Title word cross-reference

(2, 2) [PS20]. (2, 2) [AJZT19]. \((n + 1)\) [ZMD20]. \((p^r - 1)/3\) [BW09]. 1 [SW07a]. 2 [AJZT19, Gau07, Hit09, SW07a]. 3 [CC15, LL15, MW12]. 4 [Kar10]. 5 [HL19]. 6 [Kar10]. \(LWE\) [COP24]. \(ax \equiv b \pmod{n}\) [GP13]. \(GL_2(F_{p^r})\) [TNS20]. \(k\) [AMW07, BW09]. \(F_{2^{4m}}^*\) [Kar10]. \(F_{36m}^*\) [Kar10]. \(F_p\) [BW09]. \(F_{p^2}\) [DM20]. \(F_{p^k}\) [Duq11]. \(Q(\zeta_{2s})\) [BS19]. \(Z/NZ\) [ST24]. \(M\) [WP11]. \(Q\) [WP11]. \(MST_3\) [BCM09]. \(n\) [DSS20, ZMD20]. \(N = p^rq^l\) [LPS17]. \(p\) [KMNN19]. \(p + q\) [MA17]. \(\rho\) [Oka12]. \(MST_3\) [SvT10]. \(S\) [ZMD20].


2019 [DKKS20]. 256 [DT17].

7 [GZ14].


AR15, CGK13. Classes
AOY15, AJZT19, WL13. classical
BBP+20. cloud [PSU13]. CM [JLLRL20].
code [KH23]. code-based [KH23]. codes
BBB+18, EHKN24, FHMW08, JCK+18, LdV19, PS20, Per12, SPB22, Tim24.
coding [FL08, PSU13]. coefficient
LZ23, ZHM+22. colexicographically
HM07. Collision [BDJ14]. collisions
BS07. coloring [ADPS14]. combinatorics
[MN07]. combined [DSG21]. Combining
BGGJ20. Common [CCH+20, HL10].
communication [PS15]. commutative
[JCK+18]. Compact [CQS11, Per12].
comparative [CDK18]. comparison
[BK09]. complete [BGMP08, Oka12].
Complex [BCIV20]. Complex-Valued
BCIV20. complexities [SS17].
Complexity
YYTK20, AMW07, BW09, DS17.
composite [CDK18]. compositeness
[PR20]. Compression [BG16, Kar10].
computation [ADPS14, CS21, CI14, DGC+15, Duq11, DEF14, GQS07].
computational [Ano20]. computations
CDN18. Computing [Bis11, Eke21].
concrete [APS15]. concurrent [WS09].
concurrent-reset [WS09]. condition
DSS20. conferences [JP20]. confusion
LZ23, ZHM+22. conjecture [CLS09].
congruency [LU08]. conjugation [MU14].
connected [DS17]. connection [Zaj13].
Constant [TW20, AL11]. constant-size
[AL11]. constants [Grz20]. constructed
ZMD20. Constructing [CJS14].
Construction [vT18, AGH17, ADPS14, CL09, FHMW08, IK23, JCK+18].
constructions
GPR17, LdV19, PS15, WC07. Converting
CDK18. convolution [OS14]. Coprime
GP13. correlation [DR07, DT17].
corresponding [BFJT12]. Cosets [KT20].
Coskun [AK17]. Counting [DN08, WL13].
CP [COP24, COP24]. CP-ABE [COP24].
criterion [LC07]. critical [Bla09]. CRT
[CCH+20]. CRT-variant [CCH+20].
Cryptanalysing [Bla09, Mul11, Bla10].
Cryptanalysis [BCM09, BCM11, BKL22, CBW07, Esk24, LU08, LPS17, MU14, TL15, BP20, CG20, DT17, LNR09, MU10, PGS20, RST07, SS16a, SS17, SvT10, Tis11].
Cryptographic
BBPS20, CJST16, BCSV20, BFJN20, MP08, SPB22, SS09, ZMD20. cryptography
[CAR20, COP24, GGD20, GPR17].
Cryptol. [GZ14]. cryptology
[CW22, Gut09, JP20]. Cryptosystem
PGS20, BCM09, Bla10, CBW07, CG20, HF07, Jus14, Jus15, KU15, SSS11, SvT10].
cryptosystems
AOY15, CDK18, DJP14, EOS07. CSIDH
BBP+20. cubic [CC15]. cumulative
[MN07]. Curve [HKP+20, KT20, CJS14, CQS11, DJP14, FK18, Tim24]. Curves
BGK+20, BG16, Bis11, Box12, BDFM21, CDS20, DN08, DEF14, FSV09, GPRS09, GZ13, GZ14, HST10, HWCD11, Hit09, LS07, MW12, Mor08, Oka12, ST24, Sch17, Sha14, Yoo15. cyclic [AJZT19]. cyclotomic
AMW07, DSS20, Kar10, Sha14].

