

1

1.a

Given a message-signature pair (m, σ) we can easily forge a new pair: $(m-1, f(\sigma))$ which is valid:

$$f^{n-(m-1)}(x) = f^{n-m+1}(x) = f(f^{n-m}(x)) = f(\sigma)$$

1.b

Assume by contradiction that f^k is not OWP, i.e. there is an adversary A' s.t. $\Pr_x [A'(f^k(x)) = x] \geq \varepsilon$. Then we construct an adversary A as follows: given $y = f(x)$:

1. Calculate $x' = A'(y)$
2. Calculate and return $f^{k-1}(x')$

Indeed, if A' inverts f^k successfully, then:

$$x' = f^{-k}(y) = f^{-k}(f(x)) = f^{-k+1}(x)$$

And thus the second step yields: $f^{k-1}(f^{-k+1}(x)) = f^0(x) = x$.

A runs in polynomial time because k is polynomial in n . Therefore A is a PPT adversary that inverts f with probability $\geq \varepsilon$, which is a contradiction to f being a OWP. Therefore f^k is a OWP.

1.c

Assume by contradiction that there is an PPT adversary A that for every $x \in \{1, \dots, n\}$, given $(m, \sigma = f^{n-m}(x))$, outputs $(m', \sigma' = f^{n-m'}(x))$ where $m' > m$. Denote $k := m' - m > 0$. Note that:

$$f^k(\sigma') = f^{m'-m}(\sigma') = f^{m'-m}(f^{n-m'}(x)) = f^{n-m}(x) = \sigma$$

Therefore $\sigma' = f^{-k}(\sigma)$. But by (1.b) f^k is a OWP. This will lead to a contradiction.

Construct A' to invert f^k as follows: given some $\sigma = f^k(\sigma')$:

1. For each $m \in \{1, \dots, n\}$ check if $f^m(\sigma) = y$.
 - (a) When a match is found continue.
 - (b) If all checks failed, then stop.
2. Calculate $(m', \sigma') = A(m, \sigma)$
3. return σ'

If A' finds a match in step 1 then: $f^n(x) = y = f^m(\sigma)$, Therefore: $\sigma = f^{n-m}(x)$, i.e. σ is a signature of m . Therefore the pair given to A in step 2 is valid. If A succeeds, then A' indeed returns the correct σ' . Also note that step 1 takes polynomial time in n .

XXXX

1.d

We will generate a new $x' \neq x$. Set $y' = f^n(x')$. Modify the signature of message m to be $(f^{n-m}(x), f^m(x'))$. The verification of a pair $(m, (\sigma_1, \sigma_2))$ will be to check that $f^m(\sigma_1) = y$ and that $f^{n-m}(\sigma_2) = y'$. Indeed, if (σ_1, σ_2) is a correct signature of m then:

$$\begin{aligned} f^m(\sigma_1) &= f^{m+n-m}(x) = f^n(x) = y \\ f^{n-m}(\sigma_2) &= f^{n-m+m}(x') = f^n(x') = y' \end{aligned}$$

The first part of the signature pair is exactly like in the original scheme, and the second part “doesn’t give information” over the first part. Therefore the proof of (1.c) will still hold, preventing forging of signatures for $m' > m$. The second part of the signature works in a similar way to prevent forging messages $m' < m$. Therefore this is indeed a one-time signature scheme.

2

2.a

Assume $y \notin QR$. Let P^* be a prover, and let z be the number it sends in the first step. Note that:

$$\left(\frac{zy}{N}\right) = \left(\frac{z}{N}\right) \overbrace{\left(\frac{y}{N}\right)}^{=-1} = -\left(\frac{z}{N}\right)$$

Where the symbols above are jacobi symbols. Therefore if z is a QR, then $\left(\frac{zy}{N}\right) = -1$, meaning that zy is not a QR. Now see:

$$\Pr[V \text{ accepts}] = \frac{1}{2} \Pr[a_0^2 \equiv z \mid b = 0] + \frac{1}{2} \Pr[a_1^2 \equiv zy \mid b = 1]$$

$$\Pr[a_0^2 \equiv z \mid b = 0] = \Pr[a_0^2 \equiv z \mid b = 0 \wedge z \in QR] \Pr[z \in QR] + \overbrace{\Pr[a_0^2 \equiv z \mid b = 0 \wedge z \notin QR]}^{=0} \Pr[z \notin QR]$$

$$\Pr[a_1^2 \equiv zy \mid b = 1] = \overbrace{\Pr[a_1^2 \equiv zy \mid b = 1 \wedge z \in QR]}^{=0} \Pr[z \in QR] + \Pr[a_1^2 \equiv zy \mid b = 1 \wedge z \notin QR] \Pr[z \notin QR]$$

The three equations are from the law of total probability. The zero term in the second line is because z is not a QR, therefore it has no square root. The zero term in the second line is because z is a QR, and as noted at the begining, that implies that zy is not a QR. To summerize:

$$\begin{aligned} \Pr[V \text{ accepts}] &= \frac{1}{2} \left(\overbrace{\Pr[a_0^2 \equiv z \mid b = 0 \wedge z \in QR]}^{\leq 1} \mathbb{I}_{z \in QR} + \overbrace{\Pr[a_1^2 \equiv zy \mid b = 1 \wedge z \notin QR]}^{\leq 1} \mathbb{I}_{z \notin QR} \right) \\ &\leq \frac{1}{2} (\mathbb{I}_{z \in QR} + \mathbb{I}_{z \notin QR}) = \frac{1}{2} \cdot 1 = \frac{1}{2} \end{aligned}$$