communication. In: *The Bell System Technical Journal* 27 (1948), July, October, S. 379–423, 623–656. – URL <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>
- [37] SHANNON, Claude E.: Communication Theory of Secrecy Systems. In: *Bell System Technical Journal* 28 (1949), October, S. 656–715. – URL <http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf>
- [38] SIMON, Jan: *DataHash - File Exchange - MATLAB Central*. 2011. – URL <http://www.mathworks.com/matlabcentral/fileexchange/31272-datahash>
- [39] SLOTNICK, Scott D. ; DODSON, Chad S.: Support for a Continuous (Single-Process) Model of Recognition Memory and Source Memory. In: *Mem Cognit* 33 (2005), Nr. 1, S. 70–151. – ISSN 0090-502X
- [40] VOGT, Hendrik: *Secret-Key Agreement in Physical-Layer Security*, Ruhr-Universität Bochum, Diplomarbeit, March 2013