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

E-mail: `beebe@math.utah.edu`, `beebe@acm.org`, `beebe@computer.org` (Internet)
WWW URL: `https://www.math.utah.edu/~beebe/`

08 October 2025
Version 1.66

Title word cross-reference

1 [276]. 2 [491, 267, 531, 130]. 2^k [529]. 3 [342]. 31 [261]. 4 [26]. 8 [474]. $^+$ [356]. C^* [759]. d [363]. $\mathrm{GF}(2^m)$ [68]. k [276, 648, 638, 204, 402]. $L(1/3)$ [366]. $\mathbf{Q}$ [512]. NC^1 [638, 713]. $nL3 \bmod 4$ [227]. $O(n)$ [219]. $O(n^2)$ [534]. $O(\sqrt{n})$ [741, 761]. p [91]. S [29, 94, 24, 88]. $1\vec{/}p$ [653].

-Adic [130]. **-Bit** [741]. **-Box** [88]. **-Boxes** [94, 29, 24]. **-Connected** [276]. **-curve** [512]. **-Group** [91]. **-Lin** [638]. **-Means** [648]. **-Multiplicative** [363]. **-Round** [474]. **-Secure** [653]. **-th** [529]. **-tree** [402]. **-Wise** [204].

0 [465, 672]. **0-RTT** [672].

1 [465, 306, 298]. **1.3** [748]. **128** [515]. **16** [380]. **192** [474].

2 [507]. **256** [474].

3 [622]. **3G** [461].

4-Round [393].

521-Bit [745].

9796 [306, 507]. **9796-1** [306]. **9796-2** [507].

ABE [713, 638]. **abelian** [326, 408, 682, 91, 337]. **Abstract** [117]. **Accelerated** [512]. **Accelerating** [398]. **Access** [717]. **Access-Structure** [717]. **Accumulators** [730]. **Achievable** [772]. **Achieve** [603, 609, 477]. **Acoustic** [525]. **Action** [771]. **Actively** [779, 733, 690].

Adaptive [241, 544, 390, 471]. **Adaptively** [718, 523, 638, 649, 390, 577]. **Adaptively-Chosen** [577]. **Adic** [130]. **Advance** [279]. **Adversarial** [458]. **Adversaries** [723, 353, 722, 345, 357, 403, 450, 472, 501, 236]. **Adversary** [173]. **AE** [636]. **AES** [639, 373, 474, 775, 346, 642, 459]. **AES-192** [474]. **AES-256** [474]. **AES-like** [459]. **Affine** [635]. **after** [76]. **Again** [670]. **Against** [723, 353, 480, 687, 693, 696, 520, 725, 348, 500, 357, 776, 524, 214, 192, 265, 95, 485, 622, 236, 210]. **Aggregate** [429]. **Aggregation** [715]. **Agreement** [534, 741, 259, 258, 260, 128]. **AKS** [297]. **Alerts** [486]. **Algebraic** [709, 519, 521, 564, 201, 64, 92, 479]. **Algebras** [706]. **Algorithm** [146, 398, 251, 267, 377, 366, 74, 750, 765, 780, 402, 154, 79, 215]. **Algorithms** [582, 434, 88, 444]. **All-But-Many** [557]. **Almost** [731, 778, 484, 751, 322, 667, 204, 535]. **Almost-Everywhere** [484]. **Almost-Optimally** [731]. **Alternative** [160]. **among** [320]. **Amortized** [448]. **Amplification** [452, 421, 230, 129, 222]. **Analysis** [588, 374, 320, 480, 361, 266, 368, 251, 658, 644, 688, 413, 417, 305, 424, 192, 187, 765, 780, 351, 152, 88, 759, 441, 530, 182, 33, 87]. **Anonymous** [316, 223, 510, 593]. **ANSI** [208]. **Answer** [197]. **Any** [534, 744, 115, 610, 143]. **Application** [199, 289, 225, 407, 470, 759, 159, 36]. **Applications** [709, 678, 123, 427, 648, 341, 426, 624, 672, 615, 634, 149, 771, 546, 406, 439, 204, 92, 743, 155]. **Applied** [408]. **Apply** [763]. **Applying** [33]. **Approach** [482, 10, 23]. **Approaches** [344, 221]. **Approximation** [184]. **Arbiter** [530]. **Arbitrary** [254, 252]. **Arbitrary-Length** [254]. **arbitration** [22]. **Arguments** [764, 702, 763, 730, 143, 185]. **Arithmetic** [68, 199, 738, 550]. **Arthur** [541]. **ASASA** [573]. **Aspects** [177]. **Assessment** [726]. **Assignment** [399, 69]. **Assumption** [760, 310, 238, 683, 616]. **Assumptions** [513, 588, 760, 467, 562, 272, 521, 572, 335, 503, 424, 138, 551, 277, 663, 665]. **Asymmetric** [418, 198]. **Asymptotically** [571]. **Asynchronous** [723, 259, 720, 464]. **Attack** [396, 534, 133, 348, 377, 461, 636, 422, 214, 126, 539, 265, 470, 95, 489, 210, 438, 613, 41]. **Attacks** [508, 633, 567, 639, 93, 468, 511, 607, 560, 373, 644, 445, 509, 584, 474, 462, 179, 224, 622, 524, 279, 657, 201, 453, 141, 573, 314, 485, 726, 739, 346, 239, 758, 198, 14]. **Authenticated** [473, 458, 754, 320, 174, 632, 548, 214, 602, 288, 437, 268]. **Authentication** [389, 162, 147, 289, 344, 280, 547, 104, 159, 3, 39, 33, 76, 22, 9, 19, 25]. **authentication/secrecy** [39, 9]. **Authenticators** [550]. **Authenticity** [657]. **Authority** [137, 713]. **Authority-Free** [137]. **Automata** [496]. **Automated** [588]. **Automorphisms** [745]. **Auxiliary** [446, 358]. **Auxiliary-Input** [446]. **Average** [769, 281]. **Average-** [281]. **Average-Case** [769]. **Aware** [443].

Back [541]. **Bad** [692]. **Balanced** [405]. **Bandwidth** [755, 256]. **Bandwidth-Hard** [755]. **Barrier** [575, 741, 519, 686]. **Based** [367, 456, 566, 248, 744, 628, 379, 115, 325, 311, 591, 336, 361, 387, 373, 289, 632, 377, 777, 771, 493, 620, 186, 253, 300, 287, 496, 280, 751, 274, 602, 168, 321, 315, 437, 83, 655, 326, 730, 501, 571, 209, 384, 717, 485, 663, 337, 203, 198, 743, 17, 55, 8, 61, 41, 752, 79, 314, 694]. **Bases** [263]. **Basing** [270]. **Basis** [409]. **Batch** [412, 127, 128]. **Battery** [692]. **BDH** [713]. **Be** [463, 495, 135, 727, 56, 663, 516]. **being** [71]. **Benefits** [345]. **Best** [653, 454, 740]. **Best-Possible** [454]. **Better** [446]. **Between** [407, 321]. **Beyond**

[575, 519, 740, 602, 737]. **BFV** [719]. **BGV** [719]. **BGW** [518]. **Bias** [505]. **Bicomposite** [615]. **BICYCL** [724]. **Bijective** [97]. **Bilinear** [310]. **Binary** [66, 112, 60]. **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]. **BKZ** [765, 780]. **Black** [555, 338, 597, 585, 686, 145, 590]. **Black-Box** [555, 338, 597, 585, 686, 145]. **BLEACH** [742]. **Blind** [229, 185, 527]. **Blobs** [52, 21]. **Block** [643, 279, 422, 201, 141, 385, 104, 469, 232]. **Blockcipher** [336, 361, 632]. **Blockcipher-Based** [336, 632]. **Bloom** [672]. **Bluetooth** [561]. **BMR** [654, 605]. **Bonsai** [409]. **Boolean** [738, 27, 405, 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** [749, 755, 338, 110, 200, 312, 104, 167, 3, 63, 39, 25]. **Box** [607, 555, 338, 597, 585, 88, 686, 145, 590]. **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** [769, 252]. **Built** [698, 703]. **Bulletproofs** [766]. **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, 768, 769, 281, 670]. **CBC** [410, 254, 183]. **CBCM** [208]. **CCA** [463, 649]. **CCA-Secure** [649]. **CCA2** [772, 277]. **CCA2-Secure** [277]. **CCITT** [33]. **CDH** [683]. **Ceno** [781]. **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** [11]. **Chernoff** [327]. **Chernoff-Type** [327]. **Chinese** [168]. **Choose** [411, 501]. **Chor** [37, 195]. **Chosen** [348, 419, 126, 539, 577, 210, 26]. **Chosen-Ciphertext** [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, 767, 550, 572, 733]. **Circularly** [546]. **CKKS** [742]. **CL** [764]. **Class** [324, 381, 88, 616, 103, 41, 724]. **Classes** [593]. **Classical** [262, 606]. **Classification** [46]. **Cleaning** [742]. **Clocked** [224]. **CLT13** [594]. **Clustering** [648]. **CNF** [770]. **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** [770, 683, 638, 535, 431]. **Comparison** [434, 444, 139]. **Compatible** [763]. **Competitions** [746]. **Competitive** [111]. **Compiler** [767]. **Compilers** [334]. **Complete** [250, 765, 780, 477]. **Completeness** [452, 282, 568]. **Complexities** [639]. **Complexity** [637, 674, 705, 264, 466, 687, 693, 696, 718, 448, 200, 70, 335, 597, 476, 685, 737, 89, 72, 23]. **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]. **Compositions** [198]. **Comprehensive** [374]. **Compress** [125]. **Compressing** [705]. **Compression** [574]. **Computable** [533, 712, 237]. **Computation** [355, 621, 732, 514, 518, 389, 240, 653, 738, 276, 687, 693, 696, 272, 484, 545, 565, 691, 630, 408, 250, 119, 728, 260, 392, 282, 523, 608, 623, 173, 585, 652, 606, 228, 339, 331, 411, 472, 605, 752, 745, 464, 685, 737, 576]. **Computational** [212, 301, 482, 282, 231, 407, 139, 479]. **Computationally** [450, 249, 395]. **Computations** [196, 742, 729]. **computed** [56]. **Computing** [473, 286, 190, 711]. **Concealing** [323]. **Concerning** [103]. **Concrete** [610]. **Concurrent** [303, 356, 590, 647, 312, 440, 494]. **Condition** [561]. **Conditional** [674]. **Conditionally** [57]. **Conditionally-perfect** [57]. **Conditions** [98]. **Confidence** [227]. **Confidential** [548]. **Confidentiality** [657]. **Confined** [467]. **congruential** [15]. **Conjecture** [103, 405]. **Conjunctions** [522]. **Connected** [276]. **Connection** [482]. **Connectivity** [172]. **Conscious** [729]. **Consequences** [391]. **Consistency** [316]. **Constant** [513, 340, 291, 593, 116, 608, 654, 733, 640, 701, 228, 435, 605]. **Constant-Round** [291, 116, 608, 701, 228, 435, 605]. **Constant-Size** [513, 593]. **Constantinople** [259]. **Construct** [116]. **Constructing** [569, 476, 211, 237]. **Construction** [555, 492, 131, 225, 305, 700, 585, 277, 156, 88, 512, 22, 9]. **Constructions** [456, 513, 410, 329, 311, 254, 635, 416, 482, 649, 3, 39]. **Constructive** [334, 207]. **Continuous** [756]. **Continuously** [660]. **Contrast** [170]. **control** [35]. **Conventional** [602]. **Coordinates** [531]. **Coppersmith** [425]. **Core** [200]. **Correct** [370]. **Correcting** [692]. **Correction** [712, 693, 696, 780, 684]. **Correctness** [699]. **Correlation** [643, 416, 112, 179, 224, 58, 182, 41, 14]. **Correlation-Secure** [416]. **Corruptions** [484]. **Cost** [654, 239]. **Counter** [164]. **Counterexamples** [103]. **Countermeasure** [524]. **Countermeasures** [346]. **Counting** [60]. **Cover** [739]. **Covering** [617]. **Covert** [353, 357, 439, 501]. **Credentials** [593]. **CRS** [597]. **CRT** [612]. **CRT-Exponent** [612]. **Cryptanalysis** [317, 108, 140, 163, 208, 261, 465, 360, 102, 538, 415, 614, 594, 306, 507, 725, 153, 525, 369, 581, 107, 657, 459, 347, 515, 710, 318, 319, 330, 309, 483, 540, 298, 195, 561, 43, 26]. **Cryptanalyst** [148]. **Cryptanalytic** [93, 615, 635, 434, 444, 239, 155]. **CryptHOL** [628]. **Crypto** [376]. **Cryptogenography** [543]. **Cryptographers** [5]. **Cryptographic** [588, 746, 196, 189, 176, 270, 328, 598, 673, 688, 386, 349, 118, 124, 424, 231, 407, 205, 101, 91, 663, 145, 100, 177, 665, 87, 60, 27, 36, 86]. **cryptographically** [29]. **Cryptography** [212, 301, 340, 264, 566, 199, 334, 160, 170, 607, 491, 259, 381, 455, 503, 580, 650, 92, 337, 479, 198, 10, 54, 724]. **Cryptologic** [204]. **Cryptology** [427]. **Cryptomania** [625]. **CRYPTOPOST** [36]. **Cryptosystem** [490, 461, 126, 326, 180, 144, 195, 32, 37, 64].

Cryptosystems [248, 529, 287, 168, 649, 221, 314, 139, 203, 210, 161, 237, 246, 43, 28, 12, 80]. **Csiszár** [740]. **Cubic** [144, 739, 62]. **Cuckoo** [589]. **Curve** [199, 146, 334, 213, 381, 420, 126, 52, 161, 271, 246, 80, 512]. **Curves** [774, 267, 324, 252, 366, 457, 352, 381, 207, 531, 359, 750, 283, 151, 601, 165, 342, 512, 739, 40]. **Cut** [411, 501]. **Cut-and-Choose** [411]. **Cut-and-Choose-Based** [501]. **Cyclic** [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]. **Decorrelation** [232]. **Decrypting** [768]. **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, 776]. **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]. **Duplex** [779]. **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]. **Editorial** [1, 42, 372, 684, 679]. **Efficiency** [723, 720, 235, 694]. **Efficient** [604, 645, 537, 353, 199, 567, 248, 764, 460, 738, 529, 336, 387, 767, 763, 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]. **Electronic** [771]. **Elementary** [91]. **Elements** [499, 355]. **ELFs** [600]. **Eliminating** [196]. **Elliptic** [199, 146, 334, 774, 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, 772, 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]. **Equivalent** [74, 62, 7]. **Equivocal** [776]. **Erratum** [444]. **Error** [281]. **Errors** [196, 708, 742, 706, 715]. **Escape** [486]. **Escrow** [160]. **Especially** [476]. **Establishment** [596, 548]. **Estimate** [281]. **Estimations** [611]. **Evaluate** [610]. **Evaluation** [496, 564, 17]. **Even** [578, 509, 462]. **Even-Mansour** [578]. **Everlasting** [704, 576]. **Everywhere** [484]. **Evidence** [246]. **Evolution** [689]. **Exact** [206, 685]. **Exchange** [147, 106, 672, 110, 694, 274, 214, 288, 437, 268, 90, 8]. **Exhaustive** [192]. **Exist** [476]. **Existence** [132, 191]. **Existentially** [149]. **Expander** [727, 328]. **Expected** [345, 315]. **Experimental** [54]. **Experiments** [2]. **Explicit** [640]. **Exponent** [136, 612]. **Exponentially** [667]. **Exponentiation** [264, 225]. **Expressive** [651]. **Extended** [281, 610, 117, 402, 642]. **Extending** [579, 570]. **Extension** [267, 420, 739, 10]. **Extensions** [316, 537, 199]. **Extraction** [494]. **Extractors** [669, 236, 237].

F [380]. **F-FCSR-16** [380]. **F-FCSR-H** [380]. **Facets** [207]. **Factored** [233]. **Factoring** [495, 286, 419, 55, 7]. **factorization** [62]. **Factorizations** [91]. **Fail** [132]. **Fail-Stop** [132]. **Fair** [731, 370, 502, 737]. **Fairness** [545, 691, 386, 392]. **Fallacious** [162]. **Family** [438]. **Fast** [491, 722, 618, 179, 572, 580, 650, 141, 501, 681, 101, 14, 151, 159, 157, 32, 30, 79]. **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]. **Feedback** [130]. **Feistel** [492, 217]. **FHE** [735]. **Fiat** [766]. **Field** [199, 274, 78]. **Fields** [398, 252, 420, 619, 83, 151, 601, 90, 144, 161, 739, 263, 8]. **Filter** [672]. **Finding** [749]. **Fine** [769]. **Fine-Grained** [769]. **Finite** [199, 102, 398, 252, 326, 221, 263]. **first** [71]. **Fixed** [262, 383]. **FlipIt** [436]. **Fly** [280]. **Forgery** [636, 485]. **Forget** [607]. **Formal** [212, 301, 292, 658, 33]. **Formulae** [770]. **Forró** [725]. **Forward** [583, 294, 672]. **Forward-Secret** [672]. **Forward-Secure** [583, 294]. **Foundations** [656]. **Four** [640, 447]. **Four-Dimensional** [447]. **Four-State** [640]. **FPGA** [373, 378, 642]. **FPGA-friendly** [378]. **FPGA-Specific** [642]. **Fractional** [160]. **Framework** [308, 764, 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, 774, 125, 554, 369, 222, 30]. **Function-Private** [556]. **Functional** [625, 556, 562, 747, 736, 698, 703, 551, 626, 616, 89]. **Functionalities** [551, 652, 568]. **Functions** [456, 575, 749, 508, 549, 220, 460, 471, 164, 627, 336, 361, 755, 769, 328, 451, 416, 181, 299, 406, 667, 756, 647, 141, 221, 476, 375, 686, 469, 405, 103, 662, 100, 182, 743, 60, 27]. **Further** [100]. **Fuzzy** [669]. **FX** [635]. **FX-Constructions** [635].

Gabidulin [314]. **Gallant** [447]. **Game**

[514, 628, 436]. **Game-Based** [628]. **Garbled** [733]. **Garbling** [504, 572]. **Gates** [504, 779]. **GE** [376]. **General** [723, 767, 200, 112, 173, 138, 277, 339, 313]. **Generalization** [10]. **Generalizations** [778]. **Generalized** [41]. **Generates** [85]. **Generating** [233, 661]. **Generation** [4, 287, 275, 587, 359, 101, 307, 49, 99]. **Generator** [253, 179, 298, 15]. **Generators** [505, 379, 225, 224, 121, 191, 752, 222, 59, 38]. **Generic** [513, 452, 633, 588, 320, 760, 311, 700, 424, 649, 758]. **Genus** [491, 324, 531, 619, 157, 342]. **Geometric** [83]. **GGH** [330]. **Gimli** [680]. **Given** [258, 56]. **Giving** [51]. **Glitch** [373]. **Glitches** [375]. **GlobalPlatform** [768]. **GLP** [744]. **GNUC** [475]. **Go** [632, 519, 224]. **Goldreich** [242]. **Golić** [405]. **good** [29]. **GOST** [422]. **GPV** [666]. **Graded** [671]. **Grained** [769]. **Graph** [96, 727, 408]. **Graphs** [621, 498, 328]. **Grey** [607]. **Grey-Box** [607]. **Grindahl** [489]. **Group** [499, 588, 102, 656, 289, 2, 288, 730, 319, 350, 384, 85, 91]. **Groups** [310, 724, 408, 324, 280, 231, 326, 221]. **Grows** [667]. **GSM** [317, 461]. **Guaranteed** [545, 761]. **Guessing** [467]. **Guest** [372, 31, 113, 44].

H [380]. **Half** [779]. **Half-Gates** [779]. **Handling** [748, 315]. **Handshake** [688, 700, 351]. **Hard** [755, 289, 500, 200, 547, 692]. **Hard-Core** [200]. **Hard-to-Invert** [289, 500]. **Hardness** [589, 421, 708, 769, 663, 661]. **Hardness-Preserving** [589]. **Hardware** [375]. **Hash** [749, 508, 428, 633, 410, 460, 336, 361, 328, 451, 413, 369, 406, 558, 141, 469, 743, 30]. **Hash-CBC** [410]. **Hashing** [589, 442, 397, 750, 159, 98]. **having** [76]. **HB** [356]. **HElib** [664]. **Hellman** [10, 341, 184, 521, 304, 231, 245, 535, 157, 128]. **Help** [226]. **Hides** [219]. **Hiding** [621, 132, 335, 17]. **Hierarchical** [399, 655, 293]. **Hierarchy** [84]. **High** [560, 728, 227]. **High-Order** [560]. **High-Throughput** [728]. **Higher** [628]. **Higher-Order** [628]. **Highly** [336]. **Highly-Efficient** [336]. **Hints** [51]. **HMAC** [488]. **Homomorphic** [772, 734, 574, 550, 618, 634, 487, 362, 682, 717, 532]. **Homomorphic-Ciphertext** [574]. **Homomorphisms** [384]. **Honest** [732, 653, 722, 728, 737]. **Honest-Majority** [722]. **Human** [275]. **Hunting** [542]. **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]. **Identification** [506, 325, 620, 50, 169, 55, 61]. **Identity** [367, 456, 325, 311, 387, 751, 655, 6]. **Identity-Based** [367, 456, 325, 311, 387, 751, 655]. **IEC** [306]. **if** [678]. **IITM** [651]. **Im** [579]. **Im-** [579]. **imaginary** [8]. **impersonation** [81]. **Implementation** [248, 160, 102, 373, 375, 32, 21, 80]. **Implementations** [50, 52]. **Implements** [724]. **Importance** [196, 71]. **Impossibility** [586, 336, 270, 382, 383, 312]. **Impossible** [261, 552]. **Improbability** [146]. **Improve** [337]. **Improved** [566, 582, 639, 762, 725, 348, 445, 474, 680, 253, 274, 459, 378, 715, 63]. **Improvement** [133]. **Improvements** [123]. **Improving** [206]. **Incremental** [553]. **Independent** [204]. **Index** [324, 457]. **Indifferentiability** [492]. **Indifferentiable** [774]. **Indistinguishability** [569, 407]. **Indistinguishable** [627]. **Infeasibility** [630]. **Inferring** [15]. **Infinite** [103, 73]. **Information** [541, 374, 466, 240, 295, 129, 193, 543, 104, 25, 17, 63]. **Information-Theoretic** [295, 104, 25].

Inhomogeneous [582]. **Injective** [686]. **Inner** [736, 423, 747]. **Inner-Product** [747]. **Input** [340, 421, 446, 562]. **Inputs** [358, 383]. **Ins** [174]. **Insecure** [203]. **Insecurity** [215]. **instance** [751]. **Instant** [317]. **Instantiability** [539]. **instruments** [24]. **Integer** [582]. **Integral** [540]. **Integration** [418]. **Integrity** [322, 86]. **Interaction** [226]. **Interactive** [702, 773, 189, 55, 442, 111, 627, 487, 694, 649, 477, 332, 668]. **Internal** [680]. **Interpolation** [333]. **Intersection** [493, 357, 564]. **Introduction** [31, 42, 113, 44]. **Invariant** [613]. **Invariants** [643]. **Inversion** [229, 89]. **Invert** [289, 500]. **iO** [734]. **iSCREAM** [613]. **ISO** [306, 507]. **ISO/IEC** [306]. **Isogenies** [342]. **Isogeny** [620]. **Isomorphisms** [289]. **Iterated** [509]. **Iteration** [297]. **Iterative** [762]. **IV** [279].

Jacobian [531]. **Jacobians** [342]. **Joint** [119, 652].

Kangaroos [188]. **KASUMI** [461]. **Keccak** [445]. **Kedlaya** [267]. **KeeLoq** [396]. **KEM/DEM** [308]. **KEMs** [311]. **kernels** [61]. **Key** [456, 575, 452, 629, 399, 490, 639, 534, 611, 160, 278, 625, 254, 102, 266, 446, 556, 562, 147, 596, 294, 286, 150, 672, 509, 461, 474, 105, 110, 287, 28, 275, 694, 587, 580, 650, 422, 274, 214, 269, 288, 437, 383, 192, 698, 703, 265, 551, 626, 652, 326, 205, 775, 277, 255, 268, 221, 35, 101, 573, 553, 307, 314, 180, 167, 577, 203, 90, 144, 535, 128, 758, 494, 177, 32, 8, 20, 81, 7]. **Key-Dependent** [452]. **key-distribution** [20]. **Key-Exchange** [90, 8]. **Key-minimal** [28]. **Key-Recovery** [573]. **Keys** [768, 93, 485, 99]. **Keystream** [224, 191]. **Klimov** [298]. **knapsack** [37]. **Knowledge** [770, 764, 45, 115, 226, 51, 147, 166, 426, 448, 114, 771, 273, 487, 70, 82, 116, 393, 138, 647, 701, 52, 730, 390, 435, 781, 477, 143, 414, 440, 668, 494, 21, 72, 6, 74]. **Known** [279, 215]. **Known-in-Advance-IV** [279]. **Known-IV** [279]. **Koblitz** [601]. **Körner** [740]. **Kummer** [619].

