

A Complete Bibliography of Publications in the *Journal of Mathematical Cryptology*

Nelson H. F. Beebe
 University of Utah
 Department of Mathematics, 110 LCB
 155 S 1400 E RM 233
 Salt Lake City, UT 84112-0090
 USA

Tel: +1 801 581 5254
 FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org,
beebe@computer.org (Internet)
 WWW URL: <http://www.math.utah.edu/~beebe/>

19 April 2024
 Version 1.08

Title word cross-reference

(2, 2) [PS20]. (2, 2, 2) [AJZT19]. $(n + 1)$ [ZMD20]. $(p^r - 1)/3$ [BW09]. 1 [SW07a]. 2 [AJZT19, Gau07, Hit09, SW07a]. 3 [CC15, LL15, MW12]. 4 [Kar10]. 5 [HL19]. 6 [Kar10]. LWE [COP24]. $ax \equiv b \pmod{n}$ [GP13]. $\text{GL}_2(\mathbf{F}_{p^n})$ [TNS20]. k [AMW07, BW09]. \mathbf{F}_{24m}^* [Kar10]. \mathbf{F}_{36m}^* [Kar10]. \mathbf{F}_p [BW09]. \mathbf{F}_{p^2} [DM20]. \mathbf{F}_{pk} [Duq11]. $\mathbf{Q}(\zeta_{2s})$ [BS19]. \mathbf{Z}/\mathbf{NZ} [ST24]. \mathcal{M} [WP11]. \mathcal{Q} [WP11]. MST_3 [BCM09]. n [DSS20, ZMD20]. $N = p^r q^l$ [LPS17]. p [KMNN19]. $p + q$ [MA17]. ρ [Oka12]. MST_3 [SvT10]. S [ZMD20].

-ary [KMNN19]. **-bit** [ZMD20]. **-boxes** [ZMD20]. **-CP-ABE** [COP24]. **-error** [AMW07, BW09]. **-ideal** [AJZT19]. **-rotation** [CC15]. **-round** [SW07a]. **-server** [SW07a]. **-threshold** [PS20]. **-torsion** [MW12]. **-values** [Oka12].

2019 [DKKS20]. **256** [DT17].

7 [GZ14].

ABE [COP24]. **abelian** [Rei17]. **aborts** [FS11]. **Abu** [Bla10]. **Access** [KK23, DS17, GD13, JSN13]. **achieving** [AL11]. **action** [JLLRL20, RS22]. **adaptive** [AL11, FS11]. **add** [FJ13]. **add-rotate-xor** [FJ13]. **addition** [FJ13]. **additive** [BDJ14]. **admit** [DN08]. **Advanced** [Sch08]. **adversary** [Dow15]. **AE** [ASB⁺18]. **Affine**

[CLS16, HWCD11]. **AG** [Tim24]. **Against** [Joy20, BS19, BBP⁺20, Moc23, MSP12, WS09]. **aggregation** [HS15b]. **Agrawal** [PS08]. **agreement** [Bro23, Mul11]. **AJPS** [CG20]. **al.** [MU10]. **algebra** [BCSV20, KU18, RZ18]. **Algebraic** [BF09, Par18, RUS23, TKF⁺20]. **algebras** [Ano20]. **algorithm** [BGMP08, BP20, BDJ14, JLLRL20, Pop17]. **Algorithms** [CCH⁺20, AR15, DSG21, Eke21, FJ13, NV08, PP18]. **alternating** [SW15]. **alternative** [CCI24]. **Among** [KT20]. **Analogue** [DSGKS20b]. **Analysis** [KU15, KU18, Maz12, YYS⁺17, CDK18, HVV14, MU08, NM08, Nan09, OPSB13, PSU13, Sch08, Wum19]. **analyze** [FJ13]. **Annual** [CLS20, CLY20]. **anonymous** [SSA17]. **Aperiodic** [BdW12, SvT13, vT18]. **Application** [DKKS20, Duq11, GGD20, Tim24, Tis11]. **Applications** [BBPS20, GPR17, BP20, FL08, FS11, JN16, SPB22]. **approach** [BFP09, CAR20, CLS16]. **approaches** [HS15b, TKF⁺20]. **Approximate** [CCH⁺20, Laa20]. **approximations** [SS16a]. **argument** [Mie08]. **Ariffin** [Bla10]. **arithmetic** [ATW08, Duq11, Gau07, HST10, HL09]. **arrays** [MN07]. **ary** [KMNN19]. **associated** [CN22]. **asymmetric** [AR15, Jia14]. **asymptotic** [KMPS10]. **Attack** [KMU20, TW20, AK17, BP22, BBP⁺20, BF09, HF07, Mor08, MU10, Sch17, Wum19]. **Attacks** [Joy20, BS19, CW22, DHS20, GKL15, HL10, KMPS10, KHK10, Moc23, MSP12, MU08, PS08, Pou16, RUS23, RMS24, WS09]. **attribute** [AL11]. **auction** [KMNN19]. **Authenticated** [BLLN21, TSJL20, ASB⁺18, CN22]. **authentication** [ACP10, Esk24, FHLMW08, JCK⁺18, LU08, MU10, PS20]. **automated** [Kob07, Kob12]. **Automatic** [RMS24]. **auxiliary** [Kus18]. **avalanche** [LC07]. **average** [AL07]. **Balanced** [Rei21, CLS09]. **barrier** [MPST16]. **Based** [PGS20, TSJL20, ACP10, BCM11, BGGJ20, CDK18, CG20, Esk24, GKL15, Gau07, GPV24, HS08, Jia14, KH23, KU15, KU18, LMPW15, MU08, PS15, Per12, RZ18, RST07, SS09, UJ20]. **bases** [BF09, FS08]. **Beat** [DM20]. **Bent** [Rei21, FM13]. **Bergman** [BT12]. **Better** [PP18]. **between** [BBP⁺20]. **bias** [DS18]. **Biggs** [Bla09]. **binary** [ATW08, LMPW15, SW07a]. **birthday** [HF07, MPST16, MSP12]. **Bit** [TW20, ZMD20]. **black** [YH24]. **black-box** [YH24]. **blind** [FS11]. **blinding** [DSG21]. **BLISS** [TW20]. **block** [DR07, SS17, Sch08, ZLA21]. **Boolean** [BC12, CJST16, CLS09, CC15, CLS16, LZ23, ZLA21, ZHM⁺22]. **boomerang** [RMS24]. **Bound** [DM20, Kus18]. **bounds** [BDJ14, SS17, YYTK20]. **box** [YH24]. **boxes** [ZMD20]. **breaking** [MPST16]. **Brezing** [Yoo15]. **Bringer** [CWZ12]. **broadcast** [AL07]. **calculus** [LL15, YYTK20]. **Can** [DM20]. **Capitulation** [AJZT19]. **carry** [FJ13]. **carry-truncated** [FJ13]. **Cartesian** [JCK⁺18]. **case** [AK17, RST07]. **CAST** [DT17]. **CAST-256** [DT17]. **CBC** [JN16]. **CCA** [KNP13]. **CCA-secure** [KNP13]. **cells** [Laa20]. **certain** [KU15]. **Chabanne** [CWZ12]. **challenges** [AK17]. **Challenging** [MSP12]. **channel** [Sch08]. **characterisation** [HS15a]. **Characteristic** [MR20, HST10]. **characterization** [BGMP08, FM13]. **Characterizing** [DHS20]. **Cheng** [PS08]. **CHIMERA** [BGGJ20]. **choosing** [Yoo15]. **cipher** [SS17, Tis11]. **ciphers** [DR07, FMS09, Moc23, Sch08]. **ciphertext** [CLSV24]. **ciphertxts** [AL11]. **circuit** [BBP⁺20]. **circulant** [AN20]. **class**

[AR15, CGK13]. **Classes** [AÖY15, AJZT19, WL13]. **classical** [BBP⁺20]. **cloud** [PSU13]. **CM** [JLLRL20]. **code** [KH23]. **code-based** [KH23]. **codes** [BBB⁺18, EHKN24, FHLMW08, JCK⁺18, LdV19, PS20, Per12, SPB22, Tim24]. **coding** [FL08, PSU13]. **coefficient** [LZ23, ZHM⁺22]. **colexicographically** [HM07]. **Collision** [BDJ14]. **collisions** [BS07]. **coloring** [ADPS14]. **combinatorics** [MN07]. **combined** [DSG21]. **Combining** [BGGJ20]. **Common** [CCH⁺20, HL10]. **communication** [PS15]. **commutative** [JCK⁺18]. **Compact** [CQS11, Per12]. **comparative** [CDK18]. **comparison** [BK09]. **complete** [BGMP08, Oka12]. **Complex** [BCIV20]. **Complex-Valued** [BCIV20]. **complexities** [SS17]. **Complexity** [YYTK20, AMW07, BW09, DS17]. **composite** [CDK18]. **compositeness** [PR20]. **Compression** [BG16, Kar10]. **computation** [ADPS14, CS21, CI14, DGG⁺15, Duq11, DEF14, GÓ07]. **computational** [Ano20]. **computations** [CDN18]. **Computing** [Bis11, Eke21]. **concrete** [APS15]. **concurrent** [WS09]. **concurrent-reset** [WS09]. **condition** [DSS20]. **conferences** [JP20]. **confusion** [LZ23, ZHM⁺22]. **conjecture** [CLS09]. **conjugacy** [LU08]. **conjugation** [MU14]. **connected** [DS17]. **connection** [Zaj13]. **Constant** [TW20, AL11]. **constant-size** [AL11]. **constants** [Grz20]. **constructed** [ZMD20]. **Constructing** [CJS14]. **Construction** [vT18, AGH17, ADPS14, CL09, FHLMW08, IK23, JCK⁺18]. **constructions** [GPR17, LdV19, PS15, WC07]. **Converting** [CDK18]. **convolution** [OS14]. **Coprime** [GP13]. **correlation** [DR07, DT17]. **corresponding** [BFJT12]. **Cosets** [KT20]. **Coskun** [AK17]. **Counting** [DN08, WL13]. **CP** [COP24, COP24]. **CP-ABE** [COP24]. **criterion** [LC07]. **critical** [Bla09]. **CRT** [CCH⁺20]. **CRT-variant** [CCH⁺20]. **Cryptanalysing** [Bla09, Mul11, Bla10]. **Cryptanalysis** [BCM09, BCM11, BKL22, CBW07, Esk24, LU08, LPS17, MU14, TL15, BP20, CG20, DT17, LNR09, MU10, PGS20, RST07, SS16a, SS17, SvT10, Tis11]. **Cryptographic** [BBPS20, CJST16, BCSV20, BFJN20, MP08, SPB22, SS09, ZMD20]. **cryptography** [CAR20, COP24, GGD20, GPR17]. **Cryptol.** [GZ14]. **cryptology** [CW22, Gut09, JP20]. **Cryptosystem** [PGS20, BCM09, Bla10, CBW07, CG20, HF07, Jus14, Jus15, KU15, SSS11, SvT10]. **cryptosystems** [AÖY15, CDK18, DJP14, EOS07]. **CSIDH** [BBP⁺20]. **cubic** [CC15]. **cumulative** [MN07]. **Curve** [HKP⁺20, KT20, CJS14, CQS11, DJP14, FK18, Tim24]. **Curves** [BGK⁺20, BG16, Bis11, Box12, BDFM21, CDS20, DN08, DEF14, FSV09, GPRS09, GZ13, GZ14, HST10, HWCD11, Hit09, LS07, MW12, Mor08, Oka12, ST24, Sch17, Sha14, Yoo15]. **cyclic** [AJZT19]. **cyclotomic** [AMW07, DSS20, Kar10, Sha14]. **DAGS** [BBB⁺18]. **Data** [BCIV20, CN22, SS17, SU14]. **decentralized** [Pop17]. **decreasing** [YYS⁺17]. **decryption** [YYS⁺14]. **DeepBKZ** [Yas20]. **defeat** [DSG21]. **degree** [Hit09, KW19]. **degrees** [TKF⁺20]. **Delegating** [DKKS20]. **delegation** [ZSN20]. **Deligne** [Tim24]. **Dembowski** [AÖY15]. **density** [FS09]. **Dependent** [FGG⁺20]. **descent** [KMPS10]. **design** [GPR17]. **designated** [YH24]. **Designing** [BBPS20]. **detailed** [Wun19]. **determined** [KK23]. **Devastating** [TW20]. **Differential** [CCI24, DT17]. **differential-zero** [DT17]. **differentials** [DR07]. **Diffie** [KM08, Kus18, Par18]. **digital** [RUS23]. **dihedral** [CS24]. **dimension** [EHKN24].

Dimensions [MR20]. **Discrete** [HKP⁺20, MR20, BT12, Bla09, Bla10, BDJ14, CI14, Eke21, Gal12, KM08, Sho10]. **Discretisation** [MP20]. **disguised** [Mor08]. **distinguisher** [Gal12]. **Distortion** [GPRS09]. **distributed** [DGG⁺15]. **Distribution** [LS07, BS07, Jus14, Jus15, Maz12, PS08, vzGS09]. **Distributions** [MP20, DR07]. **Divisor** [CCH⁺20]. **dragon** [SSS11]. **DSA** [Pou16]. **dual** [NP19, Yas20]. **duality** [Csi20]. **Dyadic** [BBPS20, BBB⁺18, Per12].

