[ABV 89] D. Ash, I. Blake, S. Vastone - Low complexity normal bases, *Discrete Applied Mathematics*, No. 25, 1989, pp.191-210.

[AGP 86] I. Angheloiu, E. Gyorfy, V. V. Patriciu - Securitatea şi protecţia informaţiei în sistemele electronice de calcul, Editura Militară, Bucureşti, 1986.

[AI 84] T. Albu, Ion D. Ion - Capitole de teoria algebrică a numerelor, Ed. Academiei, Bucureşti, 1984.

[AM 93] L. Atkin, F. Morain-Elliptic curves, primality proving and some *Titanic* primes, Internet , Inria-ftp, 1997.

[AMOV 91] G. Agnew, R. Mullin, I. Onyszchuk, S. Vanstone - An implementation for a fast public-key cryptosystem, *Journal of Cryptology*, No.3, 1991, pp.63-79.

[AMV 93] G. Agnew, R. Mullin, S. Vanstone - An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$, *IEEE Journal on Selected Areas in Communication*, Vol.11, No.5, June 1993, pp. 804-813.

[And 91] R.J. Anderson - Tree Functions and Cipher Systems, *Cryptologia*, Vol.15, No.3, 1991, 194-206.

[Ang 72] I. Angheloiu - Teoria codurilor, Editura Militară, Bucureşti, 1972.

[APD 92] M. Antonescu, E. Petac, P. Duma - Implementarea unui algoritm DES, *Sesiune de comunicări ştiinţifice*, Academia Navală "Mircea cel Bătrân" Constanţa, noiembrie 1992, pp. 29 - 33.

[AR 82] D. Andelman, J. Reeds - On the Cryptanalysis of Rotor Machines and Substitution – Permutation Networks, *IEEE Transaction on Information Theory*, Vol.IT-28, No.4, 1982, 578-584.

[Ara 93] B. Arazi - Double – Precision Modular Multiplication Based on a Single – Precision Modular Multiplier and a Standard CPU, *IEEE Journal on Selected Areas in Communication*, Vol.11, No.5, June 1993, pp.761-769.

[Bac 90] E. Bach - Number theoretic algorithms, *Annual review in Computer Science* , No. 4, 1990, pp.119-172.

[Băc 81] C. Băcanu - Consideraţii privind alegerea unui algoritm de criptare automată a datelor, Teză de doctorat, Bucureşti, 1981.

[BC 89] A. Bender, G. Castagnoli - On the implementation of elliptic curve cryptosystems, *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Sciences, 435(1990), Springer-Verlag, pp.417-426.

[BS 63] T. C. Bartee, D. I. Schneider - Computation with Finite Fields, *Information and Control*, Vol.6, 1963, pp. 79-98.

[Ben 81] M. Ben - Probabilistic algorithms in finite fields, *22nd Annual Symposium on Foundations of Computer Science*, 1981, pp. 394-398.

[Bet 88] T. Beth - Efficient zero-knowledge identification scheme for smart cards, *Advances in Cryptology – EUROCRYPT '88*, Lecture Notes in Computer Sciences, No. 330, 1988, Springer-Verlag, pp.77-84.

[BG 89] T. Beth, D. Gollman - Algorithm enginering for public-key algorithms, *IEEE Journal on Selected Areas in Communication*, Vol.7, No.4, May 1989, pp.458-466.

[BKR 86] S. Burton, J.Kalishi, R. Rivest - Is DES a Pure Cipher?, *Proceedings on Advances in Cryptology*, Crypto'85, Springer-Verlag, 1986.

[BLSTW 83] J. Brillhard, D. Lehmer, J. Selfridge, B. Tuckerman, S. Wagstaff - Factorizations of $b^n \pm 1$, b = 2, 3, 5, 6, 7, 10, 11, 12 up to high powers, *Contemporary Mathematics*, No. 22, 1983.

[BM 84] M. Blum, S. Micali - How to generate cryptographically strong sequences of pseudo-random bits, *SIAM Journal on Computing*, No.13, 1984, pp. 850-864.

[BM 92] E. Brickell, K. McCurley - An interactive identification scheme based on discrete logarithms and factoring, *Journal of Cryptology*, No.5, 1992, pp. 29-39.

[BM 94] J. Borns, C. Mitchell - Parameter Selection for Server-Aided RSA Computation Schemes", *IEEE Transaction on Computers*, Vol.43, No. 2, 1994, pp. 163-174.

[BNŞDPIRV 83] M. Becheanu, C. Niță, M. Ștefănescu, A. Dincă, I. Purdea, I.D. Ion, N. Radu, C. Vraciu - Algebră pentru perfecționarea profesorilor, Ed. Didactică și Pedagogică, București, 1983.

[Boe 88] B. Boer - Diffie-Hellman is a strong as discrete log for certain primes, *Advances in Cryptology – CRYPTO '88*, Lecture Notes in Computer Sciences, No. 403, 1990, Springer-Verlag, pp. 530-539.

