High Performance Compact Pipeline Designs for Secure Hash Algorithms

HOANG ANH TUAN

This thesis describes several fine-grained pipeline implementations and evaluations for hash algorithms, which achieve high throughput with compact hardware size. The research purposes to overcome the throughput limitation of hash algorithms implementation with acceptable hardware penalty by balancing the pipeline stages.

The hash algorithms (MD5, SHA-2) generate the hash values from the original data and the keys through a process with many iterations. The huge computation delay generated in such iterations limits the entire throughput of the system. There are two ways to implement the hash algorithms of basic pipelining and loop unrolling technique, but they are imbalanced in stages and large in hardware size. Previous studies show good improvement using loop unrolling but the hardware size is huge due to hardware duplication, while the basic pipelining method hits the throughput limitation due to the imbalance in pipeline stages.

We have devised a method to break the critical path into smaller balanced pipeline stages by analyzing the data dependency and data movement among two continuous iterations. The computations in one iteration of MD5 are then broken into three or four pipeline stages using data forwarding and two messages processing. The same processes in SHA-2 are broken into two and three pipeline stages using data forwarding and computation postponement. Moreover, the two versions of SHA-2 (SHA-384 and SHA-512) are combined into a unique design to increase the usage of the device. The implementations of those designs on various FPGA boards are analyzed in terms of hardware size, throughput, and area performance rate. Our implementations achieve not only the best area performance rate (throughput divided by area), but also a higher throughput than almost all other related work. The experimentation results show the high performance and compact hardware designs for hash algorithms.