

Author details

✓

The language has been switched to English

✕

< Return to search results1 of 1

PrintEmail

Maire O'Neill, Máire

Follow this Author

h-index: ⓘ

20

View h-graph

Queen's University Belfast, Belfast, United Kingdom

Author ID: 35079173900 ⓘ

View potential author matches

Other name formats:

O'Neill, Maire

McLoone, Mácaire

O'Neill, Máire

O'Neill, Maire

O'Neill, Máire

McLoone, Máire

Orneill, Máire

O'Neill, Maire

McLoone, Maire

O'Neill, M.

McLoone, M.

O'Neill, Máire

View all

Subject area:

Computer Science

Engineering

Mathematics

Materials Science

Physics and Astronomy

Social Sciences

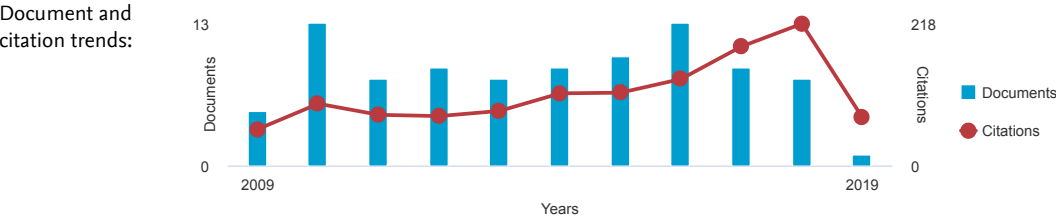
Energy

Decision Sciences

Biochemistry, Genetics and Molecular Biology

Environmental Science

View all



Get citation alerts

+ Add to ORCID ⓘ

Edit author profile

Export profile to SciVal

132 Documents

Cited by 1247 documents

92 co-authors

Author history

View them in search results format >

Sort on:

Date (newest)

Export all









Add all to list









Set document alert

Set document feed












Document title	Authors	Year	Source	Cited by
A theoretical model to link uniqueness and min-entropy for PUF evaluations	Gu, C., Liu, W., Hanley, N., Hesselbarth, R., O'Neill, M.	2019	IEEE Transactions on Computers 68(2),8444682, pp. 287-293	0
View abstract Full Text FinderView at PublisherRelated documents				
Approximate computing and its application to hardware security (Book Chapter)	Liu, W., Gu, C., Qu, G., O'Neill, M.	2018	Cyber-Physical Systems Security pp. 43-67	0
View abstract Full Text FinderView at PublisherRelated documents				
Ultra-Lightweight and Reconfigurable Tristate Inverter Based Physical Unclonable Function Design Open Access	Cui, Y., Gu, C., Wang, C., O'Neill, M., Liu, W.	2018	IEEE Access 6, pp. 28478-28487	0
View abstract Full Text FinderView at PublisherRelated documents				

Document title	Authors	Year	Source	Cited by
Design and Optimization of Modular Multiplication for SIDH	Liu, C., Ni, J., Liu, W., Liu, Z., O'Neill, M.	2018	Proceedings - IEEE International Symposium on Circuits and Systems 2018-May,8351082	1
View abstract Full Text Finder View at Publisher Related documents				
Compact, Scalable, and Efficient Discrete Gaussian Samplers for Lattice-Based Cryptography	Khalid, A., Howe, J., Rafferty, C., Regazzoni, F., O'Neill, M.	2018	Proceedings - IEEE International Symposium on Circuits and Systems 2018-May,8351009	1
View abstract Full Text Finder View at Publisher Related documents				
Design of Majority Logic (ML) Based Approximate Full Adders	Zhang, T., Liu, W., McLarnon, E., O'Neill, M., Lombardi, F.	2018	Proceedings - IEEE International Symposium on Circuits and Systems 2018-May,8350962	0
View abstract Full Text Finder View at Publisher Related documents				
On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography	Howe, J., Khalid, A., Rafferty, C., Regazzoni, F., O'Neill, M.	2018	IEEE Transactions on Computers 67(3),7792671, pp. 322-334	5
View abstract Full Text Finder View at Publisher Related documents				
A machine learning attack resistant multi-PUF design on FPGA	Ma, Q., Gu, C., Hanley, N., (...), Liu, W., O'Neill, M.	2018	Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC 2018-January, pp. 97-104	5
View abstract Full Text Finder View at Publisher Related documents				
Data Compression Device Based on Modified LZ4 Algorithm	Liu, W., Mei, F., Wang, C., O'Neill, M., Swartzlander, E.E.	2018	IEEE Transactions on Consumer Electronics 64(1), pp. 110-117	2
View abstract Full Text Finder View at Publisher Related documents				
FPGA-based strong PUF with increased uniqueness and entropy properties	Gu, C., Hanley, N., O'Neill, M.	2017	Proceedings - IEEE International Symposium on Circuits and Systems 8050838	3
View abstract Full Text Finder View at Publisher Related documents				
Compact and provably secure lattice-based signatures in hardware	Howe, J., Rafferty, C., Khalid, A., O'Neill, M.	2017	Proceedings - IEEE International Symposium on Circuits and Systems 8050566	2
View abstract Full Text Finder View at Publisher Related documents				
XOR gate based low-cost configurable RO PUF	Zhang, L., Wang, C., Liu, W., O'Neill, M., Lombardi, F.	2017	Proceedings - IEEE International Symposium on Circuits and Systems 8050628	3
View abstract Full Text Finder View at Publisher Related documents				
Time-independent discrete Gaussian sampling for post-quantum cryptography	Khalid, A., Howe, J., Rafferty, C., O'Neill, M.	2017	Proceedings of the 2016 International Conference on Field-Programmable Technology, FPT 2016 7929543, pp. 241-244	4
View abstract Full Text Finder View at Publisher Related documents				
Improved reliability of FPGA-based PUF identification generator design Open Access	Gu, C., Hanley, N., O'Neill, M.	2017	ACM Transactions on Reconfigurable Technology and Systems 10(3),20	7

