

A Bibliography of Papers in *Lecture Notes in Computer Science* (1990)

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, beebe@ieee.org (Internet)
WWW URL: <http://www.math.utah.edu/~beebe/>

29 July 2017
Version 1.10

Title word cross-reference

$2n$ [13]. $\text{Step}_{k,m}$ [67]. N [99, 13]. P [71].

-Bit [13]. -Cascades [67]. -Dimensional [99].

Abstract

[62, 21, 98, 107, 104, 54, 31, 100, 17, 10, 75, 85, 120, 86, 128, 111, 68, 127, 69, 36, 115, 41].

Abuse [75]. Abuse-Free [75]. Access [102, 64]. Active [32]. Addition [110].

Adolescence [1]. Age [61]. Agent [125].

Algebraic [63]. Algebraic-Code [63].

Algorithm [109, 88]. Algorithms [13, 28].

Alive [6]. Almost [60]. Alternative [19].

and/or [44]. Antique [94]. Any [10, 115].

Application [43]. Applications

[121, 123, 17, 116, 111, 89]. Architecture [106]. Argued [21]. Atkin [59]. Attack [56, 132, 88]. Attacks [32]. Authentications [92, 46, 65, 2, 48, 78, 12]. Authenticity [116]. Author [73, 134]. Avalanche [9].

Based [92, 40, 104, 10, 5, 99, 109, 127].

Batch [90]. Be [51, 21]. Binary [70]. Bit [76, 86, 13]. Bits [123, 24]. Block [13, 115]. Bounded} [21]. Bounds [12]. Boxes [129]. Break [37]. Bronze [61]. Brujin [52].

Call [132, 28]. Can [51, 21, 83]. Can't [51].

Card [23]. Cards [68, 95]. Cartesian [46].

Cascades [67]. Case [61]. Cash [30, 116].

Certain [70]. Certified [94]. Chain [110].

Checks [31, 30]. **Checksum** [88]. **Children** [133]. **Chip** [24]. **Chosen** [88]. **Cipher** [58, 13]. **Ciphers** [115]. **Classification** [98]. **Code** [63]. **Codes** [12]. **Cohen** [88]. **Collision** [43, 111]. **Commitment** [76, 86]. **Communication** [103]. **Commutative** [16]. **Complexity** [51, 118, 57, 70, 54, 50, 55]. **Computation** [124]. **Computational** [22]. **Computationally** [69]. **Computations** [125]. **Computer** [6, 130]. **Concrete** [118]. **Conditionally** [75]. **Conditions** [70]. **Confidential** [64]. **Congruential** [87]. **Consistency** [89]. **Constructing** [41]. **Construction** [115]. **Context** [75]. **Continued** [55]. **Control** [102, 44]. **Controlled** [123]. **Convert** [130]. **Correlation** [56]. **Counting** [9]. **Crete** [61]. **Criteria** [53]. **Criterion** [9]. **Cross** [99]. **Cross-Product** [99]. **Cryptanalysis** [40, 67, 39, 36, 89]. **Cryptel** [25]. **Crypto** [81]. **Crypto-Engine** [81]. **Cryptographers** [69]. **Cryptographic** [53, 88, 80, 28]. **Cryptographically** [125]. **Cryptography** [77, 1]. **Cryptoperiods** [14]. **Cryptosystem** [72, 4, 114, 132]. **Cryptosystems** [91, 71, 75, 101, 63, 7]. **Curve** [72, 91]. **Curves** [40].

Data [131]. **DC** [33]. **Deciphering** [61]. **Deficiencies** [18]. **Defined** [52]. **Definition** [99]. **Describe** [51]. **Design** [71, 112]. **Detection** [33]. **Diffusing** [14]. **Digital** [92, 97, 94, 103]. **Dimensional** [99]. **Dining** [69]. **Direct** [37]. **Disclose** [17]. **Disclosure** [123]. **Disco** [69]. **Diskette** [81]. **Disposable** [116]. **Disrupters** [33]. **Distributed** [27, 130]. **Distribution** [10, 103, 105]. **Distributions** [85]. **Divergence** [12]. **Diversity** [60]. **Divertible** [16]. **Domains** [100]. **Double** [125]. **Double-Agent** [125]. **Dynamic** [99].

Easy [129, 43, 111]. **Efficiency** [57]. **Efficient** [117, 31, 128, 68, 95, 127, 23]. **Electronic** [31, 25, 35, 116]. **Elliptic** [72, 91]. **Encryption** [40, 78, 106]. **End** [106]. **End-to-End** [106]. **Engine** [81]. **Enigma** [74]. **European** [28]. **Evaluation** [28]. **Every** [50]. **Everything** [21]. **Exchange** [126, 57, 104, 65, 5]. **Existence** [76]. **Existing** [25]. **Explain** [133]. **Exponent** [11]. **Exponentiation** [108]. **Exponents** [36]. **Extended** [62, 21, 98, 104, 54, 31, 100, 10, 75, 85, 120, 86, 43, 64, 127, 22, 115, 41].

Facing [29]. **Factoring** [35]. **Fast** [72, 56, 60, 109]. **Faster** [62]. **Faulty** [124, 122]. **FEAL** [132]. **FEAL-** [132]. **Feed** [56]. **Feed-Forward** [56]. **Feedback** [54, 83, 66]. **Feedforward** [52]. **Fiat** [19]. **Fields** [104]. **Filling** [40]. **Filtered** [56]. **Find** [129]. **Five** [23]. **Flexible** [102]. **Forward** [56]. **Fractions** [7, 55]. **Free** [75]. **Front** [59]. **Full** [65]. **Function** [10]. **Functions** [52, 112, 9, 53, 113, 13].

