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/  
26 September 2018  
Version 1.50

Title word cross-reference


0 [465].

Cryptanalytic [93, 434, 444, 239, 155].
Crypto [376]. Cryptogenography [543].
Cryptographers [5]. Cryptographic
[196, 189, 176, 270, 328, 386, 349, 118, 124, 424, 231, 407, 205, 101, 91, 145, 100, 177, 87, 60, 27, 36, 86], cryptographically [29].

Decommitments [382]. Decomposing [198]. Decompositions [96].
Descent [207]. Design [266, 524, 79, 29].
Detailed [187]. Deterministic [446, 286, 482, 553, 563, 577]. DHE [548].

Distinguishers [470]. Distributed [266, 296, 287, 417]. Distribution [278, 266, 255, 97, 167, 177, 20, 7].
Distributions [577, 75]. Divergence [566].

Elementary [91]. Elements [499, 355].
Endomorphism [512]. Endomorphism-Accelerated [512].
Endomorphisms [381]. Enhanced [490].

Faster [381]. Fault [175, 373, 377].
[398, 252, 420, 83, 151, 90, 144, 161, 263, 8].
Finite [199, 102, 398, 252, 326, 221, 263].
first [71]. Fixed [262, 383]. FlipIt [436].
Fly [280]. Forgery [485]. Formal
[212, 301, 292, 33]. Forward [294].
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, 558, 515, 540, 239]. Fully
[433, 487]. Function
[556, 219, 125, 554, 369, 222, 30].
Function-Private [556]. Functional
[556, 562, 551, 89]. Functionalities
[551, 568]. Functions
Further [100].
Gabadulin [314]. Gallant [447]. Game
[514, 436]. Garbling [504, 572]. Gates
[504]. GE [376]. General
[200, 112, 173, 138, 277, 339, 313].
Generalization [10]. Generalized [41].
Generates [85]. Generating [233].
Generation
Generator [253, 179, 298, 15]. Generators
[505, 379, 225, 224, 121, 191, 222, 59, 38].
Generic [513, 452, 320, 311, 424]. Genus
[491, 324, 531, 157, 342]. Geometric [83].
GGH [330]. Given [258, 56]. Giving [51].
Glitch [373]. Glitches [375]. GNUC [475].
Go [519, 224]. Goldreich [242]. Golíč [405].
good [29]. GOST [422]. Graph [96, 408].
Graphs [498, 328]. Grindahl [489]. Group
[499, 102, 289, 2, 288, 319, 350, 384, 85, 91].
Groups [310, 408, 324, 280, 313, 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, 406, 558, 141, 469, 30]. Hash-CBC
[410]. Hashing [442, 397, 159, 98]. having

One [549, 569, 229, 270, 297, 242, 523, 245, 40, 439, 221, 143, 165, 30].
One-More-RSA-Inversion [229].
One-Sided [242, 523]. One-Time [439].
One-Way [549, 569, 270, 221, 143, 40, 30].
Oracles [534, 329, 310, 387, 259, 497, 429, 481].
Oscillator-Based [379]. Other [355].
Output [545]. Overhead [480].