Ladder [377]. **Lambert** [447]. **Language** [124]. **Language-Dependent** [124]. **Languages** [166, 393]. **Large** [722, 135, 381, 616]. **Large-Scale** [722]. **Larger** [735, 516]. **Laser** [373]. **Latin** [725]. **Lattice** [566, 744, 409, 771, 148, 765, 780, 730, 571, 745, 743]. **Lattice-Based** [566, 744, 771, 730, 571, 743]. **Lattices** [631, 536]. **Layers** [748, 469]. **Leakage** [675, 687, 693, 696, 433, 599, 584, 500, 700, 503, 707, 776, 701, 606, 726]. **Leakage-Resilient** [433, 503, 707, 701]. **Leaking** [610]. **Learn** [726]. **Learning** [708, 670, 706, 547, 330, 726, 715]. **Least** [468]. **Ledger** [757]. **Lehmer** [750]. **Length** [254, 141]. **Less** [217, 376]. **Levenshtein** [41]. **Leveraging** [603]. **Levin** [242]. **Light** [756]. **Lightning** [665]. **Lightweight** [428]. **Like** [483, 459, 318, 43]. **Lilliput** [636]. **Limitations** [272]. **Limits** [694, 497]. **Lin** [638]. **Line** [109, 236, 410]. **Line/Off** [109]. **Linear** [575, 533, 712, 466, 675, 702, 538, 680, 581, 107, 544, 716, 710, 616, 16, 309, 15, 23]. **linear-complexity** [23]. **Linking** [129]. **Local** [505, 675, 652, 47]. **Locality** [340, 549, 697, 421]. **Locality-Preserving** [697]. **Locally** [533, 712, 123, 624, 237]. **Locking** [516]. **Log** [146, 634, 287, 139]. **Logarithm** [358, 184, 366, 457, 253, 420, 745, 165, 342, 21]. **Logarithmic** [714, 730]. **Logarithmic-Size** [730]. **Logarithms** [190, 188, 55]. **Logic** [628, 427]. **Long** [364]. **Long-Term** [364]. **Look** [285]. **Lookup** [763]. **Lossy** [506, 416]. **Low** [480, 687, 693, 696, 669, 136, 366, 654, 111, 201, 283, 256, 15]. **Low-Complexity** [687, 693]. **Low-Entropy** [669]. **low-order** [15]. **Lower** [749, 755, 338, 312, 76]. **LPN**

[617]. **LRW2** [646]. **Luby** [156]. **Luby-Rackoff** [156]. **Lucifer** [108]. **LWE** [694, 668].

MAC [183, 485]. **Machine** [781]. **MACs** [254]. **Magic** [600]. **mail** [36]. **Maintaining** [174]. **Majority** [732, 478, 653, 722, 728, 737]. **Making** [552, 610]. **Malicious** [731, 722, 630, 357, 403, 450, 472, 501, 704]. **Maliciously** [608]. **malleability** [532]. **Malleable** [371, 647, 520, 555, 659, 624, 660, 343, 766, 640, 756]. **Man** [214]. **Man-in-the-Middle** [214]. **Manipulation** [756]. **Mansour** [578, 509, 462]. **Manticore** [738]. **Many** [557, 554]. **Map** [594]. **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]. **Minimum** [779]. **Mining** [216]. **Minority** [45]. **missing** [15]. **MISTY1** [540]. **ML** [66]. **ML-sequences** [66]. **Mode** [208]. **Model** [504, 291, 235, 660, 766, 455, 597, 608, 733, 424, 303, 666, 651, 528, 332, 145, 237]. **Modeling** [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** [264, 562, 241, 713, 777, 451, 250, 260, 455, 751, 580, 650, 631, 585, 605, 737, 401, 753, 576]. **Multi-authority** [713]. **Multi-ciphertext** [751]. **Multi-collision** [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-scalar** [777]. **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]. **Multiplications** [777]. **Multiplicative** [363]. **multiplier** [79]. **Multisignatures** [429]. **Multivariate** [560, 759]. **Must** [727, 135]. **Mutual** [374]. **Mutually** [137]. **My** [724].

Natively [763]. **Nearly** [731, 242]. **Necessary** [98]. **Needed** [554]. **Negligible** [220]. **Neighbor** [313]. **Network** [603]. **Networks** [276, 779, 105, 748, 107, 313]. **Never** [665]. **NFS** [745]. **NIZK** [544, 721]. **NIZKs** [683, 631]. **NMAC** [488]. **No** [716]. **No-Signaling** [716]. **Noisy** [584]. **Non** [471, 627, 702, 189, 241, 520, 555, 659, 624, 408, 324, 660, 343, 371, 766, 487, 706, 694, 640, 756, 590, 647, 326, 649, 781, 477, 332, 532, 668, 441]. **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, 766, 640, 756]. **Non-uniform** [781]. **Nonces** [215]. **Noncommutative** [479]. **Noncommutative-Algebraic** [479]. **Noninteractive** [115, 138]. **Nonlinear** [667, 375, 103, 613, 182]. **Nonlinearity** [778, 92]. **nonuniform** [75]. **Normal** [263]. **NORX** [614]. **Note** [284, 220, 699, 67, 425, 435]. **Notions** [320, 773, 321, 269]. **NP** [116, 138, 526, 143, 414, 668]. **NTRU** [330]. **Number** [379, 738, 592, 667, 752, 298, 78, 38]. **Numbers** [4, 233, 101].

OAEP [238, 539, 218]. **Obfuscating** [671, 522, 388]. **Obfuscation** [641, 569, 705, 449, 599, 454, 349, 740]. **Obfustopia** [625, 698, 703, 626]. **Oblivious** [537, 697, 714, 160, 296, 230, 648, 517, 592, 603, 291, 117, 417, 397, 564, 654, 391, 390, 411, 570, 249]. **Obliviousness** [603]. **observed** [76]. **OCB** [689]. **OCB2** [657]. **Odd** [83, 161]. **Off-Line** [109]. **Offs** [323, 635]. **Okamoto** [146]. **On-Line** [109, 236, 410]. **On-Line/Off-Line** [109]. **One** [549, 569, 229, 769, 270, 297, 242, 523, 245, 40, 619, 439, 647, 221, 143, 165, 30]. **One-More-RSA-Inversion** [229]. **One-Sided** [242, 523]. **One-Time** [439]. **One-Way** [549, 569, 769, 270, 647, 221, 143, 40, 30]. **Only** [317, 275]. **onto** [373]. **Operation** [140, 163, 279]. **Operations** [403, 68]. **Optimal** [723, 534, 720, 634, 235, 558, 437]. **Optimally** [731, 502]. **Optimization** [735]. **Optimized** [154]. **Optimizing** [758]. **Oracle** [773, 766, 666, 17]. **Oracles** [534, 329, 310, 387, 259, 497, 429, 481]. **Order** [671, 744, 628, 560, 280, 619, 359, 180, 15]. **Orders** [190]. **Oscillator** [379, 752, 378]. **Oscillator-Based** [379, 752]. **Other** [355]. **Output** [545, 761]. **Overhead** [714, 480, 779, 733]. **Overlapping** [770].

Paillier [219, 213, 587]. **Pairing** [248, 247, 777, 352, 244, 337]. **Pairing-Based** [248, 777, 337]. **Pairing-Friendly** [352]. **Pairings** [611, 736, 683]. **Pairs** [94]. **Paradigm** [320, 348]. **Parallel** [673, 356, 228, 781, 414, 395, 155]. **Parallelepiped** [330]. **Parallelism** [603]. **Parameter** [735]. **Parameters** [101, 100]. **Partial** [770, 258, 392, 756, 265]. **Partially** [215]. **Party** [732, 741, 648, 241, 272, 250, 728, 260, 392, 282, 608, 587, 623, 585, 228, 331, 472, 568, 681, 685, 605, 737, 576, 411]. **Password** [289, 437, 268, 13]. **Password-Authenticated** [268]. **Password-Based** [289, 437]. **Passwords** [275, 307]. **Pattern** [357, 450]. **Patterns** [167]. **PCPs** [707, 716, 661]. **Perfect** [699, 778, 74, 173, 667, 477, 143, 21, 63, 57, 38]. **Perfectly** [518, 405]. **Periods** [66]. **permit** [22]. **Permutation** [115, 134, 131, 554, 107, 400, 143, 680]. **Permutations** [569, 115, 270, 432, 459, 209, 156, 211, 441, 40]. **permuted** [61]. **PGM** [64]. **PGV** [361]. **Photonic** [530]. **Physical** [591, 752]. **pipelined** [79]. **PIR** [240]. **Placing** [674]. **Plain** [733]. **Plaintext** [443, 539, 577]. **Plaintext-Aware** [443]. **plaintexts** [26]. **Player** [173]. **Point** [449]. **Pollard** [398]. **Polylog** [741]. **Polynomial** [136, 184, 286, 345, 564, 430, 315, 423, 485, 479, 263, 38]. **Polynomial-Based** [485]. **Polynomial-Time** [286, 345, 315, 479]. **polynomials** [66]. **Possibility** [382, 579]. **Possible** [552, 454, 740]. **Post** [700]. **Post-quantum** [700]. **Power**

[732, 529, 114, 623]. **Powering** [251]. **PPAD** [663]. **Practical** [396, 639, 51, 259, 574, 550, 507, 106, 445, 461, 636, 622, 305, 419, 365, 169, 613, 177, 561]. **Practical-Time** [461]. **Precision** [735, 580, 650]. **Predicate** [736, 242, 423]. **Predicates** [200]. **Preface** [257, 53, 171, 234, 243]. **Preimage** [508]. **Preparation** [391]. **Preprocessing** [240, 114, 631, 122]. **Prescribed** [211]. **Presence** [174, 403, 450, 168, 472, 375]. **Preserving** [513, 499, 604, 586, 697, 589, 673, 593, 216]. **Prevailing** [760]. **PRFs** [760, 564]. **Primality** [297, 281]. **Prime** [4, 252, 619, 359, 101, 227]. **Prime-Order** [619, 359]. **Primitive** [124, 378]. **Primitives** [586, 709, 270, 250, 305, 776, 145]. **PRINCE** [644, 483]. **PRINCE-Like** [483]. **Privacy** [230, 129, 84, 729, 216, 313]. **Privacy-Conscious** [729]. **Private** [541, 637, 466, 295, 276, 556, 562, 193, 391, 269, 551, 626, 302, 715, 516, 549, 240]. **Private-Key** [562, 269, 551, 626]. **Privately** [354]. **Probabilistic** [598, 673, 345, 269, 313, 23]. **Probabilistic-Termination** [673]. **Probability** [224, 18, 309]. **Probable** [227]. **Probably** [4]. **Probing** [584]. **Problem** [486, 582, 146, 341, 5, 635, 253, 74, 420, 477, 165, 342]. **Problems** [354, 229, 358, 615, 620, 304, 547, 479]. **Procedure** [274]. **processing** [35, 36]. **produced** [15]. **Product** [747, 736, 327, 22]. **Products** [423]. **profile** [23]. **Program** [599]. **Programmable** [406, 743]. **Projective** [397]. **Promised** [111]. **Proof** [518, 45, 278, 443, 74, 82, 116, 111, 138, 331, 255, 86]. **Proofs** [770, 292, 566, 628, 325, 488, 226, 627, 702, 773, 51, 189, 166, 517, 114, 610, 771, 178, 595, 487, 544, 558, 666, 315, 393, 390, 435, 668, 431, 72, 6]. **Properties** [316, 680, 82, 112, 60, 64, 58]. **Property** [451]. **Proposal** [725]. **Protect** [192]. **Protected** [164]. **Protecting** [776]. **Protocol** [518, 768, 534, 658, 634, 117, 245, 729, 331, 472, 319, 351, 90, 157, 17, 33, 87, 688]. **Protocols** [541, 353, 45, 478, 727, 176, 241, 598, 673, 761, 448, 620, 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** [575, 471, 131, 225, 121, 47, 476, 156]. **Pseudorandomness** [48]. **Public** [490, 102, 446, 294, 580, 650, 383, 652, 326, 277, 221, 101, 553, 314, 414, 180, 577, 203, 144, 535, 494, 32]. **Public-Coin** [414]. **Public-Key** [102, 446, 294, 580, 650, 383, 652, 277, 101, 553, 180, 577, 144, 494, 32]. **PUF** [378]. **PUFs** [630, 704, 530]. **Purely** [144]. **Purposes** [349].

Quadratic [281, 111, 190, 274, 601, 180, 90, 8]. **Quantum** [466, 278, 596, 323, 391, 666, 407, 606, 255, 516, 177, 665, 54, 700, 695]. **Quark** [428]. **Quarters** [731]. **Quasi** [544]. **Quasi-Adaptive** [544]. **Quaternion** [194]. **Queries** [554]. **Question** [197]. **QUIC** [748]. **Quietly** [486].

Rabin [178]. **Rackoff** [156]. **radix** [79]. **RAM** [697, 714, 517, 603, 608]. **Random** [456, 534, 379, 4, 123, 329, 164, 627, 310, 387, 259, 110, 766, 253, 554, 497, 233, 666, 429, 752, 222, 211, 307, 481, 441, 59, 38, 23]. **Randomization** [629]. **Randomize** [413]. **Randomize-Hash-then-Sign** [413]. **Randomized** [549, 551, 57]. **Randomizer** [235]. **Randomness** [175, 305, 47]. **Ranks** [355]. **Rate** [640, 63]. **Rather** [566].

Rational [370]. **RC4** [441]. **Re** [388]. **Re-Encryption** [388]. **Reactive** [524]. **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]. **Record** [748]. **Recovery** [639, 509, 265, 573, 438, 758]. **Rectangle** [758]. **Recursive** [469]. **Reduced** [639, 261, 465, 644, 445, 622, 453]. **Reduced-Round** [639]. **Reducing** [240, 335]. **Reduction** [148, 765, 780]. **Reductions** [583, 123, 589, 755, 304]. **Reflection** [483]. **Registers** [130]. **Related** [575, 93, 461]. **Related-Key** [575, 461]. **Relation** [316]. **Relations** [456, 320, 616]. **Relationships** [321]. **Relaxation** [772]. **Release** [106]. **Reliability** [313]. **Reloaded** [725]. **Remaindering** [168]. **remarks** [61]. **Remote** [391]. **Rényi** [566]. **Repetition** [395]. **Replayed** [279]. **Replayed-and-Known-IV** [279]. **Representations** [775]. **Reproducible** [546]. **Requirements** [391]. **Residue** [529]. **Residuosity** [111]. **Resilience** [723, 675, 720, 599, 519, 606]. **Resilient** [433, 503, 707, 701, 103]. **Resistance** [488, 701, 753]. **Resistant** [677, 107, 376]. **Resource** [386, 391]. **Restricted** [345]. **Results** [382, 2, 383, 312, 23]. **Retrievability** [517, 431]. **Retrieval** [466, 295, 193, 240]. **Reusable** [669]. **Revisited** [316, 637, 538, 719, 558, 590, 568, 710, 156, 440, 395, 527, 612]. **Revisiting** [723, 629]. **Rho** [398]. **Ride** [724]. **Right** [642]. **Rights** [394]. **Ring** [329, 510, 706, 694, 424, 730, 378, 715]. **rings** [66]. **RIPEMD** [125, 515]. **RIPEMD-128** [515]. **Rivest** [37, 195]. **RLWE** [717]. **RLWE-Based** [717]. **RMAC** [265]. **Robin** [761]. **Robust** [559, 295, 451, 748, 181, 299, 737]. **Root** [750]. **Rotational** [453, 710, 642]. **Round** [639, 578, 297, 673, 761, 644, 291, 445, 125, 474, 116, 622, 608, 654, 245, 393, 437, 585, 701, 228, 435, 605, 685, 737, 642]. **Round-Efficient** [585]. **Round-Optimal** [437]. **Round-Preserving** [673]. **Round-Reduced** [644, 445, 622]. **Round-Robin** [761]. **Rounds** [261, 468, 761, 609, 217]. **Routing** [458]. **RSA** [229, 495, 136, 286, 56, 127, 178, 238, 186, 181, 300, 299, 587, 539, 62, 350, 612, 99]. **RSA-Based** [186, 300]. **RSA-OAEP** [238]. **RSA-signatures** [56]. **RTT** [672]. **Rudich** [686]. **Runtime** [430].

SAFER [187, 152]. **Salsa** [725]. **Same** [665]. **Sample** [204]. **Sampling** [648, 761]. **SASAS** [360]. **Scalable** [645, 288]. **Scalar** [447, 777]. **Scale** [722]. **Schedule** [775]. **Scheme** [754, 744, 229, 147, 294, 670, 462, 149, 400, 255, 169, 55, 61, 20, 69]. **Schemes** [506, 399, 498, 325, 675, 96, 170, 394, 734, 46, 134, 132, 509, 404, 500, 343, 371, 418, 213, 620, 280, 304, 142, 158, 118, 120, 137, 682, 206, 759, 485, 481, 256, 122, 63, 77, 81, 65, 25]. **Schnorr** [595, 122]. **SCP02** [768]. **SCREAM** [613]. **SDH** [310]. **Search** [354, 496, 192, 155]. **Searchable** [316, 676]. **Searching** [302]. **Second** [508]. **Second-Preimage** [508]. **secrecy** [39, 28, 57, 9, 19]. **Secret** [370, 363, 498, 675, 625, 96, 147, 46, 762, 73, 286, 106, 672, 634, 404, 110, 142, 362, 707, 776, 120, 137, 682, 698, 703, 526, 464, 293, 333, 63, 77, 69, 65, 11]. **Secret-Key** [625, 698, 703]. **Secret-Sharing** [498, 526]. **Secrets** [674, 120]. **Secure** [17, 506, 583, 355, 514, 518, 399, 389, 45, 653, 296, 687, 693, 696, 394, 294, 373, 484, 555, 720, 545, 565, 718, 779, 630, 106, 348, 408, 105, 500, 117, 250, 119, 172, 416, 238, 418, 728, 287, 417, 260, 392, 50, 546, 282, 700, 450, 523, 564, 608, 623, 733, 419, 118, 214, 303, 262, 191, 638, 655, 649, 228, 277, 339, 390, 411, 472, 681, 378, 101, 249, 375, 616, 685, 690, 246, 197, 57, 22, 649]. **Securely** [388]. **Securing** [210]. **Security** [575, 452, 353, 292, 566, 490, 379, 229, 325, 488, 164, 278, 443, 446, 562, 176, 241, 368, 691, 658, 134, 610, 178, 595, 493, 413, 496, 225, 290, 357, 597, 609, 751, 548, 646, 602, 321, 558, 666, 269, 315, 356, 217, 285, 528, 331, 255, 206, 364, 222, 95, 185, 481, 527, 169, 232, 61, 13]. **Segment** [781]. **Selecting** [205]. **Selective** [387, 382]. **Self** [312]. **Semantically** [555]. **Semi** [549, 695]. **Semi-private** [549]. **Semi-quantum** [695]. **Sender** [5, 158]. **Separating** [231]. **sequence** [76]. **Sequences** [83, 47, 441, 15, 66, 23]. **Sequential** [429]. **Servers** [240]. **Service** [193]. **Service-Providers** [193]. **Session** [275, 307]. **Session-Key** [275, 307]. **Set** [415, 272, 493, 357, 403, 564]. **Set-Intersection** [564]. **Set-Up** [272]. **Sets** [426]. **Setting** [446, 556, 562, 587, 751, 590, 551]. **Setup** [690]. **SHA** [465, 622]. **SHA-0** [465]. **SHA-1** [465]. **SHA-3** [622]. **Shallue** [774]. **Shamir** [762, 766, 298]. **Shannon** [10]. **Share** [135, 11]. **shares** [77]. **Sharing** [370, 363, 498, 675, 96, 46, 762, 634, 404, 181, 299, 142, 707, 776, 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]. **Shpilrain** [319]. **Shrinkage** [533, 712]. **Shrinking** [604]. **Shuffle** [362, 563]. **Shuffled** [560]. **Side** [376, 530]. **Side-Channel** [376, 530]. **Sided** [242, 523]. **sieve** [78]. **Sign** [413]. **Signal** [658, 700]. **Signaling** [716]. **Signature** [583, 744, 229, 325, 394, 134, 670, 149, 500, 620, 280, 304, 652, 206, 215, 481, 49, 122]. **Signatures** [506, 513, 499, 604, 329, 467, 247, 310, 656, 510, 433, 412, 194, 507, 106, 132, 109, 595, 593, 273, 413, 186, 300, 730, 429, 571, 384, 330, 185, 401, 527, 535, 56]. **Signcryption** [292]. **Significance** [91, 27]. **Signing** [394, 681]. **SIMD** [767]. **Simple** [513, 400, 651]. **Simpler** [659, 277, 307, 715]. **Simplicity** [121]. **Simulation** [449, 493, 496, 173, 321, 315, 590, 477]. **Simulation-Based** [493, 496, 321, 315]. **Simultaneous** [541, 637]. **Single** [474, 131, 422]. **Single-Key** [474, 422]. **Six** [217]. **Size** [513, 611, 135, 593, 730, 77]. **Sizes** [205]. **Skein** [453]. **Skipjack** [261]. **SLAP** [715]. **Slender** [415]. **Slender-Set** [415]. **Slide** [567]. **Slidex** [462]. **Sliding** [251]. **Small** [505, 632, 136, 252, 420, 151, 161, 612]. **Small-Bias** [505]. **Smart** [49]. **Smooth** [397]. **SNARGs** [721]. **SNARK** [542]. **SNARKs** [677]. **Software** [154, 30]. **Software-Optimized** [154]. **Solution** [582, 574]. **Solutions** [136, 479]. **Solve** [354]. **Solving** [617]. **Some** [63, 61, 3]. **Sound** [395]. **Soundness** [212, 301, 773, 86]. **Sources** [183]. **Space** [749]. **Spaces** [204]. **Span** [130]. **SPDZ** [605, 690]. **Specific** [642]. **Specified** [355]. **Speeding** [777]. **Spin** [642]. **Split** [520, 660]. **Split-State** [520, 660]. **splitting** [39]. **Sponge** [602]. **Sponge-Based** [602]. **Spreading** [486]. **spreads** [16]. **Square** [750]. **SRAM** [373]. **SRAM-Based** [373]. **stamp** [34]. **Standard** [504, 760, 467, 572, 663, 2]. **State** [520, 660, 700, 391, 640, 652, 438, 665]. **Stateless** [592]. **States** [407]. **Statistical** [566, 226, 647, 59]. **Statistically** [720, 132, 335]. **Statistically-Hiding** [335]. **Stealthy** [436]. **Steganography** [338]. **Stegosystem** [439]. **Stochastic** [591]. **Stop** [132, 224]. **Stop/Go** [224]. **Storage** [291, 105, 235, 236, 332, 237]. **Storage-Bounded** [236]. **Strategies** [443, 315]. **Stream** [574, 380, 441, 438, 715, 182, 41, 14, 58]. **Streaming** [302]. **Strengthening** [273]. **Stretch** [164]. **Strikes** [670, 665]. **String**

[323, 455]. **Strong** [449, 769, 236, 686, 33]. **Stronger** [329, 562, 659, 178]. **Strongly** [65]. **Structural** [360, 644, 314, 139]. **Structure** [513, 499, 604, 586, 709, 84, 593, 717, 211]. **Structure-Preserving** [513, 499, 604, 586, 593]. **Structured** [29]. **Structures** [173]. **Study** [374, 13]. **Subexponential** [146]. **Subgroup** [486]. **Subliminal** [166]. **Subliminal-Free** [166]. **Sublinear** [718]. **Subset** [118]. **Subspace** [470]. **Subspaces** [544]. **Substitution** [107]. **Substitution-Permutation** [107]. **Subtleties** [463]. **Subversion** [677]. **Subversion-Resistant** [677]. **Success** [309]. **Succinct** [764, 702]. **Sufficient** [98]. **Suggestion** [345]. **Suite** [729]. **Sum** [118]. **Summation** [179]. **Sums** [164]. **Super** [763]. **Super-Efficient** [763]. **Supersingular** [620, 246]. **Supporting** [738, 423]. **SwiftEC** [774]. **Symbolic** [368]. **Symbols** [529]. **Symmetric** [676, 760, 418, 568, 85]. **Symmetries** [457, 680]. **Symmetry** [536, 642]. **Synthetic** [661]. **System** [74, 111, 138, 271, 8, 7]. **Systems** [45, 82, 116, 50, 128, 87].

