

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

$\{+, -, \times, \div, \&\}$ [Sch16]. 1 [ET16]. 4 [Ore15].
5 [EE17]. 5×5 [HHMHM15]. $\text{Aut}(F_n)$
[Ibr12]. F [ERW12, ET16, TY15, Was11].
 $F_m \times \mathbf{Z}^n$ [Sah15]. $\langle m, m, m \rangle$ [HHMHM15].
 \mathbf{Z}_q [AGG10]. $\mathbf{Z}n\star$ [Ano18a]. $\mathcal{O}((\log q)^2)$
[Sch16]. n [RS14]. p [Ano17a]. p^n [Iva15]. R
[MZ09]. $\text{BS}(1, 2)$ [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].
algebra [Bre11]. **Algebraic**
[BBC⁺14, JK10, Kre09, She10, BD09, BD11,
Ore15, Rom18, She16, She19, AAGG16].
algorithm [Bac15, CL13, CJ12, HHMHM15,
MU14, STT11]. **Algorithmic**
[Ore15, MU11b]. **Algorithms**
[Loh12, BM11, HM12, Wil12]. **Almost**
[GLS09]. **alternative** [gRHR09]. **amalgams**
[FMR09]. **analogs** [BMV15]. **Analysis**
[KPU18, GLS15]. **Andrews** [PU19]. **Anshel**
[MU09, MU09]. **apartments** [CL13].
application [GLS15, HHMHM15].
applications [CJ12, KMK19, SS16].
approach [CR16]. **arithmetic**
[KMK19, Mac09]. **Artin** [HR13, Kra13].

aspects [FGRS14]. **associative** [Bre11, KT13]. **assumption** [Ano13, Ano18a, Ano19a]. **assumptions** [Neu12]. **asymmetric** [Kra13]. **asymptotic** [CFR10]. **asymptotics** [Wil12]. **Ate** [FC16]. **attack** [LU09, MR15, Rom16]. **attacks** [JK10, Kre09]. **Authenticated** [Ush16]. **Authentication** [GS09, GN12, GS12, LU09]. **automatic** [ET16, Gil14]. **automaticity** [HR13]. **automaton** [GG19]. **automorphism** [Eic16]. **automorphisms** [She19].

base [MR14]. **based** [AAGG16, FMR13, GG19, GK16, KPU18, LU09, MZJ17, Rom15, Shp14, TY15]. **Baumslag** [Cle09]. **Ben** [Ros09]. **bilinear** [Das15]. **biography** [Ros09]. **biometric** [GN12]. **bits** [AK16]. **BN** [DG16]. **Boolean** [Ryb17]. **boundary** [Bac15]. **braid** [BD09, Ito10, KLT09, LU09, SW19]. **braids** [Ore15].

cancellation [Gil14]. **canonical** [KMT19]. **case** [Mya09, NR16]. **Cayley** [AGG10, Ant11, GM18]. **certain** [Ano18a, LU09]. **Certifying** [KN18]. **Challenge** [BBFT10]. **cheater** [PA19]. **cheaters** [PA19]. **ciphers** [BBC⁺14]. **circulant** [Mah10]. **class** [AAGG16, BD11, Bac15, KS19]. **classification** [She10]. **closest** [FMR13]. **Closure** [KS19]. **cogrowth** [ERW12]. **combinatorial** [Bac15, BBFT10, Rom17]. **commutative** [KK12, MZ09]. **commutator** [Ush16]. **compactness** [SS17]. **complete** [GHP09]. **complexity** [LT09, Mya09, NR16, Ryb13, Ryb15, TY15]. **component** [Bac15]. **Compositions** [SS16]. **compressed** [Loh12]. **computable** [Mil11]. **computation** [DG16, FC16]. **computational** [Ano13, Ano17a, Ano19a]. **compute** [Bac15, Bre11]. **Computing** [Sch16]. **conditions** [SS17]. **conjecture** [FGRS18, PU19]. **Conjugacy** [PU19, BN16, CJ12, DDM12, KLT09, KLT10, LU09, MV17, Shn09, Vas11]. **conjugation** [GS09]. **Constructing** [Ano13, Ano19a]. **construction** [KMT19]. **context** [Bro14, Ho18, KS19]. **context-free** [Ho18, KS19]. **Continuous** [GN12]. **convex** [Sah15]. **coordinate** [She10]. **coset** [CL13]. **counter** [ET16]. **covering** [KNPS16]. **covers** [KMT19]. **Cramer** [KA09]. **Cryptanalysis** [MN15, Mon19, MU09, Rom17]. **cryptographic** [Rom19]. **Cryptography** [CM17, CJ12, GK16, KMK19, MR14, Rom18, SZ09]. **cryptosystem** [FMR13, GHP09, KA09, MZJ17, Rom15, Rom17]. **Curtis** [PU19]. **curves** [DG16, FC16, Fri17]. **Cutting** [Krö10]. **Cyclic** [DDM12, But17]. **Cylinders** [Ibr12].

decidability [Ven14]. **Decision** [KA09, SZ09]. **decomposition** [Bre11, MR15, Rom16]. **decompositions** [Wil12]. **Decoy** [Shp14]. **Decoy-based** [Shp14]. **Dehornoy** [BD09]. **densities** [CFR10]. **diagonalizable** [MZJ17]. **diagrams** [KMT19, MU11b]. **diameter** [AGG10]. **differentiable** [Iva15]. **Diffie** [Eft12]. **diffusion** [SDR19]. **digital** [KK12, STT11]. **dimension** [HK13]. **dimensional** [Asb18, Bre11]. **Diophantine** [GMO17, MR14, Ryb13]. **Direct** [SS17, Wil12]. **discrete** [Mah10, MU14, Sch16]. **distributive** [KT13]. **doubles** [Pue16].

each [Asb18]. **echelon** [Ros13]. **Effective** [KMT19]. **elementary** [Ano17a, FGRS18, Fri17, GLS15]. **elements** [Asb18, But17]. **elliptic** [FC16, Fri17]. **embedding** [Cho09]. **encryption** [GKS18b, Rom15]. **endomorphism** [FFK11]. **Equations** [Rom12, CR16, GMR11, KMT19, Tim17].

eraserTM [AAGG16]. **escrow** [Das15]. **establishment** [KT13, Neu12]. **estimates** [KN18]. **Evolutionary** [CJ12, CR16]. **examples** [SW19]. **exchange** [Eft12, KKS13]. **Existence** [Mac09, Wil12]. **expanding** [LW12]. **exponentiation** [DG16]. **exponents** [GLS15]. **extensions** [DE15].

