Proof (Lemma). Need to show:

$$(\wedge') \Rightarrow (\wedge N) \Rightarrow (NN) \Rightarrow (N).$$

$(N) \Rightarrow (NN)$

$$P_r[\Pi = m] = P_r[M = m \mid C = c]$$

$$= \frac{P_r[M = m \wedge C = c]}{P_r[C = c]}$$

$$\Rightarrow P_r[M = m \wedge C = c] = P_r[\Pi = m] \cdot P_r[C = c]$$

$$\Rightarrow I(M; C) = 0 \checkmark$$

(VV) ⇒ (VVV) For m from M and c from C :

$$Pr[E_{mc}(K,m)=c] =$$

$$Pr[\underbrace{E_{mc}(K,M)}_{C}=c \mid M=m] =$$

$$Pr[C=c \mid M=m]$$

$$= Pr[C=c]$$

Replacing m with m':

$$Pr[Enc(K, m') = c] = Pr[C = c]$$

✓

(NNN) $\Rightarrow$ (N). Take any c from C:

$$Pr[C = c] = Pr[C = c \mid M = m]$$

I claim this! ↗ by (NiN)

If claim True, Then:

$$Pr[M = m \mid C = c] \cdot Pr[C = c] =$$

$$= \Pr[M = m \wedge C = c] =$$

$$\Pr[C = c \mid M = m] \cdot \Pr[M = m].$$

$$\Rightarrow \Pr[M = m] = \frac{\Pr[M = m \mid C = c] \cdot \Pr[C = c]}{\Pr[C = c \mid M = m]}$$

✓

It remains to prove the claim.

$$\Pr[C = c] = \sum_{m'} \Pr[C = c \wedge M = m']$$

$$= \sum_{m'} \Pr[C = c \mid M = m'] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, M) = c \mid M = m'] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, m') = c] \cdot \Pr[M = m']$$

