Security Models – Part Security proofs [J-L. Roch]

Important: Duration: 1h30..

- *All exercises are independent.*
- *Your answers have to be short but clearly and cleanly argued or commented.*
- *All hand written documents and handouts are allowed.*

Exercise 1 (Common for M2P SCCI and M2R SECR)
Entropy and unconditional security (points: M2P SCCI 30% – M2R SECR 30%)
Let k be a key of length n uniformly chosen in $\{0,1\}^n$; let (E_k, D_k) be an encryption scheme for messages of length m:

$$\forall k \in \{0,1\}^n, \forall x \in \{0,1\}^m : \quad D_k(E_k(x)) = x.$$

Besides, let U_n denote the uniform distribution over $\{0,1\}^n$.

1. In this question only, $n = m$ and $E_k = E_k^{OTP}$: $E_k^{OTP}(x) = x \oplus k$ where $\oplus$ denotes the bitwise XOR. What is $D_k^{OTP}(x)$?
   For any $x, x' \in \{0,1\}^m$, show that the distribution $E_{U_n}^{OTP}(x)$ is the same as $E_{U_n}^{OTP}(x')$.
2. For any (E_k, D_k): if $n < m$, show that there exist two messages $x, x' \in \{0,1\}^m$ such that $E_{U_n}(x)$ is not the same distribution as $E_{U_n}(x')$.
3. If $n \geq m$, we consider (E_k, D_k) such that $\forall x, x'$: $E_{U_n}(x)$ is the same distribution as $E_{U_n}(x')$. Show that E is then unconditionally secure *(hint: use Bayes theorem)*.

Exercise 2 (Only M2P SCCI)
Hashing and reduction (points: M2P SCCI 30%)
Let E_k be a symmetric block cipher algorithm: the key length is $2m$ bits and the block length is m bits. It is assumed impossible to compute $(k, x) \neq (k', x')$ such that $E_k(x) = E_{k'}(x')$.
Let $M = [M_1 || \dots || M_n]$ a message where each block M_i has exactly m bits.
The digest $H(M)$ of M is defined by:

- $H_0 = IV$ a fixed initial value;
- for $i = 1 \dots n$: $H_i = E_{H_{i-1}||M_i}(H_{i-1})$;
- then $H(M) = H_n$.

Questions:

1. Prove that H is resistant to collision.
2. Generalize to define the digest of a message M of arbitrary size (that may not be multiple of m).

Exercise 3 (Common for M2P SCCI and M2R SECR)
Zero-knowledge protocol (points: M2P SCCI 40% – M2R SECR 40%)
A Hamiltonian circuit (or Hamiltonian cycle) is a cycle in an undirected graph that visits each vertex exactly once and also returns to the starting vertex. Determining whether such a cycle exists in a graph is the Hamiltonian circuit problem, which is NP-complete. Consider the following interactive protocol (due to M. Blum) : initially the input graph G with n vertices is known by both the prover and the verifier.
The protocol uses a one-way function $f : \{0,1\}^n \to \{0,1\}^+$.

Moreover, the prover gets in secret an Hamiltonian cycle of G.

- *Prover's first message.* The prover chooses a random permutation π on the vertices of G. Let H be the graph G permuted by π and let M be the adjacency matrix of H: i.e. (i,j) is in edge in G iff $(\pi(i), \pi(j))$ is an edge in H, so $M_{\pi(i),\pi(j)} = 1$.
  For every $1 \leq i,j \leq n$, the prover:
  - chooses two random vectors $x^{(i,j)}$ and $r^{(i,j)}$ in $\{0,1\}^n$;
  - computes the scalar product $s_{i,j}$ of $x^{(i,j)}$ and $r^{(i,j)}$, i.e. $s_{i,j} = \left(\sum_{k=1}^{n} x_k^{(i,j)}.r_k^{(i,j)}\right) \mod 2$;
  - computes $y^{(i,j)} = f(x^{(i,j)})$ and $z_{i,j} = s_{i,j} \oplus M_{i,j}$;
  - and sends to the verifier: $r^{(i,j)}$, $y^{(i,j)}$ and $z_{i,j}$.
- *Verifier's first message.* The verifier chooses a random bit $b \in \{0,1\}$ and sends b to the prover.
- *Prover's second message.*
  If $b = 0$, the prover sends to the verifier π, M, and $x^{(i,j)}$ for $1 \leq i,j \leq n$.
  If $b = 1$, the prover computes the permuted version C' of the cycle C: for every edge (i,j) in C, C' contains the edge $(\pi(i), \pi(j))$. The prover sends C' to the verifier; moreover, for every $(i,j) \in C'$, it sends $x^{(i,j)}$ to the verifier (but only for those $(i,j) \in C'$).
- *Verifier's check.*
  If $b = 0$, the verifier checks that the two messages of the prover are consistent.
  If $b = 1$, the verifier checks that C' is an Hamiltonian cycle for H: it checks that the two messages of the prover are consistent, and that $M_{i,j} = 1$ for all $(i,j) \in C'$.
  The verifier accepts if and only if theses checks succeed.

Questions:

1. Explicit briefly the operations performed by the verifier during the check.
2. Verify that this interactive protocol runs in polynomial time.
3. Prove the completeness of this protocol.
4. Prove the soundness of this protocol with error probability $\frac{1}{2}$.
5. Prove that this protocol is zero-knowledge.
6. Briefly define an authentication protocol with error probability $< 2^{-400}$ based on this protocol.

Exercise 4 (Only M2R SCCI)
One-way function (points: M2R SECR 30%)
Let $(M_i)_{i\in\mathbb{N}}$ denote the sequence of all deterministic Turing machines (or equivalently all deterministic algorithms). For $x \in \{0,1\}^+$, we define $M_i^t(x)$ by:

- if M_i performs at most t computational steps on input x, then $M_i^t(x)$ is the output of M_i on input x;
- else $M_i^t(x) = 0^{|x|}$ (i.e. the bit O repeated $|x|$ times).

The Levin's universal function $f_U : \{0,1\}^+ \to \{0,1\}^+$ is defined by:

- treat the n input bits as a list $x_1, \ldots, x_{\log n}$ of blocks of $n/\log n$ bits each;
- output the sequence of $\log n$ results: $M_1^{n^2}(x_1), \ldots, M_{\log n}^{n^2}(x_{\log n})$.

Questions:

1. Justify that f_U can be computed in polynomial time.
2. In this question, we assume that M_1 implements a one-way function. Moreover, we assume that, for any input of n bits, M_1 uses at most n^2 computational steps and outputs exactly n bits. Show that f_U is a one-way function (hint: explicit a reduction).
3. Assume there exists a function g resistant to pre-image such that, for an input x of n bits, $g(x)$ is computed in time at most n^c (and thus has at most n^c bits).
For $x \in \{0,1\}^n$, let $L_c(x)$ denote the $\lfloor n^{1/c} \rfloor$ first bits of x and $H_c(x)$ the remainder bits: $x = L_c(x)||H_c(x)$. Define $g'(x) = g(L_c(x))$.
Show that g' is resistant to pre-image and can be computed in time $O(|x|)$.
4. Show that f_U is one-way if and only if there exists a one-way function.