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/

01 October 2017  
Version 1.47

Title word cross-reference


CRYPTOPOST [36]. Cryptosystem [490, 461, 126, 326, 180, 144, 195, 32, 37, 64].
Cryptosystems [248, 529, 287, 168, 221, 314, 139, 203, 210, 161, 237, 246, 43, 28, 12, 80].
Cut-and-Choose-Based [501]. Cycling [2].

Deal [110]. Decision [231].
Decommitments [382]. Decomposing [198]. Decompositions [96].
Definitions [329, 82, 345]. Degree [252, 366, 201, 420, 283]. Delegate [409].
Delegation [394]. Delivery [223, 545].
derived [66]. DES-like [43].
Descent [207]. Design [266, 524, 79, 29].
Designing [221, 24]. Designs [460, 104, 9].
Differential [108, 43, 538, 415, 107, 95, 309].
Differentials [261]. Difficult [495].
Difficulty [139]. Diffie [341, 184, 521, 304, 231, 245, 535, 157, 128].
Diffusion [469]. Digital [109, 413, 206, 185, 122, 34, 215].
Dimensional [447]. diminished [79].
distance [41]. Distinguishers [470]. Distributed [266, 296, 287, 417].
Distribution [278, 266, 255, 97, 167, 177, 20, 7].
Dynamic [517, 202, 256].

E0 [318]. E0-like [318]. Easily [233].
ECPP [297]. Edge [484]. Edit [224].
Embedding [283]. EMV [507].
Encryptions [362]. Endomorphism [512].
Endomorphism-Accelerated [512].
Endomorphisms [381]. Enhanced [490].
Enhancements [432]. EnRUPT [365].
Entropy [482]. Enumerating [27, 100]. Equations [136, 423]. Equivalence [286].
Equivalent [74, 62, 7]. Erratum [444].
Error [281]. Errors [196]. Escape [486].
Escrow [160]. Especially [476].
Establishment [548]. Estimate [281].
Evaluation [496, 17]. Even [509, 462].
Everywhere [484]. Evidence [246]. Exact [206]. Exchange [147, 106, 110, 274, 214, 288, 437, 268, 90, 8].


Fairness [545, 386, 392]. Fail-Stop [132].

Fast [491, 179, 141, 501, 101, 14, 151, 159, 157, 32, 30, 79]. Faster [381].

Fault [175, 373, 377]. Fault-Based [377].

Fault-Tolerance [175]. Faults [168].

Faulty [45]. FCSR [380, 438]. FEAL [26].


Finite [199, 102, 398, 252, 326, 221, 263].

first [71]. Fixed [262, 383]. FlipIt [436].


Forward-Secure [294]. Four [447].

Four-Dimensional [447]. FPGA [373, 378].

FPGA-friendly [378]. Fractional [160].

Framework [308, 521, 475]. Franklin [197].

Free [504, 166, 125, 137, 322, 350, 98].

Frequency [121]. Friendly [352, 378].

Frobenius [281]. Full [518, 422, 515, 540, 239]. Fully [433, 487].

Function [219, 125, 369, 222, 30].


Generalization [10]. Generalized [41].

Generates [85]. Generating [233].


Generator [253, 179, 298, 15]. Generators [505, 379, 225, 224, 121, 191, 222, 59, 38].


GGH [330]. Given [258, 56]. Giving [51].

Glitch [373]. Glitches [375]. GNUC [475].

Go [519]. Goldreich [242]. Golic [405].

good [29]. GOST [422]. Graph [96, 408].

Graphs [498, 328]. Grindahl [489].


Groups [310, 408, 324, 280, 231, 326, 221].

GSM [317, 461]. Guaranteed [545].

Guessing [467]. Guest [372, 31, 113, 44].

H [380]. Handling [315]. Handshake [351].

Hard [289, 500, 200, 547]. Hard-Core [200].

Hard-to-Invert [289, 500]. Hardness [421].

Hardware [375]. Hash [508, 428, 410, 460, 336, 361, 328, 451, 413, 369, 466, 141, 469, 30]. Hash-CBC [410].

Hashing [442, 397, 159, 98]. having [76].

HB [356]. Hellman [10, 341, 184, 521, 304, 231, 245, 535, 157, 128].

Help [226]. Hides [219]. Hiding [132, 335, 17]. Hierarchical [399, 293].