$$= \sum_{m'} \Pr[Enc(K, m) = c] \cdot \Pr[M = m']$$

$$= \Pr[Enc(K, m) = c] \cdot \underbrace{\sum_{m'} \Pr[M = m']}_{= 1}$$

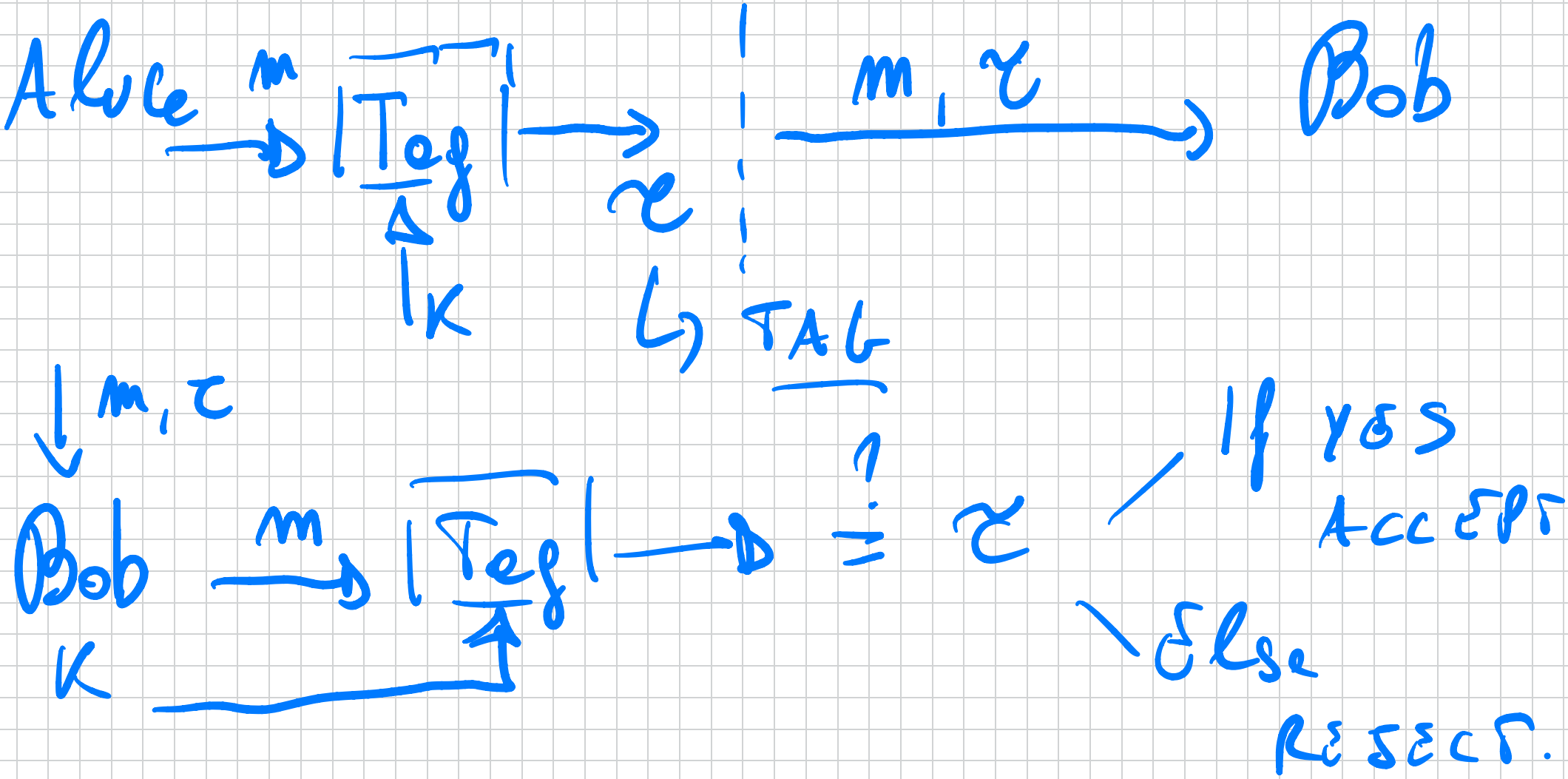
$$= \Pr[\mathrm{Enc}(k, m) = c]$$

$$= \Pr[\underbrace{\mathrm{Enc}(k, M)}_{C} = c \mid M = m]$$

$$= \Pr[C = c \mid M = m] \qquad \blacksquare$$

Message Authentication Codes

Also called MACs.



CORRECTNESS: By definition of Tag $\Rightarrow$ DETERMINISTIC.

UNFORGEABILITY: Should be hard to forge valid tag τ' on msg m'. Not only that! Hard to produce if even given a VALID pair (m, τ) as long as $m' \neq m$.

DEF (STATISTICAL SECURE MAC). We say Π = Tag has ε-statistical

security (unforgeability) if $\forall$ $m, m' \in \mathcal{M}$ with $m' \neq m$, $\forall$ $c, c' \in \tilde{\mathcal{C}}$:

$$\Pr_K[\mathrm{Tag}(K, m') = c' \mid \mathrm{Tag}(K, m) = c] \leq \varepsilon.$$

$(t = 1)$

Here ε is a parameter, e.g. $\varepsilon = 2^{-80}$.

Exercise. Impossible to get $\varepsilon = 0$.

Because a random $c' \leftarrow \tilde{\mathcal{C}}$ has

probability $\geq 1/|\mathcal{T}|$ to be correct.

Note that the def is ONE-TIME!

We will show:

- The notion is ACHIEVABLE
- It's unefficient. In fact:

Thm Any t-time $2^{-\lambda}$-stat. secure Tag has a key of size $(t+1)\cdot\lambda$.

We now show that any family of HASH FUNCTION with a particular

properly satisfies the definition.

DEF (PAIRWISE INDEPENDENCE) - A family $\mathcal{H} = \{h_k : \mathcal{U} \to \mathcal{C}\}_{k \in K}$ is PAIRWISE INDEP. if: $\forall\, m, m' \in \mathcal{U}$ s.t. $m \neq m'$, then:

$$\left(h(k, m), h(k, m')\right)$$

is UNIFORM over $\mathcal{C}^2 = \mathcal{C} \times \mathcal{C}$ for k UNIFORM in K.