University College London
Department of Computer Science

# Cryptanalysis Lab 06

J. P. Bootle, N. Courtois


April 4, 2019

jonathan.bootle.14@ucl.ac.uk
Version 2.0

## 1. Roots Of Unity

Type the following commands for the bitcoin Elliptic Curve:

```
p=115792089237316195423570985008687907853269984665640564039
457584007908834671663
Zp=Integers(p) # Here we give ourselves shorthand for the mod
Zp(2)^(p-1)
root_list = Zp.zeta(5,all=True); root_list
```

Try the same with q=
115792089237316195423570985008687907852837564279074904382
605163141518161494337

## 2. Isogenies: Morphisms of Elliptic Curves

Isogeny is a group homomorphism [not every book has the same definition]. It preserves the EC point addition. It also is a rational map (a division of 2 polynomials).

Type the following commands.

```
k = GF(11)
E = EllipticCurve(k,[1,1])
E.cardinality()
E.discriminant()
E.j_invariant()
Q = E(6,5)
phi = E.isogeny(Q)
F=phi.codomain()
F.is_isogenous(E)
F.cardinality()
F.discriminant()
F.j_invariant()
phi
```

```
P = E(4,5)
phi(P); phi(P).order()
phi(E(6,5)) - why we expect this result? [V\'{e}lu]
(X, Y) = phi.rational_maps()
X
phi.x_rational_map()
```

Write SAGE code to verify if phi preserves the addition on ECC.

## 3. Dual Isogenies and Special Multiples

There is essentially a ONE signle isogeny between tow elliptic curves. There is an interesting notion of dual isogenies, see this easy intro paper (which contains many typos like $E'$ is in fact $E_2$ etc) https://wstein.org/edu/2010/581b/projects/joanna_gaski/isogenies.pdf

```
E = EllipticCurve(GF(37), [0,0,0,1,8])
E.short_weierstrass_model()
R.<x> = GF(37)[]
f = x^3 + x^2 + 28*x + 33
phi = EllipticCurveIsogeny(E, f)
phi_hat = phi.dual()
phi.dual().dual() == phi
phi_hat.codomain() == phi.domain()
phi_hat.domain() == phi.codomain()

(X, Y) = phi.rational_maps()
(Xhat, Yhat) = phi_hat.rational_maps()
Xm = Xhat.subs(x=X, y=Y)
```

```
Ym = Yhat.subs(x=X, y=Y)
(Xm, Ym) == E.multiplication_by_m(7)
```