Gamal [4]. **General** [15, 75]. **Generalization** [4]. **Generate** [83]. **Generation** [49, 60]. **Generator** [42]. **Generators** [87]. **German** [74]. **Given** [83]. **Giving** [18]. **Good** [129, 50]. **Gradual** [123]. **Group** [8].

Half [122]. **Hardware** [107]. **Hash** [112, 113, 13]. **Hash-Functions** [13]. **Heuristics** [110]. **High** [63]. **Higher** [9, 109]. **Hints** [18]. **Homophonic** [38]. **Huang** [88]. **Hypotheses** [115].

Ideal [98, 45]. **Identification** [117, 68, 95, 127]. **Identity** [5]. **Identity-Based** [5]. **If** [51]. **Implementation** [91, 37]. **Implementations** [107]. **Impossibility** [41]. **Improve** [3]. **Improved** [58]. **Index** [73, 134]. **Infinite** [100]. **Information** [63, 38]. **Information-Theoretic** [38].

Informational [12]. **Integrity** [28].
Interactive [117, 16, 121, 92]. **Invited**
 [29, 81, 77, 107, 1, 61, 79, 34, 74, 78, 44, 80].
Keep [6]. **Kerberos** [78]. **Kernels** [127].
Key [126, 58, 57, 104, 10, 1, 65, 2, 48, 5, 63,
 7, 4, 103, 105]. **Key-Exchange** [5]. **Keying**
 [74]. **Keys** [102]. **Keystream** [50].
Knowledge [92, 118, 18, 21, 20, 15, 76, 119,
 120, 16, 116, 133, 64, 22].
Large [8]. **Later** [79]. **LCT** [89]. **Legal** [29].
Line [97]. **Line/Off** [97]. **Linear**
 [70, 54, 99, 50, 55, 89, 61]. **linearity** [11].
Local [84].
Machine [39]. **Mail** [25, 35]. **Majorities**
 [125]. **Majority** [124]. **Making** [75, 23].
Mapping [34]. **Master** [102]. **Match** [23].
Match-Making [23]. **Maximal** [60].
Medical [64]. **Message** [92]. **Minimal** [48].
Minimum [120]. **Minorities** [125]. **MIXes**
 [37]. **Mobile** [103]. **Modified** [88, 39].
Modular [108, 109].
Modular-Multiplication [109]. **Moduli**
 [60]. **Multiparty** [124, 122, 125]. **Multiple**
 [58]. **Multiplication** [109].
Navy [74]. **Network** [6, 78]. **Networks**
 [77, 8]. **News** [59]. **No** [47, 65]. **Non**
 [121, 92, 11]. **Non-interactive** [121, 92].
Non-linearity [11]. **Nonlinearity** [53].
Nonlinearly [56]. **Normal** [77]. **NP** [21].
Number [21].
Oblivious [121]. **Offline** [31]. **On-Line** [97].
On-Line/Off-Line [97]. **One** [10, 113].
One-Way [10]. **Online** [30]. **Open** [27].
Optimally [41]. **Order** [9]. **Oriented** [8].
Paper [94]. **Paradigms** [92]. **Parallel** [49].
Password [79]. **Off-Line** [97]. **or** [44].
Perfect [84, 21]. **Periodic** [82].
Permutation [71]. **Permutations** [11, 41].
Permuted [127]. **Personal** [81]. **PGM**
 [114]. **Point** [50, 26]. **Power** [22]. **Practical**
 [18, 25, 8, 80]. **Predict** [87]. **Prepositioned**
 [44]. **Previously** [65]. **Primality** [62].
Primitives [28]. **Principle** [112]. **Private**
 [63]. **Private-Key** [63]. **Problem** [125].
Problems [77, 80]. **Procedures** [64].
Processing [27, 130]. **Processor** [24].
Processors [122]. **Product** [99]. **Profile**
 [50]. **Profiles** [70, 55]. **Progress** [131].
Proofs [92, 117, 118, 18, 76, 119, 120, 16, 22].
Properties [114]. **Protection** [25, 128, 80].
Protocol [33, 8, 5, 19, 103]. **Protocols**
 [122, 126, 133]. **Provably** [115]. **Prover**
 [117]. **Providing** [77]. **Pseudo**
 [51, 84, 86, 42]. **Pseudo-random** [51, 84].
Pseudo-randomness [86]. **Pseudorandom**
 [85, 41]. **Public** [1, 2, 7, 4]. **Public-Key**
 [1, 2, 7].
Quadratic [104, 82].
Race [28]. **Radix** [109]. **Random**
 [123, 34, 16, 42, 51, 84]. **Randomness**
 [84, 86]. **Rates** [63]. **Real** [104]. **Recipient**
 [69, 32]. **Records** [64]. **Recurring** [49].
Recursive [108]. **Reducibility** [16].
Register [56, 83]. **Registers** [54, 66].
Relying [115]. **Requirements** [29].
Residues [108]. **Resource** [120]. **Results**
 [111, 41]. **RIPE** [28]. **Rotor** [39]. **Rounds**
 [21, 119]. **RSA** [107, 90, 60, 37, 24, 36].
RSA-Implementation [37]. **RSA-Moduli**
 [60].
S [129]. **S-Boxes** [129]. **Satisfiability** [23].
Satisfying [9]. **Say** [47]. **Scheme**
 [58, 15, 2, 99, 128, 127, 80, 96]. **Schemes**
 [117, 3, 98, 45, 123, 76, 46, 44]. **Schnorr** [42].
Scripts [61]. **SDNS** [106]. **Search** [43, 111].
Secrecy [48]. **Secret**
 [126, 98, 45, 100, 44, 36]. **Secrets** [17, 65].
Secure [125, 75, 65, 2, 60, 69, 115].
Security [77, 79, 131, 42, 27, 26]. **Self** [16].

