

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/>

05 April 2022
Version 1.07

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]. $ax \equiv b \pmod{n}$ [GP13]. $GL_2(\mathbf{F}_{p^n})$ [TNS20]. k [AMW07, BW09]. $\mathbf{F}_{2^{4m}}^*$ [Kar10]. $\mathbf{F}_{3^{6m}}^*$ [Kar10]. \mathbf{F}_p [BW09]. \mathbf{F}_{p^2} [DM20]. \mathbf{F}_{p^k} [Duq11]. $\mathbf{Q}(\zeta_{2s})$ [BS19]. \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]. **-error** [AMW07, BW09]. **-ideal** [AJZT19]. **-rotation** [CC15]. **-round** [SW07a]. **-server** [SW07a]. **-threshold** [PS20]. **-torsion** [MW12]. **-values** [Oka12].

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

7 [GZ14].

abelian [Rei17]. **aborts** [FS11]. **Abu** [Bla10]. **access** [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]. **Against** [Joy20, BS19, BBP⁺20, MSP12, WS09].

aggregation [HS15b]. **Agrawal** [PS08]. **agreement** [Mul11]. **AJPS** [CG20]. **al** [MU10]. **algebra** [BCSV20, KU18, RZ18]. **Algebraic** [BF09, Par18, TKF⁺20]. **algebras** [Ano20]. **algorithm** [BGMP08, BP20, BDJ14, JLLRL20, Pop17]. **Algorithms** [CCH⁺20, AR15, DSG21, Eke21, FJ13, NV08, PP18]. **alternating** [SW15]. **Among** [KT20]. **Analogue** [DSGKS20b]. **Analysis** [KU15, KU18, Maz12, YYS⁺17, CDK18, HVV14, MU08, NM08, Nan09, OPSB13, PSU13, Sch08, Wun19]. **analyze** [FJ13]. **Annual** [CLS20, CLY20]. **anonymous** [SSA17]. **Aperiodic** [BdW12, SvT13, vT18]. **Application** [DKKS20, Duq11, GGD20, 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, Wun19]. **Attacks** [Joy20, BS19, CW22, DHS20, GKL15, HL10, KMPS10, KHK10, MSP12, MU08, PS08, Pou16, WS09]. **attribute** [AL11]. **auction** [KMNN19]. **Authenticated** [BLLN21, TSJL20, ASB⁺18, CN22]. **authentication** [ACP10, FHLMW08, JCK⁺18, LU08, MU10, PS20]. **automated** [Kob07, Kob12]. **auxiliary** [Kus18]. **avalanche** [LC07]. **average** [AL07].

Balanced [Rei21, CLS09]. **barrier** [MPST16]. **Based** [PGS20, TSJL20, ACP10, BCM11, BGGJ20, CDK18, CG20, GKL15, Gau07, HS08, Jia14, 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]. **blind** [FS11]. **blinding** [DSG21]. **BLISS** [TW20]. **block** [DR07, SS17, Sch08, ZLA21]. **Boolean** [BC12, CJST16, CLS09, CC15, CLS16, ZLA21, ZHM⁺22]. **Bound** [DM20, Kus18]. **bounds** [BDJ14, SS17, YYTK20]. **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, Sch08]. **ciphertexts** [AL11]. **circuit** [BBP⁺20]. **circulant** [AN20]. **class** [AR15, CGK13]. **Classes** [AÖY15, AJZT19, WL13]. **classical** [BBP⁺20]. **cloud** [PSU13]. **CM** [JLLRL20]. **codes** [BBB⁺18, FHLMW08, JCK⁺18, LdV19, PS20, Per12, SPB22]. **coding** [FL08, PSU13]. **coefficient** [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** [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, 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]. **criterion** [LC07]. **critical** [Bla09]. **CRT** [CCH⁺20]. **CRT-variant** [CCH⁺20]. **Cryptanalysing** [Bla09, Mul11, Bla10]. **Cryptanalysis** [BCM09, BCM11, BKL22, CBW07, 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, 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]. **Curves** [BGK⁺20, BG16, Bis11, Box12, BDFM21, CDS20, DN08, DEF14, FSV09, GPRS09, GZ13, GZ14, HST10, HWCD11, Hit09, LS07, MW12, Mor08, Oka12, 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]. **Dembowski** [AÖY15]. **density** [FS09]. **Dependent** [FGG⁺20]. **descent** [KMPS10]. **design** [GPR17]. **Designing** [BBPS20]. **detailed** [Wun19]. **Devastating** [TW20]. **differential** [DT17]. **differential-zero** [DT17]. **differentials** [DR07]. **Diffie** [KM08, Kus18, Par18]. **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]. **Efficient** [BBPS20, DEF14, HST10, DGG⁺15, FM13, SSS11, SW07b, WS09]. **Efficiently** [BCIV20, Bla09]. **elementary** [Kar20a, Kar20b, ZLA21]. **elements** [Yoo15]. **Eleventh** [JLNN20]. **ElGamal** [PGS20]. **Elliptic** [BGK⁺20, HKP⁺20, KT20, Bis11, Box12, CJS14, CQS11, DJP14, DEF14, FSV09, FK18, HST10, HWCD11, LS07, MW12, Mor08, Oka12, Sch17, Sha14, Yoo15]. **EMAC** [JN16]. **embedding** [Hit09]. **encapsulation** [BBB⁺18]. **encodings** [NP19]. **Encryption** [BLLN21, BCIV20, BGGJ20, DS20, ASB⁺18, AL07, AL11, CN22, CEM15, KNP13, NP16, SPSS12, TL15, YYS⁺14]. **endomorphism** [Bis11]. **Enhancing** [SPS19]. **EPIR** [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]. **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, MSP12, OS14, SW15, SW07a, ZSN20, ZLA21, ZHM⁺22]. **fundamental** [ASB⁺18].