Document title	Authors	Year	Source	Cited by
View abstract  Full Text Finder View at Publisher Related documents				
Novel lightweight FF-APUF design for FPGA	Gu, C., Cui, Y., Hanley, N., O'Neill, M.	2017	International System on Chip Conference 7905439, pp. 75-80	5
View abstract  Full Text Finder View at Publisher Related documents				
Guest editorial: Introduction to the special issue on emerging technologies and designs for application-specific computing	Liu, W., Swartzlander, E.E., O'Neill, M.	2017	IEEE Transactions on Emerging Topics in Computing 5(2),7942331, pp. 148-150	0
Full Text Finder View at Publisher				
Lattice-based cryptography: From reconfigurable hardware to ASIC	Oder, T., Güneysu, T., Valencia, F., (...), O'Neill, M., Regazzoni, F.	2017	2016 International Symposium on Integrated Circuits, ISIC 2016 7829689	5
View abstract  Full Text Finder View at Publisher Related documents				
GLITCH: A discrete Gaussian testing suite for lattice-based cryptography	Howe, J., O'Neill, M.	2017	ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications 4, pp. 413-419	0
View abstract  Full Text Finder View at Publisher Related documents				
A reconfigurable memory PUF based on tristate inverter arrays	Cui, Y., Wang, C., Liu, W., O'Neill, M.	2016	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 7780092, pp. 171-176	4
View abstract  Full Text Finder View at Publisher Related documents				
Guest Editorial: New Frontiers in Signal Processing Applications and Embedded Processing Technologies Open Access	McAllister, J., O'Neill, M., Pelcat, M.	2016	Journal of Signal Processing Systems 84(3), pp. 293-294	0
Full Text Finder View at Publisher				
Optimised Multiplication Architectures for Accelerating Fully Homomorphic Encryption	Cao, X., Moore, C., Oneill, M., Osullivan, E., Hanley, N.	2016	IEEE Transactions on Computers 65(9),7321798, pp. 2794-2806	11
View abstract  Full Text Finder View at Publisher Related documents				
Lattice-based encryption over standard lattices in hardware	Howe, J., Moore, C., O'Neill, M., (...), Guneyusu, T., Beeden, K.	2016	Proceedings - Design Automation Conference 2016-August,7544403	9
View abstract  Full Text Finder View at Publisher Related documents				
Live demonstration: An automatic evaluation platform for physical unclonable function test	Cui, Y., Wang, C., Liu, W., O'Neill, M.	2016	Proceedings - IEEE International Symposium on Circuits and Systems 2016-July,7539068, pp. 2377	1
View abstract  Full Text Finder View at Publisher				
Low-cost configurable ring oscillator PUF with improved uniqueness	Cui, Y., Wang, C., Liu, W., (...), O'Neill, M., Lombardi, F.	2016	Proceedings - IEEE International Symposium on Circuits and Systems 2016-July,7527301, pp. 558-561	5

