Advanced Cryptography — Final Exam

Serge Vaudenay

30.6.2021

- duration: 3h
- any document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade

1 Encryption Security with a Ciphertext Checking Oracle

We consider the following One-Way under Validity Checking Attack (OW-VCA) game. The advantage of the adversary is the probability it returns 1.

Game $\Gamma^{\mathcal{A}}(1^s)$:
1: $\mathsf{Gen}(1^s) \to \mathsf{pk}, \mathsf{sk}$
2: pick $\mathsf{pt}^* \in \mathcal{M}_s$ at random
3: $\mathsf{Enc}(\mathsf{pk}, \mathsf{pt}^*) \to \mathsf{ct}^*$
4: $\mathcal{A}^{\mathsf{VCO}}(\mathsf{pk}, \mathsf{ct}^*) \to z$
5: **return** $1_{z=\mathsf{pt}^*}$

Oracle $\mathsf{VCO}(\mathsf{ct})$
6: $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to x$
7: **return** $1_{x \neq \perp}$

Where s is the security parameter, $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a public-key cryptosystem, $\mathcal{M}_s$ is the plaintext domain, and $\perp$ is the special output of Dec indicating that decryption failed.

Q.1 Is PKCS#1 v1.5 secure with respect to this notion?

Q.2 Propose a definition of KR-VCA security whose goal is key recovery.

Q.3 We recall the Regev cryptosystem over the plaintext domain $\mathcal{M} = \{0, 1\}$.
Gen selects a prime number p, integers m and n, a parameter $\sigma \ll \frac{p}{m}$. Then, it selects a secret $\mathsf{sk} \in \mathbf{Z}_p^n$ and a public key $\mathsf{pk} = (A, b)$ satisfying $b = A \times \mathsf{sk} + e \bmod p$, where $A \in \mathbf{Z}_p^{m \times n}$ is a $m \times n$ matrix and $e \in \mathbf{Z}_p^m$ is an error vector which is selected as follows: for each component i, we sample a real number with normal distribution with mean 0 and standard deviation σ and take e_i as its nearest integer.
$\mathsf{Enc}(\mathsf{pk}, \mathsf{pt})$ picks a vector $v \in \{0, 1\}^m$ at random, $c_1 = v^t \times A \bmod p$, $c_2 = \mathsf{pt} \times \left\lfloor \frac{p}{2} \right\rfloor + v^t b \bmod p$, and returns $\mathsf{ct} = (c_1, c_2)$.
$\mathsf{Dec}(\mathsf{sk}, (c_1, c_2))$ computes $d = c_2 - c_1 \times \mathsf{sk} \bmod p$ then pt' such that $d - \mathsf{pt}' \times \left\lfloor \frac{p}{2} \right\rfloor$ is congruent to an integer in the $[-\frac{p}{4}, +\frac{p}{4}]$ interval modulo p.
Prove that the cryptosystem is correct.

Q.4 Make a successful KR-CCA attack on the Regev cryptosystem.

Q.5 We define a cryptosystem over a domain $\mathcal{M}_s$ as follows: Gen is like in the Regev cryptosystem, Enc first computes $x = (\mathsf{pt}, H(\mathsf{pt}))$ using a hash function, then encrypt each of the n bits of x using the Regev cryptosystem to obtain $\mathsf{ct} = \mathsf{ct}_1, \ldots, \mathsf{ct}_n$. Dec decrypts the n ciphertexts to obtain n bits x' which are parsed into $x' = (\mathsf{pt}', h')$. If $h' = H(\mathsf{pt}')$, then pt' is returned. Otherwise, $\perp$ is returned.
Prove that this cryptosystem is not KR-VCA secure.