general [Eke21, PSU13]. **generalised** [Dow15, MN07]. **Generalization** [DS18, Par18]. **generalized** [KHK10]. **generate** [SW15]. **Generating** [FK18, vzGS13]. **generation** [ABD⁺13, BGMP08, Pop17, vzGS09]. **generator** [BS19]. **Generic** [LdV19]. **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, Bla09, CBW07, CW22, HWCD11, 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** [SS09]. **hidden-order** [SS09]. **higher** [CS21]. **Hints** [Sic20]. **HMAC** [KM13]. **HMQV** [Men07]. **Homomorphic** [BCIV20, BGGJ20, DS20, CBW07, TL15, YYS+14]. **hull** [Mur12]. **Hybrid** [BFP09, 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, GÓs07]. **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]. **insider** [BBP19]. **instantiations** [LdV19]. **Integer** [PR20, HM07]. **integers** [BK09]. **Interactive** [BGK+20, CEM15]. **interplay** [ATW08]. **intersecting** [SPS19]. **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, 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]. **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, BBGS19]. **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, 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]. **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]. **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]. **MR3101014** [GZ14]. **MRHS** [RZ18, Zaj13]. **Multi** [PSU18, FHLMW08, Hin08]. **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]. **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]. **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, GÓs07, Oka12, Sha14, Sho10, Yoo15]. **pairing-based** [CDK18]. **pairing-friendly** [Box12, FK18, Oka12, Sha14, Yoo15].

