Privacy against eavesdroppers

Indistinguishability in the presence of an eavesdropper:

$\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$:

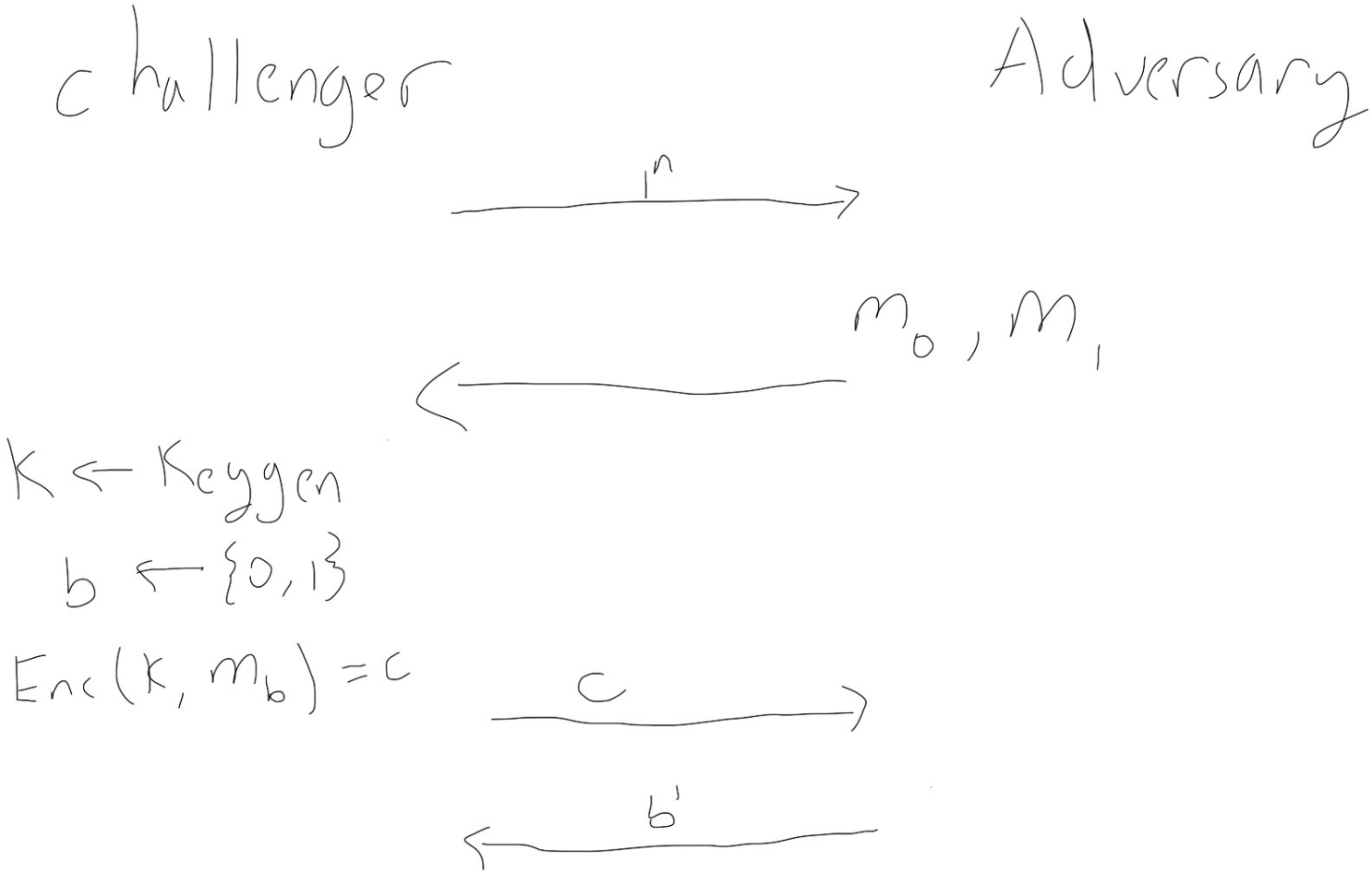
1. $\mathcal{A}$ is given 1^n and outputs m_0 and m_1 such that $|m_0| = |m_1| = \ell(n)$.
2. $k \leftarrow \mathit{Gen}(1^n)$, $b \leftarrow \{0,1\}$, and $c \leftarrow \mathit{Enc}(k, m_b)$. Then c is given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a bit b'.
4. The outcome of the experiment is 1 if $b = b'$ and 0 otherwise.

