

Podcast ab 01:16:00

$\mathcal{L}_{\text{Eager}}$

```

for  $x \in \{0,1\}^K$  do
  Table  $T[x] \leftarrow \{0,1\}^K$ 

  Get( $x$ ) {
    return  $T[x]$ 
  }
    
```

$\mathcal{L}_{\text{Lazy}}$

```

for  $x \in \{0,1\}^K$  do
  Table  $T[x] \leftarrow \perp$  Null / False

  Get( $x$ ) {
    if  $T[x] \neq \perp$  then
      return  $T[x]$ 
    else
       $T[x] \leftarrow \{0,1\}^K$ 
      return  $T[x]$ 
  }
    
```

$\Rightarrow \mathcal{L}_{\text{eager}} \equiv \mathcal{L}_{\text{lazy}}$

The different time behavior is not relevant here.

A is often called a distinguisher.

↳ The program when L is linked to? or the Adversary?

Defining encryption security with Librar \mathcal{L}

Interchangeable librar \mathcal{L} \Leftrightarrow arbitrarily powerful Adversary A

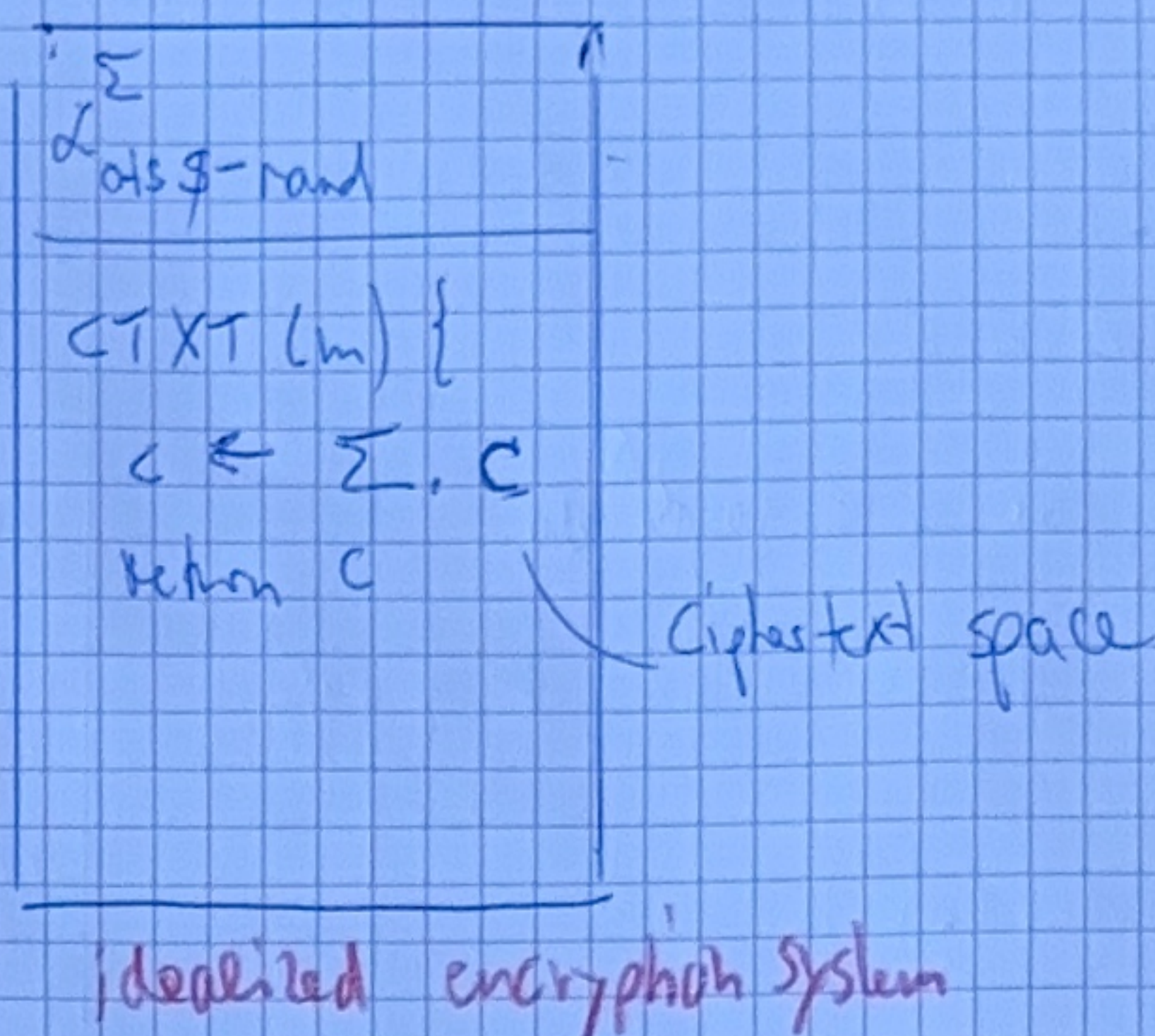
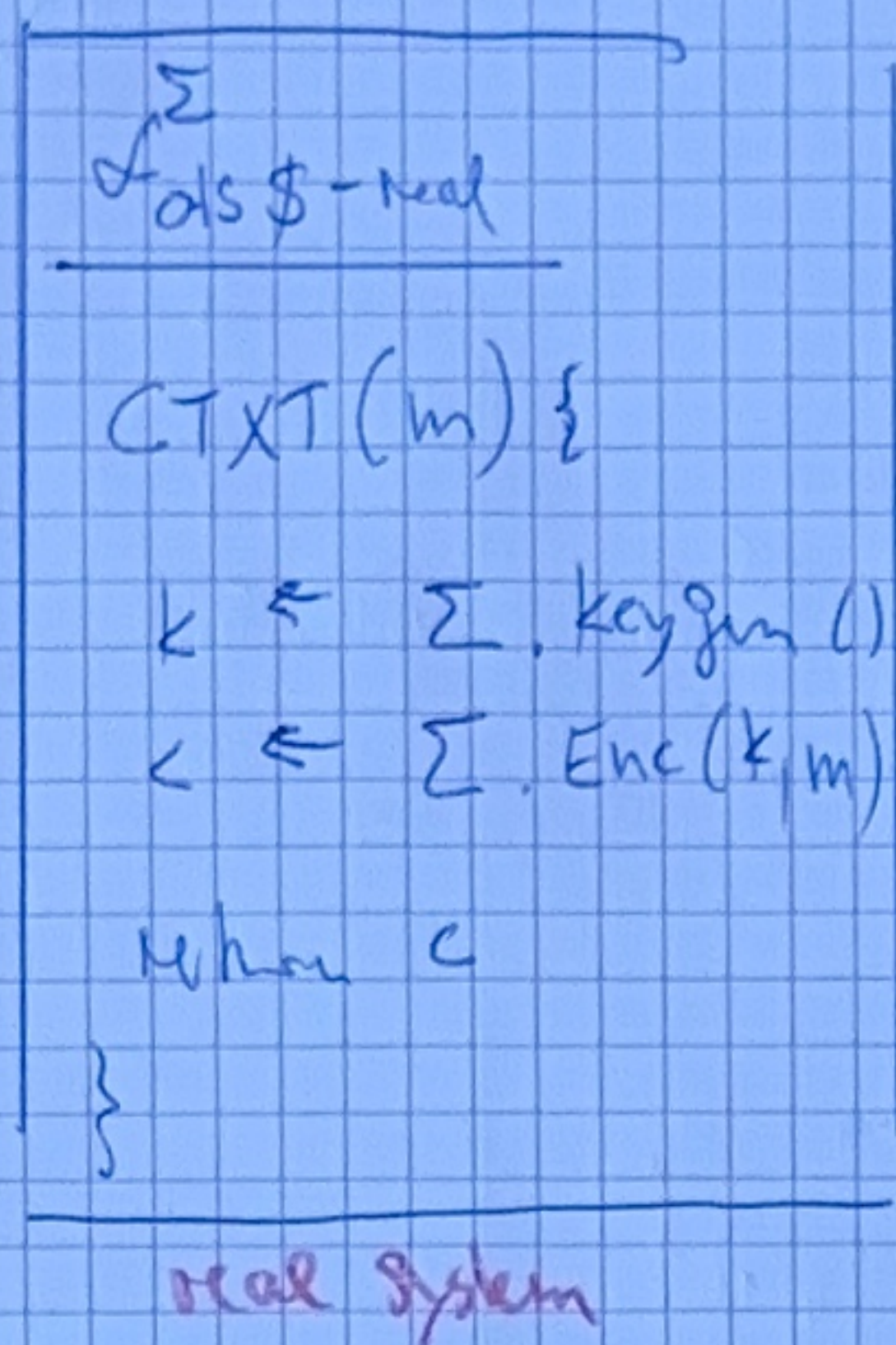
Remark: The OTP is indistinguishable from random generator, Thus two equal Librar \mathcal{L} .

