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

Nelson H. F. Beebe  
University of Utah  
Department of Mathematics, 110 LCB  
155 S 1400 E RM 233  
Salt Lake City, UT 84112-0090  
USA  
Tel: +1 801 581 5254  
FAX: +1 801 581 4148  
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)  
WWW URL: http://www.math.utah.edu/~beebe/

07 May 2021  
Version 1.06

**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]. \( ax \equiv b \mod n \) [GP13]. \( \text{GL}_d(F_{p^n}) \) [TNS20]. k [AMW07, BW09]. \( F_{24m}^* \) [Kar10]. \( F_{36m}^* \) [Kar10]. \( F_p \) [BW09]. \( F_{p^2} \) [DM20]. \( F_{p^k} \) [Duq11]. \( Q(\mathbb{C}^2) \) [BS19]. \( \mathcal{M}_p \) [WP11]. \( Q \) [WP11]. MST\(_3\) [BCM09]. \( n \) [DSS20, ZMD20]. \( N = p^r q^l \) [LPS17]. \( p \) [KMNN19]. \( p + q \) [MA17]. \( \rho \) [Oka12]. MST\(_3\) [SvT10]. \( S \) [ZMD20].

-ary [KMNN19]. -bit [ZMD20]. -boxes


2019 [DKKS20]. 256 [DT17].

7 [GZ14].


Advanced [Sch08]. adversary [Dow15]. AE [ASB+18]. Affine [CLS16, HWCD11]. Against
aggregation [HS15b]. Agrawal [PS08].
agreement [Mul11]. AJP S[CG20]. al. [MU10]. algebra [BCSV20, KU18, RZ18].
Algebraic [BF09, Par18, TKF +20].
algbras [Ano20]. algorithm [BGMP08, BP20, BDJ14, JLLRL20, Pop17].
Algorithms [CCH +20, AR15, DSG21, Eke21, FJ13, NV08, PP18]. alternating [SW15].
Among [KT20]. Analogue [DSGKS20b]. Analysis [KU15, KU18, Maz12, YYS +17, CDK18, HVV14, Mu08, NM08, Nan09, OPSB13, PSU13, Sch17, Sch08, Wun19].
analyze [FJ13].
Annual [CLS20, CLY20]. anonymous [SSA17]. Aperiodic [BdW12, SvT13, vT18].
Application [DKKS20, Duq11, GGD20, Tis11].
Applications [BBPS20, GPR17, BP20, FL08, FS11, JN16]. approach [BF09, CAR20, CLS16].
approaches [HS15b, TKF +20]. Approximate [CCH +20, Laa20].
approximations [SS16a]. argument [Mic08]. Ariffin [Bla10]. arithmetic [ATW08, Duq11, Gau07, HST10, HL09].
arrays [MN07]. ary [KMNN19]. asymmetric [AR15, Jia14].
asymptotic [KMP08]. Attack [KMU02, TW20, AK17, BBP +20, BF09, HF07, Mor08, MU10, Sch17, Wun19].
Attacks [Joy20, BS19, DHS20, GKL15, HL10, KMP08, KhK10, MSP12, Mu08, PS08, Pou16, WS09]. attribute [AL11].
auction [KMNN19]. Authenticated [BLLN21, TJSJ20, ASB +18].
authentication [ACP10, FHLMW08, JCK +18, LU08, MU10, PS20]. automated [Kob07, Kob12]. auxiliary [Kus18].
avalanche [LC07]. average [AL07].
Balanced [Rei21, CLS09]. barrier [MPST16]. Based [PGS20, TSJL20, ACP10, BCM11, BGGJ20, CDK18, CG20, GKL15, Gau07, HS08, Jia14, Ku015, Ku18, LMPW15, Mu08, PS15, Per12, RZ18, RST07, S09, UJ20]. bases [BF09, FS08]. Beat [DM20]. Bent [Rei21, FM13]. Bergman [BT12]. Better [PP18]. between [BBP +20]. bias [DS18].
Biggs [Bla09].
Binary [ATW08, LMPW15, SW07a]. birthday [HF07, MPST16, MSP12]. Bit [TW20, ZMD20]. blind [FS11],
blinding [DSG21]. BLISS [TW20]. block [DR07, SS17, Sch08, ZLA21].
Boolean [BC12, CJS16, CLS09, CC15, CLS16, ZLA21]. Bound [DM20, Kus18]. bounds [BDJ14, SS17, YYTK20]. boxes [ZMD20].
breaking [MPST16], Brezing [Yoo15].
Bringer [CWZ12], broadcast [AL07].
calculus [LL15, YYTK20]. Can [DM20].
Capitulation [AJZT19]. carry [FJ13].
Challenging [MPST12]. channel [Sch08]. characterisation [HS15a]. Characteristic [MR20, HST10].
class [AR15, CGK13]. Classes [AY15, AJZT19, WL13].
classical [BBP +20]. cloud [PSU13]. CM [JLLRL20].
codes [BBB +18, FHLMW08, JCK +18, LdV19, PS20, Per12].
coding [FL08, PSU13]. colexicographically [HM07]. Collision [BDJ14]. collisions [BS07].
coloring [ADPS14]. combinatorics [MN07]. combined [DSG21].

