VE475 Intro to Cryptography Homework 10

Taoyue Xia, 518370910087

2021/07/27

Ex1 — Group structure on an elliptic curve

Taking two points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, let $P_3 = P_1 + P_2 = (x_3, y_3)$, where $x_3 = (m^2 - x_1 - x_2)$ and $y_3 = m(x_1 - x_3) - y_1$. We first prove that for P_3, it also satisfy $y_3^2 = x_3^3 + bx_3 + c$ for different m values.

$$\begin{aligned} x_3^3 + bx_3 + c &= (m^2 - x_1 - x_2)^3 + b(m^2 - x_1 - x_2) + c \\ &= m^6 - 3m^4(x_1 + x_2) + 3m^2(x_1^2 + x_2^2) + 6m^2 x_1 x_2 \\ &\quad - 3(x_1^2 x_2 + x_2^2 x_1) - x_1^3 - x_2^3 + b(m^2 - x_1 - x_2) + c \end{aligned}$$

$$\begin{aligned} y_3^2 &= [m(x_1 - x_3) - y_1]^2 \\ &= [m(2x_1 + x_2 - m^2) - y_1]^2 \\ &= m^2(2x_1 + x_2 - m^2)^2 - 2m(2x_1 + x_2 - m^2)y_1 + y_1^2 \\ &= m^6 - 4m^4 x_1 - 2m^4 x_2 + 4m^2 x_1^2 + 4m^2 x_1 x_2 + m^2 x_2^2 - 4m x_1 y_1 \\ &\quad - 2m x_2 y_1 + 2m^3 y_1 + y_1^2 \end{aligned}$$

$$\begin{aligned} y_3^2 - (x_3^3 + bx_3 + c) &= -m^4(x_1 - x_2) + m^2 x_1^2 - 2m^2 x_2^2 - 2m^2 x_1 x_2 - 4m x_1 y_1 - 2m x_2 y_1 \\ &\quad + 2m^3 y_1 + y_1^2 + 3(x_1^2 x_2 + x_2^2 x_1) + x_1^3 + x_2^3 - b(m^2 - x_1 - x_2) - c \end{aligned}$$

When $P_1 \neq P_2$, $m = \frac{y_2-y_1}{x_2-x_1}$, thus

$$\begin{aligned} y_3^2 - (x_3^3 + bx_3 + c) = &\frac{(y_2-y_1)^4}{(x_2-x_1)^3} + \frac{(y_2-y_1)^3}{(x_2-x_1)^3}y_1 + \frac{(y_2-y_1)^2}{(x_2-x_1)^2}(x_1^2 - 2x_2^2 - 2x_1x_2 - b) \\ &- \frac{y_2-y_1}{x_2-x_1}(4x_1y_1 + 2x_2y_1) + y_1^2 + 3(x_1^2x_2 + x_2^2x_1) \\ &+ x_1^3 + x_2^3 + b(x_1+x_2) - c \end{aligned}$$

After some calculation, we can prove that $y_3^2 - (x_3^3 + bx_3 + c) = 0$. However, this part is too tedious, so it will not be illustrated.
Then when $P_1 = P_2$, indicating $x_1 = x_2,\ y_1 = y_2$, with $m = (3x_1^2 + b)/(2y_1)$, we can get:

$$\begin{aligned} y_3^2 - (x_3^3 + bx_3 + c) &= -m^4(x_1 - x_2) + m^2x_1^2 - 2m^2x_2^2 - 2m^2x_1x_2 - 4mx_1y_1 - 2mx_2y_1 \\ &\quad + 2m^3y_1 + y_1^2 + 3(x_1^2x_2 + x_2^2x_1) + x_1^3 + x_2^3 - b(m^2 - x_1 - x_2) - c \\ &= -3(\frac{3x_1^2+b}{2y_1})^2x_1^2 - 6\frac{3x_1^2+b}{2y_1}x_1y_1 + 2(\frac{3x_1^2+b}{2y_1})^3y_1 + y_1^2 + 8x_1^3 \\ &\quad - b(\frac{3x_1^2+b}{2y_1})^2 + 2bx_1 - c \\ &= \frac{-3x_1^2(9x_1^4 + 6x_1^2b + b^2) + (27x_1^6 + 27x_1^4b + 9x_1^2b^2 + b^3) - b(9x_1^4 + 6x_1^2b + b^2)}{4y_1^2} \\ &\quad - (9x_1^2 + 3b)x_1 + (x_1^3 + bx_1 + c) + 8x_1^3 + 2bx_1 - c \\ &= 0 \end{aligned}$$

Therefore, we also prove that when $P_1 = P_2$, the addition also holds. So the addition law over E is proved.