pairings [DEF14, GZ13, GZ14]. **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]. **PMAC** [NM08]. **Points** [KT20, BG16, LS07]. **poker** [jWW12]. **Pollard** [BDJ14]. **Poly** [SSS11]. **Poly-dragon** [SSS11]. **Pólya** [CLS16]. **polycyclic** [GKL15, KU15]. **polycyclic-group-based** [KU15]. **Polylogarithm** [Mie08]. **polymatroids** [MFP10]. **Polynomial** [KMNN19, CWZ12, DSS20, JLLRL20, WL13, ZSN20]. **Polynomials** [HKP⁺20, AÖY15, KW19, TJB13]. **PoRs** [LdV19]. **possessing** [SU14]. **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** [ZSN20]. **prime** [CDK18, Hin08, TKF⁺20]. **primes** [ACP10, FS09, vzGS13]. **primitive** [SS09, Yoo15]. **primitives** [BFJN20, CDN18]. **Principal** [LPS20]. **Privacy** [ZSN20]. **Privacy-preserving** [ZSN20]. **private** [DGG⁺15, HL10, KMU20, SW07a]. **Probability** [DR07]. **Problem** [CCH⁺20, HKP⁺20, LPS20, BT12, BBGS19, Bla09, Bla10, HSWZ20, Kus18, NV08]. **problems** [BCSV20, HS08, KM08, TKF⁺20]. **Proceedings** [CLS20, CLY20]. **processes** [SW07a]. **Processing** [BCIV20]. **Product** [DKKS20, MP20, OS14]. **products** [AL11]. **proof** [Kar20a, Kar20b, NP19, PSU13, PSU18]. **proof-of-retrievability** [PSU13]. **properties** [CJST16, ZMD20]. **Protecting** [Joy20]. **protocol** [CWZ12, KU18, KMU20, LU08, MU10, SW07b, jWW12, WS09]. **protocols** [AK17, BCM11, SW07a]. **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, DJP14, JLLRL20]. **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, Pop17]. **randomized** [Böc09]. **range** [YYS⁺14]. **rational** [MW12]. **ratios** [HL19]. **RC4** [BGMP08, DS18]. **realization** [SvT10]. **realizing** [PS15]. **receiver** [FHLMW08]. **reconstruction** [SW07a]. **Recovering** [FGG⁺20]. **recovery** [BFJT12]. **Recursive** [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]. **reset** [WS09]. **Residue**

[JLNN20, CS21]. **residues** [Jus14, Jus15]. **resilient** [Ala17, CAR20, HS15b, KNP13]. **resistance** [MSP12]. **resistant** [DJP14]. **restricted** [BBS19]. **results** [DS18, SW07a]. **Rethinking** [ATW08]. **Retraction** [Kar20b]. **retrievability** [PSU13, PSU18]. **retrieval** [SW07a]. **Revisited** [Joy20, AN20, Laa20, NP16, SS16b]. **Revisiting** [JN16]. **rho** [BDJ14]. **Richelot** [CDS20]. **Rigorous** [SS17]. **Ring** [DSGKS20b, Joy20, BT12, 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** [BBS19]. **SAP** [GGD20]. **scheme** [HVV14, HSWZ20, Maz12, Mul11, PS08, SSA17, SPS19, TL15]. **Schemes** [BLLN21, BGGJ20, DKKS20, BBP19, BS19, GD13, HS15a, JSN13, LS18, MFP10, MU14, PSU13, PS15, PS20, Pou16, SS16b]. **Schmidt** [YYS⁺17]. **Schnorr** [NSW09]. **search** [MA17, RZ18]. **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, GÓ07, Hin08, MPST16, NM08, Nan09, NP16, SPSS12, DSGKS20a]. **Self** [GZ13, Yas20, GZ14]. **Self-dual** [Yas20]. **Self-pairings** [GZ13, GZ14]. **Semaev** [YYTK20]. **semigroups** [CI14]. **Sensitivities** [ZLA21]. **sensor** [HS15b, PS08]. **sequences** [AMW07, BW09, LS07]. **server** [SW07a]. **set** [Gal12, MU10]. **setting** [CDK18]. **seven** [DS17]. **sharing** [Csi20, DC14, GD13, HS15a, HL19, JSN13, MFP10]. **shifted** [LU08]. **Short** [LPS20, BS19, YYS⁺17, Yas20]. **shortest** [NV08]. **Sibert** [MU10]. **side** [Sch08]. **Sidelnikov** [BW09]. **SIDH** [UJ20]. **SIDH-based** [UJ20]. **Sieve** [NV08, Grz20]. **Sieving** [MR20]. **Sign** [TW20]. **Signature** [DKKS20, HSWZ20, NP16, SS16b]. **signatures** [BdW12, FS11, HS08, NP19, NSW09, Rei17, SvT13, vT18]. **Signcryption** [BBP19, 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, 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, Tis11]. **streams** [DGG⁺15]. **Strict** [LC07]. **Strongly** [SvT13, AR15, vT18]. **structure** [DS17, JN16, JSN13]. **structures** [GD13]. **subexponential** [ADPS14, CJS14, JLLRL20]. **subexponential-time** [JLLRL20]. **subfield** [HST10, HKP⁺20]. **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]. **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, 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, SW07b]. **two-flow** [SW07b]. **Two-permutation-based** [LMPW15]. **two-round** [Mie08]. **TWOOA** [FHLMW08]. **Type** [TNS20, AJZT19, EOS07, Jus14, Jus15].

uadratic [WP11]. **ultivariate** [WP11]. **unbounded** [DGG⁺15]. **uncloning** [KMU20]. **Unconditionally** [JSN13, SS16b, PSU13, SW07a]. **Unconditionally-secure** [JSN13]. **universal** [ACP10, Ano20]. **upper** [SS17]. **use** [BP20]. **Using** [FJ13, Rei21, BBB⁺18, BF09, 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, YYS⁺17, Yas20]. **verifiable** [ZSN20]. **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].

