Relative to (Sam, $\mathcal{F}$, PSPACE)

- $\exists$ OWF
- $\nexists$ coll. res. hash-function

"Claim i": Fix randomness of Sam (hard-coding)

"Claim ii": Fix randomness of $\mathcal{A}$ (averaging)

"Claim iii": $\mathcal{A}$ is succ. on non-negl. fraction of functions (averaging)

Lemma 1: You need full look-up $= \log^2 n$ bits ... if you want to encode a non-negl. fraction of function.

"Main Lemma": Succ. $\mathcal{A}$ allows to encode non-negl. fraction of functions in less than

encoding/decoding, to make queries/answers deterministic

$\mathcal{A}(s)$

Ask Sam on $h(s, .)$ and get collision with high probability $\square$

easy

Claim 2