Hierarchy [84]. High [227]. Highly [336]. Highly-Effective [336]. Hints [51].

HMAC [488]. Homomorphic [487, 362, 532].

Homomorphisms [384]. Human [275].

Hunting [542]. Hybrid [308, 348, 487].

Hyperelliptic [267, 12, 342, 324].

IACBC [290]. IAPM [290]. IBE [316].

IDEA [468]. Ideal [46, 492, 404, 142, 120, 528, 65].

Identification [506, 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
Improved
[348, 445, 474, 253, 274, 459, 378, 63].
Improvement [133]. Improvements [123]. Improving [206]. Independent [204].
Index [324, 457]. Indifferentiability [492]. Indistinguishability [407]. Inferring [15].
Infinite [103, 73]. Information [541, 374, 466, 240, 295, 129, 193, 543, 104, 25, 17, 63].
Information-Theoretic
[229, 89]. Inversion [289, 500]. Isogenies [342]. Isomorphisms [342].
Knowledge
[45, 115, 226, 51, 147, 166, 426, 448, 114, 273, 487, 70, 82, 116, 393, 138, 52, 390, 435, 477, 143, 414, 440, 494, 21, 72, 6, 74]. Known
Length [254, 141]. Less [217, 376]. Levenshtein [41]. Levin [242].
Malicious [357, 403, 450, 472, 501]. malleability [532]. Malleable
[371, 520, 343]. Man [214].
7

Menezes-Okamoto-Vanstone [146].
Mercurial [426]. Merkle [534, 400].
Merlin [541]. Mesh [510]. Message
[452, 223, 480, 119, 397, 322, 126, 159].
Message-Ecient [119]. Messages
[541, 254, 76]. Methodology [524].
Methods [24]. Middle [214, 18]. Minimal
[250, 172, 503, 66, 28]. Minimization [427].
Minimize [487]. Mining [216]. Minority
[45]. missing [15]. MISTY1 [540]. ML [66].
ML-sequences [66]. Mode [208]. Model
[504, 291, 235, 455, 424, 303, 528, 332, 145,
237]. Models [443, 172, 383, 494]. Modes
[140, 163, 290, 279, 322]. Modifications
[78]. Modular [225, 351, 79]. Modules
[203]. Monopoly [188]. Montgomery [377].
MOV [252]. Much [516]. Multi
[264, 241, 451, 250, 260, 455, 401].
Multi-Exponentiation [264]. Multi-Party
[241, 250, 260]. Multi-Property [451].
Multi-string [455]. Multi-Verifier [401].
Multicast [313, 197]. Multipartite
[404, 333]. Multiparty
[518, 45, 478, 176, 545, 173, 339, 464].
Multiple [140, 279, 69, 120].
Multiplication [447, 151]. Multiplicative
[363]. multiplier [79]. Multisignatures
[429]. Must [135]. Mutual [374]. Mutual
ly [137].

Nearly [242]. Necessary [98]. Negligible
[220]. Neighbor [313]. Networks
[276, 105, 107, 313]. NIZK [544]. NMAC
[488]. Non [471, 189, 241, 520, 408, 324, 343,
371, 487, 326, 477, 332, 532, 441]. Non-
[441]. Non-abelian [326, 408].
Non-Adaptive [241, 471].
Non-hyperelliptic [324]. Non-Interactive
[189, 487, 477, 332]. Non-malleability
[532]. Non-Malleable [371, 520, 343].
Nonces [215]. Noncommutative [479].
Noncommutative-Algebraic [479].
Noninterative [115, 138]. Nonlinear
[375, 103, 182]. Nonlinearity [92].
nonuniform [75]. Normal [263]. Note
[284, 220, 67, 425, 435]. Notions
NTRU [330]. Number [379, 298, 78, 38].
Numbers [4, 233, 101].

OAEP [238, 539, 218]. Obfuscating
[522, 388]. Obfuscation [449, 454, 349].
Oblivious [537, 160, 296, 230, 517, 291, 117,
417, 397, 391, 390, 411, 249]. observed [76].
Odd [83, 161]. Offs [323]. Okamoto [146].
On-Line [109, 236, 410]. On-Line/
Off-Line [109]. One [229, 279, 297, 242, 523,
245, 40, 439, 221, 143, 165, 30].
One-More-RSA-Inversion [229].
One-Sided [242, 523]. One-Time [439].
One-Way [270, 221, 143, 40, 30]. Only
[317, 275]. onto [373]. Operation
[140, 163, 279]. Operations [403, 68].
Optimal [534, 235, 437]. Optimally [502].
Optimized [154]. oracle [17]. Oracles
[534, 329, 310, 387, 259, 497, 429, 481].
Order [280, 359, 180, 15]. Orders [190].
Oscillator [379, 378]. Oscillator-Based
[379]. Other [355]. Output [545].
Overhead [480].