Document title	Authors	Year	Source	Cited by
View abstract  Full Text Finder View at Publisher Related documents				
Standard lattices in hardware	Howe, J., Moore, C., O'Neill, M., (...), Güneysu, T., Beeden, K.	2016	Proceedings - Design Automation Conference 05-09-June-2016,a162	0
View abstract  Full Text Finder View at Publisher Related documents				
Secure architectures of future emerging cryptography safecrypto	O'Neill, M., O'Sullivan, E., McWilliams, G., (...), Ammar, B., Lund, D.	2016	2016 ACM International Conference on Computing Frontiers - Proceedings pp. 315-322	0
View abstract  Full Text Finder View at Publisher Related documents				
Insecurity by Design: Today's IoT Device Security Problem Open Access	O'Neill, M.	2016	Engineering 2(1), pp. 48-49	14
Full Text Finder View at Publisher Related documents				
An improved second-order power analysis attack based on a new refined expecter: Case study on protected AES	Ahn, H., Hanley, N., O'Neill, M., Han, D.-G.	2016	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9503, pp. 174-186	0
View abstract  Full Text Finder View at Publisher Related documents				
Security analysis on RFID mutual authentication protocol	Kang, Y.S., O'Sullivan, E., Choi, D., O'Neill, M.	2016	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9503, pp. 65-74	0
View abstract  Full Text Finder View at Publisher Related documents				
On the security of balanced encoding countermeasures	Won, Y.-S., Hodgers, P., O'Neill, M., Han, D.-G.	2016	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9514, pp. 242-256	0
View abstract  Full Text Finder View at Publisher Related documents				
Design and Analysis of Inexact Floating-Point Adders	Liu, W., Chen, L., Wang, C., O'Neill, M., Lombardi, F.	2016	IEEE Transactions on Computers 65(1),7070739, pp. 308-314	13
View abstract  Full Text Finder View at Publisher Related documents				
Can leakage models be more efficient? non-linear models in side channel attacks	Tian, Q., O'Neill, M., Hanley, N.	2015	2014 IEEE International Workshop on Information Forensics and Security, WIFS 2014 7084330, pp. 215-220	0
View abstract  Full Text Finder View at Publisher Related documents				
Improving RO PUF design using frequency distribution characteristics Open Access	Yu, Y., Wang, C., Liu, W., Cui, Y., O'Neill, M.	2015	IEICE Electronics Express 12(3)	3
View abstract  Full Text Finder View at Publisher Related documents				
Ultra-compact and robust FPGA-based PUF identification generator	Gu, C., O'Neill, M.	2015	Proceedings - IEEE International Symposium on Circuits and Systems 2015-July,7168788, pp. 934-937	13
View abstract  Full Text Finder View at Publisher Related documents				

Document title	Authors	Year	Source	Cited by
Pre-processing power traces to defeat random clocking countermeasures	Hodgers, P., Hanley, N., O'Neill, M.	2015	Proceedings - IEEE International Symposium on Circuits and Systems 2015-July,7168576, pp. 85-88	2
View abstract Full Text Finder View at Publisher Related documents				
Neural network based attack on a masked implementation of AES	Gilmore, R., Hanley, N., O'Neill, M.	2015	Proceedings of the 2015 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2015 7140247, pp. 106-111	15
View abstract Full Text Finder View at Publisher Related documents				
Introduction for embedded platforms for cryptography in the coming decade	Schaumont, P., O'Neill, M., Güneysu, T.	2015	ACM Transactions on Embedded Computing Systems 14(3),40	1
Full Text Finder View at Publisher				
New FMO type to flag ROI in H.264/AVC	Wang, Y., O'Neill, M., Kurugollu, F.	2015	EUVIP 2014 - 5th European Workshop on Visual Information Processing 7018403	0
View abstract Full Text Finder View at Publisher Related documents				
Privacy region protection for H.264/AVC with enhanced scrambling effect and a low bitrate overhead	Wang, Y., O'Neill, M., Kurugollu, F., O'Sullivan, E.	2015	Signal Processing: Image Communication 35,14960, pp. 71-84	6
View abstract Full Text Finder View at Publisher Related documents				
RO PUF design in FPGAs with new comparison strategies	Liu, W., Yu, Y., Wang, C., Cui, Y., O'Neill, M.	2015	Proceedings - IEEE International Symposium on Circuits and Systems 2015-July,7168574, pp. 77-80	8
View abstract Full Text Finder View at Publisher Related documents				
Practical lattice-based digital signature schemes	Howe, J., Pöppelmann, T., O'Neill, M., O'Sullivan, E., Güneysu, T.	2015	ACM Transactions on Embedded Computing Systems 14(3),41	17
View abstract Full Text Finder View at Publisher Related documents				
A unique and robust single slice FPGA identification generator	Gu, C., Murphy, J., O'Neill, M.	2014	Proceedings - IEEE International Symposium on Circuits and Systems 6865362, pp. 1223-1226	11
View abstract Full Text Finder View at Publisher Related documents				
Empirical evaluation of multi-device profiling side-channel attacks	Hanley, N., O'Neill, M., Tunstall, M., Marnane, W.P.	2014	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 6986091	0
View abstract Full Text Finder View at Publisher Related documents				
Accelerating integer-based fully homomorphic encryption using Comba multiplication	Moore, C., O'Neill, M., Hanley, N., O'Sullivan, E.	2014	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 6986063	7
View abstract Full Text Finder View at Publisher Related documents				
Bit erasure analysis of binary adders in quantum-dot cellular automata	McLarnon, E., O'Neill, M., Liu, W., Hänninen, I.	2014	14th IEEE International Conference on Nanotechnology, IEEE-NANO 2014 6968030, pp. 296-301	0

