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: https://www.math.utah.edu/~beebe/  
20 August 2024  
Version 1.64

**Title word cross-reference**


0 [465, 672]. 0-RTT [672].
Binding [323].
Binding-Concealing [323]. Birational [134]. Bit
[741, 520, 132, 546, 262, 745, 48, 59].
Bit-Wise [520]. Bitcoin [757]. Bits
[741, 219, 178, 15]. Bivariate [333, 425]. Black
Black-Box [555, 338, 597, 585, 686, 145]. BLEACH
[742]. Blind [229, 185, 527].
Blobs [52, 21]. Block
[643, 279, 201, 141, 385, 104, 469, 232].
Blockcipher [336, 361, 632]. Blockcipher-Based
Bonsai [409]. Boolean [738, 27, 100].
Boomerang [758]. Bootstrapping [719, 664]. Both
[653]. Bound
[399, 162, 740, 76]. Bounded
[519, 291, 235, 158, 236, 332, 237].
Bounded-Storage [235, 332, 237]. Bounds
Box
Boxes [94, 29, 24]. Break
[174]. Break-Ins [174]. Breaking
[741, 495, 380, 139].
Broadcast [732, 565, 258]. Bucket [159].
Bug [511]. Build [492]. Building [252].
Built [698, 703]. Buses [223]. Byzantine
[741, 259, 258].

Cache [346]. Calculation [244]. Calculus
[324, 457]. Can [678, 632, 609, 663, 516, 56].
Candidate [734]. Capacity [262, 516].
Cards [110, 49]. Cartesian [22]. Cascade
[71]. Cascaded [646]. Case
[714, 281, 670]. CBC
[410, 254, 183]. CBCM [208]. CCA
[463, 649]. CCA-Secure [649]. CCA2
[277]. CCA2-Secure [277]. CCITT [33]. CDH
[683]. Centers [266]. Central [270].
Certain [264, 56, 60, 14, 9]. Certificateless
[311]. certification [81]. Certifying [115].
ChaCha [725]. Challenge [463].
Chameleon [460]. Channel [548, 376, 530].
Channels [748, 391, 262, 197, 516].

Characteristic [267, 83, 151, 161].
Characteristics [97]. Characterization
[460, 565, 142, 269]. Chaum [229]. cheaters
Chinese [168]. Choose [411, 501]. Chor
[37, 195]. Chosen
[348, 419, 126, 539, 577, 210, 26].
Chosen-Cipher [348]. Cipher [643, 578, 492, 131, 422, 528, 209, 85, 441, 232, 57].
Ciphers [410, 574, 380, 279, 201, 217, 385, 469, 483, 438, 182, 41, 71, 14, 58, 16].
Ciphertext [317, 574, 348, 419, 210, 751].
Ciphertext-Only [317]. Ciphertexts
[747]. Cipolla [750]. circuit [17]. Circuits
[645, 671, 550, 572, 732]. Circularly [546].
CKKS [742]. Class
[324, 381, 88, 616, 103, 41, 724]. Classes
[593]. Classical [262, 606]. Classification
[46]. Cleaning [742]. Clocked [224].
CLT13 [594]. Clustering [648]. code [62].
Codes [162, 624, 660, 617, 640, 756, 314, 104, 3, 39, 22, 9, 19].
Coding [520, 740]. Coin
[731, 478, 579, 228, 502, 414]. Coin-Tossing
[731, 228]. Collection [711]. Collision
[488, 125, 622, 701, 489, 753, 98, 155].
Collision-Free [125, 98]. Collisions
[749, 680, 365]. COLM [754]. Coloring
[408]. Combinatorial [582, 23, 9].
combinatorics [19]. Combiner
[112, 318]. Combiners [633, 451, 130, 58].
Combining
[654, 605, 182]. Commitment
[132, 343, 371, 335, 158, 323, 262, 48].
Commitments [499, 604, 426, 704].
Communication
[637, 674, 317, 466, 727, 174, 720, 718, 172, 733, 111, 262, 439, 313, 89, 197, 72].
commutative [706]. Compact
[683, 638, 535, 431]. Comparison
[434, 444, 139]. Competitions [746].
Competitive [111]. Compilers [334].
Complete [250, 477]. Completeness
[452, 282, 568]. Complexities [639].
Complexity [637, 674, 705, 264, 466, 687, 693, 696, 718, 448, 200, 70, 335, 597, 476.]
Composability [598, 386, 430, 475, 383, 651, 339, 364].
Composable [757, 449, 272, 368, 592, 597, 585].
Composite [671].
Composite-Order [671].
Composition [320, 176, 673, 303, 652, 312, 339].
Concealing [323]. Concerning [103]. Concrete [610]. Concurrent [303, 356, 500, 647, 312, 440, 494].
Condition [561]. Conditional [674].
Connection [482]. Connectivity [172]. Conscious [729]. Consequences [391].
CryptHOL [628]. Crypto [376]. Cryptogenography [543].
Cryptography [427]. Cryptomania [625]. CRYPTOPOST [36]. Cryptosystem [490, 461, 126, 326, 180, 144, 195, 32, 37, 64].
5

