Review Form: 1st International Workshop on
Services and Infrastructure for the Ubiquitous and Mobile Internet (SIUMI'05)

SIUMI 2005

WEB MINDS

Columbus, Ohio, USA, June 6th, 2005

In conjunction with the 25th Int. Conference on Distributed Computing Systems (**ICDCS'05**)

Paper Number: 21
Paper Title: FPGA-based communication security for wireless sensor networks
Authors: Junaid Majeed

Reviewer1:

Familiarity Rate your familiarity with the topic	1 Novice	X Some knowledge	3 Familiar	4 Expert	
Significance Technical relevance and practicality of ideas in the paper	1 Not significant	X Somewhat significant	3 Highly significant		
Novelty How original the problem and/or solution method is	1 Not novel	X Somewhat novel	3 Highly novel		
Quality of Presentation Writing and presentation style/accuracy	1 Poorly written	2 Could be improved	X Well written		
Overall Recommendation	1 Strong reject	X Weak reject	3 Weak accept	4 Accept	5 Strong accept

Contributions

The major contribution of this paper is related to an FPGA-based implementation of a Montgomery multiplier, which is a major building block of any efficient Elliptic Curve Cryptography algorithm. That's why the author presents his work as belonging to the field of security in wireless sensor networks. The author shows how the solution he devises proves to be both scalable and highly configurable, especially when compared with alternative solutions based on ASIC implementations.

Strengths and weaknesses

My major concern about this work is related to the consideration that it does not fit at all in the intents and topics of SIUMI2005, which is dedicated to SERVICES and INFRASTRUCTURE for enabling ubiquitous communication paradigms. I do believe that the author's contribution might be appreciated in different fora (e.g. conferences/journals on embedded systems). All in all, I think the topic of the paper is not relevant to SIUMI 2005's spirit.

Detailed public comments

Reviewer2:

Familiarity Rate your familiarity with the topic	1	**2X**	3	4
	Novice	Some knowledge	Familiar	Expert

Significance Technical relevance and practicality of ideas in the paper	1	**2X**	3
	Not significant	Somewhat significant	Highly significant
Novelty How original the problem and/or solution method is	**1X**	2	3
	Not novel	Somewhat novel	Highly novel
Quality of Presentation Writing and presentation style/accuracy	1	2	**3X**
	Poorly written	Could be improved	Well written

Overall Recommendation	1	2	**3X**	4	5
	Strong reject	Weak reject	Weak accept	Accept	Strong accept

Contributions

This paper performs an analysis on FPGA based Montgomery Multipliers. It shows you the path the authors took in choosing the algorithms for their implementation and finishes with measurements, analysis and conclusions on their implementation of the algorithms. Although the work seems to be a good step for FPGA based cryptography, the novelty seems to be confined to the fine tuning of the implementation itself.

Strengths and weaknesses

The paper is easy to follow and well written. It is very in depth and considers all details of the focused issues. However, it's title seems to be a bit misleading. Although one of the applications for the results of the paper can be in telecommunications, or sensor networks in specific, they are not restricted to this area. In fact, the author does not present any focus on the application outside the abstract and introduction.

Detailed public comments

Although the paper is well presented and constructed, it does not quite fill the area promised in the introduction. It seems that the authors have not researched the area of security for wireless sensor networks in sufficient depth. It is hard therefore to fit their work with the available technologies for WSNs. As correctly put forward by the introduction, energy is one of the critical aspects in WSNs. However, while focusing on clock cycles and area, energy was left for the reader to calculate. A comparative study of doing this in a microcontroler, used in the sensor, in software would be helpful. It is my fear that the energy requirements on the FPGA might surpass those of the estimated for the sensor. This reviewer would like to see more of this integration being explicitly referred to in the paper. It would be of special interest to see how this FPGA could work with a commonly used sensor (such as the Mica2/MicaZ from xbow).

Reviewer3:

Familiarity Rate your familiarity with the topic	**1X**	**2**	3	4	
	Novice	Some knowledge	Familiar	Expert	
Significance Technical relevance and practicality of ideas in the paper	1	**2X**	3		
	Not significant	**Somewhat significant**	Highly significant		
Novelty How original the problem and/or solution method is	**1**	**2X**	3		
	Not novel	**Somewhat novel**	Highly novel		
Quality of Presentation Writing and presentation style/accuracy	1	2	**3X**		
	Poorly written	Could be improved	**Well written**		
Overall Recommendation	1	2	**3X**	4	5
	Strong reject	Weak reject	**Weak accept**	Accept	Strong accept

Contributions
Actually I feel myself unable to judge, as I know nothing about implementation by FPGA.

Strengths and weaknesses
+ seems very interesting
- I know nothing about this and I assume that many other attendees could be in my same situation.

Detailed public comments
The paper appears to be very interesting, but the work described is completely outside my domain of expertise, so that I don't feel confident enough on my understanding of the paper to be able to write any useful comment here.