

# 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](mailto:beebe@math.utah.edu), [beebe@acm.org](mailto:beebe@acm.org),  
[beebe@computer.org](mailto:beebe@computer.org) (Internet)  
WWW URL: <http://www.math.utah.edu/~beebe/>

25 March 2019  
Version 1.04

## Title word cross-reference 7 [GZ14].

$(p^r - 1)/3$  [BW09]. 1 [SW07a]. 2  
[Gau07, Hit09, SW07a]. 3  
[CC15, LL15, MW12]. 4 [Kar10]. 6 [Kar10].  
 $ax \equiv b \pmod{n}$  [GP13].  $k$   
[AMW07, BW09].  $\mathbf{F}_{24m}^*$  [Kar10].  $\mathbf{F}_{36m}^*$   
[Kar10].  $\mathbf{F}_p$  [BW09].  $\mathbf{F}_{pk}$  [Duq11].  $\mathcal{M}$   
[WP11].  $\mathcal{Q}$  [WP11].  $\text{MST}_3$  [BCM09].  
 $N = p^r q^l$  [LPS17].  $p + q$  [MA17].  $\rho$  [Oka12].  
 $\text{MST}_3$  [SvT10].

**-error** [AMW07, BW09]. **-rotation** [CC15].  
**-round** [SW07a]. **-server** [SW07a]. **-torsion**  
[MW12]. **-values** [Oka12].

**256** [DT17].

**abelian** [Rei17]. **aborts** [FS11]. **Abu**  
[Bla10]. **access** [DS17, GD13, JSN13].  
**achieving** [AL11]. **adaptive** [AL11, FS11].  
**add** [FJ13]. **add-rotate-xor** [FJ13].  
**addition** [FJ13]. **additive** [BDJ14]. **admit**  
[DN08]. **Advanced** [Sch08]. **adversary**  
[Dow15]. **AE** [ASB<sup>+</sup>18]. **Affine**  
[CLS16, HWCD11]. **against**  
[MSP12, WS09]. **aggregation** [HS15b].  
**Agrawal** [PS08]. **agreement** [Mul11]. **al.**  
[MU10]. **algebra** [KU18, RZ18]. **Algebraic**  
[BF09, Par18]. **algorithm**  
[BGMP08, BDJ14, Pop17]. **algorithms**  
[AR15, FJ13, NV08]. **alternating** [SW15].  
**Analysis** [KU15, KU18, Maz12, YYS<sup>+</sup>17,  
CDK18, HVV14, MU08, NM08, Nan09,

OPSB13, PSU13, Sch08]. **analyze** [FJ13]. **anonymous** [SSA17]. **Aperiodic** [BdW12, SvT13, vT18]. **application** [Duq11, Tis11]. **Applications** [GPR17, FL08, FS11, JN16]. **approach** [BFP09, CLS16]. **approaches** [HS15b]. **approximations** [SS16a]. **argument** [Mie08]. **Ariffin** [Bla10]. **arithmetic** [ATW08, Duq11, Gau07, HST10, HL09]. **arrays** [MN07]. **asymmetric** [AR15, Jia14]. **asymptotic** [KMPS10]. **attack** [AK17, BF09, HF07, Mor08, MU10, Sch17]. **attacks** [GKL15, HL10, KMPS10, KHK10, MSP12, MU08, PS08, Pou16, WS09]. **attribute** [AL11]. **authenticated** [ASB<sup>+</sup>18]. **authentication** [ACP10, FHLMW08, JCK<sup>+</sup>18, LU08, MU10]. **automated** [Kob07, Kob12]. **auxiliary** [Kus18]. **avalanche** [LC07]. **average** [AL07].

**balanced** [CLS09]. **barrier** [MPST16]. **based** [ACP10, BCM11, CDK18, GKL15, Gau07, HS08, Jia14, KU15, KU18, LMPW15, MU08, PS15, Per12, RZ18, RST07, SS09]. **bases** [BF09, FS08]. **bent** [FM13]. **Bergman** [BT12]. **bias** [DS18]. **Biggs** [Bla09]. **binary** [ATW08, LMPW15, SW07a]. **birthday** [HF07, MPST16, MSP12]. **blind** [FS11]. **block** [DR07, SS17, Sch08]. **Boolean** [BC12, CJST16, CLS09, CC15, CLS16]. **bound** [Kus18]. **bounds** [BDJ14, SS17]. **breaking** [MPST16]. **Brezing** [Yoo15]. **Bringer** [CWZ12]. **broadcast** [AL07].

**calculus** [LL15]. **carry** [FJ13]. **carry-truncated** [FJ13]. **Cartesian** [JCK<sup>+</sup>18]. **case** [AK17, RST07]. **CAST** [DT17]. **CAST-256** [DT17]. **CBC** [JN16]. **CCA** [KNP13]. **CCA-secure** [KNP13]. **certain** [KU15]. **Chabanne** [CWZ12]. **challenges** [AK17]. **Challenging** [MSP12]. **channel** [Sch08]. **characterisation** [HS15a]. **characteristic** [HST10]. **characterization** [BGMP08, FM13]. **Cheng** [PS08]. **choosing** [Yoo15]. **cipher** [SS17, Tis11]. **ciphers** [DR07, FMS09, Sch08]. **ciphertexts** [AL11]. **class** [AR15, CGK13]. **Classes** [AÖY15, WL13]. **cloud** [PSU13]. **codes** [FHLMW08, JCK<sup>+</sup>18, Per12]. **coding** [FL08, PSU13]. **colexicographically** [HM07]. **Collision** [BDJ14]. **collisions** [BS07]. **coloring** [ADPS14]. **combinatorics** [MN07]. **Common** [HL10]. **communication** [PS15]. **commutative** [JCK<sup>+</sup>18]. **Compact** [CQS11, Per12]. **comparative** [CDK18]. **comparison** [BK09]. **complete** [BGMP08, Oka12]. **complexities** [SS17]. **complexity** [AMW07, BW09, DS17]. **composite** [CDK18]. **Compression** [BG16, Kar10]. **computation** [ADPS14, CI14, DGG<sup>+</sup>15, Duq11, DEF14, GÓ07]. **Computing** [Bis11]. **concrete** [APS15]. **concurrent** [WS09]. **concurrent-reset** [WS09]. **conjecture** [CLS09]. **conjugacy** [LU08]. **conjugation** [MU14]. **connected** [DS17]. **connection** [Zaj13]. **constant** [AL11]. **constant-size** [AL11]. **Constructing** [CJS14]. **Construction** [vT18, AGH17, ADPS14, CL09, FHLMW08, JCK<sup>+</sup>18]. **constructions** [GPR17, PS15, WC07]. **Converting** [CDK18]. **convolution** [OS14]. **Coprime** [GP13]. **correlation** [DR07, DT17]. **corresponding** [BFJT12]. **Coskun** [AK17]. **Counting** [DN08, WL13]. **criterion** [LC07]. **critical** [Bla09]. **Cryptanalysing** [Bla09, Mul11, Bla10]. **Cryptanalysis** [BCM09, BCM11, CBW07, LU08, LPS17, MU14, TL15, DT17, LNR09, MU10, RST07, SS16a, SS17, SvT10, Tis11]. **Cryptographic** [CJST16, MP08, SS09]. **cryptography** [GPR17]. **Cryptol.** [GZ14]. **Cryptology** [Gut09]. **cryptosystem** [BCM09, Bla10, CBW07, HF07, Jus14, Jus15, KU15, SSS11, SvT10]. **cryptosystems** [AÖY15, CDK18, DJP14, EOS07]. **cubic**

