DATE: 2011/07/25
yyyy/mm/dd

Dept. Knowledge-based Info. Engr.		ID	M105701
Name	Muh. Syafiq Irsyadi		

Advisor	Shuichi Ichikawa Kazuhisa Kawai

Title	Hardware Designs of BLAKE Hash Family for Lightweight and High Throughput Systems

(800 words)

Digital communication protocols depend on cryptographic applications to protect information from unauthorized access and modification. Hash function is one of the cryptographic primitives that is used in numerous cryptographic system such as, digital signature, random number generator, check-sum and key generation for encryption. Hash function is a mathematical function that transforms arbitrary length input message into fixed-length-output hash value (digest). Commonly used hash functions such as MD5, SHA-0, and SHA-1 have been proven breakable. Therefore, on late November 2007, National Institute of Standards and Technology (NIST) opened a public competition to select new algorithm for SHA-3. On December 2010, NIST announced five finalists for SHA-3 hash competition.

In this study, hardware circuit of one of the SHA-3 hash function finalists named BLAKE algorithm was designed and implemented in Field Programmable Gate Array (FPGA). This study mainly deals with the design of a compact BLAKE hardware circuit and a high-throughput BLAKE hardware circuit. Compact hash circuit is required for limited-area devices such as smart card, while high-throughput hash circuit is required for high-speed networks such as Hash Message Authentication Code (HMAC).

Lightweight BLAKE design is mainly composed of an Arithmetic Logic Unit (ALU), data memory, and instruction memory. The ALU is pipelined into four stages and constructed from simple arithmetic and boolean logic units. Microcode from instruction memory controls data transfer from data memory to ALU and vice versa. Three compact BLAKE circuits are designed. Functionality of the designs has been verified using provided input vectors. In Altera Cyclone 3 FPGA, the most compact solution requires approximately 60% less memory bit compared to the preceding designs.

High throughput BLAKE design is designed to be able to compute all BLAKE message digest sizes. To the best of our knowledge, this is the first hardware design of BLAKE, which combines all BLAKE hash family in a single circuit resulting in significant area savings over separate data-path approach. Furthermore, the circuit also able to hash two messages at the same time by employing interleaved ALU. After the functionality of the designs has been verified, the designs are synthesized for Virtex 5 FPGA. The most optimal solution is able to achieve throughput up to 3886Mbps, which is three times faster than the previously proposed fully functional BLAKE design in FPGA.