ECC [Joy20]. **ECDLP** [DM20, YYTK20]. **Editor** [CLS20]. **Edwards** [BG16]. **effect** [Mur12]. **effectiveness** [KMPS10, Mur12]. **Efficiency** [GPV24]. **Efficient** [BBPS20, DEF14, HST10, DGG⁺15, FM13, SSS11, SW07b, WS09]. **Efficiently** [BCIV20, Bla09]. **elementary** [Kar20a, Kar20b, ZLA21]. **elements** [Yoo15]. **Eleventh** [JLNN20]. **EIGamal** [PGS20]. **Elliptic** [BGK⁺20, HKP⁺20, KT20, Bis11, Box12, CJS14, CQS10, DJP14, DEF14, FSV09, FK18, HST10, HWCD11, LS07, MW12, Mor08, Oka12, ST24, Sch17, Sha14, Yoo15]. **EMAC** [JN16]. **embedding** [Hit09]. **encapsulation** [BBB⁺18]. **encodings** [NP19]. **Encryption** [BLLN21, BCIV20, BGGJ20, DS20, ASB⁺18, AL07, AL11, CLSV24, CN22, CEM15, IK23, KNP13, NP16, SPSS12, TL15, YYS⁺14]. **endomorphism** [Bis11]. **Enhancing** [SPS19]. **EPIC** [CWZ12]. **equation** [MP08, Zaj13]. **equations** [GP09]. **Equidistribution** [KT20]. **equivalence** [CLS16, PS20, WL13]. **Equivalent** [WP11]. **Erratum** [GZ14]. **error** [AMW07, BW09]. **errors** [APS15, BBGS19]. **Establishment** [TSJL20, BCM11]. **Estimation** [BBGS19]. **Evaluation** [DS20, CDGM14, CWZ12, TJB13]. **even** [Kar20a, Kar20b]. **Evolution** [CW22, BGMP08]. **Exact** [HL19, YYS⁺14]. **examples** [DC14]. **Exchange** [BGK⁺20, RM20, Ala17, Jia14, KU18, Par18, RS22]. **Exclusion** [Rei21]. **exhaustive** [RZ18]. **existence** [WC07]. **expansions** [FS08]. **experiments** [CCI24]. **explicit** [ATW08, Grz20]. **exploration** [HWCD11]. **exponent** [HL10]. **exponentiation** [DSG21]. **Exponentiations** [DKKS20]. **exponents** [Böc09, Kar20a, Kar20b]. **Exposure** [DSGKS20a]. **expressions** [KMNN19]. **Extension** [Joy20]. **extracting** [SU14].

Factor [Kar10]. **Factor-** [Kar10]. **Factoring** [Sic20, PR20]. **factorization** [Zaj13]. **fall** [KW19]. **Families** [Hit09, MW12, Ano20, CL09, FK18, Oka12, SPB22, Sha14, WC07, Yoo15]. **Family** [BLLN21, ACP10, BFJT12, FM13]. **Fast** [Gau07, OS14, Duq11, HL09, HL10, MPST16, jWW12, vzGS09]. **Fault** [Joy20]. **FCSRs** [FMS09]. **Fermat** [Kar20b, Kar20a]. **field** [ATW08, HSWZ20, Kus18]. **fields** [ATW08, AJZT19, BFP09, GP09, HST10, LPS20, LC07]. **filtered** [OPSB13]. **find** [Rei21]. **Finding** [Gal12, BS19, PP18, Yas20]. **finite** [BFP09, CBW07, FL08, HST10, HSWZ20, JCK⁺18, Kus18, LC07, Sho10]. **first** [KW19, CLY20]. **Flattening** [DS20]. **flaw** [ASB⁺18]. **Flips** [TW20]. **flow** [SW07b]. **Foreword** [Gut09, Mag13]. **forms** [HS08]. **formulæ** [ATW08]. **formulas** [MA17]. **foundation** [PSU13]. **framework** [BP20, BCSV20]. **Free** [DS20, Ano20]. **friendly** [Box12, FK18, Oka12, Sha14, Yoo15]. **Frontmatter** [Ano17, Ano18d, Ano18a, Ano18b, Ano18c, Ano19c, Ano19a, Ano19b]. **Fully** [BGGJ20, Dow15, TL15, YYS⁺14]. **function** [ACP10, GP09, Nan09, NSW09, PS15]. **Functional** [AL11]. **Functions**

[Rei21, TNS20, BC12, CJST16, CDS20, CLS09, CC15, CLS16, FM13, Gau07, KMNN19, KHK10, LZ23, MSP12, OS14, SW15, SW07a, ZSN20, ZLA21, ZHM⁺22]. **fundamental** [ASB⁺18]. **Further** [LZ23].

general [Eke21, PSU13]. **generalised** [Dow15, MN07]. **Generalization** [DS18, Par18, Tim24]. **generalized** [KHK10]. **generate** [SW15]. **Generating** [FK18, vzGS13]. **generation** [ABD⁺13, BGMP08, Pop17, vzGS09]. **generator** [BS19]. **Generic** [LdV19, Moc23]. **Gentry** [YYS⁺14]. **genus** [ATW08, CDS20, GPRS09, Gau07, Hit09, LL15]. **genus-2** [CDS20]. **geometric** [MP08]. **geometries** [JCK⁺18]. **geometry** [FL08]. **girth** [HL19]. **global** [GP09]. **Goldreich** [SPS19]. **Goldwasser** [Jus14, Jus15, SPS19]. **GPST** [BP22]. **Gram** [YYS⁺17]. **graph** [ADPS14, DS17, GD13]. **graphs** [CK20, HL19, JN16, PS15, PP18, Sho10]. **Greatest** [CCH⁺20]. **GRH** [Bis11]. **Gröbner** [BF09]. **Group** [DKKS20, PGS20, ST24, Bla09, CBW07, CW22, HWC11, JLLRL20, KU15, Kus18, RST07, SW15, Zaj13]. **group-theoretic** [CW22]. **groups** [GKL15, Rei17, SS09]. **Grover** [BP20]. **GS** [BBB⁺18].

Halevi [SPS19, YYS⁺14]. **hard** [HS08]. **hardness** [APS15, BS19, BBGS19]. **Hash** [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. **hash-function** [ACP10]. **hashing** [FSV09, LMPW15]. **Hellman** [KM08, Kus18, Par18]. **Herley** [AK17]. **Hessian** [BDFM21]. **Heuristics** [Box12, CW22]. **HFE** [BFJT12]. **hidden** [CS24, SS09]. **hidden-order** [SS09]. **higher** [CS21]. **Hints** [Sic20]. **HMAC** [KM13]. **HMQR** [Men07]. **Homomorphic** [BCIV20,

BGGJ20, DS20, CBW07, TL15, YYS⁺14]. **hull** [Mur12]. **Hybrid** [BFP09, KH23, Wun19]. **hyper** [CW22, FM13]. **hyper-bent** [FM13]. **hyper-heuristics** [CW22]. **hyperelliptic** [ATW08, DN08, GZ13, GZ14].

ID [PS15]. **ID-based** [PS15]. **Ideal** [LPS20, AJZT19, BBP19, BS19, HS15a, JSN13]. **idealness** [Sha14]. **Identification** [HS08, AK17, SW07b, WS09]. **II** [Jus15, Kob12]. **implementation** [CDGM14, YYS⁺14]. **implications** [FMS09, GÓ07]. **impossibility** [YH24]. **improve** [MA17]. **Improved** [CG20, Kus18, NM08, Nan09, PGS20]. **Inclusion** [Rei21]. **Inclusion/Exclusion** [Rei21]. **increased** [MSP12]. **indefinite** [HS08]. **index** [LL15, YYTK20]. **Indifferentiability** [MPST16]. **Indirect** [ABD⁺13]. **inequality** [Grz20]. **Infinite** [DC14]. **information** [HL19, SW07a]. **injection** [ABD⁺13]. **inner** [AL11]. **input** [DGG⁺15]. **insecure** [Bro23]. **insider** [BBP19]. **instantiations** [LdV19]. **Integer** [PR20, HM07]. **integers** [BK09]. **Interactive** [BGK⁺20, CEM15]. **interplay** [ATW08]. **intersecting** [SPS19]. **intersection** [Esk24]. **Intervals** [KT20]. **inverting** [JLLRL20]. **Isogenies** [BGK⁺20, BDFM21, CDS20, CJS14, DJP14]. **Isogeny** [TSJL20, CK20, TKF⁺20]. **Isogeny-Based** [TSJL20]. **Isolated** [Sch17]. **isomorphism** [HSWZ20]. **Issue** [DKKS20]. **iterated** [KHK10].

J [GZ14]. **Jacobi** [DEF14]. **Jacobian** [ATW08, Sho10]. **JMC** [DKKS20]. **joint** [NP16].

KASUMI [SW15]. **Kayawood** [KMU20]. **Key** [BBB⁺18, BGK⁺20, DSGKS20a, DS20, RM20, TSJL20, Ala17, BCM09, BCM11, BFJT12, Bro23, CDN18, CAR20, CEM15,

CBW07, DS18, GGD20, Jia14, KU18, KNP13, Maz12, Mul11, Par18, PS08, PS15, RS22, SPSS12, SSS11, SvT10, TL15, WP11]. **key-recovery** [BFJT12]. **keys** [BFJT12, KMU20, Per12, WP11]. **keystream** [DS18]. **keyword** [CLSV24]. **knowledge** [SW07b]. **known** [ZMD20]. **Koblitz** [DN08].

large [Grz20]. **Last** [Kar20a, Kar20b]. **Lattice** [MR20, Pou16, Wun19, YYS⁺17, Yas20]. **lattice-reduction** [Wun19]. **lattices** [Laa20, SPS19]. **laws** [HWCD11]. **Leakage** [CDGM14, FGG⁺20, Ala17, CAR20, KNP13]. **leakage-resilient** [Ala17, CAR20, KNP13]. **learning** [APS15, BBS19]. **least** [HL19]. **Leftover** [DSGKS20b]. **Lemma** [DSGKS20b]. **Length** [GKL15, RST07, MU08]. **Length-based** [GKL15, RST07, MU08]. **lengths** [YYS⁺17]. **Lightweight** [BLLN21, GPR17]. **Linear** [HS15b, AMW07, BCSV20, BW09, CDN18, DT17, EHKN24, Mur12, RZ18]. **linearly** [OPSB13]. **Log** [MR20, KM08]. **Logarithm** [HKP⁺20, BT12, Bla09, Bla10, Sho10]. **logarithmic** [BdW12, Rei17, SvT13, vT18]. **logarithms** [BDJ14, CI14, Eke21, Gal12]. **look** [HL09, Kob07, KM08, Kob12, KM13, Men07, SS16a]. **low** [ATW08]. **lower** [Kus18]. **LPS** [PP18]. **Lusztig** [Tim24]. **LWE** [BGGJ20, DSGKS20a, MP20].

MAC [ABD⁺13, JN16]. **MAKE** [BKL22, RS22]. **maps** [GPRS09]. **masking** [Sch08]. **Masthead** [Ano13]. **Math.** [GZ14]. **MathCrypt** [CLS20, CLY20]. **Mathematical** [Gut09]. **Matrices** [PGS20, GPR17]. **matrix** [BCM11, DSS20, KU18, MU14, RS22, ZSN20]. **matrix-based** [BCM11]. **matroids** [MFP10]. **maximum** [EHKN24]. **McEliece** [EOS07, Per12]. **McEliece-type** [EOS07]. **MDS** [GPR17]. **Mean** [MU10]. **Mean-set** [MU10]. **Medium** [MR20]. **meet** [Wun19]. **meet-in-the-middle** [Wun19]. **memory** [LL15]. **mental** [jWW12]. **Mersenne** [CG20]. **message** [ABD⁺13, Dow15, FHLMW08]. **Method** [Joy20, WL13, YYTK20, Yoo15, Zaj13]. **Methods** [JP20, DSG21, HL09, JCK⁺18, Sch08]. **mF** [CN22]. **Micali** [Jus14, Jus15]. **MICKEY** [Tis11]. **middle** [Wun19]. **Miller** [Böc09]. **Minimal** [FS08, HM07]. **mixing** [LMPW15]. **mnemonic** [AGH17]. **mode** [ASB⁺18, CN22]. **model** [BBP19, DN08]. **modified** [HVV14]. **modular** [HL09]. **moduli** [LPS17]. **modulo** [Bla10]. **modulus** [HL10]. **monodromy** [Sho10]. **Monomial** [Rei21, CLS16]. **monotone** [CJST16]. **MOV** [Sch17]. **MQQs** [CGK13]. **mR** [COP24]. **MR3101014** [GZ14]. **MRHS** [RZ18, Zaj13]. **Multi** [PSU18, FHLMW08, Hin08, YH24]. **multi-designated** [YH24]. **multi-message** [FHLMW08]. **multi-prime** [Hin08]. **Multi-prover** [PSU18]. **multi-receiver** [FHLMW08]. **multicasting** [Maz12]. **Multicollision** [KHK10]. **multicubic** [LPS20]. **multilevel** [JSN13]. **Multiparty** [BGK⁺20, ADPS14, CS21]. **Multiple** [DT17, FM13]. **multiplicative** [Kus18]. **multiplier** [EHKN24]. **multivariate** [AÖY15, BFP09, CGK13, HF07, SSS11, TJBY13]. **naive** [YYTK20]. **negation** [AL11]. **network** [FL08, PS08]. **networks** [HS15b]. **NIKE** [UJ20]. **NLFSRs** [OPSB13]. **Non** [BGK⁺20, TW20, BT12, CDN18, CEM15, Jus14, Jus15, KM08, Sha14]. **Non-Constant** [TW20]. **non-idealness** [Sha14]. **Non-Interactive** [BGK⁺20, CEM15]. **non-linear** [CDN18]. **non-representable** [BT12]. **non-residues** [Jus14, Jus15]. **non-standard** [KM08]. **Nonsmooth** [Tis11]. **norm** [GP09]. **normal**

[SS16a]. **note** [CS21]. **notions** [SPSS12]. **NP** [HS08]. **NP-hard** [HS08]. **NTRU** [BF09, DHS20, DS20]. **number** [AJZT19, BBGS19, BFJN20, DSS20, MA17, Pop17, WL13, JP20]. **number-theoretic** [BFJN20, JP20]. **numbers** [vzGS09]. **Numerical** [LNR09]. **NutMiC** [DKKS20].