Document title	Authors	Year	Source	Cited by
View abstract  Full Text Finder View at Publisher Related documents				
Security issues in QCA circuit design - Power analysis attacks	Liu, W., Srivastava, S., O'Neill, M., Swartzlander Jr., E.E.	2014	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8280 LNCS, pp. 194-222	0
View abstract  Full Text Finder View at Publisher Related documents				
A first step toward cost functions for quantum-dot cellular automata designs	Liu, W., Lu, L., Oneill, M., Swartzlander, E.E.	2014	IEEE Transactions on Nanotechnology 13(3),6746210, pp. 476-487	53
View abstract  Full Text Finder View at Publisher Related documents				
Inexact floating-point adder for dynamic image processing	Liu, W., Chen, L., Wang, C., O'Neill, M., Lombardi, F.	2014	14th IEEE International Conference on Nanotechnology, IEEE-NANO 2014 6967953, pp. 239-243	7
View abstract  Full Text Finder View at Publisher Related documents				
High-speed fully homomorphic encryption over the integers	Cao, X., Moore, C., O'Neill, M., Hanley, N., O'Sullivan, E.	2014	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 8438, pp. 169-180	10
View abstract  Full Text Finder View at Publisher Related documents				
Practical homomorphic encryption: A survey	Moore, C., O'Neill, M., O'Sullivan, E., Doroz, Y., Sunar, B.	2014	Proceedings - IEEE International Symposium on Circuits and Systems 6865753, pp. 2792-2795	24
View abstract  Full Text Finder View at Publisher Related documents				
A tunable selective encryption scheme for H.264/AVC	Wang, Y., O'Neill, M., Kurugollu, F.	2013	2013 4th European Workshop on Visual Information Processing, EUVIP 2013 6623965, pp. 136-141	0
View abstract  Full Text Finder Related documents				
Targeting FPGA DSP slices for a large integer multiplier for integer based FHE	Moore, C., Hanley, N., McAllister, J., (...), O'Sullivan, E., Cao, X.	2013	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 7862 LNCS, pp. 226-237	18
View abstract  Full Text Finder View at Publisher Related documents				
Privacy region protection for H.264/AVC by encrypting the intra prediction modes without drift error in i frames	Wang, Y., O'Neill, M., Kurugollu, F.	2013	ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings 6638201, pp. 2964-2968	6
View abstract  Full Text Finder View at Publisher Related documents				
A tunable encryption scheme and analysis of fast selective encryption for CAVLC and CABAC in H.264/AVC	Wang, Y., O'Neill, M., Kurugollu, F.	2013	IEEE Transactions on Circuits and Systems for Video Technology 23(9),6469203, pp. 1476-1490	32
View abstract  Full Text Finder View at Publisher Related documents				
Pre-processing power traces with a phase-sensitive detector	Hodgers, P., Hanley, N., O'Neill, M.	2013	Proceedings of the 2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013 6581578, pp. 131-136	1
View abstract  Full Text Finder View at Publisher Related documents				











Document title	Authors	Year	Source	Cited by
Partial encryption by randomized zig-zag scanning for video encoding	Wang, Y., O'Neill, M., Kurugollu, F.	2013	Proceedings - IEEE International Symposium on Circuits and Systems 6571824, pp. 229-232	3
View abstract Full Text Finder View at Publisher Related documents				
Power analysis attack of QCA circuits: A case study of the Serpent cipher	Liu, W., Srivastava, S., Lu, L., O'Neill, M., Swartzlander, E.E.	2013	Proceedings - IEEE International Symposium on Circuits and Systems 6572282, pp. 2075-2078	0
View abstract Full Text Finder View at Publisher Related documents				
QCA Systolic array design	Lu, L., Liu, W., O'Neill, M., Swartzlander Jr., E.E.	2013	IEEE Transactions on Computers 62(3),6109234	33
View abstract Full Text Finder View at Publisher Related documents				
Are QCA cryptographic circuits resistant to power analysis attack?	Liu, W., Srivastava, S., Lu, L., Orneill, M., Swartzlander, E.E.	2012	IEEE Transactions on Nanotechnology 11(6),6323038, pp. 1239-1251	43
View abstract Full Text Finder View at Publisher Related documents				
A review of QCA adders and metrics	Liu, W., O'Neill, M., Swartzlander, E.E.	2012	Conference Record - Asilomar Conference on Signals, Systems and Computers 6489112, pp. 747-751	5
View abstract Full Text Finder View at Publisher Related documents				
The improved sign bit encryption of motion vectors for H.264/AVC	Wang, Y., O'Neill, M., Kurugollu, F.	2012	European Signal Processing Conference 6333990, pp. 1752-1756	13
View abstract Full Text Finder Related documents				
Hardware comparison of the ISO/IEC 29192-2 block ciphers	Hanley, N., O'Neill, M.	2012	Proceedings - 2012 IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2012 6296448, pp. 57-62	15
View abstract Full Text Finder View at Publisher Related documents				
Application-oriented SHA-256 hardware design for low-cost RFID	Cao, X., O'Neill, M.	2012	ISCAS 2012 - 2012 IEEE International Symposium on Circuits and Systems 6271509, pp. 1412-1415	6
View abstract Full Text Finder View at Publisher Related documents				
Adaptive binary mask for privacy region protection	Wang, Y., O'Neill, M., Kurugollu, F.	2012	ISCAS 2012 - 2012 IEEE International Symposium on Circuits and Systems 6271429, pp. 1127-1130	6
View abstract Full Text Finder View at Publisher Related documents				
Cost-efficient decimal adder design in Quantum-dot cellular automata	Liu, W., Lu, L., O'Neill, M., Swartzlander, E.E.	2012	ISCAS 2012 - 2012 IEEE International Symposium on Circuits and Systems 6271491, pp. 1347-1350	9
View abstract Full Text Finder View at Publisher Related documents				
Self-timed physically unclonable functions	Murphy, J., O'Neill, M., Burns, F., (...), Yakovlev, A., Halak, B.	2012	2012 5th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2012 Conference and Workshops 6208707	3
View abstract Full Text Finder View at Publisher Related documents				












