Speeding Up a Scalable Modular Inversion Hardware Architecture

Adnan Abdul-Aziz Gutub

Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Submitted to complete the British Council Research Program of summer2005 in collaboration with

Tatiana Kalganova

Bio-Inspired Intelligent System (BIIS) research group, Electrical & Computer Engineering Department, Brunel University, Uxbridge, United Kingdom

September 2005

Abstract:

The modular inversion is a fundamental process in several cryptographic systems. It can be computed in software or hardware, but hardware computation proven to be faster and more secure. This research focused on improving an old scalable inversion hardware architecture proposed in 2004 for finite field GF(p). The architecture has been made of two parts, a computing unit and a memory unit. The memory unit is to hold all the data bits of computation whereas the computing unit performs all the arithmetic operations in word (digit) by word bases known as scalable method.

The main objective of this project was to investigate the cost and benefit of modifying the memory unit to include parallel shifting, which was one of the tasks of the scalable computing unit. The study included remodeling the entire hardware architecture removing the shifter from the scalable computing part embedding it in the memory unit instead. This modification resulted in a speedup to the complete inversion process with an area increase due to the new memory shifting unit. Quantitative measurements of the speed area trade-off have been investigated. The results showed that the extra hardware to be added for this modification compared to the speedup gained, giving the user the complete picture to choose from depending on the application need.