Oblivious [TJBY13, FS11]. **odd** [HST10]. **off** [BBP⁺20]. **offs** [LL15]. **OMAC** [Nan09]. **One** [BK09, TW20, Bla10, PS15]. **One-round** [BK09]. **one-way-function** [PS15]. **opening** [CEM15]. **Operations** [BBPS20, CCI24]. **Optimal** [PS15, Sil07, CDGM14]. **optimality** [CDN18]. **oracle** [BP20]. **orbit** [Gal12]. **order** [CDK18, SS09]. **orders** [Eke21]. **Oribatida** [BLLN21]. **Orienting** [CK20]. **Ostrom** [AÖY15]. **overhead** [AL07, BP20]. **overstretched** [DHS20].

pair [NP19]. **pairing** [Box12, CDK18, Duq11, FK18, GÓ07, Oka12, Sha14, Sho10, Yoo15]. **pairing-based** [CDK18]. **pairing-friendly** [Box12, FK18, Oka12, Sha14, Yoo15]. **pairings** [DEF14, GZ13, GZ14]. **parallel** [CCI24]. **parameterization** [Sil07]. **parameters** [FK18]. **Partial** [DSGKS20a]. **participants** [DS17, GD13]. **Password** [TSJL20, Jia14]. **Password-Authenticated** [TSJL20]. **password-based** [Jia14]. **path** [PP18]. **path-finding** [PP18]. **Perfect** [GD13, CL09, WC07]. **period** [BW09]. **permutation** [BBP19, LMPW15]. **permutations** [AGH17]. **Persistent** [Jia14]. **pipe** [MPST16]. **Pisot** [FS08]. **PKA** [AR15]. **Plactic** [Bro23]. **PMAC** [NM08]. **Points** [KT20, BG16, LS07]. **poker** [jWW12]. **Pollard** [BDJ14]. **Poly** [SSS11]. **Poly-dragon** [SSS11]. **Pólya** [CLS16]. **polycyclic** [GKL15, KU15]. **polycyclic-group-based** [KU15]. **Polylogarithmic** [Mie08]. **polymatroids** [KK23, MFP10]. **Polynomial** [KMNN19, CWZ12, DSS20, JLLRL20, WL13, ZSN20].

Polynomials [HKP⁺20, AÖY15, KW19, TJBY13]. **PoRs** [LdV19]. **possessing** [SU14]. **post** [COP24]. **post-quantum** [COP24]. **Power** [JLNN20, ACP10, TKF⁺20]. **practical** [BFJT12, CAR20, NV08]. **practice** [HL10]. **Predicate** [NP19]. **predistribution** [PS15]. **Preface** [CLS20, CLY20, JP20]. **Prefix** [FGG⁺20]. **Prefix-Dependent** [FGG⁺20]. **presence** [Dow15, Sch08]. **preserving** [Esk24, ZSN20]. **prime** [CDK18, Hin08, TKF⁺20]. **primes** [ACP10, FS09, vzGS13]. **primitive** [SS09, Yoo15]. **primitives** [BFJN20, CDN18]. **Principal** [LPS20]. **Privacy** [ZSN20, Esk24]. **Privacy-preserving** [ZSN20, Esk24]. **private** [DGG⁺15, Esk24, HL10, KMU20, SW07a].

Probability [DR07]. **Problem** [CCH⁺20, HKP⁺20, LPS20, BT12, BBGS19, Bla09, Bla10, CS24, HSWZ20, Kus18, NV08]. **problems** [BCSV20, HS08, KM08, TKF⁺20]. **Proceedings** [CLS20, CLY20]. **processes** [SW07a]. **Processing** [BCIV20]. **Product** [DKKS20, MP20, OS14]. **products** [AL11, IK23]. **proof** [Kar20a, Kar20b, NP19, PSU13, PSU18]. **proof-of-retrievability** [PSU13]. **properties** [CJST16, ZMD20]. **property** [EHKN24]. **Protecting** [Joy20]. **protocol** [CWZ12, KU18, KMU20, LU08, MU10, SW07b, jWW12, WS09]. **protocols** [AK17, BCM11, IK23, SW07a]. **Provable** [Moc23]. **prover** [PSU18]. **proving** [Kob07, Kob12]. **proxy** [SSA17]. **Pseudo** [Ano20, BGMP08, Pop17]. **Pseudo-free** [Ano20]. **pseudo-random** [Pop17]. **pseudorandom** [Nan09, vzGS09]. **Public** [SvT10, AL11, BCM09, CAR20, CBW07, GGD20, KNP13, SPSS12, SSS11, WP11]. **public-attribute** [AL11]. **public-key**

[CAR20, CBW07, GGD20, SPSS12].

quadratic

[AÖY15, CGK13, HF07, HS08, Jus14, Jus15].

Quantum

[CI14, Eke21, BS19, BP20, BBP⁺20, CJS14, COP24, DJP14, JLLRL20, RUS23].

quantum-resistant [DJP14]. **quartic**

[AJZT19, DEF14]. **Quasi** [HKP⁺20, Per12].

quasi-dyadic [Per12]. **Quasi-subfield**

[HKP⁺20]. **quasigroups** [CGK13]. **query**

[SW07a]. **quotient** [MU08].

Rabin [Böc09]. **Ramanujan** [PP18].

Random

[MU08, BGMP08, EHKN24, Pop17].

randomized [Böc09, CLSV24]. **range**

[YY⁺14]. **rational** [MW12]. **ratios** [HL19].

RC4 [BGMP08, DS18]. **realization**

[SvT10]. **realizing** [PS15]. **receiver**

[FHLMW08]. **reconstruction** [SW07a].

Recovering [FGG⁺20]. **recovery** [BFJT12].

Recovering [BC12, CL09]. **reduced** [DT17].

reduced-round [DT17]. **reducing** [BP20].

reduction [Wun19]. **refinement** [LS18].

regular [DSG21, MSP12]. **relations**

[DS18, SPSS12]. **relying** [BS19]. **Remarks**

[RM20, FMS09]. **repairable** [LS18].

representable [BT12]. **Representation**

[DM20]. **representations** [CQS11, HM07].

Reproducible [SPB22]. **requirements**

[NSW09]. **research** [LZ23]. **reset** [WS09].

Residue [JLNN20, CS21]. **residues**

[Jus14, Jus15]. **resilient**

[Ala17, CAR20, HS15b, KNP13]. **resistance**

[MSP12]. **resistant** [DJP14]. **restricted**

[BBGS19]. **results** [DS18, LZ23, SW07a].

Rethinking [ATW08]. **Retraction**

[Kar20b]. **retrievability** [PSU13, PSU18].

retrieval [SW07a]. **Revisited**

[Joy20, AN20, Laa20, NP16, SS16b].

Revisiting [JN16]. **revocable** [COP24].

rho [BDJ14]. **Richelot** [CDS20]. **Rigorous**

[SS17]. **Rijndael** [RMS24]. **Ring**

[DSGKS20b, Joy20, BT12, YH24, BGGJ20,

DSGKS20a, MP20]. **Ring-LWE**

[DSGKS20a, MP20]. **Ring-LWE-based**

[BGGJ20]. **Rings** [PGS20, Bis11, JCK⁺18].

Rivest [HVV14]. **RNS** [Duq11]. **robust**

[JSN13, PS20]. **Roos** [DS18]. **Root** [DM20].

rotate [FJ13]. **Rotation**

[Rei21, CC15, CLS16]. **round**

[BK09, DT17, Mie08, SW15, SW07a]. **RSA**

[DSG21, Hin08, HL10, LPS17, MA17].

safe [AK17, vzGS13]. **same** [SU14].

samples [BBGS19]. **SAP** [GGD20].

scheme [Esk24, HVV14, HSWZ20, KH23,

Maz12, Mul11, PS08, SSA17, SPS19, TL15].

Schemes [BLLN21, BGGJ20, DKKS20,

BBP19, BS19, GD13, HS15a, JSN13, LS18,

MFP10, MU14, PSU13, PS15, PS20, Pou16,

RUS23, SS16b, YH24]. **Schmidt** [YY⁺17].

Schnorr [NSW09]. **search**

[CLSV24, MA17, RZ18, RMS24].

Searchable [CLSV24]. **Second**

[CLS20, Gut09]. **Secret**

[Csi20, DC14, GD13, HS15a, HL19, JSN13,

MFP10, CEM15]. **Secrets** [FGG⁺20].

Secure [Dow15, BK09, CS21, FL08, JSN13,

KNP13, Maz12, PSU13, SSA17, SW07b,

SW07a, SS16b, WS09]. **Security**

[FS11, HVV14, OPSB13, ACP10, AL11,

BBP19, CDGM14, EOS07, GÓ^S07, Hin08,

Moc23, MPST16, NM08, Nan09, NP16,

SPSS12, DSGKS20a]. **Self**

[GZ13, Yas20, GZ14]. **Self-dual** [Yas20].

Self-pairings [GZ13, GZ14]. **Semaev**

[YYTK20]. **semidirect** [IK23]. **semigroups**

[CI14]. **Sensitivities** [ZLA21]. **sensor**

[HS15b, PS08]. **sequences**

[AMW07, BW09, LS07]. **server** [SW07a].

set [Esk24, Gal12, MU10]. **setting** [CDK18].

seven [DS17]. **sharing** [Csi20, DC14, GD13,

HS15a, HL19, JSN13, MFP10]. **shifted**

[LU08]. **Short**

[LPS20, BS19, YY⁺17, Yas20]. **shortest**

[NV08]. **Sibert** [MU10]. **side** [Sch08].

Sidelnikov [BW09]. **SIDH** [GPV24, UJ20]. **SIDH-based** [GPV24, UJ20]. **Sieve** [NV08, Grz20]. **Sieving** [MR20]. **Sign** [TW20]. **Signature** [DKKS20, HSWZ20, NP16, RUS23, SS16b, YH24]. **signatures** [BdW12, FS11, GPV24, HS08, NP19, NSW09, Rei17, SvT13, vT18]. **Signcryption** [BBP19, KH23, SSA17]. **SIKE** [BP20]. **Simplified** [GÓ07]. **six** [GD13]. **size** [AL11, BBP⁺20]. **SKENO** [CEM15]. **small** [HST10, HL19, HL10, Hit09]. **SNFS** [Sil07]. **solutions** [GP13]. **solve** [Zaj13]. **solver** [RZ18]. **solvers** [LNR09]. **solving** [BFP09, Bla09, BDJ14, GP09, MP08, TKF⁺20]. **Some** [FL08, FMS09, SW07a, AJZT19, BC12, DS18, FS09, HL09, HL10, IK23, LS07]. **space** [JLLRL20]. **sparse** [AK17, FK18]. **Special** [DKKS20, CGK13, FS09]. **specified** [PS15]. **Square** [DM20]. **squared** [YYS⁺17]. **squared-sum** [YYS⁺17]. **squeezing** [CDGM14]. **Srivastava** [Per12]. **standard** [KM08]. **Statistical** [BS07]. **Stickel** [Mul11]. **Stochastic** [DSG21, Sch08]. **storage** [PSU13]. **stream** [FMS09, Moc23, Tis11]. **streams** [DGG⁺15]. **Strict** [LC07]. **Strongly** [SvT13, AR15, vT18]. **structure** [DS17, JN16, JSN13, ST24]. **structures** [GD13, KK23]. **subexponential** [ADPS14, CJS14, JLLRL20]. **subexponential-time** [JLLRL20]. **subfield** [HST10, HKP⁺20]. **subgroup** [CS24]. **subgroups** [Kar10, MU08]. **Submission** [DKKS20]. **subsequences** [BW09]. **Subset** [vzGS09]. **sum** [HF07, YYS⁺17, vzGS09]. **summary** [EOS07]. **summation** [KW19]. **supersingular** [BP22, CK20, DJP14, GPRS09]. **superspecial** [CDS20]. **support** [AL11]. **Survey** [GGD20, LS18]. **Suzuki** [Tim24]. **Symbol** [JLNN20]. **symbols** [CS21]. **Symmetric** [Rei21, CDN18, CLS09, CC15, CLS16, TL15, ZLA21]. **System** [RM20, NP19]. **systems** [BFP09, Mie08, WP11, Zaj13].