Document title	Authors	Year	Source	Cited by
A novel common control channel security framework for cognitive radio networks	Safdar, G.A., O'Neill, M.	2012	International Journal of Autonomous and Adaptive Communications Systems 5(2), pp. 125-145	4
View abstract Full Text Finder View at Publisher Related documents				
A private and scalable authentication for rfid systems using reasonable storage	Cao, X., O'Neill, M.	2011	Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011 6120841, pp. 373-380	0
View abstract Full Text Finder View at Publisher Related documents				
Variable window power spectral density attack	Hodgers, P., Boey, K.H., O'Neill, M.	2011	2011 IEEE International Workshop on Information Forensics and Security, WIFS 2011 6123145	2
View abstract Full Text Finder View at Publisher Related documents				
Power spectral density side channel attack overlapping window method	Hodgers, P., Boey, K.H., O'Neill, M.	2011	Proceedings - 2011 14th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, DSD 2011 6037421, pp. 274-278	2
View abstract Full Text Finder View at Publisher Related documents				
A forward private protocol based on PRNG and LPN for low-cost RFID	Cao, X., O'Neill, M.	2011	SECRYPT 2011 - Proceedings of the International Conference on Security and Cryptography pp. 287-292	0
View abstract Full Text Finder Related documents				
Design of quantum-dot cellular automata circuits using cut-set retiming	Liu, W., Lu, L., Orneill, M., Swartzlander Jr., E.E., Woods, R.	2011	IEEE Transactions on Nanotechnology 10(5),5724305, pp. 1150-1160	16
View abstract Full Text Finder View at Publisher Related documents				
Design rules for Quantum-dot Cellular Automata	Liu, W., Lu, L., O'Neill, M., Swartzlander, E.E.	2011	Proceedings - IEEE International Symposium on Circuits and Systems 5938077, pp. 2361-2364	39
View abstract Full Text Finder View at Publisher Related documents				
F-HB: An efficient forward private protocol	Cao, X., O'Neill, M.	2011	Proceedings - 2011 Workshop on Lightweight Security and Privacy: Devices, Protocols, and Applications, LightSec 2011 5749559, pp. 53-60	8
View abstract Full Text Finder View at Publisher Related documents				
How resistant are SBoxes to power analysis attacks?	Boey, K.H., O'Neill, M., Woods, R.	2011	2011 4th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2011 - Proceedings 5720614	2
View abstract Full Text Finder View at Publisher Related documents				
A hardware wrapper for the SHA-3 hash algorithms	Baldwin, B., Byrne, A., Lu, L., (...), O'Neill, M., Marnane, W.P.	2010	IET Conference Publications 2010(566 CP), pp. 1-6	5
View abstract Full Text Finder View at Publisher Related documents				