Self-Reducibility [16]. **Sender** [69, 32]. **Sequence** [51, 83]. **Sequences** [51, 70, 82, 52, 56, 49, 84, 50]. **Serviceability** [69]. **Shamir** [19]. **Shared** [65, 44, 96]. **Sharing** [98, 45, 100]. **Shift** [56, 83, 66]. **Shift-Register** [56]. **Short** [36]. **Shortest** [83]. **Signature** [29, 3, 94, 96]. **Signatures** [92, 93, 97, 68, 95]. **Simple** [14]. **Single** [24]. **Smart** [81, 68, 95]. **Software** [128]. **Some** [45, 70]. **Sorting** [20]. **Space** [40, 99]. **Space-Filling** [40]. **Spans** [82]. **Sparse** [85]. **spite** [32]. **Spymasters** [125]. **Standardisation** [131]. **Starting** [50, 26]. **Statistics** [34]. **Strict** [9]. **Structure** [126]. **Substitution** [38]. **Subtitle** [94]. **Summary** [43, 64, 22]. **Sums** [108]. **Survey** [107]. **Symmetric** [13]. **System** [57, 104, 25, 10]. **Systems** [48, 103, 105].

Technical [26]. **Technique** [14]. **Technology** [29]. **Ten** [79]. **Test** [59, 89]. **Testing** [62]. **Text** [88]. **Their** [123, 116]. **Theoretic** [38]. **Threshold** [101, 99]. **Token** [81]. **Tolerating** [122]. **Transfer** [121]. **Treatment** [38]. **Trick}** [23]. **Two** [117, 119]. **Type** [71].

Unclassified [77]. **Unconditional** [48, 69, 32]. **Unconditionally** [125, 75]. **Undeniable** [93]. **Universal** [81]. **UNIX** [79]. **Unproved** [115]. **Untraceability** [69, 32]. **Untraceable** [116]. **Use** [77, 7, 78]. **User** [81]. **Using** [117, 18, 108, 86, 13].

Varying [66]. **Verifiable** [17]. **Verification** [96]. **Video** [40]. **Viruses** [130]. **Voting** [58].

Way [10, 113].

Years [79].

Zero [92, 118, 18, 21, 20, 15, 76, 119, 120, 16, 116, 133, 64, 22]. **Zero-Knowledge** [118, 18,

21, 20, 15, 76, 120, 116, 133, 64, 22].

References

Diffie:1990:APK

- [1] Whitfield Diffie. The adolescence of public-key cryptography (invited). *Lecture Notes in Computer Science*, 434: 2-??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340002.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340002.pdf>.

Galil:1990:SPK

- [2] Zvi Galil, Stuart Haber, and Moti Yung. A secure public-key authentication scheme. *Lecture Notes in Computer Science*, 434:3-??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340003.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340003.pdf>.

Brassard:1990:HIS

- [3] Gilles Brassard. How to improve signature schemes. *Lecture Notes in Computer Science*, 434:16-??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340016.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340016.pdf>.

Jaburek:1990:GGP

- [4] W. J. Jaburek. A generalization of El Gamal's public key cryptosystem. *Lecture Notes in Computer Science*, 434:23–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340023.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340023.pdf>.

Gunther:1990:IBK

- [5] Christoph G. Günther. An identity-based key-exchange protocol. *Lecture Notes in Computer Science*, 434:29–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340029.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340029.pdf>.

Bauspiess:1990:HKA

- [6] Fritz Bauspieß and Hans-Joachim Knobloch. How to keep authenticity alive in a computer network. *Lecture Notes in Computer Science*, 434:38–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340038.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340038.pdf>.

Isselhorst:1990:UFP

- [7] Hartmut Isselhorst. The use of fractions in public-key cryptosystems. *Lecture Notes in Computer Science*, 434:47–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340047.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340047.pdf>.

Lecture Notes in Computer Science, 434:47–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340047.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340047.pdf>.

Frankel:1990:PPL

- [8] Yair Frankel. A practical protocol for large group oriented networks. *Lecture Notes in Computer Science*, 434:56–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340056.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340056.pdf>.

Lloyd:1990:CFS

- [9] Sheelagh Lloyd. Counting functions satisfying a higher order strict avalanche criterion. *Lecture Notes in Computer Science*, 434:63–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340063.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340063.pdf>.

Davida:1990:KDS

- [10] George I. Davida, Yvo Desmedt, and René Peralta. A key distribution system based on any one-way function (extended abstract). *Lecture Notes in Computer Science*, 434:75–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340075.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340075.pdf>.

0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340075.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340075.pdf>.

Pieprzyk:1990:NLE

- [11] Józef P. Pieprzyk. Non-linearity of exponent permutations. *Lecture Notes in Computer Science*, 434:80–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340080.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340080.pdf>.

Sgarro:1990:IDB

- [12] Andrea Sgarro. Informational divergence bounds for authentication codes. *Lecture Notes in Computer Science*, 434:93–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340093.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340093.pdf>.

Quisquater:1990:BHF

- [13] Jean-Jacques Quisquater and Marc Girault. $2n$ -bit hash-functions using n -bit symmetric block cipher algorithms. *Lecture Notes in Computer Science*, 434:102–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/>

<bibs/0434/04340102.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340102.pdf>.

Mjolsnes:1990:STD

- [14] Stig F. Mjolsnes. A simple technique for diffusing cryptoperiods. *Lecture Notes in Computer Science*, 434:110–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340110.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340110.pdf>.