[706]. Cycling [2].

Damgård [749, 400]. Dances [725]. Data
[473, 639, 635, 216, 209, 302, 183, 711, 661, 2].
Data-Dependent [209]. Davies [133]. Day
[692]. Deal [110]. Decentralized [713].
Decision [231]. Decisional [616].
Decodable [624]. Decommitments [382].
Decomposing [198]. Decompositions [96].
Decoration [232]. Decryption
[463, 180]. Deep [726]. Deficiencies [51].
Definition [463]. Definitions [329, 82, 345].
Degree [252, 366, 201, 420, 283]. Delay
[662]. Delegate [409]. Delegation [394].
Delivery [223, 545]. Demytko [126].
Deniable [344, 700]. Dense [498].
Dependence [370]. Dependent
[452, 124, 209]. Derandomization
[699, 686]. derived [66]. DES-like [43].
Descent [207]. Design
[266, 524, 689, 79, 29]. Designated [683].
Designing [221, 24]. Designs [460, 104, 9].
Destructive [334, 207]. DESX [192].
Detailed [187]. Detection [756].
Deterministic
[586, 446, 286, 482, 553, 563, 577]. Device
[610]. DHE [548]. Dichotomy [505].
Dieharder [692]. Differential
[108, 43, 538, 415, 107, 710, 95, 309].
Differentials [261]. Difficult [495].
Difficulty [139]. Diffie
[341, 184, 521, 304, 231, 245, 535, 157, 128].
Diffusion [469]. Digital
[109, 413, 652, 571, 206, 185, 122, 34, 215].
Dimensional [447]. diminished [79].
diminished-radix [79]. Dining [5]. Direct
[327]. Disallowed [463]. Disclosure [674].
Discrete
[146, 21, 358, 184, 634, 742, 366, 457, 253,
287, 74, 190, 420, 745, 188, 139, 165, 342, 55].
Discrete-Log [287]. Dishonest [478].
Disjunctions [423]. Dissection [615].
Distance [566, 41]. Distinguish [554].
Distinguishers [680, 470]. Distributed
[266, 296, 634, 287, 417]. Distribution
[278, 266, 255, 97, 167, 177, 20, 7].
Distributions [708, 669, 577, 75].
Divergence [566]. Divertible [166]. DM
[528]. Dob [759]. document [34]. Domain
[558]. domains [73]. Don't [607, 476].
Double [141]. Drinfeld [203]. DRS [670].
DTLS [748]. Dual [760]. Dynamic
[656, 517, 202, 256].

