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/  
22 June 2017  
Version 1.01

**Title word cross-reference**

\((p^r - 1)/3\) [BW09]. 1 [SW07a]. 2  
[Gau07, Hit09, SW07a]. 3  
[CC15, LL15, MW12]. 4 [Kar10]. 6 [Kar10].  
\(ax \equiv b \pmod{n}\) [GP13].  
[AMW07, BW09]. \(F_{24m}^*\) [Kar10]. \(F_{36m}^*\) [Kar10]. \(F_p\) [BW09]. \(F_{pk}\) [Duq11]. \(M\)  
[WP11]. Q [WP11]. MST_3 [BCM09].  
\(N = p^r q^t\) [LPS17]. \(\rho\) [Oka12]. MST_3 [SvT10].

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

256 [DT17].

7 [GZ14].

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].  
Affine [CLS16, HWCD11]. against  
[MSP12, WS09]. aggregation [HS15b].  
Agrawal [PS08]. agreement [Mul15]. al.  
[MU10]. *Algebraic* [BF09]. algorithm  
[BGMP08, BDJ14, Pop17]. algorithms  
[AR15, FJ13, NV08]. alternating [SW15].  
Analysis  
[KU15, Maz12, YYS+17, HVV14, MU08,  
NM08, Nan09, OPSB13, PSU13, Sch08].  
analyze [FJ13]. anonymous [SSA17].

class [AR15, CGK13]. Classes [AOY15, WL13]. cloud [PSU13].


correlation [DR07, DT17]. corresponding [BFJ12]. Counting [DN08, WL13].
criterion [LC07]. critical [Bla09]. Cryptanalysing [Bla09, Mul11, Bla10].

Cryptanalysis [BCM09, CBW07, CLS09, CC15, CLS16]. cubic [CC15]. cumulative [MN07]. curve [CJS14, CQS11, DPP14]. curves [BG16, Bis11, Box12, DN08, DEF14, FSV09, GPRS09, GZ13, GZ14, HST10, HWC11, Hit09, LS07, MW12, Mor08, Oka12, Sha14, Yoo15].
cyclotomic [AMW07, Kar10, Sha14].
data [SU14]. decentralized [Pop17]. decreasing [YYS17].
decryption
degree [Hit09], Dembowski [AÖY15], density [FS09], descent [KMP10], design [GPR17], differential [DT17], differential-zero [DT17], differentials [DR07], Diffie [KM08], discrete [BT12, Bla09, Bla10, BDJ14, CI14, Gal12, KM08, Sho10], disguised [Mor08], distinguisher [Gal12], Distortion [GPRS09], distributed [DGG+15], Distribution [LS07, BS07, Jus14, Jus15, Maz12, PS08, vzGS09], distributions [DR07], dragon [SSS11], DSA [Pou16], dyadic [Per12], Edwards [BG16], effect [Mur12], effectiveness [KMP10, Mur12], Efficient [DEF14, HST10, DGG+15, FM13, SSS11, SW07b, WS09], efficiently [Bla09], elements [Yoo15], elliptic [Bis11, Box12, CSJ14, CQS11, DJP14, DEF14, FSV09, HST10, HWCD11, LS07, MW12, Mor08, Oka12, Sho14, Yoo15], EMAC [JN16], embedding [Hit09], encryption [AL07, AL11, CEM15, KNP13, NP16, SPSS12, TL15, YYS+14], endomorphism [Bis11], EPIR [CWZ12], equation [MP08, Zaj13], equations [GP09], equivalence [CLS16, WL13], Equivalent [BP11], Erratum [GZ14], error [AMW07, BW09], errors [APS15], establishment [BCM11], evaluation [CDGM14, CWZ12, TJBY13], evolution [BGMP08], exact [YYS+14], examples [DC14], exchange [Jia14], existence [WC07], expansions [FS08], explicit [ATW08], exploration [HWCD11], exponent [HL10], exponents [Boc09], extracting [SU14],

