Title word cross-reference

1 [276]. 2 [491, 267, 531, 130]. 2\(^k\) [529]. 3 [342]. 31 [261]. 4 [26]. 8 [474]. \(d\) [363]. GF(2\(^m\)) [68]. \(k\) [276, 204, 402]. L(1/3) [366]. Q [512]. \(nL^3\) mod 4 [227]. \(O(n)\) [219]. \(p\) [91]. S [29, 94, 24, 88].


0 [465].


2 [507]. 256 [474].

3G [461].

4-Round [393].


Adversaries [353, 345, 357, 403, 450, 472, 501, 236].

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].
Finite [199, 102, 398, 252, 326, 221, 263].
first [71]. Fixed [262, 383]. FlipIt [436].
Forward-Secure [294]. Four [447].
Four-Dimensional [447]. FPGA-friendly [373, 378].
FPGA-friendly [378]. Fractional [160].
Framework [308, 521, 475]. Franklin [197].
Free [504, 166, 125, 137, 322, 350, 98].
Frequency [121]. Friendly [352, 378].
Frobenius [251]. Full [518, 422, 515, 239].
Fully [433, 487]. Function [219, 125, 369, 222, 30]. Functional [89].
Further [100].

Generalization [10]. Generalized [41].
Generates [85]. Generating [233].
Generator [253, 179, 298, 15]. Generators [505, 379, 225, 224, 121, 191, 222, 59, 38].
GGH [330]. Given [258, 56]. Giving [51].
Glitch [373]. Glitches [375]. GNUC [475].
Go [519]. Goldreich [242]. Golić [405].
good [29]. GOST [422]. Graph [96, 408].
Groups [310, 408, 324, 280, 231, 326, 221].

H [380]. Handling [315]. Handshake [351].
Hard [289, 500, 200]. Hard-Core [200].
Hard-to-Invert [289, 500]. Hardness [421].
Hashing [442, 397, 159, 98]. having [76].
HB [356]. Hellman [10, 341, 184, 521, 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, 528, 65].
Identification [506, 325, 50, 169, 55, 61].
Identity [367, 456, 325, 311, 387, 6].
Identity-Based [367, 456, 325, 311, 387].
Improbability [146]. Improve [337].
Improved [348, 445, 474, 253, 274, 459, 378, 63].
Improvement [133]. Improvements [123].
Improving [206]. Independent [204].

Vulnerabilities [136]. Vulnerability [83].


Yao [331].


