
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/

26 March 2015
Version 1.223

Title word cross-reference

References


REFERENCES

1539-9087 (print), 1558-3465 (electronic).


[ABC+12] T. W. Arnold, C. Buscaglia, F. Chan, V. Condorelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jor-
The text is a list of references with bibliographic information for various academic works. Each reference includes the author(s), title, journal or book name, volume, pages, year, and other publication details. For example, one reference is for an article titled "Tools over bilinear groups for modular design of cryptographic tasks" by Masayuki Abe, published in the proceedings of a conference on cryptography and information security. Another reference is for a book titled "Advances in Cryptology — ASIACRYPT 2010: 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010" edited by Masayuki Abe, which includes contributions from various authors on topics related to cryptography.

The references are structured in a consistent format, providing a comprehensive source of information for readers interested in the field of cryptography.
Aid:2013:DIO


Acar:2013:SPA


Arapinis:2012:RET


ALMashrafi:2012:AIM


Applebaum:2010:PKC

[ABW10] Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography
from different assumptions.


Arnedo-Moreno:2010:JRA


Arsalan:2012:IRW


Adj:2013:WDC


Ahmadian:2010:PDS


Alvarez:2012:CAB


Albrecht:2012:SDL


REFERENCES

Anon:2011:MCB

Anon:2012:SHS

Anon:2013:DSS

Anon:2013:SIS

Anon:2015:CEB

Anthes:2014:FTI

Andriotis:2013:JSD
Panagiotis Andriotis, George Oikonomou, and Theo Tryfonas. JPEG steganogra-
Agarwal:2010:BRW

Aumasson:2011:CHF

AlFardan:2013:LTB

Applebaum:2013:GXG

Albrecht:2015:FBR

Al-Qarni:2012:EI1
Garsah Farhan Al-Qarni and Farzin Deravi. Explicit integration of identity information from
REFERENCES


REFERENCES


Asaar:2015:IBM

Alsulaiman:2013:IVB

Altman:2010:AAP

Au:2011:PPT

Abdalla:2012:LRS
Anzala-Yamajako:2012:RAC

Abstract


Ahmad:2014:RTN


AlTaawy:2014:IDR


Ayub:2012:BRB


Apavatjrut:2012:EEA


Alshammari:2011:CET

Alavi:2014:RQE


Behnia:2013:IEB


Blaner:2013:IPP


Brennan:2012:ASC


Berbecaru:2010:FSM


Barbay:2012:BRB

REFERENCES


REFERENCES

Barak:2014:OEF

Beimel:2014:MLS

Boldi:2012:IUG

Bernstein:2011:PCI

Basin:2014:KYE

Bichsel:2012:DMA
Patrik Bichsel, Jan Camenisch, Bart De Decker, Jorn Lapon, and Vincent Naessens. Data-minimizing


REFERENCES


REFERENCES


Bicakci:2013:LSS


Botta:2014:PCI


Boyle:2014:EO


Basso:2011:BW


Bessani:2013:DDS


Biddle:2012:GPL

Robert Biddle, Sonia Chi-

**Bender:2012:DSP**


**Backstrom:2011:WAT**


**Bernstein:2011:HSH**


**Bendlin:2011:SHE**


**Bertoni:2011:CSF**


**Bertoni:2012:KIO**

Guido Bertoni, Joan Daemen, Michiêl Peeters, Gilles Van Assche, and Ronny Van Keer. KECCAK implementation overview. Report, STMicroelectron-

**Boldyreva:2012:SSE**


**Bitansky:2013:WFS**


**Beebe:2010:BPCd**


**Beebe:2010:BPCb**


**Berghel:2012:ITF**


**Bera:2014:QC**

REFERENCES


[BF11]


[BF12]


[BF12]

Amos Beimel, Oriol Farràs, and Yuval Mintz. Secret sharing schemes for very dense graphs. *Lecture
Battistello:2012:TBA


Barthe:2012:CA


Barak:2010:IPO


Barak:2012:IPO

[BGJT13] Barbulescu:2013:QPA


REFERENCES

0360-0300 (print), 1557-7341 (electronic).

**Berman:2013:HPR**


**Biagioli:2012:CCS**


**Biggs:2008:CII**


**Beimel:2014:CCW**


**Brumley:2010:CAI**


**Bogdanov:2012:UTC**

Dan Bogdanov, Roman Jagomägis, and Sven Laur. A universal toolkit for cryptographically secure privacy-preserving data mining. *Lecture Notes in Computer Science*, 7299:


Z. Brakerski, Y. T. Kalai,


Suvarna Bothe, Panagioti...
REFERENCES


**Bernstein:2010:PCA**


**Bernstein:2014:HEC**


**Byun:2011:SMC**


**Bai:2012:SSR**

Yu Bai and Yanlong Liu. A synchronization strengthen RFID authentication protocol based on key ar-

**Blomer:2012:TKG**

Biswas:2012:IBA

Backes:2012:GCP

Banik:2012:DFA

Bira 

Burmester:2011:LRA

Bism:2012:IBA

Bernstein:2012:SIN

BMP12

BMS12
Babamir:2014:AKP


Ben-Othman:2013:IHN


Böhme:2010:ASS


Boneh:2012:PBC


Borghoff:2010:CLC


Bowyer:2011:WSD

Kevin W. Bowyer. What surprises do identical twins have for identity science? *Computer*, 44(7):100–102, July 2011. CODEN CPTRB4. ISSN 0018-9162
REFERENCES


[BP14b] Mihir Bellare, Kenneth Paterson, and Phillip Rog-


Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware trojans? Report, University of Massachusetts (Amherst, USA); TU Delft (The Netherlands); ALaRI (University of Lugano, Switzerland); Horst Görtz Institut for IT-Security, Ruhr-Universität Bochum (Bochum, Germany), June 7, 2013. 18 pp. URL http://people.umass.edu/gbecker/BeckerChes13.pdf.

Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. Multi-instance security and its application to password-based cryptography. Lecture Notes in Computer Science, 7417:
REFERENCES


[Birrell:2013:FIM]
REFERENCES


REFERENCES

www.sciencedirect.com/
science/article/pii/S0164121214002775


[BVS+13] Joonsang Baek, Quang Hieu Vu, Abdulhadi Shoufan, Andrew Jones, and Dun-


Staff:2014:KYS


Carlson:2011:JR


Casselman:2010:VC


Cobb:2013:LMS

William E. Cobb, Rusty O. Baldwin, and Eric D. Laspe. Leakage mapping: a systematic methodology for assessing the side-channel information leakage of cryptographic implementations. *ACM Trans-


Cachin:2010:EKS


Carota:2012:FFI


Chou:2010:PSO


Chadha:2012:A


Chou:2013:UGS


Chang:2011:SFW


Cho:2014:DGA


Chen:2011:EAA


Chu:2014:KAC

Cheng-Kang Chu, Sherman S. M. Chow, Wen-
REFERENCES


REFERENCES


Carter:2013:SSA


Checkoway:2014:PED


Chang:2010:PRN


Chen:2010:IFA

Lanxiang Chen, Dan Feng, Yu Zhang, Lingfang Zeng, and Zhongying Niu. Integrating FPGA/ASIC into cryptographic storage systems to avoid re-encryption. *International
REFERENCES

Camenisch:2012:EAA

Che:2012:WAM

Cheraghchi:2014:NMC

Chaudhuri:2010:PIC

Caballero-Gil:2012:LAR

Coul:2011:ACO
Scott E. Coull, Matthew Green, and Susan Hohenberger. Access controls for


Liqun Chen, editor. *Cryptography and Coding: 13th
REFERENCES


Cheswick:2013:RP

Chen:2015:SSS

Chen:2012:SRF

Chien:2012:IAM

Chien:2013:CRC
Hung-Yu Chien. Combining Rabin cryptosystem and error correction codes to facilitate anonymous authentication with untraceability for low-end devices. Computer Networks (Amsterdam, Netherlands: 1999), 57(14):2705–2717, October 4, 2013. CODEN ???? ISSN 1389-1286 (print), 1872-7069 (elec-
Chirgwin:2013:ABB

Chmielowiec:2010:FPR

Choudary:2010:SCD

Chou:2014:EMA

Chen:2011:SEI

Chen:2013:ATK

Cilardo:2011:EPT
Alessandro Cilardo. Exploring the potential of

**Cheng:2013:EHM**


**Cao:2014:SCI**


**Chase:2013:SMN**


**Chuang:2011:LMA**


**Comon-Lundh:2010:DSP**


**Chong:2013:ASG**

Yu Chen, Song Luo, Jianbin Hu, and Zhong Chen. A novel commutative blind-}

\textit{ing identity based encryption scheme. Lecture Notes in Computer Science,}


Shih-Ying Chang, Yue-Hsun Lin, Hung-Min Sun,


REFERENCES


REFERENCES

Clark:2012:RLA


Chapin:2014:SRP


Chadwick:2014:AFI


Chen:2013:RWM


Chong:2015:SID


Chow:2012:EPV


[CVG+13] Jérémie Crenne, Romain Vaslin, Guy Gogniat, Jean-Philippe Diguet, Russell...
REFERENCES


Calmon:2014:ITM


Chung:2012:CBI


Choi:2012:LTF


Chen:2014:SBB


Chen:2014:DSE

Cao:2014:PPM

Chen:2012:IDC

Chen:2014:MLC

Chen:2015:TCP

Chen:2012:CKS

Chen:2012:FSD
Cheng Chen, Zhenfeng Zhang, and Dengguo Feng. Fully secure doubly-spatial encryption under simple assumptions. *Lecture Notes in Computer Science*, 7496:
References


Chen:2012:AIB


Chen:2012:IBE


Chen:2012:CSI


Dharwadkar:2010:SSG


Djebbar:2012:ASB


Danezis:2012:FCDb

George Danezis, editor. Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28 — March 4,
REFERENCES


Davies:2011:IST


Diong:2012:DAU


Dacosta:2012:OTC


Cordeiro:2012:IMB


DePrisco:2013:CVC

Roberto De Prisco and Alfredo De Santis. Color visual cryptography schemes for black and white secret images. Theoretical Computer Science, 510(??):62-86, October 28, 2013. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294
REFERENCES


REFERENCES


[DG10] Saar Drimer, Tim Güneysu, and Christof Paar. DSPs, BRAMs, and a pinch of logic: Extended recipes for AES on FPGAs. ACM Transactions on Reconfigurable Technology and Systems, 3(1):3:1–3:??, Jan-


REFERENCES


???? LCCN ???? URL


Qi Dong and Donggang Liu. Using auxiliary sensors for pairwise key establishment in WSN. ACM
Dong:2013:PRS

Dodis:2011:SSC

Demme:2012:SCV

David:2012:UCO

Donovan:2014:ATM

Duncan:2012:CAI


Das:2012:DPB


Dachman-Soled:2014:COF


Dini:2013:HHS


Dodis:2014:HEY


Deng:2012:VIA

Aidong Deng, Jianeng Tang, Li Zhao, and Cairong Zou. The variable-interval arithmetic coding using asymptotic deterministic randomness for data compression and encryption. *Journal of Statistical Computation and
REFERENCES