Then we will prove the commutativity, which is for $P_1, P_2 \in E,\ P_1 + P_2 = P_2 + P_1$. When $P_1 = P_2$, it is always true, so we just need to consider the case $P_1 \neq P_2$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_1 + P_2 = P_3 = (x_3, y_3)$, $P_2 + P_1 = P_3' = (x_3', y_3')$. With $m = \frac{y_2-y_1}{x_2-x_1}$, we can have:

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 = m^2 - x_2 - x_1 = x_3' \\ y_3 &= m(x_1 - x_3) - y_1 = \frac{(y_2-y_1)(2x_1 + x_2 - m^2)}{x_2 - x_1} - y_1 \\ y_3' &= m(x_1 - x_3') - y_1 = \frac{(y_2-y_1)(2x_1 + x_2 - m^2)}{x_2 - x_1} - y_1 \end{aligned}$$

Therefore, we can see that $x_3 = x_3'$ and $y_3 = y_3'$, thus $P_3 = P_3'$. Therefore, the commutativity is proved.

Then we will prove the associativity. For $\mathcal{O},\ P_1,\ P_2,\ P_3$ on E, according to the properties of elliptic curves, we can know that $P_1 + P_2,\ -(P_1 + P_2),\ P_2 + P_3,\ -(P_2 + P_3)$ are also on the curve E. Then we can see that the point $-(P_1 + P_2 + P_3)$ is on the line which passes through points $P_1 + P_2$ and P_3. Also, the point is on the line which passes through points P_1 and $P_2 + P_3$. Which gives

$$(P_1 + P_2) + P_3 + (-(P_1 + P_2 + P_3)) = 0 \qquad \text{and} \qquad P_1 + (P_2 + P_3) + (-(P_1 + P_2 + P_3)) = 0$$

Therefore, we have proved that $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Therefore, the assosciativity is proved.
The whole proposition is proved.

Ex2 — Number of points on an elliptic curve

1. We have E as $y^2 = x^3 + 3x + 7$ over $\mathbb{F}_{11}$ and $P = (8, 9)$. Since $[2]P = P + P = (x_2, y_2)$, we can calculate it as:

$$m \equiv \frac{3 \cdot 8^2 + 3}{2 \cdot 9} \equiv \frac{65}{6} \equiv 65 \cdot 2 \equiv 9 \ mod\ 11$$

$$x_2 \equiv m^2 - 2 \cdot 8 \equiv 81 - 16 \equiv 10 \ mod\ 11$$

$$y_2 \equiv m(8 - 10) - 9 \equiv -18 - 9 \equiv 6 \ mod\ 11$$

So we can see that $[2]P = (10, 6)$
For $[5]P$, we can calculate it as $[5]P = [2]P + [2]P + P$. we first calculate $[4]P = [2]P + [2]P = (x_4, y_4)$:

$$m_4 \equiv \frac{3 \cdot 10^2 + 3}{2 \cdot 6} \equiv \frac{101}{4} \equiv 101 \cdot 3 \equiv 6 \ mod\ 11$$

$$x_4 \equiv m_4^2 - 2x_2 \equiv 36 - 20 \equiv 5 \ mod\ 11$$

$$y_4 \equiv m_4(x_2 - x_4) - y_2 \equiv 6 \cdot (10 - 5) - 6 \equiv 2 \ mod\ 11$$

So we get that $[4]P = (5, 2)$. Then we can calculate $[5]P = [4]P + P = (x_5, y_5)$:

$$m_5 \equiv \frac{y_1 - y_4}{x_1 - x_4} \equiv \frac{9-2}{8-5} \equiv 7 \cdot 4 \equiv 6 \; mod \; 11$$

$$x_5 \equiv m_5^2 - x_4 - x_1 \equiv 36 - 5 - 8 \equiv 1 \; mod \; 11$$

$$y_5 \equiv m_5(x_4 - x_5) - y_4 \equiv 6 \cdot (5-1) - 2 \equiv 22 \equiv 0 \; mod \; 11$$

Therefore, we see that $[5]P = (1, 0)$.
For $[10]P$, we see that $[10]P = [5]P + [5]P$. However, we find that the y value for $[5]P$ is 0, so the line through $[5]P$ is vertical to the x axis. Therefore, $[10]P = \mathcal{O}$, the unit element.

