IITB-Monash Research Academy

An Indian-Australian research partnership

Indian Institute of Technology Bombay | MONASH University

Project Title:	**Multidimensional encryption and modes**	
Project Number	**IMURA0476**	
Monash Main Supervisor (Name, Email Id, Phone)	Phu Le Phu.Dung.Le@monash.edu	*Full name, Email*
Monash Co-supervisor(s) (Name, Email Id, Phone)		
Monash Department:	School of IT	
IITB Main Supervisor (Name, Email Id, Phone)	V R Sule vrs@ee.iitb.ac.in	*Full name, Email*
IITB Co-supervisor(s) (Name, Email Id, Phone)		
IITB Department:	Department of Electrical Engineering	

Research Academy Themes:

Highlight which of the Academy's Theme(s) this project will address? ***(****Feel free to*

nominate more than one. For more information, see www.iitbmonash.org)

	1. Advanced computational engineering, simulation and manufacture
	2. Infrastructure Engineering
	3. Clean Energy
	4. Water
	5. Nanotechnology
	6. Biotechnology and Stem Cell Research

The research problem

Define the problem

The current block and stream encryption methods are often found to be unsuitable for multimedia data as well as from the point of view of bandwidth (or alternatively speed of operation). The reason is that representation of multimedia data in blocks and streams of information bits involves overhead. The new approach is to directly develop multidimensional randomness and utilize it for encryption as well as other tasks such as integrity, hashing and message authentication. Such a method has potential to be more efficient than converting the multi dimensional data in single dimension.

Also the methods of cryptanalysis of multi dimensional encryption are likely to be different than those of single dimension algorithms prevalent currently. Similarly the statistical tests used currently for testing cryptographic algorithms are for one dimensional strings and streams. Extending these tests to more than one dimension shall involve new research problems to be resolved. Hence this project has enormous scope for new research. and application.

Project aims

Define the aims of the project Develop two dimensional data encryption schemes, develop two dimensional modes of encryption for encrypting bulk two dimensional data, develop a quantitative statistical test of randomness for two dimensional signal. Use the two dimensional algorithms for encryption of images.

Expected outcomes

Algorithms for image encryption and their implementation as application code.

Highlight the expected outcomes of the project The projected is expected to result into following outcomes: 1. Algorithms for constructing analogous block and stream ciphers for two dimensional data encryption. 2. Modes of encryption: methodologies for encryption of bulk data. 3. A quantitative statistical test for evaluation of randomness of two dimensional signals. 4. Methodologies for application in cryptography such as: development of authentication codes, multiple password generation from single seed, techniques for key escrow etc.

How will the project address the Goals of the above Themes?

Describe how the project will address the goals of one or more of the 6 Themes listed above. The project addresses a problem in computation of encryption for two dimensional data. This problem involves advanced methods in computational science and has application to Information Technology and Computer Engineering. This way the project addresses the first goal among the 6 themes.

Capabilities and Degrees Required

List the ideal set of capabilities that a student should have for this project. Feel free to be as specific or as general as you like. These capabilities will be input into the online application form and students who opt for this project will be required to show that they can demonstrate these capabilities. 1. Degree in Electrical or Computer engineering with capability in coding. 2. Background of cryptography and statistics.

Potential Collaborators

Please visit the IITB website HYPERLINK "http://www.iitb.ac.in" www.iitb.ac.in OR Monash Website HYPERLINK "http://www.monash.edu" www.monash.edu to highlight some potential collaborators that would be best suited for the area of research you are intending to float.

1. Dr. Phu Le, School of Information Technology, Monash University.