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


Kaliski:1988:DES


Stinson:1988:SCB


Beauchemin:1988:GRN


Chaum:1988:DCP


Feige:1988:ZKP

REFERENCES


REFERENCES

Piper:1989:LCS


Abadi:1990:SCE


Nishimura:1990:PMM


Stinson:1990:CAS


Gong:1990:MKD


Boyar:1990:DLI


Simmons:1990:CPC


Niederreiter:1990:CAP


Forre:1990:MID


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


Haber:1991:HTD


Matyas:1991:KPC


Pastor:1991:CCA


Lenstra:1991:CRK


Micali:1991:EPP


DeSoete:1991:NBC


Kaliski:1991:OWP


Golic:1991:GCA


Brickell:1991:EI

Biham:1991:DCL


Feigenbaum:1991:GEI


Beaver:1991:SMP


Brickell:1991:CIS


Maurer:1991:LRP


Naor:1991:BCU


Schnorr:1991:ESG


Goutier:1991:SII


Boyar:1991:PZK

Koblitz:1991:ECI


Damgaard:1992:P


Bennett:1992:EQC


Brickell:1992:IIS


Evertse:1992:WNR


Maurer:1992:CPS


Meier:1992:CPC


Maurer:1992:UST


Lloyd:1992:CBF

REFERENCES


Georgiades:1992:SRS


Loxton:1992:CRC


Brickell:1992:SIB


Magliveras:1992:APC


Phillips:1992:SIS


Dai:1992:BSD


Brassard:1993:EN


Agnew:1993:AO


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

Coppersmith:1993:MNF


Orton:1993:DFP


Menezes:1993:ECC


Lenstra:1993:UIK


Goldreich:1994:DPZ


Klapper:1994:VGS


Chor:1994:SPH


Murphy:1994:WCG


Simmons:1994:PSI

REFERENCES


REFERENCES


Pei:1995:ITB


Dyer:1995:KSS


Damgaard:1995:PPS


Heys:1996:SPN


Ben-Aroya:1996:DCL

REFERENCES


REFERENCES


Fischer:1996:SPO


Impagliazzo:1996:ECS


Cachin:1997:LIR


Klapper:1997:FSR


Even:1997:CCS


Damgaard:1997:ESH


Kilian:1998:ENZ


Sakurai:1998:SCC


Biham:1998:CMM


Knudsen:1998:AFD


Golic:1998:MCI

Naor:1998:PZK


Scheidler:1998:PKC


Schnorr:1998:BBM


Balasubramanian:1998:IEC

REFERENCES

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


REFERENCES


REFERENCES


Phillip Rogaway. Bucket hashing and its application to fast message authentication.
REFERENCES

Blundo:1999:FBA


Biham:1999:CTM


Bernstein:1999:HSR


Burmester:1999:DSF


Quinn:1999:BKD

Blundo:1999:CVC


Goldreich:2000:P


Franklin:2000:SCM


REFERENCES


[171] Shoup:1999:SPI

REFERENCES


REFERENCES


Don Coppersmith:2000:PAD


David Pointcheval:2000:SAD


J. M. Pollard:2000:KMD


Rosario Gennaro:2000:RBU


Joan Boyar:2000:SNI
REFERENCES


REFERENCES

Boneh:2001:IEE


Wang:2001:SCM


Ye:2001:DAA


Bailey:2001:EAF


Goldmann:2001:CBG


Gaudry:2002:CDF

Biham:2002:CAX

Moldovyan:2002:CBD

Shoup:2002:STC

Naor:2002:CPR

Abadi:2002:RTV


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


Miller:2004:WPE

Joux:2004:ORP

Verheul:2004:EXM

Boneh:2004:SSW

Barreto:2004:EIP

Naor:2005:CSO
REFERENCES


50

REFERENCES


Goldwasser:2005:SMP


Biham:2005:CSR


Kent:2005:SCB
von zur Gathen: 2005: PNB

Avanzi: 2005: CCM

Knudsen: 2005: PKR

Blundo: 2005: ADD

Denef: 2006: EKA

MacKenzie: 2006: TPA

Katz: 2006: CSN
REFERENCES


REFERENCES


REFERENCES


REFERENCES

Beimel:2007:RIT


Blundo:2007:USD


Cheng:2007:PPO


Tsaban:2007:TCK


Gennaro:2007:RES


Gennaro:2007:RBU


REFERENCES

Nguyen:2008:SSK


Abe:2008:TKN


Selcuk:2008:PSL


Boneh:2008:SSR


Bentahar:2008:GCI


Lindell:2008:LBI


Renault:2008:PRP

Overbeck:2008:SAP


Katz:2008:HEP


Abdalla:2008:SER


Barkan:2008:ICO


Lu:2008:CEL


Matucci:2008:CSP


Katz:2008:HEP


Abdalla:2008:SER

REFERENCES


Bellare:2008:AER


KAsters:2008:RBN


Jutla:2008:EMA


Jain:2008:NBC


Diem:2008:ICC


Bellare:2009:SPI


REFERENCES


P. Morrissey, N. P. Smart, and B. Warinschi. The TLS handshake protocol: a

**Freeman:2010:TPF**


**Aumann:2010:SAC**


**Beimel:2010:HSW**


**Aggarwal:2010:SCM**


**Katz:2010:PCS**


**Hazay:2010:EPS**


REFERENCES

Muller-Quade:2010:LTS


Indesteege:2011:PCE


Enge:2011:DLA


Abdalla:2011:WIB


Canetti:2011:UCS


Grassl:2011:CTZ


Asharov:2011:UDC

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


---


REFERENCES


REFERENCES


[395] Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of com-
puitationally sound protocols revis-
ited. Journal of Cryptology: the
journal of the International Associa-
tion for Cryptologic Research, 25(1):
116–135, January 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&

