$KG: k \xleftarrow{\$} \{0,1\}^k$

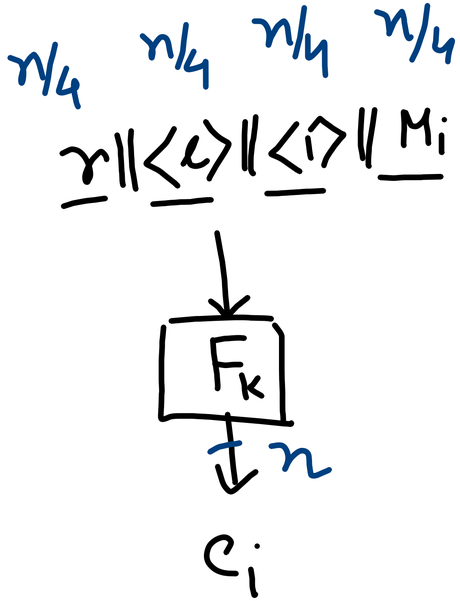
$$\Pi \begin{cases} TG_k(M_1 \| M_2 \| \cdots \| M_\ell) \\ = (r \| C_1 \| C_2 \| \cdots \| C_\ell) \\ \vdots \end{cases}$$

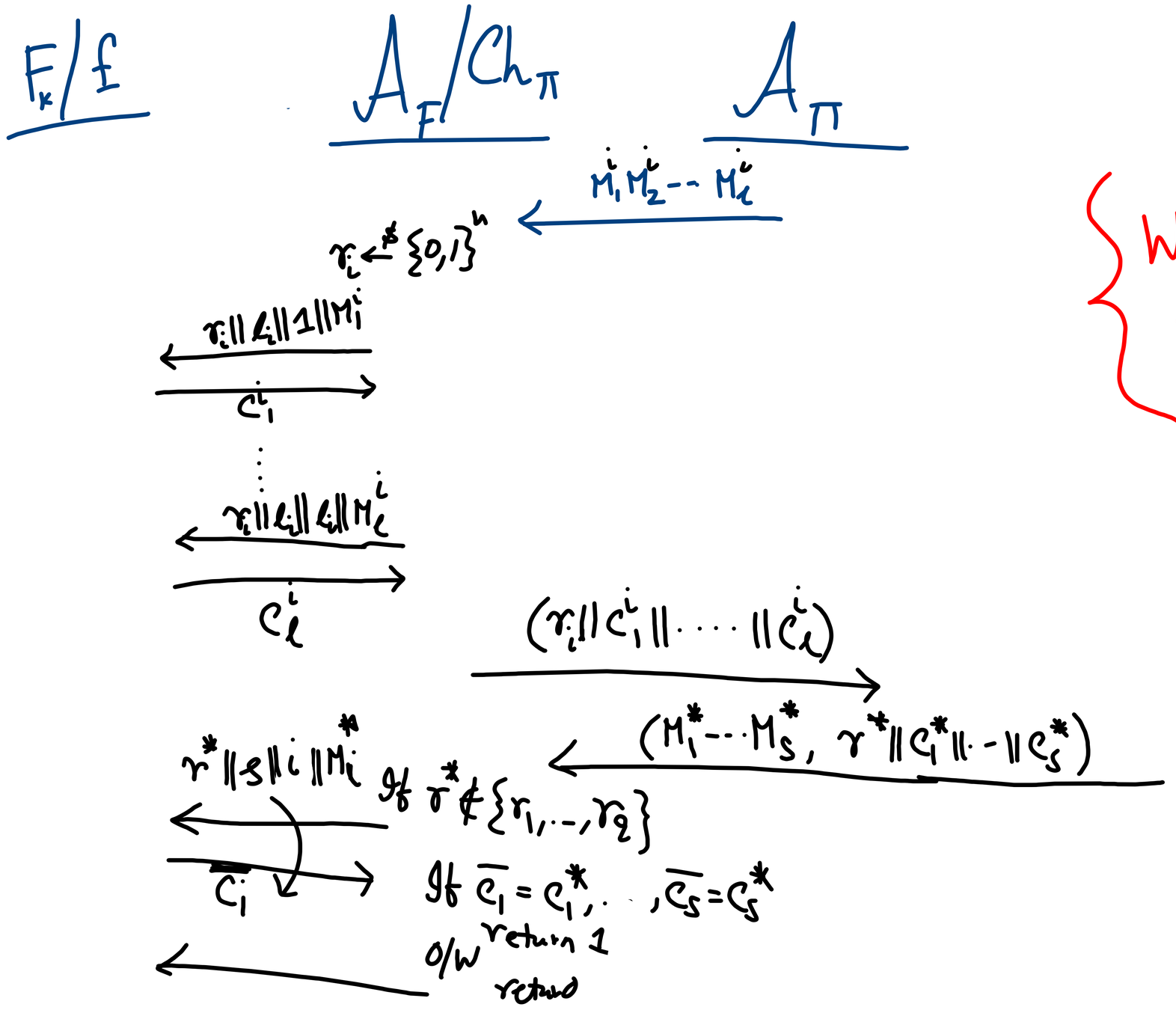
$F \rightarrow$ PRF

$\Pi \rightarrow$ MAC

$\mathcal{A}_\Pi \rightarrow$ MAC adversary

$\mathcal{A}_F \rightarrow$ breaks PRF





What happens if $r^* = r_j$?

$M_1 M_2 M_3 M_4$
$M_1 M_2 M_3$

F/f

$A_{F/f}$

A_π

$M_1 M_2 M_3$

$r \leftarrow^{\$} \{0,1\}^n$

$r \| 3 \| i \| M_i$

C_i

$r \| C_1 \| C_2 \| C_3$

① If $l = l^*$
⇓
∃ some block i s.t. $M_i \neq M_i^*$
} Try to verify the last PRF call

② If $l \neq l^*$
$r \| l \| i \| M_i \neq r \| l^* \| i \| M_i$
So verify with any block

$(M_1 \| M_2 \| M_3^*, r \| C_1 \| C_2 \| C_3^*)$

$r \| 3 \| 3 \| M_3^*$

$\overline{C_3^*}$

If $C_3^* = \overline{C_3^*}$
else return 1

If BAD doesn't occur

$$\Pr\left[\mathcal{A}^{F}_{F/f} \text{ returns } 1\right]$$

$$= \Pr\left[\mathcal{A}^{\pi} \text{ forges}\right]$$

$$\left|\Pr\left[\mathcal{A}^{\pi} \text{forges}\right] - \frac{1}{2^n}\right| \leq \text{negl}(n)$$

