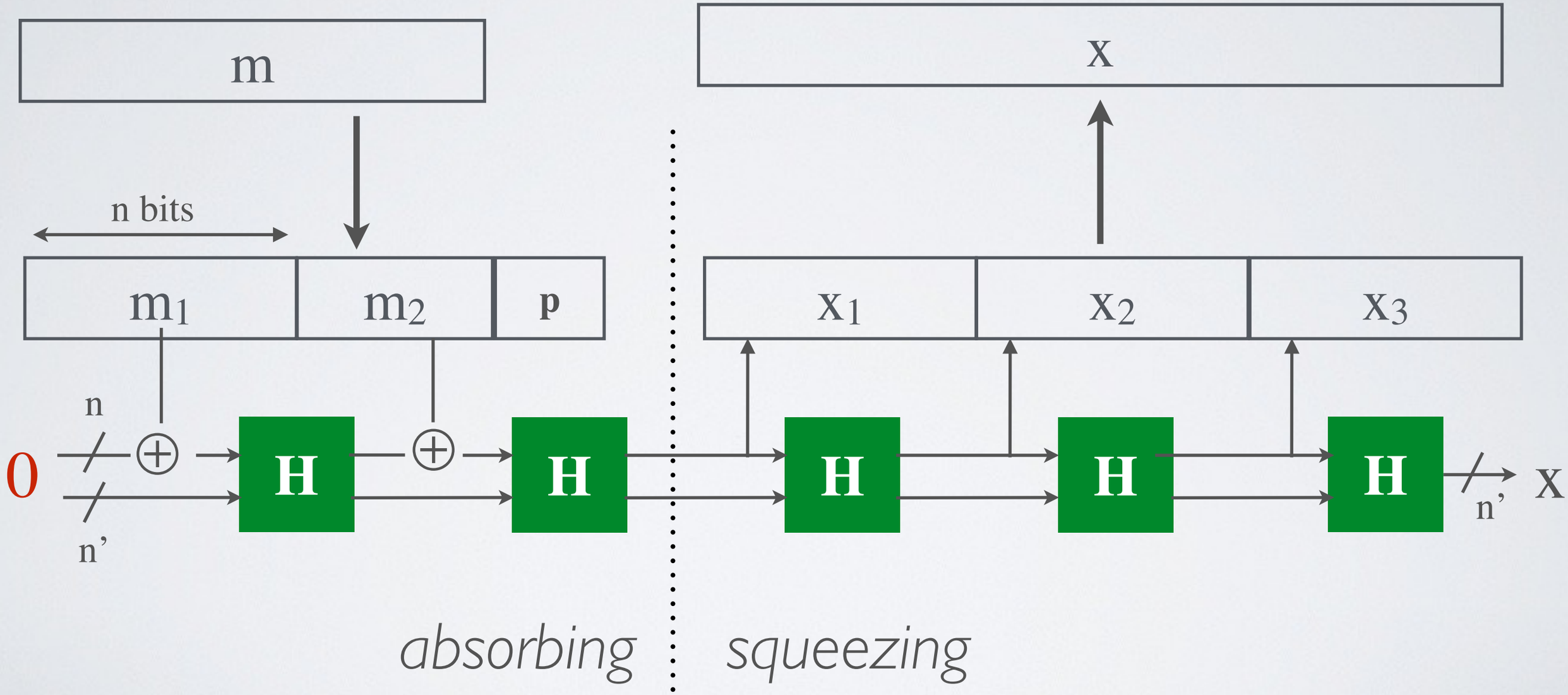
How to hash long messages ?

Sponge construction (SHA-3)

split $\mathbf{m}$ in blocks of $\mathbf{n}$ bits
and add padding $\mathbf{p}$

assemble the hash



Property : if $\mathbf{H}$ is CR then Sponge is CR

Brute-forcing a hash function

CR - Collision Resistance

➡ given $\mathbf{H}$, hard to find $\mathbf{m}$ and $\mathbf{m'}$ such that $\mathbf{H(m) = H(m') = x}$

Given a hash function $\mathbf{H}$ of $\mathbf{n}$ bits output

- There are $2^{\mathbf{n}}$ hashes
- Given a specific hash, an attacker will find the corresponding input in ~~$2^{\mathbf{n-1}}$ tries~~