Advanced Cryptography — Final Exam

Serge Vaudenay

3.8.2019

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

1 Security of Key Agreement

We consider a key agreement scheme defined by

- one PPT algorithm $\mathsf{setup}(1^s) \to \mathsf{pp}$ which generates public parameters pp;
- two probabilistic polynomially bounded interactive machines A and B with input pp and producing a secret output K (denoted by K_A for A and by K_B for B).

Correctness implies that the following game outputs 1 with probability 1.

$\mathsf{setup}(1^s) \to \mathsf{pp}$
make $A(\mathsf{pp})$ and $B(\mathsf{pp})$ interact with each other and output K_A and K_B
output $1_{K_A=K_B}$

Q.1 Give a formal definition for the security against key recovery under passive attacks.
Q.2 Formalize how to define the Diffie-Hellman protocol under this setting.
Q.3 Formally prove that the Diffie-Hellman protocol is secure in the sense of the previous question if and only if the computational Diffie-Hellman problem is hard.
Q.4 We now consider security against Alice's key recovery under active attacks as defined by the following game:

$\mathsf{setup}(1^s) \to \mathsf{pp}$
$\mathsf{st}_A \leftarrow \mathsf{pp}$, $\mathsf{finished}_A \leftarrow \mathsf{false}$
$\mathsf{st}_B \leftarrow \mathsf{pp}$, $\mathsf{finished}_B \leftarrow \mathsf{false}$
run $\mathcal{A}^{\mathsf{OA},\mathsf{OB}}(\mathsf{pp}) \to K$
output $1_{K=K_A \text{ and } \mathsf{finished}_A}$

$\mathsf{OA}(x)$:
if $\mathsf{finished}_A$ **then return**
$\mathsf{st}_A \leftarrow (\mathsf{st}_A, x)$
run $A(\mathsf{st}_A)$ to get private output st_A and next message y
if y non-final **then return** y
$\mathsf{finished}_A \leftarrow \mathsf{true}$
$K_A \leftarrow \mathsf{st}_A$
return y

And the same for oracle OB. Prove that the Diffie-Hellman protocol is insecure in this sense.

Q.5 Based on some attacks seen in the course, formalize security against key recovery under *active* attacks making $K_A = K_B$. Prove that Diffie-Hellman is secure by assuming that the problem defined by the following game is hard:

$\mathsf{setup}(1^s) \to \mathsf{pp} = (q, g)$
pick $x, y \in \mathbf{Z}_q^*$
$\mathcal{B}(\mathsf{pp}, g^x, g^y) \to (u, v, w)$
return $1_{u^x = v^y = w \text{ and } u,v,w \in \langle g \rangle \text{ and } w \neq 1}$

where g generates $\langle g \rangle$ of order q, with neutral element 1.

2 Advantage Amplification

Let $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ be $2n$ independent Boolean variables. We assume that $X_1, \ldots, X_n$ are identically distributed and that $Y_1, \ldots, Y_n$ are identically distributed. We assume that the statistical distance between the distributions of X_i and Y_j is ε. Given distinguisher, i.e. a Boolean algorithm $\mathcal{A}$ (with unbounded complexity), we define $X = \mathcal{A}(X_1, \ldots, X_n)$ and $Y = \mathcal{A}(Y_1, \ldots, Y_n)$. We are interested in $\mathcal{A}$ which maximizes the statistical distance between the distributions of X and Y. We denote by d the statistical distance and we identify random variables by their distributions when computing distances, by abuse of notation.

Q.1 Prove that $d(X, Y) = d((X_1, \ldots, X_n), (Y_1, \ldots, Y_n))$.

Q.2 Assume that $\Pr[X_i = 1] = 0$.

Q.2a Give the distributions of X_i and Y_j.

Q.2b Compute $d(X, Y)$ in terms of ε and n.

Q.2c Give an asymptotic equivalent of the minimal n such that $d(X, Y) \geq \frac{1}{2}$ in terms of ε, when $\varepsilon \to 0$.

Q.3 Assume now that $\Pr[X_i = 1] = \frac{1}{2}(1 - \varepsilon)$ and $\Pr[Y_i = 1] = \frac{1}{2}(1 + \varepsilon)$.

Q.3a Show that $\mathcal{A}(z_1, \ldots, z_n) = 1_{z_1 + \cdots + z_n < \frac{n}{2}}$ makes $d(X, Y)$ maximal.

Q.3b Given that $\Pr[X_1 + \cdots + X_n < \frac{n}{2}] = \Pr[Y_1 + \cdots + Y_n > \frac{n}{2}]$, prove that for n odd, we have $d(X, Y) = |1 - 2\Pr[X_1 + \cdots + X_n < \frac{n}{2}]|$.

Q.3c Compute the expected value and the variance of $X_1 + \cdots + X_n$.

Q.3d By approximating $X_1 + \cdots + X_n$ to a normal distribution, give an asymptotic equivalent to n so that $d(X, Y)$ is a constant.