Adding the points P and $-P$

As before, we define $P + (-P) = \infty$.

Doubling the point P

If the y-coordinate of P is zero, modulo p, then $P = -P$. To double the point $P = (x_P, y_P)$ with $y_P \not\equiv 0 \bmod p$, let s be given by $s \equiv (3x_P^2 + a)(2y_P)^{-1} \bmod p$. We define $2P = P + P = R$ where

$$x_R \equiv s^2 - 2x_P \mod p \text{ and}$$

$$y_R \equiv -y_P + s(x_P - x_R) \bmod p.$$

Example. Addition table for the points on $y^2 = x^3 + 5x + 4$ over $\mathbb{Z}_{11}$.

$+$	$(0,2)$	$(0,9)$	$(2,0)$	$(4,0)$	$(5,0)$	$(10,3)$	$(10,8)$	∞
$(0,2)$	$(5,0)$	∞	$(10,8)$	$(10,3)$	$(0,9)$	$(2,0)$	$(4,0)$	$(0,2)$
$(0,9)$	∞	$(5,0)$	$(10,3)$	$(10,8)$	$(0,2)$	$(4,0)$	$(2,0)$	$(0,9)$
$(2,0)$	$(10,8)$	$(10,3)$	∞	$(5,0)$	$(4,0)$	$(0,9)$	$(0,2)$	$(2,0)$
$(4,0)$	$(10,3)$	$(10,8)$	$(5,0)$	∞	$(2,0)$	$(0,2)$	$(0,9)$	$(4,0)$
$(5,0)$	$(0,9)$	$(0,2)$	$(4,0)$	$(2,0)$	∞	$(10,8)$	$(10,3)$	$(5,0)$
$(10,3)$	$(2,0)$	$(4,0)$	$(0,9)$	$(0,2)$	$(10,8)$	$(5,0)$	∞	$(10,3)$
$(10,8)$	$(4,0)$	$(2,0)$	$(0,2)$	$(0,9)$	$(10,3)$	∞	$(5,0)$	$(10,8)$
∞	$(0,2)$	$(0,9)$	$(2,0)$	$(4,0)$	$(5,0)$	$(10,3)$	$(10,8)$	∞

Elliptic curve cryptography

Having defined the addition of points on elliptic curves over $\mathbb{Z}_p$, we now look at how to apply these ideas to the ElGamal scheme.

Elliptic curve cryptography scheme, using Alice and Bob

An ECC scheme is a form of public-key cryptosystem. Public-key cryptosystems are a relatively new technology, developed in 1976 by Whitfield Diffie and Martin Helman, both Stanford researchers. These cryptosystems involve separate encryption and decryption operations. The encryption rule uses a *public key*, while the decryption rule employs a *private key*. Knowledge of the public key allows encryption of a message but does not permit decryption of the encrypted message. The private key is kept secret so that only the intended individual can decrypt the message [2].

ECC schemes use an elliptic curve E over a finite field such as $\mathbb{Z}_p$, where p is a very large prime, and involve both an encryption and decryption operation. There are several public key schemes that can be used to encrypt and decrypt messages, such as the Diffie-Hellman scheme, the Vanstone-Menezes scheme, and the ElGamal scheme. We will look at the ElGamal encryption and decryption scheme. For more on the ElGamal or other schemes, see [5, 6, 9].

The ElGamal public-key cryptosystem is based on the Discrete Logarithm problem in $\mathbb{Z}_p^*$, the set of integers $1, 2, \ldots, p-1$, under multiplication modulo p.

The utility of the Discrete Logarithm problem in a cryptographic setting is that finding discrete logarithms is difficult, but the inverse operation of exponentiation can be computed efficiently [9]. In other words, if a person is given α, β, and $\alpha^z \equiv \beta \bmod p$, then it is very difficult to figure out the exponent z. We will use this idea in an ECC cryptosystem and perform the operations on an elliptic curve over $\mathbb{Z}_p$. Note that in an elliptic curve group, α^z is interpreted as adding α to itself z times.