- [CC15]. **cumulative** [MN07]. **curve** [CJS14, CQS11, DJP14, FK18]. **curves** [BG16, Bis11, Box12, DN08, DEF14, FSV09, GPRS09, GZ13, GZ14, HST10, HWCD11, Hit09, LS07, MW12, Mor08, Oka12, Sch17, Sha14, Yoo15]. **cyclotomic** [AMW07, Kar10, Sha14].
- data** [SS17, SU14]. **decentralized** [Pop17]. **decreasing** [YYS<sup>+</sup>17]. **decryption** [YYS<sup>+</sup>14]. **degree** [Hit09]. **Dembowski** [AÖY15]. **density** [FS09]. **descent** [KMPS10]. **design** [GPR17]. **differential** [DT17]. **differential-zero** [DT17]. **differentials** [DR07]. **Diffie** [KM08, Kus18, Par18]. **discrete** [BT12, Bla09, Bla10, BDJ14, CI14, Gal12, KM08, Sho10]. **disguised** [Mor08]. **distinguisher** [Gal12]. **Distortion** [GPRS09]. **distributed** [DGG<sup>+</sup>15]. **Distribution** [LS07, BS07, Jus14, Jus15, Maz12, PS08, vzGS09]. **distributions** [DR07]. **dragon** [SSS11]. **DSA** [Pou16]. **dyadic** [Per12].
- Edwards** [BG16]. **effect** [Mur12]. **effectiveness** [KMPS10, Mur12]. **Efficient** [DEF14, HST10, DGG<sup>+</sup>15, FM13, SSS11, SW07b, WS09]. **efficiently** [Bla09]. **elements** [Yoo15]. **elliptic** [Bis11, Box12, CJS14, CQS11, DJP14, DEF14, FSV09, FK18, HST10, HWCD11, LS07, MW12, Mor08, Oka12, Sch17, Sha14, Yoo15]. **EMAC** [JN16]. **embedding** [Hit09]. **encryption** [ASB<sup>+</sup>18, AL07, AL11, CEM15, KNP13, NP16, SPSS12, TL15, YYS<sup>+</sup>14]. **endomorphism** [Bis11]. **EPIR** [CWZ12]. **equation** [MP08, Zaj13]. **equations** [GP09]. **equivalence** [CLS16, WL13]. **Equivalent** [WP11]. **Erratum** [GZ14]. **error** [AMW07, BW09]. **errors** [APS15]. **establishment** [BCM11]. **evaluation** [CDGM14, CWZ12, TJB13]. **evolution** [BGMP08]. **exact** [YYS<sup>+</sup>14]. **examples** [DC14]. **exchange** [Ala17, Jia14, KU18, Par18]. **exhaustive** [RZ18]. **existence** [WC07]. **expansions** [FS08]. **explicit** [ATW08]. **exploration** [HWCD11]. **exponent** [HL10]. **exponents** [Böc09]. **extracting** [SU14].
- Factor** [Kar10]. **Factor-** [Kar10]. **factorization** [Zaj13]. **Families** [Hit09, MW12, CL09, FK18, Oka12, Sha14, WC07, Yoo15]. **family** [ACP10, BFJT12, FM13]. **Fast** [Gau07, OS14, Duq11, HL09, HL10, MPST16, jWW12, vzGS09]. **FCSRs** [FMS09]. **field** [ATW08, Kus18]. **fields** [ATW08, BFP09, GP09, HST10, LC07]. **filtered** [OPSB13]. **Finding** [Gal12]. **finite** [BFP09, CBW07, FL08, HST10, JCK<sup>+</sup>18, Kus18, LC07, Sho10]. **flaw** [ASB<sup>+</sup>18]. **flow** [SW07b]. **Foreword** [Gut09, Mag13]. **forms** [HS08]. **formulæ** [ATW08]. **formulas** [MA17]. **foundation** [PSU13]. **friendly** [Box12, FK18, Oka12, Sha14, Yoo15]. **Frontmatter** [Ano17, Ano18a, Ano18b, Ano18c]. **fully** [Dow15, TL15, YYS<sup>+</sup>14]. **function** [ACP10, GP09, Nan09, NSW09, PS15]. **Functional** [AL11]. **functions** [BC12, CJST16, CLS09, CC15, CLS16, FM13, Gau07, KHK10, MSP12, OS14, SW15, SW07a]. **fundamental** [ASB<sup>+</sup>18].
- general** [PSU13]. **generalised** [Dow15, MN07]. **Generalization** [DS18, Par18]. **generalized** [KHK10]. **generate** [SW15]. **Generating** [FK18, vzGS13]. **generation** [ABD<sup>+</sup>13, BGMP08, Pop17, vzGS09]. **Gentry** [YYS<sup>+</sup>14]. **genus** [ATW08, GPRS09, Gau07, Hit09, LL15]. **geometric** [MP08]. **geometries** [JCK<sup>+</sup>18]. **geometry** [FL08]. **global** [GP09]. **Goldwasser** [Jus14, Jus15]. **Gram** [YYS<sup>+</sup>17]. **graph** [ADPS14, DS17, GD13].