E0 [318]. E0-like [318]. Easily [233].
ECDSA [681]. ECPP [297]. Edge [484].
Edit [224]. Editor [284, 31, 67, 113, 44].
[723, 720, 235, 694]. Efficient
[604, 645, 537, 353, 199, 567, 248, 460, 738,
529, 336, 387, 574, 672, 615, 149, 343, 371,
119, 493, 181, 299, 304, 158, 700, 357, 403,
523, 587, 118, 439, 138, 547, 585, 359, 472,
605, 255, 571, 38, 244, 717, 222, 464, 469, 49,
438, 346, 662, 592]. Eigenvectors [643].
Elementary [91]. Elements [499, 355].
ELFs [600]. Eliminating [196]. Elliptic
[199, 146, 334, 457, 352, 213, 381, 207, 420,
126, 52, 359, 750, 283, 80, 151, 165, 161, 512,
271, 739, 246, 40]. Embedded [580, 650].
Embedding [283]. EMV [507].
Encapsulation [456]. Encoding [671].
Encodings [549]. Encrypted
[317, 429, 711]. Encryption
[212, 301, 316, 367, 559, 308, 754, 676, 678,
320, 443, 625, 387, 446, 556, 562, 734, 294,
632, 618, 555, 747, 659, 150, 672, 348, 509,
736, 462, 119, 418, 557, 482, 487, 70, 546,
419, 751, 388, 602, 322, 2, 269, 423, 698, 703,
551, 626, 652, 655, 277, 236, 553, 563, 717,
616, 759, 532, 577, 154, 561]. Encryptions
[362]. Endomorphism [512].
Endomorphism-Accelerated [512].
Endomorphisms [381]. Enhanced [490].
Enhancements [432]. EnRUPT [365].
Entropy [669, 482, 752]. Enumerating
[27, 100]. Enumeration [745]. Equations
[136, 423]. Equivalence [286, 635, 593].
Erratum [444].

Error [281]. Errors [196, 708, 742, 706, 715].


Evaluation [496, 564, 17]. Even [578, 509, 462]. Even-Mansour [578].


Extract [316, 537, 199]. Extraction [494]. Extractors [669, 236, 237].


Factoring [495, 286, 419, 55, 7]. Factorization [62]. Factorizations [91].


Faster [381]. Fault [175, 373, 377, 606, 726].

Fault-Based [377]. Fault-Tolerance [175].

Fault-Tolerant [606]. Faults [168, 726].

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

FEAL- [26]. Feasibility [630, 570].


Filter [672]. Finding [749].

Finite [199, 102, 398, 252, 326, 221, 263]. first [71]. Fixed [262, 383]. FlipIt [436].


Formal [212, 301, 292, 658, 33]. Forró [725].

Forward [583, 294, 672]. Forward-Secret [672]. Forward-Secure [583, 294].

Foundations [656]. Four [640, 447].


FPGA-Specific [642]. Fractional [160]. Framework [308, 738, 521, 475, 649, 758]. Franklin [197]. Free [504, 166, 125, 137, 322, 350, 98].

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

Frobenius [281]. Full [518, 691, 680, 422, 558, 515, 540, 613, 239].

Full-permutation [680]. Fully [604, 656, 433, 618, 487, 590, 704, 616].

Function [556, 219, 125, 554, 369, 222, 30].

Function-Private [556]. Functional [625, 556, 562, 747, 736, 698, 703, 551, 626, 616, 89]. Functionalities [551, 652, 568].


Further [100]. Fuzzy [669]. FX [635].

FX-Constructions [635].

Gabidulin [314]. Gallant [447]. Game [514, 628, 436]. Game-Based [628].


Generalization [10]. Generalized [41].

Generates [85]. Generating [233, 661].


Generator [253, 179, 298, 15]. Generators [505, 379, 225, 224, 121, 191, 752, 222, 59, 38].


Glitches [375]. GLP [744]. GNUC [475].
Graded [671]. Graph [96, 727, 408].
Graphs [621, 498, 328]. Grey [607].
Grey-Box [607]. Grindahl [489].
Groups [310, 724, 408, 324, 280, 231, 326, 221].
Grows [667]. GSM [317, 461].

