A Complete Bibliography of Publications in the *Journal of Cryptology*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

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

12 September 2016
Version 1.43

Title word cross-reference

1 [276]. 2 [491, 267, 130]. 3 [342]. 31 [261]. 4 [26]. 8 [474]. $^+$ [356]. d [363]. GF(2^m) [68]. k [276, 204, 402]. $L(1/3)$ [366]. Q [512]. $nL3$ mod 4 [227]. $O(n)$ [219]. p [91]. S [29, 94, 24, 88].

-Adic [130]. **-Box** [88]. **-Boxes** [94, 29, 24]. **-Connected** [276]. **-curve** [512]. **-Group** [91]. **-Multiplicative** [363]. **-Round** [474]. **-tree** [402]. **-Wise** [204].

0 [465].

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

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

3G [461].

4-Round [393].

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

abelian [326, 408, 91, 337]. **Abstract** [117]. **Accelerated** [512]. **Accelerating** [398]. **Achieve** [477]. **Adaptive** [241, 390, 471]. **Adaptively** [390]. **Adic** [130]. **Advance** [279]. **Adversarial** [458]. **Adversaries** [353, 345, 357, 403, 450, 472, 501, 236]. **Adversary** [173]. **AES** [373, 474, 346, 459]. **AES-192** [474]. **AES-256** [474]. **AES-like** [459]. **after** [76]. **Against** [353, 480, 348, 500, 357, 214, 192, 265, 95, 485, 236, 210]. **Aggregate** [429]. **Agreement**

[259, 258, 260, 128]. **AKS** [297]. **Alerts** [486]. **Algebraic** [201, 64, 92, 479]. **Algorithm** [146, 398, 251, 267, 377, 366, 74, 402, 154, 79, 215]. **Algorithms** [434, 88, 444]. **Almost** [484, 322, 204]. **Almost-Everywhere** [484]. **Alternative** [160]. **among** [320]. **Amortized** [448]. **Amplification** [452, 421, 230, 129, 222]. **Analysis** [374, 320, 480, 361, 266, 368, 251, 413, 417, 305, 424, 192, 187, 351, 152, 88, 441, 182, 33, 87]. **Anonymous** [316, 223, 510]. **ANSI** [208]. **Answer** [197]. **Any** [115, 143]. **Application** [199, 289, 225, 407, 470, 159, 36]. **Applications** [123, 427, 341, 426, 149, 406, 439, 204, 92, 155]. **Applied** [408]. **Applying** [33]. **Approach** [482, 10, 23]. **Approaches** [344, 221]. **Approximation** [184]. **Arbitrary** [254, 252]. **Arbitrary-Length** [254]. **arbitration** [22]. **Arguments** [143, 185]. **Arithmetic** [68, 199]. **Aspects** [177]. **Assignment** [399, 69]. **Assumption** [310, 238]. **Assumptions** [513, 467, 272, 335, 503, 424, 138, 277]. **Asymmetric** [418, 198]. **Asynchronous** [259, 464]. **Attack** [396, 133, 348, 377, 461, 422, 214, 126, 265, 470, 95, 489, 210, 438, 41]. **Attacks** [508, 93, 468, 511, 373, 445, 509, 474, 462, 179, 224, 279, 201, 453, 141, 314, 485, 346, 239, 198, 14]. **Authenticated** [473, 458, 320, 174, 214, 288, 437, 268]. **Authentication** [389, 162, 147, 289, 344, 280, 104, 159, 3, 39, 33, 76, 22, 9, 19, 25]. **authentication/secrecy** [39, 9]. **Authority** [137]. **Authority-Free** [137]. **Automata** [496]. **Auxiliary** [446, 358]. **Auxiliary-Input** [446]. **Average** [281]. **Average-** [281]. **Aware** [443].

Balanced [405]. **Bandwidth** [256]. **Based** [367, 456, 248, 379, 115, 325, 311, 336, 361, 387, 373, 289, 377, 493, 186, 253, 300, 287, 496, 280, 274, 168, 321, 315, 437, 83, 326, 501, 209, 384, 485, 337, 203, 198, 17, 55, 8, 61, 41, 79, 314]. **Bases** [263]. **Basing** [270]. **Basis** [409]. **Batch** [412, 127, 128]. **Be** [463, 495, 135, 56]. **being** [71]. **Benefits** [345]. **Best** [454]. **Best-Possible** [454]. **Better** [446]. **Between** [407, 321]. **Bias** [505]. **Bijective** [97]. **Bilinear** [310]. **Binary** [66, 112, 60]. **Binding** [323]. **Binding-Concealing** [323]. **Birational** [134]. **Bit** [132, 262, 48, 59]. **Bits** [219, 178, 15]. **Bivariate** [333, 425]. **Black** [338, 145]. **Black-Box** [338, 145]. **Blind** [229, 185]. **Blobs** [52, 21]. **Block** [279, 422, 201, 141, 385, 104, 469, 232]. **Blockcipher** [336, 361]. **Blockcipher-Based** [336]. **Bonsai** [409]. **Boolean** [27, 405, 100]. **Bound** [399, 162, 76]. **Bounded** [291, 235, 158, 236, 332, 237]. **Bounded-Storage** [235, 332, 237]. **Bounds** [338, 110, 200, 312, 104, 167, 3, 63, 39, 25]. **Box** [338, 88, 145]. **Boxes** [94, 29, 24]. **Break** [174]. **Break-Ins** [174]. **Breaking** [495, 380, 139]. **Broadcast** [258]. **Bucket** [159]. **Bug** [511]. **Build** [492]. **Building** [252]. **Buses** [223]. **Byzantine** [259, 258].