**graphs** [JN16, PS15, Sho10]. **GRH** [Bis11]. **Gröbner** [BF09]. **group** [Bla09, CBW07, HWCD11, KU15, Kus18, RST07, SW15, Zaj13]. **groups** [GKL15, Rei17, SS09].

**Halevi** [YYS+14]. **hard** [HS08]. **hardness** [APS15]. **Hash** [NSW09, ACP10, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. **hash-function** [ACP10]. **hashing** [FSV09, LMPW15]. **Hellman** [KM08, Kus18, Par18]. **Herley** [AK17]. **Heuristics** [Box12]. **HFE** [BFJT12]. **hidden** [SS09]. **hidden-order** [SS09]. **HMAC** [KM13]. **HMQV** [Men07]. **homomorphic** [CBW07, TL15, YYS+14]. **hull** [Mur12]. **Hybrid** [BFP09]. **hyper** [FM13]. **hyper-bent** [FM13]. **hyperelliptic** [ATW08, DN08, GZ13, GZ14].

**ID** [PS15]. **ID-based** [PS15]. **ideal** [HS15a, JSN13]. **ideality** [Sha14]. **Identification** [HS08, AK17, SW07b, WS09]. **II** [Jus15, Kob12]. **implementation** [CDGM14, YYS+14]. **implications** [FMS09, GÓ07]. **improve** [MA17]. **Improved** [Kus18, NM08, Nan09]. **increased** [MSP12]. **indefinite** [HS08]. **index** [LL15]. **Indifferentiability** [MPST16]. **Indirect** [ABD+13]. **Infinite** [DC14]. **information** [SW07a]. **injection** [ABD+13]. **inner** [AL11]. **input** [DGG+15]. **integer** [HM07]. **integers** [BK09]. **interactive** [CEM15]. **interplay** [ATW08]. **isogenies** [CJS14, DJP14]. **Isolated** [Sch17]. **iterated** [KHK10].

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

**KASUMI** [SW15]. **key** [Ala17, BCM09, BCM11, BFJT12, CEM15, CBW07, DS18, Jia14, KU18, KNP13, Maz12, Mul11, Par18, PS08, PS15, SPSS12, SSS11, SvT10, TL15, WP11]. **key-recovery** [BFJT12]. **keys** [BFJT12, Per12, WP11]. **keystream** [DS18]. **knowledge** [SW07b]. **Koblitz** [DN08].

**lattice** [Pou16, YYS+17]. **laws** [HWCD11]. **Leakage** [CDGM14, Ala17, KNP13]. **leakage-resilient** [Ala17, KNP13]. **learning** [APS15]. **Length** [GKL15, RST07, MU08]. **Length-based** [GKL15, RST07, MU08]. **lengths** [YYS+17]. **lightweight** [GPR17]. **Linear** [HS15b, AMW07, BW09, DT17, Mur12, RZ18]. **linearly** [OPSB13]. **log** [KM08]. **logarithm** [BT12, Bla09, Bla10, Sho10]. **logarithmic** [BdW12, Rei17, SvT13, vT18]. **logarithms** [BDJ14, CI14, Gal12]. **look** [HL09, Kob07, KM08, Kob12, KM13, Men07, SS16a]. **low** [ATW08]. **lower** [Kus18].

**MAC** [ABD+13, JN16]. **maps** [GPRS09]. **masking** [Sch08]. **Masthead** [Ano13]. **Math.** [GZ14]. **Mathematical** [Gut09]. **matrices** [GPR17]. **matrix** [BCM11, KU18, MU14]. **matrix-based** [BCM11]. **matroids** [MFP10]. **McEliece** [EOS07, Per12]. **McEliece-type** [EOS07]. **MDS** [GPR17]. **Mean** [MU10]. **Mean-set** [MU10]. **memory** [LL15]. **mental** [jWW12]. **message** [ABD+13, Dow15, FHLMW08]. **method** [WL13, Yoo15, Zaj13]. **methods** [HL09, JCK+18, Sch08]. **Micali** [Jus14, Jus15]. **MICKEY** [Tis11]. **Miller** [Böc09]. **Minimal** [FS08, HM07]. **mixing** [LMPW15]. **mnemonic** [AGH17]. **mode** [ASB+18]. **model** [DN08]. **modified** [HV14]. **modular** [HL09]. **moduli** [LPS17]. **modulo** [Bla10]. **modulus** [HL10]. **monodromy** [Sho10]. **monomial** [CLS16]. **monotone** [CJST16]. **MOV** [Sch17]. **MQQs** [CGK13]. **MR3101014** [GZ14]. **MRHS** [RZ18, Zaj13]. **multi**

[FHLMW08, Hin08]. **multi-message** [FHLMW08]. **multi-prime** [Hin08]. **multi-receiver** [FHLMW08]. **multicasting** [Maz12]. **Multicollision** [KHK10]. **multilevel** [JSN13]. **multiparty** [ADPS14]. **Multiple** [DT17, FM13]. **multiplicative** [Kus18]. **multivariate** [AÖY15, BFP09, CGK13, HF07, SSS11, TJB13].

**negation** [AL11]. **network** [FL08, PS08]. **networks** [HS15b]. **NLFSRs** [OPSB13]. **non** [BT12, CEM15, Jus14, Jus15, KM08, Sha14]. **non-idealness** [Sha14]. **non-interactive** [CEM15]. **non-representable** [BT12]. **non-residues** [Jus14, Jus15]. **non-standard** [KM08]. **Nonsmooth** [Tis11]. **norm** [GP09]. **normal** [SS16a]. **notions** [SPSS12]. **NP** [HS08]. **NP-hard** [HS08]. **NTRU** [BF09]. **number** [MA17, Pop17, WL13]. **numbers** [vzGS09]. **Numerical** [LNR09].

**Oblivious** [TJB13, FS11]. **odd** [HST10]. **offs** [LL15]. **OMAC** [Nan09]. **One** [BK09, Bla10, PS15]. **One-round** [BK09]. **one-way-function** [PS15]. **opening** [CEM15]. **Optimal** [PS15, Sil07, CDGM14]. **orbit** [Gal12]. **order** [CDK18, SS09]. **Ostrom** [AÖY15]. **overhead** [AL07].

