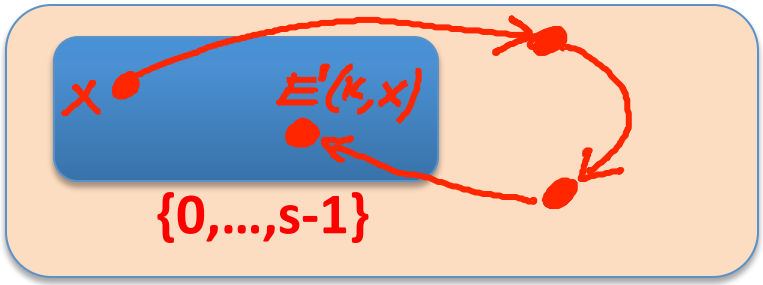
Step 2: from $\{0,1\}^t$ to $\{0,\ldots,s-1\}$

Given PRP $(E,D): K \times \{0,1\}^t \longrightarrow \{0,1\}^t$

we build $(E',D'): K \times \{0,\ldots,s-1\} \longrightarrow \{0,\ldots,s-1\}$

E'(k, x): on input $x \in \{0,\ldots,s-1\}$ do:

y⟵x; do { y ⟵ E(k, y) } until $y \in \{0,\ldots,s-1\}$; output y



Expected # iterations: 2