Brunel UNIVERSITY WEST LONDON

School of Engineering and Design

bit lab

RESEARCH SEMINAR

10 November 2005

in Howell Building Room H313 at 12:30 - 14:00

SPEEDING UP A SCALABLE MODULAR INVERSION HARDWARE ARCHITECTURE

Presented by Dr Adnan Gutub

Computer Engineering Department, King Fahd University of Petroleum & Minerals

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. In this research, we 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 research 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 modeling the 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. Measurements of the speed area trade-off have been investigated. The results showed that the extra hardware added for this modification is worth paying compared to the speedup gained.

Dr. Adnan Abdul-Aziz Gutub, Visiting researcher, summer 2005
Dr. Adnan Gutub is a Faculty Member in the Computer Engineering Department at King Fahd University of Petroleum and Minerals in Saudi Arabia. He received his Ph.D. degree in June 2002 from the Department of Electrical and Computer Engineering at Oregon State University in Cryptographic hardware design under the supervision of Prof. Alexandre Ferreira Tenca.
Adnan received his BSc degree in Electrical Engineering in 1995 and MSc degree in Computer Engineering in 1998 both from King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.
Dr. Adnan Gutub's research interests are in modeling, simulating, and synthesizing VLSI hardware for computer arithmetic operations. He worked on designing efficient integrated circuits for the Montgomery inverse computation in different finite fields.

More info can be found at

Organised by Dr T Kalganova

If you would like to give a seminar, or have suggestions for speakers who we may invite, please contact Dr Kalganova on ext. 66752
Brunel University, Uxbridge, Middlesex, UB8 3PH Tel: 01895 266752 Fax: 01895 251686 e-mail Tatiana.Kalganova@brunel.ac.uk

http://dea.brunel.ac.uk/research/events/ece-seminars/