CS4236 Assignment 3

October 7, 2022

5 assignment questions, due 5pm 21st October - rules as before

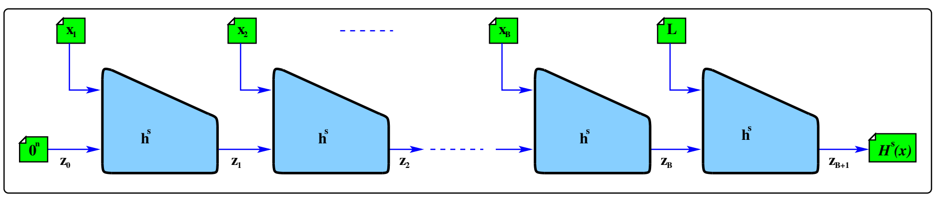
1. On page 188 is a description of the $\text{Hiding}_{\mathcal{A},\Pi}(n)$ experiment/game for a commitment scheme. Use the definition (from class) of the scheme $\Pi(n) = (\text{Setup}(1^n), \text{Commit}(a), \text{Open}(c_a))$, where $c_a \leftarrow \text{Commit}(a)$ creates the commitment, and $a \leftarrow \text{Open}(c)$ opens it. Draw the experiment/game using the same shapes and ideas as used in the game descriptions in class. Provide a formal definition of the hiding property. (4 marks)

2. Assume that $h_1 : \{0,1\}^{2\times n} \to \{0,1\}^n$ is a collision resistant compression function. This is used to define a new compression function with an extra bit b concatenated to x:

$$h_2(x + b) \stackrel{\text{def}}{=} \begin{cases} b = 1 & \to \quad b + h_1(x) \\ b = 0 & \to \quad b^{n+1} \end{cases}$$

Is $h_2 : \{0,1\}^{2\times n+1} \to \{0,1\}^{n+1}$ also collision resistant? Show your reasoning. (2 marks)

3. Given a collision resistant hash function $\mathcal{H}(x) \stackrel{\text{def}}{=} \mathcal{H}_1(\mathcal{H}_1(x))$. Prove that $\mathcal{H}_1$ is collision resistant. (4 marks)



4. The above diagram shows the Merkle Damgård construction to construct collision resistant hashes over longer messages out of compression functions. We write the final hash as $\mathcal{H}^s(x) = Z_{B+1} = h^s(Z_B + L)$. Consider the alternative final hash $\mathcal{H}^s_1(x) = Z_B + L$. Is this still collision resistant? (4 marks)

5. (Similar to the situation described in the first paragraphs of 5.6.2, but without a Merkle tree). In a scheme/system, clients upload files to a server. Later, when a client retrieves a file, it wants a "fingerprint" δ-guarantee that it is the original, unmodified file. The signature is $\Pi(n) = (\text{Put}(x_i), \text{Get}(i), \text{Vrfy}(i, x_i, \delta))$, where $\langle x_i, \delta \rangle \leftarrow \text{Get}(i)$ returns the file and a fingerprint, and $\text{ok} \leftarrow \text{Vrfy}(i, x_i, \delta)$ returns 1/0 if the fingerprint matches/does-not-match the file.

(a) Describe an experiment/game which could be used to define the security of this system - i.e. that an adversary cannot verify $\text{Vrfy}(i, x, \delta)$ unless $x = x_i$. (2 marks)

(b) Formally define the property exposed in the above game. (Π is *secure* if ... for all ...) (2 marks)

(c) Construct a "fingerprint" server, and explain why you think it has the "*secure*" property. (2 marks)