{tag} {/tag}

IJCA Special Issue on International Conference on Electronics, Communication and Information systems

ICECI - Number 3

Year of Publication: 2012

Authors:

M. Petchiammal

G. Ramyadevi

{bibtex}iceci1020.bib{/bibtex}

Abstract

The DPA attack can efficiently disclose the secret key of an AES Engine easily. To increase DPA Resistant of the AES engine by XORing the generated 16 bit from Pseudo Random Number Generator with the cipher text from the AES Engine. The cipher text is created by AES algorithm which is very Efficient Algorithm for data Securing. The 16 Bit Sequence Generator Circuit also provide Reduction in Area occupied by the Countermeasure circuit and Delay of propagation time by using pipelining process. The Speed of the DPA Countermeasure circuit also increased without degradation in throughput.

References

- P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology, 1999, pp. 388–397.
- D. Hwang, K. Tiri, A. Hodjat, B. -C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-based security coprocessor IC in 0. 18- ?m CMOS with resistance to differential power analysis side-channel attacks," IEEEJ. Solid-State Circuits, vol. 41, no. 4, pp. 781–792, Apr. 2006.
- C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," IEEE J. Solid-State Circuits, vol. 45, no. 1, pp. 23–31, Jan. 2010.
- M. -L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in Proc. CHES, 2001, pp. 309–318.
- D. Suzuki, M. Saeki, and T. Ichikawa, "Random switching logic: A countermeasure against DPA based on transition probability," Cryptology ePrint Archive, Rep. 2004/346, 2004. [Online]. Available:http://eprint. iacr. org
- E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-Box," in Proc. 12th Int. Work-shop FSE, 2005, pp. 413–423.
- E. Trichina, T. Korkishkoand, and K. H. Lee, "Small size, low power, side channel-immune AES synthesis results," in Proc. AES, vol. 3373, Lecture Notes in Computer Science, 2005, pp. 113–127.
- Mohammad Musa, Edward Schaefer, and Stephen Wedig, A simpli?ed AES algorithm and its linear and di?erentialcryptanalyses, Cryptologia 27 (April 2003), no. 2, 148–177.
- A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 19
- FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U. S. Department of Commerce, November 2001(http://csrc. nist. gov/ publications/?ps/?ps197/?ps-197. pdf).
- Stalling, W. , "The Advanced Encryption Standard",Cryptologia, vol. 26, 2002, pp. 165-188.

Index Terms

Computer Science Security

Keywords

Differential Power Analysis (dpa) Ring Oscillators True Random Number Generator

(trng) Pseudo Random Number Generator (prng)