MTAT.07.003 Cryptology II
Spring 2008 / Homework 9

1. Any instantiation of the full domain hash signature scheme defines implicitly a bundle $\mathcal{H} \bowtie \mathcal{F}_{\mathrm{tp}}$ 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 $\mathcal{H} \bowtie \mathcal{F}_{\mathrm{tp}}$ 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

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

where

```
$\mathcal{G}^{\mathcal{A}}$
    $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
    $(m, s) \leftarrow \mathcal{A}(\mathsf{pk})$
    return $[\mathrm{Hash}_{\mathsf{pk}}(m) \overset{?}{=} \mathrm{Map}_{\mathsf{pk}}(s)]$
```

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 $\mathcal{H} \bowtie \mathcal{F}_{\mathrm{tp}}$ is (t, ε)-claw-free.

(b) The bundle $\mathcal{H} \bowtie \mathcal{F}_{\mathrm{tp}}$ can be (t, ε)-claw-free only if $\mathcal{F}_{\mathrm{tp}}$ is (t, ε)-secure collection of trapdoor permutations and $\mathcal{H}$ is (t, ε)-collision resistant.

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

(d) 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

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

where

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

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.

2. Consider a following secure 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) Conclude 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.

3. 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.

4. Sometimes signature schemes are used to prove liveness of a device or a person. For instance, ATM machines normally ask PIN codes several times during long transactions to assure that the person is still present. One possibility too implement such an entity authentication procedure is through the use of one-time signatures. Let g be (t, ε_1)-secure one-way function then the simplified Merkle signature scheme works as follows.

   - Let 2^k be the maximal number of one-time signatures. Then a secret key sk is a tuple of random values $s_{0\ldots0}, \ldots s_{1\ldots1} \xleftarrow[u]{} \mathcal{M}$ and the corresponding public key is a tuple of hash values $g(s_{0\ldots0}), \ldots, g(s_{1\ldots1})$.
   - Each nonce r_i is a one-time signature that proves liveness. A signer releases nonces $s_{0\ldots0}, \ldots, s_{1\ldots1}$ one by one.
   - The ℓth one-time signature s_ℓ is correct if $g(s_\ell)$ is present in pk.

   Large size of a public and private keys is the main drawback of simplified Merkle signature scheme. Hence, the original Merkle signature scheme utilises the several enhancements.

(a) Show that we can use a (t, ε_2)-collision resistant hash function family to compact the public key. Describe the corresponding compaction procedure and the resulting signatures. Prove the security of signature scheme in the standard model with restriction that each signature can be used only once.

Hint: Binary trees provide an optimal hashing scheme.

(b) Show that we can use (t, ε_3)-pseudorandom function family $\mathcal{F}$ to compact also the private key sk. Describe the corresponding scheme and recompute the security guarantees.

Hint: How to stretch randomness in a most optimal way?

(c) Show also that the full Merkle signature scheme can be used to sign up to k-bit messages. Describe the corresponding signature scheme and provide corresponding security guarantees.

($\star$) Note that one-wayness and indistinguishability under chosen message attack are equivalent notions if the message space is $\{0, 1\}$. To be precise, OW-CPA security makes sense for a small message space only if $\mathrm{Map}_{\mathsf{pk}} : \mathcal{M} \to \mathcal{S}$ is a randomised transformation and the corresponding security game is defined as follows

```
$\mathcal{G}^{\mathcal{A}}$
    $\mathsf{pk} \leftarrow \mathsf{Gen}$
    $m_0 \overset{}{\underset{u}{\leftarrow}} \mathcal{M}$
    $y \leftarrow \mathrm{Map}_{\mathsf{pk}}(m_0)$
    $m_1 \leftarrow \mathcal{A}(\mathsf{pk}, y)$
    $\mathsf{return}\ [\exists r : \mathrm{Map}_{\mathsf{pk}}(m_1; r) = y]$
```

Evidently, IND-CPA security implies OW-CPA security for all sizes of message spaces $\mathcal{M}$. Provide a sharp upper and lower bound for the opposite reduction OW-CPA$\Rightarrow$ IND-CPA. Does this result also hold for chosen ciphertext attacks? When are one-wayness and indistinguishability qualitatively equivalent? Can we avoid the decrease in success probability by the increase of running time?

5. Construct a generic two-party signature signature from the Schnorr identification protocol. More precisely, follow the steps described below.

(a) Construct an OR identification scheme where a prover can convince an honest verifier that he or she knows either discrete logarithm of y_1 or y_2. Compute the corresponding soundness guarantees.

Reminder: A protocol is sound if the prover must knows the fixed secret key to pass the verification.

(b) Use Fiat-Shamir transformation to create the corresponding generic signature. What are the corresponding soundness guarantees in the random oracle model?

(c) Show that the corresponding two-party signature allows to implement non-transferable proofs. Namely, assume that $\mathcal{P}_1$ knows the secret key sk_1 and $\mathcal{P}_2$ knows the secret key sk_2. Then $\mathcal{P}_2$ cannot convince any outsider that $\mathcal{P}_1$ signed a document, as $\mathcal{P}_2$ could have signed the document him- or herself. Where could such a primitive be useful?

6. Construct a forward-secure signature scheme from the Fiat-Shamir identification scheme. More precisely, follow the steps given below.

   (a) Decrease the knowledge error of the Fiat-Shamir identification scheme by parallel repetition of ℓ protocols. Compute the corresponding soundness guarantees.

   (b) Use Fiat-Shamir transformation to create the corresponding generic signature. What are the corresponding soundness guarantees in the random oracle model?

   (c) Use a randomly chosen element $s \in \mathbb{Z}_n^*$ to create a sequence of secret keys. Describe how a signer can start to use a new secret key when he or she thinks that the old key is compromised.

($\star$) 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?