$$\Pr\left[\mathcal{A}^{\pi} \text{forges}\right] \leq \frac{1}{2^n} + \text{negl}(n)$$

$$\Pr\left[\mathcal{A}^{f}_{F/f} \text{ returns } 1\right]$$

$$= \Pr\left[\mathcal{A}^{\pi^*} \text{ returns } 1\right] \longrightarrow F_k \text{ replaced by } f$$

$$= \frac{1}{2^n}$$

$$\Pr\left[f(x) = y \,\middle|\, \begin{matrix} f(x_1)=y_1, \\ \vdots \\ f(x_q)=y_q \end{matrix}\right]$$

$$= \frac{1}{2^n}, \text{ if } x \notin \{x_1, \ldots x_q\}$$

Random function

$$\Pr\left[\mathcal{A}^{\pi} \text{forges}\right] \leq \Pr\left[BAD\right] + \Pr\left[\mathcal{A}^{\pi} \text{forges} \,\middle|\, \overline{BAD}\right]$$

$$\leq \frac{q^2}{2^{n/4}} + \frac{1}{2^n} + \text{negl}(n)$$

$\Downarrow$ EUF-CMA Security

If $r_i = r_j$

- $(r_i, M_1 M_2 M_3) \rightarrow (r_i, C_1 C_2 C_3)$
- $(r_j, M_1^* M_2^* M_3^*) \rightarrow (r_j, C_1^* C_2^* C_3^*)$
- $(r_i, M_1 M_2^* M_3) \rightarrow (r_i, C_1 C_2^* C_3)$

If $r_i = r_j$

- $(r_i, M_1 M_2 M_3) \rightarrow (r_i, C_1 C_2 C_3)$
- $(r_j, M_1^* M_2^* M_3^*) \rightarrow (r_j, C_1^* C_2^* C_3^*)$
- $(r_i, M_1 M_2^* M_3) \rightarrow (r_i, C_1 C_2^* C_3)$