Takes [TW20]. **Tame** [Rei17]. **technique** [NP19]. **Techniques** [UJ20]. **terms** [FM13]. **test** [Böc09]. **th** [DSS20]. **their** [EOS07]. **Theorem** [Kar20b, CLS16, Kob07, Kob12, Kar20a]. **theorem-proving** [Kob07, Kob12]. **theoretic** [BFJN20, CW22, JP20]. **Theory** [CC15, GPR17, PSU13]. **theta** [Gau07]. **Thompson** [RST07]. **Three** [MR20, BCM11]. **threshold** [JSN13, LS18, PS20]. **Tillich** [TNS20]. **Time** [LL15, TW20, CJS14, JLLRL20]. **Time-memory** [LL15]. **Timing** [TW20]. **torsion** [MW12]. **trace** [BG16, EHKN24, FM13]. **trade** [BBP⁺20, LL15]. **trade-off** [BBP⁺20]. **trade-offs** [LL15]. **tradeoffs** [Eke21]. **transfer** [FS11]. **transmission** [AL07, Dow15]. **Tropical** [RM20, KU18]. **truncated** [FJ13]. **trustless** [Pop17]. **twisted** [BG16, BDFM21]. **Two** [LMPW15, PS08, GPRS09, Mie08, RUS23, SW07b]. **two-flow** [SW07b]. **Two-permutation-based** [LMPW15]. **two-round** [Mie08]. **TWOOA** [FHLMW08]. **Type** [TNS20, AJZT19, EOS07, Jus14, Jus15, Tim24].

uadratic [WP11]. **ultivariate** [WP11]. **unbounded** [DGG⁺15]. **uncloaking** [KMU20]. **Unconditionally** [JSN13, SS16b, PSU13, SW07a]. **Unconditionally-secure** [JSN13]. **uniform** [KK23]. **universal** [ACP10, Ano20]. **upper** [SS17]. **use** [BP20]. **Using** [FJ13, Rei21, BBB⁺18, BF09, CCI24, CDS20, CW22, FK18, Kus18].

v1.3 [BLLN21]. **Valued** [BCIV20]. **values** [Oka12]. **Vandermonde** [DSS20]. **variant** [CCH⁺20, Grz20, LPS17]. **variants** [HL10, Mul11]. **vector** [NV08]. **vectors**

[BF09, EHKN24, YYS⁺17, Yas20].
verifiable [ZSN20]. **verifiers** [YH24]. **via**
 [CS21, DM20, NP19]. **view** [MP08].
Volume [CLS20, CLY20]. **Voronoi** [Laa20].
VSH [BS07].

way [PS15]. **weak** [AÖY15, BFJT12].
weight [FS08, HM07]. **weighted** [HS15a].
weights [BC12]. **Weil** [HF07, KMPS10].
Weng [Yoo15]. **wide** [MPST16]. **witnesses**
 [PR20]. **Witt** [BF09]. **Workshop** [Gut09].

xor [FJ13].

yes [GPV24].

Zémor [TNS20]. **zero** [BG16, DT17, SW07b].
zero-knowledge [SW07b].

References

AlMashrafi:2013:IMI

[ABD⁺13] Mufeed Al Mashrafi, Harry Bartlett, Ed Dawson, Leonie Simpson, and Kenneth Koon-Ho Wong. Indirect message injection for MAC generation. *Journal of Mathematical Cryptology*, 7(3):253–277, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Alomair:2010:PPS

[ACP10] Basel Alomair, Andrew Clark, and Radha Poovendran. The power of primes: security of authentication based on a universal hash-function family. *Journal of Mathematical Cryptology*, 4(2):121–148, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Asghar:2014:SCG

[ADPS14] Hassan Jameel Asghar, Yvo Desmedt, Josef Pieprzyk, and Ron Steinfeld. A subexponential construction of graph coloring for multiparty computation. *Journal of Mathematical Cryptology*, 8(4):363–403, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Antal:2017:MCP

[AGH17] Eugen Antal, Otokar Grošek, and Peter Horak. On a mnemonic construction of permutations. *Journal of Mathematical Cryptology*, 11(1):45–53, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Azizi:2019:CIC

[AJZT19] Abdelmalek Azizi, Idriss Jerriari, Abdelkader Zekhnini, and Mohammed Talbi. Capitulation of the 2-ideal classes of type (2, 2, 2) of some quartic cyclic number fields. *Journal of Mathematical Cryptology*, 13(1):27–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0037/jmc-2017-0037.xml>.

Asghar:2017:WIP

[AK17] Hassan Jameel Asghar and Mohamed Ali Kaafar. When are identification protocols with sparse challenges safe? The case

- of the Coskun and Herley attack. *Journal of Mathematical Cryptology*, 11(3):177–194, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AL07] Sarang Aravamuthan and Sachin Lodha. The average transmission overhead for broadcast encryption. *Journal of Mathematical Cryptology*, 1(4):373–384, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AL11] Nuttapon Attrapadung and Benoit Libert. Functional encryption for public-attribute inner products: achieving constant-size ciphertexts with adaptive security or support for negation. *Journal of Mathematical Cryptology*, 5(2):115–158, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Ala17] Janaka Alawatugoda. On the leakage-resilient key exchange. *Journal of Mathematical Cryptology*, 11(4):215–269, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AMW07] Hassan Aly, Wilfried Meidl, and Arne Winterhof. On the k -error linear complexity of cyclotomic sequences. *Journal of Mathematical Cryptology*, 1(3): 283–296, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AN20] Filipe Araujo and Samuel Neves. The circulant hash revisited. *Journal of Mathematical Cryptology*, 15(1):250–257, December 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2018-0054/html>.
- [Ano13] Anonymous. Masthead. *Journal of Mathematical Cryptology*, 7(3):i, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2013.7.issue-3/jmc-2013-masthead3/jmc-2013-masthead3.xml>.
- [Ano17] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 11(2):i–iv, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2017-frontmatter2/jmc-2017-frontmatter2.xml>.
- [Ano18a] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(1):i–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (elec-

- tronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2018-frontmatter1/jmc-2018-frontmatter1.xml>.
- [Ano18b] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(2):i-iv, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Ano18c] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(3):i-??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2018-frontmatter3/jmc-2018-frontmatter3.xml>.
- [Ano18d] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(4):i-??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-frontmatter4/jmc-2018-frontmatter4.xml>.
- [Ano19a] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(1):i-??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2019-frontmatter1/jmc-2019-frontmatter1.xml>.
- [Ano19b] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(2):i-??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2019-frontmatter2/jmc-2019-frontmatter2.xml>.
- [Ano19c] Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(3-4):i-??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2019-frontmatter3-4/jmc-2019-frontmatter3-4.xml>.
- [Ano20] Mikhail Anokhin. Pseudo-free families of computational universal algebras. *Journal of Mathematical Cryptology*, 15(1):197-222, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0014/html>.
- [AÖY15] Bilal Alam, Ferruh Özbudak, and Oğuz Yayla. Classes of weak

- Dembowski–Ostrom polynomials for multivariate quadratic cryptosystems. *Journal of Mathematical Cryptology*, 9(1): 11–22, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [ATW08]
- [APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3): 169–203, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Albrecht:2015:CHL**
- [AR15] Luigi Accardi and Massimo Regoli. On a class of strongly asymmetric PKA algorithms. *Journal of Mathematical Cryptology*, 9(3):151–159, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Accardi:2015:CSA**
- [ASB⁺18] Hassan Qahur Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, and Kenneth Koon-Ho Wong. A fundamental flaw in the ++AE authenticated encryption mode. *Journal of Mathematical Cryptology*, 12(1): 37–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2016-0037/jmc-2016-0037.xml>. **AlMahri:2018:FFA**
- [BBW08] R. Avanzi, N. Thériault, and Z. Wang. Rethinking low genus hyperelliptic Jacobian arithmetic over binary fields: interplay of field arithmetic and explicit formulæ. *Journal of Mathematical Cryptology*, 2(3): 227–255, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Avanzi:2008:RLG**
- [BBB⁺18] Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gu-eye, Richard Haeussler, Jean Belkhamt, Ousmane N’diaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson E. Ricardini. DAGS: Key encapsulation using dyadic GS codes. *Journal of Mathematical Cryptology*, 12(4):221–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-0027/jmc-2018-0027.xml>. **Banegas:2018:DKE**
- [BBS19] Nina Bindel, Johannes Buchmann, Florian Göpfert, and Markus Schmidt. Estimation of the hardness of the learning with errors problem with a restricted number of samples. *Journal of Mathematical Cryptology*, 13(1): 47–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Bindel:2019:EHL**

- 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0040/jmc-2017-0040.xml>.
- Bansal:2019:SSI**
- [BBP19] Tarun Kumar Bansal, Xavier Boyen, and Josef Pieprzyk. Signcryption schemes with insider security in an ideal permutation model. *Journal of Mathematical Cryptology*, 13(2): 117–150, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0006/jmc-2018-0006.xml>.
- Biasse:2020:TBC**
- [BBP+20] Jean-François Biasse, Xavier Bonnetain, Benjamin Pring, André Schrottenloher, and William Youmans. A trade-off between classical and quantum circuit size for an attack against CSIDH. *Journal of Mathematical Cryptology*, 15(1):4–17, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0070/html>.
- Banegas:2020:DED**
- [BBPS20] Gustavo Banegas, Paulo S. L. M. Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *Journal of Mathematical Cryptology*, 14(1):95–109, June 19, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0054/html>.
- Brown:2012:RWS**
- [BC12] Alyssa Brown and Thomas W. Cusick. Recursive weights for some Boolean functions. *Journal of Mathematical Cryptology*, 6(2):105–135, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0020/jmc-2011-0020.xml>.
- Bootland:2020:EPC**
- [BCIV20] Carl Bootland, Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Efficiently processing complex-valued data in homomorphic encryption. *Journal of Mathematical Cryptology*, 14(1):55–65, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0051/html>.
- Blackburn:2009:CPK**
- [BCM09] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Cryptanalysis of the MST₃ public key cryptosystem. *Journal of Mathematical Cryptology*, 3(4): 321–338, 2009. CODEN ????]

ISSN 1862-2976 (print), 1862-2984 (electronic).

Blackburn:2011:CTM

- [BCM11] Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Cryptanalysis of three matrix-based key establishment protocols. *Journal of Mathematical Cryptology*, 5(2):159–168, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bootland:2020:FCP

- [BCSV20] Carl Bootland, Wouter Castryck, Alan Szepieniec, and Frederik Vercauteren. A framework for cryptographic problems from linear algebra. *Journal of Mathematical Cryptology*, 14(1):202–217, July 21, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0032/html>.

Broon:2021:ITH

- [BDFM21] Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted Hessian curves. *Journal of Mathematical Cryptology*, 15(1):345–358, March 16, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0037/html>.

Bos:2014:CBA

- [BDJ14] Joppe W. Bos, Alina Dudeanu, and Dimitar Jetchev. Colli-

sion bounds for the additive Pollard rho algorithm for solving discrete logarithms. *Journal of Mathematical Cryptology*, 8(1):71–92, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Baumeister:2012:ALS

- [BdW12] Barbara Baumeister and Jan-Hendrik de Wiljes. Aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 6(1):21–37, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bourgeois:2009:AAN

- [BF09] Gérald Bourgeois and Jean-Charles Faugère. Algebraic attack on NTRU using Witt vectors and Gröbner bases. *Journal of Mathematical Cryptology*, 3(3):205–214, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Brier:2020:NNT

- [BFJN20] Éric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. *Journal of Mathematical Cryptology*, 14(1):224–235, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0035/html>.

Bouillaguet:2012:FWK

- [BFJT12] Charles Bouillaguet, Pierre-Alain Fouque, Antoine Joux,

- and Joana Treger. A family of weak keys in HFE and the corresponding practical key-recovery. *Journal of Mathematical Cryptology*, 5(3–4):247–275, 2012. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BFP09] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BG16] Giulia Bianco and Elisa Gorla. Compression for trace zero points on twisted Edwards curves. *Journal of Mathematical Cryptology*, 10(1):15–34, 2016. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BGGJ20] Christina Boura, Nicolas Gama, Mariya Georgieva, and Dimitar Jetchev. CHIMERA: Combining Ring-LWE-based fully homomorphic encryption schemes. *Journal of Mathematical Cryptology*, 14(1):316–338, August 7, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0026/html>.
- [BGK⁺20] Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Alice Silverberg, Mehdi Tibouchi, and Mark Zhandry. Multiparty non-interactive key exchange and more from isogenies on elliptic curves. *Journal of Mathematical Cryptology*, 14(1):5–14, June 14, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0047/html>.
- [BGMP08] Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul. A complete characterization of the evolution of RC4 pseudo random generation algorithm. *Journal of Mathematical Cryptology*, 2(3):257–289, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Bis11] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *Journal of Mathematical Cryptology*, 5(2):101–113, 2011. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BK09] Ian F. Blake and Vladimir Kolesnikov. One-round secure comparison of integers. *Journal of Mathematical Cryptology*,

Boneh:2020:MNI**Bettale:2009:HAS****Basu:2008:CCE****Bianco:2016:CTZ****Bisson:2011:CER****Boura:2020:CCR****Blake:2009:ORS**

3(1):37–68, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Brown:2022:CM

- [BKL22] Daniel R. L. Brown, Neal Koblitz, and Jason T. LeGrow. Cryptanalysis of “MAKE”. *Journal of Mathematical Cryptology*, 16(1):98–102, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2021-0016/html>. See [RS22].

Blackburn:2009:CCG

- [Bla09] Simon R. Blackburn. Cryptanalysing the critical group: efficiently solving Biggs’s discrete logarithm problem. *Journal of Mathematical Cryptology*, 3(3):199–203, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Blackburn:2010:DLP

- [Bla10] Simon R. Blackburn. The discrete logarithm problem modulo one: cryptanalysing the Ariffin–Abu cryptosystem. *Journal of Mathematical Cryptology*, 4(2):193–198, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Bhattacharjee:2021:OVF

- [BLLN21] Arghya Bhattacharjee, Cuauhtemoc Mancillas López, Eik List, and Mridul Nandi. The Oribatida v1.3 family of lightweight authenticated encryption schemes.

Journal of Mathematical Cryptology, 15(1):305–344, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0018/html>.

Bockle:2009:MRT

- [Böc09] Gebhard Böckle. The Miller–Rabin test with randomized exponents. *Journal of Mathematical Cryptology*, 3(4):307–319, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Boxall:2012:HPF

- [Box12] John Boxall. Heuristics on pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 6(2):81–104, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0004/jmc-2011-0004.xml?format=INT>.