Cache [346]. **Calculation** [244]. **Calculus** [324, 457]. **can** [56]. **Capacity** [262]. **Cards** [110, 49]. **Cartesian** [22]. **Cascade** [71]. **Case** [281]. **CBC** [410, 254, 183]. **CBCM** [208]. **CCA** [463]. **CCA2** [277]. **CCA2-Secure** [277]. **CCITT** [33]. **Centers** [266]. **Central** [270]. **Certain** [264, 56, 60, 14, 9]. **Certificateless** [311]. **certification** [81]. **Certifying** [115]. **Challenge** [463]. **Chameleon** [460]. **Channel** [376]. **Channels** [391, 262, 197]. **Characteristic** [267, 83, 151, 161]. **Characteristics** [97]. **Characterization** [460, 142, 269]. **Chaum** [229]. **cheaters** [11]. **Chernoff** [327]. **Chernoff-Type** [327]. **Chinese** [168]. **Choose** [411, 501]. **Chor** [37, 195]. **Chosen** [348, 419, 126, 210, 26].

Chosen-Ciphertext [348]. **Cipher** [492, 131, 422, 209, 85, 441, 232, 57]. **Ciphers** [410, 380, 279, 201, 217, 385, 469, 483, 438, 182, 41, 71, 14, 58, 16]. **Ciphertext** [317, 348, 419, 210]. **Ciphertext-Only** [317]. **circuit** [17]. **Class** [324, 381, 88, 103, 41]. **Classical** [262]. **Classification** [46]. **Clocked** [224]. **code** [62]. **Codes** [162, 314, 104, 3, 39, 22, 9, 19]. **Coin** [478, 228, 502, 414]. **Coin-Tossing** [228]. **Collision** [488, 125, 489, 98, 155]. **Collision-Free** [125, 98]. **Collisions** [365]. **Coloring** [408]. **Combinatorial** [23, 9]. **combinatorics** [19]. **Combiner** [112, 318]. **Combiners** [451, 130, 58]. **Combining** [182]. **Commitment** [132, 343, 371, 335, 158, 323, 262, 48]. **Commitments** [499, 426]. **Communication** [317, 466, 174, 172, 111, 262, 439, 313, 89, 197, 72]. **Compact** [431]. **Comparison** [434, 444, 139]. **Competitive** [111]. **Compilers** [334]. **Complete** [250, 477]. **Completeness** [452, 282]. **Complexity** [264, 466, 448, 200, 70, 335, 476, 89, 72, 23]. **Composability** [386, 430, 475, 383, 339, 364]. **Composable** [449, 272, 368]. **Composition** [320, 176, 303, 312, 339]. **Compositions** [198]. **Comprehensive** [374]. **Compress** [125]. **Computable** [237]. **Computation** [355, 514, 389, 240, 276, 272, 484, 408, 250, 119, 260, 392, 282, 173, 228, 339, 331, 411, 472, 464]. **Computational** [212, 301, 482, 282, 231, 407, 139, 479]. **Computationally** [450, 249, 395]. **Computations** [196]. **computed** [56]. **Computing** [473, 286, 190]. **Concealing** [323]. **Concerning** [103]. **Concurrent** [303, 356, 312, 440, 494]. **Conditionally** [57]. **Conditionally-perfect** [57]. **Conditions** [98]. **Confidence** [227]. **Confined** [467]. **congruential** [15]. **Conjecture** [103, 405]. **Connected** [276]. **Connection** [482]. **Connectivity** [172]. **Consequences** [391]. **Consistency** [316]. **Constant** [513, 340, 291, 116, 228, 435]. **Constant-Round** [291, 116, 228, 435]. **Constant-Size** [513]. **Constantinople** [259]. **Construct** [116]. **Constructing** [476, 211, 237]. **Construction** [492, 131, 225, 305, 277, 156, 88, 512, 22, 9]. **Constructions** [456, 513, 410, 329, 311, 254, 416, 482, 3, 39]. **Constructive** [334, 207]. **Contrast** [170]. **control** [35]. **Coppersmith** [425]. **Core** [200]. **Correct** [370]. **Correlation** [416, 112, 179, 224, 58, 182, 41, 14]. **Correlation-Secure** [416]. **Corruptions** [484]. **Cost** [239]. **Counter** [164]. **Counterexamples** [103]. **Countermeasures** [346]. **Counting** [60]. **Covert** [353, 357, 439, 501]. **Cryptanalysis** [317, 108, 140, 163, 208, 261, 465, 360, 102, 415, 306, 507, 153, 369, 107, 459, 347, 515, 318, 319, 330, 309, 483, 298, 195, 43, 26]. **Cryptanalyst** [148]. **Cryptanalytic** [93, 434, 444, 239, 155]. **Crypto** [376]. **Cryptographers** [5]. **Cryptographic** [196, 189, 176, 270, 328, 386, 349, 118, 124, 424, 231, 407, 205, 101, 91, 145, 100, 177, 87, 60, 27, 36, 86]. **cryptographically** [29]. **Cryptography** [212, 301, 340, 264, 199, 334, 160, 170, 491, 259, 381, 455, 503, 92, 337, 479, 198, 10, 54]. **Cryptologic** [204]. **Cryptology** [427]. **CRYPTOPOST** [36]. **Cryptosystem** [490, 461, 126, 326, 180, 144, 195, 32, 37, 64]. **Cryptosystems** [248, 287, 168, 221, 314, 139, 203, 210, 161, 237, 246, 43, 28, 12, 80]. **Cubic** [144, 62]. **Curve** [199, 146, 334, 213, 381, 420, 126, 52, 161, 271, 246, 80, 512]. **Curves** [267, 324, 252, 366, 457, 352, 381, 207, 359, 283, 151, 165, 342, 512, 40]. **Cut** [411, 501]. **Cut-and-Choose** [411]. **Cut-and-Choose-Based** [501]. **Cycling** [2].

