Problem 8.1 [Signature Compression].

Solution: We describe two solutions.

(a) Call the input $x$, and let $m = \sum_{i=1}^{k} 2^{i(w/k - \log n)}$. The output is $(x \cdot m) \gg (w - k \log n)$. This obviously takes $O(1)$ word RAM operations; $m$ can be hardcoded or can be computed in $O(1)$ time as a geometric series.

Each 1 bit in $m$ shifts a copy of $x$ by its position. In particular, the $2^{i(w/k - \log n)}$ bit shifts $h_i$ from its initial position, ending $i w/k$ bits from the left edge, to ending $i \log n$ bits from the left edge. The sum of these shifts has all the $h_i$ compressed in the leftmost $k \log n$ bits, and we then shift the whole word to put them at the right end instead.

Unfortunately, $x \cdot m$ has more terms than the ones we want: for every $i$ and $j$, it shifts $h_i$ by $2^{j(w/k - \log n)}$. We must show that only the desired shifts (when $i = j$) land in the leftmost $k \log n$ bits; the rest of the bits are ignored by the shift. Two copies of $h_i$ with different values of $j$ land at least $w/k - \log n$ bits apart. As long as this is more than $k \log n$, since the desired copy of $h_i$ lands entirely in the leftmost $k \log n$ bits, no other copy could land even partially in the leftmost $k \log n$ bits.

So it suffices to have $w/k - \log n > k \log n$. But $w/k = \log^2 n$ and $k = \log^\varepsilon n$, so this is equivalent to $\log^2 n - \log n > \log^{1+\varepsilon} n$, which is true for $\varepsilon < 1$ and sufficiently large $n$.

(b) Call the input $x$, and let $q = 2^{w/k - \log n}$. The output is $x \% q$.

To prove correctness, it suffices to show that correct output $y \equiv x \mod q$, and $y < q$. Then $x \% q = y$, as desired.

The input is $x = \sum_{i=0}^{k-1} h_{k-i} 2^{iw/k}$, and the correct output is $y = \sum_{i=0}^{k-1} h_{k-i} 2^{i \log n}$. We have

\[
\begin{align*}
2^{w/k} &\equiv 2^{\log n} \mod q \\
2^{iw/k} &\equiv 2^{i \log n} \mod q \\
h_{k-i} 2^{iw/k} &\equiv h_{k-i} 2^{i \log n} \mod q \\
x &\equiv y \mod q.
\end{align*}
\]

The correct output is zero outside the rightmost $k \log n$ bits, so

\[
y < 2^{k \log n} = 2^{\log^{1+\varepsilon} n} < 2^{\log^2 n} - 2^{\log n} = q
\]

for $\varepsilon < 1$ and sufficiently large $n$. 