DAGS
BBB+18. Data
BCIV20, CN22, SS17, SU14].
decentralized [Pop17]. decreasing
YYS+17. decryption [YYS+14].
DeepBKZ [Yas20]. defeat [DSG21].
degree [Hit09, KW19]. degrees [TKF+20].
Delegating [DKKS20]. delegation
ZSN20. Deligne [Tim24]. Dembowski
AOY15. density [FS09]. Dependent
FGG+20. descent [KPS10]. design
GPR17. designated [YH24]. Designing
BBPS20. detailed [Wun19]. determined
KK23. Devastating [TW20]. Differential
CC124, DT17. differential-zero [DT17].
differentials [DR07]. Diffie
KM08, Kus18, Par18. digital [RUS23].
dihedral [CS24]. dimension [EHKN24].

Dimensions [MR20]. Discrete
  [HKP⁺20, MR20, BT12, Bla09, Bla10, BDJ14, CI14, Eke21, Gal12, KM08, Sho10].
Discretisation [MP20], disguised [Mor08].
  Distortion [GPRS09]. distributed [DGG⁺15].
Distribution [LS07, BS07, Jus14, Jus15, Maz12, PS08, vzGS09]. Distributions
  [MP20, DR07]. Divisor [CCH⁺20]. dragon
  [SSS11]. DSA [Pou16]. dual [NP19, Yas20].
  duality [Csi20]. Dyadic
  [BBPS20, BBB⁺18, Per12].
ECC [Joy20]. ECDLP [DM20, YYTK20].
  Editor [CLS20]. Edwards [BG16]. effect
  [Mur12]. effectiveness [KMPS10, Mur12].
Efficiency [GPV24]. Efficient
  [BBPS20, DEF14, HST10, DGG⁺15, FM13, SSS11, SW07b, WS09]. Efficiently
  [BCIV20, Bla09]. elementary
  [Kar20a, Kar20b, ZLA21]. elements
  [Yoo15]. Eleventh [JLNN20]. ElGamal
  [PGS20]. Elliptic
  [BGK⁺20, HKP⁺20, KT20, Bis11, Box12, CJS14, CQ511, DJP14, DEF14, FS09, FK18, HST10, HWCD11, LS07, MW12, Mor08, Oka12, ST24, Sch17, Sha14, Yoo15].
EMAC [JV16]. embedding [Hit09].
  encapsulation [BBB⁺18]. encodings
  [NP19]. Encryption
  [BLNN21, BCIV20, BGJ20, DS20, ASB⁺18, AL07, AL11, CLS24, CN22, CEM15, IK23, KNP13, NP16, SPS12, TL15, YYS⁺14]. endomorphism [Bis11]. Enhancing
  [SPS19]. EPIR [CW12]. 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, TJBY13]. even
  [Kar20a, Kar20b]. Evolution
  [CW22, BGMP08]. Exact [HL19, YYS⁺14]. examples [DC14]. Exchange [BGK⁺20, RM20, Ala17, Jia14, KU18, Par18, RS22].
Exclusion [Rei21]. exhaustive [RZ18].
  existence [WC07], expansions [FS08].
experiments [CC12]. explicit
  [ATW08, Grz20]. exploration [HWCD11].
  exponent [HL10]. exponentiation
  [DGG11]. Exponentiations [DKKS20].
  exponents [Boc09, Kar20a, Kar20b].
Exposure [DSGKS20]. 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
  [BLNN21, 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, LP20, LC07]. filtered [OPS13]. find
  [Rei21]. Finding
  [Gal12, BS19, PP18, Yas20]. finite
  [BFP09, CBW07, FL08, HST10, HSWZ20, JCK⁺18, Kus18, LC07, Sh010]. first
  [KW19, CLY20]. Flattening [DS20]. flaw
  [ASB⁺18]. Flips [TW20]. flow [SW07b].
Foreword [Gut09, Mag13]. forms [HS08].
  formulae [ATW08]. formulæ [MA17].
foundation [PSU13]. framework
  [BP20, BCSV20]. Free [DS20, Ano20].
  friendly [Box12, FK18, Oka12, Sha14, Yoo15].
Frontmatter [Ano17, Ano18d, Ano18a, Ano18b, Ano19c, Ano19a, Ano19b].
Fully [BGJ20, Dow15, TL15, YYS⁺14]. function
  [ACP10, GP09, Nan09, NS09, PS15].
Functional [AL11]. Functions
general [Eke21, PSU13]. generalised [Dow15, MN07]. Generalization [DS18, Par18, Tim24]. generated [LZ23].