BAD

↳ $\exists i, j : r_i = r_j$

$$\Pr[\text{BAD}] \leq \frac{\binom{q}{2}}{2^{n/4}} \leq \frac{q^2}{2^{n/4}}$$

Birthday Paradox

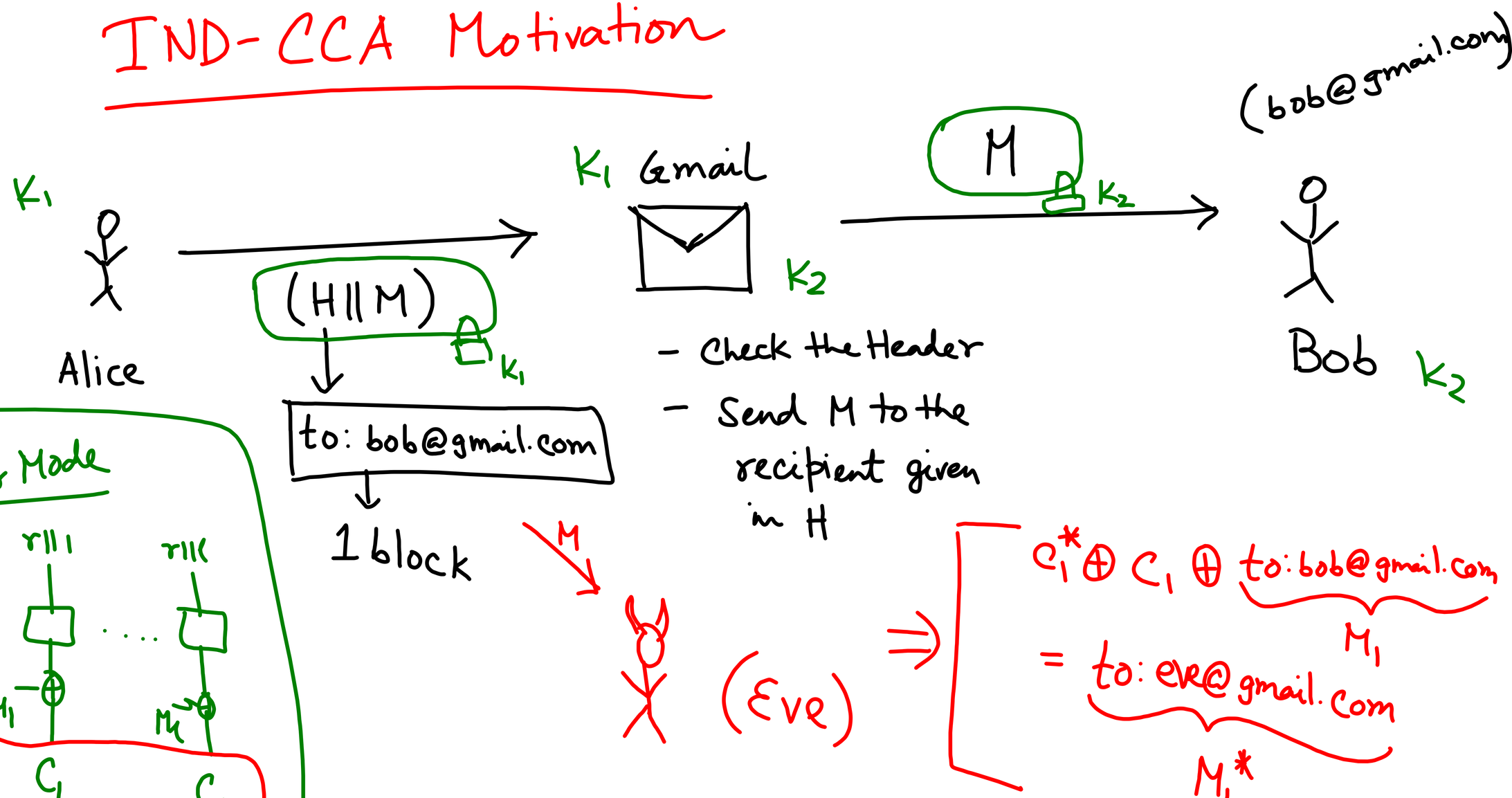
$$\frac{1}{365} \times \binom{23}{2}$$

$$\frac{365}{365} \times \frac{364}{365} \times \cdots \times \frac{(365-22)}{365}$$

