Lec 7 Idealized Models and Indifferentiability.

Random Oracle (RO)

abstracts a deterministic "looks random" function

Random Permutation (RP)

Ideal Cipher

abstracts "random looking" block cipher

Motivations:

- keyless hash function
- Key derive
- Key-dependent message attack
- Related-key attacks
- Real-world crypto construction (AES)
- Multi-party,
  Zero-knowledge Proof.

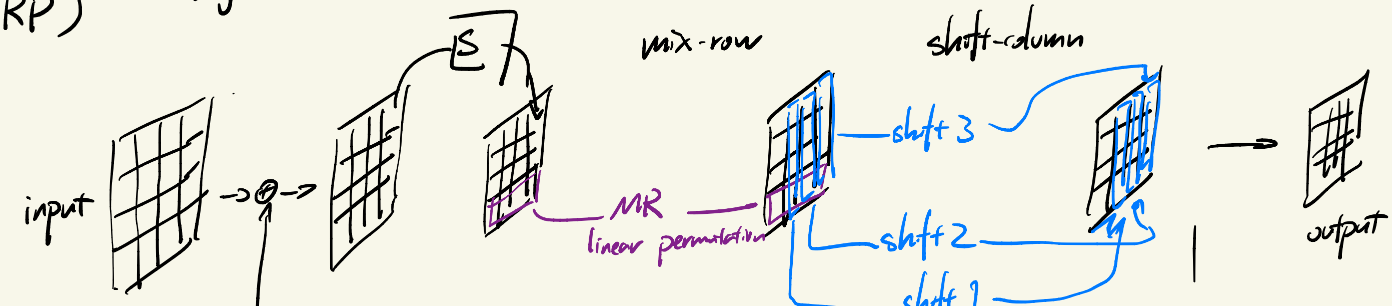
AES (Advanced Encryption Standard)

$128 = 16 \times 8$

128 bits $= 16$ bytes

block cipher: $\underbrace{\{0,1\}^{128/192/256}}_{\text{key}} \times \{0,1\}^{128} \to \{0,1\}^{128}$

($\approx$ PRP)



