Exercise sheet 4, 3 March 2022

We will work through these exercises on wonder.me; you can find the URL for the room in the Zulip chat. These are exercises to challenge your understanding of the lectures you have watched already, These are not for homework but for working on during the live session, ideally with a group of people..If you need a shared whiteboard I suggest you use https://webwhiteboard.com; one of you opens the board and then shares the url in the chat in your circle.
You can call me over by choosing "invite to circle". Please note, though, that if I am in another circle busy talking I will not come right away and invitations expire quickly. I will be in the bottom right space "Tanja's hideout" when I am not busy.

This exercise sheet covers hash-based signatures and isogeny-based crypto. The following is relevant for the latter topic. The addition law on Weierstrass curves $y^2 = x^3 + ax + b$ is given by ∞ being the neutral element, $-(x, y) = (x, -y)$ and

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),$$

where

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} \\ \frac{3x_1^2 + a}{2y_1} \end{cases} \quad \text{for} \quad \begin{cases} P_1 \neq \pm P_2 \\ P_1 = P_2 \neq -P_2 \end{cases}$$

1. The HORS (Hash to Obtain Random Subset) signature scheme is an example of a few-time signature scheme. It has integer parameters k, t, and ℓ, uses a hash function $H : \{0,1\}^* \to \{0,1\}^{k \cdot \log_2 t}$ and a one-way function $f : \{0,1\}^\ell \to \{0,1\}^\ell$. For simplicity assume that H is surjective.

   To generate the key pair, a user picks t strings $s_i \in \{0,1\}^\ell$ and computes $v_i = f(s_i)$ for $0 \leq i < t$. The public key is $P = (v_0, v_1, \ldots, v_{t-1})$; the secret key is $S = (s_0, s_1, \ldots, s_{t-1})$.

   To sign a message $m \in \{0,1\}^*$ compute $H(m) = (h_0, h_1, \ldots, h_{k-1})$, where each $h_i \in \{0, 1, 2, \ldots, t-1\}$. The signature on m is $\sigma = (s_{h_0}, s_{h_1}, s_{h_2}, \ldots, s_{h_{k-1}})$.

   To verify the signature, compute $H(m) = (h_0, h_1, \ldots, h_{k-1})$ and $(f(s_{h_0}), f(s_{h_1}), f(s_{h_2}), \ldots, f(s_{h_{k-1}}))$ and verify that $f(s_{h_i}) = v_{h_i}$ for $0 \leq i < t$.

   (a) Let $\ell = 80$, $t = 2^5$, and $k = 3$. How large (in bits) are the public and secret keys? How large is a signature? How many different signatures can the signer generate for a fixed key pair as $H(m)$ varies? Ignore that s-values could collide.

   (b) The same public key can be used for $r + 1$ signatures if H is r-subset-resilient, meaning that given r signatures and thus r vectors $\sigma_j = (s_{h_{j,0}}, s_{h_{j,1}}, s_{h_{j,2}}, \ldots, s_{h_{j,k-1}})$, $1 \leq j \leq r$ the probability that $H(m')$ consists entirely of components in $\{h_{j,i} | 0 \leq i < k, 1 \leq j \leq r\}$ is negligible.

   Even for $r = 1$, i.e. after seeing just one typical signature, an attacker has an advantage at creating a fake signature. What are the options beyond exact collisions in H?

(c) Let $\ell = 80$, $t = 2^5$, and $k = 3$. Let m be a message so that $H(m) = (h_0, h_1, h_2)$ satisfies that $h_i \neq h_j$ for $i \neq j$. You get to specify messages that Alice signs. You may not ask Alice to sign m.

State the smallest number of HORS signatures you need to request from Alice in order to construct a signature on m? How many calls to H does this require on average? You should assume that H and f do not have additional weaknesses beyond having too small parameters. Explain how you could use under 1000 evaluations of H if you are allowed to ask for two signatures.

2. Let

$$E/\mathbb{Q} : y^2 = x^3 + 1$$

and observe that $(-1, 0), (0, 1) \in E(\mathbb{Q})$.

(a) Compute $(-1, 0) + (0, 1)$ using addition law.

(b) Compute $2(0, 1)$ using the addition law.

(c) Compute the order of $(0, 1)$. (Note that over the rationals a point need not have finite order, but this one does.

3. Let

$$E_1/\mathbb{F}_{17} : y^2 = x^3 + 1, \qquad E_2/\mathbb{F}_{17} : y^2 = x^3 - 10.$$

and

$$E_3/\mathbb{F}_{17} : y^2 = x^3 + 2x + 5.$$

(a) Check that

$$f : (x, y) \mapsto ((x^3 + 4)/x^2, (x^3y - 8y)/x^3)$$

defines a map $E_1 \to E_2$.

(b) Detemine the kernel of f.

(c) What is the degree of f?

(d) Calculate the points in the preimage of $(3, 0)$ under f.

(e) Compute the number of points on $E_1(\mathbb{F}_{17}), E_2(\mathbb{F}_{17})$, and $E_3(\mathbb{F}_{17})$.

(f) Compute $j(E_1), j(E_2)$, and $j(E_3)$.

(g) Show that E_1 and E_2 are not isomorphic over $\mathbb{F}_{17}$ but that they are isomorphic over $\mathbb{F}_{17^2}$.

(h) Check that

$$g : (x, y) \mapsto ((x^2 + x + 3)/(x + 1), (x^2y + 2xy + 15y)/(x^2 + 2x + 1))$$

defines a map $E_1 \to E_3$.

(i) Determinne the kernel of g.

(j) What is the degree of g?