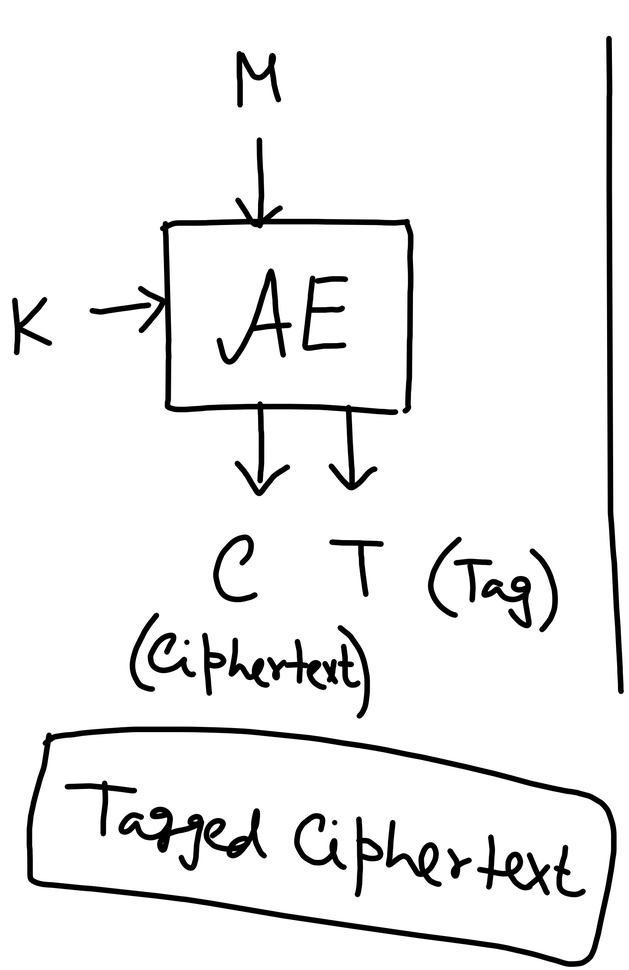
$$\approx 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \cdots \times \left(1 - \frac{22}{365}\right)$$

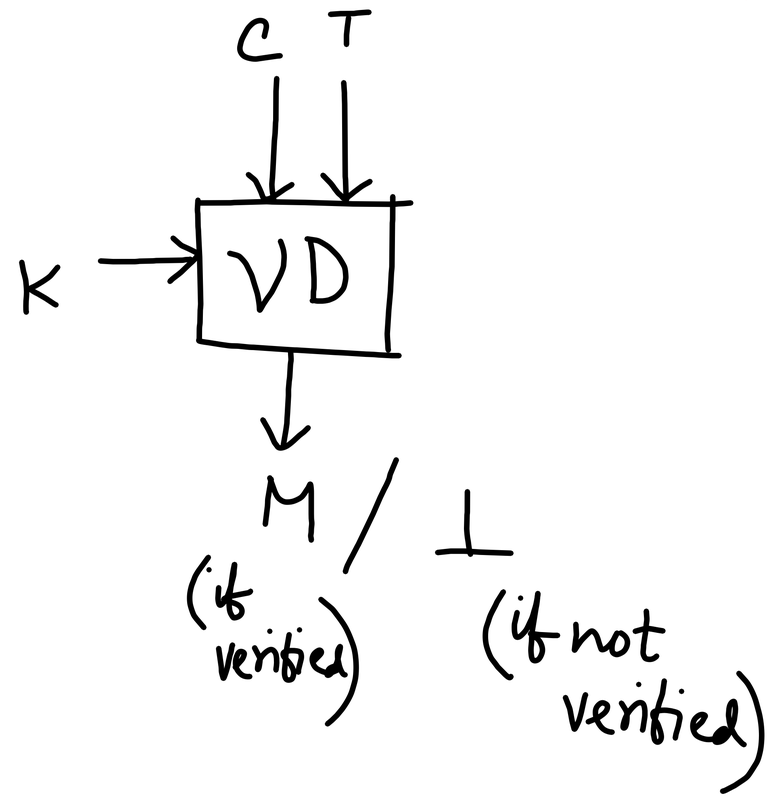
$$\left(1 - \frac{1+2+\cdots+22}{365}\right)$$

