A Complete Bibliography of Publications in the journal

Groups Complexity 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/

30 November 2019
Version 1.05

Title word cross-reference

{+, −, ×, ÷, &} [Sch16]. 1 [ET16]. 4 [Ore15].
5 [EE17]. 5 × 5 [HHMHM15]. Aut(\(F_n\)) [Ibr12]. F [ERW12, ET16, TY15, Was11].
\(F_m \times Z^n\) [Sah15]. \(\langle m, m, m \rangle\) [HHMHM15].
\(Z_q\) [AGG10]. \(Z_n^*\) [Ano18a]. \(O((\log q)^2)\)
[Sch16]. n [RS14]. p [Ano17a]. \(p^n\) [Iva15]. R
[MZ09]. BS(1, 2) [Mil14].

-braids [Ore15]. -counter [ET16]. -groups
[Ano17a]. -powered [MZ09].

2-dimensional [Asb18].

AAG [Rom19]. abelian [Ano17a, BMV15,
Cle09, Dea09, Eic16, KA09]. action [Ibr12].

Actions [BD09, KMS14]. active [Neu12].
additive [Cle09]. admitting [GLS15].
agreement [CM15, GG19, MU09, Ush16].
algorithm [Bac15, CL13, CJ12, HHHHM15,
MU14, STT11]. Algorithmic
[Ore15, MU11b]. Algorithms
[Loh12, BM11, HM12, Will12]. Almost
[GLS09]. alternative [gRHR09]. amalgams
[FMR09]. analogs [BMV15]. Analysis
[KPU18, GLS15]. Andrews [PU19]. Anshel
[MU09, MU09]. apartments [CL13].
application [GLS15, HHHHM15].
applications [CJ12, KMK19, SS16].
approach [CR16]. arithmetic
[KMK19, Mac09]. Artin [HR13, Kra13].


each [Asb18]. echelon [Ros13]. Effective [KMT19]. elementary [Ano17a, FGRS18, Fri17, GLS15]. elements [Asb18, But17]. elliptic [FC16, Fri17]. embedding [Cho09].

cryptography [GKS18b, Rom15]. endomorphism [FFK11]. Equations [Rom12, CR16, GMR11, KMT19, Tim17].
Key [CM15, Das15, GG19, Eft12, FMR13, GKS18b, GHP09, KA09, KKS13, KT13, MZJ17, MU09, Neu12, Rom15, Rom17, SZ09, Ush16]. Key-escrow [Das15]. Knapsack [MT17].


one [Bac15, GS13, Mya09]. one-way [GS13, Mya09]. open [DK16]. operations [Sch16]. orbit [Ven14]. order [Asb18]. Orderable [FGRS18]. ordered [She16]. orderings [Ito10]. oriented [Bac15]. oriented [SDR19].


Pseudo [Ano17a, Ano13, Ano18a, Ano19a].

Pseudo-free [Ano17a, Ano13, Ano18a, Ano19a].

PTIME [BN16].

Public [KKS13, MZJ17, GHP09, KA09, Rom15, Rom17, SZ09].

Public-key [MZJ17, GHP09, Rom15].

Quantum [BM11, MU14].

quasiconvex [Sah15].

quasipositive [Ore15].

questions [GLS09].

R. [Was11].

Ramp [PA19].

Random [GMO17, GMR11, MU11b, AGG10].

Randomized [SDR19].

drate [FFK11].

rational [Cle09].

real [GLS15].

Recognition [Asb18, Ore15].

Reflections [FGRS14].

regularity [HR13].

relatives [Mil14].

remark [Tim17].

representations [FR11, FR13, HK13].

residually [Pue16].

response [BBFT10].

restricted [BN16, But17].

results [BD09].

revisited [Krö10].

Rewriting [Cho09, DDM12].

Rijndael [BBC+14].

Rijndael-like [BBC+14].

rings [Eft12, GKS18b, KKS13, Kas10, MN15, MU14].

rounding [BMV15].

RSA [AK16, Rom15].

rushing [PA19].

SAT [JK10].

SAT-solvers [JK10].

satisfiability [Ryb17].

saving [DG16].

scheme [Das15, FMR13].

schemes [CZ10, KPU18, Rom18].

Search [HM12, Shp10, CJ12, HHMHM15, KA09, PU19].

searching [Ryb15].