factor [Cle09]. **Factoring** [AK16, Ano13, Ano18a, Ano19a]. **Faithful** [FR13, FR11]. **families** [Ano17a, LW12]. **family** [Ano13, Ano18a, Ano19a]. **fast** [HHMHM15]. **Faster** [FC16]. **fields** [Mil11]. **final** [DG16]. **find** [CL13]. **Fine** [Ros09]. **finite** [Ano13, Ano17a, Ano19a, AT15, Bre11, Ito10, MU14, Pue16]. **finite-dimensional** [Bre11]. **finitely** [CFR10, Chi14, Eic16, HK13, SZ18]. **fixed** [BM11]. **Free** [But17, Ano13, Ano17a, Ano18a, Ano19a, Ant11, Bro14, Cle09, Das15, Dea09, EE17, GLS09, GMR11, HK13, Ho18, KMS14, KMT19, KS19, MR14, Ros13, SZ18, Tim17, Vas11]. **Friends** [Mil14]. **Front** [Ano17b, Ano18b]. **Frontmatter** [Ano17c, Ano18c, Ano19b, Ano19c, Ano19d]. **Fuchsian** [Mac09]. **fully** [GKS18b]. **function** [GM18, Mon19]. **functions** [AAGG16, GN12, GS13, Iva15, Mya09, SS16].

galore [Kre09]. **gaps** [KN18]. **Garside** [SW19, KLT10]. **general** [Ano13, Ano18a, Ano19a, Rom18]. **generalisation** [Kra13]. **Generalized** [Gil14, BBC⁺14, BN16, gRHR09]. **generated** [CFR10, Eic16, HK13, SZ18]. **generating** [BD11]. **Generic** [FMR09, Mya09, NR16, Ryb13, Ryb17, CFR10, Ryb15, STT11]. **geodesic** [ER10, HR13]. **geometries** [CL13]. **geometry** [She10, She19]. **Goldfeld** [MU09]. **graph** [AGG10, ET16, NR16, Ryb15]. **graphs** [Ant11, AT15, Krö10, MU11a]. **Grigorchuk** [MV17]. **Group** [DE15, Ven14, Asb18, BD09, BBFT10, Cle09, Dea09, Eic16, ERW12, ET16, FFK11, FMR09, Fri17, GLS15, GK16, KKS13, LU09, Mah10, MV17, MN15, MU14, Pue16, She19, Shp10, TY15, Was11]. **group-based** [GK16]. **Group-theoretic** [Ven14]. **Groups** [Bro14, GKS18a, Ano13, Ano17a, Ano19a, Ant11, Asb18, BD11, Bac15, BN16, But17, CFR10, Chi14, Cho09, Cle09, Con10, CJ12, CR16, EE17, ER10, FR11, FR13, FGRS14, FGRS18, GLS09, GMO17, GMR11, Gil14, GG19, HK13, HR13, Ito10, KMK19, KLT09, KLT10, KNPS16, KMT19, KS19, LT09, LW12, Mac09, MZ09, MZJ17, Mil11, MT17, MU11a, MU11b, MR14, NBR10, Osi09, RS14, Rom12, Ros13, SW19, Shn09, SZ18, Tim17, Vas11, Wei10, gRHR09]. **Growth** [FFK11].

hard [GN12]. **hard-to-invert** [GN12]. **hardness** [Ryb17]. **hash** [AAGG16, GM18, Mon19]. **hashing** [SS16]. **Heisenberg** [BN16]. **Hellman** [Eft12]. **Hessian** [CM17]. **Hirsch** [EE17]. **Holmes** [GS12]. **Hom** [KMT19]. **Hom-diagrams** [KMT19]. **homology** [AT15, NBR10]. **homomorphic** [GKS18b]. **hulls** [Sah15]. **Hurwitz** [Con10]. **Hydra** [Pue16]. **hyperbolic** [KMT19, NBR10, Osi09].

identification [PA19]. **II** [FR13]. **improved** [Rom19]. **indistinguishable** [LW12]. **induced** [Ibr12]. **inert** [Ros13]. **Infinite** [KMS14, FGRS14]. **information** [Shp14]. **integer** [Ano13, Ano18a, Ano19a]. **integral** [GLS15]. **intersection** [Ros13]. **intractability** [Ano13, Ano18a, Ano19a]. **introducing** [Neu12]. **introduction** [Mil11]. **invariant** [BM11]. **invariants** [MZJ17]. **invert** [GN12]. **irreducible** [She16]. **isomorphic** [Was11]. **Isomorphism** [LW12, EE17, NR16, Ryb15].

Kampen [MU11b]. **Kaplansky** [FGRS18].

Key [CM15, Das15, GG19, Eft12, FMR13, GKS18b, GHP09, KA09, KKS13, KT13, MZJ17, MU09, Neu12, Rom15, Rom17, SZ09, Ush16]. **Key-escrow** [Das15]. **Knapsack** [MT17].

lacunary [Osi09]. **language** [Ho18, TY15]. **large** [MU11a, Wei10]. **Larue** [BD09]. **latin** [CZ10]. **lattice** [BMV15, CCR11]. **law** [Fri17, MU11a]. **layers** [SDR19]. **leak** [GS12]. **least** [AK16]. **left** [KT13]. **Lemieux** [MU09]. **length** [EE17, Ore15]. **like** [BBC⁺14]. **limit** [FR11, FR13]. **linear** [Asb18, But17, MR15, SS16]. **linearly** [She16]. **locally** [GLS09]. **Log** [MV17]. **Log-space** [MV17]. **logarithm** [Mah10, MU14]. **logarithms** [Sch16]. **look** [KM13].

Magnus [GLS09]. **mapping** [BD11, Bac15]. **mapping-class** [BD11]. **matrices** [Eft12, KKS13, Mah10, MN15, MU14]. **matrix** [GS09, HK13, HHMHM15, Kas10]. **matter** [Ano17b, Ano18b]. **max** [RS14]. **max-** [RS14]. **maximal** [Mac09]. **McCool** [BD11]. **MDS** [SDR19]. **Memory** [DG16]. **Memory-saving** [DG16]. **Metabelian** [Dea09, GLS15, MR14, RS14, Tim17]. **method** [BD11, GS12]. **model** [FC16, Mil11]. **modification** [FMR13]. **modular** [Mon19]. **moduli** [AK16]. **modulo** [Iva15]. **monoids** [Cho09, Kra13, She10]. **most** [AK16, EE17]. **multi** [AK16, Das15, Ibr12]. **multi-cylinders** [Ibr12]. **multi-power** [AK16]. **multi-signature** [Das15]. **multiple** [CJ12, Ho18, KS19]. **multiplication** [HHMHM15].

n [Ho18]. **natural** [She10]. **Nielsen** [KPU18]. **nilpotent** [Dea09, EE17, GMO17, HK13, MZ09, MT17]. **No** [GS12]. **No-leak** [GS12]. **Non** [BMV15, KK12, KT13, KA09, KM13, Mac09, Mah10].