H [380]. Handling [748, 315]. Handshake [688, 700, 351].
Hardness [589, 421, 708, 663, 661].
Hash-CBC [410]. Hashing [589, 442, 397, 750, 159, 98]. having [76].
High-Throughput [728]. Higher [628].
Higher-Order [628]. Highly [336].
Homomorphic-Ciphertext [574].
Hybrid [308, 348, 487]. Hyperelliptic [267, 12, 342, 324]. Hypothesis [629].

IACBC [290]. IAPM [290]. IBE [316, 666].
IDEA [468]. Ideal [46, 492, 404, 142, 120, 528, 65].
Identity-Based [367, 456, 325, 311, 387, 751, 655]. IEC [306].
if [678]. IITM [651]. Im [579]. Imaginary [8]. impersonation [81].
Implementation [248, 160, 102, 373, 375, 32, 21, 80].
Improvement [133]. Improvements [123].
Improving [206]. Incremental [553].
Independent [204]. Index [324, 457].
Indifferiability [492].
Information [541, 374, 466, 240, 295, 129, 193, 543, 104, 25, 17, 63].
Inner [736, 423, 747]. Inner-Product [747].
Integration [418]. Integrity [322, 86].
Isogenies [342]. Isogeny [620].
Isomorphisms [289]. Iterated [509].
Iteration [297]. IV [279].


Kummer [619].

Languages [166, 393]. Large [722, 135, 381, 616]. Large-Scale [722].
Larger [735, 516]. Laser [373]. Latin [725].
Lattice [566, 744, 409, 148, 730, 571, 745, 743].
Lattice-Based [566, 744, 730, 571, 743].
Lattices [631, 536]. Layers [748, 469].
Leakage [675, 687, 693, 696, 433, 599, 584, 500, 700, 503, 707, 701, 606, 726].
Leakage-Resilient [433, 503, 707, 701].
Like [483, 459, 318, 43]. Lilliput [636].
Locking [516]. Log [146, 634, 287, 139].
Logarithm [358, 184, 366, 457, 253, 420, 745, 165, 342, 21].
Luby-Rackoff [156]. Lucifer [108]. LWE [694, 668].