[Boo 81] K. S. Booth - Authentication of signature using public key encryption, *Communications of the ACM*, Vol.24, No.11, November 1981; pp.772-774.

[Bra 79] G. Brassard - A note on the complexity of cryptography, *IEEE Transaction on Information Theory*, No.25, 1979, pp. 232-235.

[Bra 88] G. Brassard - *Modern Cryptology: A Tutorial*, Springer-Verlag, Berlin,1988.

[Bri 90] E. Brickell - A survey of hardware implementations of RSA, *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Sciences, No. 435, 1990, Springer-Verlag, pp. 368-370.

[BS 91a] T. Beth, F.Schaefer - Non supersingular elliptic curves for public key cryptosystems, *Advances in Cryptology – EUROCRYPT '91*, Lecture Notes in Computer Sciences, No. 547, 1991, Springer-Verlag, pp. 316-327.

[BS 91b] E. Biham, A. Shamir - Differential Cryptoanalysis of FEAL and N-Hash, *Proceedings of Eurocrypt '91*, Univ. of Sussex, UK, 1991.

[BŞ 85] Z.I. Borevici, I.R. Șafarevici - Teoria numerelor, Editura Științifică și Enciclopedică, București, 1985.

[Bul 95] C. Bulăceanu - Rețele locale de calculatoare, Ed. Tehnică, București, 1995.

[BW 1988] J. Buchmann, H. Williams - A key-exchange system based on imaginary quadratic fields, *Journal of Cryptology*, No.1, 1988, pp.107-118.

[Cal 82] C. Calude, Complexitatea calculului. Aspecte calitative, Editura Științifică și Enciclopedică, București, 1982.

[Cas 91] J. Cassels - *Lectures on Elliptic Curves*, Cambridge University Press, 1991.

[CCFPP 88] L. Coculescu, V. Cristea, I. Finta, V.V. Patriciu, F. Pilat - Proiectarea sistemelor teleinformatice, Editura Militară, București, 1988.

[CCMOR 65] I. Creangă, C. Cazacu, P. Mihuț, Gh. Opaiț, C. Reischer - Introducere în teoria numerelor, Editura Didactică și Pedagogică, București, 1965.

[CK 78] I. Csiszar, J. Korner - Broadcast Channels with Confidential Messages, *IEEE Transaction on Information Theory*, Vol.IT-24, No. 3, 1978, pp.339-348.

[CL 93] C.C. Chang, H.C. Lee - A New Generalized Group-Oriented Cryptoscheme Without Trusted Centers, *IEEE Journal on Selected Areas in Communication*, Vol.11, No. 5, 1993.

[CL 96] F. Chabaud, R. Lercier - *ZEN – A new toolbox for computing in finite extensions over finite rings*, INRIA-ftp, July, 1996.

[Cop 84] D. Coppersmith - Fast evaluation of logarithms in fields of characteristic two, *IEEE Transaction on Information Theory*, No. 30, 1984, pp.587-794.

[COS 86] D. Coppersmith, A. Odlyzko, R. Schroeppel - Discrete logarithms in $GF(p^n)$, *Algorithmica*, No. 1, 1986, pp.1-15.

[CP 82] L. Coculescu, C. Poinariu - Teleprelucrarea datelor, Editura Militară, 1982.

[CR 88] B. Chor, R. Rivest - A knapsack-type public key cryptosystem based on arithmetic in fields, *IEEE Transaction on Information Theory*, No.34, 1988, pp.901-909.

[Dav 83] D. W. Davies - Applying the RSA digital signature to electronic mail, *Computer*, Vol.16, No.2, 1983, pp. 55-62.

[DD 85] M. Davio, Y. Desmedt - Efficient Hardware and Software Implementation of DES, *Proceedings of CRYPTO '84*, Springer-Verlag, 1985.

[Den 83] D. E. Denning- Protecting public keys and signature keys, *Computer*, Vol.16, No.2, 1983, pp. 27-35.

[DH 76] W. Diffie; M. Hellman - New directions in cryptography, *IEEE Transaction on Information Theory*, No. 22, 1976, pp. 644-654.

[DH 79] W. Diffie, M. Hellman - Privacy and authentication: an introduction to cryptography, *IEEE Transaction on Information Theory*, No.67, 1979, pp. 397-427.

[Dif 91] W. Diffie - The first ten years of public key cryptography, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1991, pp.135-175.

[DM 87] Y. Driencourt, J. Michon - Elliptic codes over a field of characteristic 2, *Journal of Pure and Applied Algebra*, No. 45, 1987, pp.15-39.

[DP 87] D. W. Davies, W. L. Price - Security for Computer Networks, Great Britain, John Wiley&Sons, 1987.