Paillier [219, 213]. Pairing
[248, 247, 352, 244, 337]. Pairing-Based
[248, 337]. Pairing-Friendly [352]. Pairs
[94]. Paradigm [320, 348]. Parallel
[356, 228, 414, 395, 155]. Parallelepiped
[330]. Parameters [101, 100]. Partial
[258, 392, 265]. Partially [215]. Party [241,
272, 250, 260, 392, 282, 228, 331, 472, 411].
Password [289, 437, 268, 13].
Password-Authenticated [268].
Password-Based [289, 437]. Passwords
[275, 307]. Pattern [357, 450]. Patterns
secrecy [39, 9]. Perfect
[74, 173, 477, 143, 21, 63, 57, 38]. Perfectly
[518, 405]. Periods [66]. permit [22].
Permutation [115, 134, 131, 107, 400, 143].
Permutations
[115, 270, 432, 459, 209, 156, 211, 441, 40].
permutated [61]. PGM [64]. PGV [361].
Photonic [530]. pipelined [79]. PIR [240].
Plaintext [443, 539]. Plaintext-Aware
[443]. plaintexts [26]. Player [173]. Point
[449]. Pollard [398]. Polynomial [136, 184,
286, 345, 430, 315, 423, 485, 479, 263, 38].
Polynomial-Based [485].
Polynomial-Time [286, 345, 315, 479].
polynomials [66]. Possibility [382].
Possible [454]. Power [529, 114].
Powering [251]. Practical [396, 51, 259,
507, 106, 445, 461, 305, 419, 365, 169, 177].
Practical-Time [461]. Predicate
[242, 423]. Predicates [200]. Preface
Preparation [391]. Preprocessing
[240, 114, 122]. Prescribed [211]. Presence
[174, 403, 450, 168, 472, 375]. Preserving
[513, 499, 216]. Primality [297, 281]. Prime
Primitive [124, 378]. Primitives
[270, 250, 305, 145]. PRINCE [483].
PRINCE-Like [483]. Privacy
[230, 129, 84, 216, 313]. Private [541, 466,
295, 276, 193, 351, 269, 302, 516, 240].
Private-Key [269]. Privately [354].
Probabilistic [345, 269, 313, 23].
Probability [224, 18, 309]. Probable [227].
Probably [4]. Problem
[486, 146, 341, 5, 253, 74, 420, 477, 165, 342].
Problems [354, 229, 358, 304, 547, 479].
Procedure [274]. processing [35, 36].
produced [15]. Product [327, 22].
Products [423]. profile [23].
Programmable [406]. Projective [397].
Promised [111]. Proof [518, 45, 278, 443,
74, 82, 116, 111, 138, 331, 255, 86].
Proofs [292, 325, 488, 226, 51, 189, 166, 517, 114,
178, 487, 544, 315, 393, 390, 435, 431, 72, 6].
Properties [316, 82, 112, 60, 64, 58].
Property [451]. Protect [192]. Protected
[164]. Protocol [518, 534, 117, 245, 331, 472,
319, 351, 90, 157, 17, 33, 87]. Protocols
[541, 353, 45, 478, 176, 241, 448, 273, 386,
496, 357, 303, 288, 356, 501, 395, 86].
Provable [480, 285, 95]. Provably
[399, 106, 118, 214, 57]. Provably-Secure
[399, 57]. Providers [193]. Proving [297].
Proxy [394]. Pseudo
[253, 305, 350, 222, 211]. Pseudo-Free [350].
Pseudo-Random [253, 222, 211].
Pseudo-Randomness [305].
Pseudorandom
[471, 131, 225, 121, 47, 476, 156].
Pseudorandomness [48]. Public
[490, 102, 446, 294, 383, 326, 277, 221, 101,
314, 414, 180, 203, 144, 535, 494, 32].
Public-Coin [414]. Public-Key
[102, 446, 294, 383, 277, 101, 180, 44, 494, 32].
PUF [378]. PUFs [530]. Purely [144].
Purposes [349].
Quadratic [281, 111, 190, 274, 180, 90, 8].
Quantum
[466, 278, 323, 391, 407, 255, 516, 177, 54].
Quark [428]. Quasi [544]. Quasi-Adaptive
[544]. Quaternion [194]. Question [197].
Quietly [486].
Rabin [178]. Rackoff [156]. radix [79].
RAM [517]. Random [456, 534, 379, 4, 123,
329, 164, 310, 387, 259, 110, 253, 497, 233,
429, 222, 211, 307, 481, 444, 41, 38, 23].
Randomize [413].
Randomize-Hash-then-Sign [413].
randomized [57]. Randomizer [235].
Randomness [175, 305, 47]. Ranks [355].
rate [63]. Rational [370]. RC4 [441].
Re [388]. Re-Encryption [388]. Reactive
[524]. Real [380, 274, 183, 90].
Real-Quadratic-Field-Based [274].
Real-Time [183]. Realistic [353].
Realizations [546]. Realizing [535].
Rebound [453, 470]. Receiver [158].
Recipient [5]. Reconciliation [129].
Reconciling [212, 301, 532]. Reconsidered

