

The thesis deals with arithmetics of elliptic curves over finite fields and methods to improve those calculations. In the first part, algebraic geometry helps to define elliptic curves and derive their basic properties including the group law. The second chapter seeks ways to speed up these calculations by means of time-memory tradeoff, i.e. adding redundancy. At last, the third part introduces a wholly new curve form, which is particularly effective for such purposes.