[DVG 84] Y.G. Desmedt, J.P. Vanderwalle, R.J.M. Govaerts - A Critical Analysis of the Security of Knapsack Public-Key Algorithms, *IEEE Transaction on Information Theory*,Vol.IT-30, 4(1984), pp.601-610.

[EGS 86] S. Even, O. Goldreich, A. Shamir - On The Security of Ping-Pong Protocols Using RSA, *Proceedings of CRYPTO '85*, California, 1986.

[EL 83] R. Eier, H. Lagger - Trapdoors in Knapsack Cryptosystems, *Proceedings of CRYPTO '82*, Springer-Verlag, 1983.

[EIG 85a] T. ElGamal - A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transaction on Information Theory*, No. 31, 1985, pp.469-472.

[EIG 85b] T. ElGamal - A subexponential-time algorithm for computing discrete logarithms over $GF(p^2)$, *IEEE Transaction on Information Theory*, No.31, 1985, pp.473-481.

[EMMT 78] W. F. Ehrsam, S. M. Matyas, C.H. Mayer, W.L. Tuchman - A Cryptographic Key Management Scheme for Implementing DES, *IBM Syst. Journal*, No. 2, 1978.

[Fen 89] M. Feng - A VLSI architecture for fast inversion in $GF(2^m)$, *IEEE Transaction on Computers*, No.38, 1989, pp. 1383-1386.

[FY 89] Y. Frankel - A practical protocol for large group oriented networks, *Advances in Cryptology – EUROCRYPT '89*, Lecture Notes in Computer Sciences, (1989), Springer-Verlag, pp. 56-61.

[FS 87] A. Fiat, A. Shamir - How to prove yourself: Practical solutions to identification and signature problems, *Advances in Cryptology – CRYPTO '86*, Lecture Notes in Computer Sciences, No.293, 1987, Springer-Verlag, pp.186-194.

[GG 87] W. Geiselmann, D. Gollimann - VLSI design for exponentiation in $GF(2^m)$, *Advances in Cryptology – AUSCRYPT '90*, Lecture Notes in Computer Sciences, No. 293, 1987, Springer-Verlag, pp.186-194.

[GL 92] S. Gao, H. W. Lenstra - Optimal normal based, *Designs, Codes and Cryptography*, 2(1992),pp. 315-323.

[GUQ 91] L. Guillou, M. Ugon, J. Quisquater - The smart card: a standardized security device dedicated to public cryptology, Contemporary Cryptology: The Science of Information Integrity, *IEEE Press*, New York, 1991, pp. 561-613.

[Has 86] J. Hastad - On using RSA with low exponent in a public key network, *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Sciences, No. 218, 1986, Springer-Verlag, pp. 403-408.

[Hel 77] M. Hellman - An Extension of the Shannon Theory Approach to Cryptography, *IEEE Transaction on Information Theory*, No. 3, 1977, pp. 289-294.

[HR 83] M. Hellman,M. Reyneri - Fast computation of discrete logarithms in *GF(q)*, *Advances in Cryptology – CRYPTO '82*, Plenum Press, 1983, pp. 3-13.

[Hus 87] D. Husemoller - *Elliptic Curves*, Springer-Verlag, New York,1987.

[Hwa 90] T. Hwang - Cryptosystem for group oriented cryptosystem for database sharing, *Proceedings of EUROCRYPT '90*, Belgium, 1990, pp. 317-324.

[HY 93] L. Harn, S. Yang - ID – Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution, *IEEE Journal on Selected Areas in Communication*,Vol. 11, No.5, 1993, pp.757-760.

[IN 91] Ion D. Ion, R. Nicolae, Algebra, Ed. Didactică şi Pedagogică, Bucureşti, 1991.

[Ing 82] I. Ingemarsson - Conference Key Distribution System, *IEEE Transaction on Information Theory*, 1982.

[ITT 86] T. Itoh, O. Teechai, S. Tsujii - A fast algoritm for computing multiplicative inverses in $GF(2^t)$ using normal bases, *Japan Society Electron. Comm.*, No. 44, 1986, pp. 31-36.

[Kal 87] B. Kaliski - A pseudorandom bit generator based on elliptic logarithms, *Advances in Cryptology – CRYPTO '86*, Lecture Notes in Computer Sciences, 293, 1987, Springer-Verlag, pp. 84-103.

[Kal 91] B. Kaliski - One-way permutations on elliptic curves, *Journal of Cryptology*, No. 3, 1991, pp.187-199.

[Key 76] E.L. Key - An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators, *IEEE Transaction on Information Theory*, Vol.IT-22, No.6, 1976, pp. 732-736.

[Knu 83] D. E. Knuth - Tratat de programarea calculatoarelor - Algoritmi seminumerici, Editura Tehnică, Bucureşti, 1983.

[Kob 84] N. Koblitz - Introduction to Elliptic Curves and Modular Forms, Springer-Verlag, 1984.