Definition

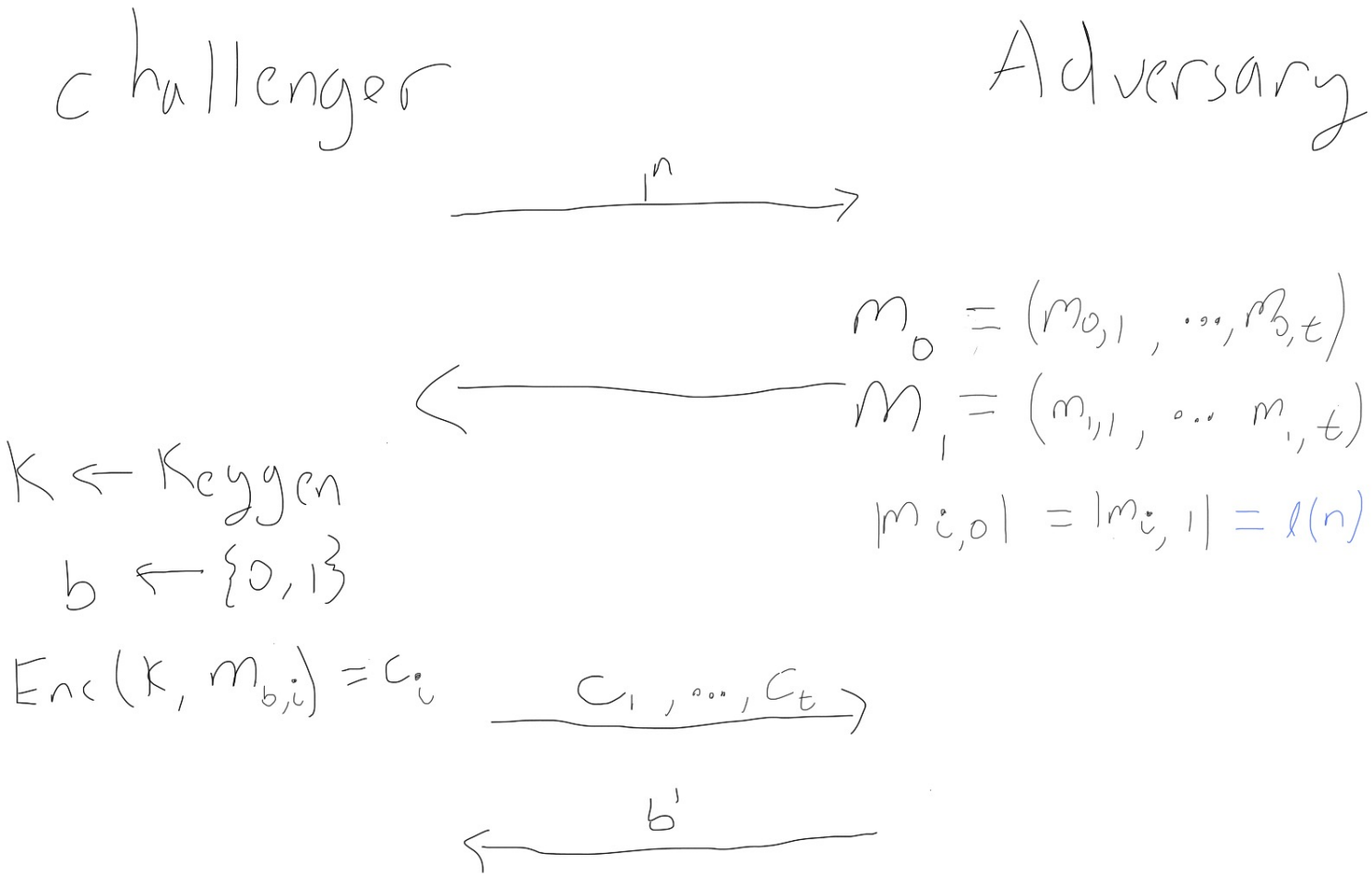
A fixed-length private-key encryption scheme $\Pi = (\mathit{Gen}, \mathit{Enc}, \mathit{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper, or is EAV-secure, if for all probabilistic polynomial-time adversaries $\mathcal{A}$, there is a negligible function negl such that, for all n,

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq 1/2 + \mathrm{negl(n)}$$

Privacy against eavesdroppers



Multiple message eavesdropping experiment



Pseudo-OTP insecure for multiple messages

Both the OTP and the Pseudo-OTP fail to meet this security requirement.

Pseudo-OTP insecure for multiple messages

Both the OTP and the Pseudo-OTP fail to meet this security requirement.