Research Project Title

Investigating the security of lightweight authenticated encryption primitives

Details of Primary Supervisor

1. Name: Dr. Iftekhar Salam
2. Department and University: Information and Communication Technology, Xiamen University Malaysia
3. Email address: iftekhar.salam@xmu.edu.my
4. Research interests: Cryptography, Cryptanalysis, Information Security

Details of Research Project

1. Duration: 2 years

2. Summary:

Lightweight cryptography is a current research topic in symmetric cryptography. It aims to provide cryptographic solutions, particularly designed for resource constrained devices such as RFID tags, sensors, smart cards, IoT devices. In the recent years, starting from 2013 the "Lightweight Cryptography (LWC) Project" was initiated by the National Institute of Standards and Technology (NIST). The aim of the lightweight cryptography project is to evaluate and standardize cryptographic algorithms which are suitable for resource constrained environment. Recently in August 2018, NIST has published a call for algorithms to be considered for lightweight cryptography project. The LWC project is currently in its final round. There is a need for a third-party analysis of the LWC finalists. The analysis provides a crucial service to the community at large as it helps to determine secure and efficient LWC standards. In this project, we aim to contribute into these security analyses. The main objective of this project is to provide an independent security analysis of the selected lightweight cryptographic algorithms from the lightweight cryptography project.

3. Skills: Good programming skills, strong mathematical background

4. Location: Xiamen University Malaysia, Sepang, Malaysia

GRA Requirements:

Number of Master place(s) available: 1

1. The candidate must be or to be enrolled in XMUM Master programme.
2. The candidate must be a Malaysian Citizen.
3. The candidate must have a Bachelor Degree in Computing or any closely related subject.