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].


2 [507]. 256 [474].

3G [461].

4-Round [393].


Cryptanalytic [93, 434, 444, 239, 155].
Crypto [376]. Cryptogenography [543].
CRYPTOPOST [36].
Cryptosystem [490, 461, 126, 326, 180, 144, 195, 32, 37, 64].


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

Endomorphism [512].
Endomorphism-Accelerated [512].
Endomorphisms [381]. Enhanced [490].
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]. Oversead [480].
Permutation [115, 134, 131, 554, 107, 400, 143].
Plaintext-Aware [443]. plaintexts [26].
Practical-Time [461]. precision [580].
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.

Two-Round

Two-Message

Tweakable

Triplets

Tripartite

Treatment

Trapdoors

Transfers

Translucent

Transitive

Timestamp

time-stamp

Tolerating

Tight

Tightley

Tillich [369].

Time

[399, 286, 461, 345, 380, 315, 439, 180, 183, 479, 34]. Time-Bound [399],
time-stamp [34]. Timestamping [332].

[478, 579, 502]. Tossing [228]. Trace [165].

Tracing [202, 256]. Trade [323].

Trade-Offs [323]. Tradeoff [434, 444].

Trading [226]. Traffic [480]. Traitor
[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 [554]. 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,
72]. **Zero-Knowledge** [45, 115, 226, 51, 147, 166, 426, 448, 114, 273, 487, 70, 82, 116, 393, 138, 52, 390, 435, 477, 143, 6, 74, 21, 72].

References

**Brickell:1988:E**


**Kaliski:1988:DES**


**Stinson:1988:SCB**


**Beauchemin:1988:GRN**


**Chaum:1988:DCP**


**Feige:1988:ZKP**


**McCurley:1988:KDS**


**Buchmann:1988:KES**


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. *Journ-
REFERENCES


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


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


Maurer:1993:CCI


Boyar:1993:CCZ


Chor:1993:SSI


Goldreich:1993:PZK


Schrift:1993:UTN


Rosenbaum:1993:LBA


Capocelli:1993:SSS


Coppersmith:1993:MNF

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

OConnor:1994:ACA

Teng:1994:FIC

Scheidler:1994:KEP

Qu:1994:FEA

Biham:1994:NTC

Davies:1995:PTS

Nyberg:1995:PSA
REFERENCES

Blundo:1995:GDS


OConnor:1995:DCB


Russell:1995:NSC


Vanstone:1995:SRK


Yang:1995:FEB


Maurer:1995:FGP


Blackburn:1995:CPK


Stinson:1995:ICC


Pei:1995:ITB

REFERENCES

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


REFERENCES


[115] Mihir Bellare and Moti Yung. Certify-

Goldreich:1996:HCC


Impagliazzo:1996:ECS


Franklin:1996:JEM


[124] Toshiya Itoh, Yuji Ohto, and Hiroki Shizuya. A language-dependent cryptographic primitive. *Journal of Cryptology: the journal of the International Association for Crypto-
REFERENCES


Dobbertin:1997:RTC


Kaliski:1997:CMA


Fiat:1997:BR


Yacobi:1997:BDK


Cachin:1997:LIR

REFERENCES


Klapper:1997:FSR

Even:1997:CCS

Damgaard:1997:ESH

Biham:1997:IDA


REFERENCES


REFERENCES


REFERENCES


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


Shoup:1999:SPI


Blundo:1999:CVC


Goldreich:2000:P


Franklin:2000:SCM


Hirt:2000:PSG

REFERENCES


Golic:2000:FCA


Paulus:2000:NPK


Gennaro:2000:RES


Zhang:2000:MCA


Petrank:2000:CMR


Coppersmith:2000:PAD

REFERENCES


REFERENCES


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


REFERENCES


**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


Vaudenay:2003:DTB


Kalai:2003:GRF


Goldreich:2004:P


Dziembowski:2004:ORE

REFERENCES


REFERENCES


REFERENCES

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. Pri-


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


REFERENCES


REFERENCES


[320] Mihir Bellare and Chanathip Namprempre. Authenticated encryp-
REFERENCES


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


Lindell:2009:GCU


Applebaum:2009:CCI


Cash:2009:TDP


Smith:2009:IDL


Fischlin:2009:ENM


DiRaimondo:2009:NAD


Goldreich:2010:EPP

REFERENCES


REFERENCES

Cheon:2010:DLP

Konstantinou:2010:EGP

Biryukov:2010:SCS

Black:2010:ABB

Groth:2010:VSS

Barkol:2010:MSS

Muller-Quade:2010:LTS


Dominguez-Oviedo:2011:FBA


Maiti:2011:IRO


Baudet:2011:SOB


Hell:2011:BSC


Galbraith:2011:EFE


Hofheinz:2011:PIR

REFERENCES


Lindell:2011:AZK


Jain:2012:RRP


Gordon:2012:PFS


Katz:2012:WLR


Boldyreva:2012:SPS


Pietrzak:2012:PRC


REFERENCES


[Minder:2012:ETA]


[Hazay:2012:ESO]


[Farras:2012:IMS]


[Smyshlyaev:2012:PBB]


[Hofheinz:2012:PHF]


[Kawachi:2012:CIB]
REFERENCES


REFERENCES


Haitner:2014:NIH


Birkett:2014:SMP


Hong:2014:EBC


Dinur:2014:IPA


Brakerski:2014:BSD


Longa:2014:FDG


Cramer:2014:ACZ

REFERENCES


Abdalla:2014:VRF

Faugere:2014:USI

Amir:2014:AAR

Jean:2014:ICA

Bellare:2014:CCH

Dunkelman:2014:PTR

Dunkelman:2015:SAE
REFERENCES


Lamberger:2015:RAS


Berman:2015:NAA


Lindell:2015:EPS


Dunkelman:2015:ISK


Hofheinz:2015:GNU


Miles:2015:CCP

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-


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

Chandran:2015:AES


Procter:2015:WKF


Aspnes:2015:SAQ


Baldi:2016:EPK

REFERENCES


Bos:2016:FCG


Coron:2016:HBI


Freedman:2016:ESI


Yao:2016:CKE


Brown:2016:BRM


Gennaro:2016:AET


Haitner:2016:LUR

[497] 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

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


REFERENCES

Biham:2016:BA


Smith:2016:CCE


Abe:2016:CSS


Asharov:2016:TGT


Landelle:2016:CFR


Winter:2017:WLC


REFERENCES


[528] Jooyoung Lee, Martijn Stam, and John Steinberger. The security of Tandem–DM in the ideal cipher model. *Jour-
REFERENCES


[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


[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


Asharov:2018:COW


Lindell:2018:FEO


Lyubashevsky:2018:AEL


Lindell:2018:KRA


Canteaut:2018:SCP

Abdalla:2018:RKS

Chen:2018:MTR

Unruh:2018:EMP

Raghunathan:2018:DPK

Hofheinz:2018:IPE

Hutter:2018:FMP