Title: A Few Primitives in Symmetric-Key Cryptography

Speaker: Dr. Sebati Ghosh

Date and Time: 7th Aug, 5pm, KD101

Abstract:

In this talk, I will, at first, briefly describe my research profile. Next, some of our interesting works in the area of modes of operations in symmetric-key cryptography will be described. Most of these works have practical applications in day-to-day life.

First, I describe, in considerable detail, a Message Authentication Code (MAC) that supports variable tag lengths. A MAC scheme ensures authentication of data, which is one of the goals of Cryptography. It is in use in everyday life, e.g. in internet traffic. A MAC scheme supporting variable tag lengths is important in resource constrained devices, like mobile phones.

Next, I describe some other works briefly. A very important primitive in symmetric-key cryptography is universal hash functions. It has applications in many important modes of operations, like in constructing MAC schemes. Two important universal hash functions based on univariate polynomials available in the literature are Horner's rule based hash function and Bernstein-Rabin-Winograd (BRW) polynomials based hash function. I will describe our work which proposes an efficient algorithm for evaluating BRW polynomials based hash function for variable length messages. The next work describes Hash2L, which is a two-level hash function that combines the advantages provided by both Horner's rule based hash function and BRW polynomials based hash function. This is the most efficient universal hash function available in the literature for a specific kind of processors.

Some other works include a disk encryption scheme called FAST, which is of immense use in today's life where sensitive data resides in vulnerable storage devices, like laptop, mobiles etc., post-quantum security of some important primitives and authenticated data structure.

I will conclude the talk with my immediate research plan which includes message franking protocol of messaging services like Facebook messenger, Whatsapp etc., authentication and authenticated encryption schemes supporting variable tag lengths, format preserving encryption etc.

Speaker Bio:

Dr. Sebati Ghosh is going to join as a postdoctoral fellow in University of York, UK from August, 2023. There she will be primarily working on a project on protecting minority ethnic communities online with Prof. Siamak Shahandashti. From November, 2021 to April, 2023 she has worked as a postdoctoral fellow in University of Bern, Switzerland. There she has worked on authenticated data structures with Prof. Christian Cachin. She earned her Ph.D. in Computer Science, under the supervision of Prof. Palash Sarkar, in August, 2021 and M.Tech in Computer Science in 2015 both from Indian Statistical Institute, Kolkata. She is Rashi Ray Memorial Gold Medal awardee for standing first in her batch of M.Tech in Computer Science. She earned her B.Tech in Electronics and Communication Engineering from Institute of Engineering and Management in Kolkata under West Bengal University of Technology in 2009. She ranked 46th in the state of West Bengal among all class X board examination candidates. Till now she has primarily worked in the area of symmetric key cryptology and she has published in journals including Designs, Codes and Cryptography and IACR Transactions on Symmetric Cryptology.