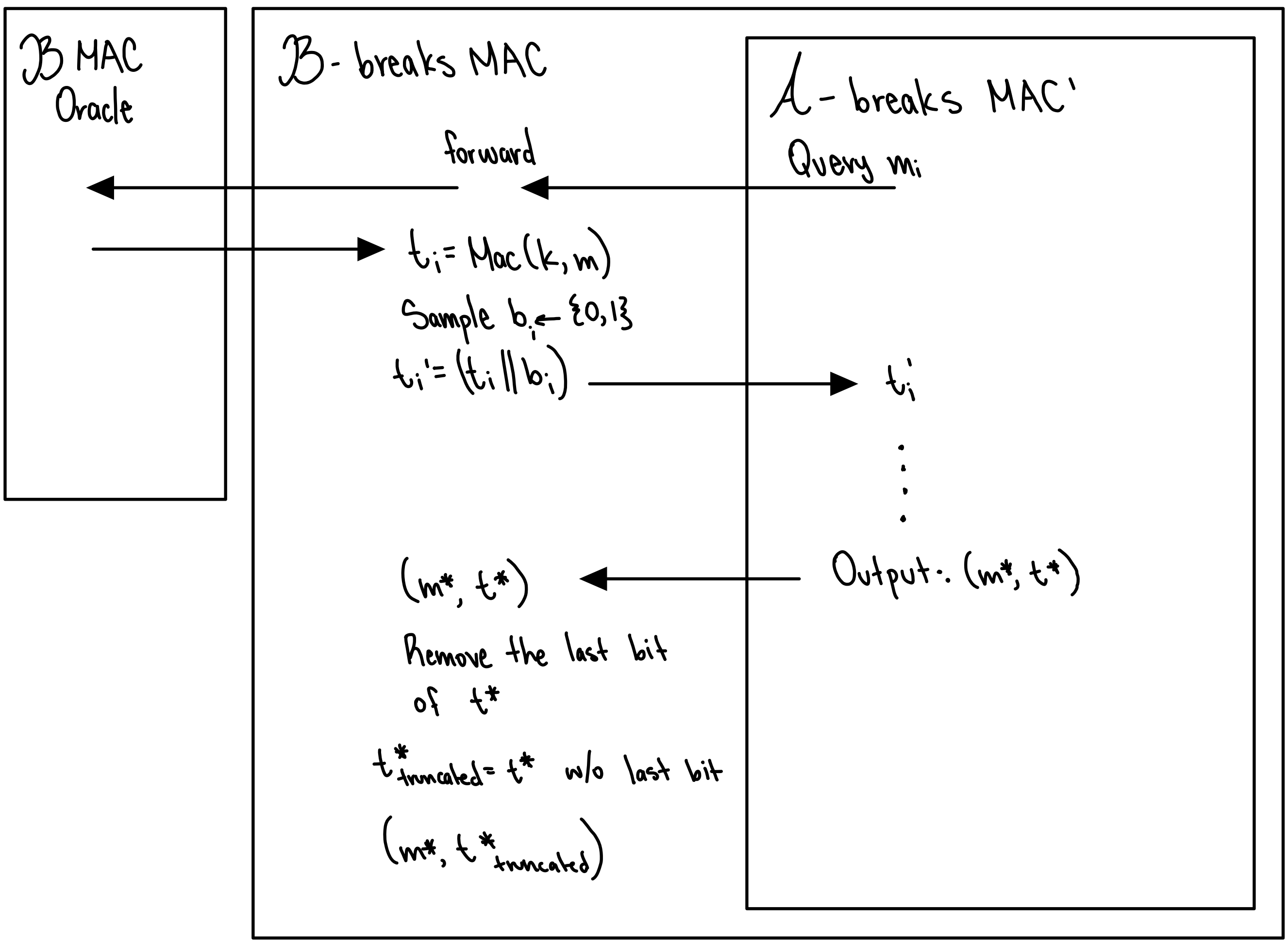
# Difference Between Regular and Strong Security for MACs

Construct a MAC $\mathsf{MAC}' := (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Verify}')$ that is secure but not strongly secure. In your construction, you may start with a secure MAC, $\mathsf{MAC} := (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Verify})$.

MAC':

- $\mathrm{Gen}'(1^n)$: Run $\mathrm{Gen}(1^n)$
- $\mathrm{Mac}'(k,m)$: 1. Compute $t = \mathrm{Mac}(k,m)$
  2. Sample $b \leftarrow \{0,1\}$
  3. Output $t' := t \| b$
- $\mathrm{Verify}'(k,m,t)$: Let $t_{truncated}$ = $t$ without the final bit. Run $\mathrm{Verify}(k,m,t_{truncated})$.

Let's prove that MAC' is secure: We will assume (toward contradiction) there is an adversary $\mathcal{A}$ that breaks MAC'. We will construct $\mathcal{B}$ that breaks MAC.




So... if $\mathcal{A}$ outputs a winning $(m^*, t^*)$, $\mathcal{B}$ can use it to break MAC (100% of the time!) since $\mathrm{Verify}'(k, m^*, t^*)$ would output 1 (implying $\mathrm{Verify}(k, m^*, t^*_{truncated})$ outputs 1.)
$\mathcal{A}$ wins w/ non-negl. probability $\longrightarrow$ $\mathcal{B}$ wins MAC game w/ non-negl. probability. So our assumption was false & MAC' is secure!

