

# Literaturverzeichnis

- [AgLa85] Agrawala, A.K.; Lakshman, T.V.: Efficient decentralized consensus protocols: *IEEE Trans. Software Enging* **12** (1985), 600–607.
- [AsKe92] Assmus, E.F.; Key, T.D.: *Designs and their Codes*: Cambridge University Press, Cambridge Tracts in Math. **103**, 1992.
- [BaBe93] Batten, L.M.; Beutelspacher, A.: *The Theory of Linear Spaces*: Cambridge University Press, 1993.
- [Baer42] Baer, R.: Homogeneity of projective planes: *Amer. J. Math.* **64** (1942), 137–152.
- [Baer46] Baer, R.: Projectivities with fixed points on every line of the plane: *Bull. Amer. Math. Soc.* **52** (1946), 273–286.
- [Bar55] Barlotti, A.: Un' estensione del teorema di Segre - Kustaanheimo, *Boll. U.M.I.*, 10, Serie III, 498-506, 1955.
- [Bat86] Batten, L.M.: *Combinatorics of finite geometries*: Cambridge University Press, 1986.
- [Benz73] Benz: *Vorlesungen über Geometrie der Algebren*: Springer-Verlag, Berlin Heidelberg New York 1973.
- [BePi82] Beker, H.; Piper, F.C.: *Cipher Systems: The Protection of Communications*: Northwood Books, London 1982.
- [Ber87] Berger, M.: *Geometry I, II*: Springer-Verlag Berlin Heidelberg 1987.
- [BeRo90] Beutelspacher, A.; Rosenbaum, U.: Geometric authentication systems: *Ratio Mathematica* **1** (1990), 39–50.
- [BeRo91] Beutelspacher, A.; Rosenbaum, U.: Essentially 1-fold secure authentication systems: *Advances in Cryptology – EUROCRYPT 90*. Lecture Notes in Computer Science **473**, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, Barcelona, Budapest, 1991, 294–305.
- [Beu82] Beutelspacher, A.: *Einführung in die endliche Geometrie I*: Bibliographisches Institut, Mannheim, Wien, Zürich, 1982.
- [Beu83] Beutelspacher, A.: *Einführung in die endliche Geometrie II*: Bibliographisches Institut, Mannheim, Wien, Zürich, 1983.
- [Beu86] Beutelspacher, A.:  $21-6 = 15$ . A connection between two distinguished geometries: *Amer. Math. Monthly* **93** (1986), 29–41.
- [Beu87] Beutelspacher, A.: A defense of the honour of an unjustly neglected little geometry or A combinatorial approach to the projective plane of order five: *J. Geometry* **30** (1987), 182–195.
- [Beu88] Beutelspacher, A.: Enciphered geometry. Some applications of geometry to cryptography: *Ann. Discrete Math.* **37** (1988), 59–68.
- [Beu90a] Beutelspacher, A.: Applications of finite geometry to cryptography: *Geometries, Codes and Cryptography*. G. Longo, M. Marchi, A. Sgarro, eds., . CISM Courses and Lectures **313**, Springer-Verlag, Wien, Berlin, Heidelberg, New York, 1990.