Damgård [400]. **Data** [473, 216, 209, 302, 183, 2]. **Data-Dependent** [209]. **Davies** [133]. **Deal** [110]. **Decision** [231]. **Decommitments** [382]. **Decomposing** [198]. **Decompositions** [96]. **Decorrelation** [232]. **Decryption** [463, 180]. **Deficiencies** [51]. **Definition** [463]. **Definitions** [329, 82, 345]. **Degree** [252, 366, 201, 420, 283]. **Delegate** [409]. **Delegation** [394]. **Delivery** [223]. **Demytko** [126]. **Deniable** [344]. **Dense** [498]. **Dependence** [370]. **Dependent** [452, 124, 209]. **derived** [66]. **DES-like** [43]. **Descent** [207]. **Design** [266, 79, 29]. **Designing** [221, 24]. **Designs** [460, 104, 9]. **Destructive** [334, 207]. **DESX** [192]. **Detailed** [187]. **Deterministic** [446, 286, 482]. **Dichotomy** [505]. **Differential** [108, 43, 415, 107, 95, 309]. **Differentials** [261]. **Difficult** [495]. **Difficulty** [139]. **Diffie** [341, 184, 304, 231, 245, 157, 128]. **Diffusion** [469]. **Digital** [109, 413, 206, 185, 122, 34, 215]. **Dimensional** [447]. **diminished** [79]. **diminished-radix** [79]. **Dining** [5]. **Direct** [327]. **Disallowed** [463]. **Discrete** [146, 21, 358, 184, 366, 457, 253, 287, 74, 190, 420, 188, 139, 165, 342, 55]. **Discrete-Log** [287]. **Dishonest** [478]. **Disjunctions** [423]. **distance** [41]. **Distinguishers** [470]. **Distributed** [266, 296, 287, 417]. **Distribution** [278, 266, 255, 97, 167, 177, 20, 7]. **distributions** [75]. **Divertible** [166]. **document** [34]. **domains** [73]. **Don't** [476]. **Double** [141]. **Drinfeld** [203]. **Dynamic** [202, 256].

E0 [318]. **E0-like** [318]. **Easily** [233]. **ECPP** [297]. **Edge** [484]. **Edit** [224]. **Editor** [284, 31, 67, 113, 44]. **Editorial** [1, 42, 372]. **Efficiency** [235]. **Efficient** [353, 199, 248, 460, 336, 387, 149, 343, 371, 119, 493, 181, 299, 304, 158, 357, 403, 118, 439, 138, 359, 472, 255, 38, 244, 222, 464, 469, 49, 438, 346]. **Elementary** [91]. **Elements** [499, 355]. **Eliminating** [196]. **Elliptic** [199, 146, 334, 457, 352, 213, 381, 207, 420, 126, 52, 359, 283, 80, 151, 165, 161, 512, 271, 246, 40]. **Embedding** [283]. **EMV** [507]. **Encapsulation** [456]. **Encrypted** [317, 429]. **Encryption** [212, 301, 316, 367, 308, 320, 443, 387, 446, 294, 150, 348, 509, 462, 119, 418, 482, 487, 70, 419, 388, 322, 2, 269, 423, 277, 236, 154]. **Encryptions** [362]. **Endomorphism** [512]. **Endomorphism-Accelerated** [512]. **Endomorphisms** [381]. **Enhanced** [490]. **Enhancements** [432]. **EnRUPT** [365]. **Entropy** [482]. **Enumerating** [27, 100]. **Equations** [136, 423]. **Equivalence** [286]. **Equivalent** [74, 62, 7]. **Erratum** [444]. **Error** [281]. **Errors** [196]. **Escape** [486]. **Escrow** [160]. **Especially** [476]. **Estimate** [281]. **Evaluation** [496, 17]. **Even** [509, 462]. **Everywhere** [484]. **Evidence** [246]. **Exact** [206]. **Exchange** [147, 106, 110, 274, 214, 288, 437, 268, 90, 8]. **Exhaustive** [192]. **Exist** [476]. **Existence** [132, 191]. **Existentially** [149]. **Expander** [328]. **Expected** [345, 315]. **Experimental** [54]. **Experiments** [2]. **Exponent** [136]. **Exponentiation** [264, 225]. **Extended** [281, 117, 402]. **Extension** [267, 420, 10]. **Extensions** [316, 199]. **Extraction** [494]. **Extractors** [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** [370, 502]. **Fairness** [386, 392]. **Fallacious** [162]. **Family** [438]. **Fast** [491, 179, 141, 501, 101, 14, 151, 159, 157, 32, 30, 79]. **Faster** [381]. **Fault** [175, 373, 377]. **Fault-Based** [377].

