VE475 Homework 10

Yiwen Yang

Ex. 1 - Group Structure on an Elliptic Curve

Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.
If $P_1 \neq P_2$

$$m = (y_2 - y_1)/(x_2 - x_1)$$

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

$$b = (y_1^2 - y_2^2 - x_1^3 + x_2^3)/(x_1 - x_2)$$

$$c = y_1^2 - x_1^3 - bx_1$$

$$\begin{aligned} x_3^3 + bx_3 + c = \frac{1}{(x_1 - x_2)^6} & (x_1^6 y_1^2 - 6x_1^4 x_2^2 y_1^2 + 4x_1^3 x_2^3 y_1^2 + 9x_1^2 x_2^4 y_1^2 - \\ & 12x_1 x_2^5 y_1^2 + 4x_2^6 y_1^2 - 2x_1^3 y_1^4 + 6x_1 x_2^2 y_1^4 - \\ & 4x_2^3 y_1^4 + y_1^6 - 4x_1^6 y_1 y_2 + 6x_1^5 x_2 y_1 y_2 + \\ & 12x_1^4 x_2^2 y_1 y_2 - 28x_1^3 x_2^3 y_1 y_2 + 12x_1^2 x_2^4 y_1 y_2 + \\ & 6x_1 x_2^5 y_1 y_2 - 4x_2^6 y_1 y_2 + 10x_1^3 y_1^3 y_2 - \\ & 6x_1^2 x_2 y_1^3 y_2 - 18x_1 x_2^2 y_1^3 y_2 + 14x_2^3 y_1^3 y_2 - \\ & 6y_1^5 y_2 + 4x_1^6 y_2^2 - 12x_1^5 x_2 y_2^2 + 9x_1^4 x_2^2 y_2^2 + \\ & 4x_1^3 x_2^3 y_2^2 - 6x_1^2 x_2^4 y_2^2 + x_2^6 y_2^2 - \\ & 18x_1^3 y_1^2 y_2^2 + 18x_1^2 x_2 y_1^2 y_2^2 + 18x_1 x_2^2 y_1^2 y_2^2 - \\ & 18x_2^3 y_1^2 y_2^2 + 15y_1^4 y_2^2 + 14x_1^3 y_1 y_2^3 - \\ & 18x_1^2 x_2 y_1 y_2^3 - 6x_1 x_2^2 y_1 y_2^3 + 10x_2^3 y_1 y_2^3 - \\ & 20y_1^3 y_2^3 - 4x_1^3 y_2^4 + 6x_1^2 x_2 y_2^4 - 2x_2^3 y_2^4 + \\ & 15y_1^2 y_2^4 - 6y_1 y_2^5 + y_2^6) \end{aligned}$$

$$y_3^2 = x_3^3 + bx_3 + c$$

If $P_1 = P_2$

$$m = (3x_1^2 + b)/(2y_1)$$

$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1$$

$$x_3^3 + bx_3 + c - y_3^2 = x_1^3 + bx_1 + c - y_1^3 = 0$$
$$y_3^2 = x_3^3 + bx_3 + c$$

So P_3 is in the group.

Ex. 2 - Number of Points on an Elliptic Curve

1. (a)

$$[2]P = P + P$$
$$m = \frac{3 \times 8^2 + 3}{2 \times 9} \equiv 9 \bmod 11$$
$$x = 9^2 - 8 - 8 \equiv 10 \bmod 11$$
$$y = 9 \times (8 - 10) - 9 \equiv 6 \bmod 11$$
$$[2]P = (10, 6)$$

(b)

$$[4]P = [2]P + [2]P$$
$$m = \frac{3 \times 10^2 + 3}{2 \times 6} \equiv 6 \bmod 11$$
$$x = 6^2 - 10 - 10 \equiv 5 \bmod 11$$
$$y = 6 \times (10 - 5) - 6 \equiv 2 \bmod 11$$
$$[4]P = (5, 2)$$
$$[5]P = [4]P + P$$
$$m = \frac{9 - 2}{8 - 5} \equiv 6 \bmod 11$$
$$x = 6^2 - 5 - 8 \equiv 1 \bmod 11$$
$$y = 6 \times (5 - 1) - 2 \equiv 0 \bmod 11$$
$$[5]P = (1, 0)$$

(c)

$$[10]P = [5]P + [5]P$$
$$[10]P = (0, 0)$$

2. There are 10 points, including the one at infinity.

x mod 11	y^2 mod 11	y mod 11	Points on E
0	7		
1	0	0	(1, 0)
2	10		
3	10		
4	6		
5	4	2 or 9	(5, 2) and (5, 9)
6	10		
7	8		
8	4	2 or 9	(8, 2) and (8, 9)
9	4	2 or 9	(9, 2) and (9, 9)
10	3	5 or 6	(10, 5) and (10, 6)

Ex. 3 - ECDSA

Alice and Bob should first agree on an elliptic curve $\mathcal{C}$, base point G on the curve and the order n of G, i.e. $[n]G = \mathcal{O}$, and n must be a prime. Alice creates a random private key $d_A \in [1, n-1]$ and calculates public key $Q_A = [d_A]G$. To sign a message m,

1. Calculate $e = Hash(m)$.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Generate a random $k \in [1, n-1]$.
4. Calculate point $(x_1, y_1) = [k]G$.
5. Calculate $r \equiv x_1 \bmod n$. If $r = 0$, reselect k.
6. Calculate $s \equiv k^{-1}(z + rd_A) \bmod n$. If $s = 0$, reselect k.
7. Send the signature as (r, s).