T [735]. **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]. **Termination** [598, 673]. **TERO** [591]. **TERO-Based** [591]. **Test** [281, 227, 59]. **Tests** [242, 75]. **Text** [496]. **TF** [298]. **TF-1** [298]. **TFHE** [618]. **th** [529]. **Their** [289, 624, 345, 406, 204, 91, 99, 80]. **Them** [763]. **Theorem** [442, 631, 425]. **Theorems** [327, 652]. **Theoretic** [514, 295, 104, 25]. **Theoretical** [543, 298]. **Theory** [232]. **Thompson** [319]. **Thorp** [563]. **Three** [731, 732, 254, 324, 728, 87, 685]. **Three-Key** [254]. **Three-Party** [732, 728]. **Three-Quarters** [731]. **Threshold** [587, 649, 268, 717, 210, 293]. **Thresholdizer** [762]. **Throughput** [728]. **Tight** [676, 595, 304, 751, 646, 481]. **Tighter** [666]. **Tightly** [506, 655]. **Tightness** [583]. **Tillich** [369]. **Time** [749, 399, 286, 635, 461, 345, 380, 315, 439, 180, 183, 479, 34]. **Time-Bound** [399]. **Time-Space** [749]. **time-stamp** [34]. **Timestamping** [332]. **Timing** [303]. **TLS** [688, 548, 351]. **Tokens** [592]. **Tolerance** [175]. **Tolerant** [606]. **Tolerating** [45]. **Toolbox** [148]. **Topical** [711]. **Topology** [621]. **Topology-Hiding** [621]. **Torus** [618]. **Toss** [478, 579, 502]. **Tossing** [731, 228]. **Tower** [745]. **Trace** [165]. **Tracing** [202, 256]. **Trade** [635, 323]. **Trade-Offs** [323, 635]. **Tradeoff** [434, 444]. **Tradeoffs** [676]. **Trading** [226]. **Traffic** [480]. **Traitor** [202, 256]. **Transaction** [757]. **Transfer** [537, 160, 296, 592, 291, 117, 417, 397, 654, 390, 411, 570, 249]. **Transfers** [230]. **Translucent** [160]. **Trapdoor** [115, 219, 289, 416, 432, 686, 271]. **Trapdoors** [730, 221]. **Treatment** [757, 70]. **tree** [402]. **Trees** [409]. **Tripartite** [245]. **Triple** [163, 150]. **Triplets** [94]. **TRNG** [591]. **Truncated** [554]. **Trusted** [137]. **Tweakable** [385]. **Twice** [665]. **Twin** [341]. **Two** [212, 301, 648, 272, 778, 578, 150, 125, 392, 397, 282, 608, 587, 623, 228, 331, 472, 568, 681, 151, 33, 411]. **Two-Key** [150]. **Two-Message** [397]. **Two-Party** [648, 272, 392, 282, 608, 587, 623, 228, 331, 472, 568, 681]. **Two-Round** [578, 125]. **two-way** [33]. **Type** [327]. **Types** [93].

UC [704]. **Unbounded** [736, 158]. **Unconditional** [5, 255, 28]. **Unconditionally** [296, 687, 510, 417, 22, 693, 696]. **Undeniable** [186, 300, 384]. **Unforgeable** [149]. **Unified** [482, 758]. **Uniform** [70, 781]. **Uniform-Complexity** [70]. **Unifying** [584]. **Universal**

[645, 762, 193, 475, 383, 651, 339, 364, 75, 59]. **Universally** [272, 368, 592, 597]. **Universe** [674]. **Unknown** [280]. **Unlinkability** [480]. **Unreliable** [748]. **Untraceability** [5]. **UOWHF** [533, 712]. **Updatable** [747, 624]. **Updates** [756]. **Updating** [611]. **Upper** [338]. **Use** [334]. **Used** [461]. **Usefulness** [497]. **User** [81]. **Ushakov** [319]. **Using** [566, 93, 261, 51, 259, 592, 457, 110, 273, 487, 275, 617, 262, 221, 48, 143, 313, 337, 726, 90, 144]. **Utility** [370].

v2.0 [614]. **Validation** [760]. **Validity** [524]. **Vanstone** [146, 447]. **Variant** [400]. **Varieties** [337]. **vectors** [35]. **Verifiable** [456, 627, 362, 464, 662]. **Verifiably** [429]. **Verification** [412, 524]. **Verifier** [683, 401]. **Version** [610, 642]. **Versus** [545, 276, 175, 241]. **Very** [498, 227]. **Via** [671, 517, 549, 160, 589, 702, 297, 740, 626, 411, 686]. **View** [514, 282]. **Views** [212, 301]. **Virtual** [781]. **Visual** [170]. **Voting** [771]. **Vulnerabilities** [136]. **Vulnerability** [83].

Want [724]. **Way** [549, 569, 769, 270, 647, 221, 143, 33, 40, 30]. **Weak** [85, 222, 485, 516]. **Weaker** [562]. **Weakness** [194]. **Weil** [247, 207, 244]. **Which** [56, 393]. **Whirlpool** [470]. **White** [607]. **White-Box** [607]. **Wildcarded** [367]. **Window** [251]. **Wiretap** [740]. **Wise** [520, 204]. **Within** [609]. **Without** [732, 768, 389, 310, 387, 272, 565, 683, 730, 429, 481, 653, 488, 329, 260]. **Witness** [627]. **Witness-Indistinguishable** [627]. **Woestijne** [774]. **World** [596]. **Worlds** [653]. **Worst** [714, 281]. **Worst-Case** [714, 281]. **Wright** [197]. **Wrong** [629]. **Wrong-Key-Randomization** [629].

X [438]. **X-FCSR** [438]. **X.509** [33]. **X3DH** [700]. **X9.52** [208]. **XOR** [504]. **XTR** [246].

Yao [331].

Zémor [369]. **Zero** [541, 764, 45, 115, 226, 51, 147, 166, 426, 448, 114, 771, 6, 273, 487, 74, 70, 82, 116, 393, 138, 647, 701, 52, 730, 390, 435, 781, 477, 143, 414, 440, 668, 21, 72]. **Zero-Knowledge** [764, 45, 115, 226, 51, 147, 166, 426, 448, 114, 771, 273, 487, 70, 82, 116, 393, 138, 647, 701, 52, 730, 390, 435, 781, 477, 143, 668, 6, 74, 21, 72]. **ZK** [767, 707]. **ZK-PCPs** [707]. **zkSNARKs** [777].

References

Brickell:1988:E

[1] E. F. Brickell. Editorial. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):1–2, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kaliski:1988:DES

[2] Burton S. Kaliski, Jr., Ronald L. Rivest, and Alan T. Sherman. Is the Data Encryption Standard a group? (results of cycling experiments on DES). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):3–36, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Stinson:1988:SCB

[3] D. R. Stinson. Some constructions and bounds for authentication codes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):37–52 (or 37–51??), ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Beauchemin:1988:GRN

[4] Pierre Beauchemin, Gilles Brassard, Claude Crépeau, Claude Goutier, and Carl Pomerance. The generation of random numbers that are probably prime. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):53–64, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Chaum:1988:DCP

[5] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(1):65–75, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/1021.html`.

Feige:1988:ZKP

[6] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):77–94, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

McCurley:1988:KDS

[7] Kevin S. McCurley. A key distribution system equivalent to factoring. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):95–105, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Buchmann:1988:KES

[8] Johannes Buchmann and H. C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):107–118, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Stinson:1988:CAS

[9] D. R. Stinson. A construction for authentication/secrecy codes from certain combinatorial designs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):119–127, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Beauchemin:1988:GHE

[10] Pierre Beauchemin and Gilles Brassard. Generalization of Hellman's extension to Shannon's approach to cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):129–131, October 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Tompa:1988:HSS

[11] Martin Tompa and Heather Woll. How to share a secret with cheaters. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(2):133–138, ???? 1988. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Koblitz:1989:HC

[12] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology: the*

journal of the International Association for Cryptologic Research, 1(3):139–150, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Luby:1989:SPS

[13] Michael Luby and Charles Rackoff. A study of password security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3):151–158, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Meier:1989:FCA

[14] Willi Meier and Othmar Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3): 159–176, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1989:ISP

[15] Joan Boyar. Inferring sequences produced by a linear congruential generator missing low-order bits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3):177–184, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Piper:1989:LCS

[16] Fred Piper and Michael Walker. Linear ciphers and spreads. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 1(3): 185–188, ???? 1989. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Abadi:1990:SCE

[17] Martin Abadi and Joan Feigenbaum. Secure circuit evaluation. A protocol based on hiding information from an oracle. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(1):1–12, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Nishimura:1990:PMM

[18] Kazuo Nishimura and Masaaki Sibuya. Probability to meet in the middle. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(1):13–22, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Stinson:1990:CAS

[19] D. R. Stinson. The combinatorics of authentication and secrecy codes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(1):23–49, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Gong:1990:MKD

[20] Li Gong and David J. Wheeler. A matrix key-distribution scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(1):51–59, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1990:DLI

[21] Joan F. Boyar, Stuart A. Kurtz, and Mark W. Krentel. Discrete logarithm implementation of perfect zero-knowledge blobs. *Journal of Cryptol-*

ogy: the journal of the International Association for Cryptologic Research, 2(2): 63–76, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Simmons:1990:CPC

[22] Gustavus J. Simmons. Cartesian product construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(2):77–104, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Niederreiter:1990:CAP

[23] Harald Niederreiter. Combinatorial approach to probabilistic results on the linear-complexity profile of random sequences. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(2):105–112, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Forre:1990:MID

[24] Réjane Forré. Methods and instruments for designing S-boxes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(3):115–130, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Walker:1990:ITB

[25] Michael Walker. Information-theoretic bounds for authentication schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(3):131–143, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Murphy:1990:CFC

[26] Sean Murphy. The cryptanalysis of FEAL-4 with 20 chosen plaintexts. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(3):145–154, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Mitchell:1990:EBF

[27] Chris Mitchell. Enumerating Boolean functions of cryptographic significance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 2(3):155–170, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Godlewski:1990:KMC

[28] Philippe Godlewski and Chris Mitchell. Key-minimal cryptosystems for unconditional secrecy. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(1): 1–25, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Adams:1990:SDC

[29] Carlisle Adams and Stafford Tavares. Structured design of cryptographically good S-boxes. *Journal of Cryptology: 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

[30] Ralph C. Merkle. A fast software one-way hash function. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(1): 43–58, ???? 1990. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Berson:1991:GEI

[31] T. A. Berson and R. A. Rueppel. Guest Editor's introduction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(2):61–62, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Agnew:1991:IFP

[32] G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone. An implementation for a fast public-key cryptosystem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(2): 63–79, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Gaarder:1991:AFA

[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 Research*, 3(2):81–98, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Haber:1991:HTD

[34] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(2):99–111, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Matyas:1991:KPC

[35] Stephen M. Matyas. Key processing with control vectors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(2): 113–136, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Pastor:1991:CCA

[36] Jose Pastor. CRYPTOPOST. A cryptographic application to mail processing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(2):137–146, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lenstra:1991:CRK

[37] H. W. Lenstra, Jr. On the Chor–Rivest knapsack cryptosystem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3):149–155, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Micali:1991:EPP

[38] S. Micali and C. P. Schnorr. Efficient, perfect polynomial random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3): 157–172, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

DeSoete:1991:NBC

[39] Marijke De Soete. New bounds and constructions for authentication/secrecy codes with splitting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3): 173–186, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kaliski:1991:OWP

[40] Burton S. Kaliski, Jr. One-way permutations on elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3):187–199, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Golic:1991:GCA

[41] Jovan Dj. Golić and Miodrag J. Mihaljević. Generalized correlation attack on a class of stream ciphers based on the Levenshtein distance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 3(3):201–212, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brickell:1991:EI

[42] E. F. Brickell. Editorial introduction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(1):1–2, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Biham:1991:DCL

[43] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(1):3–72, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Feigenbaum:1991:GEI

[44] J. Feigenbaum. Guest Editor's introduction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2):73, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Beaver:1991:SMP

[45] D. Beaver. Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty minority. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2):75–122, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brickell:1991:CIS

[46] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2): 123–134, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1991:LRP

[47] U. M. Maurer and J. L. Massey. Local randomness in pseudorandom sequences. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2):135–149, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Naor:1991:BCU

[48] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(2): 151–158, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Schnorr:1991:ESG

[49] C.-P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(3):161–174, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Goutier:1991:SII

[50] C. Goutier S. Bengio, G. Brassard, Y. G. Desmedt and J.-J. Quisquater. Secure implementations of identification systems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(3):175–183, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1991:PZK

[51] Joan Boyar, Katalin Friedl, and Carsten Lund. Practical zero-knowledge proofs: Giving hints and using deficiencies. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(3):185–206, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Koblitz:1991:ECI

[52] Neal Koblitz. Elliptic curve implementations of zero-knowledge blobs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 4(3):207–213, ???? 1991. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Damgaard:1992:P

[53] I. B. Damgård. Preface. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1):1, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Bennett:1992:EQC

[54] Charles Bennett, H., François Bessette, Gilles Brassard, and Louis Salvail. Experimental quantum cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1):3–28, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brickell:1992:IIS

[55] Ernest F. Brickell and Kevin S. McCurley. Interactive identification scheme based on discrete logarithms and factoring. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1):29–39, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Evertse:1992:WNR

[56] Jan-Hendrik Evertse and Eugène van Heyst. Which new RSA-signatures can be computed from certain given RSA-signatures? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1): 41–52, ???? 1992. CODEN JOCREQ.

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

Maurer:1992:CPS

[57] Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1): 53–66, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Meier:1992:CPC

[58] Willi Meier and Othmar Staffelbach. Correlation properties of combiners with memory in stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(1):67–86, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1992:UST

[59] Ueli M. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):89–105, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lloyd:1992:CBF

[60] Sheelagh Lloyd. Counting binary functions with certain cryptographic properties. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):107–131, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Georgiades:1992:SRS

[61] Jean Georgiades. Some remarks on the security of the identification scheme based on permuted kernels. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):133–137, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Loxton:1992:CRC

[62] J. H. Loxton, David S. P. Khoo, Gregory J. Bird, and Jennifer Seberry. A cubic RSA code equivalent to factorization. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(2):139–150, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brickell:1992:SIB

[63] E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(3):153–166, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Magliveras:1992:APC

[64] Spyros S. Magliveras and Nasir D. Memon. Algebraic properties of cryptosystem PGM. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(3):167–183, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Phillips:1992:SIS

[65] Steven J. Phillips and Nicholas C. Phillips. Strongly ideal secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(3): 185–191, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Dai:1992:BSD

[66] Zong Duo Dai. Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 5(3):193–207, ???? 1992. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brassard:1993:EN

[67] G. Brassard. Editor's note. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(1):1, Winter 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Agnew:1993:AO

[68] G. B. Agnew, T. Beth, R. C. Mullin, and S. A. Vanstone. Arithmetic operations in GF(2^m). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(1): 3–13, Winter 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Ito:1993:MAS

[69] Mitsuru Ito, Akira Saito, and Takao Nishizeki. Multiple assignment scheme for sharing secret. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(1): 15–20, Winter 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Goldreich:1993:UCT

[70] Oded Goldreich. Uniform-complexity treatment of encryption and zero-knowledge. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(1):21–53, Winter 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1993:CCI

[71] Ueli M. Maurer and James L. Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(1):55–61, Winter 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Boyar:1993:CCZ

[72] Joan Boyar, Carsten Lund, and René Peralta. On the communication complexity of zero-knowledge proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(2):65–85, Spring 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Chor:1993:SSI

[73] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains. *Journal of Cryptology: the journal of the International Association for Cryptologic*

Research, 6(2):87–95, Spring 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Goldreich:1993:PZK

[74] Oded Goldreich and Eyal Kushilevitz. A perfect zero-knowledge proof system for a problem equivalent to the discrete algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(2):97–116, Spring 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Schrift:1993:UTN

[75] A. W. Schrift and A. Shamir. Universal tests for nonuniform distributions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(3):119–133, Summer 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Rosenbaum:1993:LBA

[76] Ute Rosenbaum. Lower bound on authentication after having observed a sequence of messages. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6 (3):135–156, Summer 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Capocelli:1993:SSS

[77] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(3):157–167, Summer 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Coppersmith:1993:MNF

[78] Don Coppersmith. Modifications to the number field sieve. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6 (3):169–180, Summer 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Orton:1993:DFP

[79] Glenn Orton, Lloyd Peppard, and Stafford Tavares. Design of a fast pipelined modular multiplier based on a diminished-radix algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(4):183–208, Fall 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Menezes:1993:ECC

[80] Alfred J. Menezes and Scott A. Vanstone. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(4):209–224, Fall 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lenstra:1993:UIK

[81] Arjen K. Lenstra and Yacov Yacobi. User impersonation in key certification schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 6(4):225–232, Fall 1993. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Goldreich:1994:DPZ

[82] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge

proof systems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(1):1–32, Winter 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Klapper:1994:VGS

[83] Andrew Klapper. The vulnerability of geometric sequences based on fields of odd characteristic. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(1): 33–51, Winter 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Chor:1994:SPH

[84] Benny Chor, Mihaly Gereb-Graus, and Eyal Kushilevitz. On the structure of the privacy hierarchy. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(1): 53–60, Winter 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Murphy:1994:WCG

[85] Sean Murphy, Kenneth Paterson, and Peter Wild. A weak cipher that generates the symmetric group. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(1):61–65, Winter 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Simmons:1994:PSI

[86] G. J. Simmons. Proof of soundness (integrity) of cryptographic protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(2):69–77, Spring 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kemmerer:1994:TSC

[87] R. Kemmerer, C. Meadows, and J. Millen. Three systems for cryptographic protocol analysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(2):79–130, Spring 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

OConnor:1994:ACA

[88] Luke O'Connor. An analysis of a class of algorithms for S-box construction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(3):133–151, Summer 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Teng:1994:FIC

[89] Shang-Hua Teng. Functional inversion and communication complexity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(3):153–170, Summer 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Scheidler:1994:KEP

[90] Renate Scheidler, Johannes A. Buchmann, and Hugh C. Williams. A key-exchange protocol using real quadratic fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(3):171–199, Summer 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Qu:1994:FEA

[91] Ming Hua Qu and S. A. Vanstone. Factorizations in the elementary Abelian p-group and their cryptographic significance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(4):201–212, Fall 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

OConnor:1994:ANA

[92] Luke O'Connor and Andrew Klapper. Algebraic nonlinearity and its applications to cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(4):213–227, Fall 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Biham:1994:NTC

[93] E. Biham. New types of cryptanalytic attacks using related keys. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 7(4):229–??, Fall 1994. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Davies:1995:PTS

[94] D. Davies and S. Murphy. Pairs and triplets of DES S-boxes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(1):1–??, Winter 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Nyberg:1995:PSA

[95] Kaisa Nyberg and Lars Ramkilde Knudsen. Provable security against a differential attack. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(1):27–37, Winter 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Blundo:1995:GDS

[96] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(1):39–64, Winter 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

OConnor:1995:DCB

[97] L. O'Connor. On the distribution of characteristics in bijective mappings. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(2):67–??, Spring 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Russell:1995:NSC

[98] Alexander Russell. Necessary and sufficient conditions for collision-free hashing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(2):87–99, Spring 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Vanstone:1995:SRK

[99] S. A. Vanstone and R. J. Zuccherato. Short RSA keys and their generation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(2):101–??, Spring 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Yang:1995:FEB

[100] Yi Xian Yang and Bao An Guo. Further enumerating Boolean functions of cryptographic parameters. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8 (3):115–122, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Maurer:1995:FGP

[101] Ueli M. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(3):123–155, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Blackburn:1995:CPK

[102] Simon Blackburn, Sean Murphy, and Jacques Stern. The cryptanalysis of a public-key implementation of finite group mappings. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(3):157–166, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Stinson:1995:ICC

[103] D. R. Stinson and J. L. Massey. An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(3):167–173, Summer 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Pei:1995:ITB

[104] Ding Yi Pei. Information-theoretic bounds for authentication codes and block designs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(4): 177–188, Fall 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Dyer:1995:KSS

[105] Martin Dyer, Trevor Fenner, Alan Frieze, and Andrew Thomason. On key storage in secure networks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(4):189–??, Fall 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Damgaard:1995:PPS

[106] I. B. Damgård. Practical and provably secure release of a secret and exchange of signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 8(4): 201–??, Fall 1995. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Heys:1996:SPN

[107] Howard M. Heys and Stafford E. Tavares. Substitution-permutation networks resistant to differential and linear cryptanalysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(1): 1–19, Winter 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/bibs/9n1p1.html; http://link.`

springer.de/link/service/journals/00145/bibs/9n1p1.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n1p1.tex; http://link.springer.de/link/service/journals/00145/tocs/00901.html.

Ben-Aroya:1996:DCL

[108] Ishai Ben-Aroya and Eli Biham. Differential cryptanalysis of Lucifer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(1):21–34, Winter 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n1p21.html; http://link.springer.de/link/service/journals/00145/bibs/9n1p21.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n1p21.tex; http://link.springer.de/link/service/journals/00145/tocs/00901.html.

Even:1996:LLD

[109] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(1):35–67, Winter 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n1p35.html; http://link.springer.de/link/service/journals/00145/bibs/9n1p35.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n1p35.tex; http://link.springer.de/link/service/journals/00145/tocs/00901.html.

Fischer:1996:BSK

[110] Michael J. Fischer and Rebecca N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(2):71–99, Spring 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n2p71.html; http://link.springer.de/link/service/journals/00145/bibs/9n2p71.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n2p71.tex; http://link.springer.de/link/service/journals/00145/tocs/00902.html.

Itoh:1996:LCC

[111] Toshiya Itoh, Masafumi Hoshi, and Shigeo Tsujii. A low communication competitive interactive proof system for promised quadratic residuosity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(2):101–109, Spring 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n2p101.html; http://link.springer.de/link/service/journals/00145/bibs/9n2p101.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n2p101.tex; http://link.springer.de/link/service/journals/00145/tocs/00902.html.

Golic:1996:CPG

[112] Jovan Dj. Golic. Correlation properties of a general binary combiner with memory. *Journal of Cryptology: the*

journal of the International Association for Cryptologic Research, 9(2):111–126, Spring 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n2p111.html; http://link.springer.de/link/service/journals/00145/bibs/9n2p111.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n2p111.tex; http://link.springer.de/link/service/journals/00145/tocs/00902.html.

Crepeau:1996:GEI

[113] Claude Crépeau. Guest Editor's introduction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(3): 127–128, Summer 1996. URL http://link.springer.de/link/service/journals/00145/bibs/9n3p127.html; http://link.springer.de/link/service/journals/00145/bibs/9n3p127.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n3p127.tex; http://link.springer.de/link/service/journals/00145/tocs/00902.html.

DeSantis:1996:PPZ

[114] Alfredo De Santis and Giuseppe Persiano. The power of preprocessing in zero-knowledge proofs of knowledge. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(3):129–148, Summer 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n3p129.html; http://link.springer.de/link/service/journals/00145/bibs/9n3p129.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n3p129.tex; http://link.springer.de/link/service/journals/00145/tocs/00903.html.

Bellare:1996:CPN

[115] Mihir Bellare and Moti Yung. Certifying permutations: Noninteractive zero-knowledge based on any trapdoor permutation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(3):149–166, Summer 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n3p149.html; http://link.springer.de/link/service/journals/00145/bibs/9n3p149.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n3p149.tex; http://link.springer.de/link/service/journals/00145/tocs/00903.html.

Goldreich:1996:HCC

[116] Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(3):167–189, Summer 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n3p167.html; http://link.springer.de/link/service/journals/00145/bibs/9n3p167.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n3p167.tex; http://link.springer.de/link/service/journals/00145/tocs/00903.html.

Fischer:1996:SPO

[117] M. J. Fischer, S. Micali, and C. Rackoff. A secure protocol for the oblivious transfer (extended abstract). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(3):191–195, Summer 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n3p191.html; http://link.springer.de/link/service/journals/00145/bibs/9n3p191.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n3p191.tex; http://link.springer.de/link/service/journals/00145/tocs/00903.html.

Impagliazzo:1996:ECS

[118] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(4):199–216, Fall 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n4p199.html; http://link.springer.de/link/service/journals/00145/bibs/9n4p199.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n4p199.tex; http://link.springer.de/link/service/journals/00145/tocs/00904.html.

Franklin:1996:JEM

[119] Matthew Franklin and Stuart Haber. Joint encryption and message-efficient secure computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(4):217–232, Fall 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n4p217.html; http://link.springer.de/link/service/journals/00145/bibs/9n4p217.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n4p217.tex; http://link.springer.de/link/service/journals/00145/tocs/00904.html.

Jackson:1996:ISS

[120] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. Ideal secret sharing schemes with multiple secrets. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(4):233–250, Fall 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n4p233.html; http://link.springer.de/link/service/journals/00145/bibs/9n4p233.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n4p233.tex; http://link.springer.de/link/service/journals/00145/tocs/00904.html.

Han:1996:PGF

[121] Yenjo Han and Lane A. Hemaspaandra. Pseudorandom generators and the frequency of simplicity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 9(4):251–261, Fall 1996. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/9n4p251.html; http://link.

springer.de/link/service/journals/00145/bibs/9n4p251.pdf; http://link.springer.de/link/service/journals/00145/bibs/9n4p251.tex; http://link.springer.de/link/service/journals/00145/tocs/00904.html.

deRooij:1997:SPD

[122] Peter de Rooij. On Schnorr's preprocessing for digital signature schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(1):1–16, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n1p1.html; http://link.springer.de/link/service/journals/00145/bibs/10n1p1.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n1p1.tex; http://link.springer.de/link/service/journals/00145/tocs/01001.html.

Beaver:1997:LRR

[123] D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway. Locally random reductions: Improvements and applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(1):17–36, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n1p17.html; http://link.springer.de/link/service/journals/00145/bibs/10n1p17.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n1p17.tex; http://link.springer.de/link/service/journals/00145/tocs/01001.html.

Itoh:1997:LDC

[124] Toshiya Itoh, Yuji Ohta, and Hiroki Shizuya. A language-dependent cryptographic primitive. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(1):37–49, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n1p37.html; http://link.springer.de/link/service/journals/00145/bibs/10n1p37.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n1p37.tex; http://link.springer.de/link/service/journals/00145/tocs/01001.html.

