Cuauhtemoc Mancillas

Centro de Investigación y de Estudios Avanzados, CINVESTAV-IPN

Cryptography
Reconfigurable Hardware

	Total	Desde 2019
Citas	458	315
Índice h	12	9
Índice i10	13	8

TÍTULO	CITADO POR	AÑO
LightMAC: Fork it and make it faster N Datta, A Dutta, C Mancillas-López Advances in Mathematics of Communications, 0-0	1	2023
ISAP + : ISAP with Fast Authentication A Bhattacharjee, A Chakraborti, N Datta, C Mancillas-López, M Nandi International Conference on Cryptology in India, 195-219	3	2022
Co-design for Generation of Large Random Sequences on Zynq FPGA BM Hernández-Morales, S Díaz-Santiago, C Mancillas-López IEEE Embedded Systems Letters	1	2022
An Ultra-Fast Authenticated Encryption Scheme with Associated Data Using AES-OTR C Mancillas-López, B Ovilla-Martinez Journal of Circuits, Systems and Computers 31 (09), 2250167	4	2022
Light-OCB: parallel lightweight authenticated cipher with full security A Chakraborti, N Datta, A Jha, C Mancillas-López, M Nandi International Conference on Security, Privacy, and Applied Cryptography …	2	2021
tHyENA: Making HyENA Even Smaller A Chakraborti, N Datta, A Jha, C Mancillas-López, M Nandi International Conference on Cryptology in India, 26-48		2021
Elastic-tweak: A framework for short tweak tweakable block cipher A Chakraborti, N Datta, A Jha, C Mancillas-López, M Nandi, Y Sasaki International Conference on Cryptology in India, 114-137	17	2021
A lightweight security protocol for beacons BLE KJ Campos-Cruz, C Mancillas-López, B Ovilla-Martinez 2021 18th international conference on electrical engineering, computing …	4	2021
The use of ellipse-based estimator as a sub-key distinguisher for Side-Channel Analysis AF Martínez-Herrera, C Mex-Perera, C Mancillas-López, C Del-Valle-Soto, ... Computers & Electrical Engineering 94, 107311		2021
Designing an authenticated Hash function with a 2D chaotic map LG De la Fraga, C Mancillas-López, E Tlelo-Cuautle Nonlinear Dynamics 104 (4), 4569-4580	30	2021
FPGA implementation of some second round NIST lightweight cryptography candidates B Ovilla-Martínez, C Mancillas-López, AF Martínez-Herrera, ... Electronics 9 (11), 1940	6	2020

TÍTULO	CITADO POR	AÑO
ESTATE: A lightweight and low energy authenticated encryption mode A Chakraborti, N Datta, A Jha, C Mancillas-López, M Nandi, Y Sasaki IACR Transactions on Symmetric Cryptology, 350-389	33	2020
Pipelined hardware implementation of COPA, ELmD, and COLM L Bossuet, C Mancillas-López, B Ovilla-Martínez IEEE Transactions on Computers 69 (10), 1533-1543	4	2020
On Random Read Access in OCB A Jha, C Mancillas-López, M Nandi, SS Gupta IEEE Transactions on Information Theory 65 (12), 8325-8344	3	2019
INT-RUP secure lightweight parallel AE modes A Chakraborti, N Datta, A Jha, C Mancillas-López, M Nandi, Y Sasaki IACR Transactions on Symmetric Cryptology, 81-118	14	2019
Constant-time hardware computation of elliptic curve scalar multiplication around the 128 bit security level AU Ay, C Mancillas-López, E Öztürk, F Rodríguez-Henríquez, E Savaş Microprocessors and Microsystems 62, 79-90	10	2018
Disk encryption: do we need to preserve length? D Chakraborty, CM López, P Sarkar Journal of Cryptographic Engineering 8, 49-69	14	2018
Hardware implementation of pseudo-random number generators based on chaotic maps LG de la Fraga, E Torres-Pérez, E Tlelo-Cuautle, C Mancillas-López Nonlinear Dynamics 90, 1661-1670	131	2017
FAST: disk encryption and beyond D Chakraborty, S Ghosh, CM López, P Sarkar Cryptology ePrint Archive	13	2017
GCM implementations of Camellia-128 and SMS4 by optimizing the polynomial multiplier AF Martínez-Herrera, C Mancillas-López, C Mex-Perera Microprocessors and Microsystems 45, 129-140	8	2016