Cryptography, exercise sheet 4 for 28 Sep 2021

We will work through these exercises on wonder.me; you can find the URL for the room in the Canvas announcement and in Zulip chat under the topic "Wonder session" in the "general" stream. These are exercises to challenge your understanding of the lectures you have watched already, in particular lectures I – V about hash functions and lectures X and XI about ECC.
These are not for homework.

You can call one of us over by choosing "invite to circle". Please note, though, that if we are in another circle busy talking we will not come right away and invitations expire quickly. So pick one of us who is in the TA corner, thus not occupied.

1. In the situation of a parallel rho attack on a hash function, two walks have reached the same distinguished point D. Assume that walk 1 started from W_0 and took 15 steps to reach D while the walk 2 started from W_0' and reached D after 12 steps.
   Explain under which conditions this finds a collision and how to compute the colliding inputs.

2. 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.

3. 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.

4. **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.

5. For the Schnorr identification scheme (video ECC XI) the slides state that if Alice can compute valid s_1, s_2 on challenges $h_1 \neq h_2$ for the same fixed r (chosen by her) it

proves that she knows a but also that Bob can compute a from her answers.

Prove both statements

6. Assume that Alice's random-number generator is broken and that she uses the same r to sign messages $m_1 \neq m_2$ using ECDSA. Show how to compute a given the two signatures (R', s_1) and (R', s_2).
7. Explain to one of your team mates or one of the TAs the comment regarding the Schnorr identification scheme: "Consequence 3: Bob does not learn anything about a as he could have produced the transcript $[R', h, s]$ without Alice." from page 2 of ECC XI.