Advanced Cryptography — Midterm Exam

Serge Vaudenay

11.4.2024

- duration: 1h45
- 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 Signatures with Malicious Setup

We recall the DSA signature scheme using a hash function H.

- Public parameters setup: set group parameters (p, q, g) such that p and q are large prime numbers, q divides $p-1$, and g has order q in $\mathbf{Z}_p^*$. The group parameters are implicit inputs of other algorithms.
- Key generation: pick a random $x \in \mathbf{Z}_q$ and set $y = g^x \bmod p$. The secret key is x and the public key is y.
- Signature: pick $k \in \mathbf{Z}_q^*$ and set $r = g^k \bmod p \bmod q$ and $s = \frac{H(M)+xr}{k} \bmod q$ where M is the message to be signed. The signature is (r, s).
- Verification: compare r with $g^{\frac{H(M)}{s}} y^{\frac{r}{s}} \bmod p \bmod q$.

Q.1 The above description does not fit the definition of a signature scheme in three algorithms: key generation, signature, verification. Propose a formal definition of a signature scheme which includes the notion of public parameters setup and the notion of correctness.

Q.2 Formally define the notion of unforgeability which captures malicious setup.

Q.3 Imagine that setup is done by a malicious adversary. Show that it is possible to generate some public parameters (p, q, g) which are correct together with a pair of messages (M_0, M_1) such that $M_0 \neq M_1$ and for any public key y and any $\sigma = (r, s)$, if σ is a valid signature of M_0 for y, then σ is a valid signature of M_1 for y as well.

2 Find-then-Guess Security for Deterministic Symmetric Encryption

We consider a symmetric encryption scheme $(\{0,1\}^k, \mathcal{D}, \mathsf{Enc}, \mathsf{Dec})$. (We recall that k depends on an implicit security parameter s; we recall that $\mathcal{D}$ is the set of all bitstrings of length in an admissible set $\mathcal{L}$; we assume the scheme to be variable-length by default;

we assume no nonce; we may assume length-preservation or not.) In this exercise, we assume Enc to be deterministic. We define the Deterministic Find-then-Guess CPA security ($\mathsf{DFG\text{-}CPA}$-security) as the indistinguishability between two games Γ_0 and Γ_1. The scheme is secure if for any PPT 2-stage adversary $(\mathcal{A}_1, \mathcal{A}_2)$, the advantage Adv is negligible. The advantage is $\mathsf{Adv} = \Pr[\Gamma_1 \to 1] - \Pr[\Gamma_0 \to 1]$ with the following games:

Game Γ_b:
1: pick $K \leftarrow \{0,1\}^k$ uniformly at random
2: $S \leftarrow \emptyset$
3: $\mathcal{A}_1^{\mathsf{OEnc}_1} \to (\mathsf{pt}_0, \mathsf{pt}_1, \mathsf{st})$
4: **if** $|\mathsf{pt}_0| \neq |\mathsf{pt}_1|$ **then return** $\perp$
5: **if** $\mathsf{pt}_0 \in S$ or $\mathsf{pt}_1 \in S$ **then return** $\perp$
6: $\mathsf{ct} \leftarrow \mathsf{Enc}(K, \mathsf{pt}_b)$
7: $\mathcal{A}_2^{\mathsf{OEnc}_2}(\mathsf{st}, \mathsf{ct}) \to z$
8: **return** z

Oracle $\mathsf{OEnc}_1(\mathsf{pt})$:
9: add pt in S
10: **return** $\mathsf{Enc}(K, \mathsf{pt})$

Oracle $\mathsf{OEnc}_2(\mathsf{pt})$:
11: **if** $\mathsf{pt} \in \{\mathsf{pt}_0, \mathsf{pt}_1\}$ **then return** $\perp$
12: **return** $\mathsf{Enc}(K, \mathsf{pt})$

Q.1 If we remove line 5 in the definition of the games, prove that no deterministic symmetric encryption is $\mathsf{DFG\text{-}CPA}$-secure.

Q.2 If we remove line 11 in the definition of the games, prove that no deterministic symmetric encryption is $\mathsf{DFG\text{-}CPA}$-secure.

Q.3 Propose an extension to define $\mathsf{DFG\text{-}CPCA}$-security in a way which is not trivially impossible to achieve like in the previous questions.

Q.4 Construct a nonce-less deterministic symmetric encryption scheme which is not length-preserving, which is (presumably) $\mathsf{DFG\text{-}CPA}$-secure, and which is (certainly) not secure against CPA real-or-ideal distinguishers.

Q.5 We assume that $\mathcal{D}$ is finite. Prove that CPA security against decryption implies that $2^{-\ell}$ is negligible, where ℓ is the largest length of an element in $\mathcal{D}$.

Q.6 Prove that CPA security against real-or-ideal distinguishers implies $\mathsf{DFG\text{-}CPA}$-security.

Q.7 Prove that $\mathsf{DFG\text{-}CPA}$-security implies CPA security against decryption attacks, assuming that the $\mathcal{D}$ includes elements of length ℓ such that $2^{-\ell}$ is negligible and that $\mathcal{D}$ is finite.