2 Optimal Resistance to Linear Cryptanalysis Modulo 2

Let n be an integer. We consider $X_1, \ldots, X_n$ i.i.d. random variables which are uniform over $\mathbf{Z}_4$. We consider Y independent from $X_1, \ldots, X_n$ and uniformly distributed in $\{0, 1\}$. We let $X_{n+1} = Y + X_1 + \cdots + X_n \bmod 4$. Finally, $X = (X_1, \ldots, X_{n+1}) \in \mathbf{Z}_4^{n+1}$. We write X as a bitstring of length $2n + 2$ by concatenating the binary representation of the X_i over two bits. We denote the bits $X[1], \ldots, X[2n+2]$. Hence, $X_1 = 2X[1]+X[2]$, $X_2 = 2X[3]+X[4]$, etc. We recall that for a random variable B, we have $\mathsf{LP}(B) = \left(E((-1)^B)\right)^2$.

The goal of the exercise is to show that although for every balanced linear function $x \mapsto a \cdot x$ from $\mathbf{Z}_2^{2n+2}$ to $\mathbf{Z}_2$, the LP bias is very small, there exists a balanced Boolean function $x \mapsto f(x)$ whose LP bias is huge.

Q.1 Let B be the most significant bit of $X_{n+1} - X_1 - \cdots - X_n \bmod 4$.
Compute $\mathsf{LP}(B)$.

Q.2 Let a be a nonzero binary mask over $2n + 2$ bits such that $a[2n + 1] = 0$.
Prove that $\mathsf{LP}(a \cdot X) = 0$.

Q.3 Let a be a binary mask over $2n + 2$ bits such that $a[2n + 1] = 1$ and $a[i] = 0$ for some odd index i.
Prove that $\mathsf{LP}(a \cdot X) = 0$.
HINT: $X[2n + 1] = \sum_j X[2j - 1] + \sum_{j<j'} X[2j]X[2j'] + \sum_j X[2j]Y$ where j and j' go from 1 to n.

Q.4 Let a be a binary mask over $2n + 2$ bits such that $a[i] = 1$ for every odd index i.
Prove that $\mathsf{LP}(a \cdot X) = 2^{-n-1}$ for n odd.
HINT: For every n, $\left(\sum_{w=0}^{n-1} \binom{n}{w} (-1)^{\frac{w(w-1)}{2}}\right)^2 = 2^n \left(1 + \sin \frac{n\pi}{2}\right)$.

3 MPC-in-the-Head

Let R be a relation over bitstrings x and w defining an NP language. We assume a multiparty computation (MPC) with two participants A and B such that

- A and B have as public common input x;
- A and B have respective private inputs w_A and w_B;
- A and B have as final common output $R(x, w_A \oplus w_B)$;
- a malicious participant learns nothing about the private input of honest participants.

We let $\mathcal{U}(x, w_U; r_U)$ be the protocol run by $U \in \{A, B\}$ and $\mathsf{Run}(x, \mathcal{A}(w_A; r_A), \mathcal{B}(w_B; r_B))$ be the interaction. We will use a commitment scheme Commit.

We define a Σ protocol over the challenge set $\{A, B\}$ as follows.

- $\mathcal{P}(x, w)$ first flips w_A, r_A, r_B, sets $w_B = w_A \oplus w$, then simulates the interaction $\mathsf{Run}(x, \mathcal{A}(w_A; r_A), \mathcal{B}(w_B; r_B))$. It computes the transcript t (i.e. x and the list of exchanged messages) of the protocol.
- It flips k_A and k_B and computes $c_A = \mathsf{Commit}(w_A, r_A; k_A)$ and $c_B = \mathsf{Commit}(w_B, r_B; k_B)$.
- The message $a = (t, c_A, c_B)$ is sent to $\mathcal{V}$.
- $\mathcal{V}$ flips a challenge $e \in \{A, B\}$ and sends it to $\mathcal{P}$.
- $\mathcal{P}$ sends $z = (w_e, r_e, k_e)$.
- $\mathcal{V}$ makes a final verification.

Q.1 Describe the final verification of $\mathcal{V}$ and prove that the Σ protocol is correct.
Q.2 Define an extractor and prove it is correct.
Q.3 How would we define a simulator? (An informal argument is fine for this question.)