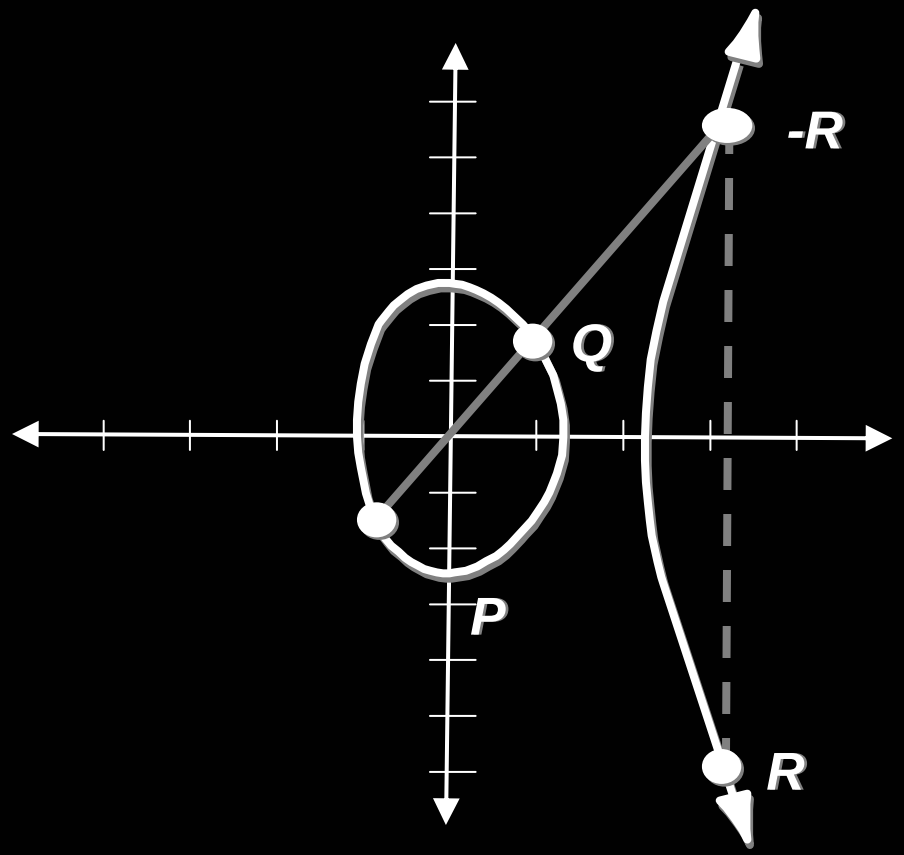
Elliptic curve cryptography

ECC is an asymmetric cryptosystem based on the elliptic curve discrete log problem.

The ECDLP arises in Abelian groups defined on elliptic curves.



$y^2 = x^3 - ax + b$

$P + Q = R.$

Defining addition (and doubling) defines multiplication by a scalar.

The ECDLP is the inverse operation to multiplication by a scalar; if K=kP, given K and P, find k.

The ECDLP is intractable; for a given field size, it is vastly harder to find k from kP and P than it is to find kP from k and P.

k is thus used as the private key; kP is used as the public.

The ECDLP is widely believed to be resistant to Number Field Sieve attacks. The best known attack is Pollard's Rho—whose difficulty grows more rapidly with the field size than do NFS methods.

Equivalent key sizes

Symmetric	ECC	DH/DSA/RSA
80	163	1024
128	283	3072
192	409	7680
256	571	15360

Four primitives/protocols

- ECDSA
- ECDH
- ECIES
- ECMQV

ECDSA

Elliptic Curve Digital Signature Algorithm

ECDSA provides sign and verify operations; it is analogous to DSA.

ECDH

Elliptic Curve Diffie-Hellman

ECDH is analogous to conventional Diffie-Hellman; p(qG) = q(pG); qG, pG are public values; p and q are private.

ECIES

Elliptic Curve Integrated Encryption Scheme.

ECIES is analogous to public key encryption.

The initiator performs an ECDH-type transform with the respondent’s static key pair; the generated key is then used for encryption/signing.

ECMQV

Elliptic Curve Menezes-Qu-Vanstone.

MQV is intended as replacement for Signed DH.

ECMQV is endorsed in the NSA’s Suite B.

Both parties must use their private key in an AVF to generate the shared key; this functions as an implicit signature, proving possession of the private key.

Uses in MIKEY

ECDH drops in for DH.

ECDSA drops in for DSA.*

ECIES and 1-pass MQV drop in for public key encryption methods.*

2-pass MQV could drop in for signed DH; this is not in the current draft.*

* These methods require EC certs.