Factor [Kar10], Factor- [Kar10], factorization [Zaj13], Families [Hit09, MW12, CL09, Oka12, Sho14, WC07, Yoo15], family [ACP10, BFJT12, FM13], Fast [Gau07, OS14, Duq11, HL09, HL10, MPST16, jWW12, vzGS09], FCSRs [FMS09], field [ATW08], fields [ATW08, BFP09, GP09, HST10, LC07], filtered [OPS13], Finding [Gal12], finite [BFP09, CBW07, FL08, HST10, LC07, Sho10], flow [SW07b], Foreword [Gut09, Mag13], forms [HS08], formulae [ATW08], foundation [PSU13], friendly [Box12, Oka12, Sho14, Yoo15], Frontmatter [Ano17], fully [Dow15, TL15, YYS+14], function [ACP10, GP09, Nan09, NW09, PS15], Functional [AL11], functions [BC12, CJST16, CLS09, CC15, CLS16, FM13, Gau07, KHK10, MSP12, OS14, SW15, SW07a],
general [PSU13], generalised [Dow15, MN07], generalized [HKH10], generate [SW15], Generating [vzGS13], generation [ABD+13, BGMP08, Pop17, vzGS09], Gentry [YYS+14], genus [ATW08, GPRS09, Gau07, Hit09, LL15], geometric [MP08], geometry [FL08], global [GP09], Goldwasser [Jus14, Jus15], Gram [YYS+17], graph [ADPS14, DS17, GD13], graphs [JN16, PS15, Sho10], GRH [Bis11], Gröbner [BF09], group [Bla09, CBW07, HWCD11, KU15, RST07, SW15, Zaj13], groups [GLK15, SS09],

Halevi [YYS+14], hard [HS08], hardness [APS15], Hash [NS09, ACP10, CL09, FJ13, KHK10, MPST16, MSP12, OS14, WC07], hash-function [ACP10], hashing [FSV09, LMPW15], Hellman [KM08], Heuristics [Box12], HFE [BFJT12], hidden [SS09], hidden-order [SS09], HMAC [KM13], HMQV [Men07], homomorphic [CBW07, TL15, YYS+14], hull [Mur12], Hybrid [BFP09], hyper
hyper-bent [FM13]. hyperelliptic
[ATW08, DN08, GZ13, GZ14].

ID [PS15]. ID-based [PS15]. ideal
[HS15a, JSN13]. idealness [Sha14].
Identification [HS08, SW07b, WS09]. II
[Jus15, Kob12]. implementation
[CDGM14, YYS+14]. implications
[FMS09, GOS07]. Improved
[NM08, Nan09]. increased [MSP12].
ideality [HS15a, JSN13]. idealness
[Sha14]. Identification
[HS08, SW07b, WS09]. II
[Jus15, Kob12]. implementation
[CDGM14, YYS+14]. implications
[FMS09, GOS07]. Improved
[NM08, Nan09]. increased [MSP12].

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]. iterated [KHK10].

KASUMI [SW15]. key
[BCM09, BCM11, BFJT12, CEM15, CBW07,
Jia14, KNP13, Maz12, Mul11, PS08, PS15,
SPSS12, SS11, SvT10, TL15, WP11].
key-recovery [BFJT12]. keys
[BFJT12, Per12, WP11]. knowledge
[SW07b]. Koblit [DN08].

lattice [Pou16, YYS+17]. laws [HWCD11].
Leakage [CDGM14, KNP13].
leakage-resilient [KNP13]. learning
[APS15]. Length [GKL15, RST07, MU08].
Length-based [GKL15, RST07, MU08].
lengths [YYS+17]. lightweight
[GP09].

Linear
[HS15b, AMW07, BW09, DT17, Mur12].
linearly [OPS13]. log [KM08]. logarithm
[BT12, Bla09, Bla10, Sho10]. logarithmic
[BdW12, SvT13]. logarithms
[BDJ14, CI14, Gal12]. look [HL09, Kob07,
KM08, Kob12, KM13, Men07, SS16a]. low
[ATW08].

MAC [ABD+13, JN16]. maps [GPRS09].
mapping [Sch08]. Masthead [Ano13].
Math. [GZ14]. Mathematical [Gut09].
matrix [BCM11, MU14]. matrix-based
[BCM11]. matroids [MFP10]. McEliece
[EOS07, Per12]. McEliece-type [EOS07].
MDS [GPR17]. Mean [MU10]. Mean-set
[MU10]. memory [LL15]. mental [jWW12].
method [WL13, Yoo15, Zaj13]. methods
[HL09, Sch08]. Micali [Jus14, Jus15].