Aerts:2012:PAK

[396] Wim Aerts, Eli Biham, Dieter De
Moitie, Elke De Mulder, Orr Dunkel-
man, Sebastiaan Indesteege, Nathan
Keller, Bart Preneel, Guy A. E. Vanden-
bosch, and Ingrid Verbauwhede. A prac-
tical attack on KeeLoq. Journal of Cryp-
tology: the journal of the Interna-
tional Association for Cryptologic Research, 25
(1):136–157, January 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&
volume=25&issue=1&page=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 Interna-
tional Association for Cryptologic Research, 25
(1):158–193, January 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&
volume=25&issue=1&page=158.

Cheon:2012:APR

[398] Jung Hee Cheon, Jin Hong, and Minkyu
Kim. Accelerating Pollard’s rho al-
gorithm on finite fields. Journal of Cryptology: the journal of the Interna-
tional Association for Cryptologic Research, 25
(2):195–242, April 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&

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 Interna-
tional Association for Cryptologic Research, 25
(2):243–270, April 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&

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 Interna-
tional Association for Cryptologic Research, 25
(2):271–309, April 2012. CODEN
JOCREQ. ISSN 0933-2790 (print),
www.springerlink.com/openurl.
asp?genre=article&issn=0933-2790&
volume=25&issue=2&page=271.

Roeder:2012:MVS

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


REFERENCES


REFERENCES


REFERENCES


Bitansky:2014:SSC


Hazay:2014:CSP


Fischlin:2014:RMP


Applebaum:2014:KDM


Khovratovich:2014:RRA


Goldwasser:2014:BPO


Groth:2014:CMS
Abdalla:2014:VRF


Faugere:2014:USI


Amir:2014:AAR


Jean:2014:ICA


Bellare:2014:CCH


Dunkelman:2014:PTR


Dunkelman:2015:SAE


Lamberger:2015:RAS


Berman:2015:NAA


Lindell:2015:EPS


Ahn:2015:CAD


Dunkelman:2015:ISK


Hofheinz:2015:GNU


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-
REFERENCES


[483] Hadi Soleimany, Céline Blondeau, Xiaoli Yu, and Wenling Wu. Reflection crypt-
REFERENCES


Bos:2016:FCG


Coron:2016:HBI


Freedman:2016:ESI


Yao:2016:CKE


Brown:2016:BRM


Gennaro:2016:AET


Haitner:2016:LUR

[497] Iftach Haitner, Eran Omri, and Hila Zarosim. Limits on the usefulness
REFERENCES

87


Beimel:2016:SSS


Abe:2016:SPS


Faust:2016:SSS


Hazay:2016:LRC


Applebaum:2016:GXG

[504] Benny Applebaum. Garbling XOR gates "for free" in the standard model. *Jour-
REFERENCES


REFERENCES


REFERENCES


Cash:2017:DPR


Cash:2017:DPR


Asharov:2017:FPB


Cheraghchi:2017:NMC


Cheraghchi:2017:NMC


Escala:2017:AFD

REFERENCES


Haza:2017:EOS


Homma:2017:DMV


Genkin:2017:AC


Komargodski:2017:SSN


Schroder:2017:SBS


Lee:2017:STD

Jooyoung Lee, Martijn Stam, and John Steinberger. The security of Tandem-DM in the ideal cipher model. Jour-
Benhamouda:2017:ECP


Hisil:2017:JCG


Tajik:2017:PSC