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/

09 October 2019
Version 1.05

**Title word cross-reference**

- (2, 2) [AJZT19]. \((p^r - 1)/3\) [BW09]. 1
- 3 [CC15, LL15, MW12]. 4 [Kar10]. 5 [HL19].
- \(ax \equiv b \pmod{n}\) [GP13]. \(k\)
- \(\mathbb{F}^*_{24m}\) [Kar10]. \(\mathbb{F}^*_{36m}\)
- [Kar10]. \(\mathbb{F}_p\) [BW09]. \(\mathbb{F}_{pk}\) [Duq11]. \(Q(\zeta_{2s})\)
- 7 [GZ14].

- abelian [Rei17]. aborts [FS11]. Abu
- add [FJ13]. add-rotate-xor [FJ13].
- addition [FJ13]. additive [BDJ14]. admit
- [DN08]. Advanced [Sch08]. adversary [Dow15]. AE [ASB+18]. Affine
- [CLS16, HWCD11]. against
- [BS19, MSP12, WS09]. aggregation
- [HS15b]. Agrawal [PS08]. agreement
- [Mul11, al. [MU10]. algebra [KU18, RZ18].
- Algebraic [BF09, Par18]. algorithm
- [BGMP08, BDJ14, Pop17]. algorithms
- [AR15, FJ13, NV08, PP18]. alternating
Analysis [KU15, KU18, Maz12, YYS+17, CDK18, HVV14, MU08, NM08, Nan09, OPSB13, PSU13, Sch08, Wun19].

analyze [FJ13]. anonymous [SSA17]. Aperiodic [BdW12, SvT13, vT18].


breaking [MPST16]. Brezing [Yoo15]. Bringer [CWZ12]. broadcast [AL07].


critical [Bl09]. Cryptanalysing [Bl09, Mul11, Bl09]. Cryptanalysis [BCM09, BCM11, CBW07, LU08, LPS17, MU14, TL15, DT17, LNR09, MU10, RST07, SS16a, SS17, SvT10, Tis11]. Cryptographic [CJS16, MP08, SS09].

Cryptography
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].

cycloptomic [AMW07, Kar10, Sha14].

DAGS [BBB+18]. data [SS17, SU14].

decentralized [Pop17]. decreasing

[YYS+17], decryption [YYS+14]. degree

[Hit09, KW19]. Dembowski [AÖY15].

density [FS09], descent [KMPS10]. design

[GP17]. detailed [Wum19]. differential

[DT17], differential-zero [DT17].

differentials [DR07]. Diffie

[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].

dual [NP19]. dyadic [BBB+18, Per12].

Edwards [BG16]. effect [Mur12], effectiveness [KMPS10, Mur12]. Efficient

[DEF14, HST10, DGG+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].

capsulation [BBB+18]. encodings

[NP19]. encryption

[ASB+18, AL07, AL11, CEM15, KNP13, NP16, SPSS12, TL15, YYS+14].

decomorphism [Bis11]. Enhancing

[SPS19]. EPIR [CWZ12]. equation

[MP08, Zaj13]. equations [GP09].

equivalence [CLS16, WL13]. Equivalent

[WP11]. Erratum [GZ14]. error

[AMW07, BW09]. errors [APS15, BBGS19].

establishment [BCM11]. Estimation

[BBGS19]. evaluation

[CDGM14, CWZ12, TJBYY13]. evolution

[BGMP08]. Exact [HL19, YYS+14].

examples [DC14]. exchange

[Ala17, Jia14, KW18, Par18]. exhaustive

[RZ18]. existence [WC07]. expansions

[FS08]. explicit [ATW08]. exploration

[HWCD11]. exponent [HL10]. exponents

[Boc09]. expressions [KMNN19].

extracting [SU14].

Factor [Kar10]. Factor-

[Kar10]. factorization [Zaj13]. fall [KW19].