Mickey [Tis11]. Miller [Böc09].
Minimal [FS08, HM07]. mixing
[LMPW15]. mnemonic [AGH17]. model
[DN08]. modified [HVX14]. modular
[HL09]. moduli [LPS17]. modulo [Blal0].
modulus [HL10]. monodromy [Sho10].
monomial [CLS16]. monotone [CJS16].
MQSs [CJS16]. MR3101014 [GZ14].
MRHS [Zaj13]. multi [FHLMW08, Hin08].
multi-message [FHLMW08]. multi-prime
[Hin08]. multi-receiver [FHLMW08].
multiplying [FHLMW08].
multicasting [Maz12]. Multicollision
[KHK10]. multilevel [JSN13]. multiparty
[ADPS14]. Multiple [DT17, FM13].
multivariate [AY15, BF09, CGK13,
HF07, SS11, TJB13].

negation [AL11]. network [FL08, PS08].
networks [HS15b]. NLFSRs [OPS13].
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 [Pop17, WL13]. numbers
[vzGS09]. Numerical [LNR09].

Oblivious [TJB13, FS11]. odd [HST10].
offs [LL15]. OMAC [Nan09]. One
One-round [BK09].

One-way function [PS15].

Opening [CEM15].

Optimal [PS15, Si07, CDGM14].

Orbit [Gal12].

Order [SS09].

Ostrom [AOY15].

Overhead [AL07].

Pairing [Box12, Duq11, GÓS07, Oka12, Sha14, Sh010, Yoo15].

Pairing-friendly [Box12, Oka12, Sha14, Yoo15].

Pairs [DEF14, GZ13, GZ14].

Parameterization [Si07].

Participants [DS17, GD13].

Password [Jia14].

Password-based [Jia14].

Perfect [GD13, CL09, WC07].

Permutation [LMPW15].

Permutations [AGH17].

Persistent [Jia14].

Pipe [MPST16].

PKA [AR15].

PMAC [NM08].

Points [BG16, LS07].

Poker [jWW12].

Pollard [BDJ14].

Poly [CLS16].

Polycyclic [GKL15, KU15].

Polycyclic-group-based [KU15].

Polynomials [CWZ12, WL13].

Polynomials [Jus14, Jus15].

Polynomials [ACP10].

Power [ACP10].

Practical [BFJT12, NV08].

Practice [HL10].

Predistribution [PS15].

Presence [Dow15, Sch08].

Prime [Hin08].

Primes [ACP10, FS09, vzGS13].

Primitive [SS09, Yoo15].

Public [SvT10, AL11, BCM09, CBW07, KNP13, SPSS12, SSS11, WP11].

Public-attribute [AL11].

Public-key [CBW07, SPSS12].

Quadratic [AOY15, 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 [Böe09].

Randome [Böe09].

Range [YYS+14].

Rational [MW12].

RC4 [BGMP08].

Realization [SvT10].

Realizing [PS15].

Receiver [FHLMW08].

Reconstruction [SW07a].

Recovery [BFJT12].

Recursive [BC12, CL09].

Reduced [DT17].

Reduced-round [DT17].

Regular [MSP12].

Relations [SPSS12].

Remarks [FMS09].

Representable [BT12].

Representations [CQS11, HM07].

Requirements [NSW09].

Reset [WS09].

Residues [Jus14, Jus15].

Resilient [HS15b, KNP13].

Resistance [MSP12].

Resistant [DJP14].

Results [SW07a].

Rethinking [ATW08].

Retrieval [SvT10].

Rivest [HVV14].

RNS [Duq11].

Robust [JSN13].

Rotate [FJ13].

Rotation [CC15].

Round [BK09, DT17, Mie18, SW15, SW07a].

RSA [Hin08, HL10, LPS17].

Safe [vzGS13].

Same [SU14].

Scheme [HVV14, Maz12, Mul11, PS08, SSA17, TL15].

Schemes [GD13, HS15a, JSN13, MFP10, MU14, PSU13, PS15, Pou16, SS16b].

Schmidt [YYS+17].

Schnorr [NSW09].

