ETH Zürich, D-INFK
Spring 2019

Prof. Ueli Maurer
Fabio Banfi
Daniel Jost
Jiamin Zhu

Cryptography Foundations
Exercise 6

6.1 The Lamport One-Time Signature Scheme

Goal: *We explore how to devise a one-time signature scheme based on one-way functions.*

A *one-time signature scheme* is a digital signature scheme for which no feasible adversary can win the signature forgery game for 1 message (according to Definition 3.18) with non-negligible probability. A *one-way function* is a function $f\colon \mathcal{X} \to \mathcal{Y}$ such that one can efficiently compute f but no feasible algorithm has non-negligible success probability in the following *inversion game*:

1. $x \in \mathcal{X}$ is chosen uniformly at random and $y := f(x) \in \mathcal{Y}$ is given to the algorithm.
2. The algorithm outputs a value $x' \in \mathcal{X}$ and wins the game if $f(x') = y$.

Let $f\colon \mathcal{X} \to \mathcal{Y}$ be a function, let the message space be $\mathcal{M} := \{0,1\}^n$ (with $n > 0$), let the signature set be $\mathcal{S} := \mathcal{X}^n$, let the verification-key set be $\mathcal{V} := \mathcal{Y}^{2n}$, and let the signing-key set be $\mathcal{Z} := \mathcal{X}^{2n}$. Devise a one-time signature scheme that is secure if f is one-way. More precisely, show how any adversary for the signature forgery game for 1 message with success probability α can be turned into an algorithm with success probability at least $\frac{\alpha}{2n}$ in the inversion game for f.

6.2 Signature Schemes from Trapdoor One-Way Permutations

Goal: *We learn that the security of TOWP-based signature schemes crucially depends on the strength of the underlying hash-function and that it is possible to prove their security in the* random oracle *model.*

Recall Definition 3.14 of a TOWP, which consists of functions $f\colon \mathcal{X} \times \mathcal{P} \to \mathcal{Y}$ and $g\colon \mathcal{Y} \times \mathcal{T} \to \mathcal{X}$[1], as well as a parameter-trapdoor distribution over $\mathcal{P} \times \mathcal{T}$. Also, consider a hash-function $h\colon \mathcal{M} \to \mathcal{Y}$ mapping a message to the codomain of the TOWP. A signature scheme for messages over $\mathcal{M}$ and signatures over $\mathcal{X}$ can then be defined as

$$\sigma\colon \mathcal{M} \times \mathcal{T} \to \mathcal{X},\ (m,t) \mapsto g(h(m),t),$$

where the trapdoor t corresponds to the signing-key, i.e., $\mathcal{Z} := \mathcal{T}$, and

$$\tau\colon \mathcal{M} \times \mathcal{X} \times \mathcal{P} \to \{0,1\},\ (m,s,p) \mapsto f(s,p) \stackrel{?}{=} h(m),$$

where the parameter p corresponds to the public verification-key, i.e., $\mathcal{V} := \mathcal{P}$, (and the distribution over $\mathcal{P} \times \mathcal{T}$ remains the same as the one of the underlying TOWP).

Recall that for the specific instantiation of the RSA TOWP we have $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n^*$ and $\mathcal{P} = \mathcal{T} = \mathbb{N} \times \mathbb{Z}_{\varphi(n)}$, $f(x,(n,e)) := [m^e \mod n]$, and $g(y,(n,d)) := [y^d \mod n]$. One then obtains the so-called *FDH-RSA signature scheme* by basing the above described scheme on the RSA TOWP and by using an appropriate hash function $h\colon \mathcal{M} \to \mathbb{Z}_n^*$.

a) Show that for the FDH-RSA signature scheme, if $\mathcal{M} = \mathbb{Z}_n^*$ and h is the identity function, it is easy to find a valid pair (m,s) (i.e., an existential forgery), only knowing the public key but no other message-signature pair.