fundamental [ASB+18]. Further [LZ23].
CBW07, DS18, GGD20, Jia14, KU18, KNP13, Maz12, Mul11, Par18, PS08, PS15, RS22, SPSS12, SSS11, SvT10, TL15, WP11.
key-recovery [BFJT12]. keys [BFJT12, KMU20, Per12, WP11].
keystream [DS18]. keyword [CLSV24].
knowledge [SW07b]. known [ZMD20].
Koblitz [DN08].
large [Grz20]. Last [Kar20a, Kar20b].
Lattice [MR20, Pou16, Wu19, YYS+17, Yas20].
lattice-reduction [Wum19]. lattices [Laa20, SPS19].
Laws [HWCD11].
Leakage [CDGM14, FGG+20, Ala17, CAR20, KNP13].
leakage-resilient [Ala17, CAR20, KNP13].
Learning [APS15, BBGS19].
least [HL19].
Leftover [DSGKS20]. Lemma [DSGKS20b].
Length [FKL15, RST07, MU08]. Length-based [FKL15, RST07, MU08]. lengths [YYS+17].
Lightweight [BLLN21, GPR17]. Linear [HS15b, AMW07, BCSV20, BW09, CDN18, DT17, EHKN24, Mur12, RZ18].
linearly [OPSB13]. Log [MR20, KM08]. Logarithm [HKP+18, BT12, Bla09, Bla10, Sho10].
logarithmic [BdW12, Rei17, SVT13, vT18].
logarithms [BDJ14, C14, Eke21, Gal12].
look [HL09, Kob07, KM08, Kob12, KM13, Men07, S16a]. low [ATW08]. lower [Kus18].
LPS [PP18]. Lusztig [Tim24].
LWE [BG20, DSGKS20a, MP20].
MAC [ABD+13, JN16]. MAKE [BKL22, RS22]. maps [GPR09]. masking [Sch08].
Masthead [Ano13]. Math. [GZ14].
MathCrypt [CLS20, CLY20].
Mathematical [Gut09]. Matrices [PGS20, GPR17].
Matrix [BCM11, DSS20, KU18, MU14, RS22, ZSN20].
Methods [JP20, DSG21, HL09, JCK+18, Sch08]. mF [CN22].
Minimal [FS08, HM07]. mixing [LMPW15]. mnemonic [AGH17]. mode [ASB+18, CN22].
model [BBP19, DN08]. modified [HVH14]. modular [HL09].
MOV [Sch17]. MQs [CGK13]. mR [COP24]. MR3101014 [GZ14]. MRHS [RZ18, Zaj13]. Multi
[PSU18, FLMW08, Hin08, YH24]. Multi-designated [YH24]. multi-message [FHLWM08]. multi-prime [Hin08].
Multi-prover [PSU18]. multi-receiver [FHLWM08]. multicasting [Maz12].
Multiple [DT17, FM13]. multiplicative [Kus18].
multiplier [EHKN24]. multivariate
[AØY15, 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
pair [NP19]. pairing
[Box12, CDK18, Duq11, FK18, GÓS07, Oka12, Sha14, Shao10, Yoo15].
pairing-based [CDK18]. pairing-friendly
[Box12, FK18, Oka12, Sha14, Yoo15].
pairings [DEF14, GZ13, GZ14]. parallel [CC124].
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]. Piatet [FS08]. PKA
[AR15]. Plactic [Bro23]. PMAC [NM08].
Points [KT20, BG16, LS07]. poker
Poly-dragon [SSS11]. Pólya [CLS16].
polyhedral [KL15, KU15].
polyhedral-group-based [KU15].
Polylogarithmic [Mie08]. polymatroids
[KK23, MFP10]. Polynomial [KMNN19,
CWZ12, DSS20, JLLRL20, WL13, ZSN20].
Polynomials
[HKP+20, AÔY15, KW19, TJBY13]. PoRs
[LdV19]. possessing [SU14]. post [COP24].
post-quantum [COP24]. Power
[JLLNN20, ACP10, TKF+20]. practical
[BFJT12, CAR20, NV08]. practice [HL10].
Predicate [NP19]. predistribution [PS15].
Preface [CLS20, CLY20, JP20]. Prefix
[FGG+20]. Prefix-Dependent [FGG+20].
presence [Dow15, Sch08]. preserving
[Esk24, ZSN20]. prime
[CDK18, Hin08, TKF+20]. primes
[ACP10, FS09, vzGS13]. primitive
[SS09, Yoo15]. primitives
[BFJN20, CDN18]. Principal [LPS20].
Privacy [ZSN20, Esk24].
Privacy-preserving [ZSN20, Esk24].
private
[DG+15, Esk24, HL10, KMU20, SW07a].