[Kob 87a] N. Koblitz - A Course in Number Theory and Cryptography, Springer-Verlag, New York, Berlin, 1987.

[Kob 87b] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, No. 48, 1987, pp. 203-209.

[Kob 89] N. Koblitz, Hyperelliptic cryptosystems, *Journal of Cryptology*, No.1, 1989, pp. 139-150.

[Kob 91] N. Koblitz - Constructing elliptic curve cryptosystems in characteristic 2, *Advances in Cryptology – CRYPTO '90*, Lecture Notes in Computer Sciences, No. 537, 1991, Springer-Verlag, pp.156-167.

[Kob 91] N. Koblitz - Elliptic curve implementation of zero-knowledge blobs, *Journal of Cryptology*, No. 4 , 1991, pp.207-213.

[KMQV 96] J. Koeller, A. Menezes, M. Qu, A. Vanstone – Standard for RSA, Diffie-Hellman and related public-key cryptography, Certicom Corp.,Ontario, Canada, 1996.

[KT 91] V. Korznik, A. Turkin - Cryptanalysis of McEliece's Public-Key Cryptosystem, *Proceedings of EUROCRYPT '91*, Univ. of Sussex, U.K., 1991.

[LG 85] L. Livovschi, H. Georgescu - Bazele informaticii. Algoritmi: Elaborare şi complexitate, Tipografia Universităţii Bucureşti, 1985.

[LG 88] J. H. van Lint, G. van der Geer - Introduction to Coding Theory and Algebraic Geometry, Birkhauser Verlag, Basel-Boston-Berlin, 1988.

[LN 87] R. Lidl, H. Niederreiter - Finite Fields, Cambridge University Press,1987.

[LW 91] Y. X. Li, X. M. Wang - A joint authentication and encryption scheme based on algebraic coding theory, *Lecture Notes in Computer Science*, Vol.539, Springer-Verlag, 1991, pp. 241-245.

[Map 91a] Maple V - First Leaves: A Tutorial Introduction to Maple V, Springer-Verlag, New York, Berlin-Heidelberg, 1991.

[Map 91b] Maple V - Language Reference Manual, Springer-Verlag, New York, Berlin-Heidelberg, 1991.

[Mas 88] J. L. Massey - An introduction to contemporary cryptology, *Proceedings of the IEEE*, Vol.76, No.5,1988, pp. 533-549.

[Mas 91] J. L. Massey - Contemporary Cryptology: The Science of Information Integrity,
IEEE Press, Piscaaway, NJ, 1991.

[MB 91] V. Muller, J. Buchmann - Computing the number of points of elliptic curves over finite fields, *Proceeding of ISSAC '91*, ACM Press 1991, pp. 179-182.

[MB 96] V. Muller, J. Buchmann - Computing the number of points of elliptic curves over finite fields, *Internet-Inria,ftp,1996.*

[McE 87a] R. J. McEliece - A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report 42-44*, Jet Propulsion Laboratory, 1987, pp. 114-116.

[McE 87b] R. J. McEliece - *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[Mer 78] R. C. Merkle - Secure communications over insecure channels, *Communications of the ACM*, Vol.21, No.4, 1978, pp.294 - 299.

[Mer 90] R. Merkle - A certified digital signature, *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Sciences, No. 435, 1990, Springer-Verlag, pp. 218-238.

[MH 78] R. C. Merkle, M. E. Hellman - Hiding information and signatures in trapdoor knapsacks, *IEEE Transaction on Information Theory*, Vol.24, No.5, 1978, pp. 525-530.

[Mil 86] V. Miller - Uses of elliptic curves in cryptography, *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Sciences, No. 218, 1986, Springer-

