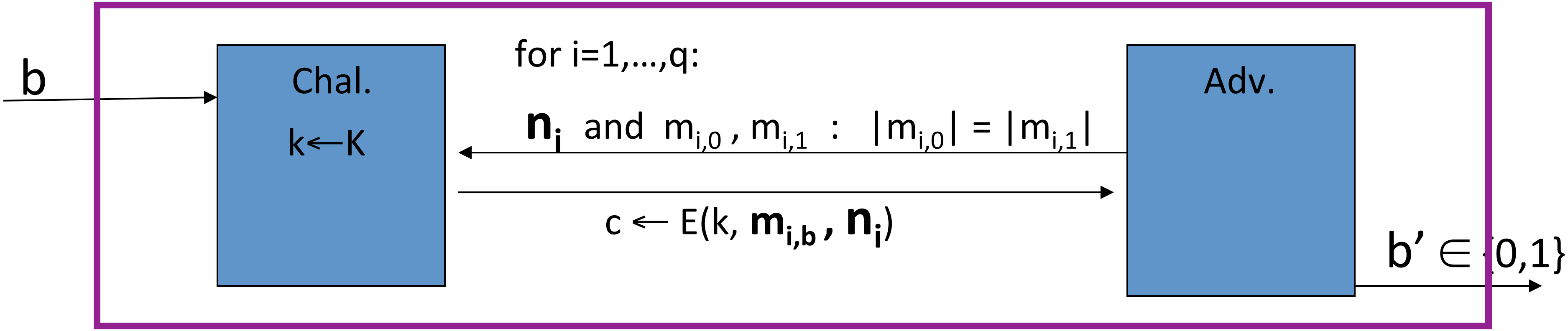
CPA security for nonce-based encryption

System should be secure when nonces are chosen adversarially.


b
Chal.
$k \leftarrow K$
for i=1,…,q:
$\mathbf{n_i}$ and $m_{i,0}$, $m_{i,1}$: $|m_{i,0}| = |m_{i,1}|$
$c \leftarrow E(k, \mathbf{m_{i,b}}, \mathbf{n_i})$
Adv.
$b' \in \{0,1\}$

All nonces $\{n_1, …, n_q\}$ must be distinct.

Def: nonce-based E is sem. sec. under CPA if for all "efficient" A:

$$\mathrm{Adv}_{\mathrm{nCPA}}[A,E] = \left| \Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1] \right|$$ is "negligible."

Dan Boneh