Dunkelman:2012:MEK


Dunkelman:2012:TCC


David:2012:PRE


Dorn:2012:ECE


Dong:2012:KKD

Dong:2012:NDI


Deng:2014:TNI


Deng:2014:CCC


Dodis:2013:OWE


Dent:2010:PS

REFERENCES


Eisenbarth:2012:CIP


Eisenbarth:2010:CCE


Elbirt:2009:UAC


ElBansarkhani:2012:ELB


Embar:2014:PWO


Estebanaz:2014:PMC

[CESRI14] César Estébanez, Yago Saez, Gustavo Recio, and Pedro Isasi. Performance of the most common non-cryptographic hash functions. *Software—Practice*
Engels:2012:HLA
Daniel Engels, Markku-Juhani O. Saarinen, and
Peter Schweitzer. The Hummingbird-2 lightweight
authenticated encryption algorithm. *Lecture Notes
LNCSD9. ISSN 0302-9743 (print), 1611-3349 (elec-
tronic). URL http://link.springer.com/chapter/
10.1007/978-3-642-25286-0_2/.

Eibach:2010:OGB
Tobias Eibach, Gunnar Völkel, and Enrico Pilz.
Optimising Gröbner bases on Bivium. *Mathematics
in Computer Science*, 3(2):159–172, April 2010. CO-
DEN ????? ISSN 1661-8270 (print), 1661-8289
(electronic). URL http://www.springerlink.com/
openurl.asp?genre=article&
issn=1661-8270&volume=3&issue=2&spage=159.

Eldib:2014:FVS
Hassan Eldib, Chao Wang, and Patrick Schaumont.
Formal verification of software countermeasures
against side-channel at-
tacks. *ACM Transactions on Software En-
ingineering and Methodology*, 24(2):11:1–11:??, De-
cember 2014. CODEN ATSMER. ISSN 1049-
331X (print), 1557-7392 (electronic).

Enos:2015:IBS
Graham Enos and Yu-
liang Zheng. An ID-
based signcryption scheme with compartmented secret
sharing for unsigncryption. *Information Pro-
cessing Letters*, 115(2):128–133, February 2015. CO-
DEN IFPLAT. ISSN 0020-0190 (print), 1872-6119
science/article/pii/S0020019014001537.

Farash:2014:ECC
Mohammad Sabzinejad Farash and Mahmoud Ah-
madian Attari. An efficient client–client password-based
authentication scheme with provable security. *The
Journal of Supercomputing*, 70(2):1002–1022, November
2014. CODEN JO- SUED. ISSN 0920-8542
(print), 1573-0484 (electronic). URL http://
link.springer.com/article/10.1007/s11227-014-1273-
z.

Farash:2014:CIE


Fischlin:2012:PKC


Ferretti:2014:DCI


Fuglerud:2011:SIA


Fehr:2010:QC

REFERENCES


Felten:2013:LBA


Faugere:2010:CLR


Fleischmann:2012:MFA


Feng:2010:CTS


Farras:2012:LTM


Faugere:2014:MCA

Jean-Charles Faugère, Domingo Gómez-Pérez, Jaime Gutierrez, and Ludovic Perret. Mathematical and computer algebra techniques in cryptography. Journal of
REFERENCES


Fan:2013:CPP


Fan:2010:PSN


Fan:2010:AMI


Fahl:2012:WEM


Fan:2014:ASA


Fawzi:2013:LDN

Omar Fawzi, Patrick Hayden, and Pranab Sen. From

**Fei:2012:GTK**


**Fan:2013:CEM**


**Fehr:2013:FCC**


**Ferguson:2010:SHF**

REFERENCES

Forler:2012:DA


Feng:2012:CAO


Faust:2014:CNM


Feng:2012:USD


Fraczek:2012:MSI


Fernandez-Mir:2012:SRA

REFERENCES


REFERENCES


Liming Fang, Willy Susilo, Chumpeng Ge, and Jian-

**Ferguson:2010:CED**


**Feng:2011:GDA**


**Fujiooka:2012:SHI**


**Fujiooka:2012:SEP**


**Fujiooka:2012:SEI**

REFERENCES

Fadlullah:2010:DCA

Fuchsbauser:2011:CSV

Fulton:2010:BRB

Feng:2013:ECE

Fanyang:2012:SAK

Feng:2011:VBF
REFERENCES


REFERENCES

81


Goranlta:2011:MKC


Gupta:2012:CDF


Gupta:2013:HPH


Guerra-Casanova:2011:SOT


Geller:2013:MIS


Gentry:2010:CAF

Craig Gentry. Computing arbitrary functions of en-

[Gentry:2013:EMH]

[Gen13]


[Gaspar:2012:SEF]

[GG10]

[Grigg:2011:CCN]


[GGHR14]

[Gen:2011:FHE]

[C. Gentry and S. Halevi. Fully homomorphic en-


REFERENCES


knowledge in the bounded
player model. Lecture
Notes in Computer Sci-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-36594-2_4/.

Geetha:2011:VRN

S. Geetha, V. Kabilan,
S. P. Chockalingam, and
N. Kamaraj. Varying radix
numeral system based
adaptive image steganogra-
phy. Information Process-
ing Letters, 111(16):792–
797, August 30, 2011. CO-
DEN IFPLAT. ISSN 0020-
0190 (print), 1872-6119 (electronic). URL http://
www.sciencedirect.com/
science/article/pii/S0020019011001414.