Biasse:2020:FRO

- [BP20] Jean-François Biasse and Benjamin Pring. A framework for reducing the overhead of the quantum oracle for use with Grover’s algorithm with applications to cryptanalysis of SIKE. *Journal of Mathematical Cryptology*, 15(1):143–156, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL

- <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0080/html>.
- [BP22] Andrea Basso and Fabien Pazuki. On the supersingular GPST attack. *Journal of Mathematical Cryptology*, 16(1): 14–19, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2021-0020/html>.
- [Bro23] Daniel R. L. Brown. Plactic key agreement (insecure?). *Journal of Mathematical Cryptology*, 17(1):??, January 2023. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0010/html>.
- [BS07] Ian F. Blake and Igor E. Shparlinski. Statistical distribution and collisions of VSH. *Journal of Mathematical Cryptology*, 1(4):329–349, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BS19] Jean-François Biasse and Fang Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbf{Q}(\zeta_{2s})$. *Journal of Mathematical Cryptology*, 13(3–4):151–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2015-0046/jmc-2015-0046.xml>.
- [BT12] Matan Banin and Boaz Tsaban. The discrete logarithm problem in Bergman’s non-representable ring. *Journal of Mathematical Cryptology*, 6(2): 171–182, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2012-0014/jmc-2012-0014.xml>.
- [BW09] Nina Brandstätter and Arne Winterhof. k -error linear complexity over \mathbf{F}_p of subsequences of Sidelnikov sequences of period $(p^r - 1)/3$. *Journal of Mathematical Cryptology*, 3(3): 215–225, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [CAR20] Suvradip Chakraborty, Janaka Alawatugoda, and Chandrasekaran Pandu Rangan. New approach to practical leakage-resilient public-key cryptography. *Journal of Mathematical Cryptology*, 14(1):172–201, July 11, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/>

- document/doi/10.1515/jmc-2019-0014/html.
- Choi:2007:CHP**
- [CBW07] Su-Jeong Choi, Simon R. Blackburn, and Peter R. Wild. Cryptanalysis of a homomorphic public-key cryptosystem over a finite group. *Journal of Mathematical Cryptology*, 1(4):351–358, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cusick:2015:TRS**
- [CC15] Thomas W. Cusick and Younhwan Cheon. Theory of 3-rotation symmetric cubic Boolean functions. *Journal of Mathematical Cryptology*, 9(1):45–62, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cheon:2020:ACV**
- [CCH⁺20] Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, and Changmin Lee. Algorithms for CRT-variant of approximate greatest common divisor problem. *Journal of Mathematical Cryptology*, 14(1):397–413, October 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0031/html>.
- Calderini:2024:DEU**
- [CCI24] Marco Calderini, Roberto Civino, and Riccardo Invernizzi. Differential experiments using parallel alternative operations. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0030/html>.
- Carlet:2014:LSO**
- [CDGM14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Housseem Maghrebi. Leakage squeezing: optimal implementation and security evaluation. *Journal of Mathematical Cryptology*, 8(3):249–295, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Chatterjee:2018:CPB**
- [CDK18] Sanjit Chatterjee, M. Prem Laxman Das, and R. Kabaleeshwaran. Converting pairing-based cryptosystems from composite to prime order setting — a comparative analysis. *Journal of Mathematical Cryptology*, 12(3):159–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0042/jmc-2017-0042.xml>.
- Chakraborti:2018:ONL**
- [CDN18] Avik Chakraborti, Nilanjan Datta, and Mridul Nandi. On the optimality of non-linear computations for symmetric key primitives. *Journal of Mathematical Cryptology*, 12(4):241–

- ??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2017-0011/jmc-2017-0011.xml>. [CGK13]
- [CDS20] Wouter Castryck, Thomas De-cru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using Riche-lot isogenies. *Journal of Math-ematical Cryptology*, 14(1):268–292, August 7, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0021/html>. [CI14]
- [CEM15] Jiageng Chen, Keita Emura, and Atsuko Miyaji. SKENO: Se-cret key encryption with non-interactive opening. *Journal of Mathematical Cryptology*, 9(2):63–74, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [CJS14]
- [CG20] Jean-Sébastien Coron and Ag-nesse Gini. Improved cryptanaly-sis of the AJPS Mersenne based cryptosystem. *Journal of Math-ematical Cryptology*, 14(1):218–223, July 21, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0027/html>. [CJST16]
- [Chen:2013:SCM] Yanling Chen, Danilo Glig-oroski, and Svein J. Knapskog. On a special class of multi-variate quadratic quasigroups (MQQs). *Journal of Mathemat-ical Cryptology*, 7(2):111–141, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (elec-tronic).
- [Childs:2014:QCD] Andrew M. Childs and Gábor Ivanyos. Quantum computation of discrete logarithms in semi-groups. *Journal of Mathematical Cryptology*, 8(4):405–416, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Childs:2014:CEC] Andrew Childs, David Jao, and Vladimir Soukharev. Construct-ing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Carlet:2016:CPM] Claude Carlet, David Joyner, Pantelimon Stănică, and Deng Tang. Cryptographic prop-erties of monotone Boolean func-tions. *Journal of Mathemat-ical Cryptology*, 10(1):1–14, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (elec-tronic). URL <http://www.degruyter.com/view/j/jmc.2016.10.issue-1/jmc-2014-0030/jmc-2014-0030.xml>.

- Colo:2020:OSI**
- [CK20] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1): 414–437, October 23, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0034/html>.
- Colbourn:2009:RCP**
- [CL09] Charles J. Colbourn and Alan C. H. Ling. A recursive construction for perfect hash families. *Journal of Mathematical Cryptology*, 3(4):291–306, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cusick:2009:CBS**
- [CLS09] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. On a conjecture for balanced symmetric Boolean functions. *Journal of Mathematical Cryptology*, 3(4):273–290, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cusick:2016:AEM**
- [CLS16] Thomas W. Cusick, K. V. Lakshmy, and M. Sethumadhavan. Affine equivalence of monomial rotation symmetric Boolean functions: a Pólya’s theorem approach. *Journal of Mathematical Cryptology*, 10(3–4):145–156, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cheon:2020:EPS**
- [CLS20] Jung Hee Cheon, Kristin Lauter, and Yongsoo Song. Editor’s preface for the Second Annual MathCrypt Proceedings volume. *Journal of Mathematical Cryptology*, 15(1):1–3, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0170/html>.
- Calderini:2024:SER**
- [CLSV24] Marco Calderini, Riccardo Longo, Massimiliano Sala, and Irene Villa. Searchable encryption with randomized ciphertext and randomized keyword search. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0029/html>.
- Cheon:2020:PFA**
- [CLY20] Jung Hee Cheon, Kristin Lauter, and Donggeon Yhee. Preface to the First Annual MathCrypt Proceedings volume. *Journal of Mathematical Cryptology*, 14(1):1–4, June 19, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0060/html>.

Chakraborty:2022:MMA

- [CN22] Bishwajit Chakraborty and Mridul Nandi. The mF mode of authenticated encryption with associated data. *Journal of Mathematical Cryptology*, 16(1): 73–97, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0054/html>.

Cianfriglia:2024:MLC

- [COP24] Marco Cianfriglia, Elia Onofri, and Marco Pedicini. mR_{LWE}-CP-ABE: A revocable CP-ABE for post-quantum cryptography. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0026/html>.

Ciet:2011:CEC

- [CQS11] Mathieu Ciet, Jean-Jacques Quisquater, and Francesco Sica. Compact elliptic curve representations. *Journal of Mathematical Cryptology*, 5(1):89–100, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Cascudo:2021:NSM

- [CS21] Ignacio Cascudo and Reto Schnyder. A note on secure multiparty computation via higher residue symbols. *Journal of Mathematical Cryptology*, 15(1):

284–297, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0013/html>.

Chen:2024:DHS

- [CS24] Imin Chen and David Sun. The dihedral hidden subgroup problem. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0029/html>.

Csirmaz:2020:SSD

- [Csi20] Laszlo Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15(1):157–173, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0045/html>.

Craven:2022:EGT

- [CW22] Matthew J. Craven and John R. Woodward. Evolution of group-theoretic cryptology attacks using hyper-heuristics. *Journal of Mathematical Cryptology*, 16(1): 49–63, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2021-0017/html>.

- Chee:2012:BCE**
- [CWZ12] Yeow Meng Chee, Huaxiong Wang, and Liang Feng Zhang. On the Bringer–Chabanne EPIR protocol for polynomial evaluation. *Journal of Mathematical Cryptology*, 5(3–4):277–301, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Dibert:2014:ISS**
- [DC14] Alexander Dibert and László Csirmaz. Infinite secret sharing — examples. *Journal of Mathematical Cryptology*, 8(2):141–168, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Duquesne:2014:ECP**
- [DEF14] Sylvain Duquesne, Nadia El Mrabet, and Emmanuel Fouotsa. Efficient computation of pairings on Jacobi quartic elliptic curves. *Journal of Mathematical Cryptology*, 8(4):331–362, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Dolev:2015:TEP**
- [DGG⁺15] Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, and Yelena Yuditsky. Towards efficient private distributed computation on unbounded input streams. *Journal of Mathematical Cryptology*, 9(2):79–94, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- DeMicheli:2020:CON**
- [DHS20] Gabrielle De Micheli, Nadia Heninger, and Barak Shani. Characterizing overstretched NTRU attacks. *Journal of Mathematical Cryptology*, 14(1):110–119, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0055/html>.
- DeFeo:2014:TQR**
- [DJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- DiCrescenzo:2020:DPG**
- [DKKS20] Giovanni Di Crescenzo, Matluba Khodjaeva, Delaram Kahrobaei, and Vladimir Shpilrain. Delegating a product of group exponentiations with application to signature schemes (submission to special NutMiC 2019 issue of JMC). *Journal of Mathematical Cryptology*, 14(1):438–459, October 30, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0036/html>.
- Delaplace:2020:CWB**
- [DM20] Claire Delaplace and Alexander May. Can we beat the square

- root bound for ECDLP over \mathbf{F}_{p^2} via representation? *Journal of Mathematical Cryptology*, 14(1): 293–306, August 18, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0025/html>. [DS18]
- [DN08] **Demirkiran:2008:CHC**
Cevahir Demirkiran and Enric Nart. Counting hyperelliptic curves that admit a Koblitz model. *Journal of Mathematical Cryptology*, 2(2):163–179, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Dow15] **Dowden:2015:SMT**
Chris Dowden. Secure message transmission in the presence of a fully generalised adversary. *Journal of Mathematical Cryptology*, 9(4):205–214, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [DS20]
- [DR07] **Daemen:2007:PDC**
Joan Daemen and Vincent Rijmen. Probability distributions of correlation and differentials in block ciphers. *Journal of Mathematical Cryptology*, 1(3): 221–242, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [DSG21]
- [DS17] **Dehkordi:2017:CCG**
Massoud Hadian Dehkordi and Ali Safi. The complexity of the connected graph access structure on seven participants. *Journal of Mathematical Cryptology*, 11(1):25–35, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Dey:2018:GRB**
- Sabyasachi Dey and Santanu Sarkar. Generalization of Roos bias in RC4 and some results on key–keystream relations. *Journal of Mathematical Cryptology*, 12(1):43–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2016-0061/jmc-2016-0061.xml>.
- Doroz:2020:FNE**
Yarkin Doröz and Berk Sunar. Flattening NTRU for evaluation key free homomorphic encryption. *Journal of Mathematical Cryptology*, 14(1):66–83, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0052/html>.
- Dugardin:2021:SMD**
Margaux Dugardin, Werner Schindler, and Sylvain Guilley. Stochastic methods defeat regular RSA exponentiation algorithms with combined blinding methods. *Journal of Mathematical Cryptology*, 15(1):408–433, April 20, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL

<https://www.degruyter.com/document/doi/10.1515/jmc-2020-0010/html>.

Dachman-Soled:2020:SRL

- [DSGKS20a] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi. (In)Security of Ring-LWE under partial key exposure. *Journal of Mathematical Cryptology*, 15(1):72–86, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0075/html>. [DT17]

Dachman-Soled:2020:TRA

- [DSGKS20b] Dana Dachman-Soled, Huijing Gong, Mukul Kulkarni, and Aria Shahverdi. Towards a ring analogue of the leftover hash lemma. *Journal of Mathematical Cryptology*, 15(1):87–110, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0076/html>. [Duq11]

DiScala:2020:CNV

- [DSS20] Antonio J. Di Scala, Carlo Sanna, and Edoardo Signorini. On the condition number of the Vandermonde matrix of the n th cyclotomic polynomial. *Journal of Mathematical Cryptology*, 15(1):174–178, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL

<https://www.degruyter.com/document/doi/10.1515/jmc-2020-0009/html>.

Dehkordi:2017:MDZ

- Massoud Hadian Dehkordi and Roghayeh Taghizadeh. Multiple differential-zero correlation linear cryptanalysis of reduced-round CAST-256. *Journal of Mathematical Cryptology*, 11(2):55–62, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0054/jmc-2016-0054.xml>.

Duquesne:2011:RAA

- Sylvain Duquesne. RNS arithmetic in \mathbf{F}_{p^k} and application to fast pairing computation. *Journal of Mathematical Cryptology*, 5(1):51–88, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Erdelyi:2024:LCR

- [EHKN24] Márton Erdélyi, Pál Hegedüs, Sándor Z. Kiss, and Gábor P. Nagy. On linear codes with random multiplier vectors and the maximum trace dimension property. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0022/html>.