When Bob wants to verify the signature,

1. Calculate $e = Hash(m)$.
2. Let z be the L_n leftmost bits of e, where L_n is the bit length of the group order n.
3. Calculate $u_1 = zs^{-1} \bmod n$ and $u_2 = rs^{-1} \bmod n$.
4. Calculate point $(x_1, y_1) = [u_1]G + [u_2]Q_A$.
5. If $(x_1, y_1) = \mathcal{O}$, the signature is invalid. Else if $r \equiv x_1 \bmod n$, the signature is valid.

ECDSA is good because for the same security level, ECDSA needs much shorter key length than DSA and calculation is faster.

Ex. 4 - BB84

Alice has two strings of bits, a and b, each is n-bit long. Then she encodes two strings into n qubits:

$$|\varphi\rangle = \bigotimes_{i=1}^{n} |\varphi_{a_i b_i}\rangle$$

where a_i and b_i are the ith bits of a and b. Together, $a_i b_i$ gives four qubit states:

$$|\varphi_{00}\rangle = |0\rangle$$

$$|\varphi_{10}\rangle = |1\rangle$$

$$|\varphi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\varphi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Then it is impossible to distinguish all of them with certainty without knowing b. Alice sends $|\varphi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\varphi\rangle\langle\varphi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by Eve. After Bob receives the string of qubits, both Bob and Eve have their own states. However, since only Alice knows b, it makes it impossible for either Bob or Eve to distinguish the states of the qubits. Bob proceeds to generate a string of random bits $b^{'}$ of the same length as b and then measures the qubits he has received from Alice, obtaining a bit string $a^{'}$. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b, i.e., the bases in which the qubits were prepared. Bob communicates over a public channel with Alice to determine which b_i and $b^{'}_i$ are not equal. Both Alice and Bob now discard the bits in a and $a^{'}$ where b and $b^{'}$ do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

Ex. 5 - Quantum Key Distribution

1. Alice and Bob can share their secret key in the quantum channel while use the classical channel to send and receive encrypted messages.

2. If Eve observes the quantum channel, then the photons being observed must collapse, and Alice and Bob will know Eve is interacting.

Ex. 6 - Simple Questions

1.

$$U_1 = \begin{pmatrix} u_{1,1,1} & \cdots & u_{1,1,n} \\ \vdots & \ddots & \vdots \\ u_{1,n,1} & \cdots & u_{1,n,n} \end{pmatrix}$$

U_2, V_1, V_2 are similarly denoted. Then

$$\begin{aligned}
(U_1 \otimes V_1) \cdot (U_2 \otimes V_2) &= \begin{pmatrix} u_{1,1,1}V_1 & \cdots & u_{1,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix} \cdot \begin{pmatrix} u_{1,1,1}V_2 & \cdots & u_{1,1,n}V_2 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_2 & \cdots & u_{1,n,n}V_2 \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^n u_{1,1,i}u_{2,i,1}V_1V_2 & \cdots & \sum_{i=1}^n u_{1,1,i}u_{2,i,1}V_1V_2 \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n u_{1,n,i}u_{2,i,n}V_1V_2 & \cdots & \sum_{i=1}^n u_{1,n,i}u_{2,i,n}V_1V_2 \end{pmatrix} \\
&= U_1U_2 \otimes V_1V_2
\end{aligned}$$

2.

$$\begin{aligned}
U_1 \otimes (V_1 + V_2) &= \begin{pmatrix} u_{1,1,1}(V_1 + V_2) & \cdots & u_{1,1,n}(V_1 + V_2) \\ \vdots & \ddots & \vdots \\ u_{1,n,1}(V_1 + V_2) & \cdots & u_{1,n,n}(V_1 + V_2) \end{pmatrix} \\
&= \begin{pmatrix} u_{1,1,1}V_1 & \cdots & u_{1,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix} + \begin{pmatrix} u_{1,1,1}V_2 & \cdots & u_{1,1,n}V_2 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_2 & \cdots & u_{1,n,n}V_2 \end{pmatrix} \\
&= U_1 \otimes V_1 + U_1 \otimes V_2
\end{aligned}$$

$$\begin{aligned}
(U_1 + U_2) \otimes V_1 &= \begin{pmatrix} (u_{1,1,1} + u_{2,1,1})V_1 & \cdots & (u_{1,1,n} + u_{2,1,n})V_1 \\ \vdots & \ddots & \vdots \\ (u_{1,n,1} + u_{2,n,1})V_1 & \cdots & (u_{1,n,n} + u_{2,n,n})V_1 \end{pmatrix} \\
&= \begin{pmatrix} u_{1,1,1}V_1 & \cdots & u_{1,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{1,n,1}V_1 & \cdots & u_{1,n,n}V_1 \end{pmatrix} + \begin{pmatrix} u_{2,1,1}V_1 & \cdots & u_{2,1,n}V_1 \\ \vdots & \ddots & \vdots \\ u_{2,n,1}V_1 & \cdots & u_{2,n,n}V_1 \end{pmatrix} \\
&= U_1 \otimes V_1 + U_2 \otimes V_1
\end{aligned}$$

So $\otimes$ is bilinear.