IND-CCA Motivation



Authenticated Encryption





VD → Verified decryption

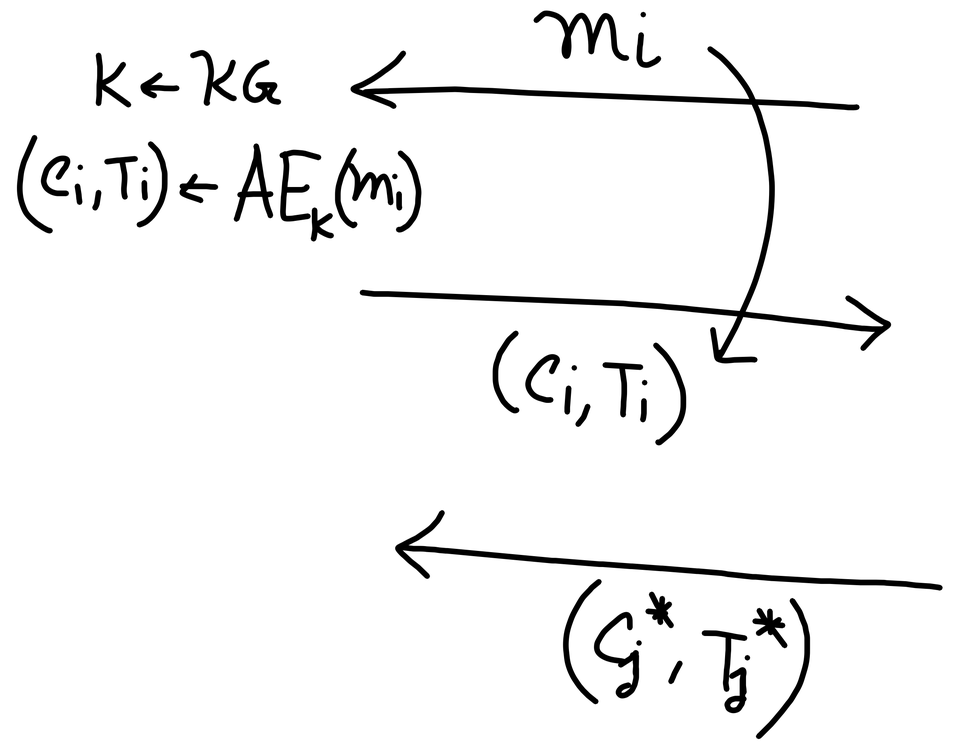
Security Notion

- IND-CPA Secure
- INT-CTXT Secure
  (Integrity under ciphertext)

} AE-Secure

$\Pi = (KG, AE, VD)$

INT-CTXT



$$Pr[A \text{ wins INT-CTXT Game}]$$

$$= Pr[(c_j^*, T_j^*) \text{ forges for at least one } j]$$

AE-Secure $\Longrightarrow$ CCA Security

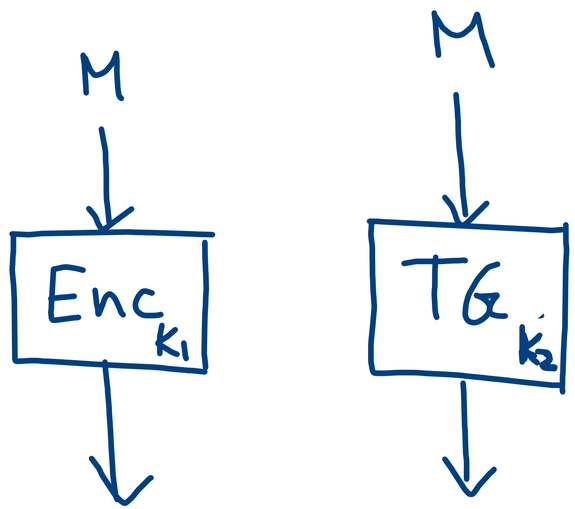
π is AE-secure

$\Rightarrow$ π is INT-CTXT secure

$\Rightarrow$ π can't make any (valid, fresh) forging query

π is CPA Secure + π can't make (Valid + fresh) forgery $\Longrightarrow$ IND-CCA

Generic Construction



Encrypt-and-MAC

$$\begin{cases} \Pi_1 = (KG_1, Enc, Dec) \\ \Pi_2 = (KG_2, TG, Vrfy) \end{cases}$$

$\Pi = (KG, AE, VD)$

$KG = (K_1, K_2)$ [K_1 is independent of K_2]

$AE = (Enc_{K_1}(M), TG_{K_2}(M))$

$VD(C^*, T^*) = \begin{cases} M^* \leftarrow Dec_{K_1}(C^*) & \text{if } T' == T^* \text{ return } M^* \\ T' \leftarrow TG_{K_2}(M^*) & \text{O/W return } \perp \end{cases}$

