Extractors for Binary Elliptic Curves

Reza Rezaeian Farashahi

October 11, 2006

EIDMA SEMINAR COMBINATORIAL THEORY

A deterministic extractor for an elliptic curve is a function that converts a random point on the curve to a random-looking bit-string, which is statistically close to a uniformly random bit-string. The problem of converting random points of an elliptic curve into random bits has several cryptographic applications. In this talk, we propose two simple and efficient deterministic extractors for an ordinary elliptic curve E defined over $\mathbb{F}_{2^N}$, where $N = 2\ell$ and ℓ is an arbitrary positive integer. Our first extractor, $\mathcal{H}_0$, for a given point P on E, outputs the first $\mathbb{F}_{2^\ell}$-coefficient of the abscissa of the point P. Similarly the second extractor, $\mathcal{H}_1$, for a given point on E, outputs the second F_{2^ℓ}-coefficient of the abscissa of the point. Provided that the point P is chosen uniformly at random, the extracted bits of the point P are indistinguishable from a uniformly random bit-string of length ℓ.