Probability [DR07]. Problem
[CCH+20, HKP+20, LPS20, BT12, BBGS19,
Bla09, Bla10, CS24, HSW20, Kus18, NV08].
problems [BCSV20, HS08, KM08, TKF+20].
Proceedings [CLS20, CL20]. processes
[SW07a]. Processing [BC120]. Product
[DKKS20, MP20, OS14]. products
[AL11, IK23]. proof
[Kar20a, Kar20b, NP19, PSU13, PSU18].
proof-of-retrievability [PSU13].
properties [CJST16, ZMD20]. property
[EHK24]. Protecting [Joy20]. protocol
[CWZ12, KU18, KMU20, LU08, MU10,
SW07b, jWW12, WS09]. protocols
[AK17, BCM11, IK23, SW07a]. Provably
[Moc23]. provable [PSU18]. proving
[Kob07, Kob12]. proxy [SSA17]. Pseudo
[Ano20, BGMP08, Pop17]. Pseudo-free
[Ano20]. pseudo-random [Pop17].
pseudorandom [NP19, vzGS09]. Public
[SvT10, AL11, BCM09, CAR20, CBW07,
GDD20, KNP13, SPSS12, SSS11, WP11].
public-attribute [AL11]. public-key
quadratic [AÖY15, CGK13, HF07, HS08, Jus14, Jus15].
Quantum [CI14, Eke21, BS19, BP20, BBP+20, CJ14, COP24, DJP14, JLLRL20, RUS23]. quantum-resistant [DJP14].
Quantum-resistant [BS19, BP20, BBP+20, CJS14, COP24, DJP14, JLLRL20, RUS23]. quantum-dyadic [Per12].
quasigroups [CGK13]. query [SW07a].
Rabin [Böc09]. Ramanujan [PP18].
Random [MU08, BGMP08, EHKN24, Pop17]. randomized [Böc09, CLSV24]. range [YYS+14].
Rational [MW12]. ratios [HL19].
RC4 [BGMP08, DS18]. realization [SvT10]. realizing [PS15]. receiver [FHLMW08]. reconstruction [SW07a].
Recovering [FGG+20]. recovery [BFJT12]. Recursive [CL09]. reduced [DT17]. reduced-round [DT17]. reducing [BP20].
Residue [JLNN20, CS21]. residues [Jus14, Jus15]. resilient [Ala17, CAR20, HS15b, KNP13]. resistance [MP12].
resistant [DJP14]. restricted [BBGS19]. results [DS18, LZ23, SW07a]. Retracting [ATW08]. Retraction [Kar20b].
rho [BDJ14]. Richelot [DS20]. Rigorous [SS17]. Rijndael [RMS24]. Ring [DSGKS20b, Joy20, BT12, YH24, BGGJ20, DSGK20a, MP20].
Ring-LWE [DSGKS20a, MP20]. Ring-LWE-based [BGGJ20].
rotate [FJ13]. Rotation [Rei21, CC15, CLS16]. round [BK09, DT17, Mie08, SW15, SW07a]. RSA [DS21, Hin08, HL10, LPS17, MA17].
safe [AK17, vzGS13]. same [SU14].
samples [BBGS19]. SAP [GGD20].
scheme [Esk24, HVV14, HSW220, KH23, Maz12, Mul11, PS08, SSA17, SPS19, TL15].
Schemes [BLGN21, BGGJ20, DKS20, BP19, BS19, GD13, HS15a, JN13, LS18, MFP10, MU14, PSU13, PS15, PS20, Poul16, RUS23, SS16b, YH24]. Schmidt [YYS+17].
Schnorr [NSW09]. search [CLS24, MA17, RZ18, RMS24]. Searchable [CLSV24]. Second [CLS20, Gut09]. Secret [Csi20, DC14, GD13, HS15a, HL19, JSN13, MFP10, CEM15]. Secrets [FGG+20].
Secure [Dow15, BK09, CS21, FL08, JSN13, KNP13, Maz12, PSU13, SSA17, SW07b, SW07a, SS16b, WS09]. Security [FS11, HVV14, OPSB13, ACP10, AL11].
BBP19, CDG14, EOS07, GÖS07, Hn08, Moc23, MPST16, NM08, Nan09, NP16, SPSS12, DSGKS20a]. Self [GZ13, Yas20, GZ14].
Sensitivities [ZLA21]. sensor [HS15b, PS08]. sequences [AMW07, BW09, LS07]. server [SW07a].
set [Esk24, Gal12, MU10]. setting [CDK18].
seven [DS17]. sharing [Csi20, DC14, GD13, HS15a, HL19, JSN13, MFP10]. shifted [LU08]. Short [LPS20, BS19, YYS+17, Yas20]. shortest [NV08]. Sibert [MU10]. side [Schar08].
Sidelnikov [BW09]. **SIDH** [GPV24, UJ20].

