MTAT.07.003 Cryptology II
Spring 2009 / Exercise Session IX

1. Consider a following message transmission protocol. A sender $\mathcal{P}_1$ knows the public encryption key pk_2 of a receiver $\mathcal{P}_2$ and the receiver $\mathcal{P}_2$ knows the public signing key pk_1 of the sender $\mathcal{P}_1$. To encrypt a message m the sender sk computes $c \leftarrow \mathsf{Enc}_{\mathsf{pk}_2}(m)$, $s \leftarrow \mathsf{Sign}_{\mathsf{sk}_1}(c)$ and sends (c, s) over unreliable channel to $\mathcal{P}_2$. The receiver $\mathcal{P}_2$ first checks the authenticity by computing $\mathsf{Ver}_{\mathsf{pk}_1}(c, s)$ and then decrypts the message $m \leftarrow \mathsf{Dec}_{\mathsf{sk}_2}(c)$.

   (a) What are properties of the encryption and the signing scheme are needed to guarantee secure message transmission? Compute the corresponding security guarantees.

   (b) Show that the message transmission protocol may become insecure if $\mathcal{P}_1$ uses the signing key sk_1 also for some other purposes. Give an explicit attack description under the assumption that the secret key sk_2 can be extracted using chosen message attacks.

   (c) Show that the message transmission protocol can become insecure if $\mathcal{P}_2$ uses sk_2 to decrypt messages of several senders.

   (d) Interpret the results. In which contexts, the this message transmission protocol is useful? When is the traditional construction based on symmetric encryption and authentication primitives better?

   ($\star$) Give a construction of secure message transmission protocol that is still based on signing and asymmetric encryption primitives but is significantly more secure against malicious behaviour.

2. Construct an identification scheme that is based on a signature scheme. Prove that the corresponding identification scheme is secure in the most powerful setting, where the adversary can run several identification protocols concurrently in order to impersonate true signer.

3. Digital signatures are often used in various electronic transaction systems. In the simplest setting, sellers issue a bills for goods that must be signed by a bank before the transaction becomes valid. However, such a setting violates the privacy of buyers as the bank will always know what its clients have bought. The latter is the main motivation for blind-signatures as they allow to hide messages from the signer. More precisely, consider an blind signature scheme, which is based on full domain hash and RSA.

   - A public key is RSA modulus n and a exponent e. The corresponding private exponent d such that $ed = 1 \mod \phi(n)$ is the secret key.
   - To sign a message m, the signer must compute $s = h(m)^d \mod n$.
   - A signature (m, s) is valid if $h(m) = s^e \mod n$.
   - To get a blind signature, a client must compute $h(m)$ and then choose $r \leftarrow_u \mathbb{Z}_n^*$ and sent $\overline{m} = h(m)r^e \mod n$ to the signer. When the signer replies $\overline{s} = \overline{m}^d \mod n$, the client computes $s = \overline{s}r^{-1} \mod n$.

(a) Show that the signature obtained in the blind signing protocol is valid and the signer learns nothing about the message, i.e., we can simulate $\overline{m}$ without seeing m.

(b) Show that the blind signature scheme can be less secure than the underlying RSA signature scheme by providing an explicit attack that works against blind signatures and not for the RSA signature.

(c) Construct a protocol for selling goods over the internet that preserves the privacy of buyers, assures that no client can spend more money than he or she owns and guarantees that sellers get their money.

(d) Is it possible to design a protocol where buyers can anonymously revoke transactions when sellers cheat.

($\star$) Prove that security of a signature scheme can be never proved through a reduction that shows how to extract secret key from an adversary who is successful in deception. More precisely, show that if such a reduction exists then there exists also an attack strategy that extracts a secret key using few signing queries. Why this impossibility result does not conflict with the security proofs in the random oracle model?

4. Let $\mathbb{G} = \langle g \rangle$ be a (t, ε_1)-secure q-element discrete logarithm group. Then the Schnorr signature scheme is defined as follows.

   - A secret key $x \xleftarrow{u} \mathbb{Z}_q$ and the corresponding public key $y \leftarrow g^x$.
   - To sign a message m, generate $r \xleftarrow{u} \mathbb{Z}_q$, compute $\alpha \leftarrow g^r$, $\beta \leftarrow h(m, \alpha)$ and then compute the reply γ of the Schnorr identification protocol. The resulting signature is a triple $s = (\alpha, \beta, \gamma)$.
   - A pair (m, s) is a valid signature if $h(m, \alpha) = \beta$ and $g^\gamma = y^\beta \alpha$.

   Prove that if h is replaced with a random oracle $\mathcal{O}_h(\cdot)$, then the Schnorr signature scheme is $(c \cdot t\varepsilon_1, \frac{\varepsilon_1}{2})$-secure against existential forgeries in the key only attack model for an appropriate constant c provided that the adversary makes only single call to $\mathcal{O}_h(\cdot)$ and that the adversary always controls the validity of the proposed signature.

