Cryptography—Homework 2

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

Daniele Venturi

Due Date: December 18, 2019

1 Hashing 25 Points

(a) Let $\mathcal{H} = \{H_s : \{0,1\}^{2n} \to \{0,1\}^n\}_{s\in\{0,1\}^\lambda}$ be a family of collision-resistant hash functions compressing $2n$ bits into n bits. Answer the following questions.

(i) Show that $\mathcal{H}$ is a seeded one-way function in the following sense: For all PPT adversaries A there exists a negligible function $\nu : \mathbb{N} \to [0,1]$ such that

$$\Pr\left[H_s(x') = y : \; s \leftarrow \{0,1\}^\lambda; x \leftarrow \{0,1\}^{2n}; y = H_s(x); x' \leftarrow \mathsf{A}(s,y)\right] \leq \nu(n).$$

(ii) What happens in case the set of functions $\mathcal{H}$ is not compressing (i.e., the domain of each function H_s is also $\{0,1\}^n$)? Does collision resistance imply one-wayness in this case?

(b) Let $\mathcal{H} = \{H_s : \{0,1\}^{4n} \to \{0,1\}^{2n}\}_{s\in\{0,1\}^\lambda}$ and $\mathcal{H}' = \{H'_s : \{0,1\}^{2n} \to \{0,1\}^n\}_{s\in\{0,1\}^\lambda}$ be families of collision-resistant hash functions. Analyse the following candidate hash function family compressing $4n$ bits into n bits: $\mathcal{H}^* := \{H^*_{s_1,s_2}\{0,1\}^{4n} \to \{0,1\}^n\}_{s_1,s_2\in\{0,1\}^\lambda}$ such that $H^*_{s_1,s_2}(x) = H'_{s_2}(H_{s_1}(x))$ for $s_1, s_2 \leftarrow\!\!\$\, \{0,1\}^\lambda$.

2 Number Theory 25 Points

(a) Recall that the CDH problem asks to compute g^{ab} given (g, g^a, g^b) for $(\mathbb{G}, g, q) \leftarrow\!\!\$\, \mathsf{GroupGen}(1^\lambda)$ and $a, b \leftarrow\!\!\$\, \mathbb{Z}_q$. Prove that the CDH problem is equivalent to the following problem: Given (g, g^a) compute g^{a^2}, where $(\mathbb{G}, g, q) \leftarrow\!\!\$\, \mathsf{GroupGen}(1^\lambda)$ and $a \leftarrow\!\!\$\, \mathbb{Z}_q$.

(b) Let $f_{g,p} : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ be the function defined by $f_{g,p}(x) := g^x \bmod p$. Under what assumption is $f_{g,p}$ one-way? Prove that the predicate $h(x)$ that returns the least significant bit of x is not hard-core for $f_{g,p}$.

(c) Let N be the product of 5 distinct odd primes. If $y \in \mathbb{Z}_N^*$ is a quadratic residue, how many solutions are there to the equation $x^2 = y \bmod N$?

3 Public-Key Encryption — 30 Points

(a) Show that for any CPA-secure public-key encryption scheme for single-bit messages, the length of the ciphertext must be super-logarithmic in the security parameter.

(b) Let $\Pi = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ be a PKE scheme with message space $\{0,1\}$ (i.e., for encrypting a single bit). Consider the following natural construction of a multi-bit PKE scheme $\Pi' = (\mathsf{KGen}', \mathsf{Enc}', \mathsf{Dec}')$ with message space $\{0,1\}^t$, for some polynomial $t = t(\lambda)$: (i) The key generation stays the same, i.e. $\mathsf{KGen}'(1^\lambda) = \mathsf{KGen}(1^\lambda)$; (ii) Upon input $m = (m[1], \ldots, m[t]) \in \{0,1\}^t$ the encryption algorithm $\mathsf{Enc}'(pk, m)$ outputs a ciphertext $c = (c_1, \ldots, c_t)$ where $c_i \leftarrow\$ \mathsf{Enc}(pk, m[i])$ for all $i \in [t]$; (iii) Upon input a ciphertext $c = (c_1, \ldots, c_t)$ the decryption algorithm $\mathsf{Dec}'(sk, c)$ outputs the same as $(\mathsf{Dec}(sk, c_1), \ldots, \mathsf{Dec}(sk, c_t))$.

(i) Show that if Π is CCA1 secure, so is Π'.

(ii) Show that, even if Π is CCA2 secure, Π' is not CCA2 secure.

