Cryptography—Homework 1*

Sapienza University of Rome
Master Degree in Computer Science
Master Degree in Cybersecurity
Master Degree in Mathematics

Daniele Venturi

Due Date: November 16, 2018

1 Perfect Secrecy — 20 Points

Let $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ be a SKE scheme with key space $\mathcal{K}$, message space $\mathcal{M}$, and ciphertext space $\mathcal{C}$. Consider the following variant of perfect secrecy: For all unbounded adversaries $\mathcal{A}$, we have that

$$\Pr\left[\mathbf{Game}^{\mathrm{eav}}_{\Pi,\mathcal{A}} = 1\right] = 1/2,$$

where $\mathbf{Game}^{\mathrm{eav}}_{\Pi,\mathcal{A}}$ is defined as follows:

$\underline{\mathbf{Game}^{\mathrm{eav}}_{\Pi,\mathcal{A}}}$:

1. The challenger picks $k \leftarrow\!\!\$\ \mathcal{K}$ and $b \leftarrow\!\!\$\ \{0,1\}$.
2. The adversary chooses $(m_0, m_1) \in \mathcal{M}^2$.
3. The challenger computes $c = \mathsf{Enc}(k, m_b)$ and gives c to the adversary.
4. The adversary chooses a bit b', and the game outputs 1 iff $b' = b$.

Prove that the above definition is equivalent to the notion of perfect secrecy we considered in class. (This means that the above formulation implies the one we gave in class, and viceversa.)
Hint: Use the following definition of perfect secrecy: $\forall m_0, m_1 \in \mathcal{M}$, $\forall c \in \mathcal{C}$, $\Pr[\mathsf{Enc}(K, m_0) = c] = \Pr[\mathsf{Enc}(K, m_1) = c]$.

*Some of the exercises are taken from the book *"Introduction to Modern Cryptography"* (second edition), by Jonathan Katz and Yehuda Lindell.

2 Universal Hashing — 20 Points

(a) Recall that a family $\mathcal{H} = \{h_s : \mathcal{X} \to \mathcal{Y}\}_{s \in \mathcal{S}}$ of hash functions is called t-wise independent if for all sequences of *distinct* inputs $x_1, \ldots, x_t \in \mathcal{X}$, and for any output sequence $y_1, \ldots, y_t \in \mathcal{Y}$ (not necessarily distinct), we have that:

$$\Pr\left[h_s(x_1) = y_1 \wedge \cdots \wedge h_s(x_t) = y_t : \ s \leftarrow\!\!\$\ \mathcal{S}\right] = \frac{1}{|\mathcal{Y}|^t}.$$

(i) For any $t \geq 2$, show that if $\mathcal{H}$ is t-wise independent, then it is also $(t-1)$-wise independent.

(ii) Let q be a prime. Show that the family $\mathcal{H} = \{h_s : \mathbb{Z}_q \to \mathbb{Z}_q\}_{s \in \mathbb{Z}_q^3}$, defined by

$$h_s(x) := h_{s_0,s_1,s_2}(x) := s_0 + s_1 \cdot x + s_2 \cdot x^2 \bmod q$$

is 3-wise independent.

(b) Say that X is a (k, n)-source if $X \in \{0,1\}^n$, and the min-entropy of X is at least k. Answer the following questions:

(i) Suppose that $\ell = 128$; what is the minimal amount of min-entropy needed in order to obtain statistical error $\varepsilon = 2^{-80}$ when applying the leftover hash lemma? What is the entropy loss?

(ii) Suppose that $k = 238$; what is the maximal amount of uniform randomness that you can obtain with statistical error $\varepsilon = 2^{-80}$ when applying the leftover hash lemma? Explain how to obtain $\ell = 320$ using computational assumptions.

3 One-Way Functions — 25 Points

(a) Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ be a PRG with one-bit stretch. Prove that G is by itself a one-way function.

(b) Let $f : \{0,1\}^n \to \{0,1\}^n$ be a OWF. Consider the function $g : \{0,1\}^{n+\log n} \to \{0,1\}^{n+\log n+1}$ defined by $g(x||j) := (f(x), j, x_j)$, where $x := (x_1, \ldots, x_n)$, and j is interpreted as an integer in $[n]$ (i.e., $|j| = \log n$).

(i) Show that g is a OWF if f is.

(ii) Show that for every $i \in [n']$ there is a PPT algorithm $\mathcal{A}_i$ for which

$$\Pr\left[\mathcal{A}_i(g(x')) = x'_i : \ x' \leftarrow\!\!\$\ \{0,1\}^{n+\log n}\right] \geq \frac{1}{2} + \frac{1}{2n},$$

where $x' = (x_1, \ldots, x_{n'})$.

Note that this exercise shows that it is not possible to claim that every OWF hides at least one specific bit of the input.