Fault-Tolerance [175]. **Faults** [168]. **Faulty** [45]. **FCSR** [380, 438]. **FEAL** [26]. **FEAL-** [26]. **Feedback** [130]. **Feistel** [492, 217]. **Field** [199, 274, 78]. **Fields** [398, 252, 420, 83, 151, 90, 144, 161, 263, 8]. **Finite** [199, 102, 398, 252, 326, 221, 263]. **first** [71]. **Fixed** [262, 383]. **FlipIt** [436]. **Fly** [280]. **Forgery** [485]. **Formal** [212, 301, 292, 33]. **Forward** [294]. **Forward-Secure** [294]. **Four** [447]. **Four-Dimensional** [447]. **FPGA** [373, 378]. **FPGA-friendly** [378]. **Fractional** [160]. **Framework** [308, 475]. **Franklin** [197]. **Free** [504, 166, 125, 137, 322, 350, 98]. **Frequency** [121]. **Friendly** [352, 378]. **Frobenius** [281]. **Full** [422, 515, 239]. **Fully** [433, 487]. **Function** [219, 125, 369, 222, 30]. **Functional** [89]. **Functions** [456, 508, 220, 460, 471, 164, 336, 361, 328, 451, 416, 181, 299, 406, 141, 221, 476, 375, 469, 405, 103, 100, 182, 60, 27]. **Further** [100].

Gabidulin [314]. **Gallant** [447]. **Game** [514, 436]. **Garbling** [504]. **Gates** [504]. **GE** [376]. **General** [200, 112, 173, 138, 277, 339, 313]. **Generalization** [10]. **Generalized** [41]. **Generates** [85]. **Generating** [233]. **Generation** [4, 287, 275, 359, 101, 307, 49, 99]. **Generator** [253, 179, 298, 15]. **Generators** [505, 379, 225, 224, 121, 191, 222, 59, 38]. **Generic** [513, 452, 320, 311, 424]. **Genus** [491, 324, 157, 342]. **Geometric** [83]. **GGH** [330]. **Given** [258, 56]. **Giving** [51]. **Glitch** [373]. **Glitches** [375]. **GNUC** [475]. **Goldreich** [242]. **Golić** [405]. **good** [29]. **GOST** [422]. **Graph** [96, 408]. **Graphs** [498, 328]. **Grindahl** [489]. **Group** [499, 102, 289, 2, 288, 319, 350, 384, 85, 91]. **Groups** [310, 408, 324, 280, 231, 326, 221]. **GSM** [317, 461]. **Guessing** [467]. **Guest** [372, 31, 113, 44].

H [380]. **Handling** [315]. **Handshake** [351]. **Hard** [289, 500, 200]. **Hard-Core** [200]. **Hard-to-Invert** [289, 500]. **Hardness** [421]. **Hardware** [375]. **Hash** [508, 428, 410, 460, 336, 361, 328, 451, 413, 369, 406, 141, 469, 30]. **Hash-CBC** [410]. **Hashing** [442, 397, 159, 98]. **having** [76]. **HB** [356]. **Hellman** [10, 341, 184, 304, 231, 245, 157, 128]. **Help** [226]. **Hides** [219]. **Hiding** [132, 335, 17]. **Hierarchical** [399, 293]. **Hierarchy** [84]. **High** [227]. **Highly** [336]. **Highly-Efficient** [336]. **Hints** [51]. **HMAC** [488]. **Homomorphic** [487, 362]. **Homomorphisms** [384]. **Human** [275]. **Hybrid** [308, 348, 487]. **Hyperelliptic** [267, 12, 342, 324].

IACBC [290]. **IAPM** [290]. **IBE** [316]. **IDEA** [468]. **Ideal** [46, 492, 404, 142, 120, 65]. **Identification** [506, 325, 50, 169, 55, 61]. **Identity** [367, 456, 325, 311, 387, 6]. **Identity-Based** [367, 456, 325, 311, 387]. **IEC** [306]. **imaginary** [8]. **impersonation** [81]. **Implementation** [248, 160, 102, 373, 375, 32, 21, 80]. **Implementations** [50, 52]. **Importance** [196, 71]. **Impossibility** [336, 270, 382, 383, 312]. **Impossible** [261]. **Improbability** [146]. **Improve** [337]. **Improved** [348, 445, 474, 253, 274, 459, 378, 63]. **Improvement** [133]. **Improvements** [123]. **Improving** [206]. **Independent** [204]. **Index** [324, 457]. **Indifferentiability** [492]. **Indistinguishability** [407]. **Inferring** [15]. **Infinite** [103, 73]. **Information** [374, 466, 240, 295, 129, 193, 104, 25, 17, 63]. **Information-Theoretic** [295, 104, 25]. **Inner** [423]. **Input** [340, 421, 446]. **Inputs** [358, 383]. **Ins** [174]. **Insecure** [203]. **Insecurity** [215]. **Instant** [317]. **instruments** [24]. **Integration** [418].

Integrity [322, 86]. **Interaction** [226]. **Interactive** [189, 55, 442, 111, 487, 477, 332]. **Interpolation** [333]. **Intersection** [493, 357]. **Introduction** [31, 42, 113, 44]. **Inversion** [229, 89]. **Invert** [289, 500]. **ISO** [306, 507]. **ISO/IEC** [306]. **Isogenies** [342]. **Isomorphisms** [289]. **Iterated** [509]. **Iteration** [297]. **IV** [279].

Jacobians [342]. **Joint** [119].

