IITB-Monash Research Academy

Indian Institute of Technology Bombay | MONASH University

An Indian-Australian research partnership

Project Title:	**Design of energy efficient cryptographic Co-processors.**	
Project Number	**IMURA0380**	
Monash Supervisor(s)	**Prof. Ron Steinfeld**	*Full names and titles*
Monash Primary Contact:	ron.steinfeld@monash.edu	*Email, phone*
Monash Head of Department:	Graham Farr	*Full name, email*
Monash Department:	Clayton School of IT	*Full name*
Monash ADRT:	Kai Ming Ting	*Full name, email*
IITB Supervisor(s)	Prof. Madhav Desai, Prof. Virendra Sule	*Full names and titles*
IITB Primary Contact:	madhav@ee.iitb.ac.in	*Email, phone*
IITB Head of Department:	Abhay Karandikar	*Name, Email,*
IITB Department:	EE	*Full name*

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

Design of energy efficient cryptographic Co-processors.

Cryptographic algorithms used in symmetric as well as public key schemes are among the most computation heavy operations performed by computers. Cryptographic applications also require stringent security and randomness generation of high quality. The purpose of the present proposal is to investigate efficient implementation of unit operations required in cryptography such as large number modular arithmetic, elliptic curve arithmetic, fast pseudorandom sequence generation and Boolean function operations on a processor which has limitations in terms of memory and power. Such a processor has typical applications in smart cards, mobile computing and portable devices.

Project aims

Define the aims of the project

1. Identify the critical unit operations for cryptographic purposes in applications such as smart cards or mobile devices.
2. Develop algorithms for these operations and solutions of problems of cryptographic primitives which are efficient and are implementable within the constraints of memory and energy available on a processing device.
3. Realize hardware to validate the algorithms and characterize their performance.

Expected outcomes

Highlight the expected outcomes of the project

1. Algorithmic knowhow on cryptographic primitives and algorithms for specific computations of unit operations under constraints of memory and power..

Hardware circuit realization of the implementation of the algorithms.

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.

Information security in mobile computing has become one of the important aspects of computational engineering. This requires incorporating security functions on mobile devices and smart cards which have stringent memory and power limitations. This project addresses this core issue of implementing cryptographic primitives on such computing devices and hence addresses the above theme.

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. B.Tech./M.Tech. In EE/CS with strong background in algorithms, digital circuits and preferable cryptography.