Title: Kummer for Genus One over Prime Order Fields

Abstract: In this talk, we will consider the problem of fast and secure scalar multiplication using curves of genus one defined over a field of prime order. Previous work by Gaudry and Lubicz in 2009 had suggested the use of the associated Kummer line to speed up scalar multiplication. In the talk, we will explore this idea in detail. The first task is to obtain an elliptic curve in Legendre form which satisfies necessary security conditions such that the associated Kummer line has small parameters and a base point with small coordinates. It turns out that the ladder step on the Kummer line supports parallelism and can be implemented very efficiently in constant time using the single-instruction multiple-data (SIMD) operations available in modern processors. For the 128-bit security level, this work presents three Kummer lines denoted as K1 := KL2519(81,20), K2 := KL25519(82,77) and K3 := KL2663(260,139) over the three primes 2^251-9, 2^255-19 and 2^266-3 respectively. Implementations of scalar multiplications for all three Kummer lines using Intel intrinsics have been done and the code is publicly available. Timing results on the recent Skylake and the earlier Haswell processors of Intel indicate that both fixed base and variable base scalar multiplications for K1 and K2 are faster than those achieved by Sandy2x, which is a highly optimised SIMD implementation in assembly of the well known Curve25519; for example, on Skylake, variable base scalar multiplication on K1 is faster than Curve25519 by about 25%. On Skylake, both fixed base and variable base scalar multiplication for K3 are faster than Sandy2x; whereas on Haswell, fixed base scalar multiplication for K3 is faster than Sandy2x while variable base scalar multiplication for both K3 and Sandy2x take roughly the same time. In fact, on Skylake, K3 is both faster and also offers about 5 bits of higher security compared to Curve25519. In practical terms, the particular Kummer lines that are introduced in this work are serious candidates for deployment and standardisation.

This is a joint work with Prof. Palash Sarkar, Applied Statistics Unit, Indian Statistical Institute Kolkata. A short version of this work is published at AsiaCrypt 2017 and the full version is under review at Journal of Cryptology (JoC).

Speaker Bio: I am a Post-Doctoral Fellow at the department of Computer Science (CPSC) of University of Calgary (UofC), working with Prof. Rei. Safavi-Naini, from 2016. At present, I am working on Hash-based One-Time-Signature schemes and Lattice-Based Cryptographic Protocols based on the hard problem of Ring-LWE. Prior to this, from 2015 to 2016, I was working as a Post-Doctoral Fellow at Turing Lab of Applied Statistics Unit (ASU) of Indian Statistical Institute (ISI), Kolkata, India with Prof. Palash Sarkar. At ISI, I was working on efficient and faster implementation of Diffie-Hellman protocol using Haswell intrinsic. I completed my Doctoral research on Elliptic-Curve Digital Signature under the guidance of Dr. Abhijit Das from the department of Computer Science and Engineering (CSE), Indian Institute of Technology (IIT) Kharagpur, India in 2015. I did my M.Tech. from the same department of IIT Kharagpur in 2010. In 2008, I graduated from the department of Computer Science and Engineering of Jadavpur University, Kolkata.

My primary research interest lies in Public- Key Cryptography, mainly Curve-based, Hash-based and Lattice-based Cryptography. My other interests include Number theory, Computational Number Theory, Algorithm Design, Analysis, and efficient implementation.