This scheme will be demonstrated using Alice and Bob as sender and receiver of a secret message, respectively. Typically, the message consists of some large secret number, which is subsequently used by the two parties to open a conventional secure communication channel. The coordinates of the points on the elliptic curve itself serve as a pool of numbers to choose from.

The encryption operation

Step 1: Bob chooses a point α on an elliptic curve E over some $\mathbb{Z}_p$ and an integer z between 1 and the order of the abelian group E.

Step 2: Bob computes $\beta = z\alpha$ on the curve and publishes α, β, E, and p. He keeps his private key z secret.

Step 3: Suppose Alice wants to send a message to Bob. Alice picks an integer k between 1 and the order of E, which will be her private key.

Step 4: To encrypt a message, Alice looks up Bob's public key. As the message, she selects a point x on the elliptic curve E. Next, Alice performs the following encryption operation to encrypt the message:

$$e_k(x, k) = (k\alpha, x + k\beta) = (y_1, y_2).$$

The encrypted message is $y = (y_1, y_2)$; it includes Alice's public key y_1.

The decryption operation

Step 5: Alice sends Bob the encrypted message. To decrypt the message, Bob uses the decryption operation:

$$d_z(y_1, y_2) = y_2 - zy_1 = (x + k\beta) - z(k\alpha) = x + k(z\alpha) - z(k\alpha) = x,$$

where z is Bob's private key.

Note the interlocking of public and private keys here: Bob's private key z will decrypt this message correctly, because it matches his public key $\beta = z\alpha$, and he can be sure that it was Alice who transmitted this message, since nobody else is in possession of the private key k that matches her public key $y_1 = k\alpha$.

An example of the encryption and decryption operations

Step 1: E is the elliptic curve $y^2 = x^3 + 5x + 4$ over $\mathbb{Z}_{11}$ (see table above), $\alpha = (10, 3)$, $z = 3$. Bob's private key: $z = 3$.

Step 2: $\beta = 3(10, 3) = (10, 8)$.
Bob's public key: $\alpha = (10, 3)$, $\beta = (10, 8)$, $y^2 = x^3 + 5x + 4$ over $\mathbb{Z}_{11}$.

Step 3: Alice chooses $k = 2$.

Step 4: Alice's message is $x = (2, 0)$, which is a point on the elliptic curve E.
$y_1 = 2(10, 3) = (5, 0)$.
$y_2 = (2, 0) + 2(10, 8) = (2, 0) + (5, 0) = (4, 0)$.
The encrypted message is $y = ((5, 0), (4, 0))$.

Step 5: Beginning with $y = ((5, 0), (4, 0))$, Bob computes
$x = (4, 0) - 3(5, 0) = (4, 0) - (5, 0) = (4, 0) + (5, 0) = (2, 0)$.
The decrypted message is $x = (2, 0)$.

References

[1] E. Brown, *Three Fermat trials to elliptic curves*, The College Mathematics Journal **31** (2000) 162–172.

[2] Certicom, *The elliptic curve cryptosystem: an introduction to information security* [Retrieved October 3, 2003], `www.certicom.com`

[3] Certicom, Online ECC tutorial [Retrieved October 10, 2003], `www.certicom.com/resources/ecc_tutorial/ecc_tut_1_0.html`

[4] J. Hastad and S. Strom, *Elliptic curves*, Seminars in Theoretical Computer Science [Retrieved April 18, 2004], `www.nada.kth.se/kurser/kth/2D1441/lecturenotes/elliptic.pdf`

[5] N. Koblitz, Algebraic aspects of cryptography, Springer-Verlag(1998).

[6] M. Rosing, Implementing elliptic curve cryptography, Manning Publications (1999).

[7] W. Rudin, Principles of mathematical analysis (3rd Edition), McGraw-Hill (1964).

[8] S. Singh, The code book: the science of secrecy from ancient Egypt to quantum cryptography, Anchor Books (1999).

[9] D. Stinson, Cryptography: theory and practice (2nd Edition), Chapman & Hall/CRC (2002).