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, AJZT19, BFP09, GP09, HST10, LC07]. filtered [OPSB13]. Finding

[Gal12, BS19, PP18]. finite

[BFP09, CBW07, FL08, HST10, JCK+18, Kus18, LC07, Sho10]. first [KW19]. flaw

[ASB+18]. flow [SW07b]. Foreword

[Gut09, Mag13]. forms [HS08]. formulæ

[ATW08]. formulas [MA17]. foundation

[PSU13]. friendly

[Box12, FK18, Oka12, Sha14, Yoo15].

Frontmatter [Ano17, Ano18d, Ano18a, Ano18b, Ano19c, Ano19a, Ano19b].

fully [Dow15, TL15, YYS+14]. function

[ACP10, GP09, Nau09, NS09, PS15].

Functional [AL11]. functions

[BC12, CJST16, CL09, CC15, CLS16, FM13, Gau07, KMNN19, KHK10, MSP12, NPP18, SSS12, TL15, YYS+14].
general [PSU13]. Generalization [Dow15, MN07]. Generalization [DS18, Par18]. Generalized [KHK10].
generate [SW15]. Generating [FK18, vzGS13]. generation [ABD+13, BGMP08, Pop17, vzGS09].
generator [BS19]. Generic [LdV19].
Gentry [YYS+14]. genus [ATW08, GPRS09, Gau07, Hit09, LL15].
geometric [MP08]. geometries [JCK+18]. geometry [FL08]. girth [HL19].
graph [ADPS14, DS17, GD13]. graphs [HL19, JN16, PS15, PP18, Sho10]. GRH [Bis11].
Gröbner [BF09]. group [Blu09, CBW07, HWCD11, KU15, Kus18, RST07, SW15, Zaj13].
groups [GKL15, Rei17, SS09]. GS [BBB+18].

Halevi [SPS19, YYS+14]. hard [HS08]. hardness [APS15, BS19, BBGS19]. 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 [BFJT09, Wun19].
hyper [FM13]. hyper-bent [FM13]. hyperelliptic [ATW08, DN08, GZ13, GZ14].

ID [PS15]. ID-based [PS15]. ideal [AJZT19, BBP19, BS19, HS15a, JSN13].
idealness [Sha14]. Identification [HS08, AK17, SW07b, WS09]. II [Jus15, Kob12]. implementation [CDGM14, YYS+14]. implications [FMS09, GÓS07]. improve [MA17].
Improved [Kus18, NM08, Nan09]. increased [MSP12]. indefinite [HS08].
index [LL15]. Indifferentiability [MPST16]. Indirect [ABD+13]. Infinite [DC14]. information [HL19, SW07a].
instantiations [LdV19]. integer [HM07]. integers [BK09]. interactive [CEM15].
interplay [ATW08]. intersecting [SPS19].
isogenies [CJS14, DJP14]. Isolated [Sch17]. iterated [KHK10].


KASUMI [SW15]. Key [BBB+18, Ala17, BCM09, BCM11, BFJT12, CDN18, 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]. Kobitz [DN08].
lattice [Pou16, Wun19, YYS+17].
leakage-resilient [Ala17, KNP13]. learning [APS15, BBGS19]. least [HL19].
Length [GKL15, RST07, MU08]. Length-based [GKL15, RST07, MU08]. lengths [YYS+17].
lightweight [GPR17]. Linear [HS15b, AMW07, BW09, CDN18, DT17, Mur12, RZ18]. linearly [OPS13]. log [KM08]. logarithm [BT12, Blu09, Bla10, Sho10]. logarithmic [BdW12, Rei17, SvT13, vT18]. logarithms [BDJ14, CI14, Gal12]. look [HL09, Kob07, KM08, Kob12, KM13, Men07, SS16a]. low [ATW08]. lower [Kus18]. LPS [PP18].