DAGS [BBB +18]. Data [BCIV20, SS17, SU14]. decentralized [Pop17], decreasing [YYS +17], decryption [YYS +14]. DeepBKZ [Yas20], defeat [DSS20], degree [Hit09, KW19], degrees [TKF +20]. Delegating [DKKS20], delegation [ZSN20]. Dembowsk [AOY15]. density [FS09]. Dependent [FGG +20], descent [KMP08], design [GPR17]. Designing [BBPS20], detailed [Wun19]. Devastating [TW20], differential [DT17], differential-zero [DT17], differentials [DR07]. Diffie [KM08, Kus18, Par18]. Dimensions [MR20]. Discrete [HKP +20, MR20, B12, Bla09, Bla10, BDJ14, CI14, Eke21, Gal12, KM08, Sho10]. Discretisation [MP20], disguised [Mor08], distinguisher [Gal12], Distortion [GPRS09], distributed [DGG +15]. Distribution [LS07, BS07, Jus14, Jus15, Maz12, Po08, vzGS09]. Distributions [MP20, DR07]. Divisor [CCH +20], dragon [SSS11]. DSA [PN16], dual [NP19, Yas20]. duality [Csi20]. Dyadic [BBPS20, BBB +18, Per12].

ECC [Joy20], ECDLP [DM20, YYTK20]. Editor [CLS20]. Edwards [BG16], effect [Mur12], effectiveness [KMP08, Mur12]. Efficient [BBPS20, DEF14, HST10, DGG +15, FM13, SSS11, SW07b, WS09].
the text in the image is a page from a document with several named entities and technical terms. The page seems to be discussing various mathematical and cryptographic concepts, including elements, elements, and specific algorithms and protocols such as ElGamal, Elliptic, EMAC, EMAC, and various other cryptographic techniques and terms. The page also mentions various authors and titles, indicating a rich discussion on complex topics within the field of cryptography and related mathematics.
Greatest [CCH+20], GRH [Bis11].
Gröbner [BF09], Group [DKKS20, PGS20, Bla09, CBW07, HWCD11, JLLR20, KU15, Kus18, RST07, SW15, Zaj13]. groups [GKL15, Rei17, SS09]. Grover [BP20], GS [BBB+18].
Halevi [SPS19, YYS+14], hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].
hardness [APS15, BS19, BBGS19]. Hash [CDS20, DSGKS20b, NSW09, TNS20, ACP10, AN20, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07]. hash-function [ACP10]. hashing [FSV09, LMPW15].
Halevi [SPS19, YYS+14]. Hard [HS08].

look [HL09, Kob07, KM08, Kob12, KM13, Men07, SS16a], low [ATW08], lower [Kus18]. LPS [PP18], LWE [BGGJ20, DSGKS20a, MP20].