Dobbertin:1997:RTC

[125] H. Dobbertin. RIPEMD with two-round compress function is not collision-free. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(1):51–69, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n1p51.html; http://link.springer.de/link/service/journals/00145/bibs/10n1p51.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n1p51.tex; http://link.springer.de/link/service/journals/00145/tocs/01001.html.

Kaliski:1997:CMA

[126] B. S. Kaliski. A chosen message attack on Demytko's elliptic curve cryptosystem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(1):71–

72, Winter 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n1p71.html; http://link.springer.de/link/service/journals/00145/bibs/10n1p71.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n1p71.tex; http://link.springer.de/link/service/journals/00145/tocs/01001.html.

Fiat:1997:BR

[127] A. Fiat. Batch RSA. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(2):75–88, Spring 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n2p75.html; http://link.springer.de/link/service/journals/00145/bibs/10n2p75.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n2p75.tex; http://link.springer.de/link/service/journals/00145/tocs/01002.html.

Yacobi:1997:BDK

[128] Y. Yacobi and M. J. Beller. Batch Diffie–Hellman key agreement systems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(2):89–96, Spring 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n2p89.html; http://link.springer.de/link/service/journals/00145/bibs/10n2p89.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n2p89.tex; http://link.springer.de/link/service/journals/00145/tocs/01002.html.

Cachin:1997:LIR

[129] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(2):97–110, Spring 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n2p97.html; http://link.springer.de/link/service/journals/00145/bibs/10n2p97.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n2p97.tex; http://link.springer.de/link/service/journals/00145/tocs/01002.html.

Klapper:1997:FSR

[130] Andrew Klapper and Mark Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(2):111–147, Spring 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n2p111.html; http://link.springer.de/link/service/journals/00145/bibs/10n2p111.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n2p111.tex; http://link.springer.de/link/service/journals/00145/tocs/01002.html.

Even:1997:CCS

[131] Shimon Even and Yishay Mansour. A

construction of a cipher from a single pseudorandom permutation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(3):151–161, Summer 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n3p151.html; http://link.springer.de/link/service/journals/00145/bibs/10n3p151.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n3p151.tex; http://link.springer.de/link/service/journals/00145/tocs/01003.html.

Damgaard:1997:ESH

[132] Ivan B. Damgård, Torben P. Pedersen, and Birgit Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(3):163–194, Summer 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n3p163.html; http://link.springer.de/link/service/journals/00145/bibs/10n3p163.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n3p163.tex; http://link.springer.de/link/service/journals/00145/tocs/01003.html.

Biham:1997:IDA

[133] Eli Biham and Alex Biryukov. An improvement of Davies' attack on DES. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(3):195–205, Summer 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n3p195.html; http://link.springer.de/link/service/journals/00145/bibs/10n3p195.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n3p195.tex; http://link.springer.de/link/service/journals/00145/tocs/01003.html.

Coppersmith:1997:SBP

[134] Don Coppersmith, Jacques Stern, and Serge Vaudenay. The security of the birational permutation signature schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(3):207–221, Summer 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n3p207.html; http://link.springer.de/link/service/journals/00145/bibs/10n3p207.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n3p207.tex; http://link.springer.de/link/service/journals/00145/tocs/01003.html.

Csirmaz:1997:SSM

[135] László Csirmaz. The size of a share must be large. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(4):223–231, Fall 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n4p223.html; http://link.springer.de/link/service/journals/00145/bibs/10n4p223.pdf; http:

//link.springer.de/link/service/journals/00145/bibs/10n4p223.tex; http://link.springer.de/link/service/journals/00145/tocs/01004.html.

Coppersmith:1997:SSP

[136] Don Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(4):233–260, Fall 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n4p233.html; http://link.springer.de/link/service/journals/00145/bibs/10n4p233.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n4p233.tex; http://link.springer.de/link/service/journals/00145/tocs/01004.html.

Jackson:1997:MTA

[137] Wen-Ai Jackson, Keith M. Martin, and Christine M. O'Keefe. Mutually trusted authority-free secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 10(4): 261–289, Fall 1997. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/10n4p261.html; http://link.springer.de/link/service/journals/00145/bibs/10n4p261.pdf; http://link.springer.de/link/service/journals/00145/bibs/10n4p261.tex; http://link.springer.de/link/service/journals/00145/tocs/01004.html.

Kilian:1998:ENZ

[138] Joe Kilian and Erez Petrank. An efficient noninteractive zero-knowledge proof system for NP with general assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(1):1–27, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n1p1.html; http://link.springer.de/link/service/journals/00145/bibs/11n1p1.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n1p1.tex; http://link.springer.de/link/service/journals/00145/tocs/01101.html.

Sakurai:1998:SCC

[139] Kouichi Sakurai and Hiroki Shizuya. A structural comparison of the computational difficulty of breaking discrete log cryptosystems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(1): 29–43, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n1p29.html; http://link.springer.de/link/service/journals/00145/bibs/11n1p29.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n1p29.tex; http://link.springer.de/link/service/journals/00145/tocs/01101.html.

Biham:1998:CMM

[140] Eli Biham. Cryptanalysis of multiple modes of operation. *Journal of Cryptology: the journal of the International Association for Crypto-*

logic Research, 11(1):45–58, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n1p45.html; http://link.springer.de/link/service/journals/00145/bibs/11n1p45.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n1p45.tex; http://link.springer.de/link/service/journals/00145/tocs/01101.html.

Knudsen:1998:AFD

[141] Lars R. Knudsen, Xuejia Lai, and Bart Preneel. Attacks on fast double block length hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(1):59–72, Winter 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n1p59.html; http://link.springer.de/link/service/journals/00145/bibs/11n1p59.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n1p59.tex; http://link.springer.de/link/service/journals/00145/tocs/01101.html.

Golic:1998:MCI

[142] Jovan Dj. Golić. On matroid characterization of ideal secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(2):75–86, Spring 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n2p75.html; http://link.springer.de/link/service/journals/00145/bibs/11n2p75.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n2p75.tex; http://link.springer.de/link/service/journals/00145/tocs/01102.html.

Naor:1998:PZK

[143] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for NP using any one-way permutation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(2):87–108, Spring 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n2p87.html; http://link.springer.de/link/service/journals/00145/bibs/11n2p87.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n2p87.tex; http://link.springer.de/link/service/journals/00145/tocs/01102.html.

Scheidler:1998:PKC

[144] R. Scheidler. A public-key cryptosystem using purely cubic fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(2):109–124, Spring 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n2p109.html; http://link.springer.de/link/service/journals/00145/bibs/11n2p109.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n2p109.tex;

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

Schnorr:1998:BBM

[145] Claus Peter Schnorr and Serge Vaudenay. The black-box model for cryptographic primitives. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(2):125–140, Spring 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n2p125.html; http://link.springer.de/link/service/journals/00145/bibs/11n2p125.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n2p125.tex; http://link.springer.de/link/service/journals/00145/tocs/01102.html.

Balasubramanian:1998:IEC

[146] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(2):141–145, Spring 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n2p141.html; http://link.springer.de/link/service/journals/00145/bibs/11n2p141.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n2p141.tex; http://link.springer.de/link/service/journals/00145/tocs/01102.html.

Brandt:1998:ZKA

[147] Jørgen Brandt, Ivan Damgård, Peter Landrock, and Torben Pedersen. Zero-knowledge authentication scheme with secret key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(3):147–159, Summer 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n3p147.html; http://link.springer.de/link/service/journals/00145/bibs/11n3p147.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n3p147.tex; http://link.springer.de/link/service/journals/00145/tocs/01103.html.

Joux:1998:LRT

[148] Antoine Joux and Jacques Stern. Lattice reduction: a toolbox for the cryptanalyst. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(3):161–185, Summer 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n3p161.html; http://link.springer.de/link/service/journals/00145/bibs/11n3p161.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n3p161.tex; http://link.springer.de/link/service/journals/00145/tocs/01103.html.

Dwork:1998:EEU

[149] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. *Journal of Cryptology: the journal of the

International Association for Cryptologic Research, 11(3):187–208, Summer 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n3p187.html; http://link.springer.de/link/service/journals/00145/bibs/11n3p187.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n3p187.tex; http://link.springer.de/link/service/journals/00145/tocs/01103.html.

Damgaard:1998:TKT

[150] Ivan B. Damgård and Lars R. Knudsen. Two-key triple encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(3):209–218, Summer 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n3p209.html; http://link.springer.de/link/service/journals/00145/bibs/11n3p209.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n3p209.tex; http://link.springer.de/link/service/journals/00145/tocs/01103.html.

Muller:1998:FME

[151] Volker Müller. Fast multiplication on elliptic curves over small fields of characteristic two. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(4):219–234, Fall 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n4p219.html; http://link.springer.de/link/service/journals/00145/bibs/11n4p219.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n4p219.tex; http://link.springer.de/link/service/journals/00145/tocs/01104.html.

Murphy:1998:AS

[152] Sean Murphy. An analysis of SAFER. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(4):235–251, Fall 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n4p235.html; http://link.springer.de/link/service/journals/00145/bibs/11n4p235.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n4p235.tex; http://link.springer.de/link/service/journals/00145/tocs/01104.html.

Dobbertin:1998:CM

[153] Hans Dobbertin. Cryptanalysis of MD4. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(4):253–271, Fall 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n4p253.html; http://link.springer.de/link/service/journals/00145/bibs/11n4p253.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n4p253.tex; http://link.springer.de/link/service/journals/00145/tocs/01104.html.

Rogaway:1998:SOE

[154] Phillip Rogaway and Don Coppersmith.

A software-optimized encryption algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 11(4): 273–287, Fall 1998. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/11n4p273.html; http://link.springer.de/link/service/journals/00145/bibs/11n4p273.pdf; http://link.springer.de/link/service/journals/00145/bibs/11n4p273.tex; http://link.springer.de/link/service/journals/00145/tocs/01104.html.

vanOorschot:1999:PCS

[155] Paul C. van Oorschot and Michael J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(1):1–28, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n1p1.html; http://link.springer.de/link/service/journals/00145/papers/12n1p1.pdf; http://link.springer.de/link/service/journals/00145/papers/12n1p1.tex.

Naor:1999:CPP

[156] Moni Naor and Omer Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(1):29–66, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n1p29.html; http://link.springer.de/link/service/journals/00145/papers/12n1p29.pdf; http://link.springer.de/link/service/journals/00145/papers/12n1p29.tex.

Smart:1999:FDH

[157] N. P. Smart and S. Siksek. A fast Diffie–Hellman protocol in genus 2. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(1):67–73, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n1p67.html; http://link.springer.de/link/service/journals/00145/papers/12n1p67.pdf; http://link.springer.de/link/service/journals/00145/papers/12n1p67.tex.

Halevi:1999:ECS

[158] Shai Halevi. Efficient commitment schemes with bounded sender and unbounded receiver. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12 (2):77–89, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n2p77.html; http://link.springer.de/link/service/journals/00145/papers/12n2p77.pdf; http://link.springer.de/link/service/journals/00145/papers/12n2p77.tex.

Rogaway:1999:BHA

[159] Phillip Rogaway. Bucket hashing and its application to fast message authentication. *Journal of Cryptology: the journal of the International Associa-*

tion for Cryptologic Research, 12(2): 91–115, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n2p91.html; http://link.springer.de/link/service/journals/00145/papers/12n2p91.pdf; http://link.springer.de/link/service/journals/00145/papers/12n2p91.tex.

Bellare:1999:TCA

[160] Mihir Bellare and Ronald L. Rivest. Translucent cryptography — an alternative to key escrow, and its implementation via fractional oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(2): 117–139, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n2p117.html; http://link.springer.de/link/service/journals/00145/papers/12n2p117.pdf; http://link.springer.de/link/service/journals/00145/papers/12n2p117.tex.

Smart:1999:ECC

[161] N. P. Smart. Elliptic curve cryptosystems over small fields of odd characteristic. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(2): 141–151, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n2p141.html; http://link.springer.de/link/service/journals/00145/papers/12n2p141.pdf; http://link.springer.de/link/service/journals/00145/papers/12n2p141.tex.

Blundo:1999:FBA

[162] Carlo Blundo, Alfredo De Santis, Kaoru Kurosawa, and Wakaha Ogata. On a fallacious bound for authentication codes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(3): 155–159, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p155.html; http://link.springer.de/link/service/journals/00145/papers/12n3p155.pdf.

Biham:1999:CTM

[163] Eli Biham. Cryptanalysis of triple modes of operation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12 (3):161–184, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p161.html; http://link.springer.de/link/service/journals/00145/papers/12n3p161.pdf.

Bernstein:1999:HSR

[164] Daniel J. Bernstein. How to stretch random functions: The security of protected counter sums. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12 (3):185–192, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p185.html; http://link.springer.de/link/service/journals/00145/papers/12n3p185.pdf.

Smart:1999:DLP

[165] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(3): 193–196, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p193.html; http://link.springer.de/link/service/journals/00145/papers/12n3p193.pdf.

Burmester:1999:DSF

[166] Mike Burmester, Yvo G. Desmedt, Toshiya Itoh, Kouichi Sakurai, and Hiroki Shizuya. Divertible and subliminal-free zero-knowledge proofs for languages. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(3): 197–223, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n3p197.html; http://link.springer.de/link/service/journals/00145/papers/12n3p197.pdf.

Quinn:1999:BKD

[167] Kathleen A. S. Quinn. Bounds for key distribution patterns. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12 (4):227–239, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n4p227.html; http://link.springer.de/link/service/journals/00145/papers/12n4p227.pdf; http://link.springer.de/link/service/journals/00145/papers/12n4p227.tex.

Joye:1999:CRB

[168] Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese remaindering based cryptosystems in the presence of faults. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12 (4):241–245, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n4p241.html; http://link.springer.de/link/service/journals/00145/papers/12n4p241.pdf; http://link.springer.de/link/service/journals/00145/papers/12n4p241.tex.

Shoup:1999:SPI

[169] Victor Shoup. On the security of a practical identification scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 12(4):247–260, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n4p247.html; http://link.springer.de/link/service/journals/00145/papers/12n4p247.pdf; http://link.springer.de/link/service/journals/00145/papers/12n4p247.tex.

Blundo:1999:CVC

[170] Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology: the journal of the International Association for*

Cryptologic Research, 12(4):261–289, 1999. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/12n4p261.html; http://link.springer.de/link/service/journals/00145/papers/12n4p261.pdf; http://link.springer.de/link/service/journals/00145/papers/12n4p261.tex.

Goldreich:2000:P

[171] Oded Goldreich. Preface. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1):1–7, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130001.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130001.pdf.

Franklin:2000:SCM

[172] Matthew Franklin and Rebecca N. Wright. Secure communication in minimal connectivity models. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1):9–30, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130009.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130009.pdf.

Hirt:2000:PSG

[173] Martin Hirt and Ueli Maurer. Player simulation and general adversary structures in perfect multiparty computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1):31–60, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130031.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130031.pdf.

Canetti:2000:MAC

[174] Ran Canetti, Shai Halevi, and Amir Herzberg. Maintaining authenticated communication in the presence of break-ins. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1):61–105, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130061.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130061.pdf.

Canetti:2000:RVF

[175] Ran Canetti, Eyal Kushilevitz, Rafail Ostrovsky, and Adi Rosén. Randomness versus fault-tolerance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1):107–142, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130107.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130107.pdf.

Canetti:2000:SCM

[176] Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(1): 143–202, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013001/00130143.html; http://link.springer.de/link/service/journals/00145/papers/0013001/00130143.pdf.

Zbinden:2000:PAQ

[177] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel. Practical aspects of quantum cryptographic key distribution. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13 (2):207–220, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013002/00130207.html; http://link.springer.de/link/service/journals/00145/papers/0013002/00130207.pdf.

Fischlin:2000:SSP

[178] R. Fischlin and C. P. Schnorr. Stronger security proofs for RSA and Rabin bits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(2): 221–244, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013002/00130221.html; http://link.springer.de/link/service/journals/00145/papers/0013002/00130221.pdf.

Golic:2000:FCA

[179] Jovan Dj. Golic, Mahmoud Salmasizadeh, and Ed Dawson. Fast correlation attacks on the summation generator. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(2): 245–262, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013002/00130245.html; http://link.springer.de/link/service/journals/00145/papers/0013002/00130245.pdf.

Paulus:2000:NPK

[180] Sachar Paulus and Tsuyoshi Takagi. A new public-key cryptosystem over a quadratic order with quadratic decryption time. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13 (2):263–272, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013002/00130263.html; http://link.springer.de/link/service/journals/00145/papers/0013002/00130263.pdf.

Gennaro:2000:RES

[181] Rosario Gennaro, Tal Rabin, Stanislav Jarecki, and Hugo Krawczyk. Robust and efficient sharing of RSA functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(2): 273–300, 2000. CODEN JOCREQ.

ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/bibs/0013002/00130273.html; http://link.springer.de/link/service/journals/00145/papers/0013002/00130273.pdf.

Zhang:2000:MCA

[182] Muxiang Zhang. Maximum correlation analysis of nonlinear combining functions in stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(3):301–314, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10007/; http://link.springer.de/link/service/journals/00145/contents/00/10007/paper/10007.pdf.

Petrank:2000:CMR

[183] Erez Petrank and Charles Rackoff. CBC MAC for real-time data sources. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(3):315–338, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10009/; http://link.springer.de/link/service/journals/00145/contents/00/10009/paper/10009.pdf.

Coppersmith:2000:PAD

[184] Don Coppersmith and Igor Shparlinski. On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(3):339–360, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10002/; http://link.springer.de/link/service/journals/00145/contents/00/10002/paper/10002.pdf.

Pointcheval:2000:SAD

[185] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(3):361–396, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10003/; http://link.springer.de/link/service/journals/00145/contents/00/10003/paper/10003.pdf.

Gennaro:2000:RBU

[186] Rosario Gennaro, Tal Rabin, and Hugo Krawczyk. RSA-based undeniable signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(4):397–416, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10001/; http://link.springer.de/link/service/journals/00145/contents/00/10001/paper/10001.pdf.

Knudsen:2000:DAS

[187] Lars R. Knudsen. A detailed analysis of SAFER K. *Journal of Cryp-*

tology: the journal of the International Association for Cryptologic Research, 13(4):417–436, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10004/; http://link.springer.de/link/service/journals/00145/contents/00/10004/paper/10004.pdf`.

Pollard:2000:KMD

[188] J. M. Pollard. Kangaroos, Monopoly and discrete logarithms. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(4):437–447, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10010/; http://link.springer.de/link/service/journals/00145/contents/00/10010/paper/10010.pdf`.

Boyar:2000:SNI

[189] Joan Boyar, Ivan Damgård, and René Peralta. Short non-interactive cryptographic proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(4):449–472, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10011/; http://link.springer.de/link/service/journals/00145/contents/00/10011/paper/10011.pdf`.

Jacobson:2000:CDL

[190] Michael J. Jacobson, Jr. Computing discrete logarithms in quadratic orders. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 13(4): 473–492, 2000. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10013/; http://link.springer.de/link/service/journals/00145/contents/00/10013/paper/10013.pdf`.

Klapper:2001:ESK

[191] Andrew Klapper. On the existence of secure keystream generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(1):1–15, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10014/; http://link.springer.de/link/service/journals/00145/contents/00/10014/paper/10014.pdf`.

Kilian:2001:HPA

[192] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(1):17–35, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10015/; http://link.springer.de/link/service/journals/00145/contents/00/10015/paper/10015.pdf`.

DiCrescenzo:2001:USP

[193] Giovanni Di Crescenzo, Yuval Ishai,

and Rafail Ostrovsky. Universal service-providers for private information retrieval. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(1):37–74, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10008/`; `http://link.springer.de/link/service/journals/00145/contents/00/10008/paper/10008.pdf`.

Coppersmith:2001:WQS

[194] Don Coppersmith. Weakness in quaternion signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(2):77–85, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10006/`; `http://link.springer.de/link/service/journals/00145/contents/00/10006/paper/10006.pdf`.

Vaudenay:2001:CCR

[195] Serge Vaudenay. Cryptanalysis of the Chor–Rivest cryptosystem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(2):87–100, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10005/`; `http://link.springer.de/link/service/journals/00145/contents/00/10005/paper/10005.pdf`.

Boneh:2001:IEE

[196] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of eliminating errors in cryptographic computations. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(2):101–119, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/00/10016/`; `http://link.springer.de/link/service/journals/00145/contents/00/10016/paper/10016.pdf`.

Wang:2001:SCM

[197] Yongge Wang and Yvo Desmedt. Secure communication in multicast channels: The answer to Franklin and Wright's question. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(2):121–135, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0002/`; `http://link.springer.de/link/service/journals/00145/contents/01/0002/paper/0002.pdf`.

Ye:2001:DAA

[198] Dingfeng Ye, Zongduo Dai, and Kwok-Yan Lam. Decomposing attacks on asymmetric cryptography based on mapping compositions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(2):137–150, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/`

journals/00145/contents/01/0001/ ; http://link.springer.de/link/service/journals/00145/contents/01/0001/paper/0001.pdf.

Bailey:2001:EAF

[199] Daniel V. Bailey and Christof Paar. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(3):153–176, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/00/10012/ ; http://link.springer.de/link/service/journals/00145/contents/00/10012/paper/10012.pdf.

Goldmann:2001:CBG

[200] Mikael Goldmann, Mats Näslund, and Alexander Russell. Complexity bounds on general hard-core predicates. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(3):177–195, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/01/0007/ ; http://link.springer.de/link/service/journals/00145/contents/01/0007/paper/0007.pdf.

Jakobsen:2001:ABC

[201] Thomas Jakobsen and Lars R. Knudsen. Attacks on block ciphers of low algebraic degree. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(3):197–210, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/01/0003/ ; http://link.springer.de/link/service/journals/00145/contents/01/0003/paper/0003.pdf.

Fiat:2001:DTT

[202] Amos Fiat and Tamir Tassa. Dynamic traitor tracing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(3):211–223, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/01/0006/ ; http://link.springer.de/link/service/journals/00145/contents/01/0006/paper/0006.pdf.

Scanlon:2001:PKC

[203] Thomas Scanlon. Public key cryptosystems based on Drinfeld modules are insecure. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(4):225–230, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/01/0004/ ; http://link.springer.de/link/service/journals/00145/contents/01/0004/paper/0004.pdf.

Kurosawa:2001:AWI

[204] Kaoru Kurosawa, Thomas Johansson, and Douglas R. Stinson. Almost k-wise independent sample spaces and their cryptologic applications. *Journal of Cryptology: the journal of the In-*

ternational Association for Cryptologic Research, 14(4):231–253, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0010/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0010/paper/0010.pdf`.

Lenstra:2001:SCK

[205] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 14(4):255–293, 2001. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0009/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0009/paper/0009.pdf`.

Micali:2002:IES

[206] Silvio Micali and Leonid Reyzin. Improving the exact security of digital signature schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(1):1–18, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0005/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0005/paper/0005.pdf`.

Gaudry:2002:CDF

[207] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(1):19–46, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0011/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0011/paper/0011.pdf`.

Biham:2002:CAX

[208] Eli Biham and Lars R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(1):47–59, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0016/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0016/paper/0016.pdf`.

Moldovyan:2002:CBD

[209] A. A. Moldovyan and N. A. Moldovyan. A cipher based on data-dependent permutations. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(1):61–72, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0012/` ; `http://link.springer.de/link/service/journals/00145/contents/01/0012/paper/0012.pdf`.

Shoup:2002:STC

[210] Victor Shoup and Rosario Gennaro. Se-

curing threshold cryptosystems against chosen ciphertext attack. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(2):75–96, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0020/`; `http://link.springer.de/link/service/journals/00145/contents/01/0020/paper/0020.pdf`.

Naor:2002:CPR

[211] Moni Naor and Omer Reingold. Constructing pseudo-random permutations with a prescribed structure. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(2):97–102, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0008/`; `http://link.springer.de/link/service/journals/00145/contents/01/0008/paper/0008.pdf`.

Abadi:2002:RTV

[212] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(2):103–127, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0014/`; `http://link.springer.de/link/service/journals/00145/contents/01/0014/paper/0014.pdf`.

Galbraith:2002:ECP

[213] Steven D. Galbraith. Elliptic curve Paillier schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(2):129–138, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0015/`; `http://link.springer.de/link/service/journals/00145/contents/01/0015/paper/0015.pdf`.

Johnston:2002:AKE

[214] Anna M. Johnston and Peter S. Gemmell. Authenticated key exchange provably secure against the man-in-the-middle attack. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(2):139–148, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/01/0017/`; `http://link.springer.de/link/service/journals/00145/contents/01/0017/paper/0017.pdf`.

Nguyen:2002:IDS

[215] Phong Q. Nguyen and Igor E. Shparlinski. The insecurity of the Digital Signature Algorithm with partially known nonces. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(3):151–176, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.de/link/service/journals/00145/contents/02/0021/index.html`; `http://link.springer.`

de/link/service/journals/00145/contents/02/0021/paper/s00145-002-0021-3.pdf.

Lindell:2002:PPD

[216] Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(3):177–206, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/01/0019/index.html; http://link.springer.de/link/service/journals/00145/contents/01/0019/paper/s00145-001-0019-2.pdf.