Perfect [74, 173, 477, 143, 21, 63, 57, 38]. Perfectly [518, 405]. Periods [66]. permit [22].
Photonic [530]. pipelined [79]. PIR [240]. Plaintext [443, 539, 577].
Proxy [394]. Pseudo
Pseudo-Free [350].
Pseudo-Random [253, 222, 211].
Pseudo-Randomness [305].
Pseudorandom
[575, 471, 131, 225, 121, 47, 476, 156].
Pseudorandomness [48].
Public [490, 102, 446, 294, 580, 383, 326, 277, 221, 101, 553, 314, 414, 180, 577, 203, 144, 535, 494, 32].
Public-Key [414].
Public-Coin [102, 446, 294, 580, 383, 277, 101, 553, 180, 577, 144, 494, 32].
PUF [378].
PUFs [530].
Purely [144].
Purposes [544].
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].
Queries [554].
Question [197].
Quietly [486].
Rabin [178].
Rackoff [156].
radix [79].
RAM [517].
Randomize [413].
Randomize-Hash-then-Sign [413].
Randomized [549, 551, 57].
Randomizer [235].
Randomness [175, 305, 47].
Ranks [355].
rate [63].
Rather [566].
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 [545].
Rebound [453, 470].
Receiver [158].
Recipient [5].
Recomputation [560].
Reconciliation [129].
Reconciling
[212, 301, 532].
Reconsidered [218].
Recovery [509, 265, 573, 438].
Recursive
[469].
Reduced [261, 465, 445, 453].
Reducing [240, 335].
Reduction [148].
Reductions [123, 304].
Reflection [483].
Registers [130].
Related [575, 93, 461].
Related-Key [575, 461].
Relation [316].
Relations [456, 320].
Relationships [321].
Release [106].
Reliability [313].
Remaindering [168].
Remarks [61].
Remote [391].
Rényi [566].
Repetition [395].
Replayed-and-Known-IV [279].
Reproducible [546].
Requirements [391].
Residue [529].
Residuoity [111].
Resilience [519].
Resilient
[433, 503, 103].
Resistance [488].
Resistant
[107, 376].
Resource [386, 391].
Restricted
[345].
Results [382, 2, 383, 312, 23].
Retrievability [517, 431].
Retrieval
[466, 295, 193, 240].
Revisited
[316, 538, 558, 568, 156, 490, 352].
Rho [398].
Rights [394].
Ring
[329, 510, 424, 378].
Rings [66].
RIPEMD
[125, 515].
RIPEMD-128 [515].
Rivest [37, 195].
RMAC [265].
Robust
[559, 295, 181, 299].
Rotational [453].
Round
[578, 297, 291, 445, 125, 474, 116, 245, 393, 437, 228, 435].
Round-Optimal
[437].
Round-Reduced
[445].
Rounds
[261, 468, 217].
Routing [458].
RSA
RSA-Based
[186, 300].
RSA-OAEP [238].
RSA-signatures [56].
Runtime [430].
SAFER [187, 152].
Sample [204].
SASAS [360].
Scalable [288].
Scalar [447].
Scheme
[229, 147, 294, 462, 149, 400, 255, 169, 55, 61, 20, 69].
Schemes
[506, 399, 498, 325, 96, 170, 394, 46, 134, 132, 509, 404, 500, 343, 371, 418, 213, 280, 304, 142, 158, 118, 120, 137, 206, 485, 481, 256, 122, 63, 77, 81, 65, 25].
Schnorr [122].
SDH [310].
Search [354, 496, 192, 155].
Searchable [316].
Searching [302].
Second
[508].
Second-Preimage [508].
Secrecy
[39, 28, 57, 9, 19].
Supersingular [246]. Supporting [423].
Symbolic [368]. Symbols [529].
Symmetric [418, 568, 85]. Symmetries
[457]. Symmetry [536]. System
[74, 111, 138, 271, 8, 7]. Systems
[45, 82, 116, 50, 128, 87].

Tables [560]. Tag [308]. Tag-KEM [308].
Tag-KEM/DEM [308]. Takeover [436].
Tamper [519]. Tampering [520]. Tandem
[528]. Taxonomy [352]. technique [33].
Techniques [264, 427]. Telephony [461].
Term [364]. Test [281, 227, 59]. Tests
[242, 75]. Text [496]. TF [298]. TF-1 [298].