Verlag, pp. 417-426.
[MKI 90] T. M. Matsumoto,K. Kato, H. Imai – Speeding up secret computations with insecure auxiliary devices, *Proceedings – CRYPTO '88*, Santa Barbara, CA, 1990, pp. 233-238.
[MM 78] S. M. Matyas, C. H. Meyer - Generation, distribution, and installation of cryptographic keys, *IBM Systems Journal*, Vol.17, No.2, 1978, pp.126-137.
[Mor 91] F. Morain - Building cyclic elliptic curves modulo large primes, *Advances in Cryptology – EUROCRYPT '91*, Lecture Notes in Computer Sciences, No.547, 1991, Springer-Verlag, pp. 328-336.
[Mor 91] C. Moreno - *Algebraic Curves over Finite Fields*, Cambridge University Press,1991.
[MOVW 89] R. Mullin, I. Onyszchuk, S. Vanstone, R. Wilson - Optimal normal based in $GF(p^n)$, *Discrete Applied Mathematics*, No.22, 1988/89, pp. 149-161.
[Mun 79] V. Munteanu - Teoria transmisiunii informației, Iași, 1979.
[MV 90a] A. Menezes, S. Vastone - The implementation of elliptic curve cryptosystem, *Advances in Cryptology – AUSCRYPT '90*, Lecture Notes in Computer Sciences, No. 453, 1990, Springer-Verlag, pp. 2-13.
[MV 90b] A. Menezes, S. Vastone - Isomorphism classes of elliptic curves over finite fields of characteristic 2, *Utilitas Mathematica*, No. 38, 1990, pp.135-154.
[MV 90c] A. Menezes, S. Vastone - Isomorphism classes of elliptic curves over finite fields, *Researce Report 90-91*, University of Waterloo, 1990.
[MV 92] A. Menezes, S. Vastone - A note on cyclic groups, finite fields, and the discrete logarithm problem, *Applicable Algebra in Engineering, Communication and Computing*, No.3, 1992, pp.67-74.
[NBS 77] National Bureau of Standards - Data Encryption Standard, Federal Information Processing Standard, U.S.Department of Commerce, FIPS PUB 46, Washington, DC, 1977.
[NBS 80] National Bureau of Standards - DES Modes of Operation, Federal Information Processing Standard, U.S.Department of Commerce, FIPS PUB 81, Washington, DC, 1980.
[NBS 81] National Bureau of Standards - Guidelines for Implementing and Using the NBS Data Encryption Standard, Federal Information Processing Standard, U.S.Department of Commerce, FIPS PUB 74, Washington, DC, 1981.
[NBS 91] National Bureau for Standards and Technology - A proposed federal information processing standard for digital signature standard (DSS), Technical Report FIPS PUB XX, Draft, August 1991.
[NBS 92] National Bureau for Standards and Technology, - Annoucement and specifications for a secure hash standard (SHS), Technical Report FIPS PUB YY, Draft, January 1992.
[Nec 91] J. Nechvatal - Public key cryptography, Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1991, pp. 177-288.
[NIST 92] National Institute of Standards and Technology - Digital Signature Standard - The Digital Signature Standard, *Communications of the ACM*, 1992.
[NIST 95a] National Institute of Standards and Technology - Secure Hash Standard, Computer Security, FIPS PUB 180-1,1995.
[NIST 95b] National Institute of Standards and Technology - Digital Signature Standard, Computer Security, FIPS PUB XX,1995.
[NKR 94] S. Nandi, B. K. Kar, P. Pal Chaudhuri –Theory and Applications of Cellular Automata in Cryptography , *IEEE Transaction on Computers*, Vol.C-43, No.12, dec. 94, pp.1346-1357.
[NN 79] C. Năstăsescu, C. Niță - Teoria calitativă a ecuațiilor algebrice, Ed. Tehnică, București, 1979.
[NNV 93] C. Năstăsescu, C. Niță,C. Vraciu - Aritmetică și Algebră, Ed. Didactică și Pedagogică, București, 1993.
[NS 78] R. M. Needham, M. D. Schroeder - Using encryption for authentication in large networks of computers, *Communications of the ACM*, Vol.21, No.12, (1978), pp. 993-999.
[Odl 84] A.M. Odlyzko - Cryptanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme, *IEEE Transaction on Information Theory*, Vol.IT-30, 4(1984), pp. 594-600.
[Odl 85] A. Odlyzko - Discrete logarithms and their cryptographic significance, *Advances in Cryptology – EUROCRYPT '84*, Lecture Notes in Computer Sciences, 209(1985), Springer-Verlag, pp. 224-314.
[Pat 94] V. V. Patriciu - Criptografia și securitatea rețelelor de calculatoare, Ed. Tehnică, București, 1994.
[PBP 98] E. Petac, M. Bursuc, D. Petac - Metode și tehnici de implementare într-o rețea de calculatoare a criptosistemelor cu chei publice construite pe curbe eliptice - *Simpozion cu participare internațională: Războiul electronic și războiul informațional - două componente inseparabile ale acțiunii militare moderne* , Academia de Înalte Studii Militare, București, 23-24 Aprilie 1998, pp. 71-78.
[PCC 86] F. Pilat, L. Coculescu, V. Cristea - Teleinformatica, *Editura Științifică și Enciclopedică*, București, 1986.
[Per 78] R. C. Peralta - A simple and fast probabilistic algorithm for computing squate roots modulo a prime number, *IEEE Transaction on Information Theory*,Vol.IT-24,No.1, 1978, pp. 106-110.
[Pet 92] E. Petac - O metodă de protecție a informației în comunicațiile digitale, *Sesiune de comunicări științifice*, Academia Navală "Mircea cel Bătrân" Constanta, noiembrie 1992, pp. 33 - 35.
[Pet 94a] E. Petac - Nonlinear Key Generator for Cryptographic Methods, *Development & Application Systems*,The University "Ștefan cel Mare" Suceava, may 26-28, 1994, pp.139-142.
[Pet 94b] E. Petac - Some Computer-Oriented Cryptographic Methods, *Development & Application Systems*, The University "Ștefan cel Mare" Suceava, may 26-28, 1994, pp.143-146.
[Pet 94c] E. Petac - Protecția informației în sistemele de transmisiuni - Stadiul actual, *Referat teză de doctorat nr.1*, Iași, 1994.
[Pet 94d] E. Petac - Protecția informației în sistemele de transmisiuni de date, *Temă de cercetare*, Vol.1 (150 pagini - T12254), Academia Navală "Mircea cel Bătrân, Constanța, 1993/1994.
[Pet 94e] E. Petac - Proiectarea unor funcții rezistente la corelații, *Sesiune de comunicări științifice* ,Centrul de cercetări al Marinei Militare - Constanța, octombrie 1994, pp.392- 395.
[Pet 95a] E. Petac - Considerații privind criptosistemele cu chei publice, *Referat teză de doctorat nr. 2*, Iași, 1995.
[Pet 95b] E. Petac - Utilizarea sistemelor neliniare în asigurarea protecției informației, *A XXVI -a Sesiune de comunicări științifice cu participare internațională*, Academia Tehnică Militară, București, 16-17 noiembrie,1995, pp.100-105.