MAC [183, 485]. MACs [254]. Magic [600].
Mapping [184, 198]. Mappings [102, 97].
Maps [641]. Masking [744, 610, 561].
Match [678]. Matching [357, 450].
Matchmaking [678]. Matrices [643].
Matrix [20]. Matroid [142]. Maximum
[182]. May [495]. McEliece [490]. MD2
[347]. MD4 [153]. Me [678, 642]. Means
[648]. Median [355]. Meet [644, 18].
Meet-in-the-Middle [644]. Memory
[639, 635, 112, 130, 318, 58]. Menezes
[146]. Menezes-Okamoto-Vanstone
[146]. Mercurial [426]. Merkle
[749, 534, 596, 400]. Merlin [541]. Mesh
[510]. Message
[452, 223, 480, 550, 119, 397, 322, 126, 159].
Message-Efficient [119]. Messages
[541, 637, 254, 76]. Messaging [658].
Methodology [524]. Methods [24].
Microprocessors [580, 650]. Middle
[644, 214, 18]. Midori64 [613]. Minicrypt
[709, 626]. Minimal
[592, 250, 172, 503, 551, 66, 28].
Minimization [427]. Minimize [487].
Minimizing [549, 578]. Mining [216].
Minority [45]. missing [15]. MISTY1
[540]. ML [66]. ML-sequences [66]. Mode
[208]. Model
[591]. Models [588, 443, 584, 172, 383, 494].
Modes [140, 163, 290, 279, 602, 322].
Modifications [78]. Modular
[225, 351, 79]. Module [708]. Modules
[203]. Money [695, 665]. Monopoly [188].
Montgomery [377]. MOV [252]. MPC
[723, 727, 722, 720, 718, 654]. MPClan
[729]. Much [516]. Müller [750]. Multi
Multi-authority [713]. Multi-ciphertext
[751]. Multi-collison [753].
Multi-Exponentiation [264]. Multi-input
[562]. Multi-instance [751]. Multi-Party
[241, 250, 260, 585, 605, 737, 576].
Multi-precision [580, 650].
Multi-Property [451]. Multi-string [455].
Multi-theorem [631]. Multi-Verifier
[401]. Multicast [313, 197].
Multidimensional [581]. Multilinear
[641, 594]. Multipartite [404, 333].
Multiparty [731, 518, 45, 478, 653, 738, 176, 545, 565, 691, 173, 339, 717, 464]. Multiple
[140, 279, 69, 120]. Multiplication
[580, 650, 447, 151]. Multiplicative [363].
multiplier [79]. Multisignatures [429].
Multivariate [560, 759]. Must [727, 135].
Mutual [374]. Mutually [137]. My [724].
Nearly [731, 242]. Necessary [98]. Needed
[554]. Negligible [220]. Neighbor [313].
Network [603]. Networks
[276, 105, 748, 107, 313]. Never [665]. NFS
[745]. NIZK [544, 721]. NIZKs [683, 631].
NMAC [488]. No [716]. No-Signaling
[716]. Noisy [584]. Non
Non- [441]. Non-abelian [326, 408].
Non-Adaptive [241, 471]. Non-black-box
[590]. Non-commutative [706].
Non-hyperelliptic [324]. Non-Interactive
[702, 189, 627, 487, 694, 649, 477, 332, 668].
Non-malleability [532]. Non-Malleable
[371, 647, 520, 555, 659, 624, 660, 343, 640, 756]. Nonces [215]. Noncommutative
[479]. Noncommutative-Algebraic [479].
Noninteractive [115, 138]. Nonlinear
[667, 375, 103, 613, 182]. Nonlinearity [92]. nonuniform [75]. Normal [263]. NORX
Notions [320, 321, 269]. NP
Number
[379, 738, 592, 667, 752, 298, 78, 38].
Numbers [4, 233, 101].
OAEPA [238, 539, 218]. Obfuscating
[671, 522, 388]. Obfuscation
[641, 569, 705, 449, 599, 454, 349, 740].
Obfustopia [625, 698, 703, 626]. Oblivious


Permutations [569, 115, 270, 432, 459, 209, 156, 211, 441, 40]. permuted [61]. PGM [64]. PGV [361].


Practical [396, 639, 51, 259, 574, 550, 114, 623, 636, 622, 305, 419, 365, 169, 613, 177, 561].


Preserving [513, 499, 604, 586, 697, 589, 673, 593, 216]. Prevailing [760]. PRFs [760, 564].


Pseudo-Randomness [305].


Pseudo-Random [253, 222, 211]. Pseudo-Randomness [305].

Pseudorandom [575, 471, 131, 225, 121, 47, 476, 156].


Randomize-Hash-then-Sign [413]. Randomized [549, 551, 57]. Randomizer [235]. Randomness [175, 305, 47]. Ranks [355]. Rate [640, 63]. Rather [566].


Real [738, 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]. Recomputation [560].

Reconciliation [129]. Reconciling [212, 301, 532]. Reconsidered [218].


 Registers [130]. Related [575, 93, 461].

Related-Key [575, 461]. Relation [316].


Reloaded [725]. Remainerding [168].


Replayed-and-Known-IV [279]. Reproducible [546]. Requirements [391].

Residue [529]. Residuosity [111].

