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]. 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].

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].

1


Informational [12]. Integrity [28]. Interactive [117, 16, 121, 92]. Invited [29, 81, 77, 107, 1, 61, 79, 34, 74, 78, 44, 80].


Knowledge [92, 118, 18, 21, 10, 15, 76, 119, 120, 16, 116, 133, 64, 22].


Modular [108, 109].


Nonlinearly [56]. Normal [77]. NP [21]. Number [21].


One-Way [10]. Online [30]. Open [27]. Optimally [41]. Order [9]. Oriented [8].


Proofs [92, 117, 118, 18, 76, 119, 120, 16, 22].

Properties [114]. Protection [25, 128, 80].

Pseudo-random [51, 84]. Pseudo-randomness [86]. Pseudorandom [85, 41]. Public [1, 2, 7, 4]. Public-Key [1, 2, 7].

Quadratic [104, 82].


Recursive [108]. Reducibility [16].

Register [56, 83]. Registers [54, 66].

Relying [115]. Requirements [29].


RSA-Implementation [37]. RSA-Moduli [60].

S [129]. S-Boxes [129]. Satisfiability [23].


Secure [125, 75, 65, 2, 60, 69, 115].

Security [77, 79, 131, 42, 27, 26]. Self [16].

References


REFERENCES


REFERENCES


Pieprzyk:1990:NLE


Sgarro:1990:IDB


Quisquater:1990:BHF


Mjolsnes:1990:STD


Burmester:1990:GZK


Okamoto:1990:DZKa


REFERENCES


REFERENCES


[41] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. Impossibility and opti-
mally results on constructing pseudorand-
ny.com/link/service/series/0558/bibs/0434/04340412.htm; http://
link.springer-ny.com/link/service/series/0558/papers/0434/04340412.
pdf.

ny.com/link/service/series/0558/bibs/0434/04340436.htm; http://
link.springer-ny.com/link/service/series/0558/papers/0434/04340436.
pdf.

[42] Rainer A. Rueppel. On the security of Schnorr's pseudo random gener-
ny.com/link/service/series/0558/bibs/0434/04340423.htm; http://
link.springer-ny.com/link/service/series/0558/papers/0434/04340423.
pdf.

[45] Ernest F. Brickell. Some ideal se-
cret 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.

[43] Jean-Jacques Quisquater and Jean-
Paul Delescaille. How easy is col-
ny.com/link/service/series/0558/bibs/0434/04340429.htm; http://
link.springer-ny.com/link/service/series/0558/papers/0434/04340429.
pdf.
REFERENCES

12

Beutelspacher:1990:HSN


Godlewski:1990:KMA


Gunther:1990:PGR


Niederreiter:1990:KSG


Beth:1990:CPR


Dai:1990:FFD


Meier:1990:NCC

REFERENCES


Maurer:1990:FGS


Duhoux:1990:DBA


Bosma:1990:FPT


Quisquater:1990:ZKP


DomingoiFerrer:1990:FSK

REFERENCES


Roggeman:1990:VFS


Gollmann:1990:CC


Schnorr:1990:EISa


Waidner:1990:DCD


Carter:1990:SCL


Brown:1990:DPT


REFERENCES


REFERENCES

Maurer:1990:PLR


Goldreich:1990:SPD


Naor:1990:BCU


Krawczyk:1990:HPC


Preneel:1990:CTA


Zeng:1990:LCT

REFERENCES


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

**Even:1990:LLD**


**Brickell:1990:CIS**


**Laih:1990:DTS**


**Chor:1990:SSI**


**Desmedt:1990:TC**


**Chick:1990:FAC**

REFERENCES


Tatebayashi:1990:KDP


Buchmann:1990:KES


Yacobi:1990:KDS


Nelson:1990:SAE


Brickell:1990:SHI


Findlay:1990:MEU

REFERENCES


[127] Adi Shamir. An efficient identifica-
REFERENCES


Anonymous:1990:AIb