Document title	Authors	Year	Source	Cited by
Evaluation of Random Delay Insertion against DPA on FPGAs	Lu, Y., O'Neill, M., McCanny, J.	2010	ACM Transactions on Reconfigurable Technology and Systems 4(1),11	8
View abstract Full Text Finder View at Publisher Related documents				
Random clock against differential power analysis	Boey, K.H., Lu, Y., O'Neill, M., Woods, R.	2010	IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings, APCCAS 5774887, pp. 756-759	12
View abstract Full Text Finder View at Publisher Related documents				
SEED masking implementations against power analysis attacks	Lu, Y., Boey, K.-H., Hodgers, P., O'Neill, M.	2010	IEEE Asia-Pacific Conference on Circuits and Systems, Proceedings, APCCAS 5775039, pp. 1199-1202	1
View abstract Full Text Finder View at Publisher Related documents				
A high-speed key exchange multi-core SoC architecture for IPSec real-time internet traffic	Moore, P., O'Neill, M., McLaughlin, K., Sezer, S.	2010	2010 IEEE Globecom Workshops, GC'10 5700456, pp. 903-907	1
View abstract Full Text Finder View at Publisher Related documents				
Montgomery modular multiplier design in quantum-dot cellular automata using cut-set retiming	Liu, W., Lu, L., O'Neill, M., Swartzlander Jr., E.E.	2010	2010 10th IEEE Conference on Nanotechnology, NANO 2010 5697740, pp. 205-210	7
View abstract Full Text Finder View at Publisher Related documents				
Lightweight DPA resistant solution on FPGA to counteract power models	Lu, Y., Boey, K.-H., Hodgers, P., O'Neill, M.	2010	Proceedings - 2010 International Conference on Field-Programmable Technology, FPT'10 5681790, pp. 178-183	5
View abstract Full Text Finder View at Publisher Related documents				
Security of AES Sbox designs to power analysis	Boey, K.H., Hodgers, P., Lu, Y., O'Neill, M., Woods, R.	2010	2010 IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2010 - Proceedings 5724741, pp. 1232-1235	6
View abstract Full Text Finder View at Publisher Related documents				
FPGA implementations of the round two SHA-3 candidates	Baldwin, B., Byrnet, A., Lu, L., (...), O'Neill, M., Marnane, W.P.	2010	Proceedings - 2010 International Conference on Field Programmable Logic and Applications, FPL 2010 5694284, pp. 400-407	20
View abstract Full Text Finder View at Publisher Related documents				
QCA systolic matrix multiplier	Lu, L., Liu, W., O'Neill, M., Swartzlander Jr., E.E.	2010	Proceedings - IEEE Annual Symposium on VLSI, ISVLSI 2010 5572762, pp. 149-154	15
View abstract Full Text Finder View at Publisher Related documents				
Differential power analysis of CAST-128	Boey, K.H., Lu, Y., O'Neill, M., Woods, R.	2010	Proceedings - IEEE Annual Symposium on VLSI, ISVLSI 2010 5572761, pp. 143-148	2
View abstract Full Text Finder View at Publisher Related documents				
Ultra-lightweight true random number generators	Wu, J., O'Neill, M.	2010	Electronics Letters 46(14), pp. 988-990	13

Document title	Authors	Year	Source	Cited by
View abstract ▾ Full Text Finder View at Publisher Related documents				
Low-cost digital signature architecture suitable for radio frequency identification tags	O'Neill, M., Robshaw, M.J.B.	2010	IET Computers and Digital Techniques 4(1), pp. 14-26	16
View abstract ▾ Full Text Finder View at Publisher Related documents				
Performance analysis of novel randomly shifted certification authority authentication protocol for MANETs Open Access	Safdar, G.A., O'Neill, M.P.	2009	Eurasip Journal on Wireless Communications and Networking 2009,243956	4
View abstract ▾ Full Text Finder View at Publisher Related documents				
ASIC evaluation of ECHO hash function	Lu, L., O'Neill, M., Swartzlander Jr., E.E.	2009	Proceedings - IEEE International SOC Conference, SOCC 2009 5398014, pp. 387-390	0
View abstract ▾ Full Text Finder View at Publisher Related documents				
Differential power analysis resistance of Camellia and countermeasure strategy on FPGAs	Lu, Y., O'Neill, M.P., McCanny, J.V.	2009	Proceedings of the 2009 International Conference on Field-Programmable Technology, FPT'09 5377650, pp. 183-189	1
View abstract ▾ Full Text Finder View at Publisher Related documents				
IS the differential frequency-based attack effective against random delay insertion?	Lu, Y., Boey, K.H., O'Neill, M., McCanny, J.V., Satoh, A.	2009	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 5336291, pp. 51-56	3
View abstract ▾ Full Text Finder View at Publisher Related documents				
Common control channel security framework for cognitive radio networks	Safdar, G.A., O'Neill, M.	2009	IEEE Vehicular Technology Conference 5073450	29
View abstract ▾ Full Text Finder View at Publisher Related documents				
FPGA implementation and analysis of random delay insertion countermeasure against DPA	Lu, Y., O'Neill, M.P., McCanny, J.V.	2008	Proceedings of the 2008 International Conference on Field-Programmable Technology, ICFPT 2008 4762384, pp. 201-208	24
View abstract ▾ Full Text Finder View at Publisher Related documents				
Differential power analysis of a SHACAL-2 hardware implementation	Lu, Y., O'Neill, M.P., McCanny, J.V.	2008	Proceedings - IEEE International Symposium on Circuits and Systems 4542072, pp. 2933-2936	5
View abstract ▾ Full Text Finder View at Publisher Related documents				
Randomly shifted certification authority authentication protocol for MANETs	Safdar, G.A., McLoone, M.	2007	2007 16th IST Mobile and Wireless Communications Summit 4299197	6
View abstract ▾ Full Text Finder View at Publisher Related documents				
Identity based public key exchange (idpke) for wireless ad hoc networks	Grath, C.M., Safdar, G.A., McLoone, M.	2007	SECURITY 2007 - International Conference on Security and Cryptography, Proceedings pp. 167-170	0
View abstract ▾ Full Text Finder Related documents				

