MONIREH REZAI RAD, University of Calgary

Jacobian Versus Infrastructure in Real Hyperelliptic Curves

Real hyperelliptic curves admit two structures: the Jacobian and the infrastructure. While both structures in real models could be employed for cryptographic purposes, it was not clear which one has better performance in practice.

In this talk, we describe that how exactly the infrastructure and the Jacobian are related. We suggest an alternative distance map for the infrastructure in order to improve the efficiency of this structure. We show that the infrastructure with the new distance and the Jacobian have identical performance in practice for cryptographic sized curves. We support this claim both mathematically and computationally.