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: #23
Paper Title: Design of Secure Hardware for ATM Networks
Authors: Engr. Junaid Majeed

Reviewer1:

Familiarity Rate your familiarity with the topic	1	2	**3X**	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

The author focus on providing security services (e.g., encryption, authentication) into ATM networks, with some novel effort for convincing readers to consider re-configurable logic for designing hardware architectures. The submission is technically correct, and the conclusion is quite straightforward.

Strengths and weaknesses

The paper is well written and cryptographic algorithms are finely presented. The application of reconfigurable logic is interesting, even if hardware implementation of cryptographic algorithms is a well known and definitely not novel topic. Moreover, the paper focus mainly on secret key cryptography and on DES, without investigate in deep the public key framework (with larger keys) and important symmetric algorithms like 3DES and AES.

Detailed public comments

Please provide in a larger contribution an in-depth analysis with other cryptographic algorithm. At least, consider the important task of key management by way of Diffie-Hellman scheme, and the behavior of

algorithms resistant against distributed brute force attacks with larger keys (e.g., triple-DES in the EDE mode and AES). Moreover, consider that types into the figures are unreadable.

Reviewer2:

Familiarity Rate your familiarity with the topic	1	2	**3X**	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	**2X**	3	
	Poorly written	Could be improved	Well written	
Overall Recommendation	**1X**	2	3	4	5
	Strong reject	Weak reject	Weak accept	Accept	Strong accept

Contributions
The paper addresses the provisioning of security services such as authentication and encryption, by proper designing hardware architectures for ATM networks.
Very limited interest for the SIUMI audience.

Strengths and weaknesses
Lack of novelty.
Out of the scope of the workshop.

Detailed public comments

Reviewer3:

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	**1X**	2	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		**2X**		3
	Poorly written		**Could be improved**		Well written
Overall Recommendation	1	**2X**	3	4	5
	Strong reject	**Weak reject**	Weak accept	Accept	Strong accept

Contributions

Strengths and weaknesses

Definitely not relevant for the topics of the SIUMI workshop.
I suggest submitting the paper to another conference.

Detailed public comments