Introduction to Cryptology ENEE459E/CMSC498R: Homework 6

Due by beginning of class on 4/5/2018.

1. Generalize the Merkle-Damgard construction for any compression function that compresses by at least one bit. You should refer to a general input length ℓ' and general output length ℓ (with $\ell' > \ell$).

2. Consider defining a MAC by $\mathsf{Mac}_k(m) = H^s(k||m)$ where H is a collision-resistant hash function. Show that this is not a secure MAC when H is constructed via the Merkle-Damgard transform. As usual, assume that the hash key s is publicly known.

3. Assume collision-resistant hash functions exist. Show a construction of a fixed-length hash function (Gen, h) that is *not* collision resistant, but such that the hash function (Gen, H) obtained from the Merkle-Damgard transform to (Gen, h) *is* collision resistant.

4. Given a degree-5 LFSR with output sequence $1, 0, 0, 0, 0, 1, 0, 1, 1, 1$ (where the output in time step 1 is on the left and the output in time step 10 is on the right). Determine the initial state and feedback coefficients of the LFSR.