**pairing** [Box12, CDK18, Duq11, FK18, GÓ07, Oka12, Sha14, Sho10, Yoo15]. **pairing-based** [CDK18]. **pairing-friendly** [Box12, FK18, Oka12, Sha14, Yoo15]. **pairings** [DEF14, GZ13, GZ14]. **parameterization** [Sil07]. **parameters** [FK18]. **participants** [DS17, GD13]. **password** [Jia14]. **password-based** [Jia14]. **Perfect** [GD13, CL09, WC07]. **period** [BW09]. **permutation** [LMPW15]. **permutations** [AGH17]. **Persistent** [Jia14]. **pipe** [MPST16]. **Pisot** [FS08]. **PKA** [AR15]. **PMAC** [NM08]. **points** [BG16, LS07]. **poker** [jWW12]. **Pollard** [BDJ14]. **Poly** [SSS11]. **Poly-dragon** [SSS11]. **Pólya** [CLS16]. **polycyclic** [GKL15, KU15]. **polycyclic-group-based** [KU15]. **Polylogarithmic** [Mie08]. **polymatroids** [MFP10]. **polynomial** [CWZ12, WL13]. **polynomials** [AÖY15, TJB13]. **possessing** [SU14]. **power** [ACP10]. **practical** [BFJT12, NV08]. **practice** [HL10]. **predistribution** [PS15]. **presence** [Dow15, Sch08]. **prime** [CDK18, Hin08]. **primes** [ACP10, FS09, vzGS13]. **primitive** [SS09, Yoo15]. **private** [DGG<sup>+</sup>15, HL10, SW07a]. **Probability** [DR07]. **problem** [BT12, Bla09, Bla10, Kus18, NV08]. **problems** [HS08, KM08]. **processes** [SW07a]. **product** [OS14]. **products** [AL11]. **proof** [PSU13]. **proof-of-retrievability** [PSU13]. **properties** [CJST16]. **protocol** [CWZ12, KU18, LU08, MU10, SW07b, jWW12, WS09]. **protocols** [AK17, BCM11, SW07a]. **proving** [Kob07, Kob12]. **proxy** [SSA17]. **pseudo** [BGMP08, Pop17]. **pseudo-random** [Pop17]. **pseudorandom** [Nan09, vzGS09]. **Public** [SvT10, AL11, BCM09, CBW07, KNP13, SPSS12, SSS11, WP11]. **public-attribute** [AL11]. **public-key** [CBW07, SPSS12].

**quadratic** [AÖY15, CGK13, HF07, HS08, Jus14, Jus15]. **Quantum** [CI14, CJS14, DJP14]. **quantum-resistant** [DJP14]. **quartic** [DEF14]. **quasi** [Per12]. **quasi-dyadic** [Per12]. **quasigroups** [CGK13]. **query** [SW07a]. **quotient** [MU08].

**Rabin** [Böc09]. **Random** [MU08, BGMP08, Pop17]. **randomized** [Böc09]. **range** [YYS<sup>+</sup>14]. **rational** [MW12]. **RC4** [BGMP08, DS18]. **realization** [SvT10].

**realizing** [PS15]. **receiver** [FHLMW08]. **reconstruction** [SW07a]. **recovery** [BFJT12]. **Recursive** [BC12, CL09]. **reduced** [DT17]. **reduced-round** [DT17]. **refinement** [LS18]. **regular** [MSP12]. **relations** [DS18, SPSS12]. **remarks** [FMS09]. **repairable** [LS18]. **representable** [BT12]. **representations** [CQS11, HM07]. **requirements** [NSW09]. **reset** [WS09]. **residues** [Jus14, Jus15]. **resilient** [Ala17, HS15b, KNP13]. **resistance** [MSP12]. **resistant** [DJP14]. **results** [DS18, SW07a]. **Rethinking** [ATW08]. **retrievability** [PSU13]. **retrieval** [SW07a]. **revisited** [NP16, SS16b]. **Revisiting** [JN16]. **rho** [BDJ14]. **Rigorous** [SS17]. **ring** [BT12]. **rings** [Bis11, JCK<sup>+</sup>18]. **Rivest** [HVV14]. **RNS** [Duq11]. **robust** [JSN13]. **Roos** [DS18]. **rotate** [FJ13]. **rotation** [CC15, CLS16]. **round** [BK09, DT17, Mie08, SW15, SW07a]. **RSA** [Hin08, HL10, LPS17, MA17].

**safe** [AK17, vzGS13]. **same** [SU14]. **scheme** [HVV14, Maz12, Mul11, PS08, SSA17, TL15]. **schemes** [GD13, HS15a, JSN13, LS18, MFP10, MU14, PSU13, PS15, Pou16, SS16b]. **Schmidt** [YYS<sup>+</sup>17]. **Schnorr** [NSW09]. **search** [MA17, RZ18]. **Second** [Gut09]. **secret** [DC14, GD13, HS15a, JSN13, MFP10, CEM15]. **Secure** [Dow15, BK09, FL08, JSN13, KNP13, Maz12, PSU13, SSA17, SW07b, SW07a, SS16b, WS09]. **Security** [FS11, HVV14, OPSB13, ACP10, AL11, CDGM14, EOS07, GÓ07, Hin08, MPST16, NM08, Nan09, NP16, SPSS12]. **Self** [GZ13, GZ14]. **Self-pairings** [GZ13, GZ14]. **semigroups** [CI14]. **sensor** [HS15b, PS08]. **sequences** [AMW07, BW09, LS07]. **server** [SW07a]. **set** [Gal12, MU10]. **setting** [CDK18]. **seven** [DS17]. **sharing** [DC14, GD13, HS15a, JSN13, MFP10]. **shifted** [LU08]. **short** [YYS<sup>+</sup>17]. **shortest** [NV08]. **Sibert** [MU10]. **side** [Sch08].