- [Eke21] **Ekeråa:2021:QAC**
 Martin Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *Journal of Mathematical Cryptology*, 15(1):359–407, April 22, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0006/html>.
- [EOS07] **Engelbert:2007:SMT**
 D. Engelbert, R. Overbeck, and A. Schmidt. A summary of McEliece-type cryptosystems and their security. *Journal of Mathematical Cryptology*, 1(2):151–199, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Esk24] **Eskeland:2024:CPP**
 Sigurd Eskeland. Cryptanalysis of a privacy-preserving authentication scheme based on private set intersection. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0032/html>.
- [FGG⁺20] **Ferradi:2020:RSP**
 Houda Ferradi, Rémi Géraud, Sylvain Guilley, David Naccache, and Mehdi Tibouchi. Recovering secrets from prefix-dependent leakage. *Journal of Mathematical Cryptology*, 14(1):15–24, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0048/html>.
- [FHLMW08] **Fuji-Hara:2008:TCM**
 Ryoh Fuji-Hara, Xiyang Li, Ying Miao, and Dianhua Wu. A TWOOA construction for multi-receiver multi-message authentication codes. *Journal of Mathematical Cryptology*, 2(1):9–28, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FJ13] **Field:2013:UCT**
 Rebecca E. Field and Brant C. Jones. Using carry-truncated addition to analyze add-rotate-xor hash algorithms. *Journal of Mathematical Cryptology*, 7(2):97–110, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FK18] **Fotiadis:2018:GPF**
 Georgios Fotiadis and Elisavet Konstantinou. Generating pairing-friendly elliptic curve parameters using sparse families. *Journal of Mathematical Cryptology*, 12(2):83–99, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FL08] **Fancsali:2008:SAF**
 Sz. L. Fancsali and P. Ligeti. Some applications of finite geometry for secure network coding. *Journal of Mathematical*

- Cryptology*, 2(3):209–225, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [FS11]
- [FM13] Jean-Pierre Flori and Sihem Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. *Journal of Mathematical Cryptology*, 7(1):43–68, 2013. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FMS09] Simon Fischer, Willi Meier, and Dirk Stegemann. Some remarks on FCSRs and implications for stream ciphers. *Journal of Mathematical Cryptology*, 3(3):227–236, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Gal12]
- [FS08] Christiane Frougny and Wolfgang Steiner. Minimal weight expansions in Pisot bases. *Journal of Mathematical Cryptology*, 2(4):365–392, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Gau07]
- [FS09] John B. Friedlander and Igor E. Shparlinski. On the density of some special primes. *Journal of Mathematical Cryptology*, 3(3):265–271, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [GD13]
- [Fischlin:2011:SBS] Marc Fischlin and Dominique Schröder. Security of blind signatures under aborts and applications to adaptive oblivious transfer. *Journal of Mathematical Cryptology*, 5(2):169–203, 2011. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Farashahi:2009:HEC] Reza R. Farashahi, Igor E. Shparlinski, and José Felipe Voloch. On hashing into elliptic curves. *Journal of Mathematical Cryptology*, 3(4):353–360, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Gallant:2012:FDL] Robert P. Gallant. Finding discrete logarithms with a set orbit distinguisher. *Journal of Mathematical Cryptology*, 6(1):1–20, 2012. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Gaudry:2007:FGA] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1(3):243–265, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Gharahi:2013:PSS] Motahharez Gharahi and Masoud Hadian Dehkordi. Perfect secret sharing schemes for graph

- access structures on six participants. *Journal of Mathematical Cryptology*, 7(2):143–146, 2013. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [GGD20] Neha Goel, Indivar Gupta, and B. K. Dass. Survey on SAP and its application in public-key cryptography. *Journal of Mathematical Cryptology*, 14(1):144–152, July 3, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2016-0004/html>. **Goel:2020:SSA** [GP13]
- [GKL15] David Garber, Delaram Kahrobaei, and Ha T. Lam. Length-based attacks in polycyclic groups. *Journal of Mathematical Cryptology*, 9(1):33–43, 2015. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Garber:2015:LBA**
- [GÓS07] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy. Simplified pairing computation and security implications. *Journal of Mathematical Cryptology*, 1(3):267–281, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Galbraith:2007:SPC** [GPRS09]
- [GP09] István Gaál and Michael E. Pohst. On solving norm equations in global function fields. *Journal of Mathematical Cryptology*, 3(3):237–248, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Grosek:2013:CS**
- [GPR17] Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. Applications of design theory for the constructions of MDS matrices for lightweight cryptography. *Journal of Mathematical Cryptology*, 11(2):85–116, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0013/jmc-2016-0013.xml>. **Gupta:2017:ADT**
- [GPR17] Steven D. Galbraith, Jordi Pujolàs, Christophe Ritzenthaler, and Benjamin Smith. Distortion maps for supersingular genus two curves. *Journal of Mathematical Cryptology*, 3(1):1–18, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Galbraith:2009:DMS**
- [GPV24] Wissam Gbantous, Federico Pintore, and Mattia Veroni. Ef-
- Gaal:2009:SNE** [GPV24]
- Gbantous:2024:ESB**

- efficiency of SIDH-based signatures (yes, SIDH). *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0023/html>.
- [Grz20] Maciej Grześkowiak. A variant of the large sieve inequality with explicit constants. *Journal of Mathematical Cryptology*, 14(1):307–315, August 7, 2020. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0022/html>.
- [Gut09] Jaime Gutierrez. Foreword: Second Workshop on Mathematical Cryptology. *Journal of Mathematical Cryptology*, 3(3):175–176, 2009. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic). Held in Santander, October 23–25, 2008.
- [GZ13] Steven D. Galbraith and Chang-An Zhao. Self-pairings on hyperelliptic curves. *Journal of Mathematical Cryptology*, 7(1):31–42, 2013. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic). See erratum [GZ14].
- [GZ14] Steven D. Galbraith and Chang-An Zhao. Erratum: Self-pairings on hyperelliptic curves [J. Math. Cryptol. 7 (2013), 31–42] [MR3101014]. *Journal of Mathematical Cryptology*, 8(1):93, 2014. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic). See [GZ13].
- [HF07] Tomohiro Harayama and Donald K. Friesen. Weil sum for birthday attack in multivariate quadratic cryptosystem. *Journal of Mathematical Cryptology*, 1(1):79–104, 2007. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Hin08] M. Jason Hinek. On the security of multi-prime RSA. *Journal of Mathematical Cryptology*, 2(2):117–147, 2008. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Hit09] Laura Hitt. Families of genus 2 curves with small embedding degree. *Journal of Mathematical Cryptology*, 3(1):19–36, 2009. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [HKP+20] Ming-Deh Huang, Michiel Kusters, Christophe Petit, Sze Ling Yeo, and Yang Yun. Quasi-subfield polynomials and the elliptic curve discrete logarithm problem. *Journal of Mathematical Cryptology*, 14(1):

- 25–38, June 14, 2020. CODEN
 ???? ISSN 1862-2976 (print),
 1862-2984 (electronic). URL
[https://www.degruyter.com/
 document/doi/10.1515/jmc-
 2015-0049/html](https://www.degruyter.com/document/doi/10.1515/jmc-2015-0049/html). [HM07]
- Hinek:2009:ALS**
- [HL09] M. Jason Hinek and Charles
 C. Y. Lam. Another look at
 some fast modular arithmetic
 methods. *Journal of Mathemat-
 ical Cryptology*, 3(2):165–174,
 2009. CODEN ???? ISSN 1862-
 2976 (print), 1862-2984 (elec-
 tronic). [HS08]
- Hinek:2010:CMA**
- [HL10] M. Jason Hinek and Charles
 C. Y. Lam. Common modulus
 attacks on small private expon-
 ent RSA and some fast variants
 (in practice). *Journal of Math-
 ematical Cryptology*, 4(1):57–93,
 2010. CODEN ???? ISSN 1862-
 2976 (print), 1862-2984 (elec-
 tronic). [HS15a]
- Harsanyi:2019:EIR**
- [HL19] Károly Harsányi and Péter
 Ligeti. Exact information rat-
 ios for secret sharing on small
 graphs with girth at least 5.
*Journal of Mathematical Cryptol-
 ogy*, 13(2):107–??, June 2019.
 CODEN ???? ISSN 1862-
 2976 (print), 1862-2984 (elec-
 tronic). URL [http://www.
 degruyter.com/view/j/jmc.
 2019.13.issue-2/jmc-2018-
 0024/jmc-2018-0024.xml](http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0024/jmc-2018-0024.xml). [HST10]
- Heuberger:2007:MWC**
- Clemens Heuberger and James A. Muir. Minimal weight and colexicographically minimal integer representations. *Journal of Mathematical Cryptology*, 1(4):297–328, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Hartung:2008:ISB**
- Rupert J. Hartung and Claus-Peter Schnorr. Identification and signatures based on NP-hard problems of indefinite quadratic forms. *Journal of Mathematical Cryptology*, 2(4):327–341, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Hameed:2015:CIW**
- Ali Hameed and Arkadii Slinko. A characterisation of ideal weighted secret sharing schemes. *Journal of Mathematical Cryptology*, 9(4):227–244, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Henry:2015:LAR**
- Kevin J. Henry and Douglas R. Stinson. Linear approaches to resilient aggregation in sensor networks. *Journal of Mathematical Cryptology*, 9(4):245–272, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Hakuta:2010:EAS**
- Keisuke Hakuta, Hisayoshi Sato, and Tsuyoshi Takagi. Efficient

- arithmetic on subfield elliptic curves over small finite fields of odd characteristic. *Journal of Mathematical Cryptology*, 4(3): 199–238, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [IK23]
- [HSWZ20] Jeffrey Hoffstein, Joseph H. Silverman, William Whyte, and Zhenfei Zhang. A signature scheme from the finite field isomorphism problem. *Journal of Mathematical Cryptology*, 14(1): 39–54, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0050/html>.
- [HVV14] Deepthi Haridas, Sarma Venkataraman, and Geeta Varadan. Security analysis of modified Rivest scheme. *Journal of Mathematical Cryptology*, 8(3):297–303, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [HWCD11] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. An exploration of affine group laws for elliptic curves. *Journal of Mathematical Cryptology*, 5(1):1–50, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [JCK+18] Wachirapong Jirakitpuwapat, Parin Chaipunya, Poom Kumam, Sompong Dhompongsa, and Phatiphat Thounthong. New methods of construction of Cartesian authentication codes from geometries over finite commutative rings. *Journal of Mathematical Cryptology*, 12(3):119–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0057/jmc-2017-0057.xml>.
- [Jia14] Shaoquan Jiang. Persistent asymmetric password-based key exchange. *Journal of Mathematical Cryptology*, 8(1):31–70, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [JLLRL20] David Jao, Jason LeGrow, Christopher Leonardi, and Luis
- Isobe:2023:CEP**
- Shuji Isobe and Eisuke Koizumi. A construction of encryption protocols over some semidirect products. *Journal of Mathematical Cryptology*, 17(1): ??, January 2023. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0018/html>.
- Hoffstein:2020:SSF**
- Jirakitpuwapat:2018:NMC**
- Haridas:2014:SAM**
- Jiang:2014:PAP**
- Hisil:2011:EAG**
- Jao:2020:STP**

- Ruiz-Lopez. A subexponential-time, polynomial quantum space algorithm for inverting the CM group action. *Journal of Mathematical Cryptology*, 14(1):129–138, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0057/html>. [JP20]
- Joye:2020:EPR**
- [JLNN20] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The eleventh power residue symbol. *Journal of Mathematical Cryptology*, 15(1):111–122, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0077/html>. [JSN13]
- Jha:2016:RSG**
- [JN16] Ashwin Jha and Mridul Nandi. Revisiting structure graphs: applications to CBC–MAC and EMAC. *Journal of Mathematical Cryptology*, 10(3–4):157–180, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [Jus14]
- Joye:2020:PEA**
- [Joy20] Marc Joye. Protecting ECC against fault attacks: The ring extension method revisited. *Journal of Mathematical Cryptology*, 14(1):254–267, August 1, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0030/html>. [Joux:2020:PNT]
- Antoine Joux and Jacek Pomykała. Preface for the Number-Theoretic Methods in Cryptology conferences. *Journal of Mathematical Cryptology*, 14(1):393–396, October 13, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0111/html>. [Jhanwar:2013:USI]
- Mahabir P. Jhanwar and Reihaneh Safavi-Naini. Unconditionally-secure ideal robust secret sharing schemes for threshold and multilevel access structure. *Journal of Mathematical Cryptology*, 7(4):279–296, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [Justus:2014:DQR]
- Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. *Journal of Mathematical Cryptology*, 8(2):115–140, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [Justus:2015:DQR]
- Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. II.

Journal of Mathematical Cryptology, 9(2):115–137, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Wei:2012:FMP

[jWW12] Tzer jen Wei and Lih-Chung Wang. A fast mental poker protocol. *Journal of Mathematical Cryptology*, 6(1):39–68, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Karabina:2010:FCC

[Kar10] Koray Karabina. Factor-4 and 6 compression of cyclotomic subgroups of $\mathbf{F}_{2^{4m}}^*$ and $\mathbf{F}_{3^{6m}}^*$. *Journal of Mathematical Cryptology*, 4(1):1–42, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Karmakar:2020:EPF

[Kar20a] Sudhangshu B. Karmakar. An elementary proof of Fermat’s Last Theorem for all even exponents. *Journal of Mathematical Cryptology*, 14(1):139–142, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2016-0018/html>. See retraction [Kar20b].

Karmakar:2020:REP

[Kar20b] Sudhangshu B. Karmakar. Retraction of: An elementary proof of Fermat’s Last Theorem for all even exponents. *Journal of Mathematical Cryptology*, 14(1):143, July 3, 2020. CODEN

???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2017-2000/html>. See [Kar20a].

Klamti:2023:CBH

[KH23] Jean Belo Klamti and M. Anwarul Hasan. A code-based hybrid signcryption scheme. *Journal of Mathematical Cryptology*, 17(1):??, January 2023. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0002/html>.

Kortelainen:2010:MAG

[KHK10] Juha Kortelainen, Kimmo Halunen, and Tuomas Kortelainen. Multicollision attacks and generalized iterated hash functions. *Journal of Mathematical Cryptology*, 4(3):239–270, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Kawa:2023:ASD

[KK23] Renata Kawa and Mieczysław Kula. Access structures determined by uniform polymatroids. *Journal of Mathematical Cryptology*, 17(1):??, January 2023. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0017/html>.