- [Beu90b] Beutelspacher, A.: How to communicate efficiently: *J. Combinat. Theory* **54** (1990), No. 2, 312–316.
- [Beu00] Beutelspacher, A.: *Geheimsprachen. Geschichte und Techniken*: C.H. Beck Verlag, 2000
- [Beu02] Beutelspacher, A.: *Kryptologie*: Verlag Vieweg, Wiesbaden (<sup>6</sup>2002).
- [BeWe93] Beutelspacher, A.; Wettl, F.: On 2-level secret sharing: *Designs, Codes and Cryptography* **3** (1993), 127–134.
- [BJL85] Beth, T.; Jungnickel, D.; Lenz, H.: *Design Theory*: Bibliographisches Institut, Mannheim, Wien, Zürich, 1985.
- [Bla83] Blahut, R.E.: *Theory and Practice of Error Control Codes*: Addison-Wesley, Reading, Massachusetts, 1983.
- [BoBu66] Bose, R.C.; Burton, R.C.: A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and MacDonald codes: *J. Combinat. Theory* **1** (1966), 96–104.
- [BoRo80] Bolker, E.D.; Roth, B.: When is a bipartite graph a rigid framework?: *Pacific Journal of Mathematics*, Vol. 90, No.1, 1980.
- [BPBS84] Berger, M.; Pansu, P.; Berry, J.P.; Saint-Raymond, X.: *Problems in Geometry*: Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1984.
- [Bra76] Brauner, H.: *Geometrie projektiver Räume I*: Bibliographisches Institut, Mannheim, Wien, Zürich, 1976.
- [BrEr48] de Bruijn, N.G.; Erdős, P.: On a combinatorial problem: *Indag. Math.* **10** (1948), 421–423.
- [BrRy49] Bruck, R.H.; Ryser, H.J.: The non-existence of certain finite projective planes: *Can. J. Math.* **1** (1949), 88–93.
- [Buc01] Buchmann, J.: *Einführung in die Kryptographie*: Springer-Verlag, 2. Auflage 2001.
- [BuBu88] Buekenhout, F.; Buset, D.: On the foundations of incidence geometry: *Geom. Dedicata* **25** (1988), 269–296.
- [Buek69a] Buekenhout, F.: Ensembles quadratiques des espaces projectifs: *Math. Z.* **110** (1969), 306–318.
- [Buek69b] Buekenhout, F.: Une caractérisation des espaces affins basée sur la notion de droite: *Math. Z.* **111** (1969), 367–371.
- [Buek79] Buekenhout, F.: Diagrams for geometries and groups: *J. Combinat. Theory (A)* **27** (1979), 121–151.
- [Buek81] Buekenhout, F.: The basic diagram of a geometry: *Geometries and Groups*. Lecture Notes in Mathematics **893**, Springer-Verlag, Berlin, Heidelberg, New York, 1981, 1–29.
- [Buek95] Buekenhout, F.: *Handbook of Incidence Geometry. Buildings and Foundations*. North-Holland, 1995.
- [BuSh74] Buekenhout, F.; Shult, E.: On the foundations of polar geometry: *Geom. Dedicata* **3** (1974), 155–170.
- [CaLi80] Cameron, P.J.; Lint, van, J.H.: *Graphs, Codes and Designs*: London Math. Soc. Lecture Notes Series **43**, Cambridge University Press, 1980.
- [CaLi91] Cameron, P.J.; Lint, van, J.H.: *Designs, Graphs, Codes and their Links*: London Math. Soc. Student Texts **22**, Cambridge University Press, 1991.
- [Cam92] Cameron, P.J.: *Projective and Polar Spaces*: QMW Maths Notes **13**, Queen Mary and Westfield College, University of London, 1992.

- [CCITT] *CCITT Recommendations X.509: the Directory – Authentication Framework*, New York, London, Sydney, Toronto, 1988.
- [Cox55] Coxeter, H.S.M.: *Reelle projektive Geometrie der Ebene*: Oldenbourg, 1955.
- [Cox74] Coxeter, H.S.M.: *Projective Geometry*: University of Toronto Press, <sup>2</sup>1974.
- [Cox81] Coxeter, H.S.M.: *Unvergängliche Geometrie*. Birkhäuser-Verlag, Basel, Stuttgart 1981.
- [DaPr89] Davies, D.W.; Price, W.L.: *Security for Computer Networks*: John Wiley & Sons, Chichester 1984, <sup>2</sup>1989.
- [Dem68] Dembowski, P.: *Finite Geometries*: Springer-Verlag, Berlin, Heidelberg, New York, 1968.
- [Den83] Denning, D.: *Cryptography and Data Security*: Addison Wesley, Reading, Mass. 1983.
- [DVW89] DeSoete, M.; Vedder, K.; Walker, M.: Cartesian authentication schemes: *Advances in Cryptology – EUROCRYPT 89*. Lecture Notes in Computer Science **434**, Springer-Verlag 1990, 476–490.
- [Edge55] Edge, W.L.: 31-point geometry: *Math. Gaz.* **39** (1955), 113–121.
- [Fåk79] Fåk, V.: Repeated use of codes which detect deception: *IEEE Trans. Inform. Theory*, Vol. **25**, No. 2, March 1979, 233–234.
- [FiSh84] Fiat, A.; Shamir, A.: Generalized “Write-Once” Memories, *IEEE Trans. Inf. Theory IT-30*, 1984, 470–480.
- [Gal91] Gallian, J.A.: The mathematics of identification numbers: *College Math. J.* **22** (1991), 194–202.
- [Gal94] Gallian, J.A.: *Contemporary Abstract Algebra*: D.C. Heath, Lexington, Mass., 3rd edn, 1994.
- [GMS74] Gilbert, E.N.; MacWilliams, F.J.; Sloane, N.J.A.: Codes which detect deception: *The Bell Sys. Techn. J.* **53**, March 1974, 405–425.
- [Gop88] Goppa, V.D.: *Geometry and Codes*: Kluwer Academic Publishers, Dordrecht, Netherlands, Boston, Mass., London, 1988.
- [Hag71] Hagelbarger, D.W.: The application of balance symmetric incomplete block designs to switching networks: *Proceeding of the International Conference on Communications*, June 14, 15, 16, 1971, Montreal.
- [HaHe76] Halder, H.-R.; Heise, W.: *Einführung in die Kombinatorik*: Carl Hanser Verlag, München-Wien, 1976.
- [HeQu95] Heise, W.; Quattrocchi, P.: *Informations- und Codierungstheorie*: Springer-Verlag Berlin Heidelberg <sup>3</sup>1995.
- [Her72] Herzer, A.: Dualitäten mit zwei Geraden aus absoluten Punkten in projektiven Ebenen: *Math. Z.* **129** (1972), 235–257.
- [Hes05] Hessenberg, G.: Beweis des Desarguesschen Satzes aus dem Pascalschen: *Math. Ann.* **61** (1905), 161–172.
- [Hil62] Hilbert, D.: *Grundlagen der Geometrie*. B.G. Teubner, Stuttgart <sup>9</sup>1962.
- [Hill86] Hill, R.: *A first course in coding theory*: Clarendon Press, Oxford, 1986.
- [Hir79] Hirschfeld, J.W.P.: *Projective geometries over finite fields*: Clarendon Press, Oxford, 1979.
- [Hir85] Hirschfeld, J.W.P.: *Finite projective spaces of three dimensions*: Clarendon Press, Oxford, 1985.
- [HiTh91] Hirschfeld, J.W.P.; Thas, J.A.: *General Galois Geometries*: Clarendon Press, Oxford, 1991.