Secrecy [GS13].

secret [CZ10, FMR13, KPU18, PA19].

secure [GM18].

security [BBFT10, Neu12, Shp14].

Selmer [FC16].

semilattices [She16].

semilinear [GKS18a].

set [Asb18].

sets [She16].

sharing [AK16, CZ10, FMR13, KPU18, PA19].

Shephard [Wei10].

Sherlock [GS12].

shifted [KLT09, LU09].

short [Krö10, Ros09].

Shortlex [HR13].

Shoup [KA09].

shuffle [Shn09].

signature [Das15, STT11].

signatures [KK12].

significant [AK16].

simple [KNPS16].

singular [Mah10].

SLP [Loh12].

SLP-compressed [Loh12].

small [Gil14, KNPS16].

software [SDR19].

software-oriented [SDR19].

Solitar [Cle09].

solution [BN16, CJ12].

solvable [RS14, Vas11].

solvers [JK10].

solving [CR16].

Some [ER10, KMK19, SW19, FGRS14, GLS09, KNPS16].

Space [LT09, MV17].

special [DE15].

spectral [KN18].

spherical [Tim17].

sporadic [KNPS16].

squares [CZ10].

Stallings [Krö10].

status [GK16].

strings [Loh12].

Strong [MU11a].

structure [Krö10].

Subgroup [KLT10].

Subgroups [Was11, Ano18a, BM11, CCR11, Cle09, FMR09, KLT10, Ros13, Sah15].

submonoids [SZ18].

subset [Mon19].

subsurfaces [SW19].

sum [Mon19].

surfaces [Bac15].

survey [GK16, Loh12].

symmetric [KNPS16].

Symmetries [AT15].

system [MN15].

systems [Cho09, CR16, KT13].

test [HM12].

tetrahedron [gRHR09].

theorem [FMR13, GLS09, Krö10].

theoretic [Ven14].

theoretical [MR14].

theory [BBFT10, FGRS18, Mil11, Osi09, SW19, Shp10].

Thompson [ERW12, ET16, TY15, Was11].

three [Ore15].

Thurston [Ito10].

Thurston-type [Ito10].

time [Vas11].

Tits [gRHR09].

Torsion [Cle09, Chi14, EE17, HK13, KMT19, Mac09, Osi09].

Torsion-free [Cle09, KMT19].

transformations [KPU18].

transitive [Iva15].

Tree [CCR11, TY15].

Tree-based [TY15].

triangles [Wei10].

triple [HHMHM15, HM12].

triples [HHMHM15, HM12].

tropical [CM15, CM17].

Tsaranov [gRHR09].

Two [Neu12, Rom18].

Two-party [Neu12].

type [Ito10].
uniformity [KM13]. unipotent [But17]. universal [KMS14, Osi09, She19]. update [Con10]. Using [SZ09, BBFT10, Das15, Eft12, JK10, KKS13, MN15, Sch16].


witness [Shp10]. word [Bro14, GKS18a, Ho18, LT09, Shn09]. words [KMS14]. wreath [RS14, Vas11].

Z [Ho18]. Zieschang [BD11].

References

Anshel:2016:CHF


Anokhin:2013:CPF


Anokhin:2017:PFF


Anonymous:2017:FM


Anonymous:2017:F

REFERENCES

Anokhin:2018:CFS

Anon:2018:FM

Antolin:2011:CGV
Asboei:2018:RDP


Atchison:2015:SF


Bacardit:2015:CA


Bacardit:2011:ZMM


Bonanome:2011:QAF

REFERENCES

CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).


**Craven:2012:EAS**


**Connor:2013:NAF**


**Clement:2009:TFA**


**Chauvet:2015:KAV**


**Conder:2010:UHG**


**Craven:2016:PEA**


**Chum:2010:LSS**

REFERENCES

Das:2015:KEF


Diekert:2012:CRC


Distler:2015:GES


Dean:2009:MPF


Duquesne:2016:MSC


Eick:2017:IPT


Eftekhari:2012:DHK


Eick:2016:AGF


Elder:2010:SGP

REFERENCES

223–229, 2010. CODEN ????
ISSN 1867-1144 (print), 1869-6104 (electronic).