Document title	Authors	Year	Source	Cited by
Exploring technology related design-space limitations of high performance network processing	McCanny, J.V., Sezer, S., O'Neill, M.	2007	ESSCIRC 2007 - Proceedings of the 33rd European Solid-State Circuits Conference 4430285, pp. 222-231	0
View abstract Full Text Finder View at Publisher Related documents				
New architectures for low-cost public key cryptography on RFID tags	McLoone, M., Robshaw, M.J.B.	2007	Proceedings - IEEE International Symposium on Circuits and Systems 4253016, pp. 1827-1830	15
View abstract Full Text Finder Related documents				
MONET special issue on next generation hardware architectures for secure mobile computing	Sklavos, N., McLoone, M., Zhang, X.	2007	Mobile Networks and Applications 12(4), pp. 229-230	8
Full Text Finder View at Publisher				
High-speed & low area hardware architectures of the whirlpool hash function	McLoone, M., Mclvor, C.	2007	Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology 47(1), pp. 47-57	3
View abstract Full Text Finder View at Publisher Related documents				
An adaptable and scalable asymmetric Cryptographic processor	Smyth, N., McLoone, M., McCanny, J.V.	2006	Proceedings of the International Conference on Application-Specific Systems, Architectures and Processors 4019538, pp. 341-346	11
View abstract Full Text Finder View at Publisher Related documents				
Limitations of existing wireless networks authentication and key management techniques for MANETs	Safdar, G.A., McGrath, C., McLoone, M.	2006	Proceedings of ISCN'06: 7th International Symosium on Computer Networks 2006,1662516	5
View abstract Full Text Finder View at Publisher Related documents				
Hardware elliptic curve cryptographic processor over GF(p)	Mclvor, C.J., McLoone, M., McCanny, J.V.	2006	IEEE Transactions on Circuits and Systems I: Regular Papers 53(9), pp. 1946-1957	81
View abstract Full Text Finder View at Publisher Related documents				
WLAN security processor	Smyth, N., McLoone, M., McCanny, J.V.	2006	IEEE Transactions on Circuits and Systems I: Regular Papers 53(7), pp. 1506-1520	12
View abstract Full Text Finder View at Publisher Related documents				
Performance analysis of SHACAL-1 encryption hardware architectures (Chapter)	McLoone, M., McCanny, J.V.	2005	<i>New Algorithms, Architectures and Applications for Reconfigurable Computing</i> pp. 251-264	0
View abstract Full Text Finder View at Publisher Related documents				
Reconfigurable processor for public-key cryptography	Smyth, N., McLoone, M., McCanny, J.V.	2005	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 2005,1579848, pp. 110-115	5
View abstract Full Text Finder View at Publisher Related documents				
High-speed hardware architectures of the whirlpool hash function	McLoone, M., Mclvor, C., Savage, A.	2005	Proceedings - 2005 IEEE International Conference on Field Programmable Technology 2005,1568539, pp. 147-153	13

Document title	Authors	Year	Source	Cited by
View abstract  Full Text Finder View at Publisher Related documents				
High-radix systolic modular multiplication on reconfigurable hardware	Mclvor, C., McLoone, M., McCanny, J.V.	2005	Proceedings - 2005 IEEE International Conference on Field Programmable Technology 2005,1568518, pp. 13-18	20
View abstract  Full Text Finder View at Publisher Related documents				
Reconfigurable instruction interface architecture for private-key cryptography on the Altera Nios-II processor	Moore, P., McLoone, M., Sezer, S.	2005	Proceedings - Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop AICT/SAPIR/ELETE 2005 2005,1517645, pp. 296-299	2
View abstract  Full Text Finder View at Publisher Related documents				
Reconfigurable cryptographic RISC microprocessor	Smyth, N., McLoone, M., McCanny, J.V.	2005	2005 IEEE VLSI-TSA International Symposium on VLSI Design, Automation and Test,(VLSI-TSA-DAT) 2005,1500012, pp. 29-32	1
View abstract  Full Text Finder View at Publisher Related documents				
Reconfigurable architectures for network processing	Sezer, S., McLoone, M., McCanny, J.	2005	2005 IEEE VLSI-TSA International Symposium on VLSI Design, Automation and Test,(VLSI-TSA-DAT) 2005,1500024, pp. 75-83	0
View abstract  Full Text Finder View at Publisher Related documents				
Hardware performance analysis of the SHACAL-2 encryption algorithm	McLoone, M.	2005	IEE Proceedings: Circuits, Devices and Systems 152(5), pp. 478-484	1
View abstract  Full Text Finder View at Publisher Related documents				
Coarsely Integrated Operand Scanning (CIOS) architecture for high-speed Montgomery modular multiplication	McLoone, M., Mclvor, C., McCanny, J.V.	2004	Proceedings - 2004 IEEE International Conference on Field-Programmable Technology, FPT '04 pp. 185-191	7
View abstract  Full Text Finder View at Publisher Related documents				
FPGA montgomery multiplier architectures - A comparison	Mclvor, C., McLoone, M., McCanny, J.V.	2004	Proceedings - 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, FCCM 2004 pp. 279-282	20
View abstract  Full Text Finder View at Publisher Related documents				
Montgomery modular multiplication architecture for public key cryptosystems	McLoone, M., Mclvor, C., McCanny, J.V.	2004	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation pp. 349-354	2
View abstract  Full Text Finder View at Publisher Related documents				
Reconfigurable hardware acceleration of wlan security	Smyth, N., McLoone, M., McCanny, J.V.	2004	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation pp. 194-199	3
View abstract  Full Text Finder View at Publisher Related documents				
Modified Montgomery modular multiplication and RSA exponentiation techniques	Mclvor, C., McLoone, M., McCanny, J.V.	2004	IEE Proceedings: Computers and Digital Techniques 151(6), pp. 402-408	107

