Exercise sheet 3, 24 February 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.

1. Assume that $f(u) = 0$ for a unique n-bit string u. Assume that the amplitude vector inside Grover's algorithm has entry a at the position u where $f(u) = 0$, and has entry b at the other $2^n - 1$ positions. The amplitude vector one iteration, i.e. one pair of Step 1 and Step 2, later then has entry a' at the position u where $f(u) = 0$, and has entry b' at the other $2^n - 1$ positions.

   (a) Find a 2×2 matrix M, depending only on n (not on a and b), such that multiplying the vector $(a \quad b)$ by M gives $(a' \quad b')$.

   (b) Explain how M can be viewed as rotating a scaled version of its input, i.e., determine a scaling factor s so that $(a \quad b \cdot s)M' = (a' \quad b' \cdot s)$ and M' is a rotation matrix.

2. Explain in your own words how the Lamport one-time-signature scheme works.

3. Explain in your own words how the the Winternitz one-time-signature scheme works.

4. Consider the simple version of Lamport's one-time signature scheme where bits of the message (rather than the hash of the message) are signed. Let messages have n bits and assume that Alice has published $2n$ hash values as her public key and knows the matching $2n$ secret bit strings representing her private key. Alice uses this signature system multiple times with the same key. Analyze the following two scenarios for your chances of faking a signature on a message M:

   (a) You get to see signatures on random messages.

   (b) You get to specify messages that Alice signs. You may not ask Alice to sign M in this scenario.

   How many signatures do you need on average in order to construct a signature on M?

   How many signatures do you need on average to be able to sign any message?

   Answer these questions in both scenarios.

5. Consider the simple version of Winternitz' one-time signature scheme where bits of the message (rather than the hash of the message) are signed. A user accidentally uses his Winternitz signature key twice. Explain how an attacker can (typically) use these signatures to create a new signature.

6. Let $H : \{0,1\}^* \to \{0,1\}^{256}$ be a cryptographic hash function. We use H as the hash function inside the Lamport and the Winternitz scheme and also as the hash function to compress messages before signing. For the random elements in the secret key you should assume that they each need 256 bits.

   (a) We use Lamport's one-time signature together with Merkle's tree construction to compress the public key of the one-time signature. To sign $H(m)$ of length 256 we need to have a tree with 256 leaves. Compute the size (in bits) of the public key, the private key, and the signature for this scheme.

   How many hash function computations are needed in signing and how many in verifying?

   (b) We use Winternitz' scheme with parameter $k = 5$, i.e., we process 5 bits at once to sign $H(m)$ of length 256. Compute the size (in bits) of the public key, the private key, and the signature for this scheme.
   Hint: Remember that you also need to sign the checksum component.
   How many hash function computations are needed in signing and how many in verifying?

   (c) Compare the two answers above to using the Winternitz scheme with parameter $k = 8$ (also for $H(m)$ of 256 bits) in terms of the size of keys and signature and also in terms of how many times you need to evaluate H.

7. In the second video it is stated that c for Winternitz decreases if any m_i increases. Explain why this is the case.