- [Hog94] Hogendijk, Jan P.: Mathematics in Medieval Islamic Spain. *Proceedings of the International Congress of Mathematicians*, Zürich 1994, Birkhäuser Verlag, Basel, 1995, 1568–1580.
- [HuPi73] Hughes, D.R.; Piper, F.C.: *Projective Planes*: Springer-Verlag New York Heidelberg Berlin: Graduate Texts in Mathematics **6**, 1973.
- [KaKr88] Karzel, H.; Kroll, H.-J.: *Geschichte der Geometrie seit Hilbert*: Wissenschaftliche Buchgesellschaft, Darmstadt 1988.
- [Kall82] Kallaher, M.J.: *Affine Planes with Transitive Collineation Groups*: North-Holland, New York, 1982.
- [KaPi70] Karzel, H.; Pieper, I.: Bericht über geschlitzte Inzidenzgruppen: *Jber. Deutsch. Math.-Verein.* **72** (1970), 70–114.
- [Ker92] Kersten, A.: Shared Secret Schemes aus geometrischer Sicht. *Mitt. Math. Sem. Univ. Giessen* **208** (1992).
- [KSW73] Karzel, H.; Sörensen, D.; Windelberg, D.: *Einführung in die Geometrie*: Vandenhock & Ruprecht, Göttingen, 1973.
- [Lam91] Lam, C.W.H.: The search for a finite projective plane of order 10: *Amer. Math. Monthly* **98** (1991), 305–318.
- [Lenz54] Lenz, H.: Zur Begründung der analytischen Geometrie: *Bayerische Akad. Wiss.* **2** (1954), 17–72.
- [Lenz65] Lenz, H.: *Vorlesungen über projektive Geometrie*: Akad. Verl. Ges. Geest & Portig, Leipzig, 1965.
- [Lin69] Lingenberg, R.: *Grundlage der Geometrie I*: Bibliographisches Institut, Mannheim 1969.
- [Lint82] Lint, van, J.H.: *Introduction to Coding Theory*: Springer-Verlag, New York, Heidelberg, Berlin, 1982.
- [Mas86] Massey, J.L.: Cryptography – a selective survey: *Alta Frequenza* **LV**, **1** (1986), 4–11.
- [Mer84] Merckx, F.: Womcodes constructed with projective geometries, *Traitement du signal* **1** (1984), 227–231.
- [Mey76] Meyberg, K.: *Algebra*, Teil 2: Carl Hanser Verlag, München - Wien, 1976.
- [MiPi87a] Mitchell, C.J.; Piper, F.C.: The cost of reducing key-storage requirements in secure networks: *Computers & Security* **6** (1987), 339–341.
- [MiPi87b] Mitchell, C.J.; Piper, F.C.: Key storage in secure networks: *J. Discrete Applied Math.* **21** (1988), 215–228.
- [Mou02] Moulton, F.R.: A simple non-desarguesian plane geometry: *Trans. Amer. Math. Soc.* **3** (1902), 192–195.
- [Mul54] Muller, D.E.: Application of Boolean algebra to switching circuit design and to error detection: *IEEE Trans. Computers* **3** (1954), 6–12.
- [MWS183] McWilliams, F.J.; Sloane N.J.A.: *The Theory of Error-Correcting Codes*: North-Holland, Amsterdam, New York, Oxford, 1983.
- [Pan55] Panella, G.: Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito, *Boll. U.M.I.*, 10, Serie III, 507-513, 1955.
- [Pas82] Pasch, M.: *Vorlesungen über neuere Geometrie*. Leipzig 1882.
- [Pas94] Pasini, A.: *Diagram Geometries*: Oxford University Press, 1994.
- [PaTh85] Payne, S.E.; Thas, J.A.: *Finite Generalized Quadrangles*: Pitman, New York 1985.