Document title	Authors	Year	Source	Cited by
View abstract  Full Text Finder View at Publisher Related documents				
FPGA montgomery modular multiplication architectures suitable for ECCs over GF(p)	McIvor, C., McLoone, M., McCanny, J.V.	2004	Proceedings - IEEE International Symposium on Circuits and Systems 3, pp. III509-III512	5
View abstract  Full Text Finder Related documents				
Improved Montgomery modular inverse algorithm	McIvor, C., McLoone, M., McCanny, J.V.	2004	Electronics Letters 40(18), pp. 1110-1112	25
View abstract  Full Text Finder View at Publisher Related documents				
Very high speed 17 Gbps SHACAL encryption architecture	McLoone, M., McCanny, J.V.	2003	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2778, pp. 111-120	5
View abstract  Full Text Finder View at Publisher Related documents				
Fast montgomery modular multiplication and RSA cryptographic processor architectures	McIvor, C., McLoone, M., McCanny, J.V., Daly, A., Marnane, W.	2003	Conference Record of the Asilomar Conference on Signals, Systems and Computers 1, pp. 379-384	89
View abstract  Full Text Finder Related documents				
High-performance FPGA implementation of DES using a novel method for implementing the key schedule	McLoone, M., McCanny, J.V.	2003	IEE Proceedings: Circuits, Devices and Systems 150(5), pp. 373-378	26
View abstract  Full Text Finder View at Publisher Related documents				
A high-speed, low latency RSA decryption silicon core	McIvor, C., McLoone, M., McCanny, J.V.	2003	Proceedings - IEEE International Symposium on Circuits and Systems 4, pp. IV133-IV136	7
View abstract  Full Text Finder Related documents				
Generic architecture and semiconductor intellectual property cores for advanced encryption standard cryptography	McLoone, M., McCanny, J.V.	2003	IEE Proceedings: Computers and Digital Techniques 150(4), pp. 239-244	12
View abstract  Full Text Finder View at Publisher Related documents				
Rijndael FPGA implementations utilising look-up tables	McLoone, M., McCanny, J.V.	2003	Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology 34(3), pp. 261-275	44
View abstract  Full Text Finder View at Publisher Related documents				
A single-chip IPSEC cryptographic processor	McLoone, M., McCanny, J.V.	2002	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation 2002-January,1049698, pp. 133-138	27
View abstract  Full Text Finder View at Publisher Related documents				
Efficient single-chip implementation of SHA-384 and SHA-512	McLoone, M., McCanny, J.V.	2002	Proceedings - 2002 IEEE International Conference on Field-Programmable Technology, FPT 2002 1188699, pp. 311-314	38
View abstract  Full Text Finder View at Publisher Related documents				

Document title	Authors	Year	Source	Cited by
Single-chip FPGA implementation of the advanced encryption standard algorithm	McLoone, M., McCanny, J.V.	2001	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2147, pp. 152-161	18
View abstract ▾ Full Text Finder View at Publisher Related documents				
High performance single-chip fpga rijndael algorithm implementations	McLoone, M., McCanny, J.V.	2001	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2162, pp. 65-76	73
View abstract ▾ Full Text Finder View at Publisher Related documents				
Rijndael FPGA implementation utilizing look-up tables	McLoone, M., McCanny, J.V.	2001	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation pp. 349-360	57
View abstract ▾ Full Text Finder Related documents				
High performance FPGA implementation of DES	McLoone, Maire, McCanny, John V.	2000	IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation pp. 374-383	12
View abstract ▾ Full Text Finder View at Publisher Related documents				

Display: 200 ▾ results per page

1

^ Top of page

The data displayed above is compiled exclusively from documents indexed in the Scopus database. To request corrections to any inaccuracies or provide any further feedback, please use the [Author Feedback Wizard](#) .

About Scopus

- What is Scopus
- Content coverage
- Scopus blog
- Scopus API
- Privacy matters

Language

- 日本語に切り替える
- 切换到简体中文
- 切换到繁體中文
- Русский язык

Customer Service

- Help
- Contact us



[Terms and conditions](#) ↗ [Privacy policy](#) ↗

Copyright © 2019 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.
We use cookies to help provide and enhance our service and tailor content. By continuing, you agree to the use of cookies.

