Crypto - HW 5

Hagai Ben Yehuda, ID num: 305237000
Jonathan Bauch, ID num: 204761233

1 1

1.a

ndeed, suppose we have the signature σ_m of $m \in \{1, ..., n\}$, then we can obtain the signature of any $k \in \{1, ..., n\}$ that satisfies $k < m$ by simply setting $\sigma_k = f^{m-k}(\sigma_m)$, then we have that

$$f^k(\sigma_k) = f^k(f^{m-k}(\sigma_m)) = f^m(\sigma_m) = y$$

With the last equality is due to the assumption that σ_m is the correct signature for m. Thus this is not a one time secure signature scheme.

1.b

First we show that f^k is also a permutation, we do so using induction:
For the base case where $k = 1$ this is true from the definition of f. Now assume that f^{k-1} is a permutation, let $x \in \{0,1\}^n$ then x has a source under f (as f is a permutation), namely there exists $y \in \{0,1\}^n$ such that $f(y) = x$, from the induction assumption we know that f^{k-1} is a permutation and thus y has a source $z \in \{0,1\}^n$ such that $f^{k-1}(z) = y$, thus $f(f^{k-1}(z)) = f(y) = x$, thus x has a source under f^k. Since $\{0,1\}^n$ is finite and since we have showed that f^k is on-to, we have that f is also one to one, Hence f is a permutation. Now assume that f^k is not a one-way then there is a polynomial time algorithm A that satisfies:

$$\Pr_{x \leftarrow \{0,1\}^n}(A(f^k(x) = x) > \epsilon$$

We define an algorithm A' that does the following on input x calculates $f^k(x)$ and feeds it to A. A' is polynomial since A and k are polynomial, also note that:

$$\Pr_{x \leftarrow \{0,1\}^n}(A'(x) = x) = \Pr_{x \leftarrow \{0,1\}^n}(A(f^k(x) = x) > \epsilon$$

Leading the a contradiction to the assumption that f is a OWP, hence no such A exists and f^k is also a OWP.

1.c

ndeed, assuming that there is some polynomial algorithm A such that for some $m \in \{1, ...n\}$, $\sigma_m = f^{n-m}(m)$ and $m' > m$, A satisfies:

$$\Pr_{x \leftarrow \{0,1\}^n}(A(\sigma_m) = \sigma(m') = f^{n-m'}(x)) > \epsilon$$

We construct a polynomial algorithm A' that inverts f with the same probability, on input $f(w)$ A' will do the following:

- Set $k = m' - m$.
- Set $\sigma_m = f^{k-1}(f(w)) = f^k(w)$.
- Execute $A(\sigma_m)$ and return its result.

Then

$$\begin{aligned}
\Pr_{w \leftarrow \{0,1\}^n}(A'(f(w)) = w) &= \Pr_{x \leftarrow \{0,1\}^n}(A'(f^{n-m}(x)) = w) \\
&= \Pr_{x \leftarrow \{0,1\}^n}(A(\sigma_m) = w) \\
&= \Pr_{x \leftarrow \{0,1\}^n}(A(\sigma_m) = f^{-k}(\sigma_m))) \\
&= \Pr_{x \leftarrow \{0,1\}^n}(A(\sigma_m) = \sigma_{m'}) > \epsilon
\end{aligned}$$

The first equality is due to the fact that given a random w, the probability for any $x \leftarrow \{0,1\}^n$ to be its k'th source is equal for every x as we assume that f was chosen uniformly form the random permutation functions. This is obviously a contradiction to the assumption that f is a OWF, showing no such algorithm A exists.

1.d

//////////// need to do this!!!!!!!!!! ////////////

2

Let $\tilde{f}$ be some one way function, and define f such that $f(xl) = f(x0)$ (with l being a single bit). Suppose that f is not a one way function, then there is an algorithm A such that

$$\Pr_{x \leftarrow \{0,1\}^n}(A(f(x)) = x) > \epsilon$$

Construct an algorithm A' that on input $\tilde{f}(x)$ executes A to receive yl and returns $y0$. Then we have:

$$\begin{aligned}
\Pr_{x \leftarrow \{0,1\}^n}(A'(\tilde{f}(x)) = x) &\geq \frac{1}{2} \Pr_{x \leftarrow \{0,1\}^{n-1}}(A'(\tilde{f}(x0)) = x0) \\
&= \frac{1}{2} \Pr_{x \leftarrow \{0,1\}^n}(A(f(x)) = x) \\
&> \frac{\epsilon}{2}
\end{aligned}$$

The equality (in the second line) is correct because A' will produce a valid result whenever A is a able to find the source of a message in $\{0,1\}^n$ because if it finds a source then we know that zeroing the last bit of the result will be the source of the original function. Now that we have constructed f and have shown that it is a one way function, then if we use Lamports scheme with f and have a valid signature $(x_{m_1,1}, ..., x_{m_n,n})$ of the message $(m_1, ..., m_2)$ then we know that if $x_{m_1,1} = xl$ then $(x\bar{l}, ..., x_{m_n,n})$ is also a signature for the same message from the construction of f, since $f(xl) = f(x\bar{l})$, showing that using f Lamports scheme is not a strong one time signature scheme.

3

4

4.a

4.b

5

6

6.a

6.b