References


REFERENCES


REFERENCES

13

Meier:1989:FCA


Boyar:1989:ISP


Piper:1989:LCS


Abadi:1990:SCE


Nishimura:1990:PMM


Stinson:1990:CAS


Gong:1990:MKD


Boyar:1990:DLI

REFERENCES


REFERENCES


Kaliski:1991:OWP

Golic:1991:GCA

Brickell:1991:EI

Biham:1991:DCL

Feigenbaum:1991:GEI

Beaver:1991:SMP

Brickell:1991:CIS

Maurer:1991:LRP

Naor:1991:BCU
REFERENCES


REFERENCES

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


REFERENCES


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


1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).


REFERENCES

23

Association for Cryptologic Research, 8 (3):115–122, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1995:F


Blackburn:1995:CPK


Stinson:1995:ICC


Pei:1995:ITB


Dyer:1995:KSS


Damgaard:1995:PPS


Heys:1996:SPN

REFERENCES


REFERENCES


Impagliazzo:1996:ECS


Franklin:1996:JEM


Han:1996:PGF


Jackson:1996:ISS


REFERENCES


REFERENCES


Coppersmith:1997:SSP


Jackson:1997:MTA


Kilian:1998:ENZ


Sakurai:1998:SAC


Biham:1998:CMM

REFERENCES


REFERENCES


REFERENCES


Burmester:1999:DSF


Quinn:1999:BKD


Joye:1999:CRB


Shoup:1999:SPI


Blundo:1999:CVC

REFERENCES


REFERENCES


Zbinden:2000:PAQ


Fischlin:2000:SSP


Golic:2000:FCA


Paulus:2000:NPK


Gennaro:2000:RES

REFERENCES

Zhang:2000:MCA


Petrank:2000:CMR


Coppersmith:2000:PAD


Pointcheval:2000:SAD


Gennaro:2000:RBU


Knudsen:2000:DAS

REFERENCES


[193] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Universal service-providers for private information retrieval. Journal of Crypt-
REFERENCES

Coppersmith:2001:WQS


Vaudenay:2001:CCR


Boneh:2001:IEE


Ye:2001:DAA


Wang:2001:SCM


REFERENCES


REFERENCES


REFERENCES

Lindell:2002:PPD


Knudsen:2002:SFC


Shoup:2002:OR


Catalano:2002:PTF


Bellare:2002:NNF


Magliveras:2002:NAD


Myers:2003:EAS


Beimel:2003:BAM

[223] Amos Beimel and Shlomi Dolev. Buses for anonymous message delivery. *Journal of Cryptology: the journal of the In-
REFERENCES


[240] Amos Beimel, Yuval Ishai, and Tal Malkin. Reducing the servers — compu
REFERENCES

48

Canetti:2004:AVN


[241]

Hast:2004:NOS


[242]

Lenstra:2004:P


[243]

Miller:2004:WPE


[244]

Boneh:2004:SSW


[245]

Joux:2004:ORP


[246]