- [Ped63] Pedoe, D.: *An Introduction to Projective Geometry*: Macmillan, New York, 1963.
- [Pick55] Pickert, G.: *Projektive Ebenen*: Springer-Verlag, Berlin, Göttingen, Heidelberg, 1955.
- [PiWa84] Piper, F.C.; Walker, M.: Binary sequences and Hadamard designs: *Geometrical Combinatorics*, F.C. Holroyd, R.J. Wilson (eds.). Research Notes in Mathematics **114**, Pitman, Boston, Mass., 1984.
- [Qvi52] Qvist, B.: Some remarks concerning curves of the second degree in a finite plane: *Ann. Acad. Sci. Fenn.* **134** (1952), 1–27.
- [Reed54] Reed, I.S.: A class of multiple-error-correcting codes and the decoding scheme: *IEEE Trans. Inform. Theory* **4** (1954), 38–49.
- [RiSh82] Rivest, R.L.; Shamir, A.: How to reuse a “Write-once” Memory, *Information and Control* **55** (1982), 1–19.
- [Ros93] Rosenbaum, U.: A lower bound on authentication after having observed a sequence of messages: *J. Cryptology* **6** (1993), 135–156.
- [Roth81] Roth, B.: Rigid and flexible frameworks: *Amer. Math. Monthly*, **88** (1981), 6–21.
- [Rue86] Rueppel, R.: *Analysis and Design of Stream Ciphers*: Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1986.
- [Sal90] Salooma, A.: *Public-Key Cryptography*: Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, Barcelona, 1990.
- [Schn96] Schneier, B.: *Applied Cryptography: Protocols, Algorithms and Source Code in C*: John Wiley & Sons, New York, 2nd edn, 1996.
- [Schr92] Schröder, E.M.: *Vorlesungen über Geometrie*, Band 1, 2, 3: Bibliographisches Institut, Mannheim, Wien, Zürich, 1991, 1992.
- [Schu91] Schulz, R.H.: *Codierungstheorie – eine Einführung*: Verlag Vieweg, Braunschweig, Wiesbaden, 1991.
- [Seg54] Segre, B.: Sulle ovali nei piani lineari finiti: *Atti Accad. Naz. Lincei Rendic.* **17** (1954), 141–142.
- [Seg61] Segre, B.: *Lectures on Modern Geometry*: Cremonese, Roma, 1961.
- [Sha49] Shannon, C.E.: Communication theory of secrecy systems: *Bell. Sys. Tech. J.* **10** (1949), 657–715.
- [Sha79] Shamir, A.: How to share a secret: *Commun. ACM* **22** (1979), 612–613.
- [Sim82] Simmons, G.J.: A game theoretical model of digital message authentication: *Congressus Numerantium* **34** (1982), 413–424.
- [Sim84] Simmons, G.J.: Authentication theory / Coding theory: *Advances in Cryptology: Proceedings of CRYPTO 1984*. Lecture Notes in Computer Science **196**, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, Hong Kong, 1984, 411–432.
- [Sim90] Simmons, G.J.: How to (really) share a secret: *Advances in Cryptology – CRYPTO 88*. Lecture Notes in Computer Science **403**, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, Hong Kong, 1990, 390–448.
- [Sim92a] Simmons, G.J.: *Contemporary Cryptology*: IEEE Press, New York, 1992.
- [Sim92b] Simmons, G.J.: An introduction to shared secret/shared control schemes: *Contemporary Cryptology*, G.J. Simmons, ed., IEEE Press, New York, 1992, 441–497.