Kangaroos [188]. **KASUMI** [461]. **Keccak** [445]. **Kedlaya** [267]. **KeeLoq** [396]. **KEM/DEM** [308]. **KEMs** [311]. **kernels** [61]. **Key** [456, 452, 399, 490, 160, 278, 254, 102, 266, 446, 147, 294, 286, 150, 509, 461, 474, 105, 110, 287, 28, 275, 422, 274, 214, 269, 288, 437, 383, 192, 265, 326, 205, 277, 255, 268, 221, 35, 101, 307, 314, 180, 167, 203, 90, 144, 128, 494, 177, 32, 8, 20, 81, 7]. **Key-Dependent** [452]. **key-distribution** [20]. **Key-Exchange** [90, 8]. **Key-minimal** [28]. **Keys** [93, 485, 99]. **Keystream** [224, 191]. **Klimov** [298]. **knapsack** [37]. **Knowledge** [45, 115, 226, 51, 147, 166, 426, 448, 114, 273, 487, 70, 82, 116, 393, 138, 52, 390, 435, 477, 143, 414, 440, 494, 21, 72, 6, 74]. **Known** [279, 215]. **Known-in-Advance-IV** [279]. **Known-IV** [279].

Ladder [377]. **Lambert** [447]. **Language** [124]. **Language-Dependent** [124]. **Languages** [166, 393]. **Large** [135, 381]. **Laser** [373]. **Lattice** [409, 148]. **Layers** [469]. **Leakage** [433, 500, 503]. **Leakage-Resilient** [433, 503]. **Learning** [330]. **Least** [468]. **Length** [254, 141]. **Less** [217, 376]. **Levenshtein** [41]. **Levin** [242]. **Lightweight** [428]. **Like** [483, 459, 318, 43]. **Limitations** [272]. **Limits** [497]. **Line** [109, 236, 410]. **Line/Off** [109]. **Linear** [466, 107, 16, 309, 15, 23]. **linear-complexity** [23]. **Linking** [129]. **Local** [505, 47]. **Locality** [340, 421]. **Locally** [123, 237]. **Log** [146, 287, 139]. **Logarithm** [358, 184, 366, 457, 253, 420, 165, 342, 21]. **Logarithms** [190, 188, 55]. **Logic** [427]. **Long** [364]. **Long-Term** [364]. **Look** [285]. **Lossy** [506, 416]. **Low** [480, 136, 366, 111, 201, 283, 256, 15]. **low-order** [15]. **Lower** [338, 312, 76]. **Luby** [156]. **Luby-Rackoff** [156]. **Lucifer** [108].

MAC [183, 485]. **MACs** [254]. **mail** [36]. **Maintaining** [174]. **Majority** [478]. **Malicious** [357, 403, 450, 472, 501]. **Malleable** [371, 343]. **Man** [214]. **Man-in-the-Middle** [214]. **Mansour** [509, 462]. **Mapping** [184, 198]. **Mappings** [102, 97]. **Matching** [357, 450]. **matrix** [20]. **Matroid** [142]. **Maximum** [182]. **May** [495]. **McEliece** [490]. **MD2** [347]. **MD4** [153]. **Median** [355]. **meet** [18]. **Memory** [112, 130, 318, 58]. **Menezes** [146]. **Menezes-Okamoto-Vanstone** [146]. **Mercurial** [426]. **Merkle** [400]. **Mesh** [510]. **Message** [452, 223, 480, 119, 397, 322, 126, 159]. **Message-Efficient** [119]. **Messages** [254, 76]. **Methods** [24]. **Middle** [214, 18]. **Minimal** [250, 172, 503, 66, 28]. **Minimization** [427]. **Minimize** [487]. **Mining** [216]. **Minority** [45]. **missing** [15]. **ML** [66]. **ML-sequences** [66]. **Mode** [208]. **Model** [504, 291, 235, 455, 424, 303, 332, 145, 237]. **Models** [443, 172, 383, 494]. **Modes** [140, 163, 290, 279, 322]. **Modifications** [78]. **Modular** [225, 351, 79]. **Modules** [203]. **Monopoly** [188]. **Montgomery** [377]. **MOV** [252]. **Multi** [264, 241, 451, 250, 260, 455, 401]. **Multi-Exponentiation** [264]. **Multi-Party** [241, 250, 260]. **Multi-Property** [451]. **Multi-string** [455]. **Multi-Verifier** [401]. **Multicast** [313, 197]. **Multipartite**

[404, 333]. **Multiparty** [45, 478, 176, 173, 339, 464]. **Multiple** [140, 279, 69, 120]. **Multiplication** [447, 151]. **Multiplicative** [363]. **multiplier** [79]. **Multisignatures** [429]. **Must** [135]. **Mutual** [374]. **Mutually** [137].

Nearly [242]. **Necessary** [98]. **Negligible** [220]. **Neighbor** [313]. **Networks** [276, 105, 107, 313]. **NMAC** [488]. **Non** [471, 189, 241, 408, 324, 343, 371, 487, 326, 477, 332, 441]. **Non-** [441]. **Non-abelian** [326, 408]. **Non-Adaptive** [241, 471]. **Non-hyperelliptic** [324]. **Non-Interactive** [189, 487, 477, 332]. **Non-Malleable** [371, 343]. **Nonces** [215]. **Noncommutative** [479]. **Noncommutative-Algebraic** [479]. **Noninteractive** [115, 138]. **Nonlinear** [375, 103, 182]. **Nonlinearity** [92]. **nonuniform** [75]. **Normal** [263]. **Note** [284, 220, 67, 425, 435]. **Notions** [320, 321, 269]. **NP** [116, 138, 143, 414]. **NTRU** [330]. **Number** [379, 298, 78, 38]. **Numbers** [4, 233, 101].