REFERENCES


REFERENCES

Gribov:2018:PPK


Gaglione:2009:ALF


Gaglione:2015:AER


Ghaaffari:2018:MSV


Garreta:2017:RNG


Gilman:2011:REF


Grigoriev:2012:CHI


grosseRebel:2009:TAT

Volkmar groe Rebel, Miriam Hahn, and Gerhard Rosenberger. The Tits alternative for


REFERENCES


REFERENCES

Maclachlan:2009:ENE

[Mac09] C. Maclachlan. Existence
and non-existence of torsion in
maximal arithmetic Fuchsian
CODEN ????? ISSN 1867-1144
(print), 1869-6104 (electronic).

Mahalanobis:2010:DLP

[Mah10] Ayan Mahalanobis. The dis-
crete logarithm problem in
the group of non-singular
CODEN ????? ISSN 1867-1144
(print), 1869-6104 (electronic).

Miller:2011:ICM

[Mil11] Russell Miller. An intro-
duction to computable model theory on
CODEN ????? ISSN 1867-1144
(print), 1869-6104 (electronic).

Miller:2014:FR

[Mil14] Charles F. Miller, III. Friends
and relatives of BS(1, 2).
Groups. Complexity. Cryptol-
ogy, 6(2):73–80, 2014. CODEN ?????
ISSN 1867-1144 (print), 1869-6104
(electronic).

Monico:2019:CHF

[Mon19] Chris Monico. Cryptanalysis
of a hash function, and the
modular subset sum problem.
Groups. Complexity. Cryptology,
CODEN ????? ISSN 1867-
1144 (print), 1869-6104 (elec-
tronic). URL https://www.de-
issue-1/gcc-2019-2001/gcc-

Myasnikov:2014:DCF

[MR14] Alexei Myasnikov and Vitalii
Roman’kov. Diophantine cryp-
tography in free metabelian
groups: theoretical base.
Groups. Complexity. Cryptol-
ogy, 6(2):103–120, 2014. CO-
DEN ????? ISSN 1867-1144
(print), 1869-6104 (electronic).

Myasnikov:2015:LDA

[MR15] Alexei Myasnikov and Vitali-
i Roman’kov. A linear decom-
CODEN ????? ISSN 1867-
1144 (print), 1869-6104 (elec-
tronic).

Monico:2015:CSU

[MN15] Chris Monico and Mara D.
Neusel. Cryptanalysis of a sys-
tem using matrices over group
CODEN ????? ISSN 1867-1144
(print), 1869-6104 (electronic).

Mishchenko:2017:KPN

[MT17] Alexei Mishchenko and Alexan-
der Treier. Knapsack problem
for nilpotent groups. Groups.
Complexity. Cryptology, 9(1):87–??,
May 2017. CODEN ?????
ISSN 1867-1144 (print), 1869-
6104 (electronic). URL https:
2017.9.issue-1/gcc-2017-0006/gcc-
2017-0006.xml.
REFERENCES

Myasnikov:2009:CAA


Mosina:2011:SLL


Myasnikov:2011:RVK


Myasnikov:2014:QAD


Miasnikov:2017:LSC


Myasnikov:2009:GCC


Majewicz:2009:PCN


Marko:2017:PKC

Neumann-Brosig:2010:NHH


Pramanik:2019:RSS


Neupane:2012:TPK


Orevkov:2015:ARQ


Pantesaleev:2019:CSP


Noskov:2016:GCC


Pueschel:2016:HGD


Osin:2009:UTT


Romankov:2012:EG

2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

**Romanov:2015:NPP**


**Romanov:2016:NDA**


**Romanov:2017:CCP**


**Romanov:2018:TGS**


**Romanov:2019:IVA**


**Rosenberger:2009:SBB**


**Rosenmann:2013:ISF**


**Riley:2014:PWW**


**Rybalov:2013:GCD**


**Rybalov:2015:GCS**


**Rybalov:2017:GHB**


**Sahattchieve:2015:CHQ**


**Schridde:2016:CDL**


**Shamsabad:2019:RNS**


**Shevlyakov:2010:AGN**


**Shevlyakov:2016:IAS**


**Shevlyakov:2019:GAU**


**Shnaps:2009:WCP**

Daniella Bak Shnaps. The word and conjugacy problem for shuf-
REFERENCES


Taback:2015:TBL

Ushakov:2016:ACK

Vassileva:2011:PTC

Ventura:2014:GTO

Wassink:2011:SRT

Weiss:2010:SGL

Wilson:2012:EAA