Burmester:1990:GZK

- [15] Mike V. D. Burmester, Yvo Desmedt, Fred Piper, and Michael Walker. A general zero-knowledge scheme. *Lecture Notes in Computer Science*, 434:122–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340122.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340122.pdf>.

Okamoto:1990:DZKa

- [16] Tatsuaki Okamoto and Kazuo Ohta. Divertible zero knowledge interactive proofs and commutative random self-reducibility. *Lecture Notes in Computer Science*, 434:134–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340134.htm>; <http://>

link.springer-ny.com/link/service/series/0558/papers/0434/04340134.pdf.

Crepeau:1990:VDS

- [17] Claude Crépeau. Verifiable disclosure for secrets and applications (abstract). *Lecture Notes in Computer Science*, 434:150–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340150.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340150.pdf>.

Boyar:1990:PZK

- [18] Joan Boyar, Katalin Friedl, and Carsten Lund. Practical zero-knowledge proofs: Giving hints and using deficiencies. *Lecture Notes in Computer Science*, 434:155–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340155.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340155.pdf>.

Stern:1990:AFS

- [19] Jacques Stern. An alternative to the Fiat–Shamir protocol. *Lecture Notes in Computer Science*, 434:173–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340173.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340173.pdf>.

Brassard:1990:SZK

- [20] Gilles Brassard and Claude Crépeau. Sorting out zero-knowledge. *Lecture Notes in Computer Science*, 434:181–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340181.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340181.pdf>.

Brassard:1990:ENC

- [21] Gilles Brassard, Claude Crépeau, and Moti Yung. Everything in NP can be argued in *Perfect* zero-knowledge in a *Bounded* number of rounds (extended abstract). *Lecture Notes in Computer Science*, 434:192–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340192.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340192.pdf>.

Yung:1990:ZKP

- [22] Moti Yung. Zero-knowledge proofs of computational power (extended summary). *Lecture Notes in Computer Science*, 434:196–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340196.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340196.pdf>.

denBoer:1990:MEM

- [23] Bert den Boer. More efficient match-making and satisfiability: *The Five Card Trick*. *Lecture Notes in Computer Science*, 434:208–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340208.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340208.pdf>.

Vandemeulebroecke:1990:SCB

- [24] André Vandemeulebroecke, Etienne Vanzieleghem, Tony Denayer, and Paul G. A. Jespers. A single chip 1024 bits RSA processor. *Lecture Notes in Computer Science*, 434:219–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340219.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340219.pdf>.

Cnudde:1990:CPP

- [25] Hedwig Cnudde. Cryptel — the practical protection of an existing electronic mail system. *Lecture Notes in Computer Science*, 434:237–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340237.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340237.pdf>.

VanAuseloos:1990:TSS

- [26] Jan Van Auseloos. Technical security: The starting point. *Lecture Notes in Computer Science*, 434:243–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340243.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340243.pdf>.

Siuda:1990:SOD

- [27] Charles Siuda. Security in open distributed processing. *Lecture Notes in Computer Science*, 434:249–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340249.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340249.pdf>.

Vandewalle:1990:ECC

- [28] Joos Vandewalle, David Chaum, Walter Fumy, Cees J. A. Jansen, Peter Landrock, and G. Roelofsen. A European call for cryptographic algorithms: RIPE: Race Integrity Primitives Evaluation. *Lecture Notes in Computer Science*, 434:267–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340267.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340267.pdf>.

Antoine:1990:LRF

- [29] Mireille Antoine, Jean-François Brake-land, Marc Eloy, and Yves Pouillet. Legal requirements facing new signature technology (invited). *Lecture Notes in Computer Science*, 434:273–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340273.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340273.pdf>.

Chaum:1990:OCC

- [30] David Chaum. Online cash checks. *Lecture Notes in Computer Science*, 434:288–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340288.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340288.pdf>.

Chaum:1990:EOE

- [31] David Chaum, Bert den Boer, Eugène van Heyst, Stig F. Mjøl̄snes, and Adri Steenbeek. Efficient offline electronic checks (extended abstract). *Lecture Notes in Computer Science*, 434:294–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340294.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340294.pdf>.

Waidner:1990:USR

- [32] Michael Waidner. Unconditional sender and recipient untraceability in spite of active attacks. *Lecture Notes in Computer Science*, 434:302–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340302.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340302.pdf>.

Bos:1990:DDD

- [33] Jurjen N. E. Bos and Bert den Boer. Detection of disrupters in the DC protocol. *Lecture Notes in Computer Science*, 434:320–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340320.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340320.pdf>.

Flajolet:1990:RMS

- [34] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics (invited). *Lecture Notes in Computer Science*, 434:329–354, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340329.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340329.pdf>; <http://www.research.att.com/~amo/doc/arch/random.mappings.pdf>; <http://www.research.att.com/~amo/doc/arch/random.mappings.ps>; <http://www.research.att.com/~amo/doc/arch/random.mappings.ps>.

research.att.com/~amo/doc/arch/
random.mappings.tex.

Jendal:1990:ITT

Lenstra:1990:FEM

- [35] Arjen K. Lenstra and Mark S. Manasse. Factoring by electronic mail. *Lecture Notes in Computer Science*, 434:355–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340355.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340355.pdf>.

Wiener:1990:CSR

- [36] Michael J. Wiener. Cryptanalysis of short RSA secret exponents (abstract). *Lecture Notes in Computer Science*, 434:372–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340372.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340372.pdf>.

Pfitzmann:1990:HBD

- [37] Birgit Pfitzmann and Andreas Pfitzmann. How to break the direct RSA-implementation of MIXes. *Lecture Notes in Computer Science*, 434:373–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340373.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340373.pdf>.