MAC [ABD+13, JN16], maps [GPRS09].

masking [Sch08], Masthead [Ano13].

Math. [GZ14], MathCrypt [CLS20, CLY20]. Mathematical [Gut09].


Mean [MU10], Mean-set [MU10].


Methods [JP20, DSG21, HL09, JCK+18, Sch08].

Micali [Jus14, Jus15], MICKEY [Tis11].


monotone [CJST16]. MOV [Sch17]. MQQs [CGK13]. MR3101014 [GZ14].


multi-receiver [FHLMW08]. multicasting [Maz12]. Multicollision [KHK10].

multicubic [LPS20]. multilevel [JSN13].

Multiparty [BGK+20, ADPS14, CS21]. Multiple [DT17, FM13]. multiplicative [Kus18]. multivariate [AÖY15, BFP09, CGK13, HF07, SSS11, TJBY13].

naive [YYTK20]. negation [AL11].

network [FL08, PS08]. networks [HS15b].

NIKE [JU20]. NLFSRs [OPSB13]. Non [BGK+20, TW20, BT12, CDN18, CEM15, Jus14, Jus15, KM08, Sha14].

Non-Constant [TW20]. non-idealness [Sha14]. Non-Interactive [BGK+20, CEM15]. non-linear [CDN18].

non-representable [BT12]. non-residues [Jus14, Jus15]. non-standard [KM08].

Nonsmooth [Tis11]. norm [GP09]. normal [SS16a]. note [CS21]. notations [SPSS12].


Numerical [LNR09]. NutMiC [DKKS20].


One [BK09, TW20, Bl10, PS15].


pair [NP19]. pairing [Box12, CDK18, Duq11, FK18, GÖS07, Oka12, Sha14, Sho10, Yoo15].

pairing-based [CDK18]. pairing-friendly [Box12, FK18, Oka12, Sha14, Yoo15].


Password-Authenticated [TSJL20].

password-based [Jia14]. path [PP18].