[Pet 96a] E. Petac - Protecţia informaţiei în sistemele de transmisiuni de date, *Temă de cercetare*, Vol.2 (125 pagini - T12255), Academia Navală "Mircea cel Bătrân, Constanţa, 1995/1996.

[Pet 96b] E. Petac - Security Management for Data-Communication Networks, *Development and application systems*, "Stefan cel Mare" University,Suceava, 23-25 May 1996, pp. 87-92.

[Pet 96c] E. Petac - On the Construction of Elliptic Curve CryptoSystems, *Development and application systems*, "Stefan cel Mare" University, , 23-25 May 1996, pp.93-96.

[Pet 96d] E. Petac - On the Constructions of Hash Functions with Algebraic Geometric Codes, *Automatic, Control and Testing Conference*, Technical University Cluj Napoca, 23-24 May 1996, pp.61-64.

[Pet 96e] E. Petac - Elemente de proiectare a criptosistemelor cu chei publice exponentiale, *Sesiune de comunicări ştiinţifice*, Centrul de cercetări al Marinei Militare - Constanţa., octombrie 1996,pp.252--257.

[Pet 96f] E. Petac - Protocoale integrate in nivelul transport, *Sesiune de comunicări ştiinţifice* - Academia Aviaţiei şi Apărării Antiaeriene - Braşov , octombrie 1996, pp.59-64.

[Pet 96g] E. Petac - Aspecte ale utilizării curbelor eliptice pentru obţinerea unor protocoale de comunicaţii, *Sesiune de comunicări ştiinţifice*, Academia Aviaţiei şi Apărării Antiaeriene - Braşov, noiembrie 1996, pp.65-68.

[Pet 96h] E. Petac - Operaţii pe curbe eliptice - Algoritmi şi metode de lucru, *Sesiune de comunicări ştiinţifice*, Academia Trupelor de Uscat, Sibiu, decembrie 1996, pp.13 -18.

[Pet 97a] E. Petac - A New Public Key Encryption Scheme Using Elliptic Curves, *SCS'97 - International Symposium on Signals Circuits and Systems*, The Faculty of Electronics and Telecommunications of "Gh. Asachi" Technical University Iaşi, , October 2-3, 1997, pp.565 - 568.

[Pet 97b] E. Petac - Public Key Encryption Schemes Using Elliptic Curves, *Proceedings of the Eighth Congress of the International Maritime Association of Mediterranean*, Istanbul Technical University, 2-9 November, 1997, pp.16.2-9 - 16.2-13.

[Pet 97c] E. Petac - Some Fast Algorithms for Counting Points on Elliptic Curves Over $F2^m$, *Proceedings of the Eighth Congress of the International Maritime Association of Mediterranean* - Istanbul Technical University, 2-9 November, 1997, pp.16.2-14 - 16.2-20.

[Pet 97d] E. Petac - Principles and Methods of Computation for Counting Points on Elliptic Curves over $F2^m$, *A XXVII-a Sesiune de comunicari stiintifice cu participare internationala, Sectiunea 11 - Informatica si automatizarea conducerii trupelor*, Academia Tehnica Militara, 13-14 Noiembrie, 1997, Bucuresti, pp.126 - 133.

[Pet 97e] E. Petac - About a Method of Distribution Keys of a Computer Network Using Elliptic Curves, *IEEE International Symposium on Consumer Electronics, 1997 (ISCE'97)*, Singapore, 2-4 December 1997, pp.309-312.

[Pet 97f] E. Petac - *Security Elements of Communications Using Elliptic Curve Cryptosystems, The Third Asia-Pacific Conference on Communications (APCC'97)*, Sydney, Australia, 7-10 December, 1997, pp. 1362-1365.