Resilience [723, 675, 720, 599, 519, 606].
Resilient [433, 503, 707, 701, 103].
Reusable [669]. Revisited [316, 637, 538, 719, 558, 590, 568, 710, 156, 440, 395, 527, 612]. Revisiting [723, 629].
RLWE-Based [717]. RMAC [265]. Robust [559, 295, 451, 748, 181, 299, 737].
Root [750]. Rotational [453, 710, 642].
Round [639, 578, 297, 673, 644, 291, 445, 125, 474, 116, 622, 608, 654, 245, 393, 437, 585, 701, 228, 435, 605, 685, 737, 642].
RSA-Based [186, 300]. RSA-OAEP [238].
Schnorr [595, 122]. SCREAM [613]. SDH [310]. Search [354, 496, 192, 155].
Servers [240]. Service [193].
Service-Providers [193]. Session [275, 307]. Session-Key [275, 307]. Set [415, 272, 493, 357, 403, 504].
SHA-1 [465]. SHA-3 [622]. Shamir [298].
Shannon [10]. Share [135, 11]. shares [77].
Sharing [370, 363, 498, 675, 96, 46, 634, 404, 181, 299, 142, 707, 120, 137, 682, 526, 464, 293, 333, 63, 77, 73, 69, 65]. Shift [130].
Short [582, 247, 310, 708, 189, 412, 384, 307, 535, 99].
Shorter [659, 544]. Should [354, 463].


Yao [331].


References


REFERENCES


REFERENCES


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


WALKER:1990:ITB


MURPHY:1990:CFC


MITCHELL:1990:EBF


GODELEWSKI:1990:KMC


ADAMS:1990:SDC


MERKLE:1990:FSO


BERSON:1991:GEI


AGNEW:1991:IFP

[33] Klaus Gaarder and Einar Snekkenes. Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol. *Journal of Cryptology: the journal of the International Association for Cryptologic Re-
REFERENCES


Haber:1991:HTD


Matyas:1991:KPC


Pastor:1991:CCA


Lenstra:1991:CRK


Micali:1991:EPP


DeSoete:1991:NBC


Kaliski:1991:OWP


Golic:1991:GCA


Brickell:1991:EI

References

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

Biham:1991:DCL


Feigenbaum:1991:GEI


Beaver:1991:SMP


Brickell:1991:CIS


Maurer:1991:LRP


Naor:1991:BCU


Schnorr:1991:ESG


Goutier:1991:SII


Boyar:1991:PZK

REFERENCES

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


REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Details</th>
</tr>
</thead>
</table>
REFERENCES

1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Coppersmith:1993:MNF


Orton:1993:DFP


Menezes:1993:ECC


Lenstra:1993:UIK


Goldreich:1994:DPZ


Klapper:1994:VGS


Chor:1994:SPH


Murphy:1994:WCG


Simmons:1994:PSI

REFERENCES

Kemmerer1994TSC


OConnor1994ACA


Teng1994FIC


Scheidler1994KEP


Qu1994FEA


OConnor1994ANA


Biham1994NTC


Davies1995PTS

REFERENCES

Nyberg:1995:PSA


Blundo:1995:GDS


OConnor:1995:DCB


Russell:1995:NSC


Vanstone:1995:SRK


Yang:1995:FEB


Maurer:1995:FGP


Blackburn:1995:CPK


Stinson:1995:ICC

173, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).


REFERENCES


Itoh:1997:LDC


Dobbertin:1997:RTC


Kaliski:1997:CMA


Fiat:1997:BR


Yacobi:1997:BDK

REFERENCES

Cachin:1997:LIR


Klapper:1997:FSR


Even:1997:CCS


Damgaard:1997:ESH

Biham:1997:IDA


Coppersmith:1997:SBP


Jackson:1997:MTA

Kilian:1998:ENZ


Sakurai:1998:SCC


Biham:1998:CMM


Knudsen:1998:AFD


Golic:1998:MCI

REFERENCES

Naor:1998:PZK

Scheidler:1998:PKC

Schnorr:1998:BBM

Balasubramanian:1998:IEC
http://link.springer.de/link/service/journals/00145/tocs/01102.html.


