Schrifttum

Veröffentlichungen in Fachzeitschriften und Fachbüchern

[1] K.Huber, L.F.Lind, "Optimal Data Transmission Filters", Electronics Letters, 16th August 1984, Vol.20 No.17, pp.697-698.

[2] K.Huber, "Zum Knick bei Kennlinien", AEÜ, Band 40, 1986, Heft 3, pp.193-194.

[3] K.Huber, "A Design Method for Pulse Shaping Filters Having Small Intersymbol Interference",IEEE CAS-34 No.9, September 1987, pp.1137-1138.

[4] K.Huber, "Closed Form Formulas for the Design of Pulse Shaping Filters Having Small Intersymbol Interference", AEÜ, Band 42, 1988, Heft 4, pp.227-229.

[5] K.Huber, "A Design Method for Partial Response Filters", International Journal of Numerical Modelling: Electronic Networks, Devices and Fields, Vol.1, pp.131-136, 1988.

[6] K.Huber, "Combined Coding and Modulation using Blockcodes", Electronics Letters, 17th August 1989, Vol.25 No.17, pp.1130-1131.

[7] M.Bossert, K.Huber: "Distributionen", in Handbuch der Informationstechnik und Elektronik. Band 1 Teil II, S.399-415, Hüthig Verlag Heidelberg 1989.

[8] K.Huber, "Beiträge zu Codierung, codierter Modulation und zum Rechnen in endlichen Körpern ", Darmstädter Dissertation, Dezember 1989.

[9] K.Huber, "Some Comments on Zech's Logarithms", IEEE Trans. on Inf. Theory, Vol.36, No.4, July 1990, pp. 946-950.

[10] K.Huber, "Practical Constructions for Binary Codes and its Decoding", AEÜ, Band 45, 1991, Heft 1, pp.55-57.

[11] K.Huber, "Combined 2-4 PSK and its Application in Block-Coded Modulation", AEÜ, Band 45, 1991, Heft 5, pp.331-334.

[12] K.Huber, "Specialised Attack on the Chor-Rivest Public Key Cryptosystem", Electronics Letters, 7th November 1991, Vol.27 No.23, pp. 2130-2131. "Erratum": Electronic Letters, 5th December 1991, Vol.27 No. 25, p.2399.

[13] K.Huber, "Some Considerations Concerning the Selection of RSA Moduli", in Advances in Cryptology, Eurocrypt '91; Lecture Notes in Computer Science 547, D.W.Davies Ed., Springer-Verlag, 1991, ISBN 3-540-54620-0 / 0-387-54620-0, pp.294-301.

[14] K.Huber, "Solving Equations in Finite Fields and Some Results Concerning the Structure of GF(pm)", IEEE Trans. on Inf. Theory, Vol.38, No.3, May 1992, pp. 1154-1162.

[15] K.Huber, "Codes over Gaussian Integers", IEEE Trans. on Inf. Theory, Vol.40, No.1, January 1994, pp.207-216.

[16] K.Huber, "On The Period Length of Generalized Inversive Pseudorandom Number Generators", AAECC, Vol.5 No.5, pp.255-260, 1994.

[17] K.Huber, "Codes over Eisenstein-Jacobi Integers",
Finite Fields: Theory, Applications and Algorithms, (Las Vegas 1993),
Contemporary Math. Vol.168, American Math. Society, Providence, RI, 1994,
pp.165-179.

[18] K.Huber, "Open Problems and Conjectures: Polynomials over Finite Fields",
Finite Fields: Theory, Applications and Algorithms, (Las Vegas 1993),
Contemporary Math. Vol.168, American Math. Society, Providence, RI, 1994,
p.397.

[19] K.Huber, "A Knapsack-type Public Key Cryptosystem Based on Gaussian
Integers", Proceedings of the Seventh Joint Swedish-Russian International
Workshop on Information Theory, St.Petersburg, Rußland, 17.-22.Juni, 1995,
pp.125-132.

[20] K.Huber, Problem 10497, American Mathematical Monthly, January 1996,
p.75. Solution: American Mathematical Monthly, February 1998, p.185.

[21] K.Huber, "Note on Decoding Binary Goppa Codes",
Electronics Letters, 18th January 1996, Vol. 32 No.2, pp. 102-103.

[22] K.Huber, "Computing Complex Convolutions Using Surrogate Fields",
Frequenz, Band 50, März/April 1996, pp. 46-48.

