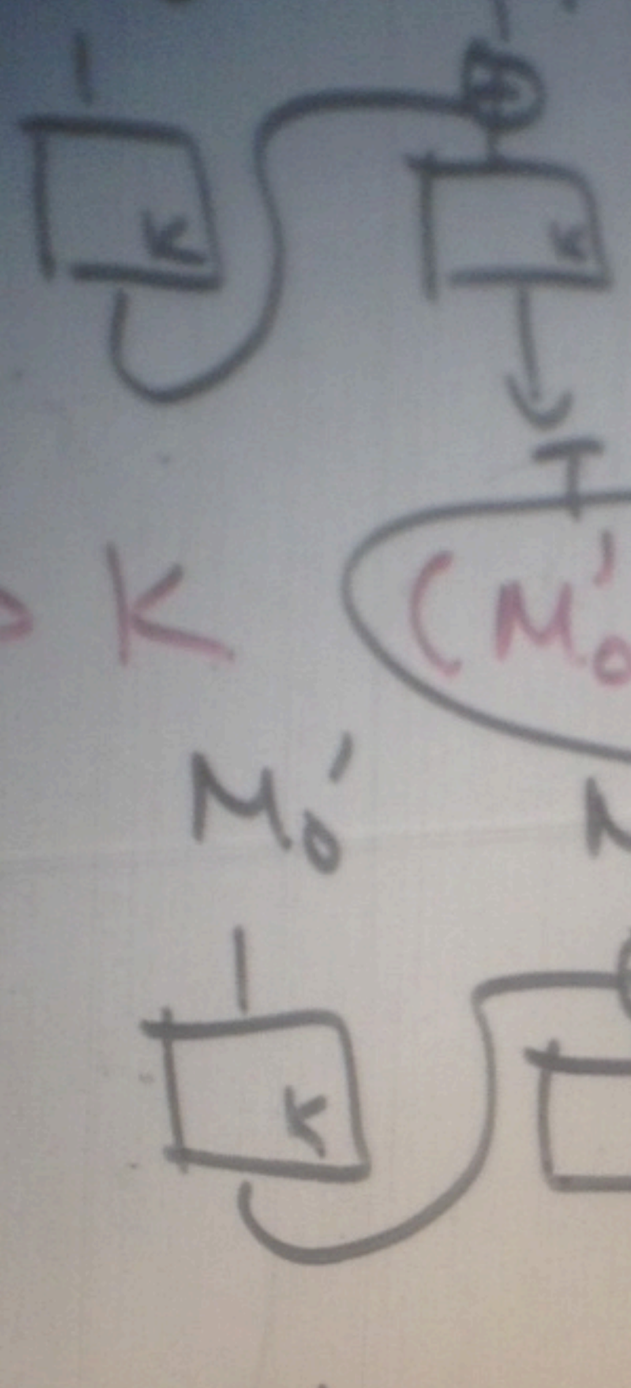
Alice (k)

$M_0$ $M_1$

$(M_0 \| M_1, T)$



???