**Sidelnikov** [BW09]. **Sieve** [NV08]. **signature** [NP16, SS16b]. **signatures** [BdW12, FS11, HS08, NSW09, Rei17, SvT13, vT18]. **signcryption** [SSA17]. **Simplified** [GÓ07]. **six** [GD13]. **size** [AL11]. **SKENO** [CEM15]. **small** [HST10, HL10, Hit09]. **SNFS** [Sil07]. **solutions** [GP13]. **solve** [Zaj13]. **solver** [RZ18]. **solvers** [LNR09]. **solving** [BFP09, Bla09, BDJ14, GP09, MP08]. **Some** [FL08, FMS09, SW07a, BC12, DS18, FS09, HL09, HL10, LS07]. **sparse** [AK17, FK18]. **special** [CGK13, FS09]. **specified** [PS15]. **squared** [YYS<sup>+</sup>17]. **squared-sum** [YYS<sup>+</sup>17]. **squeezing** [CDGM14]. **Srivastava** [Per12]. **standard** [KM08]. **Statistical** [BS07]. **Stickel** [Mul11]. **stochastic** [Sch08]. **storage** [PSU13]. **stream** [FMS09, Tis11]. **streams** [DGG<sup>+</sup>15]. **Strict** [LC07]. **Strongly** [SvT13, AR15, vT18]. **structure** [DS17, JN16, JSN13]. **structures** [GD13]. **subexponential** [ADPS14, CJS14]. **subfield** [HST10]. **subgroups** [Kar10, MU08]. **subsequences** [BW09]. **Subset** [vzGS09]. **sum** [HF07, YYS<sup>+</sup>17, vzGS09]. **summary** [EOS07]. **supersingular** [DJP14, GPRS09]. **support** [AL11]. **survey** [LS18]. **symmetric** [CLS09, CC15, CLS16, TL15]. **systems** [BFP09, Mie08, WP11, Zaj13].

**Tame** [Rei17]. **terms** [FM13]. **test** [Böc09]. **their** [EOS07]. **theorem** [CLS16, Kob07, Kob12]. **theorem-proving** [Kob07, Kob12]. **Theory** [CC15, GPR17, PSU13]. **theta** [Gau07]. **Thompson** [RST07]. **three** [BCM11]. **threshold** [JSN13, LS18]. **Time** [LL15, CJS14]. **Time-memory** [LL15]. **torsion** [MW12]. **trace** [BG16, FM13]. **trade** [LL15]. **trade-offs** [LL15]. **transfer** [FS11]. **transmission** [AL07, Dow15]. **tropical** [KU18]. **truncated** [FJ13].

**trustless** [Pop17]. **twisted** [BG16]. **Two** [LMPW15, PS08, GPRS09, Mie08, SW07b]. **two-flow** [SW07b]. **Two-permutation-based** [LMPW15]. **two-round** [Mie08]. **TWOOA** [FHLMW08]. **type** [EOS07, Jus14, Jus15].

**uadratic** [WP11]. **ultivariate** [WP11]. **unbounded** [DGG<sup>+</sup>15]. **Unconditionally** [JSN13, SS16b, PSU13, SW07a]. **Unconditionally-secure** [JSN13]. **universal** [ACP10]. **upper** [SS17]. **Using** [FJ13, BF09, FK18, Kus18].

**values** [Oka12]. **variant** [LPS17]. **variants** [HL10, Mul11]. **vector** [NV08]. **vectors** [BF09, YYS<sup>+</sup>17]. **view** [MP08]. **VSH** [BS07].

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

**xor** [FJ13].

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

## References

- [ABD<sup>+</sup>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).
- [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).
- [AGH17] Eugen Antal, Otakar 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).
- [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).

**Alomair:2010:PPS**

**Asghar:2014:SCG**

**Antal:2017:MCP**

**Asghar:2017:WIP**

**AlMashrafi:2013:IMI**

- [AL07] Sarang Aravamuthan and Sachin Lodha. The average transmission overhead for broadcast encryption. *Journal of Mathematical Cryptology*, 1(4):373–384, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AL11] Nuttapon Attrapadung and 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).
- [Ala17] Janaka Alawatugoda. On the leakage-resilient key exchange. *Journal of Mathematical Cryptology*, 11(4):215–269, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [AMW07] Hassan Aly, Wilfried Meidl, and Arne Winterhof. On the  $k$ -error linear complexity of cyclotomic sequences. *Journal of Mathematical Cryptology*, 1(3):283–296, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Ano13] Anonymou. 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.xml>.
- [Ano17] Anonymou. 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.xml>.
- [Ano18a] Anonymou. Frontmatter. *Journal of Mathematical Cryptology*, 12(1):i–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2018-frontmatter1.xml>.
- [Ano18b] Anonymou. Frontmatter. *Journal of Mathematical Cryptology*, 12(2):i–iv, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://doi.org/10.1515%2Fjmc-2018-frontmatter2>.



- [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>.
- [ASB<sup>+</sup>18] **Alam:2015:CWD** 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).
- [AÖY15] **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).
- [APS15] **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).
- [AR15] **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).
- [BC12] **Brown:2012:RWS** 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>.
- [BCM09] **Blackburn:2009:CPK** Simon R. Blackburn, Carlos Cid, and Ciaran Mullan. Crypt-

- analysis of the  $MST_3$  public key cryptosystem. *Journal of Mathematical Cryptology*, 3(4):321–338, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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).
- [BDJ14] Joppe W. Bos, Alina Dudeanu, and Dimitar Jetchev. Collision 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).
- [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).
- [BF09] Gérard 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).
- [BFJT12] Charles Bouillaguet, Pierre-Alain Fouque, Antoine Joux, and Joana Treger. A family of weak keys in HFE and the corresponding practical key-recovery. *Journal of Mathematical Cryptology*, 5(3–4):247–275, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BFP09] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BG16] Giulia Bianco and Elisa Gorla. Compression for trace zero points on twisted Edwards curves. *Journal of Mathematical Cryptology*, 10(1):15–34, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BGMP08] Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul. A complete characterization of the evolution of RC4 pseudo random generation algorithm. *Journal of Mathematical Cryptology*, 2(3):257–289, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

**Blackburn:2011:CTM**

**Bouillaguet:2012:FWK**

**Bettale:2009:HAS**

**Bos:2014:CBA**

**Bianco:2016:CTZ**

**Baumeister:2012:ALS**

**Basu:2008:CCE**

**Bourgeois:2009:AAN**

- ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Bis11] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *Journal of Mathematical Cryptology*, 5(2):101–113, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [BK09] Ian F. Blake and Vladimir Kolesnikov. One-round secure comparison of integers. *Journal of Mathematical Cryptology*, 3(1):37–68, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Bla09] Simon R. Blackburn. Cryptanalysing the critical group: efficiently solving Biggs’s discrete logarithm problem. *Journal of Mathematical Cryptology*, 3(3):199–203, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Bla10] Simon R. Blackburn. The discrete logarithm problem modulo one: cryptanalysing the Ariffin–Abu cryptosystem. *Journal of Mathematical Cryptology*, 4(2):193–198, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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).
- [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>.
- [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).
- [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>.