Theoretical [543, 298]. Theorem
[442, 425]. Theorems [327]. Theoretic
Theory [322]. Thomson [319]. Thorp
[563]. Three [254, 324, 87]. Three-Key
[254]. Threshold [268, 210, 293]. Tight
[304, 481]. Tightly [506]. Tillich [369].
Time [399, 286, 461, 345, 380, 315, 439, 180,
183, 479, 34]. Time-Bound [399].
time-stamp [34]. Timestamping [322].
Timing [303]. TLS [548, 351]. Tolerance
[175]. Tolerating [45]. Toolbox [148]. Toss
[478, 579, 502]. Tossing [228]. Trace [165].
Tracing [202, 256]. Trade [323].
Trade-Offs [323]. Tradeoff [434, 444].
Trading [226]. Traffic [480]. Traitor
[202, 256]. Transfer [537, 160, 296, 291, 117,
417, 397, 390, 411, 570, 249]. Transfers
[230]. Translucent [160]. Trapdoor
[115, 219, 289, 416, 432, 271]. Trapdoors
[221]. Treatment [70]. tree [402]. Trees
[409]. Tripartite [245]. Triple [163, 150].
Triplets [94]. Truncated [54]. Trusted
[137]. Tweakable [385]. Twin [341]. Two
[212, 301, 272, 578, 150, 125, 392, 397, 282,
228, 331, 472, 568, 151, 33, 411]. Two-Key
[150]. Two-Message [397]. Two-Party
[272, 392, 282, 228, 331, 472, 568].
Two-Round [578, 125]. two-way [33].

Type [327]. Types [93].

Unbounded [158]. Unconditional
[5, 255, 28]. Unconditionally
[296, 510, 417, 22]. Undeniable
[186, 300, 384]. Unforgeable [149]. Unified
[482]. Uniform [70]. Uniform-Complexity
70]. Universal
[193, 475, 383, 339, 364, 75, 59].
Universally [272, 368]. Unknown [280].
Unlinkability [480]. Untraceability [5].
UOWHF [533]. Upper [338]. Use [334].
Used [461]. Usefulness [497]. User [81].
Ushakov [319]. Using
[566, 93, 261, 51, 259, 457, 110, 273, 487, 275,
262, 221, 48, 143, 313, 337, 90, 144]. Utility
[370].

Validity [524]. Vanstone [146, 447].
Variant [400]. Varieties [337]. vectors [35].
Verifiable [456, 362, 464]. Verifiably [429].
Verification [412, 524]. Verifier [401].
Versus [545, 276, 175, 241]. Very [498, 227].
Via [517, 549, 160, 297, 411]. View
Vulnerabilities [136]. Vulnerability [83].

Way [549, 569, 270, 221, 143, 33, 40, 30].
Weak [85, 222, 485, 516]. Weaker [562].
Weakness [194]. Weil [247, 207, 244].
Which [56, 393]. Whirlpool [470].
Wildcarded [367]. Window [251]. Wise
[520, 204]. Without [389, 310, 387, 272, 565,
429, 481, 488, 329, 260]. Worst [281].
Worst-Case [281]. Wright [197].

X [438]. X-FCSR [438]. X.509 [33]. X9.52
[208]. XOR [504]. XTR [246].

Yao [331].

Zémor [369]. Zero [541, 45, 115, 226, 51, 147,
166, 426, 448, 114, 6, 273, 487, 74, 70, 82, 116,
393, 138, 52, 390, 435, 477, 143, 414, 440, 21,
REFERENCES


References

Brickell:1988:E

Kaliski:1988:DES

Stinson:1988:SCB

Beauchemin:1988:GRN

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

Chaum:1988:DCP

Feige:1988:ZKP

McCurley:1988:KDS

Buchmann:1988:KES


REFERENCES

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

Nishimura:1990:PMM


Stinson:1990:CAS


Gong:1990:MKD


Boyar:1990:DLI


Simmons:1990:CPC


Niederreiter:1990:CAP


Forre:1990:MID


Walker:1990:ITB


Murphy:1990:CFC

[26] Sean Murphy. The cryptanalysis of FEAL-4 with 20 chosen plaintexts. *Jour-
REFERENCES