Guo:2010:HMW

Jing-Ming Guo and Yun-
Fu Liu. Hiding multitone
watermarks in halftone im-
ages. IEEE MultiMedia, 17
(1):65, January 2010. CO-
DEN IEMUE4. ISSN 1070-
986X (print), 1941-0166 (electronic).

Gouvea:2012:HSI

Conrado P. L. Gouvéa
and Julio López. High
speed implementation of
authenticated encryption
for the MSP430X micro-
controller. Lecture Notes
in Computer Science, 7533:
288–304, 2012. CO-
DEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-33481-8_16/.

Gora

Marcin Gorawski, Michal
Lorek, and Michal Gorawski.
Encrypted adaptive stor-
age model — analysis and
performance tests. Lecture
Notes in Computer Sci-
CODEN LNCSD9. ISSN
0302-9743 (print), 1611-
3349 (electronic). URL
http://link.springer.
com/chapter/10.1007/978-
3-642-32287-7_10/.

Gligor:2012:SLT

Virgil Gligor. Street-
level trust semantics for
attribute authentication (transcript of discussion).
Lecture Notes in Com-
puter Science, 7622:116–
125, 2012. CODEN
LNCSD9. ISSN 0302-9743
(print), 1611-3349 (elec-
tronic). URL http://
link.springer.com/chapter/
10.1007/978-3-642-35694-
1_0_13/.

Gollmann:2010:SCR

Dieter Gollmann, Jean-
Louis Lanet, and Julien
Iguchi-Cartigny, editors.
Smart card research and


[GNL12] Zheng Gong, Svetla Nikova, and Yee Wei Law. KLEIN:
REFERENCES


**Goodin:2012:CBS**

Dan Goodin. Crypto breakthrough shows Flame was designed by world-class scientists: The spy malware achieved an attack unlike any cryptographers have seen before. Web document., June 7, 2012. URL http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/.

**Garcia:2012:ERP**


**Gorski:2010:CDS**


**Groth:2012:NTN**


**Goodrich:2012:EVW**


**Grossschadl:2012:EJI**

Genkin:2014:GYH

Daniel Genkin, Itamar Pippman, and Eran Tromer. Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs. Report, Technion and Tel Aviv University, Tel Aviv, Israel, July 31, 2014. 25 pp. URL http://www.cs.tau.ac.il/~tromer/handsoff/.

Gonzalez-Pardo:2012:CID


Greengard:2011:MRM


Grimes:2015:CCT


Gibson-Robinson:2012:AAL


Gierlichs:2012:ICD


Genkin:2013:RKE

Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic crypt-


Hayes:2013:NSA


Houmansadr:2013:BCN


He:2013:HEH


Hao:2012:SAM


Hwang:2010:RIB


Hsu:2011:NLM


Hore:2012:IED

[HCDM12] Bijit Hore, Ee-Chien Chang, Mamadou H. Diallo, and

Hernandez-Castro:2012:MTA


Huang:2014:FOS


Hernandez-Castro:2012:AFH


Han:2013:RMA


Heninger:2012:MYP

REFERENCES


Hwang:2012:ABA


Hermelin:2010:MLC


Herranz:2014:ABS


Hess:2012:GJC


Harn:2014:MTS


Hoang:2014:IMD

REFERENCES


REFERENCES

Hinek:2010:CRV

Hinkelmann:2011:CPA

Hur:2014:SDR

Houmansadr:2014:NBW

Heyse:2012:LEA

Heil:2014:APH
REFERENCES


REFERENCES

Hu:2012:VMS


Huang:2011:ISL


Harn:2011:FDM


Huffmire:2010:SPR


Herranz:2011:RBS


Howard:2010:DSS

Michael Howard, David LeBlanc, and John Viega.
REFERENCES


[Hohenberger:2012:DDQ]


[Huang:2014:SWC]


[Herzberg:2012:TJA]


[Hore:2012:SMR]

REFERENCES

Hoang:2012:ESB


Hirt:2014:BA


Harnik:2010:CIC


Hyla:2012:CBE


Hazay:2014:OSA


Halder:2010:WTR


Hoffstein:2008:IMC


Han:2014:GTK

Herranz:2013:SMS

Haitner:2010:EIC
Iftach Haitner, Omer Reingold, and Salil Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. In
REFERENCES


REFERENCES

Hamdy:2011:HPB

Henson:2013:MES

Hu:2010:TTW

Herbert:2012:SMP

Han:2012:MIA

Hwang:2011:NIB

Heng:2010:CNS
REFERENCES

104

Lecture notes in computer science. Springer-Verlag, Berlin, Germany / Heidelberg, Germany / London, UK / etc., 2010. ISBN 3-642-17618-6 (softcover). LCCN ????


[Han:2014:ERI] Qi Han, Yinghui Zhang,


mathematical-puzzle-solved enables-unlimited-analysis encrypted-data. See patent [GH13].

IBM:2013:IPC


IEEE:2010:PIA


IEEE:2011:ICI


IEEE:2011:PIA


Islam:2011:MD


Ioannou:2014:PKC

[Lawrence M. Ioannou and Michele Mosca. Public-key cryptography based on bounded quantum reference frames. Theoretical Computer Science, 560 (part 1)(??):33–45, Decem-]
Ishai:2014:PCP


Jie:2010:AAI


Jie:2011:RGA


Prins:2011:DCA

JR Prins and Business Unit


REFERENCES


http://link.springer.com/chapter/10.1007/978-3-642-31912-9_16.