2. We will show by the following table.

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), (5,9)
6	10		
7	8		
8	4	2 or 9	(8,2), (8,9)
9	4	2 or 9	(9,2), (9,9)
10	3	5 or 6	(10,5), (10,6)

So there are $1 + 4 \cdot 2 + 1 = 10$ points on E, containing the unit element $\mathcal{O}$.

3. The points are (1,0), (5,2), (5,9), (8,2), (8,9), (9,2), (9,9), (10,5), (10,6), and a unit element $\mathcal{O} = \infty$.

Ex3 — ECDSA

For the Elliptic Curve Digital Signature Algorithm (ECDSA), Alice and Bob need the following parameters:

1. An elliptic curve E, and the equation used.
2. A base point G on E, which generates a subgroup of large prime order n.
3. The prime order n, which means that $[n]G = \mathcal{O}$, the unit element.
4. A randomly selected private key d_A in the interval $[1, n-1]$.
5. A public key Q_A, calculated by the elliptic curve $Q_A = [d_A]G$.
6. The message m to send.

We first define a cryptographic hash function H, and the output converted to integer. For Alice to sign the message, she follows the steps:

1. Calculate $e = H(m)$.
2. Set z to be the L_n leftmost bits of e, where L_n represents for the bit length of n.
3. Select a cryptographic secure random number k in the interval $[1, n-1]$.
4. Calculate the curve point $(x_1, y_1) = [k]G$.
5. Calculate $r = x_1 \bmod n$. If $r = 0$, go back to step 3.
6. Calculate $s = k^{-1}(z + rd_A) \mod n$. If $s = 0$, go back to step 3.
7. The signature is the pair (r, s).

Note that we need to make k secret, as well as select different k for different signatures. Otherwise step 6 can be used to solve d_A, the private key. The procedures are as follows:
Given two signatures (r, s) and (r, s'), which uses the same k for different messages m and m', an attacker can calculate z and z', and since $s - s' \equiv k^{-1}(z - z') \mod n$, the attacker can find $k \equiv \frac{z-z'}{s-s'} \mod n$. Since $s \equiv k^{-1}(z + rd_A) \mod n$, the attacker can now calculate $d_A \equiv \frac{ks-z}{r}$

mod n. Therefore, using the same k multiple times is dangerous.
Then for Bob to authenticate Alice's signature, he must have a copy of her public-key curve point Q_A. Bob can first verify Q_A as a valid point as follows:

1. Check that Q_A is not equal to the unit element $\mathcal{O}$.
2. Check that Q_A lies on the curve.
3. Check that $[n]Q_A = \mathcal{O}$.

After verifying Q_A, Bob can verify the signature following these steps:

1. Verify that r and s are integers in $[1, n-1]$. If not, the signature is invalid.
2. calculate $e = H(m)$, with the same hash function H.
3. Let z be the L_n leftmost bits of e.
4. Calculate $u_1 \equiv zs^{-1} \mod n$, $u_2 \equiv rs^{-1} \mod n$.
5. Calculate the curve point $(x_1, y_1) = [u_1]G + [u_2]Q_A$. If the result is $\mathcal{O}$, then the signature is invalid.
6. Finally, the signature is valid if $r \equiv x_1 \mod n$, invalid otherwise.

Then we show the correctness of such algorithm, denote C as the curve point calculated in step 5.

$$\begin{aligned} C &= [u_1]G + [u_2]Q_A \\ &= [u_1]G + [u_2 d_A]G \\ &= [u_1 + u_2 d_A]G \\ &= [zs^{-1} + rs^{-1}d_A]G \\ &= [s^{-1}(z + rd_A)]G \\ &= [k]G = (x_1, y_1) \end{aligned}$$

Therefore, the point corresponds to the point generated by Alice, the correctness is verified.
The benefits of ECDSA is shown below:

1. It needs smaller sized keys to meet the requirement of a specific security level. Namely, if the security level is 128-bit, its key just needs two times the bit length, which is 256 bits, to be secure. However, for common RSA it should be 3072 bits.

2. Smaller key means faster calculation and faster transmission. The signature needs less time to create, less space to store, and less time to transmit to the receiver.

Ex4 — BB84

BB84 is a quantum key distribution scheme developed in 1984, which is the first quantum cryptography protocol.
In the BB84 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a tensor product of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle$$

Where a_i, b_i are the i_{th} bits of a and b. Together, $a_i b_i$ give us an index into the following four qubit states:

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

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

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

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

Alice sends $|\psi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by a third party Eve. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability 1/2 if she guesses the wrong basis.
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. 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.