- [38] Hakon N. Jendal, Yves J. B. Kuhn, and James L. Massey. An information-theoretic treatment of homophonic substitution. *Lecture Notes in Computer Science*, 434:382–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340382.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340382.pdf>.

Wichmann:1990:CMR

- [39] Peer Wichmann. Cryptanalysis of a modified rotor machine. *Lecture Notes in Computer Science*, 434:395–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340395.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340395.pdf>.

Bertilsson:1990:CVE

- [40] Michael Bertilsson, Ernest F. Brickell, and Ingemar Ingemarsson. Cryptanalysis of video encryption based on space-filling curves. *Lecture Notes in Computer Science*, 434:403–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340403.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340403.pdf>.

Zheng:1990:IOR

- [41] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. Impossibility and optimally results on constructing pseudorandom permutations (extended abstract). *Lecture Notes in Computer Science*, 434:412–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340412.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340412.pdf>.

Rueppel:1990:SSP

- [42] Rainer A. Rueppel. On the security of Schnorr’s pseudo random generator. *Lecture Notes in Computer Science*, 434:423–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340423.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340423.pdf>.

Quisquater:1990:HECa

- [43] Jean-Jacques Quisquater and Jean-Paul Descaillie. How easy is collision search? application to DES (extended summary). *Lecture Notes in Computer Science*, 434:429–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340429.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340429.pdf>.

Simmons:1990:PSS

- [44] Gustavus J. Simmons. Prepositioned shared secret and/or shared control schemes (invited). *Lecture Notes in Computer Science*, 434:436–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340436.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340436.pdf>.

Brickell:1990:SIS

- [45] Ernest F. Brickell. Some ideal secret sharing schemes. *Lecture Notes in Computer Science*, 434:468–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340468.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340468.pdf>.

DeSoete:1990:CAS

- [46] Marijke De Soete, Klaus Vedder, and Michael Walker. Cartesian authentication schemes. *Lecture Notes in Computer Science*, 434:476–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340476.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340476.pdf>.

Beutelspacher:1990:HSN

- [47] Albrecht Beutelspacher. How to say “no”. *Lecture Notes in Computer Science*, 434:491–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340491.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340491.pdf>.

Godlewski:1990:KMA

- [48] Philippe Godlewski and Chris Mitchell. Key minimal authentication systems for unconditional secrecy. *Lecture Notes in Computer Science*, 434:497–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340497.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340497.pdf>.

Gunther:1990:PGR

- [49] Christoph G. Günther. Parallel generation of recurring sequences. *Lecture Notes in Computer Science*, 434:503–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340503.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340503.pdf>.

Niederreiter:1990:KSG

- [50] Harald Niederreiter. Keystream sequences with a good linear complexity profile for every starting point.

Lecture Notes in Computer Science, 434:523–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340523.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340523.pdf>.

Beth:1990:CPR

- [51] Thomas Beth and Zong-Duo Dai. On the complexity of pseudo-random sequences — or: If you can describe a sequence it can’t be random. *Lecture Notes in Computer Science*, 434:533–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340533.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340533.pdf>.

Dai:1990:FFD

- [52] Zong-Duo Dai and Kencheng Zeng. Feedforward functions defined by de brujin sequences. *Lecture Notes in Computer Science*, 434:544–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340544.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340544.pdf>.

Meier:1990:NCC

- [53] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. *Lecture Notes*

in *Computer Science*, 434:549–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340549.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340549.pdf>.

Chan:1990:LCP

- [54] Agnes Hui Chan, Mark Goresky, and Andrew Klapper. On the linear complexity of feedback registers (extended abstract). *Lecture Notes in Computer Science*, 434:563–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340563.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340563.pdf>.

Wang:1990:LCP

- [55] Muzhong Wang. Linear complexity profiles and continued fractions. *Lecture Notes in Computer Science*, 434:571–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340571.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340571.pdf>.

Forre:1990:FCA

- [56] Réjane Forré. A fast correlation attack on nonlinearly feed-forward filtered shift-register sequences. *Lecture Notes in Computer Science*, 434:

586–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340586.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340586.pdf>.

Buchmann:1990:CEN

- [57] Johannes A. Buchmann, Stephen Düllmann, and Hugh C. Williams. On the complexity and efficiency of a new key exchange system. *Lecture Notes in Computer Science*, 434:597–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340597.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340597.pdf>.

Boyd:1990:NMK

- [58] Colin Boyd. A new multiple key cipher and an improved voting scheme. *Lecture Notes in Computer Science*, 434:617–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340617.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340617.pdf>.

Morain:1990:ATN

- [59] François Morain. Atkin’s test: News from the front. *Lecture Notes in Computer Science*, 434:626–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340626.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340626.pdf>.

Maurer:1990:FGS

- [60] Ueli M. Maurer. Fast generation of secure RSA-moduli with almost maximal diversity. *Lecture Notes in Computer Science*, 434:636–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340636.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340636.pdf>.

Duhoux:1990:DBA

- [61] Yves Duhoux. Deciphering Bronze Age scripts of Crete — the case of Linear A (invited). *Lecture Notes in Computer Science*, 434:649–650, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340649.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340649.pdf>.

Bosma:1990:FPT

- [62] Wieb Bosma and Marc Paul van der Hulst. Faster primality testing (extended abstract). *Lecture Notes in Computer Science*, 434:652–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340652.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340652.pdf>.

<http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340652.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340652.pdf>.

Hwang:1990:PKA

- [63] Tzonelih Hwang and T. R. N. Rao. Private-key algebraic-code cryptosystems with high information rates. *Lecture Notes in Computer Science*, 434:657–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340657.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340657.pdf>.