Non-abelian [BMV15, KA09]. **Non-associative** [KT13]. **Non-commutative** [KK12]. **non-existence** [Mac09]. **non-singular** [Mah10]. **non-uniformity** [KM13]. **noncommutative** [Eft12]. **nonlinear** [Rom16, SDR19]. **note** [FR11, KLT09, NBR10]. **number** [KNPS16]. **numbers** [Asb18, Cle09, MU11a, She10]. **numerical** [KN18].

one [Bac15, GS13, Mya09]. **one-way** [GS13, Mya09]. **open** [GK16]. **operations** [Sch16]. **orbit** [Ven14]. **order** [Asb18]. **Orderable** [FGRS18]. **ordered** [She16]. **orderings** [Ito10]. **orientable** [Bac15]. **oriented** [SDR19].

pairing [DG16, FC16]. **pairings** [Das15]. **Palindromic** [RS14]. **parallel** [CR16]. **parallels** [CM15]. **party** [Neu12]. **passive** [Neu12]. **password** [BBFT10]. **pencil** [CM17]. **points** [BM11]. **poly** [Bro14]. **poly-context-free** [Bro14]. **polycyclic** [CR16, GMO17, GK16]. **Polynomial** [Vas11, GLS15]. **Power** [MZ09, AK16]. **Power-commutative** [MZ09]. **powered** [MZ09]. **Practical** [GKS18b, LU09]. **presence** [PA19]. **Presentations** [Kas10, Bac15, GMO17, Gil14]. **presented** [Chi14]. **primes** [AK16]. **private** [FMR13, GKS18b]. **private-key** [GKS18b]. **probabilistic** [Rom15]. **problem** [BN16, Bro14, CJ12, EE17, Ho18, KLT09, KLT10, Mah10, MV17, MT17, Mon19, MU14, NR16, PU19, Ryb13, Ryb15, Ryb17, Shn09]. **problems** [DDM12, ER10, GMO17, GKS18a, GK16, LT09, MU11b, SZ09, Shp10]. **product** [Dea09, HHMHM15, HM12, Wil12]. **products** [RS14, SS17, Vas11]. **projective** [Asb18]. **proof** [Fri17, Krö10]. **proofs** [BD09]. **properties** [BBC⁺14, CFR10, DE15, KS19]. **property** [HHMHM15, HM12]. **protocol**

[Eft12, LU09, MU09, Rom19, Ush16]. **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]. **rate** [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].

varieties [SS17]. **vector** [FMR13]. **version** [GM18, Rom19]. **virtually** [Ant11, Eic16, SZ18].

way [GS13, Mya09]. **weakly** [Ano18a]. **Wedderburn** [Bre11]. **whose** [GKS18a]. **width** [RS14]. **without** [GS13, Neu12]. **witness** [Shp10]. **word** [Bro14, GKS18a, Ho18, LT09, Shn09]. **words** [KMS14]. **wreath** [RS14, Vas11].

Z [Ho18]. **Zieschang** [BD11].

References

[AAGG16] Iris Anshel, Derek Atkins, Dorian Goldfeld, and Paul E. Gunnells. A class of hash functions based on the algebraic eraserTM. *Groups. Complexity. Cryptology*, 8(1):1–7, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

[AGG10] Gideon Amir and Ori Gurel-Gurevich. The diameter of a random Cayley graph of \mathbf{Z}_q . *Groups. Complexity. Cryptology*, 2(1):59–65, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

[AK16] Omar Akchiche and Omar Khadir. Factoring multi-power

[Ano13]

[Ano17a]

[Ano17b]

[Ano17c]

RSA moduli with primes sharing least or most significant bits. *Groups. Complexity. Cryptology*, 8(1):47–54, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Anokhin:2013:CPF

Mikhail Anokhin. Constructing a pseudo-free family of finite computational groups under the general integer factoring intractability assumption. *Groups. Complexity. Cryptology*, 5(1):53–74, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Anokhin:2017:PFF

Mikhail Anokhin. Pseudo-free families of finite computational elementary abelian p -groups. *Groups. Complexity. Cryptology*, 9(1):1–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-0001/gcc-2017-0001.xml>

Anonymous:2017:FM

Anonymous. Front matter. *Groups. Complexity. Cryptology*, 9(2):i, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).

Anonymous:2017:F

Anonymous. Frontmatter. *Groups. Complexity. Cryptology*, 9(1):i–??, May 2017. CODEN ???? ISSN 1867-

- 1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-frontmatter1/gcc-2017-frontmatter1.xml>. [Ano19b]
- [Ano18a] Mikhail Anokhin. A certain family of subgroups of $\mathbf{Z}n^*$ is weakly pseudo-free under the general integer factoring intractability assumption. *Groups. Complexity. Cryptology*, 10(2):99–??, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ano18b] Anonymous. Front matter. *Groups. Complexity. Cryptology*, 10(2):i–iv, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ano18c] Anonymous. Frontmatter. *Groups. Complexity. Cryptology*, 10(1):i–??, May 2018. CODEN ????. ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-frontmatter1/gcc-2018-frontmatter1.xml>. [Ant11]
- [Ano19a] Mikhail Anokhin. Constructing a pseudo-free family of finite computational groups under the general integer factoring intractability assumption. *Groups. Complexity. Cryptology*, 11(2):133–134, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ano19b] Anonymous. Frontmatter. *Groups. Complexity. Cryptology*, 11(1):i–??, May 2019. CODEN ????. ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-frontmatter1/gcc-2019-frontmatter1.xml>.
- [Ano19c] Anonymous. Frontmatter. *Groups. Complexity. Cryptology*, 11(2):i–iv, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ano19d] Anonymous. Frontmatter. *Groups. Complexity. Cryptology*, 11(2):i–iv, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Asb18] Alireza Khalili Asboei. Recognition of 2-dimensional projective linear groups by the group order and the set of numbers of its elements of each or-

Anonymous:2019:Fa**Anonymous:2019:Fb****Anonymous:2019:Fc****Antolin:2011:CGV****Asboei:2018:RDP**