Ex5 — Quantum key distribution

1. Alice and Bob can use the quantum channel to generate and share a private key, and then use the classical channel to tranfer encrypted messages with that key.

2. If Eve observes photons in the quantum channel, the original state will collapse and change to another one. This change can be easily detected by Alice and Bob, since they are transmitting information. Therefore, they can simply choose another private key, and Eve cannot get any information.

Ex6 — Simple questions

1. First show the expression of $U_1 \otimes V_1$, denote the elements as $u_{1_{ij}}, v_{1_{ij}}$:

$$U_1 \otimes V_1 = \begin{pmatrix} u_{1_{11}}V_1 & u_{1_{12}}V_1 & \cdots & u_{1_{1n}}V_1 \\ u_{1_{21}}V_1 & u_{1_{22}}V_1 & \cdots & u_{1_{2n}}V_1 \\ \vdots & \vdots & \ddots & \vdots \\ u_{1_{n1}}V_1 & u_{1_{n2}}V_1 & \cdots & u_{1_{nn}}V_1 \end{pmatrix}$$

$$= \begin{pmatrix} u_{1_{11}}v_{1_{11}} & u_{1_{11}}v1_{12} & \cdots & u_{1_{11}}v1_{1n} & u_{1_{12}}v_{1_{11}} & \cdots & u_{1_{1n}}v_{1_{1n}} \\ u_{1_{11}}v_{1_{21}} & u_{1_{11}}v1_{22} & \cdots & u_{1_{11}}v1_{2n} & u_{1_{12}}v_{1_{21}} & \cdots & u_{1_{1n}}v_{1_{2n}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ u_{1_{11}}v_{1_{n1}} & u_{1_{11}}v1_{n2} & \cdots & u_{1_{11}}v1_{nn} & u_{1_{12}}v_{1_{n1}} & \cdots & u_{1_{1n}}v_{1_{nn}} \\ u_{1_{21}}v_{1_{11}} & u_{1_{21}}v1_{12} & \cdots & u_{1_{21}}v1_{1n} & u_{1_{22}}v_{1_{11}} & \cdots & u_{1_{2n}}v_{1_{1n}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ u_{1_{n1}}v_{1_{n1}} & u_{1_{n1}}v1_{n2} & \cdots & u_{1_{n1}}v1_{nn} & u_{1_{n2}}v_{1_{n1}} & \cdots & u_{1_{nn}}v_{1_{nn}} \end{pmatrix}$$

Then we can calculate U_1U_2.

$$U_1U_2 = \begin{pmatrix} \sum_{i=1}^n u_{1_{1i}}u_{2_{i1}} & \sum_{i=1}^n u_{1_{1i}}u_{2_{i2}} & \cdots & \sum_{i=1}^n u_{1_{1i}}u_{2_{in}} \\ \sum_{i=1}^n u_{1_{2i}}u_{2_{i1}} & \sum_{i=1}^n u_{1_{2i}}u_{2_{i2}} & \cdots & \sum_{i=1}^n u_{1_{2i}}u_{2_{in}} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n u_{1_{ni}}u_{2_{i1}} & \sum_{i=1}^n u_{1_{ni}}u_{2_{i2}} & \cdots & \sum_{i=1}^n u_{1_{ni}}u_{2_{in}} \end{pmatrix}$$

Similarly, we can use the same method to express $U_2 \otimes V_2$ and V_1V_2. In this way, $(U_1 \otimes U_2) \cdot (U_2 \otimes V_2)$ can be shown as:

$$\begin{pmatrix} \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{1j}}u_{2_{i1}}v_{2_{j1}} & \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{1j}}u_{2_{i1}}v_{2_{j2}} & \cdots & \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{1j}}u_{2_{in}}v_{2_{jn}} \\ \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{2j}}u_{2_{i1}}v_{2_{j1}} & \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{2j}}u_{2_{i1}}v_{2_{j2}} & \cdots & \sum_{i=1}^n \sum_{j=1}^n u_{1_{1i}}v_{1_{2j}}u_{2_{in}}v_{2_{jn}} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n \sum_{j=1}^n u_{1_{ni}}v_{1_{nj}}u_{2_{i1}}v_{2_{j1}} & \sum_{i=1}^n \sum_{j=1}^n u_{1_{ni}}v_{1_{nj}}u_{2_{i1}}v_{2_{j2}} & \cdots & \sum_{i=1}^n \sum_{j=1}^n u_{1_{ni}}v_{1_{nj}}u_{2_{in}}v_{2_{jn}} \end{pmatrix}$$