Quisquater:1990:ZKP

- [64] Jean-Jacques Quisquater and André Bouckaert. Zero-knowledge procedures for confidential access to medical records (extended summary). *Lecture Notes in Computer Science*, 434:662–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340662.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340662.pdf>.

Domingo i Ferrer:1990:FSK

- [65] Josep Domingo i Ferrer and Llorenç Huguet i Rotger. Full secure key exchange and authentication with no previously shared secrets. *Lecture Notes in Computer Science*, 434:665–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-

tronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340665.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340665.pdf>.

Roggeman:1990:VFS

- [66] Yves Roggeman. Varying feedback shift registers. *Lecture Notes in Computer Science*, 434:670–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340670.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340670.pdf>.

Gollmann:1990:CC

- [67] Dieter Gollmann and William G. Chambers. A cryptanalysis of $\text{Step}_{k,m}$ -cascades. *Lecture Notes in Computer Science*, 434:680–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340680.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340680.pdf>.

Schnorr:1990:EISa

- [68] Claus P. Schnorr. Efficient identification and signatures for smart cards (abstract). *Lecture Notes in Computer Science*, 434:688–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/>

[bibs/0434/04340688.htm](http://link.springer-ny.com/link/service/series/0558/papers/0434/04340688.htm); <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340688.pdf>.

Waidner:1990:DCD

- [69] Michael Waidner and Birgit Pfitzmann. The dining cryptographers in the disco: Unconditional sender and recipient untraceability with computationally secure serviceability (abstract). *Lecture Notes in Computer Science*, 434:690–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340690.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340690.pdf>.

Carter:1990:SCL

- [70] Glyn Carter. Some conditions on the linear complexity profiles of certain binary sequences. *Lecture Notes in Computer Science*, 434:691–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340691.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340691.pdf>.

Brown:1990:DPT

- [71] Lawrence Brown and Jennifer Seberry. On the design of permutation P in DES type cryptosystems. *Lecture Notes in Computer Science*, 434:696–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340696.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340696.pdf>.

ny.com/link/service/series/0558/bibs/0434/04340696.htm; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340696.pdf>.

Agnew:1990:FEC

- [72] Gordon B. Agnew, R. C. Mullin, and Scott A. Vanstone. A fast elliptic curve cryptosystem. *Lecture Notes in Computer Science*, 434:706–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0434/04340706.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0434/04340706.pdf>.

Anonymous:1990:AIa

- [73] Anonymous. Author index. *Lecture Notes in Computer Science*, 434:709–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/papers/0434/0434ind.pdf>.

Kahn:1990:KGN

- [74] David Kahn. Keying the German Navy’s Enigma (invited). *Lecture Notes in Computer Science*, 435:2–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350002.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350002.pdf>.

Desmedt:1990:MCS

- [75] Yvo Desmedt. Making conditionally secure cryptosystems unconditionally abuse-free in a general context (extended abstract). *Lecture Notes in Computer Science*, 435:6–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350006.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350006.pdf>.

Damgaard:1990:EBC

- [76] Ivan Bjerre Damgård. On the existence of bit commitment schemes and zero-knowledge proofs. *Lecture Notes in Computer Science*, 435:17–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350017.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350017.pdf>.

Brand:1990:PNU

- [77] Russell L. Brand. Problems with the normal use of cryptography for providing security on unclassified networks (invited). *Lecture Notes in Computer Science*, 435:30–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350030.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350030.pdf>.

Kohl:1990:UEK

- [78] John T. Kohl. The use of encryption in Kerberos for network authentication (invited). *Lecture Notes in Computer Science*, 435:35–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350035.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350035.pdf>.

Feldmeier:1990:UPS

- [79] David C. Feldmeier and Philip R. Karn. UNIX password security — ten years later (invited). *Lecture Notes in Computer Science*, 435:44–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350044.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350044.pdf>.

Smith:1990:PPC

- [80] Jonathan M. Smith. Practical problems with a cryptographic protection scheme (invited). *Lecture Notes in Computer Science*, 435:64–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350064.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350064.pdf>.

Barrett:1990:SDU

- [81] Paul Barrett and Raymund Eisele. The smart diskette — A universal user token and personal crypto-engine (invited). *Lecture Notes in Computer Science*, 435:74–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350074.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350074.pdf>.

Chan:1990:QSP

- [82] Agnes Hui Chan and Richard A. Games. On the quadratic spans of periodic sequences. *Lecture Notes in Computer Science*, 435:82–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350082.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350082.pdf>.

Jansen:1990:SFS

- [83] Cees J. A. Jansen and Dick E. Boeke. The shortest feedback shift register that can generate a given sequence. *Lecture Notes in Computer Science*, 435:90–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350090.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350090.pdf>.

Maurer:1990:PLR

- [84] Ueli M. Maurer and James L. Massey. Perfect local randomness in pseudo-random sequences. *Lecture Notes in Computer Science*, 435:100–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350100.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350100.pdf>.

Goldreich:1990:SPD

- [85] Oded Goldreich and Hugo Krawczyk. Sparse pseudorandom distributions (extended abstract). *Lecture Notes in Computer Science*, 435:113–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350113.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350113.pdf>.

Naor:1990:BCU

- [86] Moni Naor. Bit commitment using pseudo-randomness (extended abstract). *Lecture Notes in Computer Science*, 435:128–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350128.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350128.pdf>.

Krawczyk:1990:HPC

- [87] Hugo Krawczyk. How to predict congruential generators. *Lecture Notes in Computer Science*, 435:138–153, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350138.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350138.pdf>.

