A Complete Bibliography of Publications in the Journal of 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/

28 September 2015
Version 1.39

Title word cross-reference


0 [465].

3G [461].

4-Round [393].

9796 [306]. 9796-1 [306].

abelian [326, 408, 91, 337]. Abstract [117].
Accelerating [398]. Achieve [477].
Adaptive [241, 390, 471]. Adaptively [390].
Adic [130]. Advance [279]. Adversarial [458]. Adversaries [353, 345, 357, 403, 450, 472, 236].
Adversary [173]. AES [373, 474, 346, 459].
Aggregate [429]. Agreement [259, 258, 260, 128]. AKS [297]. Alerts [486]. Algebraic [201, 64, 92, 479].


circuit [17]. Class [324, 381, 88, 103, 41].

Classical [262]. Classification [46].


Collision [488, 125, 343, 371, 335, 158, 323, 262, 48]. Commitments [426].


Compilers [334]. Complete [250, 477].


Computational [212, 301, 482, 282, 231, 407, 139, 479].

Computationally [450, 249, 395].

Computations [196]. computed [56].


congruential [15]. Conjecture [103, 405].

Connected [276]. Connection [482].

Connectivity [172]. Consequences [391].


Constructions [456, 410, 329, 311, 254, 416, 482, 3, 39].

Constructive [334, 207]. Contrast [170].


Counterexamples [103].

Countermeasures [346]. Counting [60].


Cryptanalyst [148]. Cryptanalytic [93, 434, 444, 239, 155]. Crypto [376].


Cryptography [212, 301, 340, 264, 199, 334, 160, 170, 259, 381, 455, 92, 337, 479, 198, 10, 54].

Cryp
tologic [204]. Cryptology [427].

CRYPTOPOST [36]. Cryptosystem [461, 126, 326, 180, 144, 195, 32, 37, 64].

Cryptosystems [248, 287, 168, 221, 314, 139, 203, 210, 161, 237, 246, 43, 28, 12, 80].


Cut-and-Choose [411]. Cycling [2].

Damgård [400]. Data [473, 216, 209, 302, 183, 2].

Data-Dependent [209]. Davies [133].

Deal [110]. Decision [231].

Decommitments [382]. Decomposing [198]. Decompositions [96].

Decorrelation [232]. Decryption


Free [166, 125, 137, 322, 350, 98].
Frequency [121]. Friendly [352, 378]. Frobenius [281]. Full [422, 239]. Fully
[433, 487]. Function [219, 125, 369, 222, 30].
Functional [89]. Functions
Further [100].

[200, 112, 173, 138, 277, 339, 313].
Generalization [10]. Generalized [41].
Generates [85]. Generating [233].
Generation
Generator [253, 179, 298, 15]. Generators
[379, 225, 242, 121, 191, 222, 59, 38].
Generic [452, 320, 311, 424]. Genus
[324, 157, 342]. Geometric [83]. GGH
[330]. Given [258, 56]. Giving [51]. Glitch
[373]. Glitches [375]. GNUC [475].
Goldreich [242]. Golić [405]. good [29].
GOST [422]. Graph [96, 408]. Graphs
[328]. Grindahl [489]. Group
[102, 289, 2, 288, 319, 350, 384, 85, 91].
Groups [310, 408, 324, 280, 231, 326, 221].
GSM [317, 461]. Guessing [467]. Guest
[372, 31, 113, 44].

H [380]. Handling [315]. Handshake [351].
Hard [289, 200]. Hard-Core [200].
Hard-to-Invert [289]. Hardness [421].
Hardware [375]. Hash [428, 410, 460, 336, 361, 328, 451, 413, 369, 406, 141, 469, 30].
Hash-CBC [410]. Hashing
[442, 397, 159, 98]. having [76]. HB [356].
Hellman
[10, 341, 184, 304, 231, 245, 157, 128]. Help
[226]. Hides [219]. Hiding [132, 335, 17].
Hierarchical [399, 293]. Hierarchy [84].
High [227]. Highly [336]. Highly-Efficient
[336]. Hints [51]. HMAC [488].
Homomorphic [487, 362].
Homomorphisms [384]. Human [275].
Hybrid [308, 348, 487]. Hyperelliptic
[267, 12, 342, 324].