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

Paillier [219, 213]. **Pairing** [248, 247, 352, 244, 337]. **Pairing-Based** [248, 337]. **Pairing-Friendly** [352]. **Pairs** [94]. **Paradigm** [320, 348]. **Parallel** [356, 228, 414, 395, 155]. **Parallelepiped** [330]. **Parameters** [101, 100]. **Partial** [258, 392, 265]. **Partially** [215]. **Party** [241, 272, 250, 260, 392, 282, 228, 331, 472, 411]. **Password** [289, 437, 268, 13]. **Password-Authenticated** [268]. **Password-Based** [289, 437]. **Passwords** [275, 307]. **Pattern** [357, 450]. **Patterns** [167]. **DEM** [308]. **Go** [224]. **Off-Line** [109]. **secrecy** [39, 9]. **Perfect** [74, 173, 477, 143, 21, 63, 57, 38]. **Perfectly** [405]. **Periods** [66]. **permit** [22]. **Permutation** [115, 134, 131, 107, 400, 143]. **Permutations** [115, 270, 432, 459, 209, 156, 211, 441, 40]. **permuted** [61]. **PGM** [64]. **PGV** [361]. **pipelined** [79]. **PIR** [240]. **Plaintext** [443]. **Plaintext-Aware** [443]. **plaintexts** [26]. **Player** [173]. **Point** [449]. **Pollard** [398]. **Polynomial** [136, 184, 286, 345, 430, 315, 423, 485, 479, 263, 38]. **Polynomial-Based** [485]. **Polynomial-Time** [286, 345, 315, 479]. **polynomials** [66]. **Possibility** [382]. **Possible** [454]. **Power** [114]. **Powering** [251]. **Practical** [396, 51, 259, 507, 106, 445, 461, 305, 419, 365, 169, 177]. **Practical-Time** [461]. **Predicate** [242, 423]. **Predicates** [200]. **Preface** [257, 53, 171, 234, 243]. **Preimage** [508]. **Preparation** [391]. **Preprocessing** [240, 114, 122]. **Prescribed** [211]. **Presence** [174, 403, 450, 168, 472, 375]. **Preserving** [513, 499, 216]. **Primality** [297, 281]. **Prime** [4, 252, 359, 101, 227]. **Prime-Order** [359]. **Primitive** [124, 378]. **Primitives** [270, 250, 305, 145]. **PRINCE** [483]. **PRINCE-Like** [483]. **Privacy** [230, 129, 84, 216, 313]. **Private** [466, 295, 276, 193, 391, 269, 302, 240]. **Private-Key** [269]. **Privately** [354].

Probabilistic [345, 269, 313, 23]. **Probability** [224, 18, 309]. **Probable** [227]. **Probably** [4]. **Problem** [486, 146, 341, 5, 253, 74, 420, 477, 165, 342]. **Problems** [354, 229, 358, 304, 479]. **Procedure** [274]. **processing** [35, 36]. **produced** [15]. **Product** [327, 22]. **Products** [423]. **profile** [23]. **Programmable** [406]. **Projective** [397]. **Promised** [111]. **Proof** [45, 278, 443, 74, 82, 116, 111, 138, 331, 255, 86]. **Proofs** [292, 325, 488, 226, 51, 189, 166, 114, 178, 487, 315, 393, 390, 435, 431, 72, 6]. **Properties** [316, 82, 112, 60, 64, 58]. **Property** [451]. **Protect** [192]. **Protected** [164]. **Protocol** [117, 245, 331, 472, 319, 351, 90, 157, 17, 33, 87]. **Protocols** [353, 45, 478, 176, 241, 448, 273, 386, 496, 357, 303, 288, 356, 501, 395, 86]. **Provable** [480, 285, 95]. **Provably** [399, 106, 118, 214, 57]. **Provably-Secure** [399, 57]. **Providers** [193]. **Proving** [297]. **Proxy** [394]. **Pseudo** [253, 305, 350, 222, 211]. **Pseudo-Free** [350]. **Pseudo-Random** [253, 222, 211]. **Pseudo-Randomness** [305]. **Pseudorandom** [471, 131, 225, 121, 47, 476, 156]. **Pseudorandomness** [48]. **Public** [490, 102, 446, 294, 383, 326, 277, 221, 101, 314, 414, 180, 203, 144, 494, 32]. **Public-Coin** [414]. **Public-Key** [102, 446, 294, 383, 277, 101, 180, 144, 494, 32]. **PUF** [378]. **Purely** [144]. **Purposes** [349].

Quadratic [281, 111, 190, 274, 180, 90, 8]. **Quantum** [466, 278, 323, 391, 407, 255, 177, 54]. **Quark** [428]. **Quaternion** [194]. **Question** [197]. **Quietly** [486].