4x4 bytes

round key

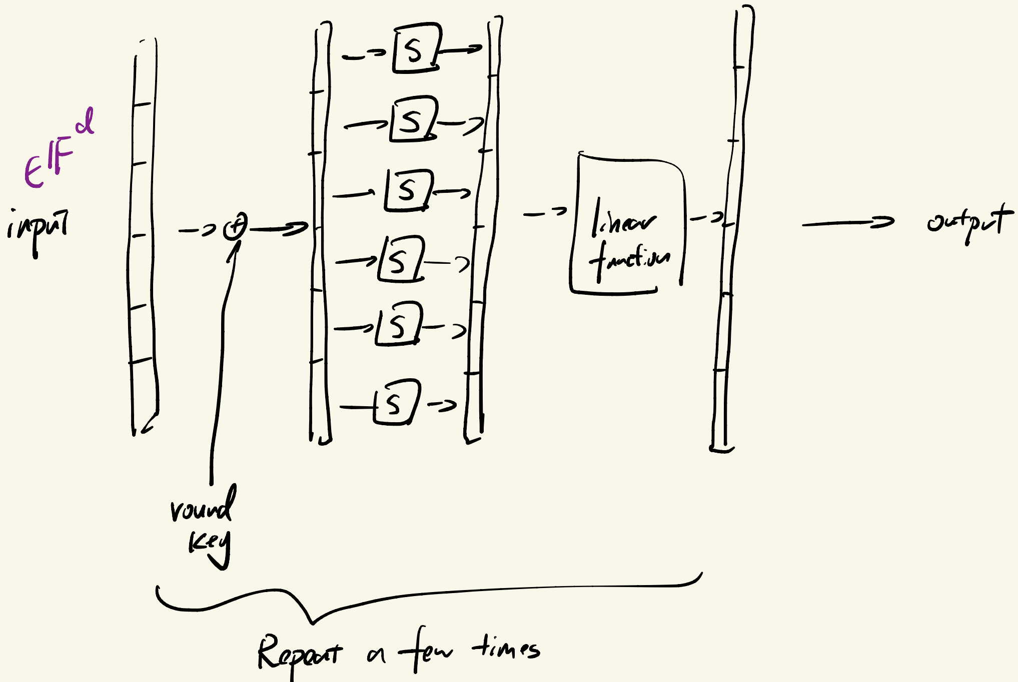
$S: \{0,1\}^8 \to \{0,1\}^8$

$x \mapsto \begin{cases} x^{-1} & \text{in } \mathbb{F}_{2^8} \\ 0 & x=0 \end{cases}$

Repeat 10 times

SPN

Substitution-Permutation Network



E.g. Encryption Scheme in Random Oracle Model

Random Oracle $O: \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$

$$\mathrm{Enc}(k, m) = (r,\ m \oplus O(k, r))$$

is secure against $\begin{cases} \text{non-uniform sampled key} \\ \text{key-dependent Msg attack} \\ \text{related key attack} \end{cases}$

"Construction" of idealized objects

Given Random permutation $P:\{0,1\}^\lambda \to \{0,1\}^\lambda$ $\quad P^{-1}$

Want Random Oracle $O:\{0,1\}^\lambda \to \{0,1\}^\lambda$

Construction

Candidate $O(x)$ is not secure

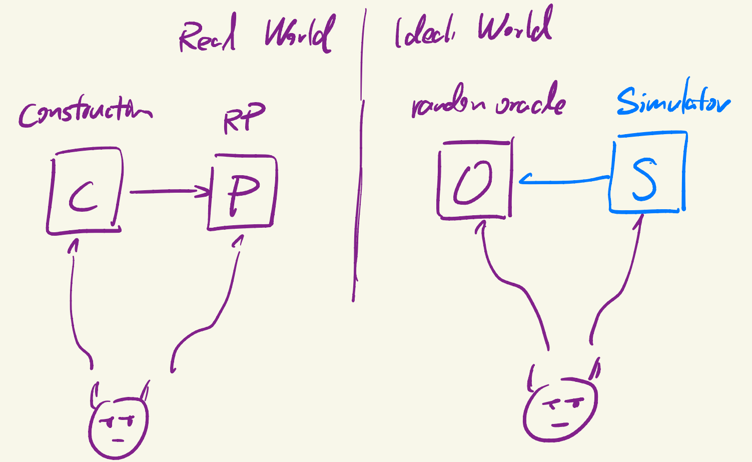
output $P(x) \oplus x$

Candidate $MAC(k, m)$ is secure

output $O(k \| m)$

Random Permutation Model

Random Oracle Model



INDIFFERENTIABILITY

initialize empty table $\tilde{P}$

upon query $P(x)$

let $\tilde{P}(x) = O(x) \oplus x$

upon query $P^{-1}(y)$

return x s.t.

$O(x) \oplus x = y$

"Construction" of idealized objects

Given Random Oracle $O_S : \{0,1\}^\lambda \to \{0,1\}$

Want Random Oracle $O_L : \{0,1\}^{\lambda - \log \lambda} \to \{0,1\}^\lambda$

Real World　　　Ideal World

Candidate Construction

$O_L(x)$

$= \left(O_S(x\|0),\ O_S(x\|1) \cdots,\ O_S(x\|\lambda-1)\right)$

$\mathrm{Sim}(x\|i)$

output i-th bit of $O_L(x)$

"Construction" of idealized objects

4-round Feistel is NOT

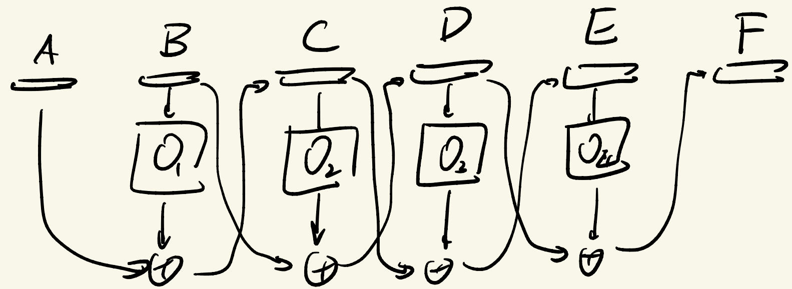
an indifferentiability secure construction of RP in RO model