**SIDH-based** [GPV24, UJ20]. **Sieve** [NV08, Grz20]. **Sieving** [MR20]. **Sign** [TW20]. **Signature** [DKKS20, HSWZ20, NP16, RUS23, SS16b, YH24]. **signatures** [BdW12, FS11, GPV24, HS08, NP19, NSW09, Rei17, SvT13, vT18]. **Signcryption** [BBP19, Kh23, SSA17].

**SIKE** [BP20]. **Simpliﬁed** [GOS07]. **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, D18, FS09, HS09, HL10, IK23, LS07]. **space** [JLLRL20]. **sparse** [AK17, FK18]. **Special** [DKKS20, CGK13, FS09]. **speciﬁed** [PS15]. **Square** [DM20]. **squared** [YYS+17]. **squeezing** [CDGM14]. **Srivastava** [Per12]. **standard** [KM08]. **Statistical** [BS07]. **Stickel** [Mul11]. **Stochastic** [DSG21, Sch08]. **storage** [PSU13]. **stream** [FMS09, Moc23, Tis11]. **streams** [DDG+15]. **Strict** [LC07].

**Strongly** [SvT13, AR15, vT18]. **structure** [DS17, JN16, JSN13, ST24]. **structures** [GD13, KK23]. **subexponential** [ADPS14, CJ14, JLLRL20]. **subexponential-time** [JLLRL20]. **subﬁeld** [HST10, HKP+20]. **subgroup** [CS24]. **subgroups** [Kar10, MU08]. **Submission** [DKKS20]. **subsequences** [BW09]. **Subset** [vzGS09]. **sum** [HF07, YYS+17, vzGS09]. **summary** [EOS07]. **summation** [KW19].