- [Sing38] Singer, J.: A theorem in finite projective geometry and some applications to number theory: *Trans. Amer. Math. Soc.* **43** (1938), 377–385.
- [SiSm89] Simmons, G.J.; Smeets, B.: A paradoxical result in unconditionally secure authentication codes – and an explanation: *IMA Conference on Cryptography and Coding*, Dec. 18–20, 1989, Cirencester, England, Clarendon Press, Oxford.
- [Ste13] Steinitz, E.H.: Bedingt konvergente Reihen und konvexe Systeme: *J. Reine Angew. Math.* **143** (1913), 128–175.
- [Sti95] Stinson, D.R.: *Cryptography. Theory and Practice*: CRC Press, Boca Raton, Fl., 1995.
- [Tall56] Tallini, G.: Sulle  $k$ -calotte di uno spazio lineare finito: *Ann. Mat. Pura Appl.* **42** (1956), 119–164.
- [Tall57] Tallini, G.: Caratterizzazione grafica delle quadriche ellittiche negli spazi finiti: *Rend. Mat. Roma* **16** (1957), 328–351.
- [Tam72] Tamaschke: *Projektive Geometrie II*. Bibliographisches Institut, Mannheim, Wien, Zürich 1972.
- [Tec87] Tecklenburg, H.: A proof of the theorem of Pappus in finite Desarguesian affine planes: *J. Geometry* **30** (1987), 172–181.
- [Tits56] Tits, J.: Les groupes de Lie exceptionnels et leur interprétation géométrique: *Bull. Soc. Math. Belg.* **8** (1956), 48–81.
- [Tits74] Tits, J.: *Buildings of Spherical Type and Finite BN-Pairs*. Springer-Verlag, Berlin Heidelberg, New York, 1974.
- [Ver26] Vernam, G.S.: Cipher printing telegraph systems for secret wire and radio telegraphic communications: *J. AIEE* **45** (1926), 109–115.
- [VeYo16] Veblen, O.; Young, J.W.: *Projective Geometry*: 2 vols. Ginn & Co., Boston, Mass., 1916.
- [Wal90] Walker, M.: Information-theoretic bounds for authentication schemes: *J. Cryptology* **2** (1990), 131–143.

# Stichwortverzeichnis

$(n, s)$ -Menge 203  
16 Punkte-Satz 67

## A

abhängig 13  
Abstand 188, 218  
Achse einer Kollineation 94  
affine Ebene 26  
affine Geometrie 26  
affine Raum der Dimension 26  
aktiver Angriff 222  
Algorithmus 222  
allgemeine Lage 47, 71  
Anführer 194  
Angriff, aktiver 222  
Angriff, passiver 221  
äquivalent 151  
aufgespannter Unterraum 10  
aufspannen 10  
Austauscheigenschaft 12  
Austauschlemma 15  
Austauschsatz 15  
Authentifikation 222  
Authentifikationscode 223, 232  
Authentifikationssystem 232  
authentifizieren 222  
authentifizierte Nachricht 222  
Automorphismus 20  
axiale Kollineation 101  
Axiom von PASCH 6

## B

BAER R. 101  
Basis 13, 191  
Basisergänzungssatz 16  
begleitender Automorphismus 118  
Betrugswahrscheinlichkeit 233, 241  
Bewegung 172  
Bewegung, eines Fachwerkes 173  
Bewegung, gerade 172  
Bewegung, infinitesimale 176  
Bewegung, starre 172  
Bogen 204  
Bogen, vollständiger 216  
BUEKENHOUT Francis 31  
BUEKENHOUT-TITS-Geometrie 35

## C

cap 204  
CEVA Giovanni 87  
charakteristischer Vektor 208

Chiffprat 224  
Code 188  
Code, dualer 192  
Code, Länge 188  
Code, perfekter 197  
Codewort 187, 188, 189  
codieren 187  
Compartment Scheme 243

## D

DANDELIN Germinal Pierre 67  
Datenauthentizität 231  
Datenintegrität 231  
Datensatz 221  
DE BRUIJN N.G. 80  
decodieren 187, 190  
DESARGUES Girard 57  
DESCARTES René 53  
Diagramm 32, 34, 153  
Differenzenmenge 82  
Dilatation 108  
Dimension 17  
Dimensionsformel 18  
direktes Produkt 45  
Dreiecksaxiom 49  
Dreieck 133  
duale Aussage 7  
duale Ebene 9  
duale Geometrie 8  
dualer Code 192  
Dualitätsprinzip 7, 8, 9