Preneel:1990:CTA

- [88] Bart Preneel, Antoon Bosselaers, René Govaerts, and Joos Vandewalle. A chosen text attack on the modified cryptographic checksum algorithm of Cohen and Huang. *Lecture Notes in Computer Science*, 435:154–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350154.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350154.pdf>.

Zeng:1990:LCT

- [89] Kencheng Zeng, C. H. Yang, and T. R. N. Rao. On the linear consistency test (LCT) in cryptanalysis with applications. *Lecture Notes in Computer Science*, 435:164–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350164.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350164.pdf>.

Fiat:1990:BR

- [90] Amos Fiat. Batch RSA. *Lecture Notes in Computer Science*, 435:175–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350175.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350175.pdf>.

Bender:1990:IEC

- [91] Andreas Bender and Guy Castagnoli. On the implementation of elliptic curve cryptosystems. *Lecture Notes in Computer Science*, 435:186–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350186.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350186.pdf>.

Bellare:1990:NPD

- [92] Mihir Bellare and Shafi Goldwasser. New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. *Lecture Notes in Computer Science*, 435:194–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350194.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350194.pdf>.

Chaum:1990:US

- [93] David Chaum and Hans van Antwerpen. Undeniable signatures. *Lecture Notes in Computer Science*, 435:212–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350212.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350212.pdf>.

Merkle:1990:CDS

- [94] Ralph C. Merkle. A certified digital signature (subtitle: That antique paper from 1979). *Lecture Notes in Computer Science*, 435:218–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350218.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350218.pdf>.

Schnorr:1990:EISb

- [95] Claus P. Schnorr. Efficient identification and signatures for smart cards. *Lecture Notes in Computer Science*, 435:239–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350239.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350239.pdf>.

Soete:1990:SSV

- [96] Marijke De Soete, Jean-Jacques Quisquater, and Klaus Vedder. A signature with

shared verification scheme. *Lecture Notes in Computer Science*, 435:253–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350253.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350253.pdf>.

Even:1990:LLD

- [97] Shimon Even, Oded Goldreich, and Silvio Micali. On-line/off-line digital signatures. *Lecture Notes in Computer Science*, 435:263–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350263.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350263.pdf>.

Brickell:1990:CIS

- [98] Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes (extended abstract). *Lecture Notes in Computer Science*, 435:278–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350278.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350278.pdf>.

Laih:1990:DTS

- [99] Chi-Sung Laih, Lein Harn, Jau-Yien Lee, and Tzonelih Hwang. Dynamic threshold scheme based on the definition of cross-product in an N -

dimensional linear space. *Lecture Notes in Computer Science*, 435:286–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350286.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350286.pdf>.

Chor:1990:SSI

- [100] Benny Chor and Eyal Kushilevitz. Secret sharing over infinite domains (extended abstract). *Lecture Notes in Computer Science*, 435:299–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350299.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350299.pdf>.

Desmedt:1990:TC

- [101] Yvo Desmedt and Yair Frankel. Threshold cryptosystems. *Lecture Notes in Computer Science*, 435:307–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350307.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350307.pdf>.

Chick:1990:FAC

- [102] Gerald C. Chick and Stafford E. Tavares. Flexible access control with master keys. *Lecture Notes in Computer Science*, 435:316–??, 1990. CODEN LNCSD9.

ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350316.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350316.pdf>.

Tatebayashi:1990:KDP

- [103] Makoto Tatebayashi, Natsume Matsuzaki, and David B. Newman, Jr. Key distribution protocol for digital mobile communication systems. *Lecture Notes in Computer Science*, 435:324–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350324.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350324.pdf>.

Buchmann:1990:KES

- [104] Johannes A. Buchmann and Hugh C. Williams. A key exchange system based on real quadratic fields (extended abstract). *Lecture Notes in Computer Science*, 435:335–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350335.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350335.pdf>.

Yacobi:1990:KDS

- [105] Yacov Yacobi and Zahava Shmueli. On key distribution systems. *Lecture Notes in Computer Science*, 435:344–??, 1990. CODEN LNCSD9.

ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350344.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350344.pdf>.

Nelson:1990:SAE

- [106] Ruth Nelson and John Heimann. SDNS architecture and end-to-end encryption. *Lecture Notes in Computer Science*, 435:356–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350356.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350356.pdf>.

Brickell:1990:SHI

- [107] Ernest F. Brickell. A survey of hardware implementations of RSA (invited), (abstract). *Lecture Notes in Computer Science*, 435:368–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350368.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350368.pdf>.

Findlay:1990:MEU

- [108] Paul A. Findlay and Brian A. Johnson. Modular exponentiation using recursive sums of residues. *Lecture Notes in Computer Science*, 435:371–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350371.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350371.pdf>.

ny.com/link/service/series/0558/bibs/0435/04350371.htm; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350371.pdf>.

Morita:1990:FMM

- [109] Hikaru Morita. A fast modular-multiplication algorithm based on a higher radix. *Lecture Notes in Computer Science*, 435:387–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350387.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350387.pdf>.

Bos:1990:ACH

- [110] Jurjen N. E. Bos and Matthijs J. Coster. Addition chain heuristics. *Lecture Notes in Computer Science*, 435:400–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350400.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350400.pdf>.

Quisquater:1990:HECb

- [111] Jean-Jacques Quisquater and Jean-Paul Descaillie. How easy is collision search. new results and applications to DES (abstract and results). *Lecture Notes in Computer Science*, 435:408–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/>

[bibs/0435/04350408.htm](http://link.springer-ny.com/link/service/series/0558/papers/0435/04350408.pdf); <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350408.pdf>.

