Cryptography, exercise sheet 2 for 12 Sep 2022

1. Show that
$$(x, y) + (-x, y) = (0, 1)$$
on a twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$.
Note: We showed this for Edwards curves, show it for twisted Edwaresd curves. The main thing you need to show is that the resulting y-coordinate equals 1.

2. Show that the following correctly computes doubling
$$2(x, y) = \Big(2xy/(ax^2 + y^2), (y^2 - ax^2)/(2 - ax^2 - y^2)\Big)$$
on a twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$.

3. Find all points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Show how you can use symmetries in the curve equation. Do not solve this exercise by brute force over all pairs x, y.

4. Let $h_1 : \{0,1\}^n \times \{0,1\}^{\ell(n)} \to \{0,1\}^n$ and $h_2 : \{0,1\}^n \times \{0,1\}^{\ell(n)} \to \{0,1\}^n$ be hash functions.
Is the following claim true or false? Either present a proof by giving a reduction as in the lecture or a counter example.

   Claim: The combined hash function $H : \{0,1\}^{2n} \times \{0,1\}^{\ell(n)} \to \{0,1\}^{2n}$, $(\langle k_1, k_2\rangle, m) \mapsto h_1(k_1, m)||h_2(k_2, m)$ is collision resistant if at least one of h_1 and h_2 is collision resistant. Here $||$ indicates concatenation, i.e., putting the values one after the other.

5. Explain to one of your team mates or one of the TAs the hash collision conundrum that one cannot define a formal notion of security for fixed hash functions (as opposed to members of a family), see page 4 of hash III.

6. **Multi-target attacks.** Sometimes an attacker gets to attack multiple targets at once and is satisfied breaking any *one* of them. For hash functions multi-target preimage attacks are interesting. We speak of a t-target preimage attack if the attacker is given the outputs $h_k(m_1), h_k(m_2), \ldots, h_k(m_t)$ (and k) but not the inputs $m_1, m_2, \ldots, m_t$ of a hash function $h : \{0,1\}^n \times \{0,1\}^{\ell(n)} \to \{0,1\}^n$ and has the goal of finding a pair (i, x) such that $h_k(x) = h_k(m_i)$.

   (a) Show that a t-target preimage attack A succeeding with probability p can be turned into a 1-target preimage attack, i.e., a regular preimage attack, taking the same time as A and succeeding with probability p/t.
   Note that you need to ensure that the inputs to A are properly distributed and that you have no influence over which i the algorithm picks.

   (b) The algorithm you just developed is actually also a reduction. What did you prove with that algorithm (In terms of property X implies property Y)?

   (c) Find an attack that takes time $2^n/t$ to succeed in finding one (i, x) with high probability.