## E

Ebene 10, 17  
Ebene, duale 9  
Ecken 171  
Elation 96  
elliptisch 147  
Empfänger 221  
endlich erzeugbar 14  
endlich erzeugt 14  
endlicher projektiver Raum 22  
entschlüsseln 222, 248  
ERDÖS P. 80  
Erster Struktursatz für affine Räume 114  
Erster Struktursatz für projektive Räume 114  
Erzeugendensystem, minimales 13  
Erzeugnis 10

**F**

Fachwerk 171  
 Fachwerk, bipartit 176  
 Fachwerke, bewegliche 173  
 Fachwerke, kongruente 173  
 Fahne 3  
 Fahne, maximale 3  
 FANO Gino 86  
 Faserung 253  
 Fehlervektor 188  
 Fixgerade 94  
 Fixpunkt 94  
 Fundamentalsatz der projektiven Geometrie 126

**G**

GALLUCCI 67  
 geheimer Schlüssel 223  
 Geheimtext 222, 224, 248  
 Generatormatrix 191  
 Geometrie 1  
 Geometrie, affine 26  
 Geometrie, duale 8  
 Geometrie, projektive 17  
 Geometrie, zusammenhängende 36  
 Geraden 5  
 Gewicht 192  
 GILBERT E.N. 233  
 GOLOMB 226  
 Grad 210  
 Gruppenschema 243

**H**

HAMMING Richard W. 188  
 HAMMING-Abstand 188  
 HAMMING-Code 196  
 HAMMING-Code, erweiterter 200  
 HAMMING-Kugel 189  
 Hierarchische Schema 243  
 homogene Koordinaten 63  
 homogenen Koordinaten einer Hyperebene 65  
 Homologie 96  
 hyperbolisch 147  
 hyperbolische Quadrik 71  
 Hyperboloid 71, 136, 142  
 Hyperebene 17  
 Hyperovale 207

**I**

Impersonation 231  
 Index 139  
 Inzidenz 2  
 induzierte quadratische Menge 137  
 induzierte Zentralkollineation 96, 131  
 infinitesimal beweglich 176  
 infinitesimal starr 176

inhomogene Koordinaten 66  
 inzident 2  
 Inzidenz 2  
 Inzidenzrelation 2  
 Inzidenzstruktur 5  
 ISBN-Code 217  
 isomorph 20  
 Isomorphismus 20

**K**

Kalotte 204  
 KANT Immanuel 1  
 Kante 32, 34, 171  
 Kantenfunktion 171  
 kartesisch 232  
 $k$ -Bogen 182  
 Kegel 136, 142, 148  
 Kegelschnitt 161  
 Key-Management 240  
 Klartext 222, 248  
 KLEIN Felix 155  
 KLEINSche quadratische Menge 155  
 KLEINSche Quadrik 166  
 Knoten 32, 34, 206, 217  
 kollinear 10  
 Kollineation 20  
 Kollineation, axiale 101  
 Kollineation, projektive 124  
 Kollusion 250  
 Kontrollmatrix 193  
 Koordinaten 63  
 Koordinaten, homogene 63  
 Koordinaten, inhomogene 66  
 koordinatisierter projektiver Raum 54  
 Körper 53  
 Kugel 189

**L**

linearer  $[n, k]$ -Code 191  
 linearer Raum 78  
 Linearmenge 9  
 Loch 226

**M**

MAC 232  
 MACWILLIAMS F.J. 233  
 Mariner 9 213  
 $\max_{d-1}(r, q)$  205  
 maximaler  $\mathcal{Q}$ -Unterräume 139  
 maximum distance separable 202  
 MDS-Code 202  
 MENELAUS von Alexandria 87  
 Message Authentication Code 232  
 Minimalabstand 189  
 Minimalgewicht 192  
 Mittelpunkt 189  
 MOULTON F.R. 74