path-finding [PP18]. Perfect [GD13, CL09, WC07]. period [BW09].
permutation [BBP19, LMPW15].
permutations [AGH17]. Persistent [Jia14].
pipe [MPST16]. Pisot [FS08]. PKA
[AR15]. PMAC [NM08]. Points
[KT20, BG16, LS07]. poker [JWW12].
Pollard [BDJ14]. Poly [SS11].
Poly-dragon [SSS11]. Polya [CLS16].
polyAl [GKL15, KU15].
polyAl-group-based [KU15].
Polylogarithmic [Mie08].
polymatroids [MFP10].
polynomial [KMNN19, CWZ12,
DSS20, JLLRL20, WL13, ZSN20].
Polynomials [HKP +20, AOY15, KV19, TJBY13]. PoRs
[LdV19]. possessing [SU14]. Power
[JLNN20, ACP10, TKF +20]. practical
[BFJT212, CAR20, NV08]. practice [HL10].
Predicate [NP19]. predistribution [PS15].
Prefix [CLS20, CLY20, JP20]. Prefix
[FGG +20]. Prefix-Dependent [FGG +20].
presence [Dow15, Sch08]. preserving
[ZN20]. prime [CDK18, Hin08, TKF +20].
primes [ACP10, FS09, vzGS13]. primitive
[SS09, Yoo15]. primitives
[BFJN20, CDN18]. Principal [LPS20].
Privacy [ZN20]. Privacy-preserving
[ZN20]. private
[DGG +15, HL10, KU20, SW07a].
Probability [DR07]. Problem
[CCH +20, HJKTP20, LPS20, BT12, BBGS19,
Bla09, BJa010, HS2020, Kus18, NV08].
problems [BCSV20, HS08, KM08, TKF +20].
Proceedings [CLS20, CLY20]. processes
[SW07a]. Processing [BCIV20]. Product
[DKKS20, MP20, OS14]. products [AL11].
proof [Kar20a, Kar20b, NP19, PSU13, PSU18].
proof-of-retrievability [PS13].
properties [CJST16, ZMD20]. Protecting
[Joy20]. protocol [CWZ12, KU18, KU20,
LU08, MU10, SW07b, jWW12, WS09].
protocols [AK17, BCM11, SW07a]. prover
[PS18]. proving [Kob07, Kob12]. proxy
[SSA17]. Pseudo [Ano20, BGMP08, Pop17].
Pseudo-free [Ano20]. pseudo-random
[Pop17]. pseudorandom [Nan09, vzGS09].
Public
[SvT10, AL11, BCM09, CAR20, CBW07,
GGD20, KNP13, SPSS12, SSS11, WP11].
public-attribute [AL11]. public-key
[CAR20, CBW07, GGD20, SPSS12].
quadratic
[AÖY15, CGK13, HF07, HS08, Jus14, Jus15].
Quantum
[CI14, Eke21, BS19, BP20,
BBP +20, CJS14, DJP14, JLLRL20].
quantum-resistant [DJP14]. quartic
[AJZT19, DEF14]. Quasi
[HKP +20, Per12].
quasi-dyadic [Per12]. Quasi-subfield
[HKP +20]. quasigroups [CGK13]. query
[SW07a]. quotient [MU08].
Rabin
[Böc09]. Ramanujan [PP18].
Random
[MU08, BGMP08, Pop17]. randomized
[Böc09]. range [YYS +14].
rational [MW12]. ratios [HL19]. RC4
[BGMP08, DS18]. realization [SvT10].
realizing [PS15]. receiver [FHLMW08].
reconstruction [SW07a]. Recovering
[FGG +20]. recovery [BFJT12]. Recursive
[BC12, CL09]. reduced [DT17].
reduced-round [DT17]. reducing [BP20].
reduction [Wun19]. refinement [LS18].
regular [DSG21, MSP12]. relations
[DS18, SPSS12]. relying [BS19]. Remarks
[RM20, FMS09]. repairable [LS18].
representable [BT12]. Representation
[DM20]. representations [CQS11, HM07].
requirements [NSW09]. reset [WS09].
Residue
[JLNN20, CS21]. residues
[JS14, Jus15]. resilient
[Ala17, CAR20, HS15b, KNP13]. resistance
[MSP12]. resistant [DJP14]. restricted
[BBGS19]. results [DS18, SW07a].
Rethinking
[ATW08]. Retraction
[Kar20b]. retrievability [PSU13, PSU18].
retrieval [SW07a]. Revisited
[Joy20, AN20, Laa20, NP16, SS16b].
Revisiting [JN16], rho [BDJ14], Richelot [CDS20], Rigorous [SS17], Ring [DSGKS20b, Joy20, BT12, BGGJ20, DSGKS20a, MP20], Ring-LWE [DSGKS20a, MP20], Ring-LWE-based [BGGJ20], Rings [PGS20, Bis11, JCK+18], Rivest [HV14], RNS [Duq11], robust [JSN13, PS20], Roos [DS18], Root [DM20], rotate [FJ13], Rotation [Rei21, CC15, CLS16], round [BK09, DT17, Mie08, SW15, SW07a], RSA [DSG21, Hin08, HL10, LPS17, MA17], safe [AK17, vzGS13], same [SU14], samples [BBGS19], SAP [GGD20], scheme [HV14, HSWZ20, Maz12, Mul11, PS08, SSA17, SPS19, TL15], Schemes [ BLLN21, BGGJ20, DKKKS20, BPB19, BS19, GD13, HS15a, JSN13, LS18, MFP10, MU14, PS13, PS20, Pou16, SS16b], Schmidt [YYS+17], Schnorr [NSW09], search [MA17, RZ18], Second [CLS20, Gut09], Secret [Csi20, DC14, GD13, HS15a, HL19, JSN13, MFP10, CEM15], Secrets [FGG+20], Secure [Dow15, BK09, CS21, FL08, JSN13, KNP13, Maz12, PSU13, SSA17, SW07b, SW07a, S16b, WS09], Security [FS11, HV14, OPSB13, ACP10, AL11, BBP19, CDGM14, EOS07, GS07, Hin08, MPST16, NM08, Nan09, NP16, SPSS12, DSGKS20a], Self [GZ13, Yas20, GZ14], Self-dual [Yas20], Self-pairings [GZ13, GZ14], Semaev [YYTK20], semigroups [Ci14], Sensitivities [ZLA21], sensor [HS15b, PS08], sequences [AMW07, BW09, LS07], server [LS07a], set [Gal12, MU10], setting [CDK18], seven [DS17], sharing [Csi20, DC14, GD13, HS15a, HL19, JSN13, MFP10], shifted [LU08], Short [LPS20, BS19, YYS+17, Yas20], shortest [NV08], Sibert [MU10], side [Sch08], Sidelnikov [BW09], SIDH [UJ20], SIDH-based [UJ20], Sieve [NV08, Grz20], Sieving [MR20], Sign [TW20], Signature [DSGKS20, HSWZ20, NP16, SS16b], signatures [BDW12, FS11, HS08, NP19, NSW09, Rei17, SVT13, vT18], Signcryption [BBP19, SSA17], SIKE [BP20], Simplified [GOS07], six [GD13], size [AL11, BBP+20], SKENO [CEM15], small [HST10, HL19, HL10, Hit09], SNFS [Sill07], solutions [GP13], solve [Zaj13], solver [RZ18], solvers [LRN09], solving [BPB09, Bla09, BDJ14, GP09, MP08, TKF+20], Some [FL08, FSM09, SW07a, AJZT19, BC12, DS18, FS09, HL10, LS07], space [JLLRL20], sparse [AK17, FK18], Special [DSG20, CGK13, FS09], specified [PS15], Square [DM20], squared [YYS+17], squared-sum [YYS+17], squeezing [CDGM14], Srivastava [Par12], standard [KM08], Statistical [BS07], Stickel [Mu11], Stochastic [DSG21, Sch08], storage [PS13], stream [FMS09, Tis11], streams [DG+15], Strict [LC07], Strongly [SVT13, AR15, vT18], structure [DS17, JN16, JSN13], structures [GD13], subexponential [ADPS14, CJS14, JLLRL20], subexponential-time [JLLRL20], subfield [HST10, HKP+20], subgroups [Kar10, MU08], Submission [DSGKS20], subsequences [BW09], Subset [vzGS09], sum [HF07, YYS+17, vzGS09], summary [EOS07], summation [KW19], supersingular [CK20, DP14, GPRS09], superspecial [CDS20], support [AL11], Survey [GGD20, LS18], Symbol [JLNN20], symbols [CS21], Symmetric [Rei21, CDN18, CLS09, CC15, CLS16, TL15, ZLA21], System [RM20, NP19], systems [BPB09, Mie08, WP11, Zaj13], Takes [TW20], Tame [Rei17], technique [NP19], Techniques [UJ20], terms [FM13], test [Boc09], th [DSS20], their [EOS07].
Theorem [Kar20b, CLS16, Kob07, Kob12, Kar20a].
theorem-proving [Kob07, Kob12].
theoretic [BFJN20, JP20]. Theory [CC15, GPR17, PSU13]. 
theta [Gau07].
Thompson [RST07]. Three [MR20, BCM11]. threshold [JSN13, LS18, PS20].
Tillich [TNS20].
Time [LL15, TW20, CJS14, JLLRL20].
Time-memory [LL15]. Timing [TW20].
torsion [MW12]. trace [BG16, FM13].
transfer [FS11]. transmission [AL07, Dow15]. Tropical [RM20, KU18].
truncated [FJ13]. trustless [Pop17].
twisted [BG16, BDFM21]. Two [LMPW15, PS08, GPRS09, Mie08, SW07b].
two-flow [SW07b].
two-permutation-based [LMPW15].
two-round [Mie08]. TWOOA [FHLMW08]. Type
[TNS20, AJZT19, EOS07, Jus14, Jus15].
unbounded [DGG15]. uncloaking [KMU20]. Unconditionally [JSN13, SS16b, PSU13, SW07a].
Unconditionally-secure [JSN13].
universal [ACP10, Ano20]. upper [SS17].
use [BP20]. Using [FJ13, Rei21, BBB+18, BF09, CDS20, FK18, Kus18].
v1.3 [BLLN21]. Valued [BCIV20]. values [Oka12]. Vandermonde [DSS20]. variant
[CCH+20, Gr20, LPS17]. variants [HL10, Mul11]. vector [NV08]. vectors
[BF09, YYS+17, Yas20]. verifiable [ZSN20].
via [CS21, DM20, NP19]. view [MP08].
Volume [CLS20, CLY20]. Voronoi [Laa20].
VSH [BS07].
way [PS15]. weak [AÖY15, BFJT12].
weight [FS08, HM07]. weighted [HS15a].