Then $(U_1U_2) \otimes (V_1V_2)$ can be expressed as:

$$\begin{pmatrix} \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i1}} V_1V_2 & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i2}} V_1V_2 & \cdots & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{in}} V_1V_2 \\ \sum_{i=1}^{n} u_{1_{2i}} u_{2_{i1}} V_1V_2 & \sum_{i=1}^{n} u_{1_{2i}} u_{2_{i2}} V_1V_2 & \cdots & \sum_{i=1}^{n} u_{1_{2i}} u_{2_{in}} V_1V_2 \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{n} u_{1_{ni}} u_{2_{i1}} V_1V_2 & \sum_{i=1}^{n} u_{1_{ni}} u_{2_{i2}} V_1V_2 & \cdots & \sum_{i=1}^{n} u_{1_{ni}} u_{2_{in}} V_1V_2 \end{pmatrix}$$

After expanding, we can have:

$$\begin{pmatrix} \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{1j}} v_{2_{j1}} & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{1j}} v_{2_{j2}} & \cdots & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{in}} \cdot \sum_{j=1}^{n} v_{1_{1j}} v_{2_{jn}} \\ \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{2j}} v_{2_{j1}} & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{2j}} v_{2_{j2}} & \cdots & \sum_{i=1}^{n} u_{1_{1i}} u_{2_{in}} \cdot \sum_{j=1}^{n} v_{1_{2j}} v_{2_{jn}} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^{n} u_{1_{ni}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{nj}} v_{2_{j1}} & \sum_{i=1}^{n} u_{1_{ni}} u_{2_{i1}} \cdot \sum_{j=1}^{n} v_{1_{nj}} v_{2_{j2}} & \cdots & \sum_{i=1}^{n} u_{1_{ni}} u_{2_{in}} \cdot \sum_{j=1}^{n} v_{1_{nj}} v_{2_{jn}} \end{pmatrix}$$

After some transforming, we can simply find that the two expressions are the same. Therefore, we proved that $(U_1 \otimes V_1) \cdot (U_2 \otimes V_2) = U_1U_2 \otimes V_1V_2$.

2. Suppose that U and V are two vector spaces both of dimension n, the operator $\otimes$ can be understood as: $\otimes :\ U \times V \to W$, where W is also a vector space. For $u,\ u_1,\ u_2 \in U$, $v,\ v_1,\ v_2 \in V$, we first define the following.

$$u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix},\ v_1 = \begin{pmatrix} v_{11} \\ v_{12} \\ \vdots \\ v_{1n} \end{pmatrix},\ v_2 = \begin{pmatrix} v_{21} \\ v_{22} \\ \vdots \\ v_{2n} \end{pmatrix}\ v_1 + v_2 = \begin{pmatrix} v_{11} + v_{21} \\ v_{12} + v_{22} \\ \vdots \\ v_{1n} + v_{2n} \end{pmatrix}$$

So $u \otimes (v_1 + v_2)$ can be expressed as:

$$\begin{aligned}
&\begin{pmatrix} u_1(v_{11}+v_{21}) & u_1(v_{12}+v_{22}) & \cdots & u_1(v_{1n}+v_{2n}) \\ u_2(v_{11}+v_{21}) & u_2(v_{12}+v_{22}) & \cdots & u_2(v_{1n}+v_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ u_n v_{11}+v_{21} & u_n(v_{12}+v_{22}) & \cdots & u_n(v_{1n}+v_{2n}) \end{pmatrix} \\
&= \begin{pmatrix} u_1v_{11} & u_1v_{12} & \cdots & u_1v_{1n} \\ u_2v_{11} & u_2v_{12} & \vdots & u_2v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ u_nv_{11} & u_nv_{12} & \cdots & u_nv_{1n} \end{pmatrix} + \begin{pmatrix} u_1v_{21} & u_1v_{22} & \cdots & u_1v_{2n} \\ u_2v_{21} & u_2v_{22} & \vdots & u_2v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_nv_{21} & u_nv_{22} & \cdots & u_nv_{2n} \end{pmatrix} \\
&= u \otimes v_1 + u \otimes v_2
\end{aligned}$$

Therefore, we can have $u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$. Then we want to analyze $(u_1 + u_2) \otimes v$. In the same way, we can also prove that:

$$(u_1 + u_2) \otimes v = (u_1 \otimes v) + (u_2 \otimes v)$$

According to the above two properties being proved, we can conclude that the operate $\otimes$ is bilinear.