COLIN WEIR, University of Calgary
Constructing and Tabulating Function Fields

We present a Kummer theoretic algorithm for constructing degree ℓ dihedral function fields over a finite field $\mathbb{F}_q$ with prescribed ramification. We then use this in a tabulation algorithm to construct all non-Galois cubic function fields over $\mathbb{F}_q$ up to a given discriminant bound and compare the data to known asymptotics. We will also survey other applications where these techniques can be made useful, such as constructing curves with many points, or in implementing cover attacks on hyperelliptic curve cryptography. Moreover, we show how our construction techniques can be extended to characteristic zero to construct interesting curves over number fields.