weights [BC12]. Weil [HF07, KMPS10].
Weng [Yoo15]. wide [MPST16]. witnesses
[PR20]. Witt [BF09]. Workshop [Gut09].
xor [FJ13].
Zémor [TNS20]. zero [BG16, DT17, SW07b].
zero-knowledge [SW07b].

References

AlMashrafi:2013:IMI

Alomair:2010:PPS

Asghar:2014:SCG
REFERENCES

**Antal:2017:MCP**


**Azizi:2019:CIC**


**Asghar:2017:WIP**


**Attrapadung:2011:FEP**


**Alawatugoda:2017:LRK**


**Aly:2007:ELC**


**Araujo:2020:CHR**

REFERENCES

Anonymous:2013:M

Anonymous:2017:F

Anonymous:2018:Fa

Anonymous:2018:Fb

Anonymous:2018:Fc

Anonymous:2018:Fc

Anonymous:2019:Fa

Anonymous:2019:Fb
REFERENCES


Anonymous:2019:F


Anokhin:2020:PFF


Alam:2015:CWD


Albrecht:2015:CHL


Accardi:2015:CSA


AlMahri:2018:FF


Avanzi:2008:RLG

REFERENCES

Banegas:2018:DKE


Bindel:2019:EHL


Banegas:2020:DED


Biasse:2020:TBC


Bansal:2019:SSI

REFERENCES


REFERENCES


[BGK+20] Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Alice Silverberg, Mehdi Tibouchi, and Mark Zhandry. Multiparty non-interactive key exchange and more from isogenies on ellip-


Choi:2007:CHP


Cusick:2015:TRS


Cheon:2020:ACV


Carlet:2014:LSO

Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Magharebi. Leakage squeezing: optimal implementation and security evaluation.

Chatterjee:2018:CPB


Chakraborti:2018:ONL


Castryc:2020:HFS


CDG14

Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Magharebi. Leakage squeezing: optimal implementation and security evaluation.
REFERENCES

19

19

Chen:2015:SSK


Coron:2020:ICA


Chen:2013:SCM


Childs:2014:QCD


Childs:2014:CEC


Carlet:2016:CPM


Colo:2020:OSI

REFERENCES


REFERENCES


REFERENCES


Delaplace:2020:CWB


Demirkiran:2008:CHC


Dowden:2015:SMT


Daemen:2007:PDC


Dehkordi:2017:CCG


Dey:2018:GRB


Doroz:2020:FNE


Dugardin:2021:SMD


**Dachman-Soled:2020:SRL**


**Dachman-Soled:2020:TRA**


**DiScala:2020:CNV**


**Duquesne:2011:RAA**


**Ekerå:2021:QAC**


**Engelbert:2007:SMT**


**Ferradi:2020:RSP**


**Fuji-Hara:2008:TCM**


**Field:2013:UCT**


**Fotiadis:2018:GPF**


**Fancsali:2008:SAF**


**Flori:2013:ECF**


**Fischer:2009:SRF**

Simon Fischer, Willi Meier, and Dirk Stegemann. Some remarks on FCSRs and implica-
REFERENCES


