SEYED LAVASANI, University of Calgary

The inside-out of cover attack

A cover attack is a method of decreasing the complexity of the discrete logarithm problem defined on the Jacobian of a curve by transferring it to the Jacobian of a new curve which admits a faster solution for this problem. The new curve shares a cover with the original curve.

In this talk we carefully study the known algorithms for implementing the different steps of this attack while looking for possible generalizations. Furthermore we present new approaches for constructing the cover and finding new sub-curves with vulnerable Jacobians. We present an algorithm to compute a model for many potential covers using their automorphism group and their ramification structure.