IACBC [290]. IAPM [290]. IBE [316].
IDEA [468]. Ideal [46, 404, 142, 120, 65].
Identification [325, 50, 169, 55, 61].
Identity [367, 456, 325, 311, 387, 6].
Identity-Based [367, 456, 325, 311, 387].
IEC [306]. imaginary [8]. impersonation
[81]. Implementation
[248, 160, 102, 373, 375, 32, 21, 80].
Implementations [50, 52]. Importance
[196, 71]. Impossibility
[336, 270, 383, 312]. Impossible [261].
Improbability [146]. Improve [337].
Improved
[348, 445, 474, 253, 274, 459, 378, 63].
Improvement [133]. Improvements [123].
Improving [206]. Independent [204].
Index [324, 457]. Indistinguishability
[407]. Inferring [15]. Infinite [103, 73].
Information
[374, 466, 240, 295, 129, 193, 104, 25, 17, 63].
Information-Theoretic [295, 104, 25].
Inner [423]. Input [340, 421, 446]. Inputs
[358, 383]. Ins [174]. Insecure [203].
Insecurity [215]. Instant [317].
instruments [24]. Integration [418].
Integrity [322, 86]. Interaction [226].
Interactive [189, 55, 442, 111, 487, 477, 332].
Interpolation [333]. Intersection [357].
Introduction [31, 42, 113, 44]. Inversion
[306]. Isogenies [342]. Isomorphisms [289].
Iteration [297]. IV [279].

Jacobians [342]. Joint [119].

Kangaroos [188]. KASUMI [461]. Keccak
[445]. Kedlaya [267]. KeeLoq [396].
KEM/DEM [308]. KEMs [311]. kernels


REFERENCES


References
REFERENCES


Beauchemin:1988:GRN


Chaum:1988:DCP


Feige:1988:ZKP


McCurlley:1988:KDS


Buchmann:1988:KES


Stinson:1988:CAS


Beauchemin:1988:GHE


Tompa:1988:HSS

REFERENCES


REFERENCES


the journal of the International Association for Cryptologic Research, 3(1): 27–41, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Merkle:1990:FSO


Berson:1991:GEI


Agnew:1991:IFP


Gaarder:1991:AFA


Haber:1991:HTD


Matyas:1991:KPC


Pastor:1991:CCA


Lenstra:1991:CRK


Micali:1991:EPP


Naor:1991:BCU


Schnorr:1991:ESG


Goutier:1991:SII


Boyar:1991:PZK


Koblitz:1991:ECI


Damgaard:1992:P


Bennett:1992:EQC


Brickell:1992:IIS


Evertse:1992:WNR

[56] Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA-signatures can...

Maurer:1992:CPS


Meier:1992:CPC


Maurer:1992:UST


Lloyd:1992:CBF


Georgiades:1992:SRS


Loxton:1992:CRC


Brickell:1992:SIB


Magliveras:1992:APC

ISSN 0933-2790 (print), 1432-1378 (electronic).

Phillips:1992:SIS


Dai:1992:BSD


Brassard:1993:EN


Agnew:1993:A0


Ito:1993:MAS


Goldreich:1993:UCT


Maurer:1993:CCI


Boyar:1993:CCZ


Chor:1993:SSI

[73] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains. *Jour-
REFERENCES

Goldreich:1993:PZK


Schrift:1993:UTN


Rosenbaum:1993:LBA


Capocelli:1993:SSS


Coppersmith:1993:MNF


Orton:1993:DFP


Menezes:1993:ECC


Lenstra:1993:UIK


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES


REFERENCES

Coppersmith:1997:SSP

Jackson:1997:MTA

Kilian:1998:ENZ

Sakurai:1998:SCC
Biham:1998:CMM


Knudsen:1998:AFD


Golic:1998:MCI


Naor:1998:PZK


Scheidler:1998:PKC

Sc


Balasubramanian:1998:IEC


Joux:1998:LRT


Dwork:1998:EEU

[149] Cynthia Dwork and Moni Naor. An


[159] Phillip Rogaway. Bucket hashing and

Bellare:1999:TCA


Blundo:1999:FBA


Biham:1999:CTM


Bernstein:1999:HSR

REFERENCES

Smart:1999:DLP


Burmester:1999:DSF


Quinn:1999:BKD


Joye:1999:CRB


Shoup:1999:SPI

REFERENCES


REFERENCES


DiCrescenzo:2001:USP


Coppersmith:2001:WQS


Vaudenay:2001:CCR


Boneh:2001:IEE


Wang:2001:SCM


Ye:2001:DAA

[198] Dingfeng Ye, Zongduo Dai, and Kwok-Yan Lam. Decomposing attacks on

Bailey:2001:EAF


Goldmann:2001:CBG


Jakobsen:2001:ABC


Fiat:2001:DTT


Scanlon:2001:PKC

REFERENCES


Shoup:2002:STC

Galbraith:2002:ECP

Naor:2002:CPR

Johnston:2002:AKE

Nguyen:2002:IDS
[215] Phong Q. Nguyen and Igor E. Shparlinski. The insecurity of the Digital Signature Algorithm with partially known nonces. Journal of Crypt-
REFERENCES