[23] K.Huber, "Biquadratic and e-th Power Residue Codes",
AEÜ, Int. J. Electron. Commun., Vol. 50, 1996, No. 6, pp. 357-361.

[24] K.Huber, "The MacWilliams Theorem for Two-Dimensional Modulo Metrics",
AAECC, Vol.8 No.1, pp. 41-48, 1997.

[25] K.Huber, "Codes over Tori", IEEE Trans. on Inf. Theory, Vol.43, No.2,
March 1997, pp.740-744.

[26] K.Huber, "Über Anwendungen der Tschebyscheffschen Polynome in der
Schaltungstechnik", Frequenz, Band 52, Januar/Februar 1998, pp. 11-13.

[27] J.Schwenk, K.Huber, "Public key encryption and digital signatures based on
permutation polynomials", Electronics Letters, 16th April 1998, Vol. 34
No.8, pp. 759-760.

[28] K.Huber, F.Tönsing, "Kryptologische Verfahren",
Deutsche Telekom Unterrichtsblätter, Jg.51 9/1998, S.436-448.

[29] E.Bach, K.Huber, "Note On Taking Square Roots Modulo N",
IEEE-IT, Vol.45 No.2, March 1999, pp.807-809.

[30] K.Huber, "Efficient Utilization of Multilevel Signal Constellations",
accepted for publication.

[31] K.Huber, U.Heister, R.Schmitz, F.Tönsing, "Kryptologische Verfahren",
Handbuch der Telekommunikation, 11.1.3.6, 1-52, Januar 2001.

[32] K.Huber, Circumference of Cassinic Curves, problem 10889,
American Mathematical Monthly, August-September 2001, p.667,
Solution: American Mathematical Monthly, Oktober 2002, pp.765-766.

[33] K.Huber, Taking pth Roots Modulo Polynomials over Finite Fields,
Designs, Codes and Cryptography, 28, 303-311, 2003.

[34] K.Huber, 'On the design of Cauer Filters',
AEÜ Int. J. Electron. Commun., Vol. 58, 2004, No. 3, pp.223-224.

[35] K.Huber, H.Knospe, 'Functions for Two-Dimensional Signal Representation, Interpolation, and a new Approach toward the Compression of Data', AEÜ Int. J. Electron. Commun., Vol. 58, 2004, No. 3, pp.225-228.

[36] K.Huber, 'New Modulation Scheme based on Elliptic Functions', AEÜ, Int.J.Electron. Commun., Vol. 59, 2005, No.8, pp.491-494.

[37] K.Huber, "Cauer Filters", BoD, Norderstedt, 2011.

[38] K.Huber, "Relativistic Motion", BoD, Norderstedt, 2011.

[49] K.Huber, 'Relativistic Orbits and the Zeros of $\wp(θ)$',arXiv:1207.4688v1 06.07.2012.

[40] K.Huber, 'All-Pole Filters Matched to Specifications', Journal of the Audio Engineering Society, Vol.61 No.12, pp.1022-1025, December 2013.

[50] K.Huber, 'From Kepler's Laws to Newtonian Motion and the Direction Angle of Hamilton's Hodograph',arXiv:2101.05041, 13.01.2021.

Patente / Erfindungsmeldungen

[1] K.Huber: Verfahren zur gesicherten Datenübertragung über ungesicherte Verbindungen. 19.03.1993, DE 43 08 825 A1, EP 0 616 447 A2

[2] K.Huber, S.Wolter: Verfahren und Anordnung zur Realisierung von kryptologischen Funktionen. 16.07.1994, DE 44 25 158 A1.

[3] K.Huber, F.Tönsing: Verfahren und Anordnung zum Nachweis des Zeitpunktes der Durchführung eines kryptografischen Prozesses. 16.03.1996, DE 196 10 401 A1, EP 0795 979 A2.

[4] K.Huber, A.Scheerhorn: Verfahren und Vorrichtung zum Aufzeichnen/Verarbeiten von authentischen Tondaten. 18.04.1996, DE 196 15 302 A1, WO 97/40603.

[5] K.Huber, A.Scheerhorn: Verfahren und Vorrichtung zum Aufzeichnen/Verarbeiten von authentischen Bild- und/oder Tondaten. 18.04.1996, DE 196 15 301 A1, WO 97/40496.

[6] A.Scheerhorn, K.Huber: Verfahren zur Übertragung von Signalen. 01.10.1996, DE 196 40 526 A1, WO 98/15085, US Patent Nr. 7188361 erteilt am 06.03.2007.