David Garber, Delaram Kahrobaei, and Ha T. Lam. Length-based

Galbraith:2007:SPC


Galbraith:2009:DMS


Gaal:2009:SNE


Grzeskowiak:2020:VLS


Gutierrez:2009:FSW


Gupta:2017:ADT


Grozek:2013:CS

Otokar Grošek and Štefan Porubský. Coprime solutions to \( ax \equiv b \pmod{n} \). *Journal of Mathematical Cryptology*, 7(3):217–224, 2013. CODEN ????. ISSN 1862-2976 (print), 1862-2984 (electronic).

Gutierrez:2009:FSW

S. D. Galbraith and Chang-An Zhao. Self-pairings on hyperelliptic curves. *Journal of Math-
REFERENCES


REFERENCES


Heuberger:2007:MWC


Hartung:2008:ISB


Hameed:2015:CIW


Henry:2015:LAR


Hakuta:2010:EAS


Hoffstein:2020:SSF


Haridas:2014:SAM


Hisil:2011:EAG


**Jirakitpuwapat:2018:NMC**


**Jiang:2014:PAP**


**Jao:2020:STP**


**Joye:2020:PEA**


**Jha:2016:RSG**


**Joye:2020:EPR**

REFERENCES

Joux:2020:PNT


Jhanwar:2013:USI


Justus:2014:DQR


Justus:2015:DQR


Wei:2012:FMP


Karabina:2010:FCC


Karmakar:2020:EPF


Karmakar:2020:REP

Kortelainen:2010:MAG


Koblitz:2008:ALN


Koblitz:2013:ALH


Kaji:2019:PEP


Karabina:2010:AEW


Kotov:2020:AKP


Kurosawa:2013:NLR


Koblitz:2007:ALA


REFERENCES

Li:2007:SAC


Lamberger:2009:NSC


Lavauzelle:2019:GCP


Laine:2015:TMT


Lesavourey:2020:SPI


Luykx:2015:TPB


Lu:2017:CR


Lange:2007:DSS


References


[MU10] Natalia Mosina and Alexander Ushakov. Mean-set attack:

**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


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Issue</th>
<th>Pages</th>
<th>Year</th>
<th>DOI</th>
<th>URL</th>
</tr>
</thead>
</table>

**References:**

- Paterson:2013:CTF
- Paterson:2018:MPP
- Reid:2021:UIE
- Raddum:2018:MSB
- Schindler:2008:ASM

Scholl:2017:IEC


Sha:2014:NIC


Shokrieh:2010:MPD


Sica:2020:FH


Silverman:2007:OPS


Sipasseuth:2019:EGG


Sepahi:2012:NSN


Saxena:2009:CPB

REFERENCES


REFERENCES

Stinson:2007:SRQ


Stinson:2007:EST


Sparr:2015:RFK


Tischhauser:2011:NCA


Tassa:2013:OEM


Takahashi:2020:AAS


Tsaban:2015:CMS


Tomkins:2020:NZT

[Hayley Tomkins, Monica Nevins, and Hadi Salmasian. New Zémor–Tillich type hash functions over $\text{GL}_2(F_p)$. *Journal of Mathematical Cryptology*, 14(1):]
REFERENCES


REFERENCES

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


REFERENCES


**Yokoyama:2020:CBS**


**Zajac:2013:NMS**


**Zhang:2021:SBS**


**Zhou:2020:CPB**


**Zhang:2020:PPV**