ELLIPTIC LOOPS

DANIELE TAUFER

Given a local ring $(R, \mathfrak{m})$ with $6 \in R^*$ and an elliptic curve $E(R/\mathfrak{m})$, a new object called *elliptic loop* is defined as the set of points in $\mathbb{P}^2(R)$ lying over E with respect to the canonical projection. When the curve E has no even-torsion elements, the corresponding elliptic loop may be endowed with an operation inherited by the curve's addition law. This object is proved to be a power-associative abelian algebraic loop.

Although elliptic loops are not necessarily associative, they contain several abelian varieties defined over R by linear combinations of the curve Weierstrass polynomial and its Hessian. Those algebraic curves are called *layers*, as they provide a stratification of the affine part of their elliptic loop. The 0-layer coincides with the classical elliptic curve $E(R)$ lifting E.

Special properties are obtained when the underlying ring is $\mathbb{Z}/p^e\mathbb{Z}$, for which the infinity part of an elliptic loop may be realized as a direct product of two cyclic sub-loops. Moreover, the possible groups arising from layers over such rings are characterized by establishing a generator of their infinity parts.

When the underlying curve E has trace 1, the layer's group structure is employed for producing an isomorphism attack to the discrete logarithm on this family of curves. This attack has the same computational complexity as the known arithmetic approaches, but it involves only finite-precision objects.

Stronger properties are derived for small values of the exponent e, which lead to an explicit description of the infinity group and to characterizing the geometry of rational $|E|$-torsion points inside the overlying elliptic loop.

CISPA - Helmholtz Center for Information Security
Email address: daniele.taufer@cispa.de