


10.1109/ISICIR.2014.7029580

10.1016/j.ipl.2014.01.007

Albrecht MR, Fitzpatrick R, Göpfert F. 2014. On the Efficacy of Solving LWE by Reduction to Unique-SVP. In Information
Science, Vol. 8565). Available from: 10.1007/978-3-319-12160-4_18

Distinguishers for Feistel- and Skipjack-Type Ciphers. In Applied Cryptography and Network Security. Springer. pp. 271-
288. (Lecture Notes in Computer Science, Vol. 8479). Available from: 10.1007/978-3-662-43933-3_2


8544). Available from: 10.1007/978-3-319-08344-5_28


In Proceedings of 2012 International Conference on Reconfigurable Computing and FPGAs (ReConFig). IEEE. Available
from: 10.1109/ReConFig.2012.6416743

Resistance for Constrained Hardware. In Cryptographic Hardware and Embedded Systems - CHES 2013: 15th
Notes in Computer Science, Vol. 8086). Available from: 10.1007/978-3-642-40349-1_9


Bogdanov A, Kavun EB, Tischhauser E, Yalcin T. 2012. Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks. In International Conference on Reconfigurable Computing and FPGAs (ReConFig) 2012 . IEEE. Available from: 10.1109/ReConFig.2012.6416744