Crypto MiHWoLL 26.2.2025

Podcast ab 01:16:00

$\mathcal{L}$ Eager

```
for x ∈ {0,1}^κ do
    Table T[x] ← {0,1}^λ
Gen(x) {
    return T[x]
}
```

$\mathcal{L}$ Lazy

```
for x ∈ {0,1}^κ do
    Table T[x] ← ⊥
Gen(x) {
    if T[x] ≠ ⊥ then
        T[x] ← {0,1}^λ
    return T[x]
}
```

NULL / False

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

The different time behavior is not relevant here.

$\mathcal{A}$ is often called a distinguisher.

↑ The Program when $\mathcal{L}$ is linked to? Or the Adversary?

Defining encryption security with Libraries

Interchangeable Libraries $\Leftrightarrow$ arbitrarily powerful Adversary $\mathcal{A}$

Remark: The OTP is indistinguishable from randomgenerator. Thus two equal Libraries.

Def An encryption scheme Σ has uniform ciphertext if

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

/ $\$$ = random (flip coin)

ots = one time security

$\mathcal{E}^{\Sigma}_{ots\$\text{-}real}$

CTXT(m) {

$k \xleftarrow{\$} \Sigma.keygen()$

$c \xleftarrow{\$} \Sigma.Enc(k, m)$

return c

}

real system

$\mathcal{E}^{\Sigma}_{ots\$\text{-}rand}$

CTXT(m) {

$c \xleftarrow{\$} \Sigma.\mathcal{C}$

return c

}

$\mathcal{C}$: ciphertext space

ideal encryption system

Example: $Enc(k, m) \to (m \oplus k) \| 0101$ (*)

here $\mathcal{E}^{\Sigma}_{ots\$\text{-}real} \not\equiv \mathcal{E}^{\Sigma}_{ots\$\text{-}rand}$

but still secure. This need new notion.

$\Rightarrow$ Notion good but too strong!

Def An encryption scheme Σ has one-time secrecy if

$$\mathcal{E}_{ots\text{-}Left} \equiv \mathcal{E}_{ots\text{-}R}$$

$\mathcal{E}_{ots\text{-}L}$

Eavesdropper(m_L, m_R) {

$k \xleftarrow{\$} \{0,1\}^{\lambda}$

$c \leftarrow Enc(k, m_L)$

return c

}

$\mathcal{E}_{ots\text{-}R}$

Eavesdropper(m_L, m_R) {

$k \xleftarrow{\$} \{0,1\}^{\lambda}$

$c \leftarrow Enc(k, m_R)$

return c

}

This represents a best case for $\mathcal{A}$

$\Leftrightarrow$

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

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