Knudsen:2002:SFC

[217] Lars R. Knudsen. The security of Feistel ciphers with six rounds or less. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(3):207–222, 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.de/link/service/journals/00145/contents/02/9839/index.html; http://link.springer.de/link/service/journals/00145/contents/02/9839/paper/s00145-002-9839-y.pdf.

Shoup:2002:OR

[218] Victor Shoup. OAEP reconsidered. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(4):223–249, September 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Catalano:2002:PTF

[219] Dario Catalano, Rosario Gennaro, and Nick Howgrave-Graham. Paillier's trapdoor function hides up to $O(n)$ bits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(4):251–269, September 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Bellare:2002:NNF

[220] Mihir Bellare. A note on negligible functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(4):271–284, September 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Magliveras:2002:NAD

[221] S. S. Magliveras, D. R. Stinson, and Tran van Trung. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 15(4):285–297, September 2002. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Myers:2003:EAS

[222] Steven Myers. Efficient amplification of the security of weak pseudo-random function generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(1):1–24, January 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Beimel:2003:BAM

[223] Amos Beimel and Shlomi Dolev. Buses for anonymous message delivery. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(1):25–39, January 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Golic:2003:EPC

[224] Jovan Dj. Golic and Renato Menicocci. Edit probability correlation attacks on stop/go clocked keystream generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(1):41–68, January 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Goldreich:2003:SME

[225] Oded Goldreich and Vered Rosen. On the security of modular exponentiation with application to the construction of pseudorandom generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(2):71–93, March 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Ben-Or:2003:THI

[226] Michael Ben-Or and Dan Gutfreund. Trading help for interaction in statistical zero-knowledge proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(2):95–116, March 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Muller:2003:PPT

[227] Siguna Müller. A probable prime test with very high confidence for $nL3$ mod 4. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(2):117–139, March 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lindell:2003:PCT

[228] Yehuda Lindell. Parallel coin-tossing and constant-round secure two-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(3):143–184, June 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Bellare:2003:OMR

[229] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko. The one-more-RSA-inversion problems and the security of Chaum's blind signature scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(3):185–215, June 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Brassard:2003:OTP

[230] Gilles Brassard, Claude Crépeau, and Stefan Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(4):219–237, September 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Joux:2003:SDD

[231] Antoine Joux and Kim Nguyen. Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *Journal of Cryptology: the journal of the International*

Association for Cryptologic Research, 16(4):239–247, September 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Vaudenay:2003:DTB

[232] Serge Vaudenay. Decorrelation: a theory for block cipher security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(4):249–286, September 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kalai:2003:GRF

[233] Adam Kalai. Generating random factored numbers, easily. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 16(4):287–289, September 2003. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://people.cs.uchicago.edu/~kalai/factor/factor.html`.

Goldreich:2004:P

[234] Oded Goldreich. Preface. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(1):1–3, January 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Dziembowski:2004:ORE

[235] Stefan Dziembowski and Ueli Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(1):5–26, January 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lu:2004:EAS

[236] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(1):27–42, January 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Vadhan:2004:CLC

[237] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(1):43–77, January 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Fujisaki:2004:ROS

[238] Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. RSA-OAEP is secure under the RSA assumption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(2):81–104, March 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Wiener:2004:FCC

[239] Michael J. Wiener. The full cost of cryptanalytic attacks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(2):105–124, March 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Beimel:2004:RSC

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

tation in Private Information Retrieval: PIR with preprocessing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(2):125–151, March 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Canetti:2004:AVN

[241] Ran Canetti, Ivan Damgård, Stefan Dziembowski, Yuval Ishai, and Tal Malkin. Adaptive versus non-adaptive security of multi-party protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(3):153–207, June 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Hast:2004:NOS

[242] Gustav Hast. Nearly one-sided tests and the Goldreich–Levin predicate. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(3):209–229, June 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lenstra:2004:P

[243] Arjen K. Lenstra. Preface. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4):233, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=233`.

Miller:2004:WPE

[244] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4):235–261, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=235`.

Joux:2004:ORP

[245] Antoine Joux. A one round protocol for tripartite Diffie–Hellman. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4):263–276, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=263`.

Verheul:2004:EXM

[246] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4):277–296, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=277`.

Boneh:2004:SSW

[247] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4):297–319, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http:`

//www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=297.

Barreto:2004:EIP

[248] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 17(4): 321–334, September 2004. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=17&issue=4&spage=321.

Naor:2005:CSO

[249] Moni Naor and Benny Pinkas. Computationally secure oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18 (1):1–35, January 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=1&spage=1.

Fitzi:2005:MCP

[250] Matthias Fitzi, Juan A. Garay, Ueli Maurer, et al. Minimal complete primitives for secure multi-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18 (1):37–61, January 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=1&spage=37.

Cohen:2005:ASW

[251] Henri Cohen. Analysis of the sliding window powering algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(1):63–76, January 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=1&spage=63.

Dupont:2005:BCA

[252] Régis Dupont, Andreas Enge, and François Morain. Building curves with arbitrary small MOV degree over finite prime fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):79–89, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=79.

Gennaro:2005:IPR

[253] Rosario Gennaro. An improved pseudo-random generator based on the discrete logarithm problem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):91–110, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=91.

Black:2005:CMA

[254] John Black and Phillip Rogaway. CBC MACs for arbitrary-length messages: The three-key constructions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):111–131, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=111`.

Lo:2005:EQK

[255] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):133–165, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=133`.

Tassa:2005:LBD

[256] Tamir Tassa. Low bandwidth dynamic traitor tracing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(2):167–183, April 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=2&spage=167`.

Canetti:2005:P

[257] Ran Canetti. Preface. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(3):187–189, July 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=3&spage=187`.

Considine:2005:BAG

[258] Jeffrey Considine, Matthias Fitzi, Matthew Franklin, Leonid A. Levin, Ueli Maurer, and David Metcalf. Byzantine agreement given partial broadcast. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18 (3):191–217, July 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=3&spage=191`.

Cachin:2005:ROC

[259] Christian Cachin, Klaus Kursawe, and Victor Shoup. Random oracles in Constantinople: Practical asynchronous Byzantine agreement using cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18 (3):219–246, July 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=3&spage=219`.

Goldwasser:2005:SMP

[260] Shafi Goldwasser and Yehuda Lindell. Secure multi-party computation without agreement. *Journal of Cryptology: the journal of the International*

Association for Cryptologic Research, 18(3):247–287, July 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=3&spage=247`.

Biham:2005:CSR

[261] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4): 291–311, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=291`.

Kent:2005:SCB

[262] Adrian Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4):313–335, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=313`.

vonzurGathen:2005:PNB

[263] Joachim von zur Gathen and Michael Nöcker. Polynomial and normal bases for finite fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4):337–355, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=337`.

Avanzi:2005:CCM

[264] Roberto M. Avanzi. The complexity of certain multi-exponentiation techniques in cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4):357–373, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=357`.

Knudsen:2005:PKR

[265] Lars R. Knudsen and Chris J. Mitchell. Partial key recovery attack against RMAC. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4): 375–389, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=375`.

Blundo:2005:ADD

[266] Carlo Blundo and Paolo D'Arco. Analysis and design of distributed key distribution centers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 18(4):391–414, September 2005. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=18&issue=4&spage=391`.

Denef:2006:EKA

[267] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (1):1–25, January 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=1&spage=1.

MacKenzie:2006:TPA

[268] Philip MacKenzie, Thomas Shrimpton, and Markus Jakobsson. Threshold password-authenticated key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (1):27–66, January 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=1&spage=27.

Katz:2006:CSN

[269] Jonathan Katz and Moti Yung. Characterization of security notions for probabilistic private-key encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(1):67–95, January 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=1&spage=67.

Chang:2006:IBO

[270] Yan-Cheng Chang, Chun-Yuan Hsiao, and Chi-Jen Lu. The impossibility of basing one-way permutations on central cryptographic primitives. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(1):97–114, January 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=1&spage=97.

Teske:2006:ECT

[271] Edlyn Teske. An elliptic curve trapdoor system. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (1):115–133, January 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=1&spage=115.

Canetti:2006:LUC

[272] Ran Canetti, Eyal Kushilevitz, and Yehuda Lindell. On the limitations of universally composable two-party computation without set-up assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (2):135–167, April 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=2&spage=135.

Garay:2006:SZK

[273] Juan A. Garay, Philip MacKenzie, and Ke Yang. Strengthening zero-knowledge protocols using signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(2):169–209, April 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=2&spage=169`.

Jacobson:2006:IRQ

[274] Michael J. Jacobson, Renate Scheidler, and Hugh C. Williams. An improved real-quadratic-field-based key exchange procedure. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(2):211–239, April 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=2&spage=211`.

Goldreich:2006:SKG

[275] Oded Goldreich and Yehuda Lindell. Session-key generation using human passwords only. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(3):241–340, July 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=3&spage=241`.

Blaser:2006:PCC

[276] Markus Bläser, Andreas Jakoby, Maciej Liskiewicz, and Bodo Manthey. Private computation: k-connected versus 1-connected networks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(3):341–357, July 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=3&spage=341`.

Lindell:2006:SCC

[277] Yehuda Lindell. A simpler construction of CCA2-secure public-key encryption under general assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19(3):359–377, July 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=3&spage=359`.

Biham:2006:PSQ

[278] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):381–439, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=381`.

Hong:2006:KIK

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

IV attacks on multiple modes of operation of block ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):441–462, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=441`.

Girault:2006:FAS

[280] Marc Girault, Guillaume Poupard, and Jacques Stern. On the fly authentication and signature schemes based on groups of unknown order. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):463–487, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=463`.

Damgard:2006:EQF

[281] Ivan Bjerre Damgard and Gudmund Skovbjerg Frandsen. An extended quadratic Frobenius primality test with average- and worst-case error estimate. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):489–520, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=489`.

Harnik:2006:CTP

[282] Danny Harnik, Moni Naor, Omer Reingold, and Alon Rosen. Completeness in two-party secure computation: a computational view. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):521–552, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=521`.

Luca:2006:ECL

[283] Florian Luca and Igor E. Shparlinski. Elliptic curves with low embedding degree. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 19 (4):553–562, October 2006. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=19&issue=4&spage=553`.

Anonymous:2007:EN

[284] Anonymous. Editor's note. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(1):1, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=1`.

Koblitz:2007:ALS

[285] Neal Koblitz and Alfred J. Menezes. Another look at "provable security". *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20 (1):3–37, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print),

1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=3.

Coron:2007:DPT

[286] Jean-Sebastien Coron and Alexander May. Deterministic polynomial-time equivalence of computing the RSA secret key and factoring. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(1):39–50, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=39.

Gennaro:2007:SDK

[287] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(1):51–83, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=51.

Katz:2007:SPA

[288] Jonathan Katz and Moti Yung. Scalable protocols for authenticated group key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(1):85–113, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=85.

Catalano:2007:THI

[289] Dario Catalano, David Pointcheval, and Thomas Pornin. Trapdoor hard-to-invert group isomorphisms and their application to password-based authentication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(1):115–149, January 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=1&spage=115.

Haastad:2007:SII

[290] Johan Håstad. The security of the IAPM and IACBC modes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(2):153–163, April 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=2&spage=153.

Ding:2007:CRO

[291] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-round oblivious transfer in the bounded storage model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(2):165–202, April 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=2&spage=165.

Baek:2007:FPS

[292] Joonsang Baek, Ron Steinfeld, and Yuliang Zheng. Formal proofs for the security of signcryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(2):203–235, April 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=2&spage=203`.

Tassa:2007:HTS

[293] Tamir Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(2):237–264, April 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=2&spage=237`.

Canetti:2007:FSP

[294] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):265–294, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=265`.

Beimel:2007:RIT

[295] Amos Beimel and Yoav Stahl. Robust information-theoretic private information retrieval. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):295–321, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=295`.

Blundo:2007:USD

[296] Carlo Blundo, Paolo D'Arco, Alfredo De Santis, and Douglas Stinson. On unconditionally secure distributed oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):323–373, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=323`.

Cheng:2007:PPO

[297] Qi Cheng. Primality proving via one round in ECPP and one iteration in AKS. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):375–387, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=375`.

Tsaban:2007:TCK

[298] Boaz Tsaban. Theoretical cryptanalysis of the Klimov–Shamir number generator TF-1. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):389–392, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print),

1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=389.

Gennaro:2007:RES

[299] Rosario Gennaro, Tal Rabin, Stanislav Jarecki, and Hugo Krawczyk. Robust and efficient sharing of RSA functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):393, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=393.

Gennaro:2007:RBU

[300] Rosario Gennaro, Tal Rabin, and Hugo Krawczyk. RSA-based undeniable signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):394, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=394.

Abadi:2007:RTV

[301] Martin Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(3):395, July 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=3&spage=395.

Ostrovsky:2007:PSS

[302] Rafail Ostrovsky and William E. Skeith. Private searching on streaming data. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(4):397–430, October 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=4&spage=397.

Kalai:2007:CCS

[303] Yael Tauman Kalai, Yehuda Lindell, and Manoj Prabhakaran. Concurrent composition of secure protocols in the timing model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(4):431–492, October 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=20&issue=4&spage=431.

Goh:2007:ESS

[304] Eu-Jin Goh, Stanislaw Jarecki, Jonathan Katz, and Nan Wang. Efficient signature schemes with tight reductions to the Diffie–Hellman problems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 20(4):493–514, October 2007. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0933-2790&volume=20&issue=4&spage=493.

Haastad:2008:PCA

[305] Johan Håstad and Mats Näslund. Practical construction and analysis of pseudo-randomness primitives. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):1–26, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=1.

Coppersmith:2008:CII

[306] D. Coppersmith, J. S. Coron, F. Grieu, S. Halevi, C. Jutla, D. Naccache, and J. P. Stern. Cryptanalysis of ISO/IEC 9796-1. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):27–51, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=27.

Nguyen:2008:SSK

[307] Minh-Huyen Nguyen and Salil Vadhan. Simpler session-key generation from short random passwords. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):52–96, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=52.

Abe:2008:TKN

[308] Masayuki Abe, Rosario Gennaro, and Kaoru Kurosawa. Tag-KEM/DEM: a new framework for hybrid encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):97–130, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=97.

Selcuk:2008:PSL

[309] Ali Aydın Selçuk. On probability of success in linear and differential cryptanalysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(1):131–147, January 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=1&spage=131.

Boneh:2008:SSR

[310] Dan Boneh and Xavier Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(2):149–177, April 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=2&spage=149.

Bentahar:2008:GCI

[311] K. Bentahar, P. Farshim, J. Malone-Lee, and N. P. Smart. Generic constructions of identity-based and certificateless KEMs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(2):178–199, April 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=2&spage=178.

Lindell:2008:LBI

[312] Yehuda Lindell. Lower bounds and impossibility results for concurrent self composition. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21 (2):200–249, April 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=2&spage=200.

Renault:2008:PRP

[313] Jérôme Renault and Tristan Tomala. Probabilistic reliability and privacy of communication using multicast in general neighbor networks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(2):250–279, April 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=2&spage=250.

Overbeck:2008:SAP

[314] R. Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(2):280–301, April 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=2&spage=280.

Katz:2008:HEP

[315] Jonathan Katz and Yehuda Lindell. Handling expected polynomial-time strategies in simulation-based security proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21 (3):303–349, July 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=3&spage=303.

Abdalla:2008:SER

[316] 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 anonymous IBE, and extensions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(3):350–391, July 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=3&spage=350.

Barkan:2008:ICO

[317] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21 (3):392–429, July 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=3&spage=392`.

Lu:2008:CEL

[318] Yi Lu and Serge Vaudenay. Cryptanalysis of an E0-like combiner with memory. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21 (3):430–457, July 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=3&spage=430`.

Matucci:2008:CSP

[319] Francesco Matucci. Cryptanalysis of the Shpilrain–Ushakov protocol for Thompson's group. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(3):458–468, July 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=3&spage=458`.

Bellare:2008:AER

[320] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21 (4):469–491, October 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=4&spage=469`.

KAsters:2008:RBN

[321] Ralf Küsters, Anupam Datta, John C. Mitchell, and Ajith Ramanathan. On the relationships between notions of simulation-based security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(4): 492–546, October 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=4&spage=492`.

Jutla:2008:EMA

[322] Charanjit S. Jutla. Encryption modes with almost free message integrity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(4): 547–578, October 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=4&spage=547`.

Jain:2008:NBC

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

ment. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(4): 579–592, October 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=4&spage=579`.

Diem:2008:ICC

[324] Claus Diem and Emmanuel Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 21(4): 593–611, October 2008. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=21&issue=4&spage=593`.

Bellare:2009:SPI

[325] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(1):1–61, January 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=1`.

Lempken:2009:PKC

[326] Wolfgang Lempken, Trung van Tran, Spyros S. Magliveras, and Wandi Wei. A public key cryptosystem based on non-abelian finite groups. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(1):62–74, January 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=62`.

Impagliazzo:2009:CTD

[327] Russell Impagliazzo, Ragesh Jaiswal, and Valentine Kabanets. Chernoff-type direct product theorems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(1):75–92, January 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=75`.

Charles:2009:CHF

[328] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(1):93–113, January 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=93`.

Bender:2009:RSS

[329] Adam Bender, Jonathan Katz, and Ruggero Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (1):114–138, January 2009. CODEN

JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=1&spage=114.

Nguyen:2009:LPC

[330] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (2):139–160, April 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=2&spage=139.

Lindell:2009:PSY

[331] Yehuda Lindell and Benny Pinkas. A proof of security of Yao's protocol for two-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(2):161–188, April 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=2&spage=161.

Moran:2009:NIT

[332] Tal Moran, Ronen Shaltiel, and Amnon Ta-Shma. Non-interactive timestamping in the bounded-storage model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(2):189–226, April 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=2&spage=189.

Tassa:2009:MSS

[333] Tamir Tassa and Nira Dyn. Multipartite secret sharing by bivariate interpolation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (2):227–258, April 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=2&spage=227.

Barbosa:2009:CDU

[334] M. Barbosa, A. Moss, and D. Page. Constructive and destructive use of compilers in elliptic curve cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (2):259–281, April 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=2&spage=259.

Haitner:2009:RCA

[335] Iftach Haitner, Omer Horvitz, Jonathan Katz, Chiu-Yuen Koo, Ruggero Morselli, et al. Reducing complexity assumptions for statistically-hiding commitment. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (3):283–310, July 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=283.

Black:2009:IHE

[336] J. Black, M. Cochran, and T. Shrimpton. On the impossibility of highly-efficient blockcipher-based hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (3):311–329, July 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=311.

Rubin:2009:UAV

[337] K. Rubin and A. Silverberg. Using Abelian varieties to improve pairing-based cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(3):330–364, July 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=330.

Dedic:2009:ULB

[338] Nenad Dedić, Gene Itkis, Leonid Reyzin, and Scott Russell. Upper and lower bounds on black-box steganography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(3):365–394, July 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=365.

Lindell:2009:GCU

[339] Yehuda Lindell. General composition and universal composability in secure multiparty computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(3):395–428, July 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=3&spage=395.

Applebaum:2009:CCI

[340] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography with constant input locality. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (4):429–469, October 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=4&spage=429.

Cash:2009:TDP

[341] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie–Hellman problem and applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (4):470–504, October 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=4&spage=470.

Smith:2009:IDL

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

Jacobians of genus 3 hyperelliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(4): 505–529, October 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=4&spage=505.

Fischlin:2009:ENM

[343] Marc Fischlin and Roger Fischlin. Efficient non-malleable commitment schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22(4): 530–571, October 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=4&spage=530.

DiRaimondo:2009:NAD

[344] Mario Di Raimondo and Rosario Gennaro. New approaches for deniable authentication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 22 (4):572–615, October 2009. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=22&issue=4&spage=572.

Goldreich:2010:EPP

[345] Oded Goldreich. On expected probabilistic polynomial-time adversaries: a suggestion for restricted definitions and their benefits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(1):1–36, January 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=1&spage=1.

Tromer:2010:ECA

[346] Eran Tromer, Dag Arne Osvik, and Adi Shamir. Efficient cache attacks on AES, and countermeasures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(1):37–71, January 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=1&spage=37.

Knudsen:2010:CM

[347] Lars R. Knudsen, John Erik Mathiassen, Frédéric Muller, and Søren S. Thomsen. Cryptanalysis of MD2. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(1):72–90, January 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=1&spage=72.

Desmedt:2010:NIP

[348] Yvo Desmedt, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. A new and improved paradigm for hybrid encryption secure against chosen-ciphertext attack. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(1):91–120, January 2010. CODEN

JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=1&spage=91.

Hofheinz:2010:OCP

[349] Dennis Hofheinz, John Malone-Lee, and Martijn Stam. Obfuscation for cryptographic purposes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23 (1):121–168, January 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=1&spage=121.

Micciancio:2010:RGP

[350] Daniele Micciancio. The RSA group is pseudo-free. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(2):169–186, April 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=2&spage=169.

Morrissey:2010:THP

[351] P. Morrissey, N. P. Smart, and B. Warinschi. The TLS handshake protocol: a modular analysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(2):187–223, April 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=2&spage=187.

Freeman:2010:TPF

[352] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(2):224–280, April 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=2&spage=224.

Aumann:2010:SAC

[353] Yonatan Aumann and Yehuda Lindell. Security against covert adversaries: Efficient protocols for realistic adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(2):281–343, April 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=2&spage=281.

Beimel:2010:HSW

[354] Amos Beimel, Tal Malkin, Kobbi Nissim, and Enav Weinreb. How should we solve search problems privately? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23 (2):344–371, April 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=2&spage=344.

Aggarwal:2010:SCM

[355] Gagan Aggarwal, Nina Mishra, and Benny Pinkas. Secure computation of the median (and other elements of specified ranks). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(3):373–401, July 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=3&spage=373.

Katz:2010:PCS

[356] Jonathan Katz, Ji Sun Shin, and Adam Smith. Parallel and concurrent security of the HB and HB^+ protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(3):402–421, July 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=3&spage=402.

Hazay:2010:EPS

[357] Carmit Hazay and Yehuda Lindell. Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(3):422–456, July 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=3&spage=422.

Cheon:2010:DLP

[358] Jung Hee Cheon. Discrete logarithm problems with auxiliary inputs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(3):457–476, July 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=3&spage=457.

Konstantinou:2010:EGP

[359] Elisavet Konstantinou, Aristides Kontogeorgis, Yannis C. Stamatiou, and Christos Zaroliagis. On the efficient generation of prime-order elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(3):477–503, July 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=3&spage=477.

Biryukov:2010:SCS

[360] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(4):505–518, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=505.

Black:2010:ABB

[361] J. Black, P. Rogaway, T. Shrimpton, and M. Stam. An analysis of

the blockcipher–based hash functions from PGV. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23 (4):519–545, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=519`.

Groth:2010:VSS

[362] Jens Groth. A verifiable secret shuffle of homomorphic encryptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(4): 546–579, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=546`.

Barkol:2010:MSS

[363] Omer Barkol, Yuval Ishai, and Enav Weinreb. On d-multiplicative secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23(4): 580–593, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=580`.

Muller-Quade:2010:LTS

[364] Jörn Müller-Quade and Dominique Unruh. Long-term security and universal composability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 23 (4):594–671, October 2010. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=23&issue=4&spage=594`.

Indesteege:2011:PCE

[365] Sebastiaan Indesteege and Bart Preneel. Practical collisions for EnRUPT. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (1):1–23, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=1`.

Enge:2011:DLA

[366] Andreas Enge, Pierrick Gaudry, and Emmanuel Thomé. An $L(1/3)$ discrete logarithm algorithm for low degree curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (1):24–41, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=24`.

Abdalla:2011:WIB

[367] Michel Abdalla, James Birkett, Dario Catalano, Alexander W. Dent, John Malone-Lee, Gregory Neven, Jacob C. N. Schuldt, and Nigel P. Smart. Wildcarded identity-based encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24

(1):42–82, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=42.

Canetti:2011:UCS

[368] Ran Canetti and Jonathan Herzog. Universally composable symbolic security analysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (1):83–147, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=83.

Grassl:2011:CTZ

[369] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt. Cryptanalysis of the Tillich–Zémor hash function. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(1): 148–156, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=148.

Asharov:2011:UDC

[370] Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair rational secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (1):157–202, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=157.

Fischlin:2011:ENM

[371] Marc Fischlin and Roger Fischlin. Efficient non-malleable commitment schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(1): 203–244, January 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=1&spage=203.

Paar:2011:GE

[372] Christof Paar, Jean-Jacques Quisquater, and Berk Sunar. Guest editorial. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (2):245–246, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=245.

Canivet:2011:GLF

[373] G. Canivet, P. Maistri, R. Leveugle, J. Clédière, F. Valette, and M. Renaudin. Glitch and laser fault attacks onto a secure AES implementation on a SRAM-based FPGA. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(2):247–268, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.

asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=247.

Batina:2011:MIA

[374] Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. Mutual information analysis: a comprehensive study. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (2):269–291, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=269.

Nikova:2011:SHI

[375] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure hardware implementation of nonlinear functions in the presence of glitches. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(2):292–321, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=292.

