Abstract

Cryptography is dealing with a lot of different algorithms which are much secure in various aspects but there are two major problems coming in the cryptographic algorithms, first the portability of algorithm from heavy applications to light applications and second the current Method of Formal Coding-Side Channel Attack (MFCSCA) which are targeting XOR function of the algorithms. To resolve these two problems we propose a new algorithm by using AES algorithm with lattice concept of multidimensionality. In this paper, we propose a new algorithm by combining the concepts of mathematics and multidimensionality concept of physics which solve both the problems of the encryption algorithms.

References

- Changyong Peng, Chuangying Zhu, Yuefei Zhu, Fei Kang; "Symbolic computation in block cipher with application to PRESENT";
- Paweł Chodowiec and Kris Gaj; "Very Compact FPGA Implementation of the AES
Proposal for Portable Approach in Advance Encryption Standard

- Changyong Peng, Chuangying Zhu, Yuefei Zhu, Fei Kang; Improved side channel attack on the block cipher NOEKEON.
- P. S. L. M. Barreto and V. Rijmen; The Whirlpool hashing function.
- Taizo Shirai and Kyoji Shubitani; On Feistel Structures Using a Diusion Switching Mechanism.
- FIPS PUB 180-4, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION: Secure Hash Standard (SHS); Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900, March 2012
- John Kelsey, Bruce Schneier, and David Wagner; Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA.
- M. L. Miller, I. J. Cox and J. Bloom, Informed Embedding Exploiting Image and
- E Biham, A Biryukov, An Improvement of Davies’ Attack on DES”, in Journal of Cryptology v 10 no 3 (Summer 97) pp 195–205

Index Terms

Computer Science  Security

Keywords
Lattice based transpose  Feistel structure  S-Box  Key Permutation
Kirchhoff’s principle
MFCSCA