- der. *Groups. Complexity. Cryptology*, 10(2):111–??, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- Atchison:2015:SFG**
- [AT15] Benjamin Atchison and Edward C. Turner. Symmetries of finite graphs and homology. *Groups. Complexity. Cryptology*, 7(1):11–30, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Bacardit:2015:CAC**
- [Bac15] Lluís Bacardit. A combinatorial algorithm to compute presentations of mapping class groups of orientable surfaces with one boundary component. *Groups. Complexity. Cryptology*, 7(2):95–115, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Babinkostova:2014:APG**
- [BBC⁺14] Liljana Babinkostova, Kevin W. Bombardier, Matthew C. Cole, Thomas A. Morrell, and Cory B. Scott. Algebraic properties of generalized Rijndael-like ciphers. *Groups. Complexity. Cryptology*, 6(1):37–54, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Baumslag:2010:CRP**
- [BBFT10] Gilbert Baumslag, Yegor Bryukhov, Benjamin Fine, and Douglas Troeger. Challenge response password security using combinatorial group theory. *Groups. Complexity. Cryptology*, 2(1):67–81, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Bacardit:2009:ABG**
- [BD09] Lluís Bacardit and Warren Dicks. Actions of the braid group, and new algebraic proofs of results of Dehornoy and Larue. *Groups. Complexity. Cryptology*, 1(1):77–129, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Bacardit:2011:ZMM**
- [BD11] Lluís Bacardit and Warren Dicks. The Zieschang–McCool method for generating algebraic mapping-class groups. *Groups. Complexity. Cryptology*, 3(2):187–220, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Bonanome:2011:QAF**
- [BM11] Marianna Bonanome and Stephen Majewicz. Quantum algorithms for fixed points and invariant subgroups. *Groups. Complexity. Cryptology*, 3(2):329–348, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Begelfor:2015:NAA**
- [BMV15] Evgeni Begelfor, Stephen D. Miller, and Ramarathnam Venkatesan. Non-abelian analogs of lattice rounding. *Groups. Complexity. Cryptology*, 7(2):117–133, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

- [BN16] **Blaney:2016:PSR**
 Kenneth R. Blaney and Andrey Nikolaev. A PTIME solution to the restricted conjugacy problem in generalized Heisenberg groups. *Groups. Complexity. Cryptology*, 8(1):69–74, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Bre11] **Bremner:2011:HCW**
 Murray R. Bremner. How to compute the Wedderburn decomposition of a finite-dimensional associative algebra. *Groups. Complexity. Cryptology*, 3(1):47–66, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Bro14] **Brough:2014:GPC**
 Tara Brough. Groups with poly-context-free word problem. *Groups. Complexity. Cryptology*, 6(1):9–29, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [But17] **Button:2017:FCG**
 Jack O. Button. Free by cyclic groups and linear groups with restricted unipotent elements. *Groups. Complexity. Cryptology*, 9(2):137–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [CCR11] **Carbone:2011:TLS**
 Lisa Carbone, Leigh Cobbs, and Gabriel Rosenberger. Tree lattice subgroups. *Groups. Complexity. Cryptology*, 3(1):1–23, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [CFR10] **Carstensen:2010:ADG**
 Celine Carstensen, Benjamin Fine, and Gerhard Rosenberger. On asymptotic densities and generic properties in finitely generated groups. *Groups. Complexity. Cryptology*, 2(2):113–121, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Chi14] **Chiodo:2014:TFP**
 Maurice Chiodo. On torsion in finitely presented groups. *Groups. Complexity. Cryptology*, 6(1):1–8, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Cho09] **Chouraqui:2009:RSE**
 Fabienne Chouraqui. Rewriting systems and embedding of monoids in groups. *Groups. Complexity. Cryptology*, 1(1):131–140, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [CJ12] **Craven:2012:EAS**
 Matthew J. Craven and Henri C. Jimbo. Evolutionary algorithm solution of the multiple conjugacy search problem in groups, and its applications to cryptography. *Groups. Complexity. Cryptology*, 4(1):135–165, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

- [CL13] **Connor:2013:NAF** [Con10] Thomas Connor and Dimitri Leemans. A new algorithm to find apartments in coset geometries. *Groups. Complexity. Cryptology*, 5(1):75–89, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Cle09] **Clement:2009:TFA** [CR16] Anthony E. Clement. Torsion-free abelian factor groups of the Baumslag–Solitar groups and subgroups of the additive group of the rational numbers. *Groups. Complexity. Cryptology*, 1(2):165–168, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [CM15] **Chauvet:2015:KAU** [CZ10] Jean-Marie Chauvet and Eric Mahé. Key agreement under tropical parallels. *Groups. Complexity. Cryptology*, 7(2):195–198, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [CM17] **Chauvet:2017:CTH** [Das15] Jean-Marie Chauvet and Eric Mahé. Cryptography from the tropical Hessian pencil. *Groups. Complexity. Cryptology*, 9(1):19–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-0002/gcc-2017-0002.xml>
- Conder:2010:UHG** [Con10] Marston Conder. An update on Hurwitz groups. *Groups. Complexity. Cryptology*, 2(1):35–49, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Craven:2016:PEA** [CR16] Matthew J. Craven and Daniel Robertz. A parallel evolutionary approach to solving systems of equations in polycyclic groups. *Groups. Complexity. Cryptology*, 8(2):109–125, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Chum:2010:LSS** [CZ10] Chi Sing Chum and Xiaowen Zhang. The latin squares and the secret sharing schemes. *Groups. Complexity. Cryptology*, 2(2):175–202, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Das:2015:KEF** [Das15] Manik Lal Das. Key-escrow free multi-signature scheme using bilinear pairings. *Groups. Complexity. Cryptology*, 7(1):47–57, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Diekert:2012:CRC** [DDM12] Volker Diekert, Andrew Duncan, and Alexei G. Myasnikov. Cyclic rewriting and conjugacy problems. *Groups. Complexity.*

- Cryptology*, 4(2):321–355, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [DE15] Andreas Distler and Bettina Eick. Group extensions with special properties. *Groups. Complexity. Cryptology*, 7(1):1–10, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Dea09] Margaret H. Dean. Metabelian product of a free nilpotent group with a free abelian group. *Groups. Complexity. Cryptology*, 1(2):169–180, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [DG16] Sylvain Duquesne and Loubna Ghammam. Memory-saving computation of the pairing final exponentiation on BN curves. *Groups. Complexity. Cryptology*, 8(1):75–90, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [EE17] Bettina Eick and Ann-Kristin Engel. The isomorphism problem for torsion free nilpotent groups of Hirsch length at most 5. *Groups. Complexity. Cryptology*, 9(1):55–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-0004/gcc-2017-0004.xml>
- [Eft12] Mohammad Eftekhari. A Diffie–Hellman key exchange protocol using matrices over noncommutative rings. *Groups. Complexity. Cryptology*, 4(1):167–176, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Eic16] Bettina Eick. The automorphism group of a finitely generated virtually abelian group. *Groups. Complexity. Cryptology*, 8(1):35–45, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [ER10] Murray Elder and Andrew Rechnitzer. Some geodesic problems in groups. *Groups. Complexity. Cryptology*, 2(2):223–229, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [ERW12] Murray Elder, Andrew Rechnitzer, and Thomas Wong. On the cogrowth of Thompson’s group F . *Groups. Complexity. Cryptology*, 4(2):301–320, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [ET16] Murray Elder and Jennifer Taback. Thompson’s group F

is 1-counter graph automatic. *Groups. Complexity. Cryptology*, 8(1):21–33, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fouotsa:2016:FAP