Bob k

$(M_0' \| M_1', T')$

$M_0'$ $M_1'$

if $T'' == T'$
then retvalid
else return invalid

$(M_0 \| M_1, T)$ ⟶ ⟶

$(M_0' \| M_1', T')$ ⟶ ⟶

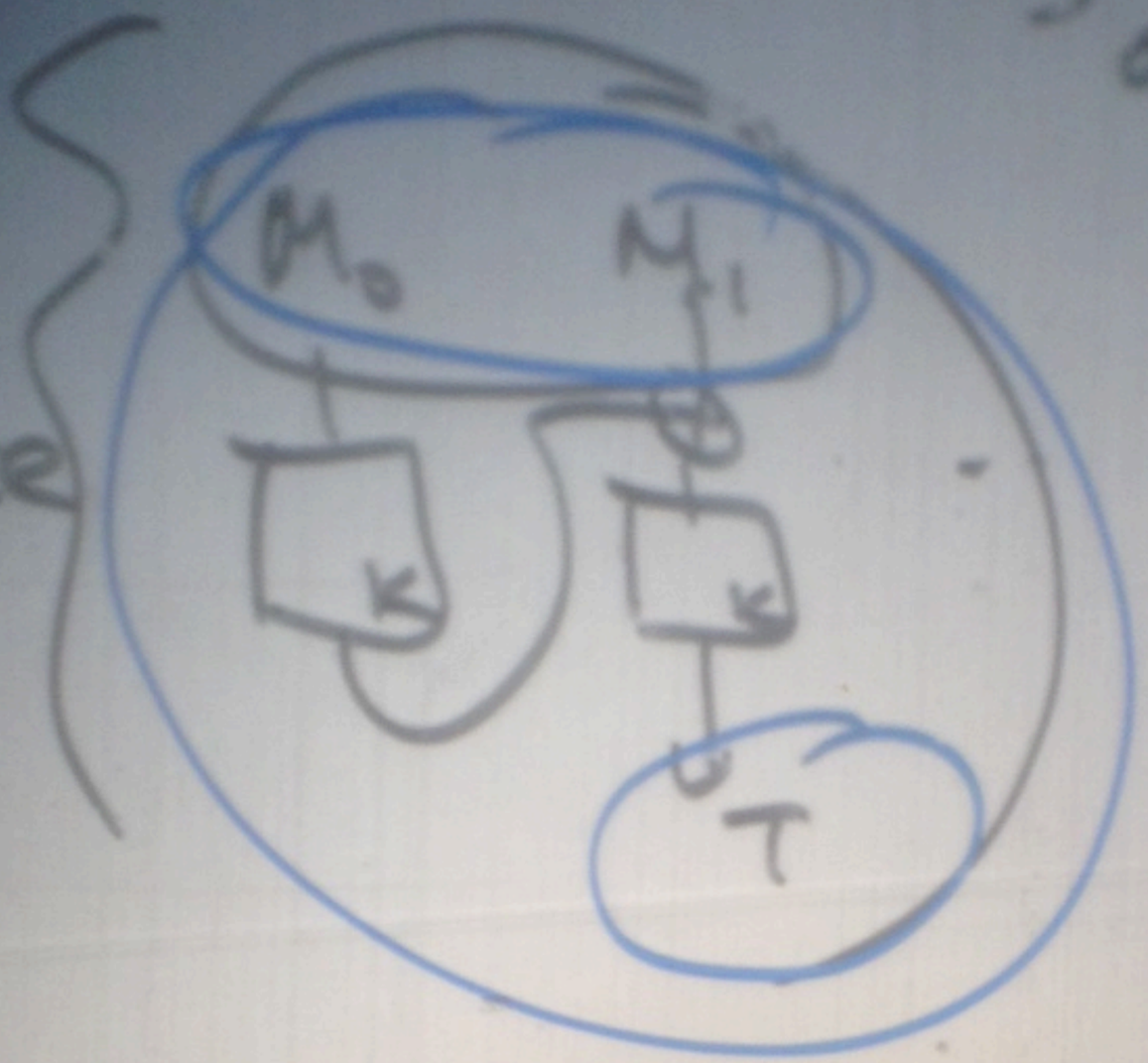
$(M_0'' \| M_1'', T'')$ invalid

$\neq$

CBC MAC NOT SECURE AGAINST VARIABLE-LENGTH MESSAGES

$(M_0 \| M_1, T) \longrightarrow$

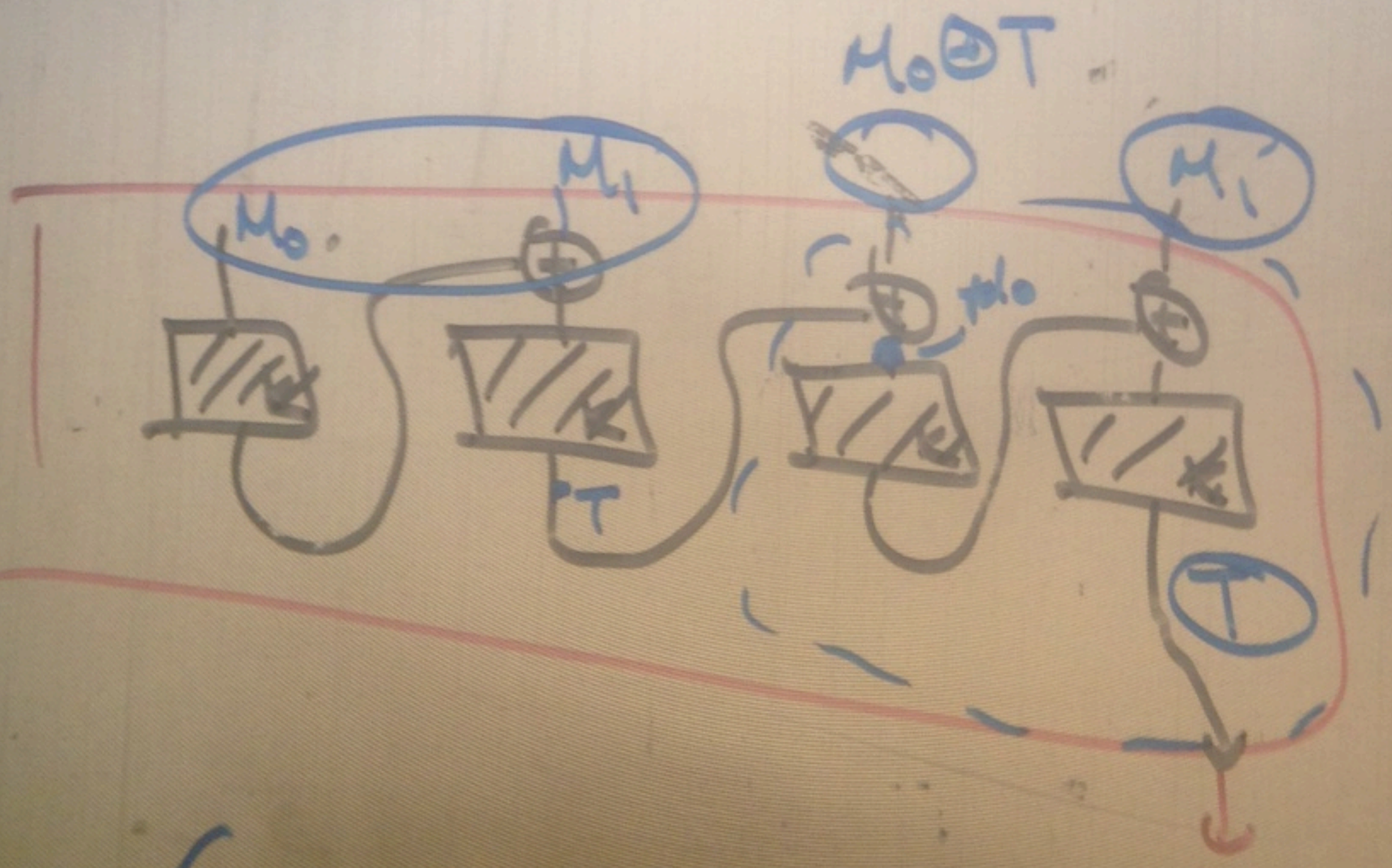
adversary




Alice