Juels:2014:HEE


Juels:2014:INC


Joux:2014:SAC

REFERENCES


[Karthigaikumar:2010:PPV] P. Karthigaikumar and K. Baskaran. Partially pipelined VLSI implementation of Blowfish en-
REFERENCES

[113]


REFERENCES

114


Kim:2014:MBM

KHMB13

Kai:2011:CIS

Kiayias:2011:TCC

Kia11

Kaw12:SHS
REFERENCES


REFERENCES


Patrick Koeberl, Jiantao Li, Roel Maes, Anand Rajan, Claire Vishik, and Marcin Wójcik. Evaluation of a PUF device authentication scheme on a discrete 0.13um SRAM. Lecture
CODEN LNCS9D. ISSN 0302-9743 (print), 1611-3349 (electronic). URL
http://link.springer.com/chapter/10.1007/978-3-642-32298-3_18/.

http://link.springer.com/chapter/10.1007/978-3-642-33191-6_3/.


REFERENCES

Kifer:2014:PFM


Kasamatsu:2012:TSE


Kiyoshima:2014:CRB


Karger:2011:LLB


Kanwal:2015:TTM


Khovratovich:2010:RCA

Khovratovich:2010:RRA


Koblitz:2010:BRB


Kasper:2012:SCA


Kang:2012:AKM


Kocabaș:2012:CPB


Keskinarkaus:2010:IWD

[KPS10] A. Keskinarkaus, A. Pramila, and T. Seppänen. Im-


REFERENCES


Kim:2012:SSS


Kim:2012:SAH


Kawachi:2012:SKE


Klisowski:2012:CCP


[KY10] A. A. Kamal and A. M. Youssef. Enhanced implementation of the NTRU-Encrypt algorithm using graphics cards. In Chaud-
huri et al. [CGB+10], pages 168–174. ISBN 1-4244-7675-5. LCCN ???.

Kate:2010:PBO


Lu:2010:MSC


Launchbury:2012:TBC


Liu:2013:PAE


Luo:2012:ESI

Lupu:2012:IBK


Lu:2013:CSA


Liu:2015:IAC


Liu:2013:IAG


Lathrop:2011:SPI


Lavington:2012:ATH

REFERENCES


Li:2015:CEH


Liang:2014:CCS


Lotz:2015:SCS


Launchbury:2012:ELT


Lago-Fernandez:2014:NAA

REFERENCES

0644 (print), 1097-024X (electronic).


REFERENCES


Liu:2012:FVC

Lee:2010:ISC

Lee:2010:CGC

Li:2010:EBB

Lee:2011:PSE

Lin:2011:NIB
Han-Yu Lin and Chien-Lung Hsu. A novel


[LHL14] Jin Li, Xinyi Huang, Jing-


Pei-Yu Lin. Imperceptible visible watermarking based on postcamera histogram operation. *The
REFERENCES


Lindell:2014:TCT


Lin:2015:DVS


Litton:2014:TFA


Liu:2015:LBD


Li:2012:OEA


Laszka:2014:STC

Aron Laszka, Benjamin Johnson, Pascal Schöttle,


REFERENCES

Lee:2015:TSS


Lee:2010:PMB


Lee:2011:TAT


Li:2015:IBE


Li:2012:RIB


Li:2010:DCY


Lai:2013:SAS

REFERENCES


Lu:2012:IEC


Lee:2006:DCK


Ling:2012:NCC

Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, and Weijia Jia. A new cell-counting-based attack against Tor. IEEE/ACM Transactions on Net-


Luo:2012:FSI


Lu:2012:BBE


Lambert-Mogiliansky:2012:EII

Ariane Lambert-Mogiliansky and Jerome R. Busemeyer. Emergence and instability of individual iden-
REFERENCES

135


Li:2011:NRA


Lv:2013:NTP


Lv:2013:NTP


Li:2011:CIB

REFERENCES

Liu:2015:SAB

Lopriore:2015:PCR

Low:2012:BRB

Lin:2011:CRN

Ling:2012:SHS
Huo-Chong Ling and Raphael C.-W. Phan. On the secu-
REFERENCES

Lamberti:2010:KES

Lubicz:2015:GMA

Lukowiak:2014:CEB

Liskiewicz:2013:GBS
REFERENCES


Lane:2014:PBD

Luo:2012:FSU

Lei:2012:RA

Liu:2011:DBA

Lee:2012:IBS

Lei:2013:RSW
Baiying Lei, Insu Song, and Shah Atiqur Rahman. Robust and secure watermarking scheme


REFERENCES

**Lewko:2011:DAB**


**Lewko:2011:UHA**


**Lewko:2012:NPM**


**Liu:2013:SIP**


**Liu:2013:TIE**

REFERENCES


REFERENCES

Liu:2010:SET

Liu:2011:PIA

Li:2010:GCP

Lou:2010:NAS

Luo:2012:ICB


Luo:2012:LVT


Liu:2014:PKE


Liu:2014:CRA


Li:2010:PES


Li:2012:ESS


Michail:2012:EHT

Malkin:2013:SCB


Mangard:2013:KSL


Martin:2010:XMA


Matsuda:2014:IBP


Maurer:2012:CCN


Mazurczyk:2013:VSD


Milo:2011:FGB

REFERENCES

Malone:2013:MOD

Mukhopadhyay:2011:PEA

Madanayake:2012:BPS

McGrayne:2011:TWH

McKay:2010:SLB

McKay:2011:SLB
Sinclair McKay. *The secret life of Bletchley Park: the history of the wartime codebreaking centre by the men and women who were there*. Gardners Books,
REFERENCES


Meshram:2015:EIB


Moreno:2013:NIP


Marmol:2010:TPA

[MGP10] Félix Gómez Mármol, Joao Girao, and Gregorio Martínez Pérez. TRIMS, a privacy-aware trust and reputation model for identity management systems. *Computer Net-


Matsuda:2014:CCS


Meziani:2012:IPS


Miller:2014:ADS

DEN SINODQ. ISSN 0362-1340 (print), 1523-2867 (print), 1558-1160 (electronic). POPL ’14 conference proceedings.  