- [KM08] Neal Koblitz and Alfred Menezes. Another look at non-standard discrete log and Diffie–Hellman problems. *Journal of Mathematical Cryptology*, 2(4):311–326, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Koblitz:2008:ALN**
- [KM13] Neal Koblitz and Alfred Menezes. Another look at HMAC. *Journal of Mathematical Cryptology*, 7(3):225–251, 2013. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Koblitz:2013:ALH**
- [KMNN19] Shizuo Kaji, Toshiaki Maeno, Koji Nuida, and Yasuhide Numata. Polynomial expressions of p -ary auction functions. *Journal of Mathematical Cryptology*, 13(2):69–??, June 2019. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0016/jmc-2018-0016.xml>. **Kaji:2019:PEP**
- [KMPS10] Koray Karabina, Alfred Menezes, Carl Pomerance, and Igor E. Shparlinski. On the asymptotic effectiveness of Weil descent attacks. *Journal of Mathematical Cryptology*, 4(2):175–191, 2010. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Karabina:2010:AEW**
- [KMU20] Neal Koblitz and Alfred Menezes. Another look at non-standard discrete log and Diffie–Hellman problems. *Journal of Mathematical Cryptology*, 15(1):237–249, December 1, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0015/html>. **Koblitz:2008:ALN**
- [KNP13] Kaoru Kurosawa, Ryo Nojima, and Le Trieu Phong. New leakage-resilient CCA-secure public key encryption. *Journal of Mathematical Cryptology*, 7(4):297–312, 2013. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Kurosawa:2013:NLR**
- [Kob07] Neal Koblitz. Another look at automated theorem-proving. *Journal of Mathematical Cryptology*, 1(4):385–403, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Koblitz:2007:ALA**
- [Kob12] Neal Koblitz. Another look at automated theorem-proving II. *Journal of Mathematical Cryptology*, 5(3–4):205–224, 2012. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). **Koblitz:2012:ALA**
- [KT20] Taechan Kim and Mehdi Tibouchi. Equidistribution among **Kim:2020:EAC**

- cosets of elliptic curve points in intervals. *Journal of Mathematical Cryptology*, 14(1):339–345, August 7, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0020/html>.
- [KW19] **Kousidis:2019:FFD**
Stavros Kousidis and Andreas Wiemers. On the first fall degree of summation polynomials. *Journal of Mathematical Cryptology*, 13(3–4):229–??, September 2019. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2017-0022/jmc-2017-0022.xml>.
- [KU15] **Kotov:2015:ACP**
Matvei Kotov and Alexander Ushakov. Analysis of a certain polycyclic-group-based cryptosystem. *Journal of Mathematical Cryptology*, 9(3):161–167, 2015. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Laa20] **Kotov:2018:AKE**
Matvei Kotov and Alexander Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–??, September 2018. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2016-0064/jmc-2016-0064.xml>.
- [Kus18] **Kushwaha:2018:ILB**
Prabhat Kushwaha. Improved lower bound for Diffie–Hellman problem using multiplicative group of a finite field as auxiliary group. *Journal of Mathematical Cryptology*, 12(2):101–118, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [LdV19] **Li:2007:SAC**
Yuan Li and T. W. Cusick. Strict avalanche criterion over finite fields. *Journal of Mathematical Cryptology*, 1(1):65–78, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Lc07] **Lavauzelle:2019:GCP**
Julien Lavauzelle and Françoise Levydit Vehel. Generic constructions of PoRs from codes and instantiations. *Journal of Mathematical Cryptology*, 13(2):81–??, June 2019. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).

- (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0018/jmc-2018-0018.xml>.
- [LL15] Kim Laine and Kristin Lauter. Time-memory trade-offs for index calculus in genus 3. *Journal of Mathematical Cryptology*, 9(2):95–114, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Laine:2015:TMT**
- [LMPW15] Atul Luykx, Bart Mennink, Bart Preneel, and Laura Winen. Two-permutation-based hashing with binary mixing. *Journal of Mathematical Cryptology*, 9(3):139–150, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Luykx:2015:TPB**
- [LNR09] Mario Lamberger, Tomislav Nad, and Vincent Rijmen. Numerical solvers and cryptanalysis. *Journal of Mathematical Cryptology*, 3(3):249–263, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Lamberger:2009:NSC**
- [LPS17] Yao Lu, Liqiang Peng, and Santanu Sarkar. Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. *Journal of Mathematical Cryptology*, 11(2):117–130, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL [https://www.degruyter.com/view/j/jmc.2017.11.issue-](https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0025/jmc-2016-0025.xml)
- [LPS20] Andrea Lesavourey, Thomas Plantard, and Willy Susilo. Short principal ideal problem in multicubic fields. *Journal of Mathematical Cryptology*, 14(1):359–392, August 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0028/html>. **Lesavourey:2020:SPI**
- [LS07] Tanja Lange and Igor E. Shparlinski. Distribution of some sequences of points on elliptic curves. *Journal of Mathematical Cryptology*, 1(1):1–11, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Lange:2007:DSS**
- [LS18] Thalia M. Laing and Douglas R. Stinson. A survey and refinement of repairable threshold schemes. *Journal of Mathematical Cryptology*, 12(1):57–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0058/jmc-2017-0058.xml>. **Laing:2018:SRR**
- [LU08] Jonathan Longrigg and Alexander Ushakov. Cryptanalysis of the shifted conjugacy authentication protocol. *Journal of*
- Longrigg:2008:CSC**

- Mathematical Cryptology*, 2(2): 109–116, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [LZ23] Zhenyu Liu and Zepeng Zhuo. Further research results on confusion coefficient of Boolean functions. *Journal of Mathematical Cryptology*, 17(1): ??, January 2023. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2021-0039/html>.
- [MA17] Ahmed Mohammed and Abdulrahman Alkhelaifi. RSA: A number of formulas to improve the search for $p + q$. *Journal of Mathematical Cryptology*, 11(4): 195–203, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Mag13] Spyros S. Magliveras. Foreword. *Journal of Mathematical Cryptology*, 7(3):181–182, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2013.7.issue-3/jmc-2013-5001/jmc-2013-5001.xml>.
- [Maz12] Gérard Maze. Analysis of a key distribution scheme in secure multicasting. *Journal of Mathematical Cryptology*, 6(1):69–80, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Men07] Alfred Menezes. Another look at HMQV. *Journal of Mathematical Cryptology*, 1(1):47–64, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MFP10] Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *Journal of Mathematical Cryptology*, 4(2):95–120, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Mie08] Thilo Mie. Polylogarithmic two-round argument systems. *Journal of Mathematical Cryptology*, 2(4):343–363, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MN07] Keith Martin and Siaw-Lynn Ng. The combinatorics of generalised cumulative arrays. *Journal of Mathematical Cryptology*, 1(1):13–32, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Moc23] Alexander Moch. Provable security against generic attacks on stream ciphers. *Journal of Mathematical Cryptology*, 17(1): ??, January 2023. CODEN

- ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0033/html>.
- [Mor08] David J. Mireles Morales. An attack on disguised elliptic curves. *Journal of Mathematical Cryptology*, 2(1):1–8, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MP08] S. Murphy and M. B. Paterson. A geometric view of cryptographic equation solving. *Journal of Mathematical Cryptology*, 2(1):63–107, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MP20] Sean Murphy and Rachel Player. Discretisation and product distributions in Ring-LWE. *Journal of Mathematical Cryptology*, 15(1):45–59, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0073/html>.
- [MPST16] Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. Indifferentiability security of the fast wide pipe hash: breaking the birthday barrier. *Journal of Mathematical Cryptology*, 10(2): 101–133, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MR20] **Morales:2008:ADE** Gary McGuire and Oisín Robinson. Lattice sieving in three dimensions for discrete log in medium characteristic. *Journal of Mathematical Cryptology*, 15(1):223–236, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0008/html>.
- [MSP12] **Murphy:2008:GVC** Nicky Mouha, Gautham Sekar, and Bart Preneel. Challenging the increased resistance of regular hash functions against birthday attacks. *Journal of Mathematical Cryptology*, 6(3–4):229–248, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-3-4/jmc-2011-0010/jmc-2011-0010.xml>.
- [MU08] **Murphy:2020:DPD** Alexei G. Myasnikov and Alexander Ushakov. Random subgroups and analysis of the length-based and quotient attacks. *Journal of Mathematical Cryptology*, 2(1):29–61, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MU08] **Moody:2016:ISF** **Myasnikov:2008:RSA**

- [MU10] **Mosina:2010:MSA**
 Natalia Mosina and Alexander Ushakov. Mean-set attack: cryptanalysis of Sibert et al. authentication protocol. *Journal of Mathematical Cryptology*, 4(2):149–174, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MU14] **Myasnikov:2014:CMC**
 Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of matrix conjugation schemes. *Journal of Mathematical Cryptology*, 8(2):95–114, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Mul11] **Mullan:2011:CVS**
 Ciaran Mullan. Cryptanalysing variants of Stickel’s key agreement scheme. *Journal of Mathematical Cryptology*, 4(4):365–373, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Mur12] **Murphy:2012:ELH**
 Sean Murphy. The effectiveness of the linear hull effect. *Journal of Mathematical Cryptology*, 6(2):137–147, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0025/jmc-2011-0025.xml>.
- [MW12] **Moody:2012:FEC**
 Dustin Moody and Hongfeng Wu. Families of elliptic curves with rational 3-torsion. *Journal of Mathematical Cryptology*, 5(3–4):225–246, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Nan09] **Nandi:2009:ISA**
 Mridul Nandi. Improved security analysis for OMAC as a pseudorandom function. *Journal of Mathematical Cryptology*, 3(2):133–148, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [NM08] **Nandi:2008:ISA**
 Mridul Nandi and Avradip Mandal. Improved security analysis of PMAC. *Journal of Mathematical Cryptology*, 2(2):149–162, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [NP16] **Nandi:2016:SJS**
 Mridul Nandi and Tapas Pandit. On the security of joint signature and encryption revisited. *Journal of Mathematical Cryptology*, 10(3–4):181–221, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [NP19] **Nandi:2019:PSP**
 Mridul Nandi and Tapas Pandit. Predicate signatures from pair encodings via dual system proof technique. *Journal of Mathematical Cryptology*, 13(3–4):197–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

- (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2017-0007/jmc-2017-0007.xml>. **Neven:2009:HFR** [OS14]
- [NSW09] Gregory Neven, Nigel P. Smart, and Bogdan Warinschi. Hash function requirements for Schnorr signatures. *Journal of Mathematical Cryptology*, 3(1):69–87, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Nguyen:2008:SAS** [Par18]
- [Oka12] Keiji Okano. On the ρ -values of complete families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 6(3–4):249–268, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-3-4/jmc-2012-0011/jmc-2012-0011.xml?format=INT>. **Okano:2012:VCF** [Per12]
- [OPSB13] Mohammad Ali Orumiehchiha, Josef Pieprzyk, Ron Steinfeld, and Harry Bartlett. Security analysis of linearly filtered NLF-SRs. *Journal of Mathematical Cryptology*, 7(4):313–332, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Orumiehchiha:2013:SAL** [PGS20]
- Sami Omar and Housseem Sabri. Fast hash functions and convolution product. *Journal of Mathematical Cryptology*, 8(2):169–187, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Omar:2014:FHF**
- Juha Partala. Algebraic generalization of Diffie–Hellman key exchange. *Journal of Mathematical Cryptology*, 12(1):1–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0015/jmc-2017-0015.xml>. **Partala:2018:AGD**
- Edoardo Persichetti. Compact McEliece keys based on quasi-dyadic Srivastava codes. *Journal of Mathematical Cryptology*, 6(2):149–169, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2012.6.issue-2/jmc-2011-0099/jmc-2011-0099.xml>. **Persichetti:2012:CMK**
- Atul Pandey, Indivar Gupta, and Dhiraj Kumar Singh. Improved cryptanalysis of a ElGamal cryptosystem based on matrices over group rings. *Journal*

- of *Mathematical Cryptology*, 15 (1):266–279, December 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0054/html>.
- [Pop17] Serguei Popov. On a decentralized trustless pseudo-random number generation algorithm. *Journal of Mathematical Cryptology*, 11(1):37–43, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Pou16] Dimitrios Poulakis. New lattice attacks on DSA schemes. *Journal of Mathematical Cryptology*, 10(2):135–144, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [PP18] Eduardo Carvalho Pinto and Christophe Petit. Better path-finding algorithms in LPS Ramanujan graphs. *Journal of Mathematical Cryptology*, 12(4):191–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2017-0051/jmc-2017-0051.xml>.
- [PR20] Jacek Pomykała and Maciej Radziejewski. Integer factoring and compositeness witnesses. *Journal of Mathematical Cryptology*, 14(1):346–358, August 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0023/html>.
- [PS08] M. B. Paterson and D. R. Stinson. Two attacks on a sensor network key distribution scheme of Cheng and Agrawal. *Journal of Mathematical Cryptology*, 2(4):393–403, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [PS15] Maura B. Paterson and Douglas R. Stinson. Optimal constructions for ID-based one-way-function key predistribution schemes realizing specified communication graphs. *Journal of Mathematical Cryptology*, 9(4):215–225, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [PS20] Maura B. Paterson and Douglas R. Stinson. On the equivalence of authentication codes and robust $(2, 2)$ -threshold schemes. *Journal of Mathematical Cryptology*, 15(1):179–196, November 25, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/>

Popov:2017:DTP**Paterson:2008:TAS****Poulakis:2016:NLA****Paterson:2015:OCI****Pinto:2018:BPF****Paterson:2020:EAC****Pomykala:2020:IFC**