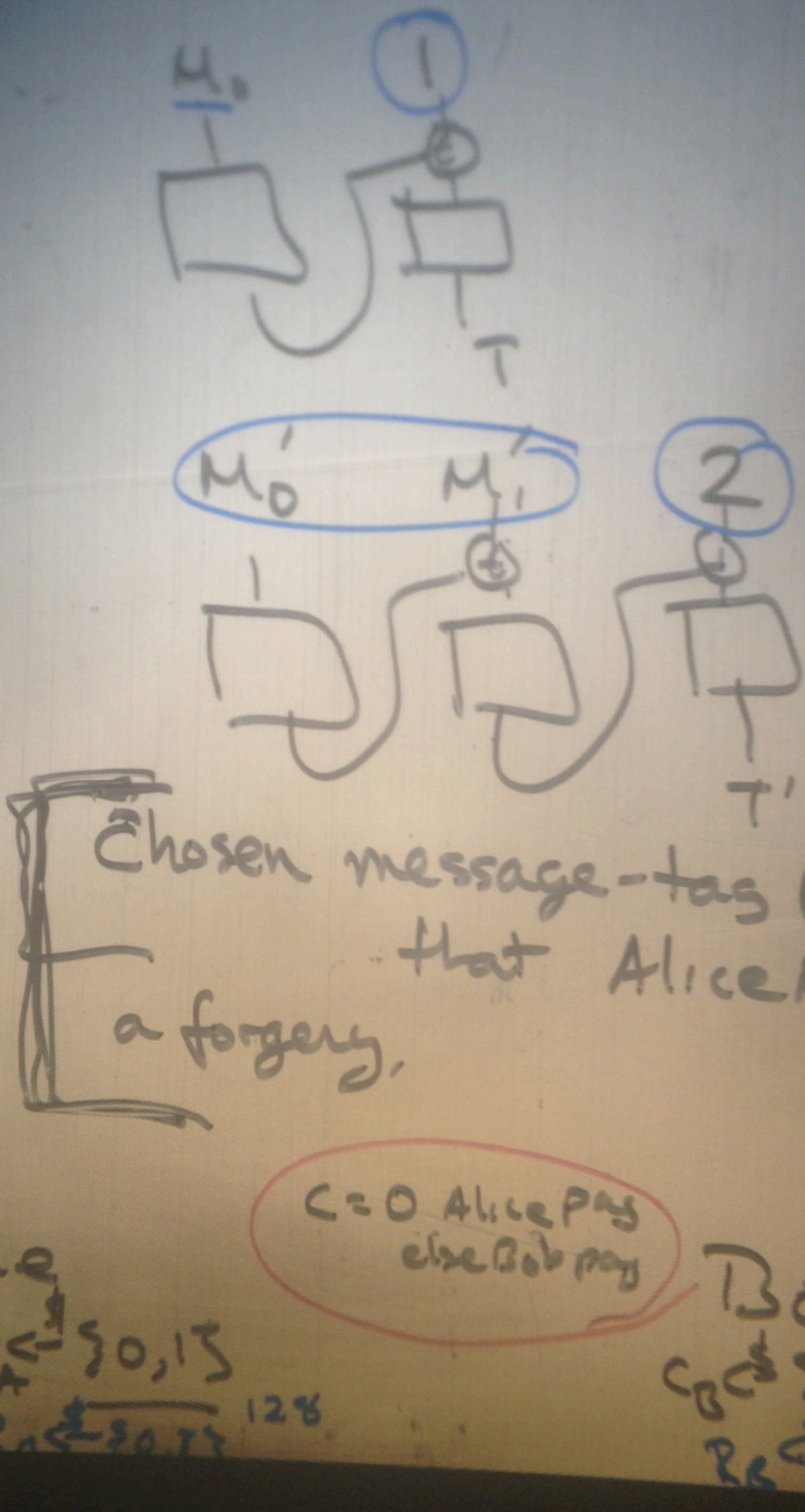
Bob

$(\quad , T')$




$(M_0 \| M_1, \| M_0 \oplus T \| M_1, , T'')$

CBC-MAC variant that appends
block length to end of message




Chosen message-tag pairs that Alice MACs

a forgery.

C=0 Alice pays
else Bob pays

Alice

$C_A \leftarrow \$0,13$

$R_A \leftarrow \$0,13$ 128

Bob.

$C_B \leftarrow \$0,13$

$R_B \leftarrow \$0,13$ 128

$C_A \xleftarrow{\$} \{0,1\}$

$R_A \xleftarrow{\$} \{0,1\}^{128}$

$H_A = h(R_A \| C_A \| \text{Alice})$

$C_B \xleftarrow{\$} \{0,1\}$

$R_B \xleftarrow{\$} \{0,1\}^{128}$

$H_B = h(R_B \| C_B \| \text{Bob})$

Alice

Bob.

$C=0$ Alice pay else Bob pay

one-way

commit

$H_A$

$H_B$

no collisions

$x = h(0)$

$y = h(1)$

$H_A = H_B$ @ random is very small

reveal

$R_A, C_A$

$R_B, C_B$

- collision resistance.