REFERENCES

Moessner:2012:SAS


Muller:2012:HPC


Malik:2012:AIC


Marconato:2013:VLC


Mozaffari-Kermani:2010:CSI


Montecchi:2012:QSE

[MLBL12] Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli, and Ernesto La Mattina. Quantitative security evaluation of a


Hirak Kumar Maity and Santi P. Maity. FPGA implementation of reversible watermarking in digital images using reversible contrast mapping. The Journal of Systems and Software, 96(??):93–104, October 2014. CODEN JS-
REFERENCES


REFERENCES


Moran:2010:BCP

Mukhopadhayay:2014:EMP

This paper provides a correction to the algorithm presented in [HZSL05], and also supplies a complicated correctness proof.

Minier:2012:RKI

Mizuki:2011:ASN

Maimut:2012:LCR

Minamoto:2014:BDI
Teruya Minamoto and Ryuji Ohura. A blind digital image watermarking method based on the dyadic wavelet transform and interval arithmetic. *Applied Math-
REFERENCES

Mone:2013:FPE

Moore:2012:RFF

Moody:2014:DMW

Morad:2012:OEA

Minier:2012:EEC

Mironov:2012:IDP
REFERENCES


References

Maitra:2012:NAC


Maitra:2013:DSM


Maitra:2013:HEM


Maitra:2013:HPM


Myers:2012:BCM


Marton:2010:RDC


Mosca:2013:QKD

[MSU13] Michele Mosca, Douglas

Morozov:2012:ZKP


Malkin:2011:ECS


Murphy:2010:BRB


Miri:2012:SAC

REFERENCES

642-28495-7. ISSN 0302-9743 (print), 1611-3349 (electronic). URL http://www.springerlink.com/content/978-3-642-28495-3.

Maes:2012:PFF

Mathew:2012:EIC

Ma:2012:CIS

Mahmoody:2013:LEZ

Ma:2013:PVP

Manshaei:2013:GTM
Mohammad Hossein Man-
 REFERENCES


Ma:2015:PKE


Nagy:2010:OTP


Nagy:2010:QCS


Noureddine:2013:AMT


Naskar:2012:FIR

[Ruchira Naskar and Rajat Subhra Chakraborty. Fuzzy inference rule based reversible watermarking for digital images. Lecture
Naskar:2013:GTL


Naranjo:2013:FDA


Narasimhan:2013:HTD


Newell:2013:PCD


Naeem:2014:EIC

REFERENCES


Ning:2012:DCA


Nieto:2014:FSH


Nguyen:2012:DQB


Nagy:2010:KD


Navin:2010:ETU


Nose:2011:SW

Peter Nose. Security weaknesses of authenticated key agreement protocols. *Information Processing Let-
REFERENCES

165


[NPS12] Mehrdad Nojoumian and Douglas R. Stinson. Sociocentric secret sharing as


[NVB13] Xuyun Nie, Zhaohu Xu, and Johannes Buchmann. Cryptanalysis of hash-based tamed transformation and minus signature scheme. Lecture
Newell:2014:NCR

Nikooghadam:2010:EUE

Obana:2011:AOC


Obrenovic:2012:IUC

Obrien:2012:EPM
Ou:2010:CPA


Oliveira:2012:STA


Ohtake:2012:AAH


Orlandi:2014:SCN


Oppliger:2011:CC


Orejel:2014:E

REFERENCES

Owczarek:2012:LPL


Okamoto:2012:AAH


Otmani:2010:CTM


Ohzeki:2012:NWM


Ortiz-Yepes:2014:BSA


Praba:2010:MAC

V. Lakshmi Praba and G. Arumugam. Message authentication code algorithm for IP-SEC. *Inter-

Pandey:2014:ACR


Parent:2012:WAI


Park:2012:APO


Pass:2013:USP


Pranata:2013:MDR


Paulson:2010:SDO

REFERENCES

Pandit:2012:EFS


Park:2014:FRI


Pun:2014:GIT


Papadopoulos:2014:LQA


Premnath:2014:EHR


Pang:2014:PPA

REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-35362-8_16/.

Pfleeger:2010:CJD


Peinado:2012:CAT


Poppelmann:2012:TEA


Peng:2010:SFW


Park:2012:IDF


Pohls:2012:RDI

Henrich C. Pöhls and Focke Höhne. The role of data integrity in EU digital signature legislation — achieving statutory trust for sanitizable signature schemes. *Lecture Notes in Computer Science*, 7170:175–192, 2012. CODEN LNCSD9. ISSN 0302-9743 (print), 1611-
REFERENCES


REFERENCES

0167-739X (print), 1872-7115 (electronic).