[FC16]

Emmanuel Fouotsa and Abdoul Aziz Ciss. Faster Ate pairing computation on Selmer’s model of elliptic curves. *Groups. Complexity. Cryptology*, 8(1):55–67, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Falconer:2011:GRE

[FFK11]

Kenneth J. Falconer, Benjamin Fine, and Delaram Kahrobaei. Growth rate of an endomorphism of a group. *Groups. Complexity. Cryptology*, 3(2):285–300, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fine:2014:RSA

[FGRS14]

Benjamin Fine, Anthony Gaglione, Gerhard Rosenberger, and Dennis Spellman. Reflections on some aspects of infinite groups. *Groups. Complexity. Cryptology*, 6(2):81–91, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fine:2018:OGE

[FGRS18]

Benjamin Fine, Anthony Gaglione, Gerhard Rosenberger, and Dennis Spellman. Orderable groups, elementary theory, and the Kaplansky conjecture. *Groups. Complexity. Cryptology*, 10(1):

43–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0005/gcc-2018-0005.xml>.

Fine:2009:GSG

[FMR09]

Benjamin Fine, Alexei Myasnikov, and Gerhard Rosenberger. Generic subgroups of group amalgams. *Groups. Complexity. Cryptology*, 1(1):51–61, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fine:2013:SSS

[FMR13]

Benjamin Fine, Anja I. S. Moldenhauer, and Gerhard Rosenberger. A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem. *Groups. Complexity. Cryptology*, 5(2):223–238, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fine:2011:NFR

[FR11]

Benjamin Fine and Gerhard Rosenberger. A note on faithful representations of limit groups. *Groups. Complexity. Cryptology*, 3(2):349–355, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Fine:2013:FRL

[FR13]

Benjamin Fine and Gerhard Rosenberger. Faithful representations of limit groups II.

- Groups. Complexity. Cryptology*, 5(1):91–96, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [GK16]
- Friedl:2017:EPG**
- [Fri17] Stefan Friedl. An elementary proof of the group law for elliptic curves. *Groups. Complexity. Cryptology*, 9(2):117–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- Grigorchuk:2019:KAB**
- [GG19] Rostislav Grigorchuk and Dima Grigoriev. Key agreement based on automaton groups. *Groups. Complexity. Cryptology*, 11(2):77–81, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- Grigoriev:2009:CPK**
- [GHP09] Dima Grigoriev, Edward A. Hirsch, and Konstantin Pervyshev. A complete public-key cryptosystem. *Groups. Complexity. Cryptology*, 1(1):1–12, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gilman:2014:GSC**
- [Gil14] Robert H. Gilman. Generalized small cancellation presentations for automatic groups. *Groups. Complexity. Cryptology*, 6(2):93–101, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gryak:2016:SPG**
- Jonathan Gryak and Delaram Kahrobaei. The status of polycyclic group-based cryptography: a survey and open problems. *Groups. Complexity. Cryptology*, 8(2):171–186, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gilman:2018:GWW**
- [GKS18a] Robert H. Gilman, Robert P. Kropholler, and Saul Schleimer. Groups whose word problems are not semilinear. *Groups. Complexity. Cryptology*, 10(2):53–??, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gribov:2018:PPK**
- [GKS18b] Alexey Gribov, Delaram Kahrobaei, and Vladimir Shpilrain. Practical private-key fully homomorphic encryption in rings. *Groups. Complexity. Cryptology*, 10(1):17–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0006/gcc-2018-0006.xml>.
- Gaglione:2009:ALF**
- [GLS09] Anthony M. Gaglione, Seymour Lipschutz, and Dennis Spellman. Almost locally free groups and a theorem of Magnus: some questions. *Groups. Complexity. Cryptology*, 1(2):181–198, 2009.

- CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gaglione:2015:AER**
- [GLS15] Anthony M. Gaglione, Seymour Lipschutz, and Dennis Spellman. An application of elementary real analysis to a metabelian group admitting integral polynomial exponents. *Groups. Complexity. Cryptology*, 7(1):59–68, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Ghaffari:2018:MSV**
- [GM18] Mohammad Hossein Ghaffari and Zohreh Mostaghim. More secure version of a Cayley hash function. *Groups. Complexity. Cryptology*, 10(1):29–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0002/gcc-2018-0002.xml>.
- Garreta:2017:RNG**
- [GMO17] Albert Garreta, Alexei Miasnikov, and Denis Ovchinnikov. Random nilpotent groups, polycyclic presentations, and Diophantine problems. *Groups. Complexity. Cryptology*, 9(2):99–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- Gilman:2011:REF**
- [GMR11] Robert H. Gilman, Alexei Myasnikov, and Vitalii Roman’kov. Random equations in free groups. *Groups. Complexity. Cryptology*, 3(2):257–284, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Grigoriev:2012:CHI**
- [GN12] Dima Grigoriev and Sergey Nikolenko. Continuous hard-to-invert functions and biometric authentication. *Groups. Complexity. Cryptology*, 4(1):19–32, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- grosseRebel:2009:TAT**
- [gRHR09] Volkmar große Rebel, Miriam Hahn, and Gerhard Rosenberger. The Tits alternative for Tsaranov’s generalized tetrahedron groups. *Groups. Complexity. Cryptology*, 1(2):207–216, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Grigoriev:2009:AMC**
- [GS09] Dima Grigoriev and Vladimir Shpilrain. Authentication from matrix conjugation. *Groups. Complexity. Cryptology*, 1(2):199–205, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Grigoriev:2012:NLA**
- [GS12] Dima Grigoriev and Vladimir Shpilrain. No-leak authentication by the Sherlock Holmes method. *Groups. Complexity. Cryptology*, 4(1):177–189, 2012.

- CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Ho18]
- [GS13] Dima Grigoriev and Vladimir Shpilrain. Secrecy without one-way functions. *Groups. Complexity. Cryptology*, 5(1):31–52, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [HHMH15] Sarah Hart, Ivo Hedtke, Matthias Müller-Hannemann, and Sandeep Murthy. A fast search algorithm for $\langle m, m, m \rangle$ triple product property triples and an application for 5×5 matrix multiplication. *Groups. Complexity. Cryptology*, 7(1):31–46, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [HR13]
- [HK13] Maggie Habeeb and Delaram Kahrobaei. On the dimension of matrix representations of finitely generated torsion free nilpotent groups. *Groups. Complexity. Cryptology*, 5(2):193–209, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Ibr12]
- [HM12] Ivo Hedtke and Sandeep Murthy. Search and test algorithms for triple product property triples. *Groups. Complexity. Cryptology*, 4(1):111–133, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Ito10]
- [Iva15] Artyom S. Ivachev. On transitive differentiable modulo p^n .
- Meng-Che Ho. The word problem of z_n is a multiple context-free language. *Groups. Complexity. Cryptology*, 10(1):9–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0003/gcc-2018-0003.xml>.
- Derek F. Holt and Sarah Rees. Shortlex automaticity and geodesic regularity in Artin groups. *Groups. Complexity. Cryptology*, 5(1):1–23, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Ito2010:FTT]
- Fedaa Ibrahim. Cylinders, multi-cylinders and the induced action of $\text{Aut}(F_n)$. *Groups. Complexity. Cryptology*, 4(2):357–375, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Tetsuya Ito. On finite Thurston-type orderings of braid groups. *Groups. Complexity. Cryptology*, 2(2):123–155, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

- functions. *Groups. Complexity. Cryptology*, 7(2):183–190, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [KKS13]
- [JK10] Philipp Jovanovic and Martin Kreuzer. Algebraic attacks using SAT-solvers. *Groups. Complexity. Cryptology*, 2(2):247–259, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [KLT09]
- [KA09] Delaram Kahrobaei and Michael Anshel. Decision and search in non-abelian Cramer–Shoup public key cryptosystem. *Groups. Complexity. Cryptology*, 1(2):217–225, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [KLT10]
- [Kas10] Martin Kassabov. Presentations of matrix rings. *Groups. Complexity. Cryptology*, 2(1):51–57, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [KK12] Delaram Kahrobaei and Charalambos Koupparis. Non-commutative digital signatures. *Groups. Complexity. Cryptology*, 4(2):377–384, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [KMK19]
- Kahrobaei:2013:PKE**
Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. Public key exchange using matrices over group rings. *Groups. Complexity. Cryptology*, 5(1):97–115, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Kalka:2009:NSC**
Arkadius Kalka, Eran Liberman, and Mina Teicher. A note on the shifted conjugacy problem in braid groups. *Groups. Complexity. Cryptology*, 1(2):227–230, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Kalka:2010:SCP**
Arkadius Kalka, Eran Liberman, and Mina Teicher. Subgroup conjugacy problem for Garside subgroups of Garside groups. *Groups. Complexity. Cryptology*, 2(2):157–174, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Koblitz:2013:ALN**
Neal Koblitz and Alfred Menezes. Another look at non-uniformity. *Groups. Complexity. Cryptology*, 5(2):117–139, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Kahrobaei:2019:SAA**
Delaram Kahrobaei and Keivan Mallahi-Karai. Some applications of arithmetic groups

- in cryptography. *Groups. Complexity. Cryptology*, 11(1): 25–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-2002/gcc-2019-2002.xml>.
- [KMS14] Olga Kharlampovich, Alexei Myasnikov, and Denis Serbin. Infinite words and universal free actions. *Groups. Complexity. Cryptology*, 6(1):55–69, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [KMT19] Olga Kharlampovich, Alexei Myasnikov, and Alexander Taam. Effective construction of covers of canonical Hom-diagrams for equations over torsion-free hyperbolic groups. *Groups. Complexity. Cryptology*, 11(2):83–101, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [KN18] Marek Kaluba and Piotr W. Nowak. Certifying numerical estimates of spectral gaps. *Groups. Complexity. Cryptology*, 10(1):33–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0004/gcc-2018-0004.xml>.
- [KNPS16] Luise-Charlotte Kappe, Daniela Nikolova-Popova, and Eric Swartz. On the covering number of small symmetric groups and some sporadic simple groups. *Groups. Complexity. Cryptology*, 8(2):135–154, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [KPU18] Matvei Kotov, Dmitry Pan-teleev, and Alexander Ushakov. Analysis of secret sharing schemes based on Nielsen transformations. *Groups. Complexity. Cryptology*, 10(1):1–??, May 2018. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2018.10.issue-1/gcc-2018-0001/gcc-2018-0001.xml>.
- [Kra13] Daan Krammer. An asymmetric generalisation of Artin monoids. *Groups. Complexity. Cryptology*, 5(2):141–167, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Kre09] Martin Kreuzer. Algebraic attacks galore! *Groups. Complexity. Cryptology*, 1(2):231–259, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Kappe:2016:CNS**Kharlampovich:2014:IWU****Kotov:2018:ASS****Kharlampovich:2019:ECC****Krammer:2013:AGA****Kaluba:2018:CNE****Kreuzer:2009:AAG**

- [Krö10] **Kron:2010:CGR**
Bernhard Krön. Cutting up graphs revisited — a short proof of Stallings’ structure theorem. *Groups. Complexity. Cryptology*, 2(2):213–221, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [KS19] **Kropholler:2019:CPC**
Robert P. Kropholler and Davide Spriano. Closure properties in the class of multiple context-free groups. *Groups. Complexity. Cryptology*, 11(1):1–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-2004/gcc-2019-2004.xml>.
- [KT13] **Kalka:2013:NAK**
Arkadius Kalka and Mina Teicher. Non-associative key establishment for left distributive systems. *Groups. Complexity. Cryptology*, 5(2):169–191, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Loh12] **Lohrey:2012:ASC**
Markus Lohrey. Algorithms on SLP-compressed strings: a survey. *Groups. Complexity. Cryptology*, 4(2):241–299, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [LT09] **Lakin:2009:SCW**
Stephen R. Lakin and Richard M. Thomas. Space complexity and word problems of groups. *Groups. Complexity. Cryptology*, 1(2):261–273, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [LU09] **Longrigg:2009:PAC**
Jonathan Longrigg and Alexander Ushakov. A practical attack on a certain braid group based shifted conjugacy authentication protocol. *Groups. Complexity. Cryptology*, 1(2):275–286, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [LW12] **Lewis:2012:IEF**
Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups. Complexity. Cryptology*, 4(1):73–110, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Mac09] **Maclachlan:2009:ENE**
C. Maclachlan. Existence and non-existence of torsion in maximal arithmetic Fuchsian groups. *Groups. Complexity. Cryptology*, 1(2):287–295, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Mah10] **Mahalanobis:2010:DLP**
Ayan Mahalanobis. The discrete logarithm problem in the group of non-singular circulant matrices. *Groups. Complexity. Cryptology*, 2(1):83–89, 2010.

- CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Mil11] Russell Miller. An introduction to computable model theory on groups and fields. *Groups. Complexity. Cryptology*, 3(1):25–45, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MR14] **Miller:2011:ICM** Alexei Myasnikov and Vitalii Roman’kov. Diophantine cryptography in free metabelian groups: theoretical base. *Groups. Complexity. Cryptology*, 6(2):103–120, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Mil14] Charles F. Miller, III. Friends and relatives of $BS(1, 2)$. *Groups. Complexity. Cryptology*, 6(2):73–80, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MR15] **Miller:2014:FR** Alexei Myasnikov and Vitalii Roman’kov. A linear decomposition attack. *Groups. Complexity. Cryptology*, 7(1):81–94, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MN15] Chris Monico and Mara D. Neusel. Cryptanalysis of a system using matrices over group rings. *Groups. Complexity. Cryptology*, 7(2):175–182, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MT17] **Monico:2015:CSU** Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups. Complexity. Cryptology*, 9(1):87–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc-2017-0006/gcc-2017-0006.xml>
- [Mon19] Chris Monico. Cryptanalysis of a hash function, and the modular subset sum problem. *Groups. Complexity. Cryptology*, 11(1):17–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc-2019-11.issue-1/gcc-2019-2001/gcc-2019-2001.xml>
- [MU09] **Monico:2019:CHF** Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of the Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. *Groups. Complexity. Cryptology*, 1(1):63–75, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Myasnikov:2014:DCF] Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of the Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. *Groups. Complexity. Cryptology*, 6(2):103–120, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Myasnikov:2015:LDA] Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of the Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. *Groups. Complexity. Cryptology*, 7(1):81–94, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Mishchenko:2017:KPN] Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of the Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. *Groups. Complexity. Cryptology*, 1(1):63–75, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Myasnikov:2009:CAA] Alex D. Myasnikov and Alexander Ushakov. Cryptanalysis of the Anshel–Anshel–Goldfeld–Lemieux key agreement protocol. *Groups. Complexity. Cryptology*, 1(1):63–75, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

- [MU11a] **Mosina:2011:SLL** Natalia Mosina and Alexander Ushakov. Strong law of large numbers on graphs and groups. *Groups. Complexity. Cryptology*, 3(1):67–103, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MU11b] **Myasnikov:2011:RVK** Alexei Myasnikov and Alexander Ushakov. Random van Kampen diagrams and algorithmic problems in groups. *Groups. Complexity. Cryptology*, 3(1):121–185, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MU14] **Myasnikov:2014:QAD** Alexey D. Myasnikov and Alexander Ushakov. Quantum algorithm for discrete logarithm problem for matrices over finite group rings. *Groups. Complexity. Cryptology*, 6(1):31–36, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MV17] **Miasnikov:2017:LSC** Alexei Miasnikov and Svetla Vassileva. Log-space conjugacy problem in the Grigorchuk group. *Groups. Complexity. Cryptology*, 9(1):77–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-0005/gcc-2017-0005.xml>
- [Mya09] **Myasnikov:2009:GCC** Alex D. Myasnikov. Generic case complexity and one-way functions. *Groups. Complexity. Cryptology*, 1(1):13–31, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MZ09] **Majewicz:2009:PCN** Stephen Majewicz and Marcos Zyman. Power-commutative nilpotent R -powered groups. *Groups. Complexity. Cryptology*, 1(2):297–309, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [MZJ17] **Marko:2017:PKC** František Marko, Alexandr N. Zubkov, and Martin Juráš. Public-key cryptosystem based on invariants of diagonalizable groups. *Groups. Complexity. Cryptology*, 9(1):31–??, May 2017. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2017.9.issue-1/gcc-2017-0003/gcc-2017-0003.xml>
- [NBR10] **Neumann-Brosig:2010:NHH** Matthias Neumann-Brosig and Gerhard Rosenberger. A note on the homology of hyperbolic groups. *Groups. Complexity. Cryptology*, 2(2):203–212, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Neu12] **Neupane:2012:TPK** Kashi Neupane. Two-party key establishment: from pas-

- sive to active security without introducing new assumptions. *Groups. Complexity. Cryptology*, 4(1):1–17, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [PU19]
- Noskov:2016:GCC**
- [NR16] Gennady A. Noskov and Alexander N. Rybalov. Generic case complexity of the graph isomorphism problem. *Groups. Complexity. Cryptology*, 8(1):9–20, 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Orevkov:2015:ARQ**
- [Ore15] Stepan Yu. Orevkov. Algorithmic recognition of quasipositive 4-braids of algebraic length three. *Groups. Complexity. Cryptology*, 7(2):157–173, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Pue16]
- Osin:2009:UTT**
- [Osi09] D. Osin. On the universal theory of torsion and lacunary hyperbolic groups. *Groups. Complexity. Cryptology*, 1(2):311–319, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). [Rom12]
- Pantelev:2019:CSP**
- Dmitry Pantelev and Alexander Ushakov. Conjugacy search problem and the Andrews–Curtis conjecture. *Groups. Complexity. Cryptology*, 11(1):43–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-2005/gcc-2019-2005.xml>.
- Pueschel:2016:HGD**
- Kristen Pueschel. Hydra group doubles are not residually finite. *Groups. Complexity. Cryptology*, 8(2):163–170, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Romankov:2012:EG**
- Vitalii Roman’kov. Equations over groups. *Groups. Complexity. Cryptology*, 4(2):191–239, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- Romankov:2015:NPP**
- [PA19] Jyotirmoy Pramanik and Avishek Adhikari. Ramp secret sharing with cheater identification in presence of rushing cheaters. *Groups. Complexity. Cryptology*, 11(2):103–113, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic). [Rom15]
- Pramanik:2019:RSS**
- Jyotirmoy Pramanik and Avishek Adhikari. Ramp secret sharing with cheater identification in presence of rushing cheaters. *Groups. Complexity. Cryptology*, 11(2):103–113, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).