[Pet 98a] E. Petac - Asupra unui protocol de tip token de distribuire a cheilor criptografice, *Simpozion cu participare internaţională: Războiul electronic şi războiul informaţional - două componente inseparabile ale acţiunii militare moderne*, Academia de Înalte Studii Militare, Bucureşti, 23-24 Aprilie 1998, pp. 79-86.

[Pet 98b] E. Petac – An elliptic curve conference key distribution system, *The 6th Biennial Conference on Electronics and Microsystems Technology – Baltic Electronics Conference, BEC '98*, Tallinn Technical University, Estonia, October 7-9, 1998 (în curs de publicare).

[PG 93] F. Păunescu, D. P. Golesteanu - Sisteme cu prelucrare distribuită şi aplicaţiile lor, Ed. Tehnică, Bucureţti, 1993.

[PH 78] S. Pohlig, M. Hellman - An improved algorithm for computing logarithms over *GF(p)* and its cryptographic significance, *IEEE Transaction on Information Theory*, No. 24, 1978, 106-110.

[Pie 85] J.P. Pieprzyk - On Public-Key Cryptosystems Built Using Polinomial Rings, *Proceedings of EUROCRYPT '85*, Austria, 1985.

[PL 97] E. Petac, L.. Livadariu - A Method for Distribution Keys Using Elliptic Curves, *A XXVII-a Sesiune de comunicari stiintifice cu participare internationala, Sectiunea 11 - Informatica si automatizarea conducerii trupelor*, Academia Tehnica Militara, Bucuresti,13-14 Noiembrie, 1997, pp.118 - 125.

[PP 95] E. Petac, D. Petac - A Method for Obtaining Public Key Cryptosystems with Goppa Codes, *Engineering Modern Electric Systems EMES '95*, Universitatea Oradea, 2-4 iunie 1995, pp. 282 - 285.

[PP 98] E. Petac, D. Petac - Some Elliptic Curve Protocols for the Security of Communications, *4th International Conference Telecommunication' 98*, Dom techniky ZSVTS Bratislava 21-22 April, Slovacia, 1998, pp.173-176.

[PSM 96a] E. Petac, T. Susanu, C Mamo - Security Architecture for Electronic Data Interchange, *Sintes 8 - International Symposium on Systems Theory*, University of Craiova, 6-7 June 1996, pp.183-188.

[PSM 96b] E. Petac, T. Susanu, C Mamo - An Analysis of Elliptic Curve Cryptosystems, *Sintes 8 - International Symposium on Systems Theory*, University of Craiova , 6-7 June 1996, pp.189-192.

[Pur 82] I. Purdea - Tratat de algebră modernă, Ed. Academiei, Bucureşti, 1982.

[PV 86] D. Popescu, C. Vraciu - Elemente de teoria grupurilor finite, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1986.

[Rit 90] T. Ritter - Substitution Cipher with pseudo-Random Shuffling: The Dynamic Substitution Combiner, *Cryptologia*,Vol.14, No.4, 1990, pp. 289-303.

[Riv 91] R. Rivest - The MD4 message digest algorithm, *Advances in Cryptology – CRYPTO '90*, Lecture Notes in Computer Sciences, 537, 1991, Springer-Verlag, pp. 303-311.

[RMSSF 93] F. Recacha, J.L. Melas, X. Simon, M. Soriano, J. Forne - Secure Data Transmision in Extended Ethernet Environments, *IEEE Journal on Selected Areas in Communication*,Vol.11, 5(1993), pp.794-803.

[RN 89] T. R. N. Rao., K. H. Nam - Private-key algebraic-code encryptions, *IEEE Transactions on Information Theory*, Vol.35, no.4, 1989, pp. 829-833.

[RSA 78] R. Rivest, A. Shamir, L. Adleman - A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, 21, 1978, pp. 120-126.

[Rub 79] F. Rubin - Decrypting a Stream Cipher Based on J-K Flip-Flops, *IEEE Transaction on Computers*, Vol.C-28, No.7, 1979, pp. 483-487.

[Ruc 87] H. Ruck - A note on elliptic curves over finite fields, *Mathematics of*