Pang:2013:IMA


Peris-Lopez:2010:CSP


Pande:2013:SMC


Poursakidis:2010:TPC


Powers:2014:OSCa

REFERENCES


REFERENCES

http://link.springer.com/chapter/10.1007/978-3-642-33383-5_1/

[PPS12a] Duong Hieu Phan, David Pointcheval, and Mario Stre

[PPS12b] Duong Hieu Phan, David Pointcheval, and Mario Stre


Pereira:2013:SLC


Picazo-Sanchez:2013:CRS


Park:2013:PPM


Papamanthou:2013:SCC


Papakostas:2014:MBL

REFERENCES


REFERENCES

Pei:2015:SWT


Papadopoulos:2010:CAR


Patsakis:2015:PSM


Qian:2014:IAF


Rabin:2010:ACC


Rankin:2010:HLH


Rankin:2014:HEY

Kyle Rankin. Hack and /: encrypt your dog (Mutt


[RG10] Ren:2010:CSH


Oded Regev and Bo’az Klartag. Quantum one-way communication can be exponentially stronger


REFERENCES


[Ren:2014:HHM] Jian Ren, Jie Wu, Yun
REFERENCES


Rogaway:2012:SCS


Ristenpart:2010:WGR


SA12

[SU12]

Ren:2013:DSE


Rajendran:2015:FAB


Sang:2012:SSF


Somanatha:2015:RAK

Revathi Bangalore Somanatha and J. William
REFERENCES


Saarinen:2012:PPK


Suoranta:2012:SAM


Schutz:2010:DIN


Sahai:2013:TCT


Sarier:2010:IAS

Neyire Deniz Sarier. Improving the accuracy and


REFERENCES

CODEN CACMA2. ISSN 0001-0782 (print), 1557-7317 (electronic).


Schneier:2013:HDD


Schaefer:2015:BRB


Schneier:2015:DGH


Seberry:2010:CT


Seberry:2010:CTAb


Saleh:2010:GTF

[SD10] Mohamed Saleh and Mourad

[Shen:2012:PAS]


[SD12]

Shakiba:2010:IID


[SDM10]

Souissi:2012:OCP


[SEHK12]

Shakiba:2014:CCI


[SE14]

Seo:2014:RHI


[Sasaki:2012:IKK]

Yu Sasaki, Sareh Emami,

Sendrier:2010:PQC


Su:2012:IIIN


Shabtai:2010:SAP


Schneier:2015:SWC


Savas:2014:SMQ


REFERENCES


Shyu:2015:VCR


Satir:2012:CBT


Siad:2012:NAP


Shakeri:2012:RZW


Sachnev:2012:IME


[Scheidat:2012:STT] Tobias Scheidat, Karl Kümmel, and Claus Vielhauer. Short term template aging effects on biometric dynamic handwriting authentication perfor-
REFERENCES


Schmitz:2012:NAC


Srivatsa:2011:ESA


Schultz:2010:MMP


Somani:2010:IDS

U. Somani, K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. In Chaudhuri et al. [CGB+10], pages 211–216. ISBN 1-4244-7675-5. LCCN ????.

Shao:2012:AKP


Sarkar:2010:CRM

REFERENCES

IFPLAT. ISSN 0020-0190 (print), 1872-6119 (electronic).


**Swierczynski:2015:PSE**


**Stankovski:2014:CFE**


**Safavi-Naini:2011:USC**


**Seyedzadeh:2014:RCI**


**Suriadi:2012:PCV**

Serwadda:2013:ELK

Shaikh:2010:CTO

Shiaeles:2015:FI1

Schilling:2012:ATU

Sun:2013:IUP

Sur:2012:SSU
Stefan:2012:ACT


Saxena:2010:SGC


Szaban:2011:IQB


Saxena:2012:BIT


Shparlinski:2012:CSD

REFERENCES

December 2012. CODEN CM-BUA3. ISSN 0008-4395 (print), 1496-4287 (electronic).

**Sendrier:2013:HCE**


**Singh:2013:QBF**


**Smith:2011:SMC**


**Shrivastava:2012:UIE**


**Strydis:2013:SAP**

Sood:2011:SDI


Sahai:2012:DCC


Schillewaert:2014:CCA


Stallings:2011:CNS


Stanoyevitch:2011:ICM


Stanek:2012:TEM

[Sta12] Martin Stanek. Threshold encryption into mul-

**Stewart:2011:CCI**


**Stenn:2015:SNT**


**Stipcevic:2011:QRN**


**Stolte:2012:EDA**


**Suciu:2012:SED**


**Sung:2011:DCE**

REFERENCES

ISSN 0020-0190 (print), 1872-6119 (electronic).


REFERENCES


REFERENCES

Tang:2015:ETE


[Tan15]

Tarnovsky:2010:DSP


[Tar10]

Taylor:2014:WSE


[Tay14]

Tuan:2010:AWB


[TC10]

Tang:2015:CER


[TCL15]

Tian:2014:DFS

Haibo Tian, Xiaofeng Chen, and Willy Susilo. Deniability and forward

Tiplea:2014:NSC


Tao:2013:SMS


Terai:2011:BRB


Tassa:2012:SDC


Tian:2015:IBP


Tian:2012:TOE

Hui Tian, Hong Jiang, Ke Zhou, and Dan Feng.
REFERENCES


Thabit:2014:RRW


Tu:2014:EPB


Tani:2012:EQA


Tu:2013:PAQ


Tariq:2014:SBL

Tsaur:2012:ESM


Tsai:2013:ZWS


Tetali:2013:MSA


Tang:2012:RSS


Tsay:2012:VUL


Tang:2015:ECP

REFERENCES


Tormo:2013:IMP


Terrovitis:2011:LGR


Terrovitis:2012:PPD


Tsougenis:2012:PEM


Tang:2014:PAB

REFERENCES


[TTL10] H.-H. Tsai, H.-C. Tseng, and Y.-S. Lai. Robust...