   (a) Show that an that if an adversary $\mathcal{A}$ succeeds with probability ε, there exists an adversary $\mathcal{B}$ that succeeds with probability ε in the Schnorr identification protocol and has same time complexity.

   (b) Use the theorem about matrix games to estimate the average running-time of a knowledge extractor for the Schnorr protocol and use Markov inequality to find success probability for a strict time bound.

   (c) Note that the previous result holds only for the values of public keys y such that the success probability is large enough. Show that if the average success probability $\mathsf{Adv}^{\mathsf{ent\text{-}auth}}(\mathcal{B}) > \varepsilon$ then the probability of getting a bad key y such that $\varepsilon_y < \frac{\varepsilon}{2}$ is low.

5. Construct a generic signature scheme from the Fiat-Shamir identification protocol. Recall that the Fiat-Shamir protocol works as follows.
   - A secret key $s \xleftarrow{u} \mathbb{Z}_n^*$ and the public key $v \leftarrow s^2 \mod n$.
   - To authenticate, the prover generates $r \xleftarrow{u} \mathbb{Z}_n^*$ and sends $\alpha \leftarrow r^2 \mod n$ to the verifier. The verifier sends $\beta \xleftarrow{u} \{0,1\}$ to the prover who replies $\gamma \leftarrow rs^b \mod n$. The prover succeeds if $\gamma^2 = \alpha v^b \mod n$.

6. Any instantiation of the full domain hash signature scheme defines implicitly a bundle $\mathcal{H} \ltimes \mathcal{F}_{\mathrm{tp}}$ of function families $\mathcal{H}$ and $\mathcal{F}_{\mathrm{tp}}$. Namely, the signature scheme is determined by a tuple of algorithms $(\mathsf{Gen}, \mathrm{Map}, \mathrm{Inv}, \mathrm{Hash})$, where $(\mathsf{Gen}, \mathrm{Map}, \mathrm{Inv})$ determines the collection of trapdoor permutations $\mathcal{F}_{\mathrm{tp}}$ and functions $\mathrm{Inv}_{\mathsf{sk}} : \mathcal{M}_{\mathsf{pk}} \to \mathcal{S}$ and $\mathrm{Hash}_{\mathsf{pk}} : \mathcal{M} \to \mathcal{T}_{\mathsf{pk}}$ have matching input and output domains $\mathcal{T}_{\mathsf{pk}} \subseteq \mathcal{M}_{\mathsf{pk}}$ for every $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$. The corresponding bundle $\mathcal{H} \ltimes \mathcal{F}_{\mathrm{tp}}$ of function families $\mathcal{H}$ and $\mathcal{F}_{\mathrm{tp}}$ is (t, ε)-claw-free if for any t-time adversary $\mathcal{A}$ the following advantage

$$\mathsf{Adv}^{\mathsf{c\text{-}free}}_{\mathcal{F}_{\mathrm{tp}} \ltimes \mathcal{H}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right] \leq \varepsilon$$

where

$$\mathcal{G}^{\mathcal{A}}$$
$$\begin{bmatrix} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\ (m, s) \leftarrow \mathcal{A}(\mathsf{pk}) \\ \textbf{return } [\mathrm{Hash}_{\mathsf{pk}}(m) \stackrel{?}{=} \mathrm{Map}_{\mathsf{pk}}(s)] \end{bmatrix}$$

Prove the following facts about the full domain hash signature scheme.

   (a) The signature scheme is (t, ε)-secure against existential forgeries in the model, where the adversary cannot access the signing oracle, if the bundle $\mathcal{H} \ltimes \mathcal{F}_{\mathrm{tp}}$ is (t, ε)-claw-free.

   (b) Generalise the notion of claw-free bundles so that (t, ε)-security is sufficient for the standard attack model.

7. Consider a full domain hash signature as in the previous exercise. Assume that the hash function family $\mathcal{H}$ is strongly ε_1-regular, i.e., for every key pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$ and the output distribution of $\mathrm{Hash}_{\mathsf{pk}}(m)$ where $m \xleftarrow{u} \mathcal{M}$ and uniform distribution over $\mathcal{M}_{\mathsf{pk}}$ are ε_1-close. Now consider the security against universal forgeries

$$\mathsf{Adv}^{\mathsf{u\text{-}forge}}_{\mathcal{H} \ltimes \mathcal{F}_{\mathrm{tp}}}(\mathcal{A}) = \Pr\left[\mathcal{G}^{\mathcal{A}} = 1\right]$$

where

$$\mathcal{G}^{\mathcal{A}}$$
$$\begin{bmatrix} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen} \\ m \xleftarrow{u} \mathcal{M} \\ s \leftarrow \mathcal{A}(m, \mathsf{pk}) \\ \textbf{return } \mathsf{Ver}_{\mathsf{pk}}(m, s) \end{bmatrix}$$

and prove that (t, ε)-security of trapdoor collection $\mathcal{F}_{\mathrm{tp}}$ is sufficient for security. Generalise the notion of one-wayness so that it is also sufficient against chosen message attacks.