**Title:** Fixed-Point Arithmetic in Somewhat Homomorphic Encryption Schemes

**Date:** 19-Dec-2018.

**Time:** 5:00 PM

**Location:** KD-102

**Speaker:** Srinivas Vivek, IIIT Bangalore

**Abstract:** Homomorphic encryption schemes allow users to meaningfully manipulate ciphertexts "without revealing" any information about the underlying plaintexts. In this work, we investigate issues related to performing fixed-point arithmetic homomorphically using existing fully/somewhat homomorphic encryption (FHE/SHE) schemes. We analyse and compare various encoding schemes to encode fractional numbers in the native algebraic plaintext space of an SHE scheme and derive bounds on the parameters to used by an SHE scheme. We will see how a particular choice of encoding can significantly affect the practical performance. As an application of these bounds, we investigate homomorphic image processing and also perform an implementation using the HElib homomorphic encryption library.

**Biography:** Dr. Srinivas Vivek is currently an Assistant Professor at IIIT Bangalore. Previously, he was a postdoctoral researcher in the Cryptography group at the University of Bristol, UK. He has obtained his doctoral, masters, and bachelors degrees from the University of Luxembourg (Luxembourg), IISc, Bangalore, and NITK, Surathkal, respectively. His research interests are in the design, analysis and implementation of (1) countermeasures against side-channel attacks, and (2) homomorphic encryption schemes.