Poschmann:2011:SCR

[376] Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-channel resistant crypto for less than 2,300 GE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (2):322–345, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=322.

Dominguez-Oviedo:2011:FBA

[377] Agustin Dominguez-Oviedo, M. Anwar Hasan, and Bijan Ansari. Fault-based attack on Montgomery's ladder algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(2):346–374, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=346.

Maiti:2011:IRO

[378] Abhranil Maiti and Patrick Schaumont. Improved ring oscillator PUF: An FPGA-friendly secure primitive. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24 (2):375–397, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=375.

Baudet:2011:SOB

[379] Mathieu Baudet, David Lubicz, Julien Micolod, and André Tassiaux. On the security of oscillator-based random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(2):398–425, April 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http:

//www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=2&spage=398.

Hell:2011:BSC

[380] Martin Hell and Thomas Johansson. Breaking the stream ciphers F-FCSR-H and F-FCSR-16 in real time. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):427–445, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=427.

Galbraith:2011:EFE

[381] Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):446–469, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=446.

Hofheinz:2011:PIR

[382] Dennis Hofheinz. Possibility and impossibility results for selective decommitments. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):470–516, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=470.

Kidron:2011:IRU

[383] Dafna Kidron and Yehuda Lindell. Impossibility results for universal composability in public-key models and with fixed inputs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):517–544, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=517.

Monnerat:2011:SUS

[384] Jean Monnerat and Serge Vaudenay. Short undeniable signatures based on group homomorphisms. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):545–587, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=545.

Liskov:2011:TBC

[385] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(3):588–613, July 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=3&spage=588.

Garay:2011:RFC

[386] Juan A. Garay, Philip MacKenzie, Manoj Prabhakaran, and Ke Yang.

Resource fairness and composability of cryptographic protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(4):615–658, October 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=4&spage=615.

Boneh:2011:ESI

[387] Dan Boneh and Xavier Boyen. Efficient selective identity-based encryption without random oracles. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(4):659–693, October 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=4&spage=659.

Hohenberger:2011:SOR

[388] Susan Hohenberger, Guy N. Rothblum, Abhi Shelat, and Vinod Vaikuntanathan. Securely obfuscating re-encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(4):694–719, October 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=4&spage=694.

Barak:2011:SCA

[389] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(4):720–760, October 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=4&spage=720.

Lindell:2011:AZK

[390] Yehuda Lindell and Hila Zarosim. Adaptive zero-knowledge proofs and adaptively secure oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 24(4):761–799, October 2011. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=24&issue=4&spage=761.

Jain:2012:RRP

[391] Rahul Jain. Resource requirements of private quantum channels and consequences for oblivious remote state preparation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):1–13, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=1.

Gordon:2012:PFS

[392] S. Dov Gordon and Jonathan Katz. Partial fairness in secure two-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25

(1):14–40, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=14.

Katz:2012:WLR

[393] Jonathan Katz. Which languages have 4-round zero-knowledge proofs? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):41–56, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=41.

Boldyreva:2012:SPS

[394] Alexandra Boldyreva, Adriana Palacio, and Bogdan Warinschi. Secure proxy signature schemes for delegation of signing rights. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):57–115, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=57.

Pietrzak:2012:PRC

[395] Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of computationally sound protocols revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):116–135, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=116.

Aerts:2012:PAK

[396] Wim Aerts, Eli Biham, Dieter De Moitié, Elke De Mulder, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, Bart Preneel, Guy A. E. Vandenbosch, and Ingrid Verbauwhede. A practical attack on KeeLoq. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):136–157, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=136.

Halevi:2012:SPH

[397] Shai Halevi and Yael Tauman Kalai. Smooth projective hashing and two-message oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(1):158–193, January 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=1&spage=158.

Cheon:2012:APR

[398] Jung Hee Cheon, Jin Hong, and Minkyu Kim. Accelerating Pollard's rho algorithm on finite fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(2):195–242, April 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http:

//www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=2&spage=195.

Ateniese:2012:PST

[399] Giuseppe Ateniese, Alfredo De Santis, Anna Lisa Ferrara, and Barbara Masucci. Provably-secure time-bound hierarchical key assignment schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (2):243–270, April 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=2&spage=243.

Hirose:2012:SVM

[400] Shoichi Hirose, Je Hong Park, and Aaram Yun. A simple variant of the Merkle–Damgård scheme with a permutation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (2):271–309, April 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=2&spage=271.

Roeder:2012:MVS

[401] Tom Roeder, Rafael Pass, and Fred B. Schneider. Multi-verifier signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (2):310–348, April 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=2&spage=310.

Minder:2012:ETA

[402] Lorenz Minder and Alistair Sinclair. The extended k-tree algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(2):349–382, April 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=2&spage=349.

Hazay:2012:ESO

[403] Carmit Hazay and Kobbi Nissim. Efficient set operations in the presence of malicious adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(3):383–433, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=383.

Farras:2012:IMS

[404] Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(3):434–463, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=434.

Smyshlyaev:2012:PBB

[405] Stanislav V. Smyshlyaev. Perfectly balanced Boolean functions and Golić Conjecture. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (3):464–483, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=464.

Hofheinz:2012:PHF

[406] Dennis Hofheinz and Eike Kiltz. Programmable hash functions and their applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (3):484–527, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=484.

Kawachi:2012:CIB

[407] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(3):528–555, July 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=3&spage=528.

Desmedt:2012:GCA

[408] Yvo Desmedt, Josef Pieprzyk, Ron Steinfeld, Xiaoming Sun, Christophe Tartary, Huaxiong Wang, and Andrew Chi-Chih Yao. Graph coloring applied to secure computation in non-Abelian groups. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25 (4):557–600, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=557.

Cash:2012:BTH

[409] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(4): 601–639, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=601.

Bellare:2012:LCH

[410] M. Bellare, A. Boldyreva, L. Knudsen, and C. Namprempre. On-line ciphers and the hash-CBC constructions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(4): 640–679, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=640.

Lindell:2012:STP

[411] Yehuda Lindell and Benny Pinkas. Secure Two–Party computation via cut-and-choose oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(4):680–722, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=680.

Camenisch:2012:BVS

[412] Jan Camenisch, Susan Hohenberger, and Michael Østergaard Pedersen. Batch verification of short signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(4):723–747, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=723.

Gauravaram:2012:SAR

[413] Praveen Gauravaram and Lars R. Knudsen. Security analysis of Randomize-Hash-then-Sign digital signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 25(4):748–779, October 2012. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://www.springerlink.com/openurl.asp?genre=article&issn=0933-2790&volume=25&issue=4&spage=748.

Pass:2013:PCP

[414] Rafael Pass, Alon Rosen, and Wei-Lung Dustin Tseng. Public-coin parallel zero–knowledge for NP. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):1–10, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9110-5.

Borghoff:2013:SSD

[415] Julia Borghoff, Lars R. Knudsen, Gregor Leander, and Søren S. Thomsen. Slender-set differential cryptanalysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):11–38, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9111-4.

Freeman:2013:MCL

[416] David Mandell Freeman, Oded Goldreich, Eike Kiltz, Alon Rosen, and Gil Segev. More constructions of lossy and correlation-secure trapdoor functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):39–74, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9112-3.

Ghodosi:2013:AUS

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

ogy: the journal of the International Association for Cryptologic Research, 26(1):75–79, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9113-2.

Fujisaki:2013:SIA

[418] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):80–101, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9114-1.

Hofheinz:2013:PCC

[419] Dennis Hofheinz, Eike Kiltz, and Victor Shoup. Practical chosen ciphertext secure encryption from factoring. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):102–118, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9115-0.

Joux:2013:ECD

[420] Antoine Joux and Vanessa Vitse. Elliptic curve discrete logarithm problem over small degree extension fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):119–143, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9116-z.

Bogdanov:2013:ILH

[421] Andrej Bogdanov and Alon Rosen. Input locality and hardness amplification. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26 (1):144–171, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-011-9117-y.

Isobe:2013:SKA

[422] Takanori Isobe. A single-key attack on the full GOST block cipher. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(1):172–189, January 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9118-5.

Katz:2013:PES

[423] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):191–224, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9119-4.

Jager:2013:ACA

[424] Tibor Jager and Jörg Schwenk. On the analysis of cryptographic assumptions in the generic ring model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):225–245, April 2013.

CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9120-y`.

Coron:2013:NBC

[425] Jean-Sébastien Coron, Alexey Kirichenko, and Mehdi Tibouchi. A note on the Bivariate Coppersmith Theorem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):246–250, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9121-x`.

Chase:2013:MCA

[426] Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, and Leonid Reyzin. Mercurial commitments with applications to zero-knowledge sets. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):251–279, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9122-9`.

Boyar:2013:LMT

[427] Joan Boyar, Philip Matthews, and René Peralta. Logic minimization techniques with applications to cryptology. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):280–312, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9124-7`.

Aumasson:2013:QLH

[428] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. QUARK: a lightweight hash. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):313–339, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9125-6`.

Lu:2013:SAS

[429] Steve Lu, Rafail Ostrovsky, Amit Sahai, Hovav Shacham, and Brent Waters. Sequential aggregate signatures, multisignatures, and verifiably encrypted signatures without random oracles. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(2):340–373, April 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9126-5`.

Hofheinz:2013:PRC

[430] Dennis Hofheinz, Dominique Unruh, and Jörn Müller-Quade. Polynomial runtime and composability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(3):375–441, July 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9127-4`.

Shacham:2013:CPR

[431] Hovav Shacham and Brent Waters. Compact proofs of retrievability. *Journal of Cryptology: the journal of the International Association for Cryptologic*

Research, 26(3):442–483, July 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9129-2.

Goldreich:2013:ETP

[432] Oded Goldreich and Ron D. Rothblum. Enhancements of trapdoor permutations. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(3):484–512, July 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9131-8.

Boyle:2013:FLR

[433] Elette Boyle, Gil Segev, and Daniel Wichs. Fully leakage-resilient signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(3): 513–558, July 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9136-3.

Hong:2013:CCT

[434] Jin Hong and Sunghwan Moon. A comparison of cryptanalytic tradeoff algorithms. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(4):559–637, October 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9128-3. See erratum [444].

Lindell:2013:NCR

[435] Yehuda Lindell. A note on constant-round zero-knowledge proofs of knowledge. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26 (4):638–654, October 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9132-7.

vanDijk:2013:FGS

[436] Marten van Dijk, Ari Juels, Alina Oprea, and Ronald L. Rivest. FlipIt: The game of “stealthy takeover”. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(4):655–713, October 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9134-5.

Katz:2013:ROP

[437] Jonathan Katz and Vinod Vaikuntanathan. Round-optimal password-based authenticated key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 26(4):714–743, October 2013. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-012-9133-6.

Stankovski:2014:ESR

[438] Paul Stankovski, Martin Hell, and Thomas Johansson. An efficient state recovery attack on the X-FCSR family of stream ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic*

Research, 27(1):1–22, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9130-9`.

Kiayias:2014:OTS

[439] Aggelos Kiayias, Yona Raekow, and Alexander Russell. A one-time stegosystem and applications to efficient covert communication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):23–44, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9135-4`.

Pass:2014:CZK

[440] Rafael Pass and Wei-Lung Dustin Tseng. Concurrent zero knowledge, revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):45–66, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9137-2`.

SenGupta:2014:NRS

[441] Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. (non-)random sequences from (non-)random permutations — analysis of RC4 stream cipher. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):67–108, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9138-1`.

Haitner:2014:NIH

[442] Iftach Haitner and Omer Reingold. A new interactive hashing theorem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):109–138, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9139-0`.

Birkett:2014:SMP

[443] James Birkett and Alexander W. Dent. Security models and proof strategies for plaintext-aware encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):139–180, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9141-6`.

Hong:2014:EBC

[444] Jin Hong and Sunghwan Moon. Erratum to: *A Comparison of Cryptanalytic Tradeoff Algorithms*. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(1):181, January 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9140-7`; `http://link.springer.com/content/pdf/10.1007/s00145-012-9140-7.pdf`. See [434].

Dinur:2014:IPA

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

of Cryptology: the journal of the International Association for Cryptologic Research, 27(2):183–209, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9142-5`.

Brakerski:2014:BSD

[446] Zvika Brakerski and Gil Segev. Better security for deterministic public-key encryption: The auxiliary-input setting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(2): 210–247, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9143-4`.

Longa:2014:FDG

[447] Patrick Longa and Francesco Sica. Four-dimensional Gallant–Lambert–Vanstone scalar multiplication. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(2):248–283, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-012-9144-3`.

Cramer:2014:ACZ

[448] Ronald Cramer, Ivan Damgård, and Marcel Keller. On the amortized complexity of zero-knowledge protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(2):284–316, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9145-x`.

Bitansky:2014:SSC

[449] Nir Bitansky and Ran Canetti. On strong simulation and composable point obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(2):317–357, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9146-9`.

Hazay:2014:CSP

[450] Carmit Hazay and Tomas Toft. Computationally secure pattern matching in the presence of malicious adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(2):358–395, April 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9147-8`.

Fischlin:2014:RMP

[451] Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3): 397–428, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9148-7`.

Applebaum:2014:KDM

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

tion and completeness. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3):429–451, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9149-6.

Khovratovich:2014:RRA

[453] Dmitry Khovratovich, Ivica Nikolić, and Christian Rechberger. Rotational rebound attacks on reduced Skein. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3):452–479, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9150-0.

Goldwasser:2014:BPO

[454] Shafi Goldwasser and Guy N. Rothblum. On best-possible obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3):480–505, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9151-z.

Groth:2014:CMS

[455] Jens Groth and Rafail Ostrovsky. Cryptography in the multi-string model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3):506–543, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9152-y.

Abdalla:2014:VRF

[456] Michel Abdalla, Dario Catalano, and Dario Fiore. Verifiable random functions: Relations to identity-based key encapsulation and new constructions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(3):544–593, July 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9153-x.

Faugere:2014:USI

[457] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(4):595–635, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9158-5.

Amir:2014:AAR

[458] Yair Amir, Paul Bunn, and Rafail Ostrovsky. Authenticated adversarial routing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(4):636–771, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9157-6.

Jean:2014:ICA

[459] Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin. Improved cryptanalysis of AES-like permutations. *Jour-*

nal of Cryptology: the journal of the International Association for Cryptologic Research, 27(4):772–798, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9156-7.

Bellare:2014:CCH

[460] Mihir Bellare and Todor Ristov. A characterization of chameleon hash functions and new, efficient designs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(4):799–823, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9155-8.

Dunkelman:2014:PTR

[461] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 27(4):824–849, October 2014. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9154-9.

Dunkelman:2015:SAE

[462] Orr Dunkelman, Nathan Keller, and Adi Shamir. Slidex attacks on the Even–Mansour encryption scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(1):1–28, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9164-7.

Bellare:2015:SDI

[463] Mihir Bellare, Dennis Hofheinz, and Eike Kiltz. Subtleties in the definition of IND–CCA: When and how should challenge decryption be disallowed? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(1):29–48, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9167-4.

Patra:2015:EAV

[464] Arpita Patra, Ashish Choudhury, and C. Pandu Rangan. Efficient asynchronous verifiable secret sharing and multiparty computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(1):49–109, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9172-7.

Biham:2015:CSR

[465] Eli Biham, Rafi Chen, and Antoine Joux. Cryptanalysis of SHA-0 and reduced SHA-1. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(1):110–160, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9179-8.

Baumeler:2015:QPI

[466] Ämin Baumeler and Anne Broadbent. Quantum private information retrieval has linear communication complexity. *Journal of Cryp-*

tology: the journal of the International Association for Cryptologic Research, 28(1):161–175, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9180-2.

Bohl:2015:CGN

[467] Florian Böhl, Dennis Hofheinz, Tibor Jager, Jessica Koch, and Christoph Striecks. Confined guessing: New signatures from standard assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(1):176–208, January 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9183-z.

Biham:2015:NAI

[468] Eli Biham, Orr Dunkelman, Nathan Keller, and Adi Shamir. New attacks on IDEA with at least 6 rounds. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):209–239, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9162-9.

Sajadieh:2015:ERD

[469] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, and Pouyan Sepehrdad. Efficient recursive diffusion layers for block ciphers and hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):240–256, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9163-8.

Lamberger:2015:RAS

[470] Mario Lamberger, Florian Mendel, Martin Schläffer, Christian Rechberger, and Vincent Rijmen. The rebound attack and subspace distinguishers: Application to Whirlpool. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):257–296, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9166-5.

Berman:2015:NAA

[471] Itay Berman and Iftach Haitner. From non-adaptive to adaptive pseudorandom functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):297–311, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-013-9169-2.

Lindell:2015:EPS

[472] Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):312–350, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9177-x.

Ahn:2015:CAD

[473] Jae Hyun Ahn, Dan Boneh, Jan Camenisch, Susan Hohenberger, Abhi Shelat, and Brent Waters. Computing on authenticated data. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(2):351–395, April 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-014-9182-0`.

Dunkelman:2015:ISK

[474] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):397–422, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9159-4`.

Hofheinz:2015:GNU

[475] Dennis Hofheinz and Victor Shoup. GNUC: A new universal composability framework. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):423–508, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9160-y`.

Miles:2015:CCP

[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 International Association for Cryptologic Research*, 28(3):509–532, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9161-x`.

Malka:2015:HAP

[477] Lior Malka. How to achieve perfect simulation and a complete problem for non-interactive perfect zero-knowledge. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):533–550, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9165-6`.

Beimel:2015:PMC

[478] Amos Beimel, Eran Omri, and Ilan Orlov. Protocols for multiparty coin toss with a dishonest majority. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):551–600, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9168-3`.

Tsaban:2015:PTS

[479] Boaz Tsaban. Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):601–622, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9170-9`.

Berman:2015:PUA

[480] Ron Berman, Amos Fiat, Marcin Gomulkiewicz, and Marek Klonowski. Provable unlinkability against traffic analysis with low message overhead. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):623–640, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9171-8`.

Schage:2015:TSS

[481] Sven Schäge. Tight security for signature schemes without random oracles. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):641–670, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9173-6`.

Fuller:2015:UAD

[482] Benjamin Fuller, Adam O'Neill, and Leonid Reyzin. A unified approach to deterministic encryption: New constructions and a connection to computational entropy. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):671–717, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9174-5`.

Soleimany:2015:RCP

[483] Hadi Soleimany, Céline Blondeau, Xiaoli Yu, and Wenling Wu. Reflection cryptanalysis of PRINCE-like ciphers. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(3):718–744, July 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9175-4`.

Chandran:2015:AES

[484] Nishanth Chandran, Juan A. Garay, and Rafail Ostrovsky. Almost-everywhere secure computation with edge corruptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28 (4):745–768, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-013-9176-3`.

Procter:2015:WKF

[485] Gordon Procter and Carlos Cid. On weak keys and forgery attacks against polynomial-based MAC schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(4):769–795, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/article/10.1007/s00145-014-9178-9`.

Aspnes:2015:SAQ

[486] James Aspnes, Zoë Diamadi, Aleksandr Yampolskiy, and Kristian Gjøsteen. Spreading alerts quietly and the subgroup escape problem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(4):796–819, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL

http://link.springer.com/article/10.1007/s00145-014-9181-1.

Gentry:2015:UFH

[487] Craig Gentry, Jens Groth, Yuval Ishai, Chris Peikert, and Amit Sahai. Using fully homomorphic hybrid encryption to minimize non-interactive zero-knowledge proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(4):820–843, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9184-y.

Bellare:2015:NPN

[488] Mihir Bellare. New proofs for NMAC and HMAC: Security without collision resistance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(4):844–878, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9185-x.

Peyrin:2015:CAG

[489] Thomas Peyrin. Collision attack on Grindahl. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 28(4):879–898, October 2015. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9186-9.

Baldi:2016:EPK

[490] Marco Baldi, Marco Bianchi, Franco Chiaraluce, and Joachim Rosenthal. Enhanced public key security for the McEliece cryptosystem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):1–27, January 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9187-8.

Bos:2016:FCG

[491] Joppe W. Bos, Craig Costello, Huseyin Hisil, and Kristin Lauter. Fast cryptography in genus 2. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):28–60, January 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9188-7.

Coron:2016:HBI

[492] Jean-Sébastien Coron, Thomas Holenstein, and Robin Künzler. How to build an ideal cipher: The indifferentiability of the Feistel construction. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):61–114, January 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9189-6.

Freedman:2016:ESI

[493] Michael J. Freedman, Carmit Hazay, Kobbi Nissim, and Benny Pinkas. Efficient set intersection with simulation-based security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):115–155, January 2016. CODEN JOCREQ. ISSN 0933-2790

(print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9190-0.

Yao:2016:CKE

[494] Andrew Chi-Chih Yao, Moti Yung, and Yunlei Zhao. Concurrent knowledge extraction in public-key models. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):156–219, January 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9191-z.

Brown:2016:BRM

[495] Daniel R. L. Brown. Breaking RSA may be as difficult as factoring. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(1):220–241, January 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9192-y.

Gennaro:2016:AET

[496] Rosario Gennaro, Carmit Hazay, and Jeffrey S. Sorensen. Automata evaluation and text search protocols with simulation-based security. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):243–282, April 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9193-x.

Haitner:2016:LUR

[497] Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness of random oracles. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):283–335, April 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9194-9.

Beimel:2016:SSS

[498] Amos Beimel, Oriol Farràs, and Yuval Mintz. Secret-sharing schemes for very dense graphs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):336–362, April 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9195-8.

Abe:2016:SPS

[499] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):363–421, April 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-014-9196-7.

Faust:2016:SSS

[500] Sebastian Faust, Carmit Hazay, Jesper Buus Nielsen, Peter Sebastian Nordholt, and Angela Zottarel. Signature schemes secure against hard-to-invert leakage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):422–455, April 2016. CO-

DEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9197-1.

Lindell:2016:FCC

[501] Yehuda Lindell. Fast cut-and-choose-based protocols for malicious and covert adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(2):456–490, April 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9198-0.

Moran:2016:OFC

[502] Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):491–513, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9199-z.

Hazay:2016:LRC

[503] Carmit Hazay, Adriana López-Alt, Hoeteck Wee, and Daniel Wichs. Leakage-resilient cryptography from minimal assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):514–551, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9200-x.

Applebaum:2016:GXG

[504] Benny Applebaum. Garbling XOR gates "for free" in the standard model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):552–576, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9201-9.

Applebaum:2016:DLS

[505] Benny Applebaum, Andrej Bogdanov, and Alon Rosen. A dichotomy for local small-bias generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):577–596, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9202-8.

Abdalla:2016:TSS

[506] Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi. Tightly secure signatures from lossy identification schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):597–631, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/article/10.1007/s00145-015-9203-7.

Coron:2016:PCI

[507] Jean-Sébastien Coron, David Naccache, Mehdi Tibouchi, and Ralf-Philipp Weinmann. Practical cryptanalysis of ISO 9796-2 and EMV signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(3):632–656, July 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL

http://link.springer.com/article/10.1007/s00145-015-9205-5.

Andreeva:2016:NSP

[508] Elena Andreeva, Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, Jonathan Hoch, John Kelsey, Adi Shamir, and Sébastien Zimmer. New second-preimage attacks on hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):657–696, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9206-4; http://link.springer.com/article/10.1007/s00145-015-9206-4.

Dinur:2016:KRA

[509] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key recovery attacks on iterated Even–Mansour encryption schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):697–728, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9207-3; http://link.springer.com/article/10.1007/s00145-015-9207-3.

Boyen:2016:UAR

[510] Xavier Boyen. Unconditionally anonymous ring and mesh signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):729–774, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9208-2; http://link.springer.com/article/10.1007/s00145-015-9208-2.

Biham:2016:BA

[511] Eli Biham, Yaniv Carmeli, and Adi Shamir. Bug attacks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):775–805, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9209-1; http://link.springer.com/article/10.1007/s00145-015-9209-1.

Smith:2016:CCE

[512] Benjamin Smith. The $\mathbf{Q}$-curve construction for endomorphism-accelerated elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):806–832, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9210-8; http://link.springer.com/article/10.1007/s00145-015-9210-8.

Abe:2016:CSS

[513] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):833–

878, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9211-7; http://link.springer.com/article/10.1007/s00145-015-9211-7.

Asharov:2016:TGT

[514] Gilad Asharov, Ran Canetti, and Carmit Hazay. Toward a game theoretic view of secure computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):879–926, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9212-6; http://link.springer.com/article/10.1007/s00145-015-9212-6.

Landelle:2016:CFR

[515] Franck Landelle and Thomas Peyrin. Cryptanalysis of full RIPEMD-128. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 29(4):927–951, October 2016. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9213-5; http://link.springer.com/article/10.1007/s00145-015-9213-5.

Winter:2017:WLC

[516] Andreas Winter. Weak locking capacity of quantum channels can be much larger than private capacity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):1–21, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9215-3; http://link.springer.com/article/10.1007/s00145-015-9215-3.

Cash:2017:DPR

[517] David Cash, Alptekin Küpçü, and Daniel Wichs. Dynamic proofs of retrievability via oblivious RAM. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):22–57, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9216-2; http://link.springer.com/article/10.1007/s00145-015-9216-2.

Asharov:2017:FPB

[518] Gilad Asharov and Yehuda Lindell. A full proof of the BGW protocol for perfectly secure multiparty computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):58–151, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9214-4; http://link.springer.com/article/10.1007/s00145-015-9214-4.