Rabin [178]. **Rackoff** [156]. **radix** [79]. **Random** [456, 379, 4, 123, 329, 164, 310, 387, 259, 110, 253, 497, 233, 429, 222, 211, 307, 481, 441, 59, 38, 23]. **Randomize** [413]. **Randomize-Hash-then-Sign** [413]. **randomized** [57]. **Randomizer** [235]. **Randomness** [175, 305, 47]. **Ranks** [355]. **rate** [63]. **Rational** [370]. **RC4** [441]. **Re** [388]. **Re-Encryption** [388]. **Real** [380, 274, 183, 90]. **Real-Quadratic-Field-Based** [274]. **Real-Time** [183]. **Realistic** [353]. **Rebound** [453, 470]. **Receiver** [158]. **Recipient** [5]. **Reconciliation** [129]. **Reconciling** [212, 301]. **Reconsidered** [218]. **Recovery** [509, 265, 438]. **Recursive** [469]. **Reduced** [261, 465, 445, 453]. **Reducing** [240, 335]. **Reduction** [148]. **Reductions** [123, 304]. **Reflection** [483]. **Registers** [130]. **Related** [93, 461]. **Related-Key** [461]. **Relation** [316]. **Relations** [456, 320]. **Relationships** [321]. **Release** [106]. **Reliability** [313]. **Remaindering** [168]. **remarks** [61]. **Remote** [391]. **Repetition** [395]. **Replayed** [279]. **Replayed-and-Known-IV** [279]. **Requirements** [391]. **Residuosity** [111]. **Resilient** [433, 503, 103]. **Resistance** [488]. **Resistant** [107, 376]. **Resource** [386, 391]. **Restricted** [345]. **Results** [382, 2, 383, 312, 23]. **Retrievability** [431]. **Retrieval** [466, 295, 193, 240]. **Revisited** [316, 156, 440, 395]. **Rho** [398]. **Rights** [394]. **Ring** [329, 510, 424, 378]. **rings** [66]. **RIPEMD** [125, 515]. **RIPEMD-128** [515]. **Rivest** [37, 195]. **RMAC** [265]. **Robust** [295, 451, 181, 299]. **Rotational** [453]. **Round** [297, 291, 445, 125, 474, 116, 245, 393, 437, 228, 435]. **Round-Optimal** [437]. **Round-Reduced** [445]. **Rounds** [261, 468, 217]. **Routing** [458]. **RSA** [229, 495, 136, 286, 56, 127, 178, 238, 186, 181, 300, 299, 62, 350, 99]. **RSA-Based** [186, 300]. **RSA-OAEP** [238]. **RSA-signatures** [56]. **Runtime** [430].

SAFER [187, 152]. **Sample** [204]. **SASAS**

[360]. **Scalable** [288]. **Scalar** [447]. **Scheme** [229, 147, 294, 462, 149, 400, 255, 169, 55, 61, 20, 69]. **Schemes** [506, 399, 498, 325, 96, 170, 394, 46, 134, 132, 509, 404, 500, 343, 371, 418, 213, 280, 304, 142, 158, 118, 120, 137, 206, 485, 481, 256, 122, 63, 77, 81, 65, 25]. **Schnorr** [122]. **SDH** [310]. **Search** [354, 496, 192, 155]. **Searchable** [316]. **Searching** [302]. **Second** [508]. **Second-Preimage** [508]. **secrecy** [28, 57, 19]. **Secret** [370, 363, 498, 96, 147, 46, 73, 286, 106, 404, 110, 142, 362, 120, 137, 464, 293, 333, 63, 77, 69, 65, 11]. **Secret-Sharing** [498]. **Secrets** [120]. **Secure** [17, 506, 355, 514, 399, 389, 45, 296, 394, 294, 373, 484, 106, 348, 408, 105, 500, 117, 250, 119, 172, 416, 238, 418, 287, 417, 260, 392, 50, 282, 450, 419, 118, 214, 303, 262, 191, 228, 277, 339, 390, 411, 472, 378, 101, 249, 375, 246, 197, 57, 22]. **Securely** [388]. **Securing** [210]. **Security** [452, 353, 292, 490, 379, 229, 325, 488, 164, 278, 443, 446, 176, 241, 368, 134, 178, 493, 413, 496, 225, 290, 357, 321, 269, 315, 356, 217, 285, 331, 255, 206, 364, 222, 95, 185, 481, 169, 232, 61, 13]. **Selecting** [205]. **Selective** [387, 382]. **Self** [312]. **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]. **Set-Up** [272]. **Sets** [426]. **Setting** [446]. **SHA** [465]. **SHA-0** [465]. **SHA-1** [465]. **Shamir** [298]. **Shannon** [10]. **Share** [135, 11]. **shares** [77]. **Sharing** [370, 363, 498, 96, 46, 404, 181, 299, 142, 120, 137, 464, 293, 333, 63, 77, 73, 69, 65]. **Shift** [130]. **Short** [247, 310, 189, 412, 384, 307, 99]. **Should** [354, 463]. **Shpilrain** [319]. **Shuffle** [362]. **Side** [376]. **Side-Channel** [376]. **Sided** [242]. **sieve** [78]. **Sign** [413]. **Signature** [229, 325, 394, 134, 149, 500, 280, 304, 206, 215, 481, 49, 122]. **Signatures** [506, 513, 499, 329, 467, 247, 310, 510, 433, 412, 194, 507, 106, 132, 109, 273, 413, 186, 300, 429, 384, 330, 185, 401, 56]. **Signcryption** [292]. **Significance** [91, 27]. **Signing** [394]. **Simple** [513, 400]. **Simpler** [277, 307]. **Simplicity** [121]. **Simulation** [449, 493, 496, 173, 321, 315, 477]. **Simulation-Based** [493, 496, 321, 315]. **Single** [474, 131, 422]. **Single-Key** [474, 422]. **Six** [217]. **Size** [513, 135, 77]. **Sizes** [205]. **Skein** [453]. **Skipjack** [261]. **Slender** [415]. **Slender-Set** [415]. **Slidex** [462]. **Sliding** [251]. **Small** [505, 136, 252, 420, 151, 161]. **Small-Bias** [505]. **Smart** [49]. **Smooth** [397]. **Software** [154, 30]. **Software-Optimized** [154]. **Solutions** [136, 479]. **Solve** [354]. **Some** [63, 61, 3]. **Sound** [395]. **Soundness** [212, 301, 86]. **Sources** [183]. **Spaces** [204]. **Span** [130]. **Specified** [355]. **splitting** [39]. **Spreading** [486]. **spreads** [16]. **SRAM** [373]. **SRAM-Based** [373]. **stamp** [34]. **Standard** [504, 467, 2]. **State** [391, 438]. **States** [407]. **Statistical** [226, 59]. **Statistically** [132, 335]. **Statistically-Hiding** [335]. **Stealthy** [436]. **Steganography** [338]. **Stegosystem** [439]. **Stop** [132, 224]. **Stop/Go** [224]. **Storage** [291, 105, 235, 236, 332, 237]. **Storage-Bounded** [236]. **Strategies** [443, 315]. **Stream** [380, 441, 438, 182, 41, 14, 58]. **Streaming** [302]. **Strengthening** [273]. **Stretch** [164]. **String** [323, 455]. **Strong** [449, 236, 33]. **Stronger** [329, 178]. **Strongly** [65]. **Structural** [360, 314, 139]. **Structure** [513, 499, 84, 211]. **Structure-Preserving** [513, 499]. **Structured** [29]. **Structures** [173]. **Study** [374, 13]. **Subexponential** [146]. **Subgroup** [486]. **Subliminal** [166]. **Subliminal-Free** [166]. **Subset** [118]. **Subspace** [470]. **Substitution** [107].