[7] K.Huber: Verfahren und Anordnung zur Erzeugung von Sinus/Cosinusschwingungen. 15.01.1997, DE 197 01 068 A1, WO 98/32219.

[8] K.Huber: Verfahren und Anordnung zur Frequenzvervielfachung. 15.01.1997, DE 197 01 067.

[9] J.Schwenk, K.Huber: Verfahren zum Verschlüsseln einer als Zahlenwert dargestellten Nachricht. 04.02.1997, DE 197 03 928 A1, WO 98/34372, Europäisches Patent Nr. 0958675 erteilt am 23.07.2008.

[10] J.Schwenk, K.Huber: Verfahren zum Generieren einer digitalen Signatur und Verfahren zur Überprüfung der Signatur, 04.02.1997, DE 197 03 929 A1, WO 98/34373, Europäisches Patent Nr. 0958676 erteilt am 16.04.2008.

[11] K.Huber, K.-H. Hofmann: Verfahren und Schaltungsanordnung zur Übertragung von Nachrichten, 13.08.1997, DE 197 35097, Europäisches Patent Nr.1018221 erteilt am 18.09.2002, Kanadische Patent Nr. 2296079 erteilt am 24.01.2006, US Patent No.7016424 erteilt am 21.03.2006.

[12] K.Huber: Verfahren und Schaltungsanordnung zur verbesserten Datenübertragung, 15.01.1997, Europäisches Patent Nr. 0958685.

[13] K.Huber, U.Heister, F.Schäfer-Lorinser, T.Martin, T.Breitbach: Verfahren und Vorrichtung zum Erzeugen einer Pseudozufallsfolge, 07.12.2000, Europäisches Patent Nr. 1342153 erteilt am 07.06.2006.

[14] K.Huber, P.Windirsch, T.Schneider, R.Schaffelhofer, M.Baumgart: Verfahren zur Kompression von Daten, Aug.2001, P01064, US Patent 6714147 B2 erteilt am 30.04.2004.

[15] K.Huber, U.Heister: Biometrisches Verfahren zum Zugangsschutz, P02034, Juli.2002.

[16] K.Huber, Verfahren und Anordnung zum Einstellen eines analogen Filters, Patentanmeldung, Okt. 2002, freigeg. von Dt.Telekom, alle Rechte beim Erfinder.

[17] K.Huber, H.Knospe: 'Verfahren zur zweidimensionalen Darstellung, Interpola-tion und zur Kompression von Daten, 14.10.2002, US Patent Nr. 7318077 erteilt am 08.01.2008.

[18] K.Huber, M.Baumgart, T.Schneider: Verschlüsselungsverfahren basierend auf Faktorisierung, P02039, Juli 2002.

[19] K.Huber, E.Saar, J.Schaaf: Verfahren und Anordnung zur Etablierung eines kostenpflichtigen E-Mail-Dienstes P02153, 19.05.2003, EP 1 480 398 B1.

[20] K.Huber: Analoge Schaltungsanordnung zur Erzeugung elliptischer Funktionen, P03025, Mai 2003.

[21] E.Saar, B.Löhlein, K.Huber, M.Gunkel: Verfahren und Kommunikationssystem zur Freigabe einer Datenverarbeitungseinheit, P03026, März 2003.

[22] K.Huber: Verfahren zur Modulation eines Trägersignals sowie Verfahren zur Demodulation eines modulierten Trägersignals, P03033, Mai 2003.

[23] K.Huber: Verfahren und Anordnung zur Korrektur von Fehlern bei QAM-Übertragung, Oktober 2004, freigeg. von Dt.Telekom, alle Rechte beim Erfinder.

[24] E.Saar, J.Schaaf, K.Huber: Verfahren und Vorrichtung zum Nachweis der Verschlüsselung von digitalen Daten innerhalb eines DRM-Systems, P04073,Feb. 2003.

[25] K.Huber: Verfahren und Anordnung zum Einbringen von elektronischen Wasserzeichen in analoge Signale, 05.07.2008, DE 10 2008 031760A1.

[26] K.Huber: Verfahren zur verbesserten Realisierung von Filterfunktionen dritter Ordnung,16.04.2013, AKZ 10 2013 006 537.2.

[27] K.Huber: Verfahren zur Realisierung von universellen Filterfunktionen n-ter Ordnung, 06.06.2013, AKZ 10 2013 009 560.3.

