# Provable Security Concepts

expect HW1 release later today

## Recap:

libraries, calling programs / distinguishers

interchangeable : $\mathcal{L}_1 \equiv \mathcal{L}_2$ means $\forall A$:

$$\Pr[A \diamond \mathcal{L}_1 \text{ outputs } 1] = \Pr[A \diamond \mathcal{L}_2 \text{ outputs } 1]$$

"no program behaves differently in presence of $\mathcal{L}_1$ vs $\mathcal{L}_2$"

## Prime Directive

want to say "some info hidden from attacker"?

- Design 2 libraries, same interface
- interface capture what attacker can do
- difference between libs is info you want to hide

If libs interchangeable ⇒ info hidden from attacker

**Def:** $\Sigma$ has one-time secrecy if

$$\boxed{\begin{array}{l}\underline{\text{QUERY}(m_L, m_R):} \\ \quad k \leftarrow \Sigma.\text{KeyGen} \\ \quad \text{return } \Sigma.\text{Enc}(k, m_L)\end{array}} \equiv \boxed{\begin{array}{l}\underline{\text{QUERY}(m_L, m_R):} \\ \quad k \leftarrow \Sigma.\text{KeyGen} \\ \quad \text{return } \Sigma.\text{Enc}(k, m_R)\end{array}}$$

one-time secrecy ⇒ when Adv sees enc of chosen ptxts [interface]

choice of ptxt is hidden [diff. in libs]

**Ex:** (2.5) Prove that this scheme does <u>NOT</u> satisfy one-time secrecy

| | | |
|---|---|---|
| $\mathcal{K} = \{1, \ldots 9\}$ | <u>KeyGen</u> | <u>Enc(k,m)</u> |
| $\mathcal{M} = \{1, \ldots 9\}$ | $k \leftarrow \mathcal{K}$ | $c = k \cdot m \bmod 10$ |
| $\mathcal{C} = \{0, \ldots 9\}$ | ret $k$ | ret $c$ |

In other words, show a distinguisher for

```
QUERY(m_L, m_R):
  k ← {1,.. 9}
  ret k · m_L mod 10
```

&

```
QUERY(m_L, m_R):
  k ← {1,.. 9}
  ret k · m_R mod 10
```

distinguisher is a program that calls this interface and outputs 1 bit ("guess" of which lib)

**Obs:** $\text{Enc}(k, \boxed{1})$ is never $0$ (no overflow mod 10)
$\text{Enc}(k, \boxed{2})$ can be $0$ ? (e.g., $k=5$)

A:

```
c = QUERY(1, 2)            // c is either Enc of 1 or 2
if c = 0 then return 1     // return c==0
         else return 0
```

In presence of left library:

```
c = QUERY(1,2)      QUERY(m_L, m_R):
ret c==0        ◇     k ← {1...9}
                      ret k · m_L % 10
```

c is never $0$

$\Pr[\text{output true}] = 0$

In presence of right library:

$c$ is Enc of $\boxed{2}$

| $c = \text{QUERY}(1,2)$ | $\diamond$ | $\text{QUERY}(m_L, m_R)$: |
|---|---|---|
| ret $c == 0$ | | $k \leftarrow \{1 \ldots 9\}$ |
| | | ret $k \cdot m_R \% 10$ |

$\Pr[\text{output true}]$
$= \Pr[c = 0]$
$= \Pr[k = 5] = \frac{1}{9}$

Different output probabilities in presence of 2 libraries $\Rightarrow$ NOT interchangeable

---

Ex: Modify OTP to avoid all-zeroes key

(in OTP, if $k = 00\cdots00$, then ctxt reveals ptxt in the clear!)

Show that these are NOT interchangeable

all strings except $00\cdots00$

| $\text{QUERY}(m_L, m_R)$: | $\text{QUERY}(m_L, m_R)$: |
|---|---|
| $k \leftarrow \{0,1\}^\lambda \setminus \{0^\lambda\}$ | $k \leftarrow \{0,1\}^\lambda \setminus \{0^\lambda\}$ |
| ret $k \oplus m_L$ | ret $k \oplus m_R$ |

Obs: If $m = 00\cdots00$ then $c$ can't be $00\cdots00$

(generally: $\text{Enc}(k, m)$ can never equal $m$)

## Calling Prog:

A
$$\boxed{\begin{array}{l} c = \text{QUERY}(0^\lambda, 1^\lambda) \\ \text{return } c == 0^\lambda \end{array}}$$

In presence of Left library:

c is Enc of $0^\lambda$

$\Rightarrow$ c is NEVER $0^\lambda$

$\Rightarrow \Pr[\text{output true}] = 0$

Right library:

c is Enc of $1^\lambda$

$\Rightarrow \Pr[\text{output true}]$

$= \Pr[c = 0^\lambda]$

$= \Pr[k = 1^\lambda] = \dfrac{1}{2^\lambda - 1}$

$\Rightarrow$ <u>Diff</u> behavior in presence of 2 libraries