

PROPOSAL TUGAS AKHIR KEAMANAN SISTEM INFORMASI (EC 5010)

Oleh : Ahmad Rifqi Hadiyanto
NIM : 13200013
Tema : Algoritma Kunci Simetris “Camellia” dan Implementasinya (studi kasus pada FPGA)

Nb: judul akan ditentukan kemudian

Abstrak:

Dalam dunia sekarang ini dengan arus informasi yang semakin global, kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan. Ada berbagai algoritma kriptografi yang sekarang ini telah dan sedang dikembangkan, baik algoritma kunci simetris ataupun asimetris (pembagian berdasarkan kunci). Namun sebenarnya, isu yang dibawa adalah tak akan jauh dari tingkat keamanan algoritma dan kecepatan transfer data yang mampu diberikan oleh implementasi algoritma tersebut, walaupun masih ada parameter-parameter lain, seperti: kemampuan sebuah algoritma untuk diimplementasikan dalam berbagai macam platform, kebutuhan resource yang kecil (*memori* pada “programmable device”, atau *area* pada “custom device”),dll.

Camellia adalah sebuah algoritma kriptografi kunci simetris yang bekerja pada ukuran blok 128 bit dengan panjang key 128-bit, 192-bit, atau 256-bit. Camellia pertama kali dikembangkan secara bersama oleh NTT dan Mitsubishi Electric Corporation pada tahun 2000 . Kedua instansi ini pernah mengembangkan algoritma kriptografi yang cukup terkenal: E2 (dikembangkan oleh NTT) dan MISTY (dikembangkan oleh Mitsubishi) sehingga diharapkan *Camellia* mengadopsi beberapa fitur menguntungkan dari kedua macam algoritma kriptografi tersebut.

Paper ini akan membahas algoritma kriptografi kunci simetrik “Camellia” serta beberapa hal dasar dalam mengimplementasikannya dengan piranti FPGA (Field Programmable Gate Array).

Referensi:

- [1] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita. *Camellia a 128-bit block cipher suitable for multiple platforms*. NTT and Mitsubishi Electric Corporation, 2000. Tersedia di <http://info.isl.ntt.co.jp/camellia/>.
- [2] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita. *Specification of Camellia - a 128-bit block cipher*. NTT and Mitsubishi Electric Corporation, 2000. Tersedia di <http://info.isl.ntt.co.jp/camellia/>
- [3] Rogawski, Marcin. *Analysis of Implementation of Hierocrypt-3 Algorithm (and its comparison to camellia algorithm) using altera devices*. Military University of Technology Institute of Mathematics and Cryptology Faculty of Cybernetics, 2003 .
- [4] Yiqun Lisa Yin. *A Note on the Block Cipher Camellia*. NTT Multimedia Communication Laboratories, 2000.
- [5] Paar, Christof. *Reconfigurable Hardware in Modern Cryptography*. Cryptography and Information Security Group Electrical & Computer Engineering Dept. and Computer Science Dept. Worcester Polytechnic Institute Worcester, MA, USA <http://www.ece.wpi.edu/Research/crypt>