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).

- [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). **Asghar:2014:SCG**
- [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). **Antal:2017:MCP**
- [AJZT19] Abdelmalek Azizi, Idriss Jerri, 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>. **Azizi:2019:CIC**
- [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). **Asghar:2017:WIP**
- [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). **Aravamuthan:2007:ATO**
- [AL11] Nuttapong Attrapadung and Benoît 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). **Attrapadung:2011:FEP**
- [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). **Alawatugoda:2017:LRK**
- [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] **Araujo:2020:CHR**
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:2013:M**
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:2017:F**
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:2018:Fa**
Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(1):i–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (elec-
- [Ano18b] **Anonymous:2018:Fb**
Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 12(2):i–iv, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2018-frontmatter1/jmc-2018-frontmatter1.xml>.
- [Ano18c] **Anonymous:2018:Fc**
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:2018:F**
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:2019:Fa**
Anonymous. Frontmatter. *Journal of Mathematical Cryptology*, 13(1):i–??, March 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (elec-

- 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>. [APS15]
- [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>. [AR15]
- [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>. [ASB+18]
- [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).
- [Albrecht:2015:CHL] 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).
- [Accardi:2015:CSA] 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).
- [AlMahri:2018:FFA] 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>.

- [ATW08] **Avanzi:2008:RLG**
 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). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0040/jmc-2017-0040.xml>.
- [BBB⁺18] **Banegas:2018:DKE**
 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 Belo Klamti, 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>.
- [BBGS19] **Bindel:2019:EHL**
 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). URL <https://www.degruyter.com/view/j/jmc.2019.13.issue-1/jmc-2017-0040/jmc-2017-0040.xml>.
- [BBP19] **Bansal:2019:SSI**
 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>.
- [BBP⁺20] **Biasse:2020:TBC**
 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>.
- [BBPS20] **Banegas:2020:DED**
 Gustavo Banegas, Paulo S. L. M. Barreto, Edoardo Persichetti, and Paolo Santini. Designing efficient dyadic operations for cryptographic applications. *Journal of Mathe-*

- 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>. [BCM11]
- 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, Iliia 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 MST_3 public key cryptosystem. *Journal of Mathematical Cryptology*, 3(4): 321–338, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2015-0054/html>.
- 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, Thinkh 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).

Bettale:2009:HAS

[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).

Bianco:2016:CTZ

[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).

Boura:2020:CCR

[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] **Boneh:2020:MNI** 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] **Basu:2008:CCE** 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] **Bisson:2011:CER** 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] **Blake:2009:ORS** Ian F. Blake and Vladimir Kolesnikov. One-round secure comparison of integers. *Journal of Mathematical Cryptology*, 3(1):37–68, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BKL22] **Brown:2022:CM** 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].
- [Bla09] **Blackburn:2009:CCG** 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).
- [Bla10] **Blackburn:2010:DLP** 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).
- [BLLN21] **Bhattacharjee:2021:OVF** 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>. [BP22]
- 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>. [BS19]
- 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>. **Basso:2022:SGA**
- 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>. **Blake:2007:SDC**
- [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). **Biasse:2019:QAA**
- 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 $\mathbb{Q}(\zeta_{2s})$. *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>. **Banin:2012:DLP**
- [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>. ■
- [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).
- [CC15] Thomas W. Cusick and Youn-hwan 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).
- [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>.
- [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).
- [CDK18] Sanjit Chatterjee, M. Prem Laxman Das, and R. Kabaleeshwaran. Converting pairing-

Cusick:2015:TRS**Cheon:2020:ACV****Brandstatter:2009:ELC****Chakraborty:2020:NAP****Choi:2007:CHP****Carlet:2014:LSO****Chatterjee:2018:CPB**