Damgaard:2017:BTR

[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

International Association for Cryptologic Research, 30(1):152–190, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9218-0`; `http://link.springer.com/article/10.1007/s00145-015-9218-0`.

Cheraghchi:2017:NMC

[520] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):191–241, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9219-z`; `http://link.springer.com/article/10.1007/s00145-015-9219-z`.

Escala:2017:AFD

[521] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie–Hellman assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):242–288, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9220-6`; `http://link.springer.com/article/10.1007/s00145-015-9220-6`.

Brakerski:2017:OC

[522] Zvika Brakerski and Guy N. Rothblum. Obfuscating conjunctions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):289–320, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9221-5`; `http://link.springer.com/article/10.1007/s00145-015-9221-5`.

Hazay:2017:EOS

[523] Carmit Hazay and Arpita Patra. Efficient one-sided adaptively secure computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(1):321–371, January 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9222-4`; `http://link.springer.com/article/10.1007/s00145-015-9222-4`.

Homma:2017:DMV

[524] Naofumi Homma, Yu ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, and Takafumi Aoki. Design methodology and validity verification for a reactive countermeasure against EM attacks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):373–391, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-015-9223-3`; `http://link.springer.com/article/10.1007/s00145-015-9223-3`.

Genkin:2017:AC

[525] Daniel Genkin, Adi Shamir, and Eran

Tromer. Acoustic cryptanalysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):392–443, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9224-2; http://link.springer.com/article/10.1007/s00145-015-9224-2.

Komargodski:2017:SSN

[526] Ilan Komargodski, Moni Naor, and Eylon Yogev. Secret-sharing for NP. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):444–469, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9226-0; http://link.springer.com/article/10.1007/s00145-015-9226-0.

Schroder:2017:SBS

[527] Dominique Schröder and Dominique Unruh. Security of blind signatures revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):470–494, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-015-9225-1; http://link.springer.com/article/10.1007/s00145-015-9225-1.

Lee:2017:STD

[528] Jooyoung Lee, Martijn Stam, and John Steinberger. The security of Tandem–DM in the ideal cipher model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):495–518, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-016-9230-z; http://link.springer.com/article/10.1007/s00145-016-9230-z.

Benhamouda:2017:ECP

[529] Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert. Efficient cryptosystems from $\mathbf{2^{\vec{k}}}$-th power residue symbols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):519–549, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-016-9229-5; http://link.springer.com/article/10.1007/s00145-016-9229-5.

Tajik:2017:PSC

[530] Shahin Tajik, Enrico Dietz, Sven Frohmann, Helmar Dittrich, Dmitry Nedospasov, Clemens Helfmeier, Jean-Pierre Seifert, Christian Boit, and Heinz-Wilhelm Hübers. Photonic side-channel analysis of arbiter PUFs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):550–571, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s00145-016-9228-6; http://link.springer.com/article/10.1007/s00145-016-9228-6.

Hisil:2017:JCG

[531] Huseyin Hisil and Craig Costello. Jacobian coordinates on genus 2 curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(2):572–600, April 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s00145-016-9227-7; http://link.springer.com/article/10.1007/s00145-016-9227-7`.

Prabhakaran:2017:RNM

[532] Manoj Prabhakaran and Mike Rosulek. Reconciling non-malleability with homomorphic encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):601–671, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Applebaum:2017:LCU

[533] Benny Applebaum and Yoni Moses. Locally computable UOWHF with linear shrinkage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3): 672–698, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). See correction [712].

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

Seo:2017:SSD

[535] Jae Hong Seo. Short signatures from Diffie–Hellman: Realizing almost compact public key. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3): 735–759, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Lenstra:2017:LS

[536] H. W. Lenstra, Jr. and A. Silverberg. Lattices with symmetry. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):760–804, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Asharov:2017:MEO

[537] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer extensions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):805–858, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Blondeau:2017:DLC

[538] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. Differential–linear cryptanalysis revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):859–888, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Kiltz:2017:IRO

[539] Eike Kiltz, Adam O'Neill, and Adam Smith. Instantiability of RSA–OAEP under chosen–plaintext attack. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):889–919, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Todo:2017:ICF

[540] Yosuke Todo. Integral cryptanalysis on full MISTY1. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(3):920–959, July 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

Applebaum:2017:PSM

[541] Benny Applebaum and Pavel Raykov. From private simultaneous messages to zero–information Arthur–Merlin protocols and back. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):961–988, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9239-3`.

Bitansky:2017:HS

[542] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Shafi Goldwasser, Huijia Lin, Aviad Rubinstein, and Eran Tromer. The hunting of the SNARK. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):989–1066, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9241-9`.

Jakobsen:2017:ITC

[543] Sune K. Jakobsen. Information theoretical cryptogenography. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1067–1115, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9242-8`; `https://link.springer.com/content/pdf/10.1007/s00145-016-9242-8.pdf`.

Jutla:2017:SQA

[544] Charanjit S. Jutla and Arnab Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1116–1156, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9243-7`.

Cohen:2017:FVG

[545] Ran Cohen and Yehuda Lindell. Fairness versus guaranteed output delivery in secure multiparty computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1157–1186, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9245-5`.

Hajiabadi:2017:RCS

[546] Mohammad Hajiabadi and Bruce M. Kapron. Reproducible circularly secure bit encryption: Applications and realizations. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1187–1237, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9246-4`.

Kiltz:2017:EAH

[547] Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi, David Cash, and Abhishek Jain. Efficient authentication from hard learning problems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1238–1275, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9247-3`.

Jager:2017:ACC

[548] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. Authenticated confidential channel establishment and the security of TLS–DHE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 30(4):1276–1324, October 2017. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9248-2`.

Applebaum:2018:MLO

[549] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Minimizing locality of one-way functions via semi-private randomized encodings. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):1–22, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9244-6`.

Catalano:2018:PHM

[550] Dario Catalano and Dario Fiore. Practical homomorphic message authenticators for arithmetic circuits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):23–59, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9249-1`.

Komargodski:2018:FER

[551] Ilan Komargodski, Gil Segev, and Eylon Yogev. Functional encryption for randomized functionalities in the private-key setting from minimal assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):60–100, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-016-9250-8`.

Boura:2018:MIP

[552] Christina Boura, Virginie Lallemand,

María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):101–133, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-016-9251-7.

Mironov:2018:IDP

[553] Ilya Mironov, Omkant Pandey, Omer Reingold, and Gil Segev. Incremental deterministic public-key encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):134–161, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9252-1.

Gilboa:2018:HMQ

[554] Shoni Gilboa, Shay Gueron, and Ben Morris. How many queries are needed to distinguish a truncated random permutation from a random function? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):162–171, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9253-0.

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 Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):172–201, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9254-z.

Brakerski:2018:FPF

[556] Zvika Brakerski and Gil Segev. Function-private functional encryption in the private–key setting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):202–225, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9255-y.

Fujisaki:2018:AME

[557] Eiichiro Fujisaki. All-but-many encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):226–275, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9256-x.

Kakvi:2018:OSP

[558] Saqib A. Kakvi and Eike Kiltz. Optimal security proofs for full domain hash, revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(1):276–306, January 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/

article/10.1007/s00145-017-9257-9.

Abdalla:2018:RE

[559] Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):307–350, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9258-8.

Bruneau:2018:MHO

[560] Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Teglia. Multivariate high-order attacks of shuffled tables recomputation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):351–393, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9259-7.

Zhang:2018:PCB

[561] Bin Zhang, Chao Xu, and Dengguo Feng. Practical cryptanalysis of Bluetooth encryption with condition masking. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):394–433, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9260-1.

Brakerski:2018:MIF

[562] Zvika Brakerski, Ilan Komargodski, and Gil Segev. Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):434–520, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9261-0.

Morris:2018:DET

[563] Ben Morris, Phillip Rogaway, and Till Stegers. Deterministic encryption with the Thorp shuffle. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):521–536, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9262-z.

Hazay:2018:OPE

[564] Carmit Hazay. Oblivious polynomial evaluation and secure set-intersection from algebraic PRFs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):537–586, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9263-y.

Cohen:2018:CSM

[565] Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem. Charac-

terization of secure multiparty computation without broadcast. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):587–609, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9264-x`.

Bai:2018:ISP

[566] Shi Bai, Tancrède Lepoint, Adeline Roux-Langlois, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(2):610–640, April 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9265-9`.

Bar-On:2018:ESA

[567] Achiya Bar-On, Eli Biham, Orr Dunkelman, and Nathan Keller. Efficient slide attacks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3): 641–670, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9266-8`.

Lindell:2018:CST

[568] Yehuda Lindell, Eran Omri, and Hila Zarosim. Completeness for symmetric two-party functionalities: Revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):671–697, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9267-7`.

Asharov:2018:COW

[569] Gilad Asharov and Gil Segev. On constructing one-way permutations from indistinguishability obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):698–736, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9268-6`.

Lindell:2018:FEO

[570] Yehuda Lindell and Hila Zarosim. On the feasibility of extending oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3): 737–773, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-017-9269-5`.

Lyubashevsky:2018:AEL

[571] Vadim Lyubashevsky and Daniele Micciancio. Asymptotically efficient lattice-based digital signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):774–797, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/`

article/10.1007/s00145-017-9270-z.

Gueron:2018:FGC

[572] Shay Gueron, Yehuda Lindell, Ariel Nof, and Benny Pinkas. Fast garbling of circuits under standard assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):798–844, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9271-y.

Minaud:2018:KRA

[573] Brice Minaud, Patrick Derbez, Pierre-Alain Fouque, and Pierre Karpman. Key-recovery attacks on ASASA. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):845–884, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9272-x.

Canteaut:2018:SCP

[574] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(3):885–916, July 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9273-9.

Abdalla:2018:RKS

[575] Michel Abdalla, Fabrice Benhamouda, Alain Passelègue, and Kenneth G. Paterson. Related-key security for pseudorandom functions beyond the linear barrier. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):917–964, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9274-8.

Unruh:2018:EMP

[576] Dominique Unruh. Everlasting multi-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):965–1011, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9278-z; https://link.springer.com/content/pdf/10.1007/s00145-018-9278-z.pdf.

Raghunathan:2018:DPK

[577] Ananth Raghunathan, Gil Segev, and Salil Vadhan. Deterministic public-key encryption for adaptively-chosen plaintext distributions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):1012–1063, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9287-y.

Chen:2018:MTR

[578] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John Steinberger. Minimizing the two-round even-Mansour cipher. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):1064–1119, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9295-y`.

Hofheinz:2018:IPE

[579] Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. On the (im-)possibility of extending coin toss. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):1120–1163, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9296-x`; `https://link.springer.com/content/pdf/10.1007/s00145-018-9296-x.pdf`.

Hutter:2018:FMP

[580] Michael Hutter and Erich Wenger. Fast multi-precision multiplication for public-key cryptography on embedded microprocessors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 31(4):1164–1182, October 2018. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9298-8`.

Hermelin:2019:MLC

[581] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional linear cryptanalysis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(1):1–34, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9308-x`; `https://link.springer.com/content/pdf/10.1007/s00145-018-9308-x.pdf`.

Bai:2019:ICA

[582] Shi Bai, Steven D. Galbraith, Liangze Li, and Daniel Sheffield. Improved combinatorial algorithms for the inhomogeneous short integer solution problem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(1):35–83, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9304-1`.

Abdalla:2019:TFS

[583] Michel Abdalla, Fabrice Benhamouda, and David Pointcheval. On the tightness of forward-secure signature reductions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(1):84–150, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9283-2`.

Duc:2019:ULM

[584] Alexandre Duc, Stefan Dziembowski,

and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32 (1):151–177, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9284-1; https://link.springer.com/content/pdf/10.1007/s00145-018-9284-1.pdf.

Kiyoshima:2019:REB

[585] Susumu Kiyoshima. Round-efficient black-box construction of composable multi-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(1):178–238, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9276-1.

Abe:2019:ISP

[586] Masayuki Abe, Jan Camenisch, Rafael Dowsley, and Maria Dubovitskaya. On the impossibility of structure-preserving deterministic primitives. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(1):239–264, January 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9292-1.

Hazay:2019:ERK

[587] Carmit Hazay, Gert Læssøe Mikkelsen, Tal Rabin, Tomas Toft, and Angelo Agatino Nicolosi. Efficient RSA key generation and threshold Paillier in the two-party setting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):265–323, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-017-9275-7.

Barthe:2019:AAC

[588] Gilles Barthe, Edvard Fagerholm, Dario Fiore, John Mitchell, Andre Scedrov, and Benedikt Schmidt. Automated analysis of cryptographic assumptions in generic group models. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):324–360, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9302-3.

Berman:2019:HPR

[589] Itay Berman, Iftach Haitner, Ilan Komargodski, and Moni Naor. Hardness-preserving reductions via cuckoo hashing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):361–392, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9293-0.

Kiyoshima:2019:NBB

[590] Susumu Kiyoshima. Non-black-box simulation in the fully concurrent setting, revisited. *Journal of Cryptology: the journal of the Interna-*

tional Association for Cryptologic Research, 32(2):393–434, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-09309-5.

Bernard:2019:PSM

[591] Florent Bernard, Patrick Haddad, Viktor Fischer, and Jean Nicolai. From physical to stochastic modeling of a TERO-based TRNG. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):435–458, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9291-2; https://link.springer.com/content/pdf/10.1007/s00145-018-9291-2.pdf.

Choi:2019:EUC

[592] Seung Geol Choi, Jonathan Katz, Dominique Schrögder, Arkady Yerukhimovich, and Hong-Sheng Zhou. (Efficient) universally composable oblivious transfer using a minimal number of stateless tokens. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):459–497, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9288-x.

Fuchsbauer:2019:SPS

[593] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):498–546, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9281-4.

Cheon:2019:CCM

[594] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the CLT13 multilinear map. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):547–565, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9307-y; https://link.springer.com/content/pdf/10.1007/s00145-018-9307-y.pdf.

Fleischhacker:2019:TSP

[595] Nils Fleischhacker, Tibor Jager, and Dominique Schröder. On tight security proofs for Schnorr signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(2):566–599, April 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09311-5.

Brassard:2019:KEM

[596] Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail. Key establishment à la Merkle in a quantum world. *Journal of Cryptology: the journal of the International Association for Cryptologic*

Research, 32(3):601–634, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09317-z`; `https://link.springer.com/content/pdf/10.1007/s00145-019-09317-z.pdf`.

Hazay:2019:BBC

[597] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. On black-box complexity of universally composable security in the CRS model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):635–689, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09326-y`.

Cohen:2019:PTC

[598] Ran Cohen, Sandro Coretti, Juan Garay, and Vassilis Zikas. Probabilistic termination and composability of cryptographic protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):690–741, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9279-y`.

Dachman-Soled:2019:LRP

[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 Cryptologic Research*, 32(3):742–824, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9286-z`.

Zhandry:2019:ME

[600] Mark Zhandry. The magic of ELFs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):825–866, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9289-9`.

Oliveira:2019:KCQ

[601] Thomaz Oliveira, Julio López, Daniel Cervantes-Vázquez, and Francisco Rodríguez-Henríquez. Koblitz curves over quadratic fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):867–894, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9294-z`.

Jovanovic:2019:BCS

[602] Philipp Jovanovic, Atul Luykx, Bart Mennink, Yu Sasaki, and Kan Yasuda. Beyond conventional security in sponge-based authenticated encryption modes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):895–940, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.`

1007/s00145-018-9299-7; https://link.springer.com/content/pdf/10.1007/s00145-018-9299-7.pdf.

Dachman-Soled:2019:ONR

[603] Dana Dachman-Soled, Chang Liu, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin. Oblivious network RAM and leveraging parallelism to achieve obliviousness. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):941–972, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9301-4.

Abe:2019:EFS

[604] Masayuki Abe, Jens Groth, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Efficient fully structure-preserving signatures and shrinking commitments. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):973–1025, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9300-5.

Lindell:2019:ECR

[605] Yehuda Lindell, Benny Pinkas, Nigel P. Smart, and Avishay Yanai. Efficient constant-round multi-party computation combining BMR and SPDZ. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(3):1026–1069, July 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09322-2.

Lacerda:2019:CLR

[606] Felipe G. Lacerda, Joseph M. Renes, and Renato Renner. Classical leakage resilience from fault-tolerant quantum computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1071–1094, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09310-6.

Bock:2019:WBC

[607] Estuardo Alpirez Bock, Joppe W. Bos, Chris Brzuska, Charles Hubain, Wil Michiels, Cristofaro Mune, Eloi Sanfelix Gonzalez, Philippe Teuwen, and Alexander Treff. White-box cryptography: Don't forget about grey-box attacks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1095–1143, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09315-1.

Hazay:2019:CRM

[608] Carmit Hazay and Avishay Yanai. Constant-round maliciously secure two-party computation in the RAM model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1144–1199, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (elec-

tronic). URL `https://link.springer.com/article/10.1007/s00145-019-09321-3`.

Hazay:2019:WSC

[609] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. What security can we achieve within 4 rounds? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1200–1262, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09323-1`.

Duc:2019:MMS

[610] Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete (or how to evaluate the security of any leaking device), extended version. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1263–1297, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9277-0`.

Barbulescu:2019:UKS

[611] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1298–1336, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9280-5`.

Takayasu:2019:SCE

[612] Atsushi Takayasu, Yao Lu, and Liqiang Peng. Small CRT-exponent RSA revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1337–1382, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9282-3`.

Todo:2019:NIA

[613] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM, and Midori64. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1383–1422, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9285-0`.

Chaigneau:2019:CNV

[614] Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jérémy Jean, and Jean-René Reinhard. Cryptanalysis of NORX v2.0. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1423–1447, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-018-9297-9`.

Dinur:2019:EDB

[615] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Efficient dissection of bicomposite problems with

cryptanalytic applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4):1448–1490, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9303-2.

Okamoto:2019:FSF

[616] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with a large class of relations from the decisional linear assumption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 32(4): 1491–1573, October 2019. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9305-0; https://link.springer.com/content/pdf/10.1007/s00145-018-9305-0.pdf.

Guo:2020:SLU

[617] Qian Guo, Thomas Johansson, and Carl Löndahl. Solving LPN using covering codes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):1–33, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09338-8; https://link.springer.com/content/pdf/10.1007/s00145-019-09338-8.pdf.

Chillotti:2020:TFF

[618] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):34–91, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09319-x.

Karati:2020:KGO

[619] Sabyasachi Karati and Palash Sarkar. Kummer for genus one over prime-order fields. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):92–129, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09320-4.

Galbraith:2020:IPS

[620] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1): 130–175, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09316-0; https://link.springer.com/content/pdf/10.1007/s00145-019-09316-0.pdf.

Akavia:2020:THC

[621] Adi Akavia, Rio LaVigne, and Tal Moran. Topology-hiding computation on all graphs. *Journal of Cryp-*

tology: the journal of the International Association for Cryptologic Research*, 33(1):176–227, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09318-y.

Guo:2020:PCA

[622] Jian Guo, Guohong Liao, Guozhen Liu, Meicheng Liu, Kexin Qiao, and Ling Song. Practical collision attacks against round-reduced SHA-3. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):228–270, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09313-3.

Hazay:2020:PST

[623] Carmit Hazay and Muthuramakrishnan Venkitasubramaniam. On the power of secure two-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):271–318, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09314-2.

Dachman-Soled:2020:LDU

[624] Dana Dachman-Soled, Feng-Hao Liu, Elaine Shi, and Hong-Sheng Zhou. Locally decodable and updatable non-malleable codes and their applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(1):319–355, January 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-018-9306-z.

Bitansky:2020:COT

[625] Nir Bitansky, Ryo Nishimaki, Alain Passelègue, and Daniel Wichs. From cryptomania to obfustopia through secret-key functional encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):357–405, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09337-9.

Komargodski:2020:MOP

[626] Ilan Komargodski and Gil Segev. From minicrypt to obfustopia via private-key functional encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):406–458, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09327-x.

Bitansky:2020:VRF

[627] Nir Bitansky. Verifiable random functions from non-interactive witness-indistinguishable proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):459–493, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/

article/10.1007/s00145-019-09331-1.

Basin:2020:CGB

[628] David A. Basin, Andreas Lochbihler, and S. Reza Sefidgar. CryptHOL: Game-based proofs in higher-order logic. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):494–566, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09341-z.

Ashur:2020:RWK

[629] Tomer Ashur, Tim Beyne, and Vincent Rijmen. Revisiting the wrong-key-randomization hypothesis. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):567–594, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09343-2.

Dachman-Soled:2020:FIS

[630] Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya, and Dominique Schröder. Feasibility and infeasibility of secure computation with malicious PUFs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(2):595–617, April 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09329-9.

Kim:2020:MTP

[631] Sam Kim and David J. Wu. Multi-theorem preprocessing NIZKs from lattices. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):619–702, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09324-0.

Chakraborti:2020:BBA

[632] Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi. Blockcipher-based authenticated encryption: How small can we go? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):703–741, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09325-z.

Bao:2020:GAH

[633] Zhenzhen Bao, Itai Dinur, Jian Guo, Gaëtan Leurent, and Lei Wang. Generic attacks on hash combiners. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):742–823, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09328-w.

Dinur:2020:ODD

[634] Itai Dinur, Nathan Keller, and Ohad Klein. An optimal distributed discrete log protocol with applications to

homomorphic secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):824–873, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09330-2`.

Dinur:2020:CTM

[635] Itai Dinur. Cryptanalytic time–memory–data trade-offs for FX-constructions and the affine equivalence problem. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):874–909, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09332-0`.

Dunkelman:2020:PFA

[636] Orr Dunkelman, Nathan Keller, Eran Lambooij, and Yu Sasaki. A practical forgery attack on Lilliput–AE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):910–916, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09333-z`.

Applebaum:2020:CCP

[637] Benny Applebaum, Thomas Holenstein, Manoj Mishra, and Ofer Shayevitz. The communication complexity of private simultaneous messages, revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):917–953, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09334-y`.

Kowalczyk:2020:CAS

[638] Lucas Kowalczyk and Hoeteck Wee. Compact adaptively secure ABE for NC^1 from k-Lin. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):954–1002, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09335-x`.

Bar-On:2020:IKR

[639] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1003–1043, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-019-09336-w`.

Kanukurthi:2020:FSN

[640] Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Four-state non-malleable codes with explicit constant rate. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1044–1079, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

URL https://link.springer.com/article/10.1007/s00145-019-09339-7.

Albrecht:2020:MMO

[641] Martin R. Albrecht, Pooya Farshim, Shuai Han, Dennis Hofheinz, Enrique Larraia, and Kenneth G. Paterson. Multilinear maps from obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1080–1113, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09340-0; https://link.springer.com/content/pdf/10.1007/s00145-019-09340-0.pdf.

Wegener:2020:SMR

[642] Felix Wegener, Lauren De Meyer, and Amir Moradi. Spin me right round rotational symmetry for FPGA-specific AES: Extended version. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1114–1155, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-019-09342-y; https://link.springer.com/content/pdf/10.1007/s00145-019-09342-y.pdf.

Beyne:2020:BCI

[643] Tim Beyne. Block cipher invariants as eigenvectors of correlation matrices. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1156–1183, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09344-1.

Derbez:2020:MMA

[644] Patrick Derbez and Léo Perrin. Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1184–1215, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09345-0.

Alhassan:2020:ESU

[645] Masaud Y. Alhassan, Daniel Günther, Ágnes Kiss, and Thomas Schneider. Efficient and scalable universal circuits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33 (3):1216–1271, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09346-z; https://link.springer.com/content/pdf/10.1007/s00145-020-09346-z.pdf.

Jha:2020:TSC

[646] Ashwin Jha and Mridul Nandi. Tight security of cascaded LRW2. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1272–1317, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09347-y.

Kiyoshima:2020:SCN

[647] Susumu Kiyoshima. Statistical concurrent non-malleable zero-knowledge from one-way functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1318–1361, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09348-x`.

Bunn:2020:OSA

[648] Paul Bunn and Rafail Ostrovsky. Oblivious sampling with applications to two-party k-means clustering. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(3):1362–1403, July 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09349-w`.

Libert:2020:ASN

[649] Benoît Libert and Moti Yung. Adaptively secure non-interactive CCA-Secure threshold cryptosystems: Generic framework and constructions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1405–1441, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09350-3`.

Hutter:2020:FMP

[650] Michael Hutter and Erich Wenger. Fast multi-precision multiplication for public-key cryptography on embedded microprocessors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1442–1460, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09351-2`.

Kusters:2020:IMS

[651] Ralf Küsters, Max Tuengerthal, and Daniel Rausch. The IITM model: A simple and expressive model for universal composability. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1461–1584, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09352-1`; `https://link.springer.com/content/pdf/10.1007/s00145-020-09352-1.pdf`.

Kusters:2020:JSC

[652] Ralf Küsters, Max Tuengerthal, and Daniel Rausch. Joint state composition theorems for public-key encryption and digital signature functionalities with local computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1585–1658, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09353-0`; `https://link.springer.com/content/pdf/10.1007/s00145-020-09353-0.pdf`.

