CPSC/PMAT 629 — Elliptic Curves and Cryptography
ASSIGNMENT 3

Problem 1. *A supersingular curve and its embedding degree*

Consider the elliptic curve E defined by

$$E : y^2 + y = x^3 \quad \text{over } \mathbb{F}_2 \ . \qquad (*)$$

(1) Prove that

$$|E(\mathbb{F}_{2^n})| = \begin{cases} 2^n + 1 & \text{if } n \text{ is odd,} \\ 2^n + 1 - 2(-2)^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Conclude that E is supersingular.

(2) For any elliptic curve E over a field $\mathbb{F}_q$ with group order $N = |E(\mathbb{F}_q)|$, the *embedding degree*[1] is the smallest integer d such that $\mu_N \subseteq \mathbb{F}_{q^d}^*$, i.e. $\mathbb{F}_{q^d}$ contains the N-th roots of unity. Equivalently, d is the order of q in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. Fix n and consider the elliptic curve $(*)$ over $\mathbb{F}_{2^n}$. Determine the embedding degree for E over $\mathbb{F}_{2^n}$. (Note: it is dependent on the parity of n).

Problem 2. *Anomalous Curves*

We say that an elliptic curve E over $\mathbb{F}_q$ is *anomalous over* $\mathbb{F}_{q^n}$ if $|E(\mathbb{F}_{q^n})| = q^n$.

(1) Consider a prime power $q \geq 7$. Show that if an elliptic curve E over $\mathbb{F}_q$ contains a point of order q, then it is anomalous over $\mathbb{F}_q$.
(2) Show that if E is anomalous over $\mathbb{F}_q$, then E is not anomalous over $\mathbb{F}_{q^2}$.
(3) Show that if E is anomalous over $\mathbb{F}_2$, then E is anomalous over $\mathbb{F}_{16}$.

Problem 3. *Point multiplication*

(1) Construct a binary expansion and a NAF binary expansion for $n = 917$.
(2) Construct a τ-adic expansion for 917 for the elliptic curve given by

$$E : y^2 + xy = x^3 + x^2 + 1 \text{ over } \mathbb{F}_{2^k}$$

where τ represents the endomorphism generated by the frobenius map ϕ_2 for $\mathbb{F}_2$.

(3) Consider an elliptic curve over $\mathbb{F}_q$ where $q \approx 2^{160}$. Instead of choosing my scalar multiple at random (in ECDH, ECDSA or the like), I choose an integer which has a sparse binary representation, say on average only 1 out of every 10 bits is a 1. I claim this is more efficient than using NAF.
   (a) Is this claim true?
   (b) Is there any loss of true security in using this approach?

[1] One can prove $E[N] \subseteq E(\mathbb{F}_{q^d})$, so the Weil pairing "embeds" $E(\mathbb{F}_q)$ into $\mathbb{F}_{q^d}$. For supersingular curves, $d \leq 6$, so the ECDLP for such a curve is no harder than the DLP in an at worst slightly larger finite field.

NOTE: Please do any *two* of Problems 4 to 7.

Problem 4. *Speeding up Pollard rho using automorphisms*

Recall that the number of operations on average required to solve a discrete log instance on an elliptic curve of size N using Pollard-rho is $\sqrt{\pi N/2}$. We will say that the discrete logarithm problems on two elliptic curves have the same complexity if the number of elliptic curve operations required to solve the ECDLP on both using Pollard-rho is essentially the same.

(1) If a curve has a trivially computable automorphism of order m, how much larger must the resulting group be than one without any such automorphisms for the two problems to have the same complexity?
(2) In particular, if we consider binary anomalous curves (i.e. Koblitz curves) over $\mathbb{F}_{2^n}$, what size binary field (using a non-Koblitz curve) gives the same complexity?
(3) Why are the above arguments/definition not entirely "perfect"? How close are they?

Problem 5. *Security aspects of elliptic curve cryptographic protocols*

(1) Explain why, in the ECDSA protocol, the check that r and s are in $[1, n-1]$ is required for signature verification, by describing a means by which an adversary can forge a signature on an arbitrary message m that will succeed if this check is omitted.
(2) Explain why, in the ECDSA protocol, the same random value k must not be used to sign multiple messages by describing an attack that succeeds otherwise.
(3) Explain why the embedded public key validation step is required in the ECIES and ECMQV protocols by describing an attack that will succeed if this validation is omitted.

Problem 6. *Discrete logarithm problems*

Be sure to include details of your work for this question.

(1) Consider the elliptic curve E given by

$$E : y^2 = x^3 + 436743x + 67111 \text{ over } \mathbb{F}_{1048583} \ .$$

The number of points on E is 1049580. Find the discrete logarithm $\log_P(Q)$ for $P = (169541 : 556330)$ and $Q = (858751 : 762468)$ using the Pohlig-Hellman attack.
(2) Consider the elliptic curve E given by

$$E : y^2 = x^3 + 900410x + 465299 \text{ over } \mathbb{F}_{1048583} \ .$$

The number of points on this curve is 1049623. Find the discrete log problem $\log_P(Q)$ for $P = (815314 : 582035)$ and $Q = (67861 : 1005415)$ using any technique EXCEPT brute force.
(3) Compare the number of elliptic curve operations required to solve both problems.

Problem 7. *ECDSA*

Take as domain parameters for an ECDSA algorithm the field $\mathbb{F}_{751}$, with standard representation, the elliptic curve $E : y^2 = x^3 - x - 563$, the basepoint $P = (2, 373)$ which has order 727, and the cofactor is 1 (i.e. P generates the group of points on the curve). For each lower case letter assign a value between 1 and 26 (inclusive), and each capital letter a value between 27 and 52. Define a (really stupid) hash function to be the sum of the message modulo 727. Your private key is $d = 113$.

(1) Use ECDSA to create a signature for the message "I am great" using $k = 235$ as your random value for k. (Show each step of ECDSA, AND show the sequence of points that occur in the double-and-add used to compute kP.)
(2) Verify that your signature is correct using your public key $Q = 113P$ (you will first need to compute this).
(3) Find another message (that's not just garbage) that you have also "signed" by signing this message.

NOTE: We (the designers of this course) would appreciate answers from everyone for the following "Problem"!

Problem 8. *Conclusion*

Only effort will be graded for your responses to this question:

(1) What topics in the course were the most interesting?
(2) What were the least?
(3) What material should have been covered in more depth?
(4) What material should have been covered in less depth?
(5) Do you have any suggestions for the ordering of the material in the course?