(c) Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let $\mathbb{G}$ be the group of squares modulo p (so $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of $\mathbb{G}$. The private key is $(\mathbb{G}, g, q, x)$ and the public key is $(\mathbb{G}, g, q, h)$, where $h = g^x$ and $x \in \mathbb{Z}_q$ is chosen uniformly. To encrypt a message $m \in \mathbb{Z}_q$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 := g^r \bmod p$ and $c_2 := h^r + m \bmod p$, and let the ciphertext be (c_1, c_2). Is this scheme CPA-secure? Prove your answer.

4 Signature Schemes — 20 Points

(a) Consider a weaker variant of UF-CMA in which the attacker receives (pk, m^*) at the beginning of the experiment, where the message m^* is uniformly random over $\mathbb{Z}_N^*$, and thus it has to forge on m^* after possibly seeing polynomially-many signatures σ_i on uniformly random messages $m_i \leftarrow\$ \mathbb{Z}_N^*$ chosen by the challenger. Call this notion random-message unforgeability under random-message attacks (RUF-RMA).

Formalize the above security notion, and prove that UF-CMA implies RUF-RMA but not viceversa.

(b) Recall the textbook-version of RSA signatures.

$\mathsf{KGen}(1^\lambda)$: Run $(N, e, d) \leftarrow_\$ \mathsf{GenModulus}(1^\lambda)$, and let $pk = (e, N)$ and $sk = (N, d)$.

$\mathsf{Sign}(sk, m)$: Output $\sigma = m^d \bmod N$.

$\mathsf{Vrfy}(pk, m, \sigma)$: Output 1 if and only if $\sigma^e \equiv m \bmod N$.

Prove that the above signature scheme $\Pi = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ satisfies RUF-RMA under the RSA assumption.

5 Actively Secure ID Schemes 30 Points

Let $\Pi = (\mathsf{KGen}, \mathsf{P}, \mathsf{V})$ be an ID scheme. Informally, an ID scheme is actively secure if no efficient adversary A (given just the public key pk) can make V accept, even after A participates maliciously in poly-many interactions with P (where the prover is given both the public key pk and the secret key sk). More formally, we say that Π satisfies active security if for all PPT adversaries A there is a negligible function $\nu : \mathbb{N} \to [0, 1]$ such that

$$\Pr\left[\mathbf{Game}^{\mathsf{mal\text{-}id}}_{\Pi,\mathsf{A}}(\lambda) = 1\right] \leq \nu(\lambda),$$

where the game $\mathbf{Game}^{\mathsf{mal\text{-}id}}_{\Pi,\mathsf{A}}(\lambda)$ is defined as follows:

- The challenger runs $(pk, sk) \leftarrow_\$ \mathsf{KGen}(1^\lambda)$, and returns pk to A.
- Let $q(\lambda) \in \text{poly}(\lambda)$ be a polynomial. For each $i \in [q]$, the adversary can run the protocol Π with the challenger (where the challenger plays the prover and the adversary plays the malicious verifier), obtaining transcripts $\tau_i \leftarrow_\$ (\mathsf{P}(pk, sk) \rightleftarrows \mathsf{A}(pk))$.
- Finally, the adversary tries to impersonate the prover in an execution of the protocol with the challenger (where now the challenger plays the honest verifier), yielding a transcript $\tau^* \leftarrow_\$ (\mathsf{A}(pk) \rightleftarrows \mathsf{V}(pk))$.
- The game outputs 1 if and only if the transcript τ^* is accepting, i.e. $\mathsf{V}(pk, \tau^*) = 1$.

Answer the following questions.

(a) Prove that passive security is strictly weaker than active security. Namely, show that every ID scheme Π that is actively secure is also passively secure, whereas there exists a (possibly contrived) ID scheme Π_{bad} that is passively secure but not actively secure.

(b) Let $\Pi' = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme, with message space $\mathcal{M}$. Prove that if Π' is UF-CMA, the following ID scheme $\Pi = (\mathsf{KGen}, \mathsf{P}, \mathsf{V})$ (based on Π') achieves active security:

$\mathsf{P}(pk, sk) \rightleftarrows \mathsf{V}(pk)$: The verifier picks random $m \leftarrow_\$ \mathcal{M}$, and forwards m to the prover. The prover replies with $\sigma \leftarrow_\$ \mathsf{Sign}(sk, m)$, and finally the verifier accepts if and only if $\mathsf{Vrfy}(pk, m, \sigma) = 1$.

(c) Is the above protocol honest-verifier zero-knowledge? Prove your answer.