Substitution-Permutation [107]. **Subtleties** [463]. **Success** [309]. **Sufficient** [98]. **Suggestion** [345]. **Sum** [118]. **Summation** [179]. **Sums** [164]. **Supersingular** [246]. **Supporting** [423]. **Symbolic** [368]. **Symmetric** [418, 85]. **Symmetries** [457]. **System** [74, 111, 138, 271, 8, 7]. **Systems** [45, 82, 116, 50, 128, 87].

Tag [308]. **Tag-KEM** [308]. **Tag-KEM/DEM** [308]. **Takeover** [436]. **Taxonomy** [352]. **technique** [33]. **Techniques** [264, 427]. **Telephony** [461]. **Term** [364]. **Test** [281, 227, 59]. **Tests** [242, 75]. **Text** [496]. **TF** [298]. **TF-1** [298]. **Their** [289, 345, 406, 204, 91, 99, 80]. **Theorem** [442, 425]. **Theorems** [327]. **Theoretic** [514, 295, 104, 25]. **Theoretical** [298]. **Theory** [232]. **Thompson** [319]. **Three** [254, 324, 87]. **Three-Key** [254]. **Threshold** [268, 210, 293]. **Tight** [304, 481]. **Tightly** [506]. **Tillich** [369]. **Time** [399, 286, 461, 345, 380, 315, 439, 180, 183, 479, 34]. **Time-Bound** [399]. **time-stamp** [34]. **Timestamping** [332]. **Timing** [303]. **TLS** [351]. **Tolerance** [175]. **Tolerating** [45]. **Toolbox** [148]. **Toss** [478, 502]. **Tossing** [228]. **Trace** [165]. **Tracing** [202, 256]. **Trade** [323]. **Trade-Offs** [323]. **Tradeoff** [434, 444]. **Trading** [226]. **Traffic** [480]. **Traitor** [202, 256]. **Transfer** [160, 296, 291, 117, 417, 397, 390, 411, 249]. **Transfers** [230]. **Translucent** [160]. **Trapdoor** [115, 219, 289, 416, 432, 271]. **Trapdoors** [221]. **Treatment** [70]. **tree** [402]. **Trees** [409]. **Tripartite** [245]. **Triple** [163, 150]. **Triplets** [94]. **Trusted** [137]. **Tweakable** [385]. **Twin** [341]. **Two** [212, 301, 272, 150, 125, 392, 397, 282, 228, 331, 472, 151, 33, 411]. **Two-Key** [150]. **Two-Message** [397]. **Two-Party** [272, 392, 282, 228, 331, 472]. **Two-Round** [125]. **two-way** [33]. **Type** [327]. **Types** [93].

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

Vanstone [146, 447]. **Variant** [400]. **Varieties** [337]. **vectors** [35]. **Verifiable** [456, 362, 464]. **Verifiably** [429]. **Verification** [412]. **Verifier** [401]. **versus** [276, 175, 241]. **Very** [498, 227]. **via** [160, 297, 411]. **View** [514, 282]. **Views** [212, 301]. **Visual** [170]. **Vulnerabilities** [136]. **Vulnerability** [83].

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

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

Yao [331].

Zémor [369]. **Zero** [45, 115, 226, 51, 147, 166, 426, 448, 114, 6, 273, 487, 74, 70, 82, 116, 393, 138, 52, 390, 435, 477, 143, 414, 440, 21, 72]. **Zero-Knowledge** [45, 115, 226, 51, 147, 166, 426, 448, 114, 273, 487, 70, 82, 116, 393, 138,

52, 390, 435, 477, 143, 6, 74, 21, 72].

References

Brickell:1988:E

[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, ???? 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 Cryptology: 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. *Jour-*

nal 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 Cryptol-*

ogy: 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. Certify-

ing 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 Crypto-*

logic 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 Cryptologic 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 Association 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 Cryptology: 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 cryp-

tographic 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 International 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. Securing 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 Interna-*

tional 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 — computation 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 pseudorandom 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 Interna-*

tional 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. Pri-

vate 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 encryp-

tion: 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 commitment. *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, Khoong-ming 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 Cryptology: 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 amplification 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. *Journal 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 Cryptology: 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 Interna-*

tional 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 crypt-

analysis 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. CODEN 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. *Jour-*

nal 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 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.