- Brandstatter:2009:ELC**
- [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).
- Choi:2007:CHP**
- [CBW07] Su-Jeong Choi, Simon R. Blackburn, and Peter R. Wild. Cryptanalysis of a homomorphic public-key cryptosystem over a finite group. *Journal of Mathematical Cryptology*, 1(4):351–358, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cusick:2015:TRS**
- [CC15] Thomas W. Cusick and Younhwan Cheon. Theory of 3-rotation symmetric cubic Boolean functions. *Journal of Mathematical Cryptology*, 9(1): 45–62, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Carlet:2014:LSO**
- [CDGM14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssein Maghrebi. Leakage squeezing: optimal implementation and security evaluation. *Journal of Mathematical Cryptology*, 8(3):249–295, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Chatterjee:2018:CPB**
- [CDK18] Sanjit Chatterjee, M. Prem Laxman Das, and R. Kabaleeshwaran. Converting pairing-based cryptosystems from composite to prime order setting — a comparative analysis. *Journal of Mathematical Cryptology*, 12(3):159–??, September 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-3/jmc-2017-0042/jmc-2017-0042.xml>.
- Chen:2015:SSK**
- [CEM15] Jiageng Chen, Keita Emura, and Atsuko Miyaji. SKENO: Secret key encryption with non-interactive opening. *Journal of Mathematical Cryptology*, 9(2):63–74, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Chen:2013:SCM**
- [CGK13] Yanling Chen, Danilo Gligoroski, and Svein J. Knapskog. On a special class of multivariate quadratic quasigroups (MQQs). *Journal of Mathematical Cryptology*, 7(2):111–141, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Childs:2014:QCD**
- [CI14] Andrew M. Childs and Gábor Ivanyos. Quantum computation of discrete logarithms in semigroups. *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. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Carlet:2016:CPM**
- [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>.
- Colbourn:2009:RCP**
- [CL09] Charles J. Colbourn and Alan C. H. Ling. A recursive construction for perfect hash families. *Journal of Mathematical Cryptology*, 3(4):291–306, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Cusick:2009:CBS**
- [CLS09] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică. On a conjecture for balanced symmetric Boolean functions. *Journal of Mathematical Cryptology*, 3(4):273–290, 2009. CODEN ????
- Cusick:2016:AEM**
- [CLS16] Thomas W. Cusick, K. V. Lakshmy, and M. Sethumadhavan. Affine equivalence of monomial rotation symmetric Boolean functions: a Pólya’s theorem approach. *Journal of Mathematical Cryptology*, 10(3–4):145–156, 2016. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- 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).
- Chee:2012:BCE**
- [CWZ12] Yeow Meng Chee, Huaxiong Wang, and Liang Feng Zhang. On the Bringer–Chabanne EPIR protocol for polynomial evaluation. *Journal of Mathematical Cryptology*, 5(3–4):277–301, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Dibert:2014:ISS**
- [DC14] Alexander Dibert and László Csirmaz. Infinite secret sharing — examples. *Journal of Mathematical Cryptology*, 8(2):141–168, 2014. CODEN ????

- ISSN 1862-2976 (print), 1862-2984 (electronic).
- [DEF14] Sylvain Duquesne, Nadia El Mrabet, and Emmanuel Fouotsa. Efficient computation of pairings on Jacobi quartic elliptic curves. *Journal of Mathematical Cryptology*, 8(4):331–362, 2014. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [DGG<sup>+</sup>15] Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, and Yelena Yuditsky. Towards efficient private distributed computation on unbounded input streams. *Journal of Mathematical Cryptology*, 9(2):79–94, 2015. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [DJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [DN08] 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] 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).
- [DR07] 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).
- [DS17] 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] 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>.

- [DT17] **Dehkordi:2017:MDZ**  
 Massoud Hadian Dehkordi and Roghayeh Taghizadeh. Multiple differential-zero correlation linear cryptanalysis of reduced-round CAST-256. *Journal of Mathematical Cryptology*, 11(2):55–62, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc-2017.11.issue-2/jmc-2016-0054/jmc-2016-0054.xml>.
- [Duq11] **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).
- [EOS07] **Engelbert:2007:SMT**  
 D. Engelbert, R. Overbeck, and A. Schmidt. A summary of McEliece-type cryptosystems and their security. *Journal of Mathematical Cryptology*, 1(2):151–199, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FJ13] **Field:2013:UCT**  
 Rebecca E. Field and Brant C. Jones. Using carry-truncated addition to analyze add-rotate-xor hash algorithms. *Journal of Mathematical Cryptology*, 7(2):97–110, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FK18] **Fotiadis:2018:GPF**  
 Georgios Fotiadis and Elisavet Konstantinou. Generating pairing-friendly elliptic curve parameters using sparse families. *Journal of Mathematical Cryptology*, 12(2):83–99, June 2018. ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://doi.org/10.1515%2Fjmc-2017-0024>.
- [FL08] **Fancsali:2008:SAF**  
 Sz. L. Fancsali and P. Ligeti. Some applications of finite geometry for secure network coding. *Journal of Mathematical Cryptology*, 2(3):209–225, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [FHLMW08] **Fuji-Hara:2008:TCM**  
 Ryoh Fuji-Hara, Xiyang Li, Ying Miao, and Dianhua Wu. A TWWOA 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).
- [FM13] **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).