- document/doi/10.1515/jmc-2019-0048/html.
- [PSU13] Maura B. Paterson, Douglas R. Stinson, and Jalaj Upadhyay. A coding theory foundation for the analysis of general unconditionally secure proof-of-retrievability schemes for cloud storage. *Journal of Mathematical Cryptology*, 7(3):183–216, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [PSU18] Maura B. Paterson, Douglas R. Stinson, and Jalaj Upadhyay. Multi-prover proof of retrievability. *Journal of Mathematical Cryptology*, 12(4):203–??, December 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-4/jmc-2018-0012/jmc-2018-0012.xml>.
- [Rei17] Dominik Reichl. Tame logarithmic signatures of abelian groups. *Journal of Mathematical Cryptology*, 11(4):205–214, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Rei21] Elizabeth M. Reid. Using inclusion/exclusion to find bent and balanced monomial rotation symmetric functions. *Journal of Mathematical Cryptology*, 15(1):298–304, January 29, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0021/html>.
- [RM20] Dylan Rudy and Chris Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology*, 15(1):280–283, December 20, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0061/html>.
- [RMS24] Loïc Rouquette, Marine Minier, and Christine Solnon. Automatic boomerang attacks search on Rijndael. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0027/html>.
- [RS22] Nael Rahman and Vladimir Shpilrain. MAKE: a matrix action key exchange. *Journal of Mathematical Cryptology*, 16(1):64–72, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc->

- 2020-0053/html. See successful attack [BKL22].
- [RST07] **Ruinskiy:2007:LBC**
Dima Ruinskiy, Adi Shamir, and Boaz Tsaban. Length-based cryptanalysis: the case of Thompson’s group. *Journal of Mathematical Cryptology*, 1(4): 359–372, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Sch17]
- [RUS23] **Romankov:2023:AQA**
Vitaly Roman’kov, Alexander Ushakov, and Vladimir Shpilrain. Algebraic and quantum attacks on two digital signature schemes. *Journal of Mathematical Cryptology*, 17(1): ??, January 2023. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0023/html>. [Sha14]
- [RZ18] **Raddum:2018:MSB**
Håvard Raddum and Pavol Zajač. MRHS solver based on linear algebra and exhaustive search. *Journal of Mathematical Cryptology*, 12(3):143–??, September 2018. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0005/jmc-2017-0005.xml>. [Sho10]
- [Sch08] **Schindler:2008:ASM**
Werner Schindler. Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. *Journal of Mathematical Cryptology*, 2(3):291–310, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Scholl:2017:IEC]
- [Sch17] Travis Scholl. Isolated elliptic curves and the MOV attack. *Journal of Mathematical Cryptology*, 11(3):131–146, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). [Sha:2014:NIC]
- [Sha14] Min Sha. On the non-idealness of cyclotomic families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 8(4):417–440, 2014. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Shokrieh:2010:MPD]
- [Sho10] Farbod Shokrieh. The monodromy pairing and discrete logarithm on the Jacobian of finite graphs. *Journal of Mathematical Cryptology*, 4(1):43–56, 2010. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). [Sica:2020:FH]
- [Sic20] Francesco Sica. Factoring with hints. *Journal of Mathematical Cryptology*, 15(1):123–130, November 17, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0078/html>.

- [Sil07] **Silverman:2007:OPS**
Robert D. Silverman. Optimal parameterization of SNFS. *Journal of Mathematical Cryptology*, 1(2):105–124, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [SS09]
- [SPB22] **Santini:2022:RFC**
Paolo Santini, Edoardo Persichetti, and Marco Baldi. Reproducible families of codes and cryptographic applications. *Journal of Mathematical Cryptology*, 16(1):20–48, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0003/html>. [SS16a]
- [SPS19] **Sipasseuth:2019:EGG**
Arnaud Sipasseuth, Thomas Plantard, and Willy Susilo. Enhancing Goldreich, Goldwasser and Halevi’s scheme with intersecting lattices. *Journal of Mathematical Cryptology*, 13(3–4):169–??, September 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2016-0066/jmc-2016-0066.xml>. [SS17]
- [SPSS12] **Sepahi:2012:NSN**
Reza Sepahi, Josef Pieprzyk, Siamak F. Shahandashti, and Berry Schoenmakers. New security notions and relations for public-key encryption. *Journal of Mathematical Cryptology*, 6(3–4):183–227, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [SS09]
- Saxena:2009:CPB**
Amitabh Saxena and Ben Soh. A cryptographic primitive based on hidden-order groups. *Journal of Mathematical Cryptology*, 3(2):89–132, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Samajder:2016:ALN**
Subhabrata Samajder and Palash Sarkar. Another look at normal approximations in cryptanalysis. *Journal of Mathematical Cryptology*, 10(2):69–99, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Swanson:2016:USS**
Colleen M. Swanson and Douglas R. Stinson. Unconditionally secure signature schemes revisited. *Journal of Mathematical Cryptology*, 10(1):35–67, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [SS16b]
- Samajder:2017:RUB**
Subhabrata Samajder and Palash Sarkar. Rigorous upper bounds on data complexities of block cipher cryptanalysis. *Journal of Mathematical Cryptology*, 11(3):147–175, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

- [SSA17] **Saraswat:2017:SAP** Vishal Saraswat, Rajeev Anand Sahu, and Amit K. Awasthi. A secure anonymous proxy sign-cryption scheme. *Journal of Mathematical Cryptology*, 11(2): 63–84, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2015-0014/jmc-2015-0014.xml>.
- [SSS11] **Singh:2011:PDE** Rajesh P. Singh, A. Saikia, and B. K. Sarma. Poly-dragon: an efficient multivariate public key cryptosystem. *Journal of Mathematical Cryptology*, 4(4): 349–364, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [ST24] **Sala:2024:GSE** Massimiliano Sala and Daniele Taufer. Group structure of elliptic curves over $\mathbf{Z}/N\mathbf{Z}$. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0025/html>.
- [SU14] **Stinson:2014:EDS** Douglas R. Stinson and Jalaj Upadhyay. Is extracting data the same as possessing data? *Journal of Mathematical Cryptology*, 8(2):189–207, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SvT10] **Svaba:2010:PKC** Pavol Svaba and Tran van Trung. Public key cryptosystem MST_3 : cryptanalysis and realization. *Journal of Mathematical Cryptology*, 4(3):271–315, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SvT13] **Staszewski:2013:SAL** Reiner Staszewski and Tran van Trung. Strongly aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 7(2): 147–179, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2013.7.issue-2/jmc-2013-5000/jmc-2013-5000.xml>.
- [SW07a] **Stinson:2007:SRQ** D. R. Stinson and R. Wei. Some results on query processes and reconstruction functions for unconditionally secure 2-server 1-round binary private information retrieval protocols. *Journal of Mathematical Cryptology*, 1(1):33–46, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SW07b] **Stinson:2007:EST** D. R. Stinson and J. Wu. An efficient and secure two-flow zero-knowledge identification protocol. *Journal of Mathematical Cryptology*, 1(3):201–220, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

- [SW15] **Sparr:2015:RFK** Rüdiger Sparr and Ralph Wernsdorf. The round functions of KASUMI generate the alternating group. *Journal of Mathematical Cryptology*, 9(1):23–32, 2015. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [TKF⁺20] **Takahashi:2020:AAS** Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, and Kazuhiro Yokoyama. Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology*, 15(1):31–44, November 17, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0072/html>.
- [Tim24] **Timpanella:2024:GDL** Marco Timpanella. On a generalization of the Deligne–Lusztig curve of Suzuki type and application to AG codes. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0024/html>.
- [TL15] **Tsaban:2015:CMS** Boaz Tsaban and Noam Lifshitz. Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. *Journal of Mathematical Cryptology*, 9(2):75–78, 2015. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Tis11] **Tischhauser:2011:NCA** Elmar Tischhauser. Nonsmooth cryptanalysis, with an application to the stream cipher MICKEY. *Journal of Mathematical Cryptology*, 4(4):317–348, 2011. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [TIS20] **Tomkins:2020:NZT** Hayley Tomkins, Monica Nevins, and Hadi Salmasian. New Zémor–Tillich type hash functions over $\text{GL}_2(\mathbf{F}_{p^n})$. *Journal of Mathematical Cryptology*, 14(1):236–253, August 1, 2020. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0033/html>.
- [TJBY13] **Tassa:2013:OEM** Tamir Tassa, Ayman Jarrous, and Yonatan Ben-Ya’akov. Oblivious evaluation of multivariate polynomials. *Journal of Mathematical Cryptology*, 7(1):1–29, 2013. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [TSJL20] **Taraskin:2020:TIB** Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T.

- LeGrow. Towards isogeny-based password-authenticated key establishment. *Journal of Mathematical Cryptology*, 15(1):18–30, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0071/html>. [vzGS09]
- Tibouchi:2020:OBA**
- [TW20] Mehdi Tibouchi and Alexandre Wallet. One bit is all it takes: A devastating timing attack on BLISS’s non-constant time sign flips. *Journal of Mathematical Cryptology*, 15(1):131–142, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0079/html>. [vzGS13]
- Urbanik:2020:NTS**
- [UJ20] David Urbanik and David Jao. New techniques for SIDH-based NIKE. *Journal of Mathematical Cryptology*, 14(1):120–128, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0056/html>. [WC07]
- vanTrung:2018:CSA**
- [vT18] Tran van Trung. Construction of strongly aperiodic logarithmic signatures. *Journal of Mathematical Cryptology*, 12(1):23–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0048/jmc-2017-0048.xml>. [vzGS09]
- vonzurGathen:2009:SSP**
- Joachim von zur Gathen and Igor E. Shparlinski. Subset sum pseudorandom numbers: fast generation and distribution. *Journal of Mathematical Cryptology*, 3(2):149–163, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- vonzurGathen:2013:GSP**
- Joachim von zur Gathen and Igor E. Shparlinski. Generating safe primes. *Journal of Mathematical Cryptology*, 7(4):333–365, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Walker:2007:PHF**
- Robert A. Walker II and Charles J. Colbourn. Perfect Hash families: constructions and existence. *Journal of Mathematical Cryptology*, 1(2):125–150, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Wang:2013:MCN**
- [WL13] Tianze Wang and Dongdai Lin. A method for counting the number of polynomial equivalence classes. *Journal of Mathematical Cryptology*, 7(1):69–95, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

- [WP11] Christopher Wolf and Bart Preneel. Equivalent keys in Multivariate Quadratic public key systems. *Journal of Mathematical Cryptology*, 4(4): 375–415, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Wolf:2011:EKU**
- [WS09] J. Wu and D. R. Stinson. An efficient identification protocol secure against concurrent-reset attacks. *Journal of Mathematical Cryptology*, 3(4):339–352, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Wu:2009:EIP**
- [Wun19] Thomas Wunderer. A detailed analysis of the hybrid lattice-reduction and meet-in-the-middle attack. *Journal of Mathematical Cryptology*, 13(1): 1–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2016-0044/jmc-2016-0044.xml>. **Wunderer:2019:DAH**
- [Yas20] Masaya Yasuda. Self-dual Deep-BKZ for finding short lattice vectors. *Journal of Mathematical Cryptology*, 14(1):84–94, June 14, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0053/html>. **Yasuda:2020:SDD**
- [YH24] Kyosuke Yamashita and Keisuke Hara. On the black-box impossibility of multi-designated verifiers signature schemes from ring signature schemes. *Journal of Mathematical Cryptology*, 18(1):??, January 2024. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2023-0028/html>. **Yamashita:2024:BBI**
- [Yoo15] Kisoon Yoon. A new method of choosing primitive elements for Brezing–Weng families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 9(1):1–9, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Yoon:2015:NMC**
- [YYS+14] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, and Takeshi Koshihara. On the exact decryption range for Gentry–Halevi’s implementation of fully homomorphic encryption. *Journal of Mathematical Cryptology*, 8(3): 305–329, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Yasuda:2014:EDR**
- [YYS+17] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama,

- Jun Kogure, and Takeshi Koshiha. Analysis of decreasing squared-sum of Gram–Schmidt lengths for short lattice vectors. *Journal of Mathematical Cryptology*, 11(1):1–24, 2017. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [ZLA21]
- Yokoyama:2020:CBS**
- [YYTK20] Kazuhiro Yokoyama, Masaya Yasuda, Yasushi Takahashi, and Jun Kogure. Complexity bounds on Semaev’s naive index calculus method for ECDLP. *Journal of Mathematical Cryptology*, 14(1):460–485, October 30, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0029/html>.
- Zajac:2013:NMS**
- [Zaj13] Pavol Zajac. A new method to solve MRHS equation systems and its connection to group factorization. *Journal of Mathematical Cryptology*, 7(4):367–381, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Zhou:2022:CCB**
- [ZHM⁺22] Yu Zhou, Jianyong Hu, Xudong Miao, Yu Han, and Fuzhong Zhang. On the confusion coefficient of Boolean functions. *Journal of Mathematical Cryptology*, 16(1):1–13, January 2022. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2021-0012/html>.
- Zhang:2021:SBS**
- Jing Zhang, Yuan Li, and John O. Adeyeye. Sensitivities and block sensitivities of elementary symmetric Boolean functions. *Journal of Mathematical Cryptology*, 15(1):434–453, April 22, 2021. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0042/html>.
- Zhou:2020:CPB**
- [ZMD20] Yu Zhou, Daoguang Mu, and Xinfeng Dong. On cryptographic properties of $(n + 1)$ -bit S -boxes constructed by known n -bit S -boxes. *Journal of Mathematical Cryptology*, 15(1):258–265, December 8, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0004/html>.
- Zhang:2020:PPV**
- [ZSN20] Liang Feng Zhang and Reihaneh Safavi-Naini. Privacy-preserving verifiable delegation of polynomial and matrix functions. *Journal of Mathematical Cryptology*, 14(1):153–171, July 3, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/>

document/doi/10.1515/jmc-
2018-0039/html.