- 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>. [CG20]
- [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 Mathematical 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). [Coron:2020:ICA]
- Jean-Sébastien Coron and Ag-nese Gini. Improved cryptanaly-sis of the AJPS Mersenne based cryptosystem. *Journal of Mathe-matical 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>. [Chen:2013:SCM]
- Yanling Chen, Danilo Glig-eroski, 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]
- [CJS14] 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).
- [CJST16] Claude Carlet, David Joyner, Pantelimon Stănică, and Deng Tang. Cryptographic properties of monotone Boolean functions. *Journal of Mathematical Cryptology*, 10(1):1–14, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc-2016.10.issue-1/jmc-2014-0030/jmc-2014-0030.xml>.
- [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>.
- [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).
- [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).
- [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).
- [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>.
- [CLY20] Jung Hee Cheon, Kristin Lauter, and Dongeon Yhee. Preface to the First Annual MathCrypt Proceedings volume. *Journal of Mathe-*

- 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>. [Csi20]
- 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>. [CW22]
- 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). [CWZ12]
- 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>. [DC14]
- Csirmaz:2020:SSD**
- 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**
- 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**
- 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**
- 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).

- [DEF14] **Duquesne:2014:ECP** 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).
- [DGG⁺15] **Dolev:2015:TEP** 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).
- [DHS20] **DeMicheli:2020:CON** 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>.
- [DJP14] **DeFeo:2014:TQR** 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).
- [DKKS20] **DiCrescenzo:2020:DPG** 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>.
- [DM20] **Delaplace:2020:CWB** 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>.
- [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] **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>.
- [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] **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>.
- [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).
- [DS18] **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>.
- [DSGKS20a] **Dachman-Soled:2020:SRL** 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>.

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>. [Eke21]

Dehkordi:2017:MDZ

- [DT17] 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>. [FGG+20]

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).

Ekerää:2021:QAC

Martin Ekerää. 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>.

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).

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>. [FM13]
- Fuji-Hara:2008:TCM**
- [FHLMW08] 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).
- Field:2013:UCT**
- [FJ13] 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).
- Fotiadis:2018:GPF**
- [FK18] 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).
- Fancsali:2008:SAF**
- [FL08] 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).
- Flori:2013:ECF**
- 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).
- Fischer:2009:SRF**
- [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).
- Frougny:2008:MWE**
- [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).
- Friedlander:2009:DSS**
- [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).
- Fischlin:2011:SBS**
- [FS11] Marc Fischlin and Dominique Schröder. Security of blind sig-

- natures 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).
- [FSV09] 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).
- [Gal12] 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).
- [Gau07] 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).
- [GD13] Motahhareh 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>.
- [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).
- [GÓ07] Steven D. Galbraith, Colm Ó hÉigartaigh, 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).
- [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).

- [GP13] **Grosek:2013:CS**
 Otokar Grošek and Štefan Porubský. Coprime solutions to $ax \equiv b \pmod{n}$. *Journal of Mathematical Cryptology*, 7(3): 217–224, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Gut09] **Gutierrez:2009:FSW**
 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.
- [GPR17] **Gupta:2017:ADT**
 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>.
- [GZ13] **Galbraith:2013:SPH**
 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].
- [GPRS09] **Galbraith:2009:DMS**
 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).
- [GZ14] **Galbraith:2014:ESP**
 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].
- [Grz20] **Grzeskowiak:2020:VLS**
 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
- [HF07] **Harayama:2007:WSB**
 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 ???? (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2019-0022/html>.