- 2976 (print), 1862-2984 (electronic).
- [FMS09] Simon Fischer, Willi Meier, and Dirk Stegemann. Some remarks on FCSRs and implications for stream ciphers. *Journal of Mathematical Cryptology*, 3(3):227–236, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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).
- [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).
- [FS11] Marc Fischlin and Dominique Schröder. Security of blind signatures under aborts and applications to adaptive oblivious transfer. *Journal of Mathematical Cryptology*, 5(2):169–203, 2011. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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).
- [GKL15] David Garber, Delaram Kahrobaei, and Ha T. Lam. Length-based attacks in polycyclic groups. *Journal of Mathematical Cryptology*, 9(1):33–43, 2015. CO-



- DEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Galbraith:2007:SPC**
- [GÓŠ07] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy. Simplified pairing computation and security implications. *Journal of Mathematical Cryptology*, 1(3):267–281, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- Gaal:2009:SNE**
- [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).
- Grošek:2013:CS**
- [GP13] 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).
- Gupta:2017:ADT**
- [GPR17] Kishan Chand Gupta, Sumit Kumar Pandey, and Indranil Ghosh Ray. Applications of design theory for the constructions of MDS matrices for lightweight cryptography. *Journal of Mathematical Cryptology*, 11(2):85–116, June 2017. ISSN 1862-2976 (print), 1862-2984 (electronic). URL [https://www.degruyter.com/view/j/jmc.2017.11.issue-](https://www.degruyter.com/view/j/jmc.2017.11.issue-2/jmc-2016-0013/jmc-2016-0013.xml)
- Galbraith:2009:DMS**
- [GPRS09] 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).
- Gutierrez:2009:FSW**
- [Gut09] Jaime Gutierrez. Foreword: Second Workshop on Mathematical Cryptology. *Journal of Mathematical Cryptology*, 3(3):175–176, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). Held in Santander, October 23–25, 2008.
- Galbraith:2013:SPH**
- [GZ13] Steven D. Galbraith and Chang-An Zhao. Self-pairings on hyperelliptic curves. *Journal of Mathematical Cryptology*, 7(1):31–42, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). See erratum [GZ14].
- Galbraith:2014:ESP**
- [GZ14] Steven D. Galbraith and Chang-An Zhao. Erratum: Self-pairings on hyperelliptic curves [J. Math. Cryptol. **7** (2013), 31–42] [MR3101014]. *Journal of Mathematical Cryptology*, 8(1):93, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). See [GZ13].

- [HF07] **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 ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Hin08] **Hinek:2008:SMP**  
M. Jason Hinek. On the security of multi-prime RSA. *Journal of Mathematical Cryptology*, 2(2):117–147, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Hit09] **Hitt:2009:FGC**  
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).
- [HL09] **Hinek:2009:ALS**  
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).
- [HL10] **Hinek:2010:CMA**  
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).
- [HM07] **Heuberger:2007:MWC**  
Clemens Heuberger and James A. Muir. Minimal weight and colexicographically minimal integer representations. *Journal of Mathematical Cryptology*, 1(4):297–328, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [HS08] **Hartung:2008:ISB**  
Rupert J. Hartung and Claus-Peter Schnorr. Identification and signatures based on NP-hard problems of indefinite quadratic forms. *Journal of Mathematical Cryptology*, 2(4):327–341, 2008. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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).
- [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<sup>+</sup>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).
- [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).
- [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] Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. *Journal of Mathematical Cryptology*, 8(2):115–140, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Justus:2014:DQR**
- [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). **Justus:2015:DQR**
- [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). **Wei:2012:FMP**
- [Kar10] Koray Karabina. Factor-4 and 6 compression of cyclotomic subgroups of  $\mathbf{F}_{24m}^*$  and  $\mathbf{F}_{36m}^*$ . *Journal of Mathematical Cryptology*, 4(1):1–42, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Karabina:2010:FCC**
- [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). **Koblitz:2008:ALN**
- [KM08] Neal Koblitz and Alfred Menezes. Another look at non-standard discrete log and Diffie–Hellman problems. *Journal of Mathematical Cryptology*, 2(4):311–326, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Koblitz:2013:ALH**
- [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). **Karabina:2010:AEW**
- [KMPS10] Koray Karabina, Alfred Menezes, Carl Pomerance, and Igor E. Shparlinski. On the asymptotic effectiveness of Weil descent attacks. *Journal of Mathematical Cryptology*, 4(2):175–191, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Kurosawa:2013:NLR**
- [KNP13] Kaoru Kurosawa, Ryo Nojima, and Le Trieu Phong. New leakage-resilient CCA-secure public key encryption. *Journal of Mathematical Cryptology*, 7(4):297–312, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). **Kortelainen:2010:MAG**
- [KHK10] Juha Kortelainen, Kimmo Halunen, and Tuomas Kortelainen. Multicollision attacks and generalized iterated hash

- [Kob07] Neal Koblitz. Another look at automated theorem-proving. *Journal of Mathematical Cryptology*, 1(4):385–403, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [Kob12] Neal Koblitz. Another look at automated theorem-proving II. *Journal of Mathematical Cryptology*, 5(3–4):205–224, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [KU15] Matvei Kotov and Alexander Ushakov. Analysis of a certain polycyclic-group-based cryptosystem. *Journal of Mathematical Cryptology*, 9(3):161–167, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [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>.
- [Kus18] Prabhath 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). URL <https://doi.org/10.1515%2Fjmc-2017-0053>.
- [LC07] 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).
- [LL15] Kim Laine and Kristin Lauter. Time-memory trade-offs for index calculus in genus 3. *Journal of Mathematical Cryptology*, 9(2):95–114, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [LMPW15] Atul Luykx, Bart Mennink, Bart Preneel, and Laura Winzen. Two-permutation-based hashing with binary mixing. *Journal of Mathematical Cryptology*, 9(3):139–150, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [LNR09] Mario Lamberger, Tomislav Nad, and Vincent Rijmen. Nu-

**Koblitz:2007:ALA****Kushwaha:2018:ILB****Koblitz:2012:ALA****Li:2007:SAC****Kotov:2015:ACP****Laine:2015:TMT****Kotov:2018:AKE****Luykx:2015:TPB****Lamberger:2009:NSC**

- merical solvers and cryptanalysis. *Journal of Mathematical Cryptology*, 3(3):249–263, 2009. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [LU08]
- [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>. Lu:2017:CRV
- [LS07] Tanja Lange and Igor E. Shparlinski. Distribution of some sequences of points on elliptic curves. *Journal of Mathematical Cryptology*, 1(1):1–11, 2007. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). Lange:2007:DSS
- [LS18] Thalia M. Laing and Douglas R. Stinson. A survey and refinement of repairable threshold schemes. *Journal of Mathematical Cryptology*, 12(1):57–??, March 2018. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2018.12.issue-1/jmc-2017-0058/jmc-2017-0058.xml>. Laing:2018:SRR
- [Mag13] Spyros S. Magliveras. Foreword. *Journal of Mathematical Cryptology*, 7(3):181–182, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). URL <https://www.degruyter.com/view/j/jmc.2013.7.issue-3/jmc-2013-5001/jmc-2013-5001.xml>. Magliveras:2013:F
- [Maz12] Gérard Maze. Analysis of a key distribution scheme in secure multicasting. *Journal of Mathematical Cryptology*, 6(1):69–80, 2012. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). Maze:2012:AKD
- [Men07] Alfred Menezes. Another look at HMQV. *Journal of Mathematical Cryptology*, 1(1):47–64, 2007. Menezes:2007:ALH
- [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). Mohammed:2017:RNF
- [Longrigg:2008:CSC] 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).