REFERENCES


REFERENCES


[253] Rosario Gennaro. An improved pseudorandom generator based on the dis-


REFERENCES


Carlo Blundo and Paolo D’Arco. Analysis and design of distributed key dis-
REFERENCES


[Denef:2006:EKA]


[Chang:2006:IBO]


[Teske:2006:ECT]


[Katz:2006:CSN]
REFERENCES


Koblitz:2007:ALS


Coron:2007:DPT


Gennaro:2007:SDK


Katz:2007:SPA


Catalano:2007:THI


Haastad:2007:SII


Ding:2007:CRO

[291] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-

**Baek:2007:FPS**


**Tassa:2007:HTS**


**Canetti:2007:FSP**


**Beimel:2007:RIT**


**Blundo:2007:USD**


**Cheng:2007:PPO**


Tsaban:2007:TCK


Gennaro:2007:RBU


Abadi:2007:RTV


Ostrovsy:2007:PSS


Kalai:2007:CCS


Dan Boneh and Xavier Boyen. Short signatures without random oracles


Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anony-
REFERENCES


REFERENCES


[335] Iftach Haitner, Omer Horvitz, Jonathan Katz, Chiu-Yuen Koo, Ruggero Morselli,


REFERENCES


Fischlin:2009:ENM


DiRaimondo:2009:NAD


Goldreich:2010:EPP


Tromer:2010:ECA


Knudsen:2010:CM

REFERENCES


REFERENCES


Black:2010:ABB


Groth:2010:VSS


Barkol:2010:MSS


Muller-Quade:2010:LTS


Indesteege:2011:PCE


Enge:2011:DLA


Abdalla:2011:WIB

[367] Michel Abdalla, James Birkett, Dario Catalano, Alexander W. Dent, John...


Batina:2011:MIA

Nikova:2011:SHI

Poschmann:2011:SCR

Dominguez-Oviedo:2011:FBA

Maiti:2011:IRO

Baudet:2011:SOB
Mathieu Baudet, David Lubicz, Julien Micolod, and André Tassiau. On the security of oscillator-based random number generators. Journal of Cryptol-


REFERENCES


Gordon:2012:PFS


Katz:2012:WLR


Boldyreva:2012:SPS


Pietrzak:2012:PRC


Aerts:2012:PAK


Halevi:2012:SPH


Cheon:2012:APR

[398] Jung Hee Cheon, Jin Hong, and Minkyu Kim. Accelerating Pollard’s rho al-


REFERENCES


Lindell:2012:STP


Pass:2013:PCP


Camenisch:2012:BVS


Borghoff:2013:SSD


Freeman:2013:MCL

REFERENCES


[424] Tibor Jager and Jörg Schwenk. On the analysis of cryptographic assump-


[431] Hovav Shacham and Brent Waters. Compact proofs of retrievability. Jour-
Goldreich:2013:ETP

Boyle:2013:FLR

Hong:2013:CCT

Lindell:2013:NCR

vanDijk:2013:FGS

Katz:2013:ROP

Stankovski:2014:ESR


Itai Dinur, Orr Dunkelman, and Adi Shamir. Improved practical attacks on round-reduced Keccak. Journal
REFERENCES


Benny Applebaum. Key-dependent message security: Generic amplifica-
REFERENCES


Khovratovich:2014:RRA


Goldwasser:2014:BPO


Groth:2014:CMS


Abdalla:2014:VRF


Faugere:2014:USI


Amir:2014:AAR

REFERENCES


Amin Baumeler and Anne Broadbent. Quantum private information retrieval has linear communication complexity. *Journal of Cryp-
REFERENCES


Ahn:2015:CAD


Dunkelman:2015:ISK


Hofheinz:2015:GNU


Malka:2015:HAP


Beimel:2015:PMC


Tsaban:2015:PTS

Berman:2015:PUA

Ron Berman, Amos Fiat, Marcin Go

Schage:2015:TSS


Fuller:2015:UAD


Soleimany:2015:RCP


Chandran:2015:AES


Procter:2015:WKF


Aspnes:2015:SAQ

REFERENCES


[Gentry:2015:UFH]

[Bellare:2015:NPN]

[Peyrin:2015:CAG]