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, GÖS07, 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]. seven [DS17].
sharing [DC14, GD13, JSN13, MFP10]. shifted
[LU08]. short [YYS+17]. shortest
[NV08]. Sibert [MU10]. side [Sch08].
Sidelnikov [BW09]. Sieve [NV08].
signature [NP16, SS16b]. signatures
[BdW12, FS11, HS08, SW09, SvT13].
signcryption [SSA17]. Simplified [GÖS07].
six [GD13]. size [AL11]. SKENO [CEM15].
small [HST10, HL10, Hit09]. SNFS [Sil07].
solutions [GP13]. solve [Zaj13]. solvers
[LNR09]. solving [BF09, Bla09, BDJ14, GP09, MP08]. Some
[FL08, FMS09, Sw07a, BC12, FS09, HL09, HL10, LS07]. special [CGK13, FS09]. specified [FS15]. squared [YYS+17].
squared-sum [YYS+17]. squeezing [CDGM14]. Srivastava [Per12]. standard
[KM08]. Statistical [BS07]. Stickel
[Mul11]. stochastic [Sch08]. storage
[PSU13]. stream [FMS09, Tis11]. streams
[DGG+15]. Strict [LC07]. Strongly
[SvT13, AR15]. structure
[DS17, JN16, JSN13]. structures [GD13].
subexponential [ADPS14, CJS14].
subfield [HST10]. subgroups
[Kar10, MU08]. subsequences [BW09].
Subset [vzGS09]. sum
[HF07, YYS+17, vzGS09]. summary
[EOS07]. supersingular [DPJ14, GPRS09].
support [AL11]. symmetric
[CLS09, CC15, CLS16, TL15]. systems
[BFF09, Mic08, WP11, Zaj13].
terms [FM13]. test [Böc09]. their
[EOS07]. theorem [CLS16, Kob07, Kob12].
theo}\n
References

AlMashrafi:2013:IMI


Joppe W. Bos, Alina Dudeanu, and Dimitar Jetchev. Collision bounds for the additive Pol-

Baumeister:2012:ALS


Bourgeois:2009:AAN


Bouillaguet:2012:FWK


Bettale:2009:HAS


Bianco:2016:CTZ


Basu:2008:CCE


Bisson:2011:CER


Blake:2009:ORS

REFERENCES


REFERENCES


REFERENCES


**[Dowden:2015:SMT]**


**[Duq11]**


**[DR07]**


**[Duquesne:2011:RAA]**


**[EOS07]**


**[FJ13]**

Rebecca E. Field and Brant C. Jones. Using carry-truncated addition to analyze add-rotate-xor hash algorithms. *Journal of Mathematical Cryptology*, 7
REFERENCES


REFERENCES


Gharahi:2013:PSS

Garber:2015:LBA

Galbraith:2007:SPC

Gaal:2009:SNE

Grosek:2013:CS

Gupta:2017:ADT

Galbraith:2009:DMS

Gutierrez:2009:FSW

**Galbraith:2013:SPH**


**Galbraith:2014:ESP**


**Harayama:2007:WSB**


**Hinek:2008:SMP**


**Hitt:2009:FGC**


**Hinek:2009:ALS**


**Hinek:2010:CMA**


**Heuberger:2007:MWC**


**Hartung:2008:ISB**

Rupert J. Hartung and Claus-Peter Schnorr. Identification

**Hameed:2015:CIW**


**Henry:2015:LAR**


**Hakuta:2010:EAS**


**Haridas:2014:SAM**


**Hisil:2011:EA**


**Jiang:2014:PAP**


**Jha:2016:RSG**


**Jhanwar:2013:USI**

REFERENCES

Justus:2014:DQR


Justus:2015:DQR


Wei:2012:FMP


Karabina:2010:AEM


Kurosawa:2013:NLR

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


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

Longrigg:2008:CSC

Magliveras:2013:F

Maze:2012:AKD

Menezes:2007:ALH

Marti-Farré:2010:SSS

Mie:2008:PTR

Martin:2007:CGC

Morales:2008:ADE

Murphy:2008:GVC

Moody:2016:ISF
Dustin Moody, Souradyuti Paul, and Daniel Smith-Tone. Indif-


Mridul Nandi. Improved security analysis for OMAC as a

**Nandi:2008:ISA**


**Nandi:2016:SJS**


**Neven:2009:HFR**


**Nguyen:2008:SAS**


**Okano:2012:VCF**


**Orumiehchiha:2013:SAL**


**Omar:2014:FHF**


**Persichetti:2012:CMK**


[Sho10] Farbod Shokrieh. The monodromy pairing and discrete logarithm on the Jacobian of finite
Silverman:2007:OPS


Sepahi:2012:NSN


Saxena:2009:CPB


Samajder:2016:ALN


Swanson:2016:USS


Saraswat:2017:SAP


Singh:2011:PDE


Stinson:2014:EDS

Svaba:2010:PKC


Staszewski:2013:SAL


Stinson:2007:SRQ


Stinson:2007:EST


Sparr:2015:RFK


Tischhauser:2011:NCA


Tassa:2013:OEM


Tsaban:2015:CMS


von zur Gathen:2009:SSP

[vzGS09] Joachim von zur Gathen and Igor E. Shparlinski. Subset


Zajac:2013:NMS