[28] K.Huber: Erweitertes Verfahren zur Realisierung von universellen Filterfunktionen n-ter Ordnung, 17.12.2013, AKZ 10 2013 021 189.1.

[29] K.Huber: Verfahren zur Realisierung von sicheren Kommunikationssystemen, 06.01.2014, AKZ 10 2014 014 869.6.

Vorträge auf internationalen Konferenzen

K.Huber: "A New Simple Block Coding Scheme",
AAECC-5 Conference, Menorca, Spanien, 15-19 Juni 1987.

K.Huber: "Some Comments on Zech's Logarithms",
Fourth Joint Swedish-Soviet International Workshop on Information Theory,
Proceedings pp.65-69, Gotland, Sweden, August 27 - September 1, 1989.

K.Huber: "On the Number of Keyelements of GF(pm), p>2 which are Necessary to Compute all Zech Logarithms of the Field", Open Problems, Fourth Joint Swedish-Soviet International Workshop on Information Theory, Proceedings p.16, Gotland, Sweden, August 27 - September 1, 1989.

K.Huber: "Combined Coding and Modulation Using Block Codes",
IEEE Symposium on Information Theory, San Diego, USA, January 14-19, 1990.

K.Huber: "Some Considerations Concerning the Selection of RSA-Moduli",
Eurocrypt '91, Brighton, England, April 8-11, 1991.

K.Huber: "Solving Equations in Finite Fields",
AAECC-9, New Orleans, USA, October 7-11, 1991.

K.Huber: "Codes over Gaussian Integers",
CDS-92 Conference, Königsberg (Kaliningrad), Rußland 7.-11.September 1992.

K.Huber: "Codes over Gaussian Integers",
IEEE Symposium on Information Theory, San Antonio, USA, January 17-22, 1993.

K.Huber: "Codes over Eisenstein-Jacobi Integers",
Second International Conference on Finite Fields: Theory, Applications, and Algorithms, Las Vegas, USA, August 17-21, 1993.

K.Huber: "Polynomials over Finite Fields", Open Problems and Conjectures,
Second International Conference on Finite Fields:
Theory, Applications, and Algorithms, Las Vegas, USA, August 17-21, 1993.

K.Huber: "Decoding Algorithms for Block Codes over Two-Dimensional Signal-Constellations", IEEE Symposium on Information Theory, Trondheim, Norway, June 27 - July 1, 1994.

K.Huber: "A Knapsack-type Public Key Cryptosystem Based on Gaussian Integers",
Seventh Joint Swedish-Soviet International Workshop on Information Theory,
St.Petersburg, Rußland, 17.-22. Juni, 1995.

K.Huber, E.Bach, "Note On Taking Square Roots Modulo N",
International Conference on Coding Theory, Cryptography and related Areas,
20-24 April, 1998, of Guanajuato, Mexico.

K.Huber: "Efficient Utilisation of Multilevel Signal Constellations",
International Symposium on Information Theory, MIT, August 16-21,1998.

K.Huber, R.Schmitz, "Synchronisation for QAM-/PSK signaling",
SETA 98 Conference, December 14-17,1998, Singapur.

K.Huber, "Decoding Of Icyclic Codes For The Mannheim Metric, International Symposium on Information Theory and its Applications, ISITA 2004, Parma, Italy, October 10-13, 2004.

Weitere Vorträge

K.Huber: "Neue Kryptographische Verfahren durch Kombination von Operationen in endlichen Körpern mit der schnellen Walshtransformation", Telesec Arbeitskreis Kryptosysteme, FTZ Darmstadt, 2. Oktober 1990.

K.Huber: "Zum Rechnen in endlichen Körpern unter besonderer Berücksichtigung von Körpern der Charakteristik p=2", IBM, Wissenschaftliches Zentrum Heidelberg, 17. Januar 1991.

K.Huber: "Zum Lösen von Gleichungen in endlichen Körpern und einige Ergebnisse zur Struktur von GF(p^m)", Technische Hochschule Darmstadt, Institut für Netzwerk- und Signaltheorie, 8. Februar 1991.

K.Huber: "Ergebnisse zur Struktur von GF(p^m) mit einer Anwendung auf das Chor-Rivest Verfahren", Tagung Datensicherheit in Rechnern und Netzwerken, Institut für experimentelle Mathematik, Universität Essen, 30. Oktober 1991.