MOULTON-Ebene 74

MULLER D.E. 208

Multilevel Scheme 243

## N

Nachricht 187, 188, 232, 248

natürlicher Parallelismus 27

negativer Punkt 106

Netz 236

$n$ -fach perfektes Authentifikationssystem 238

nichtausgeartet 7

nichtausgeartete quadratische Form 159

nichtkollinear 10

## O

one-time pad 224

Ordnung 23, 30, 82

orthogonal 193

out-of-phase Autokorrelation 227

Oval 141

Ovalebene 207

Ovoid 142

## P

PAPPOS 57

parabolisch 147

parallel 27

Parallelenscharen 27

Parallelismus 26, 236

Parallelismus, natürlicher 27

Parkett 41

Parkett, reguläres 42

Pasch, Moritz 6

passiver Angriff 221

perfekter Code 197

perfektes Authentifikationssystem 235

perfektes Shared Secret Scheme 244

perfektes Verschlüsselungssystem 225

Periode 226

periodische Folge 226

platonischen Körper 47

PLAYFAIRSches Parallelenaxiom 28

PLÜCKER Julius 162

PLÜCKER-Koordinaten 162

PLÜCKERSche Quadrik 166

Polarräume 158

Präschlüssel 249

projektive Ebene 7

projektive Geometrie 17

projektive Kollineation 124

projektiver Abschluss 26

projektiver Raum 7

projektiver Raum, direktes Produkt 45

projektiver Raum, verallgemeinerter 44

Punktaddition 105

Punkte 5

## Q

$\mathbb{Q}$ -Gerade 135

quadratische Form 158

quadratische Form, nichtausgeartet 159

quadratische Menge 135

quadratische Menge, induzierte 137

quadratische Menge, nichtausgeartet 137

Quadrik 159

Quadrik, affine 179

Quadrik, hyperbolische 71

$\mathbb{Q}$ -Unterraum 135

$\mathbb{Q}$ -Unterraum, maximaler 139

Quotientengeometrie  $A/Q$  46

Quotientengeometrie  $A/U$  46

Quotientengeometrie  $P/Q$  19

QVIST B. 206

## R

Radikal 137

Radius 189

Rahmen 125

Rahmen, geordneter 125

Rang 3

Rang  $r$ -Geometrie 3

rationale Normkurve 72

REED I.S. 208

REED-MULLER-Code 208

Regelfläche 69

regulär 103

Regulus 69, 142

Regulus, entgegengesetzter 69

Residuum 33

resistent 250

## S

Satz von BAER 98

Satz von CEVA 87

Satz von DESARGUES 58

Satz von HESSENBERG 62

Satz von MENELAUS 87

Satz von PAPPOS 60

scharf transitiv 103

Schiefkörper 53

Schiefkörper, echter 53

Schließungssätze 57

Schlüssel 224, 248

Schwelle 243

Schwellenschema 242

Sekante 204

semilineare Abbildung mit begleitendem

Automorphismus 118

Sender 221

SHANNON C. 225

Shared Secret Scheme, perfektes 244

Shared Secret Scheme, robustes 242

SINGER-Zyklus 84, 227

Singleton-Bound 202  
 SLOANE N.J.A. 233  
 Spitze 136, 137, 142, 148  
 Starrheitsmatrix 174  
 String 226  
 Stromchiffre 224  
 Struktursätze 114, 122  
 Substitution 231  
 symmetrische Differenz 209  
 symmetrische Kryptoverfahren 223  
 Syndrom 194  
 Syndrom-Decodierung 195

## T

Tangente 135  
 Tangentialraum 135  
 Teilgeheimnis 240  
 Teilnehmergruppe, legale 241  
 Teilnehmergruppe, nichtlegale 241  
 $t$ -fehlererkennenden Code 216  
 $t$ -fehlerkorrigierender Code 189  
 Threshold Scheme 242  
 TITS Jaques 31  
 Translation 96, 103  
 Transversale 67  
 Trapezaxiom 49  
 Trialität 158  
 trivialer Unterraum 17  
 Typ 3

## U

unabhängig 13  
 uneigentliche Hyperebene 26  
 unendlich ferne Punkte 26  
 Unterraum 9  
 Unterraum, trivialer 17

## V

VEBLEN-YOUNG-Axiom 6  
 Vektorraum 53  
 verallgemeinerter projektiver Raum 44  
 verallgemeinertes Viereck 154  
 Verbindungssatz 44  
 VERNAM G.S. 224  
 verschlüsseln 222, 248  
 Verschlüsselung 221  
 Verschlüsselungsalgorithmus 248  
 Viereck 42

## W

windschief 67  
 windschiefe Unterräume 67  
 WITT E. 146  
 WOM-Code 213

## Z

Zentralkollineation 94  
 Zentralkollineation, induzierte 96, 131  
 Zentrum einer Kollineation 94  
 Zugriffsstruktur 241  
 Zweiter Struktursatz für affine Räume 122  
 Zweiter Struktursatz für projektive Räume 122  
 Zyklus 226