Beimel:2020:SMC

[653] Amos Beimel, Yehuda Lindell, Eran

Omri, and Ilan Orlov. $1\vec{/}p$-secure multiparty computation without an honest majority and the best of both worlds. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1659–1731, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09354-z.

Hazay:2020:LCC

[654] Carmit Hazay, Peter Scholl, and Eduardo Soria-Vazquez. Low cost constant round MPC combining BMR and oblivious transfer. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1732–1786, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09355-y.

Langrehr:2020:TSH

[655] Roman Langrehr and Jiaxin Pan. Tightly secure hierarchical identity-based encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1787–1821, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09356-x; https://link.springer.com/content/pdf/10.1007/s00145-020-09356-x.pdf.

Bootle:2020:FFD

[656] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth. Foundations of fully dynamic group signatures. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1822–1870, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09357-w; https://link.springer.com/content/pdf/10.1007/s00145-020-09357-w.pdf.

Inoue:2020:COA

[657] Akiko Inoue, Tetsu Iwata, Kazuhiko Minematsu, and Bertram Poettering. Cryptanalysis of OCB2: Attacks on authenticity and confidentiality. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1871–1913, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09359-8.

Cohn-Gordon:2020:FSA

[658] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A formal security analysis of the signal messaging protocol. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1914–1983, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09360-1.

Coretti:2020:NME

[659] Sandro Coretti, Yevgeniy Dodis, Ueli Maurer, Björn Tackmann, and Daniele

Venturi. Non-malleable encryption: Simpler, shorter, stronger. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):1984–2033, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09361-0`.

Faust:2020:CNM

[660] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. Continuously non-malleable codes in the split-state model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):2034–2077, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09362-z`; `https://link.springer.com/content/pdf/10.1007/s00145-020-09362-z.pdf`.

Ullman:2020:PHG

[661] Jonathan Ullman and Salil Vadhan. PCPs and the hardness of generating synthetic data. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):2078–2112, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09363-y`.

Wesolowski:2020:EVD

[662] Benjamin Wesolowski. Efficient verifiable delay functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 33(4):2113–2147, October 2020. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09364-x`.

Rosen:2021:CPH

[663] Alon Rosen, Gil Segev, and Ido Shahaf. Can PPAD hardness be based on standard cryptographic assumptions? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09369-6`.

Halevi:2021:BH

[664] Shai Halevi and Victor Shoup. Bootstrapping for HElib. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-020-09368-7`.

Zhandry:2021:QLN

[665] Mark Zhandry. Quantum lightning never strikes the same state twice. or: Quantum money from cryptographic assumptions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

URL https://link.springer.com/article/10.1007/s00145-020-09372-x.

Katsumata:2021:TSP

[666] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV–IBE in the quantum random oracle model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09371-y.

Kaspers:2021:NAP

[667] Christian Kaspers and Yue Zhou. The number of almost perfect nonlinear functions grows exponentially. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09373-w.

Rothblum:2021:TNI

[668] Ron D. Rothblum, Adam Sealfon, and Katerina Sotiraki. Toward non-interactive zero-knowledge proofs for NP from LWE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1): ??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09365-w.

Canetti:2021:RFE

[669] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. Reusable fuzzy extractors for low-entropy distributions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09367-8.

Ducas:2021:LSA

[670] Léo Ducas and Yang Yu. Learning strikes again: The case of the DRS signature scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(1):??, January 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09366-9.

Applebaum:2021:OCC

[671] Benny Applebaum and Zvika Brakerski. Obfuscating circuits via composite-order graded encoding. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09378-z.

Derler:2021:BFE

[672] David Derler, Kai Gellert, Tibor Jager, Daniel Slamanig, and Christoph

Striecks. Bloom filter encryption and applications to efficient forward-secret 0-RTT key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09374-3; https://link.springer.com/content/pdf/10.1007/s00145-021-09374-3.pdf.

Cohen:2021:RPP

[673] Ran Cohen, Sandro Coretti, Juan Garay, and Vassilis Zikas. Round-preserving parallel composition of probabilistic-termination cryptographic protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09377-0.

Applebaum:2021:PCD

[674] Benny Applebaum and Prashant Nalini Vasudevan. Placing conditional disclosure of secrets in the communication complexity universe. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09376-1.

Benhamouda:2021:LLR

[675] Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin. On the local leakage resilience of linear secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09375-2.

Asharov:2021:TTS

[676] Gilad Asharov, Gil Segev, and Ido Shahaf. Tight tradeoffs in searchable symmetric encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(2):??, April 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-020-09370-z.

Abdolmaleki:2021:SRS

[677] Behzad Abdolmaleki, Helger Lipmaa, Janno Siim, and Michał Zając. On subversion-resistant SNARKs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(3):??, July 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09379-y.

Ateniese:2021:MMI

[678] Giuseppe Ateniese, Danilo Francati, David Nuñez, and Daniele Venturi. Match me if you can: Matchmaking encryption and its applications. *Journal of Cryptology: the journal of the International Association for*

Cryptologic Research, 34(3):??, July 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09381-4.

Vincent:2021:E

[679] Rijmen Vincent. Editorial. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(3):??, July 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09380-5; https://link.springer.com/content/pdf/10.1007/s00145-021-09380-5.pdf.

Florez-Gutierrez:2021:ISL

[680] Antonio Flórez-Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, and Ferdinand Sibleyras. Internal symmetries and linear properties: Full-permutation distinguishers and improved collisions on Gimli. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09413-z.

Lindell:2021:FST

[681] Yehuda Lindell. Fast secure two-party ECDSA signing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09409-9.

Jafari:2021:AHS

[682] Amir Jafari and Shahram Khazaei. On Abelian and homomorphic secret sharing schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09410-2.

Katsumata:2021:CDV

[683] Shuichi Katsumata, Ryo Nishimaki, Shota Yamada, and Takashi Yamakawa. Compact designated verifier NIZKs from the CDH assumption without pairings. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09408-w.

Rijmen:2021:CE

[684] Vincent Rijmen. Correction to: Editorial. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34 (4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09407-x; https://link.springer.com/content/pdf/10.1007/s00145-021-09407-x.pdf.

Patra:2021:ERC

[685] Arpita Patra and Divya Ravi. On the exact round complexity of secure three–party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09404-0.

Rotem:2021:ITF

[686] Lior Rotem and Gil Segev. Injective trapdoor functions via derandomization: How strong is Rudich's black-box barrier? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09405-z.

Bogdanov:2021:USC

[687] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09402-2. See corrections [693, 696].

Dowling:2021:CAT

[688] Benjamin Dowling, Marc Fischlin, Felix Günther, and Douglas Stebila. A cryptographic analysis of the TLS 1.3 Handshake Protocol. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09384-1; https://link.springer.com/content/pdf/10.1007/s00145-021-09384-1.pdf.

Krovetz:2021:DEO

[689] Ted Krovetz and Phillip Rogaway. The design and evolution of OCB. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 34(4):??, October 2021. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09399-8; https://link.springer.com/content/pdf/10.1007/s00145-021-09399-8.pdf.

Rotaru:2022:ASS

[690] Dragos Rotaru, Nigel P. Smart, Titouan Tanguy, Frederik Vercauteren, and Tim Wood. Actively secure setup for SPDZ. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09416-w.

Cohen:2022:FFS

[691] Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem. From fairness to full security in multiparty computation. *Journal of Cryptology: the journal of the International Association for*

Cryptologic Research, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09415-x.

Sys:2022:BDH

[692] Marek Sýs, Lubomír Obrátil, Vashek Matyás, and Dusan Klinec. A bad day to die hard: Correcting the Dieharder Battery. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09414-y.

Bogdanov:2022:CUSa

[693] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Correction to: Unconditionally secure computation against low-complexity leakage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09412-0; https://link.springer.com/content/pdf/10.1007/s00145-021-09412-0.pdf. See [687, 696].

Guo:2022:LER

[694] Siyao Guo, Pritish Kamath, Alon Rosen, and Katerina Sotiraki. Limits on the efficiency of (ring) LWE–Based non-interactive key exchange. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(1):??, January 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09406-y.

Radian:2022:SQM

[695] Roy Radian and Or Sattath. Semi-quantum money. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35 (2):??, April 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09418-8.

Bogdanov:2022:CUSb

[696] Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Correction to: Unconditionally secure computation against low–complexity leakage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(2):??, April 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-021-09417-9; https://link.springer.com/content/pdf/10.1007/s00145-021-09417-9.pdf. See [687, 693].

Asharov:2022:LPO

[697] Gilad Asharov, T.-H. Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren, and Elaine Shi. Locality-preserving oblivious RAM. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35 (2):??, April 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (elec-

tronic). URL https://link.springer.com/article/10.1007/s00145-022-09419-1.

Kitagawa:2022:OBSa

[698] Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka. Obfustopia built on secret-key functional encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(3):??, July 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09429-z.

Bitansky:2022:NPC

[699] Nir Bitansky and Vinod Vaikuntanathan. A note on perfect correctness by derandomization. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(3):??, July 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09428-0.

Hashimoto:2022:EGC

[700] Keitaro Hashimoto, Shuichi Katsumata, and Thomas Prest. An efficient and generic construction for signal's handshake (X3DH): Post-quantum, state leakage secure, and deniable. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(3):??, July 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09427-1.

Kiyoshima:2022:CRL

[701] Susumu Kiyoshima. Constant-round leakage-resilient zero-knowledge from collision resistance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(3):??, July 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09426-2.

Bitansky:2022:SNI

[702] Nir Bitansky, Alessandro Chiesa, and Omer Paneth. Succinct non-interactive arguments via linear interactive proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(3):??, July 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09424-4.

Kitagawa:2022:OBSb

[703] Fuyuki Kitagawa, Ryo Nishimaki, and Keisuke Tanaka. Obfustopia built on secret-key functional encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(4):??, October 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09429-z.

Magri:2022:EUC

[704] Bernardo Magri, Giulio Malavolta, and Dominique Unruh. Everlasting UC commitments from fully malicious PUFs. *Journal of Cryptology: the journal*

of the International Association for Cryptologic Research, 35(4):??, October 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09432-4.

Asharov:2022:CCO

[705] Gilad Asharov, Ilan Komargodski, and Naomi Sirkin. On the complexity of compressing obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(4):??, October 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09431-5.

Grover:2022:NCR

[706] Charles Grover, Andrew Mendelsohn, and Roope Vehkalahti. Noncommutative ring learning with errors from cyclic algebras. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(4):??, October 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09430-6.

Hazay:2022:ZPL

[707] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. ZK-PCPs from leakage-resilient secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 35(4):??, October 2022. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09433-3.

Boudgoust:2023:HML

[708] Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. On the hardness of module learning with errors with short distributions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(1):??, January 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09441-3.

Alamati:2023:MPA

[709] Navid Alamati, Hart Montgomery, Sikhar Patranabis, and Arnab Roy. Minicrypt primitives with algebraic structure and applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(1):??, January 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09442-2.

Liu:2023:RDL

[710] Yunwen Liu, Zhongfeng Niu, Siwei Sun, Chao Li, and Lei Hu. Rotational differential–linear cryptanalysis revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(1):??, January 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-022-09440-4.

Pointcheval:2023:TCC

[711] David Pointcheval and Nigel Paul Smart. Topical collection on computing on encrypted data. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09444-8`.

Applebaum:2023:CLC

[712] Benny Applebaum and Yoni Moses. Correction: Locally computable UOWHF with linear shrinkage. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09443-9`. See [533].

Datta:2023:DMA

[713] Pratish Datta, Ilan Komargodski, and Brent Waters. Decentralized multi-authority ABE for NC^1 from BDH. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09445-7`.

Asharov:2023:ORW

[714] Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, and Elaine Shi. Oblivious RAM with worst-case logarithmic overhead. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09447-5`.

Takeshita:2023:SSI

[715] Jonathan Takeshita, Ryan Karl, Ting Gong, and Taeho Jung. SLAP: Simpler, improved private stream aggregation from ring learning with errors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09450-w`.

Kiyoshima:2023:NSL

[716] Susumu Kiyoshima. No-signaling linear PCPs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09448-4`.

Mouchet:2023:ETA

[717] Christian Mouchet, Elliott Bertrand, and Jean-Pierre Hubaux. An efficient threshold access-structure for RLWE-based multiparty homomorphic encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-

2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09452-8`.

Cohen:2023:ASM

[718] Ran Cohen, Abhi Shelat, and Daniel Wichs. Adaptively secure MPC with sublinear communication complexity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09446-6`.

Geelen:2023:BBB

[719] Robin Geelen and Frederik Vercauteren. Bootstrapping for BGV and BFV revisited. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09454-6`.

Choudhury:2023:CES

[720] Ashish Choudhury and Arpita Patra. On the communication efficiency of statistically secure asynchronous MPC with optimal resilience. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09451-9`.

Kitagawa:2023:NS

[721] Fuyuki Kitagawa, Takahiro Matsuda, and Takashi Yamakawa. NIZK from SNARGs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(2):??, April 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09449-3`.

Chida:2023:FLS

[722] Koji Chida, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Daniel Genkin, Yehuda Lindell, and Ariel Nof. Fast large-scale honest-majority MPC for malicious adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09453-7`.

Appan:2023:REA

[723] Ananya Appan, Anirudh Chandramouli, and Ashish Choudhury. Revisiting the efficiency of asynchronous MPC with optimal resilience against general adversaries. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09457-3`.

Bouvier:2023:WRM

[724] Cyril Bouvier, Guilhem Castagnos, Laurent Imbert, and Fabien Laguillaumie.

I want to ride my BICYCL: BICYCL implements CryptographY in CLass groups. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09459-1`.

Coutinho:2023:LDR

[725] Murilo Coutinho, Iago Passos, Juan C. Grados Vásquez, Santanu Sarkar, Fábio L. L. de Mendonça, Rafael T. de Sousa, and Fábio Borges. Latin dances reloaded: Improved cryptanalysis against Salsa and ChaCha, and the proposal of Forró. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09455-5`.

Saha:2023:LYF

[726] Sayandeep Saha, Manaar Alam, Arnab Bag, Debdeep Mukhopadhyay, and Pallab Dasgupta. Learn from your faults: Leakage assessment in fault attacks using deep learning. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09462-6`.

Boyle:2023:MCG

[727] Elette Boyle, Ran Cohen, Deepesh Data, and Pavel Hubáček. Must the communication graph of MPC protocols be an expander? *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09460-8`.

Furukawa:2023:HTS

[728] Jun Furukawa, Yehuda Lindell, Ariel Nof, and Or Weinstein. High-throughput secure three-party computation with an honest majority. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09461-7`.

Koti:2023:MPS

[729] Nishat Koti, Shravani Patil, Arpita Patra, and Ajith Suresh. MPClan: Protocol suite for privacy-conscious computations. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-023-09469-z`.

Libert:2023:ZKA

[730] Benoît Libert, San Ling, Khoa Nguyen, and Huaxiong Wang. Zero-knowledge

arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09470-6.

Alon:2023:AOF

[731] Bar Alon and Eran Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09466-2.

Alon:2023:PHM

[732] Bar Alon, Ran Cohen, Eran Omri, and Tom Suad. On the power of an honest majority in three-party computation without broadcast. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09456-4.

Hazay:2023:ASG

[733] Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Actively secure garbled circuits with constant communication overhead in the plain model. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09465-3.

Brakerski:2023:CIH

[734] Zvika Brakerski, Nico Döttling, Sanjam Garg, and Giulio Malavolta. Candidate iO from homomorphic encryption schemes. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09471-5.

Bergerat:2023:POL

[735] Loris Bergerat, Anas Boudi, Quentin Bourgerie, Ilaria Chillotti, Damien Ligier, Jean-Baptiste Orfila, and Samuel Tap. Parameter optimization and larger precision for (T)FHE. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09463-5.

Dowerah:2023:UPI

[736] Uddipana Dowerah, Subhranil Dutta, Aikaterini Mitrokotsa, Sayantan Mukherjee, and Tapas Pal. Unbounded predicate inner product functional encryption from pairings. *Journal of Cryptology: the journal of the In-*

ternational Association for Cryptologic Research, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09458-2.

Patra:2023:BHM

[737] Arpita Patra and Divya Ravi. Beyond honest majority: The round complexity of fair and robust multi-party computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09468-0.

Belorgey:2023:MFE

[738] Mariya Georgieva Belorgey, Sergiu Carpov, Kevin Deforth, Dimitar Jetchev, Abson Sae-Tang, Marius Vuille, Nicolas Gama, Jon Katz, Iraklis Leontiadis, and Mohsen Mohammadi. Manticore: A framework for efficient multiparty computation supporting real number and Boolean arithmetic. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 36(3):??, July 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09464-4.

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 Cryptologic Research*, 36(4):??, October 2023. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09474-2.

Ishai:2024:BCK

[740] Yuval Ishai, Alexis Korb, Paul Lou, and Amit Sahai. Beyond the Csiszár–Körner bound: Best–possible wiretap coding via obfuscation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, March 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09482-2.

Boyle:2024:BSB

[741] Elette Boyle, Ran Cohen, and Aarushi Goel. Breaking the $O(\sqrt{n})$-bit barrier: Byzantine agreement with polylog bits per party. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09484-0.

Drucker:2024:BCE

[742] Nir Drucker, Guy Moshkowich, Tomer Pelleg, and Hayim Shaul. BLEACH: Cleaning errors in discrete computations over CKKS. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-

2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09483-1.

Zhang:2024:LBP

[743] Jiang Zhang, Yu Chen, and Zhenfeng Zhang. Lattice-based programmable hash functions and applications. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09488-w.

Barthe:2024:MGL

[744] Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, and Mehdi Tibouchi. Masking the GLP lattice-based signature scheme at any order. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09485-z.

Micheli:2024:LEA

[745] Gabrielle De Micheli, Pierrick Gaudry, and Cécile Pierrot. Lattice enumeration and automorphisms for tower NFS: a 521-bit discrete logarithm computation. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09487-x.

Bernstein:2024:CC

[746] Daniel J. Bernstein. Cryptographic competitions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09467-1.

Cini:2024:IPF

[747] Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks, and Erkan Tairi. (Inner-product) functional encryption with updatable ciphertexts. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(1):??, January 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09486-y.

Fischlin:2024:RCH

[748] Marc Fischlin, Felix Günther, and Christian Janson. Robust channels: Handling unreliable networks in the record layers of QUIC and DTLS 1.3. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, June 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-023-09489-9.

Akshima:2024:TSL

[749] Akshima, Siyao Guo, and Qipeng Liu. Time-space lower bounds for finding collisions in Merkle–Damgård hash functions. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09491-9`.

Koshelev:2024:HEC

[750] Dmitrii Koshelev. Hashing to elliptic curves through Cipolla–Lehmer–Müller's square root algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09490-w`.

Hofheinz:2024:IBE

[751] Dennis Hofheinz, Jessica Koch, and Christoph Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09496-4`.

Lubicz:2024:ECO

[752] David Lubicz and Viktor Fischer. Entropy computation for oscillator-based physical random number generators. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09494-6`.

Rothblum:2024:CRM

[753] Ron D. Rothblum and Prashant Nalini Vasudevan. Collision resistance from multi-collision resistance. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09495-5`.

Andreeva:2024:CAE

[754] Elena Andreeva, Andrey Bogdanov, Nilanjan Datta, Atul Luykx, Bart Mennink, Mridul Nandi, Elmar Tischhauser, and Kan Yasuda. The COLM authenticated encryption scheme. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09492-8`.

Blocki:2024:BHF

[755] Jeremiah Blocki, Peiyuan Liu, Ling Ren, and Samson Zhou. Bandwidth-hard functions: Reductions and lower bounds. *Journal of Cryptology: the journal of the International Association*

for Cryptologic Research, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09497-3`.

Kiayias:2024:CNM

[756] Aggelos Kiayias, Feng-Hao Liu, and Yiannis Tselekounis. (Continuous) non-malleable codes for partial functions with manipulation detection and light updates. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09498-2`.

Badertscher:2024:BTL

[757] Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. Bitcoin as a transaction ledger: a composable treatment. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09493-7`.

Yang:2024:ORB

[758] Qianqian Yang, Ling Song, Nana Zhang, Danping Shi, Libo Wang, Jiahao Zhao, Lei Hu, and Jian Weng. Optimizing rectangle and boomerang attacks: a unified and generic framework for key recovery. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(2):??, April 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09499-1`.

Oygarden:2024:AME

[759] Morten Øygarden, Patrick Felke, and Håvard Raddum. Analysis of multivariate encryption schemes: Application to Dob and C^*. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(3):??, September 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09501-w`.

Bellare:2024:SDP

[760] Mihir Bellare and Anna Lysyanskaya. Symmetric and dual PRFs from standard assumptions: a generic validation of a prevailing assumption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 37(4):??, December 2024. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09513-6`.

Cohen:2025:GOR

[761] Ran Cohen, Jack Doerner, Yashvanth Kondi, and Abhi Shelat. Guaranteed output in $O(\sqrt{n})$ rounds for round-robin sampling protocols. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic).

URL https://link.springer.com/article/10.1007/s00145-024-09523-4.

Cheon:2025:IUT

[762] Jung Hee Cheon, Wonhee Cho, and Jiseung Kim. Improved universal thresholdizer from iterative Shamir secret sharing. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09536-z.

Campanelli:2025:NCS

[763] Matteo Campanelli, Dario Fiore, and Rosario Gennaro. Natively compatible super-efficient lookup arguments and how to apply them. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09535-0.

Beaugrand:2025:ESZ

[764] Agathe Beaugrand, Guilhem Castagnos, and Fabien Laguillaumie. Efficient succinct zero-knowledge arguments in the CL framework. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09534-1.

Li:2025:CAB

[765] Jianwei Li and Phong Q. Nguyen. A complete analysis of the BKZ lattice reduction algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09527-0. See correction [780].

Ganesh:2025:FSB

[766] Chaya Ganesh, Claudio Orlandi, Mahak Pancholi, Akira Takahashi, and Daniel Tschudi. Fiat–Shamir bulletproofs are non-malleable (in the random oracle model). *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09525-2.

Bui:2025:EZC

[767] Dung Bui, Haotian Chu, Geoffroy Couteau, Xiao Wang, Chenkai Weng, Kang Yang, and Yu Yu. An efficient ZK compiler from SIMD circuits to general circuits. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09531-4.

Avoine:2025:DKC

[768] Gildas Avoine and Loïc Ferreira. De-

crypting without keys: The case of the GlobalPlatform SCP02 protocol. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09528-z`.

Brzuska:2025:BFG

[769] Chris Brzuska and Geoffroy Couteau. On building fine-grained one-way functions from strong average-case hardness. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09518-1`.

Avitabile:2025:CPP

[770] Gennaro Avitabile, Vincenzo Botta, Daniele Friolo, Daniele Venturi, and Ivan Visconti. Compact proofs of partial knowledge for overlapping CNF formulae. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09532-3`.

Farzaliyev:2025:LBZ

[771] Valeh Farzaliyev, Calvin Pärn, Heleen Saarse, and Jan Willemson. Lattice-based zero-knowledge proofs in action: Applications to electronic voting. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09530-5`.

Akavia:2025:ACR

[772] Adi Akavia, Craig Gentry, Shai Halevi, and Margarita Vald. Achievable CCA2 relaxation for homomorphic encryption. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09526-1`.

Block:2025:SNI

[773] Alexander R. Block, Albert Garreta, Pratyush Ranjan Tiwari, and Michał Zajac. On soundness notions for interactive oracle proofs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09520-7`.

Chavez-Saab:2025:SSV

[774] Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. SwiftEC: Shallue–van de Woestijne indifferentiable function to elliptic curves. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-

2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09529-y.

Leurent:2025:NRA

[775] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09522-5.

Hazay:2025:PDP

[776] Carmit Hazay, Muthuramakrishnan Venkitasubramaniam, and Mor Weiss. Protecting distributed primitives against leakage: Equivocal secret sharing and more. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(1):??, January 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-024-09524-3.

Fan:2025:SMS

[777] Xinxin Fan, Veronika Kuchta, Francesco Sica, and Lei Xu. Speeding up multi-scalar multiplications for pairing-based zkSNARKs. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(2):??, April 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-025-09540-x.

Carlet:2025:TGA

[778] Claude Carlet. Two generalizations of almost perfect nonlinearity. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(2):??, April 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-025-09538-5.

Cui:2025:ASH

[779] Hongrui Cui, Xiao Wang, Kang Yang, and Yu Yu. Actively secure half-gates with minimum overhead under duplex networks. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(2):??, April 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-025-09539-4.

Li:2025:CCA

[780] Jianwei Li and Phong Q. Nguyen. Correction to: A complete analysis of the BKZ lattice reduction algorithm. *Journal of Cryptology: the journal of the International Association for Cryptologic Research*, 38(2):??, April 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL https://link.springer.com/article/10.1007/s00145-025-09537-6. See [765].

Liu:2025:ECN

[781] Tianyi Liu, Zhenfei Zhang, Yuncong Zhang, Wenqing Hu, and Ye Zhang. `Ceno`: Non-uniform, segment and parallel zero-knowledge virtual machine.

Journal of Cryptology: the journal of the International Association for Cryptologic Research, 38(2):??, April 2025. CODEN JOCREQ. ISSN 0933-2790 (print), 1432-1378 (electronic). URL `https://link.springer.com/article/10.1007/s00145-024-09533-2`.