REFERENCES

Murphy:1998:AS  

Dobbertin:1998:CM  

Rogaway:1998:SOE  

vanOorschot:1999:PCS  

Naor:1999:CPP  
REFERENCES


REFERENCES


REFERENCES


Coppersmith:2000:PAD


Pointcheval:2000:SAD


Gennaro:2000:RBU


Knudsen:2000:KMD


Pollard:2000:KMD


Boyar:2000:SNI

Jacobson:2000:CDL


Klapper:2001:ESK


Kilian:2001:HPA


Coppersmith:2001:WQS


Vaudenay:2001:CCR

REFERENCES


Jakobsen:2001:ABC


Fiat:2001:DTT


Scanlon:2001:PKC


Kurosawa:2001:AWI


Lenstra:2001:SCK


Micalli:2002:IES


Galbraith:2002:ECP


Johnston:2002:AKE


Nguyen:2002:IDS


Lindell:2002:PPD


Knudsen:2002:SFC


[226] Michael Ben-Or and Dan Gutfreund. Trading help for interaction in statisti-
REFERENCES

50


Muller:2003:PPT


Lindell:2003:PCT


Bellare:2003:OMR


Brassard:2003:OTP


Joux:2003:SDD


Vaudenay:2003:DTB


Kalai:2003:GRF


Goldreich:2004:P


REFERENCES


REFERENCES


REFERENCES

von zur Gathen: 2005: PNB


Avanzi: 2005: CCM


Knudsen: 2005: PKR


Blundo: 2005: ADD


Denef: 2006: EKA


MacKenzie: 2006: TPA


Katz: 2006: CSN

REFERENCES


Chang:2006:IBO


Teske:2006:ECT


Canetti:2006:LUC


Goldreich:2006:SKG


Jacobson:2006:IRQ


Garay:2006:SZK


REFERENCES


REFERENCES


Abadi:2007:RTV


Ostrovsky:2007:PSS


Kalai:2007:CCS


Goh:2007:ESS


Haastad:2008:PCA


Coppersmith:2008:CII

REFERENCES

Nguyen:2008:SSK


Abe:2008:TKN


Selcuk:2008:PSL


Boneh:2008:SSR


Bentahar:2008:GCI


Lindell:2008:LBI


Renault:2008:PRP

REFERENCES


Overbeck:2008:SAP


Katz:2008:HEP


Lu:2008:CEL


Matucci:2008:CSP


REFERENCES


REFERENCES


[370] Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair ratio-

Fischlin:2011:ENM


Paar:2011:GE


Canivet:2011:GLF


Batina:2011:MIA


Nikova:2011:SHI


Poschmann:2011:SCR

[376] Axel Poschmann, Amir Moradi, Khoong Ming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than
REFERENCES


REFERENCES


<table>
<thead>
<tr>
<th>Reference</th>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Volume</th>
<th>Pages</th>
<th>Year</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pietrzak:2012:PRC</td>
<td>Krzysztof Pietrzak and Douglas Wikström</td>
<td>Parallel repetition of com-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


[401] Tom Roeder, Rafael Pass, and Fred B. Schneider. Multi-verifier signatures. *Journal of Cryptology: the jour-
REFERENCES