[35] Stephen M. Matyas. Key processing with control vectors. *Journal of Cryptol-
REFERENCES


Beaver:1991:SMP


Brickell:1991:CIS


Maurer:1991:LRP


Naor:1991:BCU


Schnorr:1991:ESG


Goutier:1991:SII


Boyar:1991:PZK


Koblitz:1991:ECI


Damgaard:1992:P

REFERENCES

Bennett:1992:EQC


Brickell:1992:IIS


Evertse:1992:WNR


Maurer:1992:CPS


Meier:1992:CPC


Maurer:1992:UST


Lloyd:1992:CBF


Georgiades:1992:SRS

REFERENCES


REFERENCES


Orton:1993:DFP


Menezes:1993:ECC


Lenstra:1993:UIK


Goldreich:1994:DPZ


Klapper:1994:VGS


Chor:1994:SPH


Murphy:1994:WCG


Simmons:1994:PSI


Kemmerer:1994:TSC

REFERENCES


REFERENCES


REFERENCES

177–188, Fall 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).


REFERENCES


[15] Mihir Bellare and Moti Yung. Certify-

Goldreich:1996:HCC


Impagliazzo:1996:ECS


Franklin:1996:JEM

REFERENCES


Dobbertin:1997:RTC


Kaliski:1997:CMA


Fiat:1997:BR


Yacobi:1997:BDK


Cachin:1997:LIR

REFERENCES


Sakurai:1998:SCC


Biham:1998:CMM


Knudsen:1998:AFD


Golic:1998:MCI

REFERENCES


REFERENCES


REFERENCES


[162] Carlo Blundo, Alfredo De Santis, Kaoru Kurosawa, and Wakaha Ogata. On
REFERENCES


[168] Marc Joye, Arjen K. Lenstra, and Jean-


REFERENCES


REFERENCES

Golic:2000:FCA


Paulus:2000:NPK


Gennaro:2000:RES


Zhang:2000:MCA


Petrank:2000:CMR


Coppersmith:2000:PAD

Pointcheval:2000:SAD


Pollard:2000:KMD


Gennaro:2000:RBU


Boyar:2000:SNI


Knudsen:2000:DAS


Jacobson:2000:CDL

REFERENCES


Klapper:2001:ESK


Kilian:2001:HPA


DiCrescenzo:2001:USP


Coppersmith:2001:WQS


Vaudenay:2001:CCR


Boneh:2001:IEE

[196] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of eliminating errors in crypt-


REFERENCES


REFERENCES

Johnston:2002:AKE


Nguyen:2002:IDS


Knudsen:2002:SFC


Shoup:2002:OR


Catalano:2002:PTF

Dario Catalano, Rosario Gennaro, and Nick Howgrave-Graham. Paillier’s...

Bellare:2002:NNF


Magliveras:2002:NAD


Myers:2003:EAS


Beimel:2003:BAM


Golic:2003:EPC


Goldreich:2003:SME


Ben-Or:2003:THI


Muller:2003:PPT

2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lindell:2003:PCT


Bellare:2003:OMR


Brassard:2003:OTP


Joux:2003:SDD


Kalai:2003:GRF


Goldreich:2004:P


Dziembowski:2004:ORE


REFERENCES

49


REFERENCES

51


Considine:2005:BAG


Cachin:2005:ROC


Goldwasser:2005:SMP


Biham:2005:CSR


Kent:2005:SCB


von zur Gathen:2005:PNB

REFERENCES


[276] Markus Bläser, Andreas Jakoby, Maciej Liskiewicz, and Bodo Manthey.