## CPA-Secure Encryption

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme. Below, we will construct another encryption scheme and prove that it is also CPA-secure.

In the encryption scheme below, let the message $m$ belong to $\{0,1\}^n$.

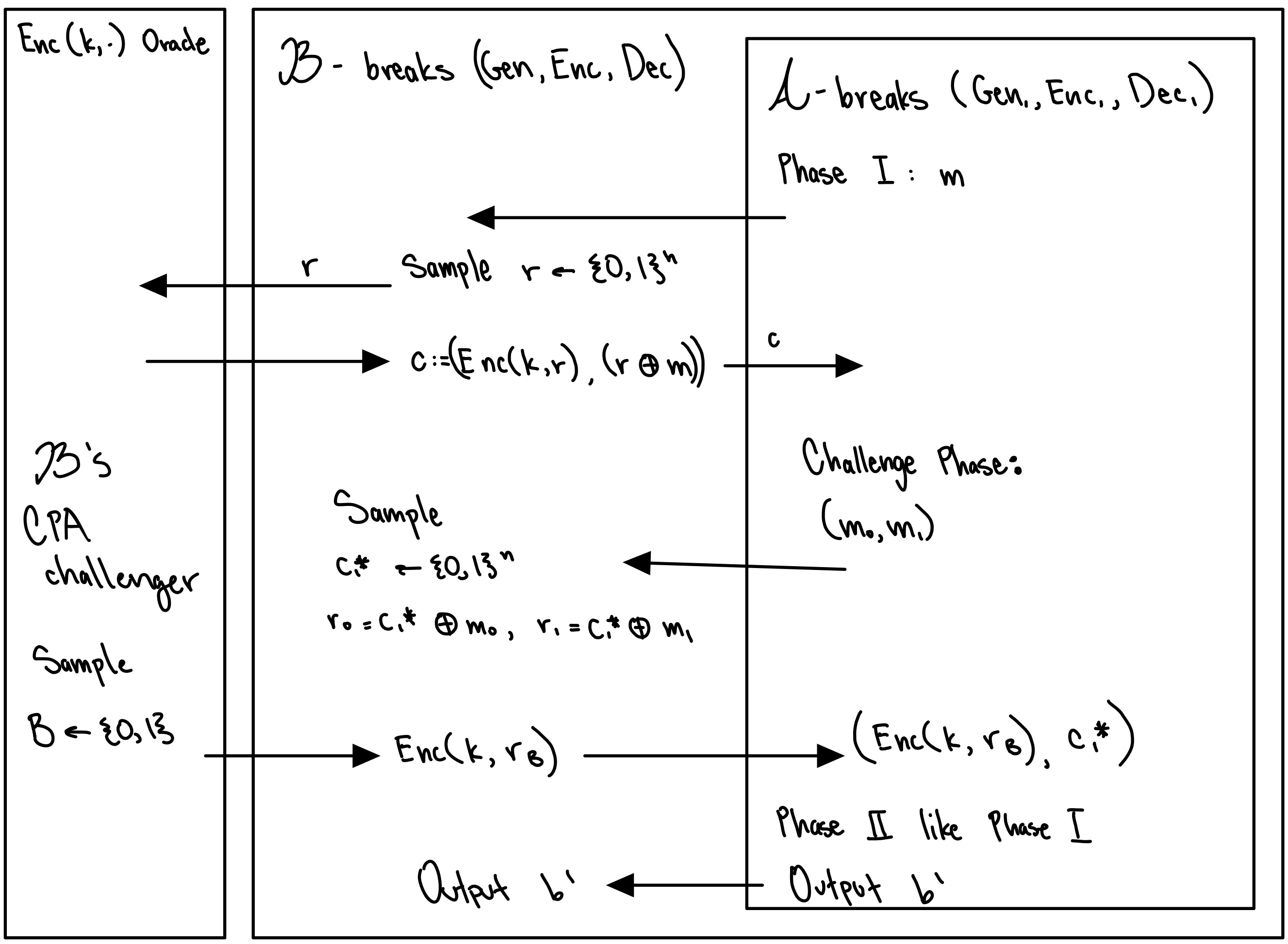
- $\mathsf{Gen}_1(1^n)$: Sample the key as follows: $k \leftarrow \mathsf{Gen}(1^n)$.
- $\mathsf{Enc}_1(k, m)$: Sample $r \leftarrow \{0,1\}^n$ uniformly at random. Then compute $c_0 := \mathsf{Enc}(k, r)$ and $c_1 := r \oplus m$. Output the ciphertext $c = (c_0, c_1)$.
- $\mathsf{Dec}_1(k, (c_0, c_1))$: Compute $r' := \mathsf{Dec}(k, c_0)$ & compute $m' := r' \oplus c_1$. Output $m'$.

Prove that $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ satisfies CPA security.

Assume $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ is not CPA secure.

We will assume (toward contradiction) there is an adversary $\mathcal{A}$ that breaks (wins the CPA game) for $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ w.p. $\frac{1}{2}$ + non-negl.

We will construct $\mathcal{B}$ that breaks $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.




- For either $B$ (0 or 1), $(\mathsf{Enc}(k, r_B), c_1^*)$ is a valid encryption of $m_B$ under $\mathsf{Enc}_1(k, \cdot)$
- $c_1^* = r_B \oplus m_B$
- $r_B$ is uniformly random & independent of $(m_0, m_1, B)$.

$\mathcal{A}$ & $\mathcal{B}$ have the same success probability!