[TYK+12] John Trammel, Ümit Yalçınalp, Andrei Kalfas,

[Ulutas:2011:MIS]

[Ulutas:2013:ISI]

[Vai12]

[Valamehr:2012:IRM]

[VanDam:2011:TQC]
Wim van Dam, Vivian M. Kendon, and Simone Severini, editors. Theory of quantum computation,
REFERENCES


Visegrady:2014:SCV


VenafiLabs:2014:VLQ


Vetter:2010:ABV


Viennot:2014:MSG


Vu:2015:NAN


Vleju:2012:CCA

REFERENCES


REFERENCES


Ding Wang, Chun guang

[Wei:2012:NCI]


[WHG+12]


[Wang:2012:FOP]


[Wang:2012:NFS]


Yuechuan Wei, Chao Li, and Dan Cao. Improved related-key rectangle attack on the full HAS-160 encryption mode. International Journal of Foundations of Computer Science (IJFCS), 23(3):733–??, April 2012. CODEN IFCSEN. ISSN 0129-0541 (print), 1793-6373 (electronic).

Wei:2012:IRK


Wang:2013:HCL


Wu:2011:HQI


Weissman:2011:LLB


Wang:2012:MCE

Wang:2011:RBM


Xiaotian Wu and Wei Sun. Random grid-based visual secret sharing for

Williams:2013:APC


Whitworth:2014:SPC


Watanabe:2012:ITT


Wang:2012:PAC


Wu:2010:EUA


Wu:2010:IBM

[TWT10b] Tsu-Yang Wu and Yuh-Min Tseng. An ID-based mutual authentication and

Wang:2013:NMC


Wu:2012:RIB


Wu:2012:AST


Willis:2013:IFI


Wang:2014:ATF

REFERENCES

Wen:2014:MZC

Wang:2011:MMW

Weng:2012:NCC

Wang:2011:CIB

Wang:2011:CHI

Weir:2012:AVC
Jonathan Weir and WeiQi Yan. Authenticating visual cryptography shares using 2D barcodes. Lecture


REFERENCES

Xiao:2010:TAT

Xie:2012:ORI

Xie:2013:SIP

Xiong:2012:CBP

Xie:2014:SCP

Xie:2012:DPK
REFERENCES


Bo-Yin Yang, editor. Post-Quantum Cryptography:


Yamada:2012:PBR Takaaki Yamada and Isao

**Yoshida:2012:OGT**


**Yang:2014:MDF**


**Yoo:2010:IRR**


**Yu:2012:IRI**

REFERENCES

Young:2013:TPC


Yum:2012:OPE


Yoshino:2012:SIP


Yuen:2011:A


Yang:2012:WSI

Chunfang Yang, Fenlin Liu, Shiguo Lian, Xiangyang Luo, and Daoshun Wang. Weighted stego-image steganalysis of messages hidden into each bit plane. *The Co-

You:2012:DDS


You:2010:PSI


Yu:2011:CLE


Yavuz:2012:BFB

[YNR12a] Attila A. Yavuz, Peng Ning, and Michael K. Reiter. BAF and FIBAF: Efficient and publicly verifiable cryptographic schemes for se-

Yavuz:2012:ECR


Yong:2012:SPP


Yoneyama:2012:ORA


Yang:2012:EMA


Yengisetty:2011:AVC


Yang:2012:SAK

Zheng Yang and Jörg Schwenk. Strongly authenticated key exchange protocol from bilinear

Yang:2015:EPS


Yang:2011:CPK


Ylonen:2014:SAA


Yang:2011:CCK


Yang:2011:TRR

REFERENCES

March 4, 2011. CODEN TCSCDI. ISSN 0304-3975 (print), 1879-2294 (electronic).

Yamada:2012:UEW


[YT12]

Yang:2014:IBI


[YTM+14]

Yasuda:2012:ASM


[YTS12]

Yang:2011:ACD


[YTP11]

Yao:2010:ASP


[YWK10]

Yang:2015:RCI

Hong-Ying Yang, Xiang-Yang Wang, Pan-Pan Niu, and Ai-Long Wang. Robust color image watermarking using geometric invariant quaternion polar harmonic transform. ACM

Wang:2011:RDA


Yu:2012:SM


Yoon:2011:SBC


Yang:2012:LUC

Bo Yang and Mingwu Zhang. LR-UESDE: a continual-leakage resilient encryption with un-

Yang:2012:BPN


Yang:2012:NIB


Yang:2014:PST


Zhang:2011:TNT


Zhu:2012:JLS

Xinglei Zhu and Chang W. Chen. A joint layered scheme for reliable and


REFERENCES


Zhao:2010:PSA


Gao:2012:DES


Zadeh:2015:ASP


Zhang:2012:LDC


Zhang:2015:STR


Zhu:2015:IDM


Zhao:2012:IAS


Zhang:2012:EEF


Zhang:2015:RBA


Zhang:2012:CCB


Zhang:2010:ESP


Zhang:2010:NSS

[ZMM+10] Qing Zhang, John McCullogh, Justin Ma, Nabil Scheir, Michael Vrable, Amin Vahdat, Alex C. Snoeren, Geoffrey M. Voelker, and Stefan Savage. Neon: system support for derived


REFERENCES

244

Zhang:2014:NCM


Zhu:2015:PPD


Zwattendorfer:2012:CBL


Zhang:2015:FAA


Zhang:2014:LFL

Zhang:2011:AGK


Zilberberg:2013:PCM


Zhang:2015:FER


Zhou:2011:PSA


Zhang:2014:EFH


REFERENCES

FODY. ISSN 0167-7055 (print), 1467-8659 (electronic).