Design and implementation of advanced encryption standard using verilog HDL

Suhaili, Shamsiah Binti[a]; Fredrick, Rene Brooke[a]; Zain, Zainah Md.[b]; Julai, Norhuzaimin[a]
[a] Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Malaysia Sarawak, Kota Samarahan, Sarawak, 94300, Malaysia
[b] Robotics, Intelligent System & Control Engineering (RISC) Research Group, Faculty of Electrical and Electronics Engineering Technology, Universiti Malaysia Pahang, Pekan Branch, Pekan, Pahang, 26600, Malaysia

ABSTRACT
Encryption plays an important role in data security against third-party attacks and it is significant to safeguard sensitive data and personal information for the community. Within this era of technology, privacy and confidentiality are the essential considerations to be addressed as a result of the exponential development of the Internet. One of the main concerns involving software implementation of encryption algorithm is the possibility of slower processing when transmitting and receiving data which consequently will encounter low security level during process of encryption for real-time application. The focus of this paper is to match with the existing cryptography algorithm, 128-bit Advanced Encryption Algorithm and improving the processing speed for the design with hardware implementation. Real-time application is essential for today's modern world and Field Programmable Gate Array approach is applied for this purpose. The optimization approaches include loop release, pipeline architecture and Look-Up-Table (LUT) which allow for exact synchronization in order to meet applications' requirements in real time. The design is coded using the Verilog HDL and the hardware design is analyzed and tested with Altera Cyclone II-V in Quartus II and ModelSim. Through comparative analysis with previous implementation, the maximum throughput for this design is 31.37 Gbit/s for the encryption process can operate at 244.89 MHz. The complete 128-bit AES encryption cycle requires only 41 clock cycles to get the encrypted data.

KEYWORDS
AES; Encryption; FPGA; Loop unrolling; Verilog

ACKNOWLEDGEMENTS
The author would like to thank Universiti Malaysia Sarawak (UNIMAS) for providing opportunity and facilities to support this project.