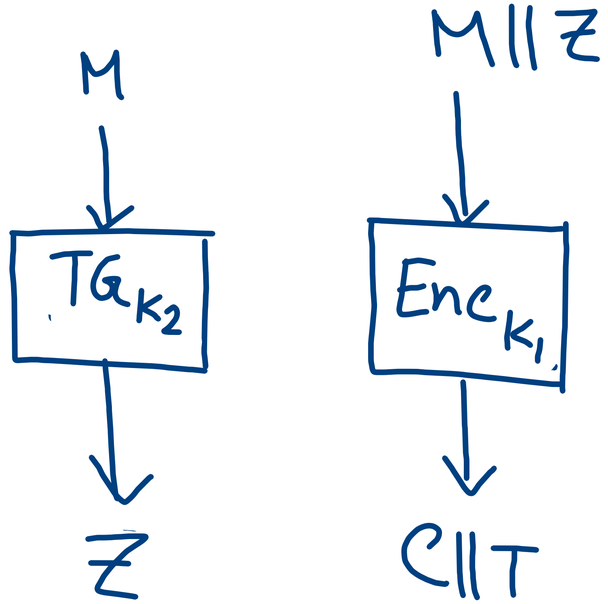
Not generically secure

↳ (Take any IND-CPA secure Π_1 & any SUF-CMA secure $\Pi_2 \Rightarrow \Pi$ with AE Security)

Example

$TG_{K_2}(M) = F_{K_2}(M) \| msb(M)$

Generic Construction



Not generically secure

↳ (Take any IND-CPA secure Π_1 & any SUF-CMA secure $\Pi_2 \Rightarrow \Pi$ with AE Security)

MAC-then-Encrypt

$$\begin{cases} \Pi_1 = (KG_1, Enc, Dec) \\ \Pi_2 = (KG_2, TG, Vrfy) \end{cases}$$

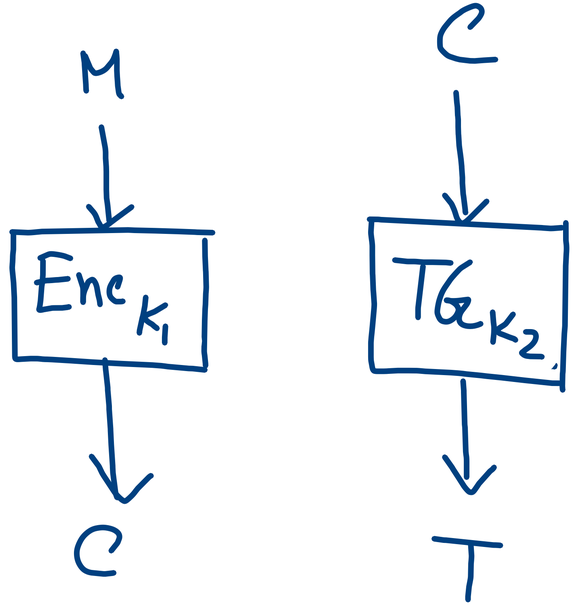
$\Pi = (KG, AE, VD)$

$KG = (K_1, K_2)$ [K_1 is independent of K_2]

$AE = Enc_{K_1}(M \| TG_{K_2}(M))$

$VD(C^*, T^*) = \begin{cases} M^* \| Z^* \leftarrow Dec_{K_1}(C^* \| T^*) \\ Z' \leftarrow TG_{K_2}(M^*) \end{cases}$ if $Z' == Z^*$ return M^*; O/W return $\perp$

Generic Construction



Encrypt-then-MAC

$$\begin{cases} \Pi_1 = (KG_1, Enc, Dec) \\ \Pi_2 = (KG_2, TG, Vrfy) \end{cases}$$

$$\Pi = (KG, AE, VD)$$

$KG = (K_1, K_2)$ [K_1 is independent of K_2]

$AE = (Enc_{K_1}(M), TG_{K_2}(Enc_{K_1}(M)))$

$VD(C^*, T^*) = \{ T' \leftarrow TG_{K_2}(C^*)$ if $T' = T^*$ return $Dec_{K_1}(C^*)$ o/w return $\perp$ $\}$

Generically Secure

↳ (Take any IND-CPA secure Π_1 & any SUF-CMA secure $\Pi_2 \Rightarrow \Pi$ with AE Security)