Damgaard:1990:DPH

- [112] Ivan Bjerre Damgård. A design principle for hash functions. *Lecture Notes in Computer Science*, 435:416–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350416.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350416.pdf>.

Merkle:1990:OWH

- [113] Ralph C. Merkle. One way hash functions and DES. *Lecture Notes in Computer Science*, 435:428–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350428.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350428.pdf>.

Magliveras:1990:PCP

- [114] Spyros S. Magliveras and Nasir D. Memon. Properties of cryptosystem PGM. *Lecture Notes in Computer Science*, 435:447–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350447.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350447.pdf>.

Zheng:1990:CBC

- [115] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses (extended abstract). *Lecture Notes in Computer Science*, 435:461–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350461.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350461.pdf>.

Okamoto:1990:DZKb

- [116] Tatsuaki Okamoto and Kazuo Ohta. Disposable zero-knowledge authentications and their applications to untraceable electronic cash. *Lecture Notes in Computer Science*, 435:481–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350481.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350481.pdf>.

Ben-Or:1990:EIS

- [117] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Efficient identification schemes using two prover interactive proofs. *Lecture Notes in Computer Science*, 435:498–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350498.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350498.pdf>.

[series/0558/papers/0435/04350498.pdf](http://link.springer-ny.com/link/service/series/0558/papers/0435/04350498.pdf).

Boyar:1990:CCZ

- [118] Joan Boyar and René Peralta. On the concrete complexity of zero-knowledge proofs. *Lecture Notes in Computer Science*, 435:507–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350507.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350507.pdf>.

Feige:1990:ZKP

- [119] Uriel Feige and Adi Shamir. Zero knowledge proofs of knowledge in two rounds. *Lecture Notes in Computer Science*, 435:526–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350526.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350526.pdf>.

Kilian:1990:MRZ

- [120] Joe Kilian, Silvio Micali, and Rafail Ostrovsky. Minimum resource zero-knowledge proofs (extended abstract). *Lecture Notes in Computer Science*, 435:545–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350545.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350545.pdf>.

Bellare:1990:NIO

- [121] Mihir Bellare and Silvio Micali. Non-interactive oblivious transfer and applications. *Lecture Notes in Computer Science*, 435:547–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350547.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350547.pdf>.

Beaver:1990:MPT

- [122] Donald Beaver. Multiparty protocols tolerating half faulty processors. *Lecture Notes in Computer Science*, 435:560–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350560.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350560.pdf>.

Cleve:1990:CGD

- [123] Richard Cleve. Controlled gradual disclosure schemes for random bits and their applications. *Lecture Notes in Computer Science*, 435:573–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350573.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350573.pdf>.

Beaver:1990:MCF

- [124] Donald Beaver and Shafi Goldwasser. Multiparty computation

with faulty majority. *Lecture Notes in Computer Science*, 435:589–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350589.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350589.pdf>.

Chaum:1990:SDA

- [125] David Chaum. The spymasters double-agent problem: Multiparty computations secure unconditionally from minorities and cryptographically from majorities. *Lecture Notes in Computer Science*, 435:591–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350591.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350591.pdf>.

Bellare:1990:SSK

- [126] Mihir Bellare, Lenore Cowen, and Shafi Goldwasser. On the structure of secret key exchange protocols. *Lecture Notes in Computer Science*, 435:604–??, 1990. CODEN LNCS9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350604.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350604.pdf>.

Shamir:1990:EIS

- [127] Adi Shamir. An efficient identifica-

tion scheme based on permuted kernels (extended abstract). *Lecture Notes in Computer Science*, 435:606–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350606.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350606.pdf>.

Ostrovsky:1990:ESP

- [128] Rafail Ostrovsky. An efficient software protection scheme (abstract). *Lecture Notes in Computer Science*, 435:610–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350610.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350610.pdf>.

Adams:1990:GBE

- [129] Carlisle M. Adams and Stafford E. Tavares. Good S-boxes are easy to find. *Lecture Notes in Computer Science*, 435:612–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350612.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350612.pdf>.

White:1990:CDP

- [130] Steve R. White. Convert distributed processing with computer viruses. *Lecture Notes in Computer Science*, 435:616–??, 1990. CODEN LNCSD9.

ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350616.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350616.pdf>.

Price:1990:PDS

- [131] Wyn L. Price. Progress in data security standardisation. *Lecture Notes in Computer Science*, 435:620–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350620.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350620.pdf>.

Miyaguchi:1990:FCC

- [132] Shoji Miyaguchi. The FEAL- 8 cryptosystem and a call for attack. *Lecture Notes in Computer Science*, 435:624–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350624.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350624.pdf>.

Quisquater:1990:HEZ

- [133] Jean-Jacques Quisquater, Louis C. Guillou, and Thomas A. Berson. How to explain zero-knowledge protocols to your children. *Lecture Notes in Computer Science*, 435:628–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL <http://link.springer-ny.com/link/service/series/0558/bibs/0435/04350628.htm>; <http://link.springer-ny.com/link/service/series/0558/papers/0435/04350628.pdf>.

ny.com/link/service/series/0558/
bibs/0435/04350628.htm; [http://
link.springer-ny.com/link/service/
series/0558/papers/0435/04350628.
pdf](http://link.springer-ny.com/link/service/series/0558/papers/0435/04350628.pdf).

Anonymous:1990:AIb

- [134] Anonymous. Author index. *Lecture Notes in Computer Science*, 435:633–??, 1990. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-3349 (electronic). URL [http://link.springer-ny.com/
link/service/series/0558/papers/
0435/0435ind.pdf](http://link.springer-ny.com/link/service/series/0558/papers/0435/0435ind.pdf).