Probability [DR07]. problem
[BT12, BBGS19, Bla09, Bla10, Kus18, NV08].
problems [HS08, KM08]. processes
[SW07a]. product [OS14]. products
[AL11]. proof [NP19, PSU13, PSU18].
proof-of-retrievability [PSU13].
properties [CJST16]. protocol
[CWZ12, KU18, LU08, MU10, SW07b, jWW12, WS09].
protocols [AK17, BCM11, SW07a]. prover [PSU18].
proving [Kob07, Kob12]. proxy [SSA17].
pseudo [BGMP08, Pop17].
pseudo-random [Pop17]. pseudorandom
[Nan09, vzGS09]. Public
[SvT10, AL11, BCM09, CBW07, KNP13, SPSS12, SS11, WP11]. public-attribute
[AL11]. public-key [CBW07, SPSS12].

quadratic
[AÖY15, CGK13, HF07, HS08, Jus14, Jus15].
Quantum [CI14, BS19, CJS14, DJP14].
quadratic-resistant [DJP14]. quartic
[AJZT19, DEF14]. quasi [Per12].

quasi-dyadic [Per12]. quasigroups
[CGK13]. query [SW07a]. quotient
[MU08].

Rabin [Boc09]. Ramanujan [PP18].
Random [MU08, BGMP08, Pop17].
randomized [Boc09]. range [YYS+14].
rational [MW12]. ratios [HL19]. RC4
[BGMP08, DS18]. realization [SvT10].
realizing [PS15]. receiver [FHLMW08].
reconstruction [SW07a]. recovery
[BFJT12]. Recursive [BC12, CL09].
reduced [DT17]. reduced-round [DT17].
reduction [Wan19]. refinement [LS18].
regular [MSP12]. relations
[DS18, SPSS12]. relying [BS19]. remarks
[FMS09]. repairable [LS18]. representable
[BT12]. representations [CQS11, HM07]. requirements
[NSW09]. reset [WS09]. residues
[Jus14, Jus15]. resilient
[Ala17, HS15b, KNP13]. resistance
[MSP12]. resistant [DJP14]. restricted
[BBGS19]. results [DS18, SW07a].
Rethinking [ATW08]. retrievability
[PSU13, PSU18]. retrieval [SW07a].
revisited [NP16, SS16b]. Revisiting
[JN16]. rho [BDJ14]. Rigorous [SS17]. ring
[BT12]. rings [Bis11, JCK+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].
samples [BBGS19]. scheme [HVV14, Maz12, Mul11, PS08, SSA17, SPS19, TL15].
schemes
[BBP19, BS19, GD13, HS15a, JSN13, LS18, MFP10, MU14, PSU13, PS15, P16, SS16b].
Schmidt [YYS+17]. Schnorr [NSW09].
search [MA17, RZ18]. Second [Gut09].
secret [DC14, GD13, HS15a, HL19, JSN13, MFP10, CEM15].
Secure [Dow15, BK09, FL08, JSN13, KNP13, Maz12, PSU13, SSA17, SW07b, SW07a].
security
[FS11, HVV14, OPSB13, ACP10, AL11, BBP19, CDGM14, EOS07, GÖS07, Hin08, MPST16, NM08, Nan09, NP16, SS16b].
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, HL19, JSN13, MFP10].
shifted [LU08]. short [BS19, YYS+17].
shortest [NV08]. Siebert [MU10].
side [Sch08]. Sidelnikov [BW09]. Sieve [NV08].
signature [NP16, SS16b]. signatures
[BdW12, FS11, HS08, NP19, NV09, Rei17, SvT13, vT18]. Signcryption
[BBP19, SSA17]. Simplified [GÖS07]. six
[GD13]. size [AL11]. SKENO [CEM15].
REFERENCES


xor [FJ13].

zero [BG16, DT17, SW07b].

zero-knowledge [SW07b].