Verheul:2004:EXM


[247]
Barreto:2004:EIP

Naor:2005:CSO

Fitzi:2005:MCP

Cohen:2005:ASW

Dupont:2005:BCA

Gennaro:2005:IPR
REFERENCES


Biham:2005:CSR


Kent:2005:SCB


vonzurGathen:2005:PNB


Avanzi:2005:CCM


Knudsen:2005:PKR


Blundo:2005:ADD

REFERENCES


REFERENCES


[279] Deukjo Hong, Seokhie Hong, Wonil Lee, Sangjin Lee, Jongin Lim, Jaecheul Sung, and Okyeon Yi. Known-IV, known-in-advance-IV, and replayed-and-known-

Girault:2006:FAS


Damgard:2006:EQF


Harnik:2006:CTP


Luca:2006:ECL


Anonymous:2007:EN


Koblitz:2007:ALS

REFERENCES


References


REFERENCES


Gennaro:2007:RES


Gennaro:2007:RBU


Abadi:2007:RTV


Ostrovy:2007:PSS


Kalai:2007:CCS


Goh:2007:ESS

Haastad:2008:PCA


Coppersmith:2008:CII


Nguyen:2008:SSK


Abe:2008:TKN


Selcuk:2008:PSL


Boneh:2008:SSR

REFERENCES


[323] Rahul Jain. New binding-concealing trade-offs for quantum string commit-
REFERENCES

61


[Diem:2008:ICC]


[Bellare:2009:SPI]


[Lempken:2009:PKC]


[Impagliazzo:2009:CTD]


[Charles:2009:CHF]


342] Benjamin Smith. Isogenies and the discrete logarithm problem in

Fischlin:2009:ENM


DiRaimondo:2009:NAD


Goldreich:2010:EPP


Tromer:2010:ECA


Knudsen:2010:CM


Desmedt:2010:NIP

Hofheinz:2010:OCP


Micciancio:2010:RGP


Morrissey:2010:THP


Freeman:2010:TPF


Aumann:2010:SAC


Beimel:2010:HSW


Canetti:2011:UCS


Grassl:2011:CTZ


Asharov:2011:UDC


Fischlin:2011:ENM


Paar:2011:GE


Canivet:2011:GLF


REFERENCES


REFERENCES


[417] Hossein Ghodosi. Analysis of an unconditionally secure distributed oblivious transfer. *Journal of Cryptol-
REFERENCES


Coron:2013:NBC


Chase:2013:MC


Boyar:2013:LMT


Aumasson:2013:QLH


Lu:2013:SAS


Hofheinz:2013:PR


Shacham:2013:CPR

REFERENCES


REFERENCES


Kiyias:2014:OTS


Pass:2014:CZK


SenGupta:2014:NRS


Haitner:2014:NIH


Birkett:2014:SMP


Hong:2014:EBC


Dinur:2014:IPA

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

80


Brakerski:2014:BSD


Longa:2014:FDG


Cramer:2014:ACZ


Bitansky:2014:SSC


Hazay:2014:CSP


Fischlin:2014:RMP


Applebaum:2014:KDM

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


REFERENCES


[Bellare:2014:CCH]


[Dunkelman:2014:PTR]


[Dunkelman:2015:SAE]


[Bellare:2015:SDI]


[Patra:2015:EA]


[Biham:2015:CSR]


[Baumeler:2015:QPI]
REFERENCES

83


Bohl:2015:CGN


Biham:2015:NAI


Sajadieh:2015:ERD


Lamberger:2015:RAS


Berman:2015:NAA


Lindell:2015:EPS


REFERENCES


Bellare:2015:NPN


Peyrin:2015:CAG


Baldi:2016:EPK


Bos:2016:FCG


Coron:2016:HBI


Freedman:2016:ESI

REFERENCES


REFERENCES

Andreeva:2016:NSP

Dinur:2016:KRA

Boyen:2016:UAR

Biham:2016:BA

Smith:2016:CCE

Abe:2016:CSS
REFERENCES


[519] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, and Daniele Venturi. Bounded tamper resilience: How to go beyond the algebraic barrier. Journal of Cryptology: the journal of the
REFERENCES


REFERENCES

Hisil:2017:JCG


Prabhakaran:2017:RNM


Applebaum:2017:LCU


Barak:2017:MKA


Seo:2017:SSD


Lenstra:2017:LS


Asharov:2017:MEO


Blondeau:2017:DLC

REFERENCES

Kiltz:2017:IR


Todo:2017:ICF


Applebaum:2017:PSM


Bitansky:2017:HS


Jutla:2017:SQA


Cohen:2017:FVG