REFERENCES


Aumasson:2013:QLH

Lu:2013:SAS

Hofheinz:2013:PRC

Shacham:2013:CPR

Goldreich:2013:ETP

Boyle:2013:FLR

Hong:2013:CCT
Lindell:2013:NCR


vanDijk:2013:FGS


Katz:2013:ROP


Kiaayias:2014:OTS


Pass:2014:CZK


SenGupta:2014:NRS

Haitner:2014:NIH


Birkett:2014:SMP


Hong:2014:EBC


Dinur:2014:IPA


Cramer:2014:ACZ


Longa:2014:FDG


Dinur:2014:IPA

REFERENCES


REFERENCES

Abdalla:2014:VRF


Faugere:2014:USI


Amir:2014:AAR


Jean:2014:ICA


Bellare:2014:CCH


Dunkelman:2014:PTR


Dunkelman:2015:SAE

REFERENCES

Bellare:2015:SDI


Patra:2015:EAV


Biham:2015:CSR


Sajadieh:2015:ERD


Bohl:2015:CGN


Biham:2015:NAI


Sa

Lamberger:2015:RAS


Berman:2015:NAA


Lindell:2015:EPS


Ahn:2015:CAD


Hofheinz:2015:GNU


Dunkelman:2015:ISK


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-
REFERENCES


[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

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


Cash:2017:DPR


Asharov:2017:FPB


Cheraghchi:2017:NMC


Escala:2017:AFD


Brakerski:2017:OC

[522] Zvika Brakerski and Guy N. Rothblum. Obfuscating conjunctions. *Journal of Cryptology: the journal of the...
REFERENCES

Haza:2017:EOS


Homma:2017:DMV


Genkin:2017:AC


Komargodski:2017:SSN


Schro:2017:SBS


Lee:2017:STD

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


REFERENCES

98


Jutla:2017:SQA


Cohen:2017:FVG


Hajiabadi:2017:RCS


Kiltz:2017:EAH


Jager:2017:ACC

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

100


Asharov:2018:COW


Lindell:2018:FEO


Lyubashevsky:2018:AEL


Gueron:2018:FGC


Minaud:2018:KRA


Canteaut:2018:SCP


REFERENCES


[587] Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, Tomas Toft, and Angelo Agatino Nicolosi. Efficient RSA


Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous
REFERENCES


[599] Dana Dachman-Soled, S. Dov Gordon, Feng-Hao Liu, Adam O’Neill, and Hong-Sheng Zhou. Leakage resilience from program obfuscation. *Journal of Cryptology: the journal of the International Association for Crypto-

Zhandry:2019:ME


Oliveira:2019:KCQ


Jovanovic:2019:BCS


Dachman-Soled:2019:ONR


Abe:2019:EFS


Lindell:2019:ECR

REFERENCES


REFERENCES


[618] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène.
REFERENCES


REFERENCES


REFERENCES


REFERENCES


[662] Benjamin Wesolowski. Efficient verifiable delay functions. *Journal of
REFERENCES


Canetti:2021:RFE


Ducas:2021:LSA


Applebaum:2021:OCC


Derler:2021:BFE


Cohen:2021:RPP


Applebaum:2021:PCD


Benhamouda:2021:LLR


REFERENCES


[688] Benjamin Dowling, Marc Fischlin, Felix Günther, and Douglas Stebila. A


REFERENCES

Radian:2022:SQM

Bogdanov:2022:CUSb

Asharov:2022:LPO

Kitagawa:2022:OBSa

Bitansky:2022:NPC

Hashimoto:2022:EGC
REFERENCES


Boudgoust:2023:HML


Alamati:2023:MPA


Liu:2023:RDL


Pointcheval:2023:TCC


Applebaum:2023:CLC


Datta:2023:DMA


Asharov:2023:ORW

[714] Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, and Elaine Shi. Oblivious


Kitagawa:2023:NS


Chida:2023:FLS


Appan:2023:REA


Bouvier:2023:WRM


Coutinho:2023:LDR


Saha:2023:LYF

REFERENCES


[733] Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Actively secure garbled circuits with constant communication overhead in the

Brakerski:2023:CIH


Bergerat:2023:POL


Dowerah:2023:UPI


Tian:2023:CAE

[739] Song Tian. Cover attacks for elliptic curves over cubic extension fields. *Journal of Cryptology: the journal of the International Association for Crypto-
REFERENCES


REFERENCES

Bernstein:2024:CC


Cini:2024:IPF


Fischlin:2024:RCH


Akshima:2024:TSL


Koshelev:2024:HEC


Hofheinz:2024:IBE


Lubicz:2024:ECO

[752] David Lubicz and Viktor Fischer. Entropy computation for oscillator-based

**Rothblum:2024:CRM**


**Andreeva:2024:CAE**


**Blocki:2024:BHF**


**Kiayias:2024:CNM**


**Badertscher:2024:BTL**


**Yang:2024:ORB**

2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).