References

AlMashrafi:2013:IMI


Alomair:2010:PPS

[ACP10] Basel Alomair, Andrew Clark, and Radha Poovendran. The

**Asghar:2014:SCG**


**Antal:2017:MCP**


**Azizi:2019:CIC**


**Asghar:2017:WIP**


**Aravamuthan:2007:ATO**


**Attrapadung:2011:FEP**


**Alawatugoda:2017:LRK**

REFERENCES

Aly:2007:ELC


Anonymous:2013:M


Anonymous:2017:F


Anonymous:2018:Fa


Anonymous:2018:Fb


Anonymous:2018:Fc


Anonymous:2018:Fd


Anonymous:2019:Fa

REFERENCES


REFERENCES

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

Baumeister:2012:ALS

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

Bourgeois:2009:AAN

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

Bouillaguet:2012:FWK

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

Bettale:2009:HAS


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

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

Basu:2008:CCE

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

Bisson:2011:CER

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

Blake:2009:ORS

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

Blackburn:2009:CCG


Blackburn:2010:DLP


Bockle:2009:MRT


Boxall:2012:HPF


Blake:2007:SDC


Biassse:2019:QAA


Banin:2012:DLP


Brandstatter:2009:ELC

BW09] Nina Brandstätter and Arne Winterhof. k-error linear complexity over $\mathbb{F}_p$ of subsequences of Sidelnikov sequences of period $(p^r - 1)/3$. *Journal of

Choi:2007:CHP


Cusick:2015:TRS


Carlet:2014:LSO


Chatterjee:2018:CPB


Chakraborti:2018:ONL


Chen:2015:SSK


Chen:2013:SCM


Dibert:2014:ISS

Duquesne:2014:ECP

Dolev:2015:TEP

DeFeo:2014:TQR

Demirkiran:2008:CHC

Dowden:2015:SMT

Daemen:2007:PDC

Dehkordi:2017:CCG

Dey:2018:GRB
REFERENCES


Dehkordi:2017:MDZ


Duquesne:2011:RAA


Engelbert:2007:SMT


Fuji-Hara:2008:TCM


Field:2013:UCT


Fancsali:2008:SAF


Flori:2013:ECF

[FM13] Jean-Pierre Flori and Sihem Mesnager. An efficient characterization of a family of hyper-


(1):93, 2014. CODEN ????
ISSN 1862-2976 (print), 1862-2984 (electronic). See [GZ13].


REFERENCES


**REFERENCES**

**Jhanwar:2013:USI**


**Justus:2014:DQR**


**Justus:2015:DQR**


**Wei:2012:FMP**


**Karabina:2010:FCC**


**Kortelainen:2010:MAG**


**Koblitz:2008:ALN**


**Koblitz:2013:ALH**


**Kaji:2019:PEP**

Kotov:2015:ACP

Kotov:2018:AKE

Kushwaha:2018:ILB

Kousidis:2019:FFD
References


REFERENCES


REFERENCES


REFERENCES

Moody:2012:FEC


Nandi:2009:ISA


Nandi:2008:ISA


Nandi:2016:SJS


Nandi:2019:PSP


Neven:2009:HFR


Nguyen:2008:SAS


Okano:2012:VCF


Orumiehchiha:2013:SAL

[OPSB13] Mohammad Ali Orumiehchiha, Josef Pieprzyk, Ron Steinfeld,

Omar:2014:FHF


Pou16


Partala:2018:AGD


Persichetti:2012:CMK


Pinto:2018:BPF


Paterson:2015:OCI


Popov:2017:DTP


Poulakis:2016:NLA

[M. B. Paterson and D. R. Stinson. Optimal constructions for ID-based one-way-function key predistribu-

**Paterson:2013:CTF**


**Paterson:2018:MPP**


**Reichl:2017:TLS**


**Ruinskiy:2007:LBC**


**Raddum:2018:MSB**


**Schindler:2008:ASM**


**Scholl:2017:IEC**

Sha:2014:NIC


Shokrieh:2010:MPD


Silverman:2007:OPS


Sipasseuth:2019:EGG


Sepahi:2012:NSN


Saxena:2009:CPB


Samajder:2016:ALN


Swanson:2016:USS


Samajder:2017:RUB

Subhabrata Samajder and Palash Sarkar. Rigorous upper bounds
REFERENCES


[SvT15] Rüdiger Sparr and Ralph Wernsdorf. The round functions of KASUMI generate the alternating group. *Journal of Math-


Wolf:2011:EKU


Wu:2009:EIP


Wunderer:2019:DAH


Yoon:2015:NMC


Yasuda:2014:EDR


Yasuda:2017:ADS


Zajac:2013:NMS