$H_B' = h(R_B \| C_B \| \text{Bob})$

if $H_B \neq H_B'$ halts

$H_A' = h(R_A \| C_A \| \text{Alice})$

if $H_A \neq H_A'$ halts

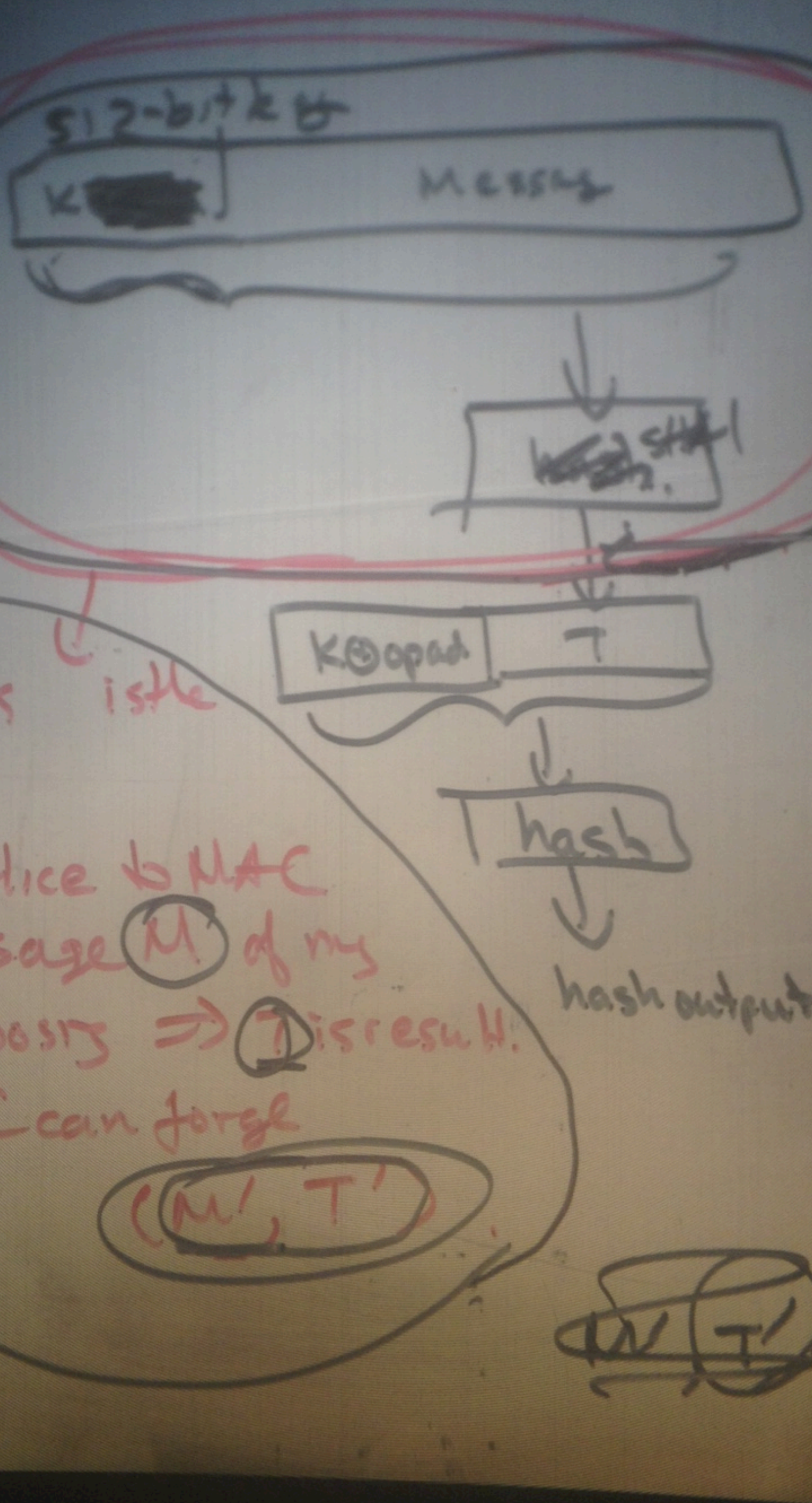
$C = C_A \oplus C_B$

$C = C_A \oplus C_B$

$h(R_B^1 \| 0 \| \text{Bob}) = h(R_B^2 \| 1 \| \text{Bob}) = H_B$

random coin $C = C_A \oplus C_B$

HMAC,




If this is the MAC.

Ask Alice to MAC message M of my choosing ⇒ T is result.

Now I can forge (M', T')