**supersingular** [BP22, CK20, DJP14, GPRS09]. **superspecial** [CDS20]. **support** [AL11]. **Survey** [GGD20, LS18]. **Suzuki** [Tim24]. **Symbol** [JLNN20]. **symbols** [CS21]. **Symmetric** [Rei21, CDN18, CL19, CC16, TL15, ZLA21]. **System** [RM20, NP19]. **systems** [BFP09, Mie08, WP11, Zaj13].

**Takes** [TW20]. **Tame** [Rei17]. **technique** [NP19]. **Techniques** [UJ20]. **terms** [FM13]. **test** [Böe09]. **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, CJ14, JLLRL20]. **Time-memory** [LL15]. **Timing** [TW20].

**torsion** [MW12]. **trace** [BG16, EHKN24, FM13]. **trade** [BBP+20, LL15]. **trade-off** [BBP+20]. **trade-offs** [LL15]. **tradeoffs** [Eke21]. **transfer** [FS11]. **transmission** [AL07, Dow15]. **Tropical** [RM20, KU18].

**truncated** [FJ13]. **trustless** [Pop17]. **twisted** [BG16, BDFM21]. **Two** [LMPW15, PS08, GPRS09, Mie08, RUS23, SW07b]. **two-ﬂow** [SW07b]. **Two-permutation-based** [LMPW15]. **two-round** [Mie08]. **TWOOA** [FHLMW08]. **Type** [TNS20, AJZT19, EOS07, Jus14, Jus15, Tim24].

**ultratrace** [BP11]. **ultivariate** [WP11]. **unbounded** [DDG+15]. **uncloaking** [KMU20]. **Unconditionally** [JSN13, SS16b, PSU13, SW07a]. **Unconditionally-secure** [JSN13]. **uniform** [KK23]. **universal** [ACP10, Ano20]. **upper** [SS17]. **use** [BP20]. **Using** [FJ13, Rei21, BBB+18, BF09, CCI24, CDS20, CW22, FK18, Kus18].

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

[BF09, EHKN24, YYS+17, Yas20].

verifiable [ZSN20]. verifiers [YH24]. via
[CS21, DM20, NP19]. view [MP08].

Volume [CLS20, CLY20]. Voronoi [Laa20].

VSH [BS07].

way [PS15]. weak [AÖY15, BFJT12].

weight [FS08, HM07]. weighted [HS15a].

weights [BC12]. Weil [HF07, KMPS10].

Weng [Yoo15]. wide [MPST16]. witnesses
[PR20]. Witt [BF09]. Workshop [Gut09].

xor [FJ13].

yes [GPV24].

Zémor [TNS20]. zero [BG16, DT17, SW07b].

zero-knowledge [SW07b].

References


**Albrecht:2015:CHL**


**Accardi:2015:CSA**


**AlMahri:2018:FFA**


**Avanzi:2008:RLG**


**Banegas:2018:DKE**


**Bindel:2019:EHL**

REFERENCES


REFERENCES

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

Blackburn:2011:CTM

Bootland:2020:FCP

Broon:2021:ITH

Bos:2014:CBA

Baumeister:2012:ALS

Bourgeois:2009:AAN

Brier:2020:NNT

Bouillaguet:2012:FWK
Charles Bouillaguet, Pierre-Alain Fouque, Antoine Joux,

\textbf{Bettale:2009:HAS}


\textbf{Bianco:2016:CTZ}


\textbf{Boura:2020:CCR}


\textbf{Boneh:2020:MNI}


\textbf{Basu:2008:CCE}


\textbf{Bisson:2011:CER}


\textbf{Blake:2009:ORS}

Broksen:2022:CM

Blackburn:2009:CCG

Blackburn:2010:DLP

Bhattacharjee:2021:OVF
REFERENCES


REFERENCES


REFERENCES

Castryc:2020:HFS

Wouter Castryck, Thomas De-cru, and Benjamin Smith. Hash functions from superspe-
cial genus-2 curves using Riche-
lot isogenies. *Journal of Math-
ematical Cryptology*, 14(1):268–
292, August 7, 2020. CODEN
???? ISSN 1862-2976 (print),
1862-2984 (electronic). URL
https://www.degruyter.com/
document/doi/10.1515/jmc-

Chen:2015:SSK

Jiageng Chen, Keita Emura,
and Atsuko Miyaji. SKENO: Se-
cret key encryption with non-
interactive opening. *Journal of Mathemati-
???? ISSN 1862-2976 (print), 1862-
2984 (electronic).

