Introduction to Cryptography: Homework 11

December 8, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, December 20, 17:00 sharp!

Grading: You can score a total of 100 points for the hand-in assignments. To get full points, please **explain all answers clearly**.

Exercises:

1. **Practicing with elliptic curve additions.** Given the elliptic curve $\mathcal{E} : y^2 = x^3 + 5x + 3$ over the finite field $\mathbb{F}_{11}$. In table 1, we demonstrate part of the additive table for this elliptic curve.

$+$	$\mathcal{O}$	$(0,5)$			$(1,8)$	$(3,1)$	$(3,10)$	$(8,4)$	$(8,7)$
$\mathcal{O}$									
$(0,5)$		$(3,10)$		$(3,1)$		$(0,6)$	$(1,8)$	$(8,7)$	$(1,3)$
				$(8,7)$	$(3,10)$		$(0,5)$	$(1,8)$	$(8,4)$
						$(8,4)$		$(0,5)$	$(3,10)$
$(1,8)$					$(1,3)$	$(0,5)$	$(8,7)$		$(0,6)$
$(3,1)$								$(3,10)$	
$(3,10)$							$(8,4)$	$(1,3)$	$(3,1)$
$(8,4)$								$(0,6)$	
$(8,7)$									

Table 1: The additive table for $\mathcal{E} : y^2 = x^3 + 5x + 3$ over $\mathbb{F}_{11}$.

(a) Copy and finish the table using your knowledge of group theory and the fact that $\mathcal{E}(\mathbb{F}_{11})$ is an abelian group. [Hints:

i. How can you recognize $-P$ when given P?
ii. What is the neutral element of the elliptic curve group?
iii. How can you observe the abelianness of a group in its additive table?
iv. How many times can a single element appear in each row or column?
v. In an abelian group $-(P+Q) = -P + -Q$, how does this relate to doubling points?

Procedure:

- Use the answer to hint (i) to complete the indices (sorted by ascending x-coordinate);
- Use the answer to hint (ii) to complete the first row and column;
- Use the answer to hint (iii) to complete several values in the lower triangle;
- Use the answer to hint (v) to complete the diagonal;
- Use the answer to hints (iv) and (iii) to complete the remainder of the table.

]

(b) Compute the additions (or doubles) that you entered in part (a) using the formulas explicitly and check them with your table. [Do as many as you need to do, in order to get comfortable with the formulas and computations.]

(c) Give a subgroup of order 3 of $\mathcal{E}(\mathbb{F}_{11})$. [Hint: A subgroup is generated by an element G for which $[2]G = -G$.]

(d) Is $\mathcal{E}(\mathbb{F}_{11})$ cyclic? If yes, give a generator. If no, show that no generator exists.

2. **Order of elliptic curve groups.** Given an elliptic curve $\mathcal{E} : y^2 = x^3 + ax + b$ over a finite field $\mathbb{F}_q$.

   (a) Explain that for every possible value of x, there can be at most two values of y such that $(x, y) \in \mathcal{E}(\mathbb{F}_q)$.

   (b) Give an upper bound on $\#\mathcal{E}(\mathbb{F}_q)$ using part (a).

   (c) Verify your upper bound where $q = 13$, $a = 2$ and $b = 1$. (I.e., show that $\#\mathcal{E}(\mathbb{F}_q)$ is indeed less than the bound from part (b).)

3. **Points of intersection of elliptic curves and lines.** Given the elliptic curve $\mathcal{E} : y^2 = x^3 + 1$ over the real numbers. Consider the line $L : y = \frac{1}{2\sqrt{2}}x + \frac{5}{4\sqrt{2}}$.

   (a) Substitute L into $\mathcal{E}$ to get a cubic equation. Show that $x = \frac{1}{2}$ is a solution to this cubic equation.

   (b) Do a long division of your cubic equation by $x - \frac{1}{2}$ to get a quadratic equation.

   (c) Find the roots of the quadratic equation.

4. **EC Schnorr completeness.** Show that the ECSchnorr protocol is complete. [Hint: The ECSchnorr protocol was discussed in slide 15 of slides_12_ecc2.]

5. **Scalar multiplication versus exponentiation.** In this exercise, we are going to compare the computational costs of a scalar multiplication (on elliptic curves) with the costs of an exponentiation (in a modular group). For a fair comparison, we consider an elliptic curve over a field $\mathbb{F}_p$ with a subgroup of order q generated by G. We also consider a modular group $(\mathbb{Z}/p'\mathbb{Z})^*$ with a subgroup $\langle g \rangle$ generated by g of order q. Here, p' is a prime number of 3072 bits, and p and q prime numbers of 256 bits. Let $x \in \mathbb{Z}/q\mathbb{Z}$ be a 256-bit integer, of which the bit representation has roughly 128 ones and 128 zeros.

   (a) How many bits of security does the modular group provide with respect to the discrete log problem?