# Symbolverzeichnis

$(k_0:k_1:\dots:k_d)$	homogene Koordinaten eines Punktes 63	$\mathbf{P}(V)$	von $V$ erzeugter projektiver Raum 54
$(k_1, \dots, k_d)$	inhomogenen Koordinaten eines Punktes 66	$\mathcal{P}^*$	Punktmenge des affinen Raumes $\mathbf{P} \setminus \mathbf{H}$ 105
$[k_0:k_1:\dots:k_d]$	homogene Koordinaten einer Hyperebene 65	$\mathbf{P}/Q$	Quotientengeometrie 19
$\parallel$	Parallelismus 26	$\text{PG}(d, K)$	über $K$ koordinatisierter projektiver Raum der Dimension $d$ 57
$\mathbf{A} = \mathbf{P} \setminus \mathbf{H}_\infty$	affiner Raum 26	$\text{PG}(d, q)$	über endlichen Körper mit $q$ Elementen koordinatisierter projektiver Raum der Dimension $d$ 57
$\mathbf{A}/Q$	Quotientengeometrie 46	$\mathbf{p}\Delta$	dualer projektiver Raum 9
$\mathbf{A}/U$	Quotientengeometrie 46	$\mathcal{Q}$	quadratische Menge 135
$\text{AG}(d, K)$	den über $K$ koordinatisierten affinen Raum der Dimension $d$ 66	$\mathcal{Q}_p$	Tangentialraum 135
$\text{AG}(q, d)$	über endlichen Körper mit $q$ Elementen koordinatisierter affiner Raum der Dimension $d$ 66	$\text{Rad}(\mathcal{Q})$	Radikal von $\mathcal{Q}$ 137
$\mathbf{C}^\perp$	dualer Code 192	$\text{Res}(\mathcal{F})$	Residuum von $\mathcal{F}$ 33
$d(\mathbf{C})$	Minimalabstand des Codes $\mathbf{C}$ 189	$S_r(v)$	HAMMING-Kugel 189
$\dim(\mathbf{P})$	Dimension eines projektiven Raums 17	$\mathbf{T}(\mathbf{H})$	Gruppe der Translationen (Zentralkollineationen mit Achse $\mathbf{H}$ und Zentrum auf $\mathbf{H}$ ) 103
$\dim V$	Vektorraumdimension 54	$\mathbf{T}(\mathbf{H})$	Gruppe der Translationen von $\mathbf{A} = \mathbf{P} \setminus \mathbf{H}$ 116
$D_{\mathbf{O}}$	Gruppe der Dilatationen (Zentralkollineation mit Achse $\mathbf{H}$ und Zentrum $\mathbf{O} \notin \mathbf{H}$ ) 108	$\mathbf{T}(Z, \mathbf{H})$	Gruppe der Zentralkollineationen mit Achse $\mathbf{H}$ und Zentrum $Z \in \mathbf{H}$ 107
$\mathcal{F}$	Fahne 3	$\mathbf{U}$	Unterraum 9
$\mathbf{G} = (\Omega, I)$	Geometrie 1	$\langle v \rangle^\perp$	160
$\mathbf{G}^\Delta$	duale Geometrie 8	$\mathcal{U}(\mathbf{P})$	Menge der Unterräume von $\mathbf{P}$ 17
$\text{Ham}(r)$	HAMMING-Code 196	$\mathcal{U}^*(\mathbf{P})$	Menge der nichttrivialen Unterräume von $\mathbf{P}$ 17
$\text{Ham}(r)^*$	erweiterter HAMMING-Code 200	$w(\mathbf{C})$	Minimalgewicht des Codes $\mathbf{C}$ 192
$H^T$	zu $H$ transponierte Matrix 65	$\Gamma$	Gruppe der Kollineationen von $\mathbf{A}$ 116
$\mathbf{H}_\infty$	uneigentliche Hyperebene 26	$\Gamma_{\mathbf{O}}$	Gruppe der Kollineationen von $\mathbf{A}$ , die den Punkt $\mathbf{O}$ festlassen 116
$I$	Inzidenzrelation 2	$\Theta_r(q)$	$q^r + \dots + q + 1$ 24
$\max_{d-1}(r, q)$	maximales $n$ , sodass in $\text{PG}(r-1)$ eine $(n, d-1)$ -Menge existiert 205	$\chi(\mathcal{R})$	charakteristischer Vektor 208
$\mathbf{O}$	festgehaltener Punkt von $\mathbf{P} \setminus \mathbf{H}$ 105	$\langle \mathcal{X} \rangle$	Erzeugnis der Menge $\mathcal{X}$ 10
$\mathbf{P} = (\mathcal{P}, \mathcal{Q}, I)$	projektiver Raum 7		