Childs:2014:QCD

Andrew M. Childs and Gábor
Ivanyos. Quantum computa-
tion of discrete logarithms in semi-
???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Childs:2014:CEC

Andrew Childs, David Jao, and
Vladimir Soukharev. Construct-
ing elliptic curve isogenies in quan-
???? ISSN 1862-2976 (print), 1862-2984 (electronic).

Carlet:2016:CPM

Claude Carlet, David Joyner,
Pantelimon Stănică, and Deng
Tang. Cryptographic proper-
ties of monotone Boolean func-


Chakraborty:2022:MMA


Cianfriglia:2024:MLC


Ciet:2011:CEC


Cascudo:2021:NSM


Chen:2024:DHS


Csirmaz:2020:SSD


Craven:2022:EGT

REFERENCES

Chee:2012:BCE


Dibert:2014:ISS


Duquesne:2014:ECP


Dolev:2015:TEP


DeMicheli:2020:CON


DeFeo:2014:TQR


DiCrescenzo:2020:DPG


Delaplace:2020:CWB

[DM20] Claire Delaplace and Alexander May. Can we beat the square
REFERENCES


Demirkiran:2008:CHC


Dowden:2015:SMT


Daemen:2007:PDC


Dehkordi:2017:CCG


Dey:2018:GRB


Doroz:2020:FNE


Dugardin:2021:SMD

REFERENCES


Dachman-Soled:2020:SRL


Dachman-Soled:2020:TRA


DiScala:2020:CNV


Dachman-Soled:2020:TRA


Duquesne:2011:RAA


Erdelyi:2024:LCR

Ekeraa:2021:QAC


Engelbert:2007:SMT


Eskeland:2024:CPP


Ferradi:2020:RSP


Fuji-Hara:2008:TCM


Field:2013:UCT


Fotiadis:2018:GPF


Fancsali:2008:SAF

REFERENCES


Flori:2013:ECF


Fischer:2009:SRF


Frougny:2008:MWE


Friedlander:2009:DSS


Motahhareh Gharahi and Masoud Hadian Dehkordi. Perfect secret sharing schemes for graph

**Goel:2020:SBA**


**Garber:2015:LBA**


**Galbraith:2007:SPC**


**Gaal:2009:SNE**


**Gupta:2017:ADT**


**Galbraith:2009:DMS**


**Ghantous:2024:ESB**

Wissam Ghantous, Federico Pintore, and Mattia Veroni. Ef-

**Grzeskowiak:2020:VLS**  

**Hinek:2008:SMP**  

**Hitt:2009:FGC**  

**Huang:2020:QSP**  
REFERENCES


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).

**Hoffstein:2020:SSF**

[HSWZ20] Jeffrey Hoffstein, Joseph H. Sil-
verman, William Whyte, and
Zhenfei Zhang. A signature
scheme from the finite field iso-
morphisms 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.

**Haridas:2014:SAM**

[HVV14] Deepthi Haridas, Sarma Venkatara-
man, and Geeta Varadan. Security
analysis of modified Rivest
scheme. *Journal of Mathemat-
ical Cryptology*, 8(3):297–303,
2014. CODEN ????
ISSN 1862-2976 (print), 1862-
2984 (electronic).

**Hisil:2011:EAG**

[HWCD11] Huseyin Hisil, Kenneth Koon-
Ho Wong, Gary Carter, and
Ed Dawson. An exploration
of affine group laws for elliptic
curves. *Journal of Mathemat-
CODEN ????
ISSN 1862-2976
(print), 1862-2984 (electronic).

**Isobe:2023:CEP**

Shuji Isobe and Eisuke Koizumi.
A construction of encryption
protocols over some semidi-
rect products. *Journal of
Mathematical Cryptology*, 17(1):
??, January 2023. CODEN ????
ISSN 1862-2976 (print),
1862-2984 (electronic). URL
https://www.degruyter.com/
document/doi/10.1515/jmc-
2022-0018/html.