Computation, No. 49, 1987, pp. 301-304.
[Sal 93] A. Salomaa - Criptografie cu chei publice, Ed. Militara, Bucuresti, 1993.
[Săm 86] G. Sâmboan - Teoria lui Galois, Editura Tehnică, București, 1986.
[Sch 84] M.R. Schroeder - Number theory in science and communication, 1984.
[Sch 85] R. Schoof - Elliptic curves over finite fields and the computation of square roots mod *p*, *Mathematics of Computation*, No. 44, 1985, pp.483-494.
[Sch 87] R. Schoof - Nonsingular plane cubic curves over finite fields, *Journal of Combinatorial Theory*, A 46, 1987, pp. 183-211.
[Sch 90] C. P. Schnorr - Efficient identification and signatures for smart cards, *Advances in Cryptology – CRYPTO '89*, Lecture Notes in Computer Sciences, No. 435, 1990, Springer-Verlag, pp. 239-252.
[Sch 94] Schneier, B. - Applied cryptography, John Wiley and Sons, New York, 1994.
[Sha 49] C.E. Shannon - Communication theory of secrecy systems, *Bell System Technical Journal*, 28(1949), pp. 656-715.
[Sha 70] D. Shanks - Class number, a theory of factorization and generators, *Proc. Symposium of Pure Math. 20*, AMS 1970, pp. 415-440.
[Sha 84] A. Shamir - A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem, *IEEE Transaction on Information Theory*, Vol.IT-30, No.5,1984, pp.699-704.
[Sha 85] A. Shamir - Identity Based Cryptosystems and Signature Schemes, *Proceedings of CRYPTO '84*, Springer-Verlag, 1985, pp.47-53.
[Sho 92] V. Shoup – On fast and provably secure message authenticatiuon based on universal hashing, *Advances in Cryptology – CRYPTO '96*, Lecture Notes in Computer Sciences, No. 1109, 1996, Springer-Verlag, pp. 313-328.
[Shp 92] I.E. Shparlinski - Computational and Algorithmic Problems in Finite Fields, Kluwer Academic Publishers, Dordrecht/Boston/London, Vol.88, 1992.
[Sil 86] J. Silverman - The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.
[Sim 79] G. J. Simmons - Symmetric and asymmetric encryption, *ACM Computing Surveys*, Vol.11, No.4, 1979, pp. 305-330.
[Sim 91] G. Simmons (editor) - Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1991.
[Smi 81] M.E. Smid - Integrating the Data Encryption Standard into Computer Networks, *IEEE Transactions on Communications*, Vol.COM-29, No.6, 1981, pp.762-777.
[Spi 81] T Spircu - Structuri algebrice prin probleme, Ed. Științifică, București, 1981.
[SSTP 88] P. Scott, S. Simmons. S. Tavares, L. Peppard - Architectures for exponentiation in *GF(2ⁿ)*", *IEEE Journal on Selected Areas in Communication*, No. 6, 1988, pp. 578-586.
[ST 92] J. Silverman, J. Tate - Rational Points on Elliptic Curves, Springer-Verlag, New York,1992.
[SVH 96] B. Serpette, J. Vuillemin, J.C. Herve - Big Num.:A Portable and Efficient Package for Arbitrary-Precision Arithmetic, *Institute National de Recherche en Informatique et Automatique*, INRIA-ftp, June, 1996.
[Șaf 76] I. R. Șafarevici - Bazele geometriei algebrice, Ed. Științifică și Enciclopedică, București, 1976.
[Ște 93] M. Ștefănescu - Introducere în teoria grupurilor, Editura Universității "A. I. Cuza" ,Iași, 1993.
[Tak 92] N. Takagi - A Radix-4 Modular Multiplication Hardware Algorithm for Modular Exponentiation, *IEEE Transactions on Computers*, No.7, 1992, pp.949-956.
[TCA 93] S. Tsujii, J. Chao, K. Araki - A Simple ID – Based Scheme for Key Sharing, *IEEE Journal on Selected Areas in Communication*, Vol.11, No.5, 1993, pp.730-734.
[TI 89] S. Tsujii, T. Itoh - An ID-based cryptosystem based on the discret logaritm problem, *IEEE Journal on Selected Areas in Communication*, No.8, 1989, pp.467-473.
[Til 94] Johan von Tilburg - Security-Analysis of a Class of Cryptosystems Based on Linear Error-Correcting Codes, Teză de doctorat, Leidschendam, Germany, 1994.
[TY 92] N. Takagi, S. Yajima - Modular Multiplication Hardware Algorithms with a Redundant Representation and Their Application to RSA Cryptosystem, *IEEE Transactions on Computers*, No.7, 1992, pp. 887-892.
[Wat 69] W. C. Waterhouse - Abelian varieties over finite fields, *Ann. Sci. Ecole Norm. Sup.*, 4ᵉ ser. 2, 1969, pp. 521-560.
[Wie 90] M. Wiener - Cryptanalysis of Short RSA Secret Exponents, *IEEE Transaction on Information Theory*, Vol.36, No.3, 1990, pp. 553-558.
[Wil 80] M. Willett - Deliberate Noise in a Modern Cryptographic System, *IEEE Transaction on Information Theory*, Vol.IT-26, No.1, 1980, pp.102-104.
[WP 90] C. Wang, D. Pei - A VLSI design for computing exponentitions in *GF(2ⁿ)* and its application to generate pseudorandom number sequences, *IEEE Transactions on Computers*, 39, 1990, pp. 258-262.
[WT 86] A. F. Webster, S.E. Tavares – On the Design of S-Boxes, *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Sciences, 1986, Springer-Verlag, pp. 523-530.