- ISSN 1862-2976 (print), 1862-2984 (electronic). **Hinek:2010:CMA**
- [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). **Hinek:2008:SMP**
- [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). **Hitt:2009:FGC**
- [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>. **Huang:2020:QSP**
- [HL09] M. Jason Hinek and Charles C. Y. Lam. Another look at some fast modular arithmetic methods. *Journal of Mathematical Cryptology*, 3(2):165–174, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Hinek:2009:ALS**
- [HL10] M. Jason Hinek and Charles C. Y. Lam. Common modulus attacks on small private exponent RSA and some fast variants (in practice). *Journal of Mathematical Cryptology*, 4(1):57–93, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Hinek:2010:CMA**
- [HL19] Károly Harsányi and Péter Ligeti. Exact information ratios for secret sharing on small graphs with girth at least 5. *Journal of Mathematical Cryptology*, 13(2):107–??, June 2019. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0024/jmc-2018-0024.xml>. **Harsanyi:2019:EIR**
- [HM07] 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). **Heuberger:2007:MWC**
- [HS08] 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).
- [HS15a] **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).
- [HS15b] **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).
- [HST10] **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).
- [HSWZ20] **Hoffstein:2020:SSF** 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] **Haridas:2014:SAM** 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] **Hisil:2011:EAG** 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] **Jirakitpuwapat:2018:NMC** 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] **Jiang:2014:PAP**
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] **Jao:2020:STP**
David Jao, Jason LeGrow, Christopher Leonardi, and Luis 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>.
- [JLNN20] **Joye:2020:EPR**
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>.
- [JN16] **Jha:2016:RSG**
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).
- [Joy20] **Joye:2020:PEA**
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>.
- [JP20] **Joux:2020:PNT**
Antoine Joux and Jacek Pomykala. 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>.
- [JSN13] **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).
- [Jus14] **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).
- [Jus15] 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).
- [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).
- [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).
- [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].
- [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].
- [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).
- [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).
- [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). [KNP13]
- Kaji:2019:PEP**
- [KMNN19] Shizuo Kaji, Toshiaki Maeno,
 Koji Nuida, and Yasuhide Nu-
 mata. Polynomial expressions of
 p -ary auction functions. *Jour-
 nal of Mathematical Cryptol-
 ogy*, 13(2):69–??, 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-
 0016/jmc-2018-0016.xml](http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0016/jmc-2018-0016.xml).
- Karabina:2010:AEW**
- [KMPS10] Koray Karabina, Alfred Menezes,
 Carl Pomerance, and Igor E. Sh-
 parlinski. On the asymptotic ef-
 fectiveness of Weil descent at-
 tacks. *Journal of Mathematical
 Cryptology*, 4(2):175–191, 2010.
 CODEN ???? ISSN 1862-2976
 (print), 1862-2984 (electronic). [KT20]
- Kotov:2020:AKP**
- [KMU20] Matvei Kotov, Anton Menshov,
 and Alexander Ushakov. At-
 tack on kayawood protocol: un-
 cloaking private keys. *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](https://www.degruyter.com/document/doi/10.1515/jmc-2019-0015/html). [KU15]
- Kurosawa:2013:NLR**
- 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).
- Koblitz:2007:ALA**
- [Kob07] Neal Koblitz. Another look
 at automated theorem-proving.
*Journal of Mathematical Cryptol-
 ogy*, 1(4):385–403, 2007. CO-
 DEN ???? ISSN 1862-2976
 (print), 1862-2984 (electronic).
- Koblitz:2012:ALA**
- [Kob12] Neal Koblitz. Another look
 at automated theorem-proving
 II. *Journal of Mathemati-
 cal Cryptology*, 5(3–4):205–224,
 2012. CODEN ???? ISSN 1862-
 2976 (print), 1862-2984 (elec-
 tronic).
- Kim:2020:EAC**
- Taechan Kim and Mehdi Ti-
 bouchi. Equidistribution among
 cosets of elliptic curve points
 in intervals. *Journal of Math-
 ematical 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](https://www.degruyter.com/document/doi/10.1515/jmc-2019-0020/html).
- Kotov:2015:ACP**
- Matvei Kotov and Alexan-
 der 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**
- [KU18] 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>. [LC07]
- Kushwaha:2018:ILB**
- [Kus18] 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]
- Kousidis:2019:FFD**
- [KW19] 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>. [LL15]
- Laarhoven:2020:AVC**
- Thijs Laarhoven. Approximate Voronoi cells for lattices, revisited. *Journal of Mathematical Cryptology*, 15(1):60–71, November 17, 2020. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/document/doi/10.1515/jmc-2020-0074/html>.
- 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).
- 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). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-2/jmc-2018-0018/jmc-2018-0018.xml>.
- Laine:2015:TMT**
- 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).