K.Huber: "Ergebnisse zur Struktur von GF(pm) mit einer Anwendung auf das Chor-Rivest Verfahren", Telesec Arbeitskreis Kryptosysteme, FTZ Darmstadt, 7. November 1991.

K.Huber: "Kryptographie mit AXIOM ", IBM Düsseldorf, 6. Mai 1992.

K.Huber: "Codes über Gaußschen ganzen Zahlen" Technische Hochschule Darmstadt, Institut für Netzwerk- und Signaltheorie, 8. Mai 1992.

K.Huber: "Ein schneller Algorithmus um eine ganze Zahl als Summe von 4 Quadraten darzustellen", Telesec Arbeitskreis Kryptosysteme, 24. September 1992, FTZ Darmstadt.

K.Huber: "Zur Periodenlängen- und Parameterbestimmung von verallgemeinerten inversiven Pseudozufallszahlengeneratoren", Telesec Arbeitskreis Kryptosysteme, FTZ Darmstadt, 28. Januar 1993.

K.Huber: "Zum Chor Rivest Verschlüsselungsverfahren", GMD Seminar Darmstadt, 7.April 1993.

K.Huber: "Die Mannheim-Metrik und ihre Anwendung in der Codierungstheorie", Seminar im Fachbereich Mathematik, Technische Hochschule Darmstadt, 16. April 1993.

K.Huber: "Ein öffentliches Verschlüsselungsverfahren nach dem Rucksackprinzip basierend auf Gaußschen ganzen Zahlen", GMD Seminar Darmstadt, 20.Oktober 1993.

K.Huber: "Über Anwendungen von Algebra und Zahlentheorie in der Nachrichtentechnik", Elektrotechnisches Kolloquium, Universität Ulm, 31. Januar 1996.

K.Huber: "Zur Decodierung von Goppa-Codes", Telesec Arbeitskreis Kryptosysteme, TZ Darmstadt, 29. Februar 1996.

K.Huber: "Zum Wurzelziehen Modulo N", Telesec Arbeitskreis Kryptosysteme, TZ Berlin, 07. November 1996.

K.Huber: "Sicherheitsanforderungen an WLL-Systeme: Kryptographische Verfahren zur Authentifikation und zum Verschlüsseln", Technische Akademie Esslingen, 14.-16.12.1998, Lehrgang Nr. 24013/74508.

K.Huber: "Anwendungen von Elliptischen Funktionen in der Nachrichtentechnik", 29.10.2003, Universität Bremen.

K.Huber: "Applications of Algebra and Numbertheory in Communications", 19.11.2003, University of Illinois at Urbana Champaign.

K.Huber: "Applications of Elliptic Functions in Communications" 08.12.2003, University of Illinois at Urbana Champaign.

K.Huber: "Applications of Algebra and Numbertheory in Communications" 05.01.2004, University of Wisconsin, Madison.

K.Huber: "Anwendungen von Elliptischen Funktionen in der Nachrichtentechnik", 19.03.2004, FTW / Universität Wien.

K.Huber: "Anwendungen von Elliptischen Funktionen in der Nachrichtentechnik", 29.04.2004, Universität Erlangen.

K.Huber: "Prinzip und Anwendung der Abtastung elektrischer Signale", 29.11.2004, Hochschule Bremen.

K.Huber: "Algebraic Coding of QAM-Signals", 29.11.2004, Hochschule Bremen.

K.Huber: "Verbesserung der Leistungsfähigkeit von Kanalcodes bezüglich der Fehlerkorrektur durch Soft-Decision Decoding",18.04.2007, Hochschule für Telekommunikation Leipzig.

K.Huber: "Relativistische Bahnkurven und Cauer Filter", Bremen-Oldenburg relativity seminar, Zarm, Universität Bremen, 16th December, 2010, available at http://www.researchgate.net/profile/Klaus_Huber/

K.Huber: "Codierung von QAM-Signalen", Hochschule der Bayerischen Wirtschaft, München, 07.05.2014.

Gutachtertätigkeit für Fachzeitschriften

Mathematics of Computation

AAECC Applicable Algebra in Engineering, Communication, and Computing

IEEE Transactions on Information Theory

IEEE Transactions on Circuits and Systems

IEEE Transactions on Vehicular Technology

IEEE Transactions on Computers

European Transactions on Communications

Electronics Letters

IEE Proceedings Computers and Digital Techniques

Finite Fields & Their Applications