REFERENCES/BIBLIOGRAPHY


[38] E. Biham,(1992) “On the applicability of differential cryptanalysis to hash functions,” E.I.S.S. Workshop on Cryptographic Hash Functions, Oberwolfach (D), March 25-27,


[58] HoWon Kim1, YongJe Choi1 and MooSeop Kim1(2005), Design and Implementation of a Crypto Processor and Its Application to Security System Department of Information Security, CIS’ Proceedings of the 2005 international conference on Computational Intelligence and Security - Volume Part II Pages 1104-1109


On the Elliptic Curve Digital Signature Algorithm, Tunghai Science Vol. 8: 109–126


[73] Josh Jaffe(2007), A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter, Published in: Proceeding CHES ’ Proceedings of the 9th international workshop on Cryptographic Hardware and Embedded Systems Pages 1 - 13


CA, January 17,


[91] Mike Hamburg, Accelerating AES with Vector Permute

Instructions, Proceeding CHES ’09 Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems Pages 18 – 32


Curry, Ian, Entrust Technologies, “Version 3 X.509 Certificates”, version 1.0


(DAC), ACM Press, pp. 753–760.


[125] S. Murphy and M.J.B. Robshaw(2002), Essential Algebraic Structure Within the AES
Published in: · Proceeding CRYPTO ' Proceedings of the 22nd Annual International Cryptology
Conference on Advances in Cryptology, Pages 1-16

RMI based Java Message Passing Systems. In Proc. 5th ACIS Intl. Conf. on Software
Engineering Research, Management and Applications (SERA’07),
pages 153 – 159, Busan, Korea. pages 17

[127] Stephen N. Freund and John C. Mitchell.(1999) A formal framework for the
Java bytecode language and vernier. In Proceedings of the Conference on
Object-Oriented Programming, Systems, Languages, and Applications,
pages 147{166. ACM Press.


cryptography-- Electronica pp 14-17,

[130] Tim Good and Mohammed Benaiissa, AES on FPGA from the Fastest to the Smallest
Published in: · Proceeding CHES'05 Pages 427-440

[131] Toru Akishita and Tsuyoshi Takagi.(2003) Zero-value point attacks on elliptic
curve cryptosystem. In Information Security, 6th International Conference,
volume 2851 of Lecture Notes in Computer Science, pages 218–233,
Bristol, UK. Springer-Verlag.


[138] Vinodh Gopal, Kirk Yap, Martin Dixon (January 2011) *Cryptographic Performance on the 2nd Generation Intel core processor family*, released at Intel Corporation,