Def An encryption scheme Σ has uniform ciphertext if

$$\mathcal{L}_{\text{otp } \$ - \text{real}} \equiv \mathcal{L}_{\text{otp } \$ - \text{rand}}$$

$\$ = \text{random}$
(flip coin)

otp & one time
Security



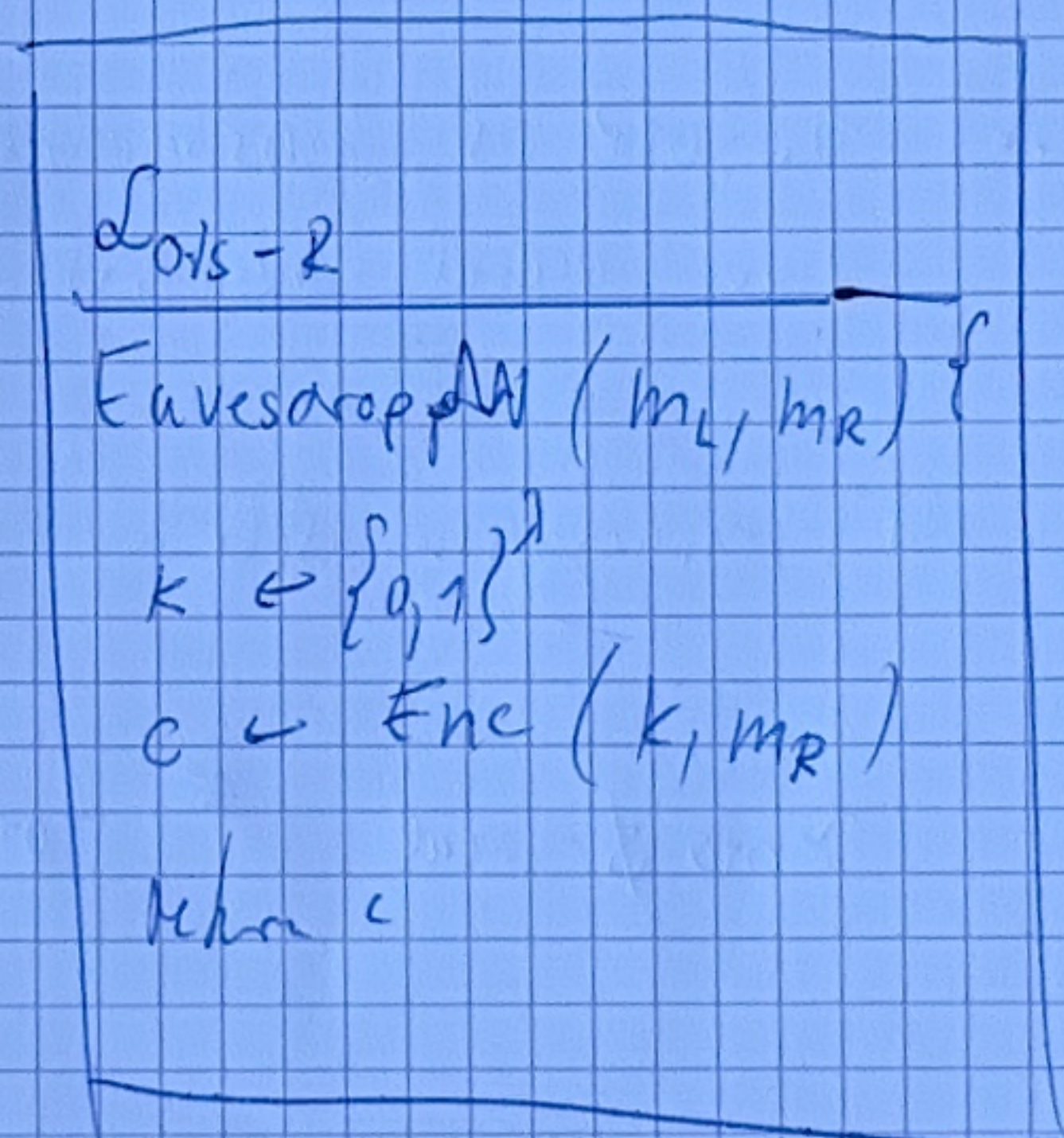
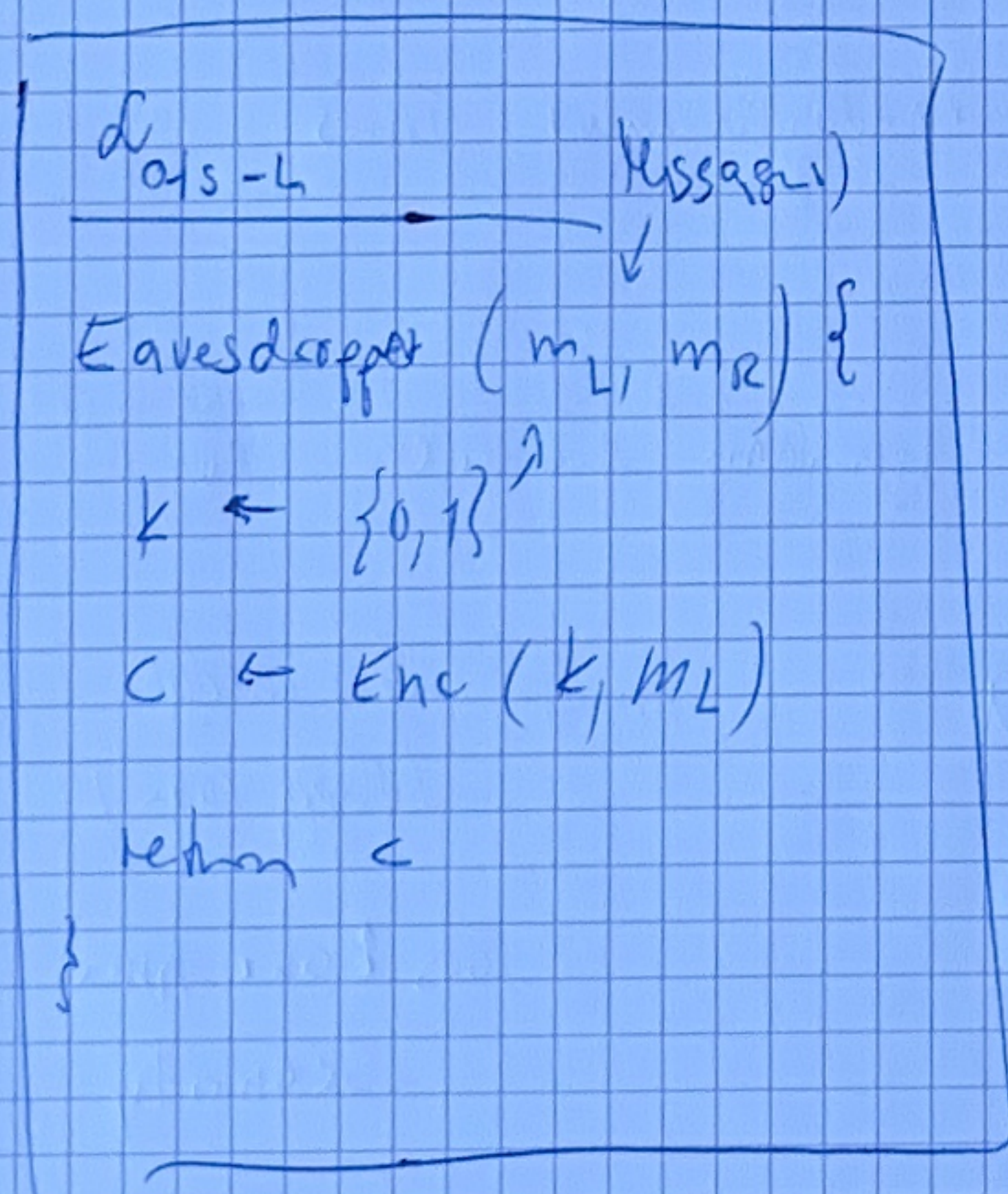
Example: $\text{Enc}(k, m) \rightarrow (m \oplus k) \parallel 0101$ (*)

here $\Sigma_{\text{ots} \S - \text{real}} \neq \Sigma_{\text{ots} \S - \text{rand}}$

but still secure. Thus need new notion.

\Rightarrow Notion good but too strong!

Def An encryption scheme Σ has one-time secrecy if

$$\mathcal{L}_{\text{ots-left}} \equiv \mathcal{L}_{\text{ots-right}}$$


This represents a best case for A

\Leftrightarrow

This is worst case for $\Sigma = (\text{keygen}, \text{Enc}, \text{Dec})$.

(*) this scheme has one time secrecy but not uniform distribution