   (b) How many bits of security does the elliptic-curve group provide with respect to the elliptic-curve discrete log problem?

   (c) Suppose that you compute g^x with the square-and-multiply algorithm. How many squarings and how many multiplications do you need to perform?

   (d) Suppose that you compute $[x]G$ with the double-and-add algorithm. How many doublings and how many additions do you need to perform?

   To compare the costs of computing g^x with the costs of computing $[x]G$, we need to know the costs of doublings $\mathbf{D}$ and additions $\mathbf{A}$ (on the elliptic curve), multiplications $\mathbf{M}_p$ and squarings $\mathbf{S}_p$ in $\mathbb{F}_p$, and multiplications $\mathbf{M}_{p'}$ and squarings $\mathbf{S}_{p'}$ in $(\mathbb{Z}/p'\mathbb{Z})^*$. For this exercise, you may assume that $\mathbf{M}_p = \mathbf{S}_p$, $\mathbf{M}_{p'} = \mathbf{S}_{p'}$, $\mathbf{D} = 7\mathbf{M}_p$ and $\mathbf{A} = 16\mathbf{M}_p$. Furthermore, $\mathbf{M}_{p'} \approx 50\mathbf{M}_p$.

   (e) Express the costs of computing g^x in the number of multiplications $\mathbf{M}_p$.

   (f) Express the costs of computing $[x]G$ in the number of multiplications $\mathbf{M}_p$.

Hand in assignments

1. **(40 points) Elliptic curves computations.** Consider the elliptic curve $\mathcal{E} : y^2 = x^3 + 11x + 18$ over the finite field $\mathbb{F}_{23}$. Let it be given that $\#\mathcal{E}(\mathbb{F}_{23}) = 31$.

   (a) Which of the points $(19, 5)$ and $(2, 17)$ are on the curve? 3 pt

   (b) How many points with coordinate $x = 10$ are on the curve? Write down all points and explain your answer. 3 pt

   (c) The points $P = (15, 4)$ and $Q = (14, 8)$ lie on the curve. Compute $P + Q$. 8 pt

   (d) Compute $[2]P$. 8 pt

   (e) Give a generator of the group $\mathcal{E}(\mathbb{F}_{23})$. Explain your answer! 6 pt

   (f) Let $P = (x, y)$ and $-P = (x, -y)$ be on the curve and not have order 2. Show that, if y is even modulo 23, that $-y$ is odd modulo 23 and vice versa. 4 pt

   (g) What happens with points of order 2? 2 pt

   (h) Are there elements of order 2 in $\mathcal{E}(\mathbb{F}_{23})$? 3 pt

   Because of (f), we can express points in their *compressed point representation.* We will write 0 instead of the y-coordinate, if the y-coordinate is even, and 1 if the y-coordinate is odd. For example, for the point $R = (9, 8)$, we can write $R^c = (9, 0)$, while for $-R = (9, 15)$, we can write $R^c = (9, 1)$.

   (i) What is the point T, for which the compressed point representation is $T^c = (20, 1)$? 3 pt

2. (**20 points**) **Elliptic curves and orders of points.** Consider the elliptic curve $\mathcal{E} : y^2 = x^3 + 12x + 15$ over $\mathbb{F}_{23}$. Let it be given that $\#\mathcal{E}(\mathbb{F}_{23}) = 33$.

   (a) Show that $Q := (3, 3)$ lies on the curve $\mathcal{E}$. 2 pt

   (b) Compute $[2]Q$. 8 pt

   (c) What are the possible orders of a point R in $\mathcal{E}(\mathbb{F}_{23})$? [Hint: Lagrange's Theorem.] 2 pt

   (d) Consider $Q = (3, 3)$, that is not a generator of the *entire* group $\mathcal{E}(\mathbb{F}_{23})$. What is the order of Q? 4 pt

   (e) Give (homogeneous) projective coordinates for the point Q. 1 pt

   (f) Let $R_{\mathbb{P}} = (9 : 20 : 4)$ be a point represented by (homogeneous) projective coordinates. Give the affine representation of the point R. 3 pt

3. **(40 points) Elliptic-curve Merkle-Diffie-Hellman.** Alice and Bob want to share a key and they decide to use the elliptic-curve Merkle-Diffie-Hellman key agreement. They have decided on the subgroup of the elliptic curve $\mathcal{E} : y^2 = x^3 + 5x + 4$ over the field $\mathbb{F}_{13}$ generated by $G = (1, 7)$.

   (a) Determine Alice's public key, given that Alice's private key is $a = 3$. 17 pt

   (b) Give the compressed point representation of Alice's public key. 1 pt

   (c) Suppose Bob's public key $B = (4, 1)$ is given in compressed point representation. Convert Bob's public key to affine coordinates. 4 pt

   (d) Using Bob's public key B, compute the shared secret of Alice and Bob. 18 pt