**Jirakitpuwapat:2018:NMC**

Wachirapong Jirakitpuwapat,
Parin Chaipunya, Poom Kum-
am, Sompong Dhompongsa,
and Phatiphat Thounthong.
New methods of construction of
Cartesian authentication codes
from geometries over finite com-
mutative rings. *Journal of
Mathematical Cryptology*, 12
CODEN ????
ISSN 1862-
2976 (print), 1862-2984 (elec-
degruyter.com/view/j/jmc.
2018.12.issue-3/jmc-2017-

**Jiang:2014:PAP**

Shaoquan Jiang. Persistent
asymmetric password-based key
exchange. *Journal of Mathe-
matical Cryptology*, 8(1):31–70,
2014. CODEN ????
ISSN 1862-
2976 (print), 1862-2984 (elec-
tronic).

**Jao:2020:STP**

David Jao, Jason LeGrow,
Christopher Leonardi, and Luis

Joye:2020:EPR


Jha:2016:RSG


Joye:2020:PEA


Joux:2020:PNT


Jhanwar:2013:USI


Justus:2014:DQR


Justus:2015:DQR

Benjamin Justus. The distribution of quadratic residues and non-residues in the Goldwasser–Micali type of cryptosystem. II.
References

Wei:2012:FMP


Karabina:2010:FCC


Kortelainen:2010:MAG


Kawa:2023:ASD


Klamti:2023:CBH


Karmakar:2020:EPF


Karmakar:2020:REP


Karmakar:2020:REP
Koblitz:2008:ALN


Koblitz:2013:ALH


Kaji:2019:PEP


Kurosawa:2013:NLR


Koblitz:2007:ALA


Koblitz:2012:ALA


Kim:2020:EAC


**Kotov:2015:ACP**


**Kotov:2018:AKE**


**Kousidis:2019:FFD**


**Laarhoven:2020:AVC**


**Li:2007:SAC**


**Lavauzelle:2019:GCP**


Jonathan Longrigg and Alexander Ushakov. Cryptanalysis of the shifted conjugacy authentication protocol. *Journal of
REFERENCES


REFERENCES

MORALES:2008:ADE


MURPHY:2008:GVC


MURPHY:2020:DPD


MUEHLER:2016:ISF


MCGUIRE:2020:LST


MOUHA:2012:CIR


MUASINOV:2008:RSA

Mosina:2010:MSA


Myasnikov:2014:CMC


Mullan:2011:CVS


Murphy:2012:ELH


Moody:2012:FEC


Nandi:2009:ISA


Nandi:2008:ISA


Nandi:2016:SJS


Nandi:2019:PSP


REFERENCES


REFERENCES

Paterson:2013:CTF

Paterson:2018:MPP

Reichl:2017:TLS

Rudy:2020:RTK

Rouquette:2024:ABA

Rahman:2022:MMA
REFERENCES

2020-0053/html. See successful attack [BKL22].

Ruinskiy:2007:LBC


Romankov:2023:AQA


Raddum:2018:MSB


Schindler:2008:ASM


Scholl:2017:IEC


Sha:2014:NIC


Shokrieh:2010:MPD


Sica:2020:FH


Romankov:2023:AQA


Raddum:2018:MSB


Schindler:2008:ASM


Scholl:2017:IEC


Sha:2014:NIC


Shokrieh:2010:MPD


Sica:2020:FH

REFERENCES

Silverman:2007:OPS


Santini:2022:RFC


Sipasseuth:2019:EGG


Saxena:2009:CPB


Samajder:2016:ALN


Swanson:2016:USS


Samajder:2017:RUB

Saraswat:2017:SAP


Singh:2011:PDE


Sala:2024:GSE


Stinson:2014:EDS


Stinson:2007:SRQ


Stinson:2007:EST


Svaba:2010:PKC


Staszewski:2013:SAL

REFERENCES

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
</table>


[Yasuda:2017:ADS] Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama,

Yokoyama:2020:CBS


Zajac:2013:NMS


Zhou:2022:CCB


Zhang:2021:SBS


Zhou:2020:CPB


Zhang:2020:PPV