[1] Assume that $\mathcal{X}$ and $\mathcal{Y}$ are finite sets of equal cardinality.

b) Again for the FDH-RSA signature scheme, show that under the same conditions on h as in **a)**, given any message m, it is easy to find a valid signature s for this m if the adversary has access to a signing oracle.

c) In the following, let $h\colon \mathcal{M} \to \mathcal{Y}$ be modeled as a truly random function—a so-called *random oracle*. This actually means that instead of thinking of h as a function with a certain concrete description, we assume that an additional system $\mathbf{H}$ is available in the random experiments that behaves as follows: on input x to the system $\mathbf{H}$, if x has not been queried before, a value y from the output domain is chosen uniformly at random and the system internally sets $h(x) := y$. Finally, y is output as the response to this query. If x has been queried before to $\mathbf{H}$, the already defined value $y = h(x)$ is returned.

Consider the *fixed-message forgery game* $G^{\mathsf{sig\text{-}fix}}_{t,\tilde{m}}$, where the goal of an adversary is to provide a forgery for the known message $\tilde{m}$. In the random oracle model, this game is defined as follows:

1. A random secret key/public key pair (z, v) is sampled according to the key-pair distribution, and output (upon request).
2. The adversary can ask at most t queries of the following two kinds:
   - He can query a message $m \neq \tilde{m}$ and obtain $s := \sigma(m, z)$ (note that σ can query $\mathbf{H}$).
   - He can query the random oracle $\mathbf{H}$ on arbitrary inputs x and receive the result.
3. The game takes an input $\tilde{s}$. The game is won, if and only if $\tau(\tilde{m}, \tilde{s}, v) = 1$ (where τ can depend on $\mathbf{H}$).

Now consider an arbitrary TOWP-based signature scheme. Prove that in the random oracle model, for any winner W in the above forgery game $G^{\mathsf{sig\text{-}fix}}_{t,\tilde{m}}$, there exists a winner W' (which internally uses W) with the same advantage in the TOWP inversion game.

Hint: Try to "program" the uniformly random function table describing h in a clever way for the replies to W (you can assume that sampling uniformly from sets $\mathcal{X}$ and $\mathcal{Y}$ is easy).

d) Again, consider an arbitrary TOWP-based signature scheme. Informally argue, why (in the random oracle model) any winner W with success probability α in the *normal forgery game* G^{sig}_t can be transformed in a winner W' with success probabilitz roughly $\frac{\alpha}{t}$ in the TOWP inversion game.

6.3 The Boneh–Lynn–Shacham Signature Scheme

Goal: *While in the lecture we have seen that pairings can be used to break cryptographic assumptions, we here learn that they can also be used to build cryptographic schemes.*

Let $\mathbb{G} = \langle g \rangle$ and $\mathbb{G}_T = \langle g_T \rangle$ be two cyclic groups of the same cardinality n. Assume that an efficiently computable pairing E between those two groups is known. That is, an efficiently computable function $\mathrm{E}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, such that $\mathrm{E}(g^a, g^b) = \mathrm{E}(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_n$, and $\mathrm{E}(g, g) = g_T$. In the following, let $h\colon \mathcal{M} \to \mathbb{G}$ be an appropriate hash function, let $\mathcal{V} := \mathbb{G}$, and $\mathcal{Z} := \mathbb{Z}_n$. Now, consider the signature scheme that uses the uniform distribution over $\{(g^x, x) \mid x \in \mathbb{Z}_n\}$ as the key-pair distribution and the following signing function:

$$\sigma\colon \mathcal{M} \times \mathbb{Z}_n \to \mathbb{G},\ (m, x) \mapsto (h(m))^x.$$

a) Describe the corresponding signature verification function $\tau\colon \mathcal{M} \times \mathbb{G} \times \mathbb{G} \to \{0, 1\}$, that given a message m, a signature s, and the verification key g^x decides whether the signature is valid.

Hint: Use the pairing E to "solve" the CDH problem.

b) Argue (informally) why in the random oracle model (cf. **6.2 c)**) this signature scheme is secure under the CDH assumption in $\mathbb{G}$.