4 Pseudorandom Generators — 15 Points

(a) Let $G_1, G_2 : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be two deterministic functions mapping λ bits into $\lambda+\ell$ bits (for $\ell \geq \lambda+1$). You know that at least one of G_1, G_2 is a secure PRG, but you don't know which one. Show how to design a secure PRG $G^* : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda+\ell}$ by combining G_1 and G_2.

(b) Can you improve your construction obtaining a PRG with optimal seed length (i.e., $G^* : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$)?

5 Pseudorandom Functions — 25 Points

(a) Show that no PRF family can be secure against computationally unbounded distinguishers.

(b) Analyze the following candidate PRFs. For each of them, specify whether you think the derived construction is secure or not; in the first case prove your answer, in the second case exhibit a concrete counterexample.

(i) $F_k(x) = G'(k) \oplus x$, where $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ is a PRG, and G' denotes the output of G truncated to λ bits.

(ii) $F_k(x) := F_x(k)$, where $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\ell$ is a PRF.

(iii) $F'_k(x) = F_k(x||0)||F_k(x||1)$, where $x \in \{0,1\}^{n-1}$.

6 Secret-Key Encryption — 20 Points

(a) Recall the CBC mode of operation: Given a message $m = (m_1, \ldots, m_t)$ consisting of t blocks $m_i \in \{0,1\}^n$, and a random key $k \in \{0,1\}^\lambda$, the ciphertext is $c = (c_0, c_1, \ldots, c_n)$ where $c_0 \leftarrow\!\!\$\ \{0,1\}^n$, $c_i = P_k(c_{i-1} \oplus m_i)$ for all $i \in [n]$, and $P : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ is a secure pseudorandom permutation.

In class, we mentioned that CBC mode yields a CPA-secure secret-key encryption scheme. Show that CBC mode is *not* CCA secure.

(b) Consider the following mode of operation (a.k.a. the Output Feedback mode, OFB): Given a message $m = (m_1, \ldots, m_t)$ consisting of t blocks $m_i \in \{0,1\}^n$, and a random key $k \in \{0,1\}^\lambda$, the ciphertext is $c = (r_0, c_1, \ldots, c_t)$ where $r_0 \leftarrow\!\!\$\ \{0,1\}^n$, $r_i = F_k(r_{i-1})$, and $c_i = r_i \oplus m_i$ for all $i \in [t]$, and $F : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^n$ is a secure pseudorandom function.

One can prove that OFB mode yields a CPA-secure secret-key encryption scheme. Show that OFB mode is *not* CCA secure.

7 Message Authentication — 25 Points

(a) Assume a generalization of MACs where a MAC Π consists of a pair of algorithms $(\mathsf{Tag}, \mathsf{Vrfy})$, such that Tag is as defined in class (except that it could be randomized), whereas Vrfy is a deterministic algorithm that takes as input a candidate pair (m, ϕ) and returns a decision bit $d \in \{0,1\}$ (indicating whether ϕ is a valid tag of m). Consider a variant of the game defining UF-CMA security of a MAC $\Pi = (\mathsf{Tag}, \mathsf{Vrfy})$, with key space $\mathcal{K} = \{0,1\}^\lambda$, where the adversary is additionally granted access to a verification oracle $\mathsf{Vrfy}(k, \cdot, \cdot)$.

(i) Make the above definition precise, using the formalism we used in class. Call the new notion "unforgeability under chosen-message and verification attacks" (UF-CMVA).

(ii) Show that whenever a MAC has unique tags (i.e., for every key k there is only one valid tag ϕ for each message m) then UF-CMA implies UF-CMVA.

(iii) Show that if tags are not unique there exists a MAC that satisfies UF-CMA but not UF-CMVA.

(**Hint:** Given an arbitrary MAC $\Pi = (\mathsf{Tag}, \mathsf{Vrfy})$ satisfying UF-CMA construct a contrived MAC $\Pi' = (\mathsf{Tag}', \mathsf{Vrfy}')$ with non-unique tags such that Π' is still UF-CMA but an attacker with access to a verification oracle can leak the entire secret key.)

(b) Recall that in CBC-MAC the tag of a message $m = (m_1, \ldots, m_t) \in (\{0,1\}^n)^t$ is the value $\phi_t \in \{0,1\}^n$ computed using the following recursive equations: $\forall i \in [t], \phi_i = F_k(m_i \oplus \phi_{i-1})$ with $\phi_0 = 0^n$ and where F_k is sampled from a PRF family. Establish whether the following modifications of CBC-MAC are secure or not.

(i) Using CBC-MAC directly for authenticating variable-length messages.

(ii) A variant of CBC-MAC where, each time a tag is computed, a different value ϕ_0 is sampled uniformly at random from $\{0,1\}^n$ and output together with ϕ_t.

(iii) A variant of CBC-MAC where the output consists of all values $\phi_0, \phi_1, \ldots, \phi_t$.