CSCI 5440: Cryptography — Homework 1
The Chinese University of Hong Kong, Fall 2020 — due Tuesday September 29

Please list your collaborators and provide any references that you may have used in your solutions. Submit your homework here by Tuesday September 29.

Question 1

Consider the following candidate secret sharing algorithms for a 1-bit secret (0 or 1) and $n = 9$ parties. Does it yield a (perfectly) secure t-threshold secret sharing scheme for a suitable value of t? If yes, say which t, describe the reconstruction algorithm, and give a proof of security. If no, prove that security or reconstruction fails for all t.

(a) To share a 0 send a distinct random number between 1 and 9 to each party. To share a 1 send the same random number between 1 and 9 to each party.

(b) To share a 0 send 5 zeros and 4 ones in a random order. To share a 1 do the opposite.

(c) To share $b \in \{0, 1\}$ send the number $bi + r \bmod 10$ to party $i \in \{1, \dots, 9\}$, where r is a random number between 0 and 9.

Question 2

Let (Enc, Dec) be a (deterministic) encryption scheme with key length k and message length m. Suppose that $Enc(K, M)$ and $Enc(K, M')$ are strictly less than 1/2-statistically close for every two messages M, M'.

(a) Show that $Enc(K, M')$ is a possible encryption of M with probability more than 1/2.

(b) Fix a message M. Show that there exists a key K for which $Enc(K, M')$ is a possible encryption of M for more than half the messages M'.

(c) Show that if $m > k$ then (Enc, Dec) is not an encryption scheme.

Question 3

Let F_K be a pseudorandom function. Are these functions also pseudorandom? Assume the key length, input length, and output length are all equal to the security parameter k.

(a) The function $F'_K(x) = F_K(x) + F_K(\ell(x))$, where $\ell(x)$ is the lexicographic successor of x if $x \neq 1^n$ and 0^n if $x = 1^n$ (e.g., $\ell(\texttt{010}) = \texttt{011}, \ell(\texttt{011}) = \texttt{100}, \ell(\texttt{111}) = \texttt{000}$).

(b) The function $F'_{K,K'}(x, y) = F_K(x) + F_{K'}(y)$, where K and K' are independent.

(c) **(Optional)** The function $F'_K(x) = F_K(x + K)$.

If you answer yes, you need to give a proof that F' is pseudorandom if F is, namely prove that if F' has an efficient distinguisher so does F. Try to work out the best parameters you can.
If you answer no, you need to give a pair of functions F, F' such that F is pseudorandom but F' is not (assuming pseudorandom functions exist).

Question 4

In our setup of private-key encryption we assumed that Alice and Bob share identical copies of the random key. Now suppose that Alice's and Bob's copies of the key are noisy. Specifically, the keys K_A, K_B are elements of the group $\mathbb{Z}_{2^k}$ (i.e., integers modulo 2^k) that are individually uniformly distributed such that the difference $K_A - K_B$ is in the range from $-2^b + 1$ to 2^b modulo 2^k (where $b < k$).

(a) Give a definition of a noisy key encryption scheme.

(b) Show that if the message length is less than $k - b$ then there exists a perfectly secure noisy key encryption scheme.

(c) Show that if the message length is $k - b$ or more then perfect security is no longer possible. Show how to construct a message-simulatable (computationally secure) scheme assuming the existence of a pseudorandom generator. Provide a proof of security.