Danny Harnik, Moni Naor, Omer Reingold, and Alon Rosen. Completeness in

Luca:2006:ECL


Anonymous:2007:EN


Koblitz:2007:ALS


Coron:2007:DPT


Gennaro:2007:SDK


Katz:2007:SPA


REFERENCES


REFERENCES

Abe:2008:TKN


Selcuk:2008:PSL


Boneh:2008:SSR


Bentahar:2008:GCI


Lindell:2008:LBI


Renault:2008:PRP


Mihir Bellare and Chanathip Namprempre. Authenticated encryp-


[Wolfgang Lempken, Trung van Tran, Spyros S. Magliveras, and Wandi Wei.](#Lempken:2009:PKC) A public key cryptosystem based on non-abelian finite groups. *Journal of
REFERENCES


Tassa:2009:MSS


Barbosa:2009:CDU


Black:2009:IHE


Haitner:2009:RCA


Rubin:2009:UAV


Dedic:2009:ULB
REFERENCES

Lindell:2009:GCU


Applebaum:2009:CCI


Cash:2009:TDP


Smith:2009:IDL


Fischlin:2009:ENM


DiRaimondo:2009:NAD


Goldreich:2010:EPP

REFERENCES


REFERENCES


REFERENCES

Kidron:2011:IRU


Monnerat:2011:SUS


Lisko:2011:TBC


Garay:2011:RFC


Boneh:2011:ESI


Hohenberger:2011:SOR


Barak:2011:SCA


Lindell:2011:AZK


Jain:2012:RRP


Pietrzak:2012:PRC


References


Pass:2013:PCP

Borghoff:2013:SSD

Freeman:2013:MCL

Ghodosi:2013:AUS

Fujisaki:2013:SIA

Hofheinz:2013:PCC

Joux:2013:ECD
REFERENCES


REFERENCES


Lindell:2013:NCR

vanDijk:2013:FGS

Katz:2013:ROP

Stankovski:2014:ESR

Kiayias:2014:OTS

Pass:2014:CZK

SenGupta:2014:NRS
REFERENCES


REFERENCES


REFERENCES


[476] Eric Miles and Emanuele Viola. On the complexity of constructing pseudorandom functions (especially when they don’t exist). Journal of Cryptology: the journal of the Interna-
REFERENCES


[483] Hadi Soleimany, Céline Blondeau, Xiaoli Yu, and Wenling Wu. Reflection crypt-


REFERENCES


Bos:2016:FCG


Coron:2016:HBI


Freedman:2016:ESI


Yao:2016:CKE


Brown:2016:BRM


Gennaro:2016:AET


Haitner:2016:LUR

Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness

Beimel:2016:SSS


Abe:2016:SPS


Faust:2016:SSS


Lindell:2016:FCC


Moran:2016:OFC


Hazay:2016:LRC


Applebaum:2016:GXG

[504] Benny Applebaum. Garbling XOR gates "for free" in the standard model. *Jour-
REFERENCES


90


REFERENCES


REFERENCES

Haza:2017:EOS


Homma:2017:DMV


Genkin:2017:AC


Komargodski:2017:SSN


Schroder:2017:SBS


Lee:2017:STD

REFERENCES

Benhamouda:2017:ECP


Hisil:2017:JCG


Tajik:2017:PSC


Prabhakaran:2017:RNM


Applebaum:2017:LCU


Barak:2017:MKA

[534] Boaz Barak and Mohammad Mahmoody. Merkle’s key agreement protocol is optimal: An $O(n^2)$ attack on any key agreement from random oracles. Journal of Cryptology: the journal of the International Association for Cryptologic Research, 30(3):699–734, July 2017. CO-
REFERENCES


REFERENCES

Applebaum:2018:MLO


Catalano:2018:PHM


Komargodski:2018:FER


Boura:2018:MIP


Mironov:2018:IDP


Gilboa:2018:HMQ


Choi:2018:BBC

[555] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. A black-box construction of non-malleable encryption from semantically secure encryption. Journal of
REFERENCES


REFERENCES


Abdalla:2018:RKS


Unruh:2018:EMP


Raghunathan:2018:DPK


Chen:2018:MTR


Hofheinz:2018:IPE


Hutter:2018:FMP