- Luykx:2015:TPB**
- [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).
- Lamberger:2009:NSC**
- [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).
- Lu:2017:CRV**
- [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-2/jmc-2016-0025/jmc-2016-0025.xml>.
- Lesavourey:2020:SPI**
- [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>.
- Lange:2007:DSS**
- [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).
- Laing:2018:SRR**
- [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>.
- Longrigg:2008:CSC**
- [LU08] Jonathan Longrigg and Alexander Ushakov. Cryptanalysis of the shifted conjugacy authentication protocol. *Journal of Mathematical Cryptology*, 2(2):109–116, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Mohammed:2017:RNF**
- [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] **Magliveras:2013:F** 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] **Maze:2012:AKD** 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] **Menezes:2007:ALH** Alfred Menezes. Another look at HMQV. *Journal of Mathematical Cryptology*, 1(1):47–64, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [MFP10] **Marti-Farre:2010:SSS** 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] **Mie:2008:PTR** 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] **Martin:2007:CGC** 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).
- [Mor08] **Morales:2008:ADE** 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] **Murphy:2008:GVC** 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] **Murphy:2020:DPD** 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] **Moody:2016:ISF** 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] 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] 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] 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).
- [MU10] 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] 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] 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] 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). URL <http://www.degruyter.com/view/j/jmc.2019.13.issue-3-4/jmc-2017-0007/jmc-2017-0007.xml>.
- [NSW09] **Neven:2009:HFR**
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] **Nguyen:2008:SAS**
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).
- [Oka12] **Okano:2012:VCF**
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>.
- [OPSB13] **Orumiehchiha:2013:SAL**
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).
- [OS14] 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).
- [Par18] 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>.
- [Per12] 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>.
- [PGS20] 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] **Pomykala:2020:IFC**
 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] **Paterson:2008:TAS**
 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] **Paterson:2015:OCI**
 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] **Paterson:2020:EAC**
 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/document/doi/10.1515/jmc-2019-0048/html>.
- [PSU13] **Paterson:2013:CTF**
 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] **Paterson:2018:MPP**
 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] **Reichl:2017:TLS**
 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] **Reid:2021:UIE**
 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] **Rudy:2020:RTK**
 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>.
- [RS22] **Rahman:2022:MMA**
 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).
- [RZ18] **Raddum:2018:MSB**
 Håvard Raddum and Pavol Zafac. 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>.
- [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).
- [Sch17] **Scholl:2017:IEC**
 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).
- [Sha14] **Sha:2014:NIC**
 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>.

Silverman:2007:OPS

[Sil07] Robert D. Silverman. Optimal parameterization of SNFS. *Journal of Mathematical Cryptology*, 1(2):105–124, 2007. CODEN ????

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

Santini:2022:RFC

[SPB22] 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>.

Sipasseuth:2019:EGG

[SPS19] 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>.

Sepahi:2012:NSN

[SPSS12] 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).

Saxena:2009:CPB

[SS09] 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

[SS16a] 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).
- [SS16b] 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).
- [SS17] 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] Vishal Saraswat, Rajeev Anand Sahu, and Amit K. Awasthi. A secure anonymous proxy signature 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] 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).
- [SU14] 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] 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] 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] D. R. Stinson and R. Wei. Some results on query processes and reconstruction functions for unconditionally secure 2-server 1-round binary private informa-

- tion 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).
- [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).
- [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).
- [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>.
- [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).
- [TNS20] **Tomkins:2020:NZT** Hayley Tomkins, Monica Nevins, and Hadi Salmasian. New Zémor–Tillich type hash functions over $GL_2(\mathbf{F}_{p^n})$. *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>.

- [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>.
- [TW20] **Tibouchi:2020:OBA**
 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>.
- [UJ20] **Urbanik:2020:NTS**
 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>.
- [vT18] **vanTrung:2018:CSA**
 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).
- [vzGS13] **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).
- [WC07] **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).
- [WL13] **Wang:2013:MCN**
 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).

Wolf:2011:EKU

- [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).

Wu:2009:EIP

- [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).

Wunderer:2019:DAH

- [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>.

Yasuda:2020:SDD

- [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>.

Yoon:2015:NMC

- [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).

Yasuda:2014:EDR

- [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:2017:ADS

- [YYS+17] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, and Takeshi Koshihara. 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).

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

- [ZLA21] 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>.