- 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 ????
- [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).
- [MSP12] **Mouha:2012:CIR** 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] **Myasnikov:2008:RSA** 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] **Mosina:2010:MSA** Natalia Mosina and Alexander Ushakov. Mean-set attack: cryptanalysis of Sibert et al. authentication protocol. *Journal*

- of *Mathematical Cryptology*, 4(2):149–174, 2010. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic). [Nan09]
- Myasnikov:2014:CMC**
- [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). [NM08]
- Mullan:2011:CVS**
- [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). [NP16]
- Murphy:2012:ELH**
- [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>. [NSW09]
- Moody:2012:FEC**
- [MW12] 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). [NV08]
- 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).
- 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).
- 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).
- 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).
- 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  $\rho$ -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] **Omar:2014:FHF** 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] **Partala:2018:AGD** 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] **Persichetti:2012:CMK** 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>.
- [Pop17] **Popov:2017:DTP** 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] **Poulakis:2016:NLA** 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).
- [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).

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

**Paterson:2015:OCI**

- [PS15] Maura B. Paterson and Douglas R. Stinson. Optimal constructions for ID-based one-way-function key predistribution schemes realizing specified communication graphs. *Journal of Mathematical Cryptology*, 9(4):215–225, 2015. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

**Paterson:2013:CTF**

- [PSU13] Maura B. Paterson, Douglas R. Stinson, and Jalaj Upadhyay. A coding theory foundation for the analysis of general unconditionally secure proof-of-retrievability schemes for cloud storage. *Journal of Mathematical Cryptology*, 7(3):183–216, 2013. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

**Reichl:2017:TLS**

- [Rei17] Dominik Reichl. Tame logarithmic signatures of abelian groups. *Journal of Mathematical Cryptology*, 11(4):205–214, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

**Ruinskiy:2007:LBC**

- [RST07] 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).

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

**Raddum:2018:MSB**

- [RZ18] 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>.

**Schindler:2008:ASM**

- [Sch08] Werner Schindler. Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. *Journal of Mathematical Cryptology*, 2(3):291–310, 2008. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

**Scholl:2017:IEC**

- [Sch17] Travis Scholl. Isolated elliptic curves and the MOV attack. *Journal of Mathematical Cryptology*, 11(3):131–146, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).

**Sha:2014:NIC**

- [Sha14] Min Sha. On the non-idealness of cyclotomic families of pairing-friendly elliptic curves. *Journal of Mathematical Cryptology*, 8(4):417–440, 2014. CODEN ???? ISSN 1862-2976 (print), 1862-2984 (electronic).

- [Sho10] **Shokrieh:2010:MPD** 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).
- [Sil07] **Silverman:2007:OPS** Robert D. Silverman. Optimal parameterization of SNFS. *Journal of Mathematical Cryptology*, 1(2):105–124, 2007. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SPSS12] **Sepahi:2012:NSN** Reza Sepahi, Josef Pieprzyk, Siamak F. Shahandashti, and Berry Schoenmakers. New security notions and relations for public-key encryption. *Journal of Mathematical Cryptology*, 6(3–4):183–227, 2012. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SS09] **Saxena:2009:CPB** Amitabh Saxena and Ben Soh. A cryptographic primitive based on hidden-order groups. *Journal of Mathematical Cryptology*, 3(2):89–132, 2009. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SS16a] **Samajder:2016:ALN** Subhabrata Samajder and Palash Sarkar. Another look at normal approximations in cryptanalysis. *Journal of Mathematical Cryptology*, 10(2):69–99, 2016. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SS16b] **Swanson:2016:USS** Colleen M. Swanson and Douglas R. Stinson. Unconditionally secure signature schemes revisited. *Journal of Mathematical Cryptology*, 10(1):35–67, 2016. CODEN ????? ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SS17] **Samajder:2017:RUB** Subhabrata Samajder and Palash Sarkar. Rigorous upper bounds on data complexities of block cipher cryptanalysis. *Journal of Mathematical Cryptology*, 11(3):147–175, 2017. ISSN 1862-2976 (print), 1862-2984 (electronic).
- [SSA17] **Saraswat:2017:SAP** Vishal Saraswat, Rajeev Anand Sahu, and Amit K. Awasthi. A secure anonymous proxy 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] **Singh:2011:PDE** Rajesh P. Singh, A. Saikia, and B. K. Sarma. Poly-dragon: an efficient multivariate public key cryptosystem. *Journal of Mathematical Cryptology*, 4(4):349–364, 2011. CODEN ?????

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

**Stinson:2014:EDS**

[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).

**Svaba:2010:PKC**

[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).

**Staszewski:2013:SAL**

[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>.

**Stinson:2007:SRQ**

[SW07a]

D. R. Stinson and R. Wei. Some results on query processes and reconstruction functions for unconditionally secure 2-server 1-round binary private information retrieval protocols. *Journal of Mathematical Cryptology*, 1(1):33–46, 2007. CODEN ????

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

**Stinson:2007:EST**

[SW07b]

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).

**Sparr:2015:RFK**

[SW15]

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).

**Tischhauser:2011:NCA**

[Tis11]

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).

**Tassa:2013:OEM**

[TJBY13]

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).

- [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).
- [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).
- [WP11] **Wolf:2011:EKU**  
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).
- [WS09] **Wu:2009:EIP**  
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).
- [Yoo15] **Yoon:2015:NMC**  
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).

**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).