- [Rom16] Vitalii Roman'kov. A nonlinear decomposition attack. *Groups. Complexity. Cryptology*, 8(2):197–207, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Rom17] Vitalii Roman'kov. Cryptanalysis of a combinatorial public key cryptosystem. *Groups. Complexity. Cryptology*, 9(2):125–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Rom18] Vitaly Roman'kov. Two general schemes of algebraic cryptography. *Groups. Complexity. Cryptology*, 10(2):83–??, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Rom19] Vitalii Roman'kov. An improved version of the AAG cryptographic protocol. *Groups. Complexity. Cryptology*, 11(1):35–??, May 2019. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic). URL <https://www.degruyter.com/view/j/gcc.2019.11.issue-1/gcc-2019-2003/gcc-2019-2003.xml>.
- [Ros09] Gerhard Rosenberger. A short biography of Ben Fine. *Groups. Complexity. Cryptology*, 1(2):141–142, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ros13] Amnon Rosenmann. On the intersection of subgroups in free groups: echelon subgroups are inert. *Groups. Complexity. Cryptology*, 5(2):211–221, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [RS14] Tim R. Riley and Andrew W. Sale. Palindromic width of wreath products, metabelian groups, and max- n solvable groups. *Groups. Complexity. Cryptology*, 6(2):121–132, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ryb13] Alexander Rybalov. Generic complexity of the Diophantine problem. *Groups. Complexity. Cryptology*, 5(1):25–30, 2013. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ryb15] Alexander Rybalov. On the generic complexity of the searching graph isomorphism problem. *Groups. Complexity. Cryptology*, 7(2):191–193, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ryb17] Alexander Rybalov. Generic hardness of the Boolean satisfi-

Romankov:2016:NDA**Rosenmann:2013:ISF****Romankov:2017:CCP****Riley:2014:PWW****Romankov:2018:TGS****Rybalov:2013:GCD****Romanakov:2019:IVA****Rybalov:2015:GCS****Rosenberger:2009:SBB****Rybalov:2017:GHB**

- ability problem. *Groups. Complexity. Cryptology*, 9(2):151–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Sah15] **Sahattchiev:2015:CHQ**
Jordan Sahattchiev. On convex hulls and the quasiconvex subgroups of $F_m \times \mathbf{Z}^n$. *Groups. Complexity. Cryptology*, 7(1):69–80, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Sch16] **Schridde:2016:CDL**
Christian Schridde. Computing discrete logarithms using $\mathcal{O}((\log q)^2)$ operations from $\{+, -, \times, \div, \&\}$. *Groups. Complexity. Cryptology*, 8(2):91–107, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SDR19] **Shamsabad:2019:RNS**
Mohammad Reza Mirzaee Shamsabad, Seyed Mojtaba Dehnavi, and Akbar Mahmoodi Rishakani. Randomized nonlinear software-oriented MDS diffusion layers. *Groups. Complexity. Cryptology*, 11(2):123–131, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [She10] **Shevlyakov:2010:AGN**
A. Shevlyakov. Algebraic geometry over natural numbers. The classification of coordinate monoids. *Groups. Complexity. Cryptology*, 2(1):91–111, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [She16] **Shevlyakov:2016:IAS**
Artem N. Shevlyakov. On irreducible algebraic sets over linearly ordered semilattices. *Groups. Complexity. Cryptology*, 8(2):187–195, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [She19] **Shevlyakov:2019:GAU**
Artem N. Shevlyakov. On group automorphisms in universal algebraic geometry. *Groups. Complexity. Cryptology*, 11(2):115–121, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Shn09] **Shnaps:2009:WCP**
Daniella Bak Shnaps. The word and conjugacy problem for shuffle groups. *Groups. Complexity. Cryptology*, 1(2):143–164, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Shp10] **Shpilrain:2010:SWP**
Vladimir Shpilrain. Search and witness problems in group theory. *Groups. Complexity. Cryptology*, 2(2):231–246, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Shp14] **Shpilrain:2014:DBI**
Vladimir Shpilrain. Decoy-based information security. *Groups. Complexity. Cryptology*, 6(2):149–155, 2014. CO-

- DEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SS16] Vladimir Shpilrain and Bianca Sosnovski. Compositions of linear functions and applications to hashing. *Groups. Complexity. Cryptology*, 8(2):155–161, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SS17] Mohammad Shahryari and Artem Shevlyakov. Direct products, varieties, and compactness conditions. *Groups. Complexity. Cryptology*, 9(2):159–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [STT11] Jennifer Seberry, Vinhbuu To, and Dongvu Tonien. A new generic digital signature algorithm. *Groups. Complexity. Cryptology*, 3(2):221–237, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SW19] Saul Schleimer and Bert Wiest. Garside theory and subsurfaces: Some examples in braid groups. *Groups. Complexity. Cryptology*, 11(2):61–75, November 2019. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SZ09] **Shpilrain:2016:CLF**
Vladimir Shpilrain and Gabriel Zapata. Using decision problems in public key cryptography. *Groups. Complexity. Cryptology*, 1(1):33–49, 2009. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [SZ18] **Shahryari:2017:DPV**
Pedro V. Silva and Alexander Zakharov. On finitely generated submonoids of virtually free groups. *Groups. Complexity. Cryptology*, 10(2):63–??, November 2018. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Tim17] **Timoshenko:2017:RSE**
Evgeny I. Timoshenko. A remark on spherical equations in free metabelian groups. *Groups. Complexity. Cryptology*, 9(2):155–??, November 2017. ISSN 1867-1144 (print), 1869-6104 (electronic).
- [TY15] **Taback:2015:TBL**
Jennifer Taback and Sharif Younes. Tree-based language complexity of Thompson’s group F . *Groups. Complexity. Cryptology*, 7(2):135–152, 2015. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).
- [Ush16] **Ushakov:2016:ACK**
Alexander Ushakov. Authenticated commutator key agreement protocol. *Groups. Com-*

plexity. Cryptology, 8(2):127–133, November 2016. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Vassileva:2011:PTC

- [Vas11] Svetla Vassileva. Polynomial time conjugacy in wreath products and free solvable groups. *Groups. Complexity. Cryptology*, 3(1):105–120, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Ventura:2014:GTO

- [Ven14] Enric Ventura. Group-theoretic orbit decidability. *Groups. Complexity. Cryptology*, 6(2):133–148, 2014. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Wassink:2011:SRT

- [Was11] Bronlyn Wassink. Subgroups of R. Thompson’s group F that are isomorphic to F . *Groups. Complexity. Cryptology*, 3(2):239–256, 2011. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Weiss:2010:SGL

- [Wei10] Uri Weiss. On Shephard groups with large triangles. *Groups. Complexity. Cryptology*, 2(1):1–34, 2010. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).

Wilson:2012:EAA

- [Wil12] James B. Wilson. Existence, algorithms, and asymptotics of direct product decompositions,

I. *Groups. Complexity. Cryptology*, 4(1):33–72, 2012. CODEN ???? ISSN 1867-1144 (print), 1869-6104 (electronic).