Given Random Oracle $O_1, O_2, O_3, O_4 : \{0,1\}^\lambda \to \{0,1\}^\lambda$

Want Random permutation $P : \{0,1\}^{2\lambda} \to \{0,1\}^{2\lambda}$ P^{-1}

Feistel (A, B)

output (E, F)



AB	EF
$A'B'$	$E'F'$
$A''B''$	$E''F''$
$A'''B'''$	$E'''F'''$

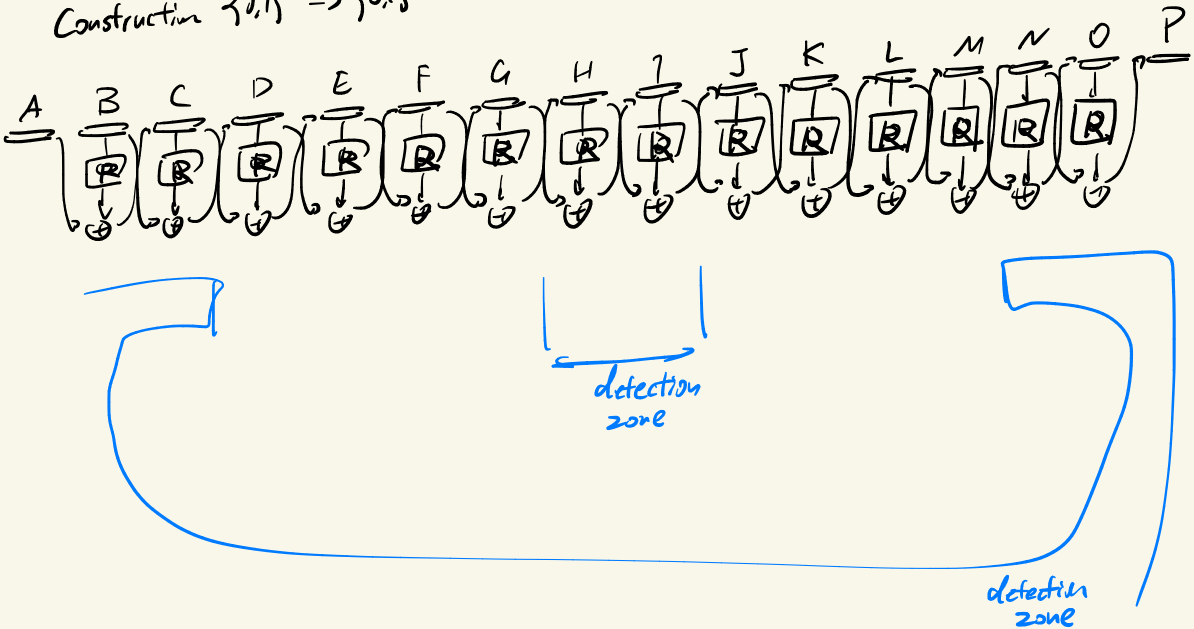
A	$B = O_2(C) \oplus D$	C	D	$E = O_3(D) \oplus C$	F
A''	$B'' = O_2(C) \oplus D'$	C	D'	$E'' = O_3(D') \oplus C$	F''
A'''	$B''' = O_2(C') \oplus D$	C'	D	$E''' = O_3(D) \oplus C'$	F'''
A'	$B' = O_2(C') \oplus D'$	C'	D'	$E' = O_3(D') \oplus C'$	F'

Real World

$R_1, R_2, \cdots, R_{14} : \{0,1\}^\lambda \to \{0,1\}^\lambda$

Construction $\{0,1\}^{2\lambda} \to \{0,1\}^{2\lambda}$

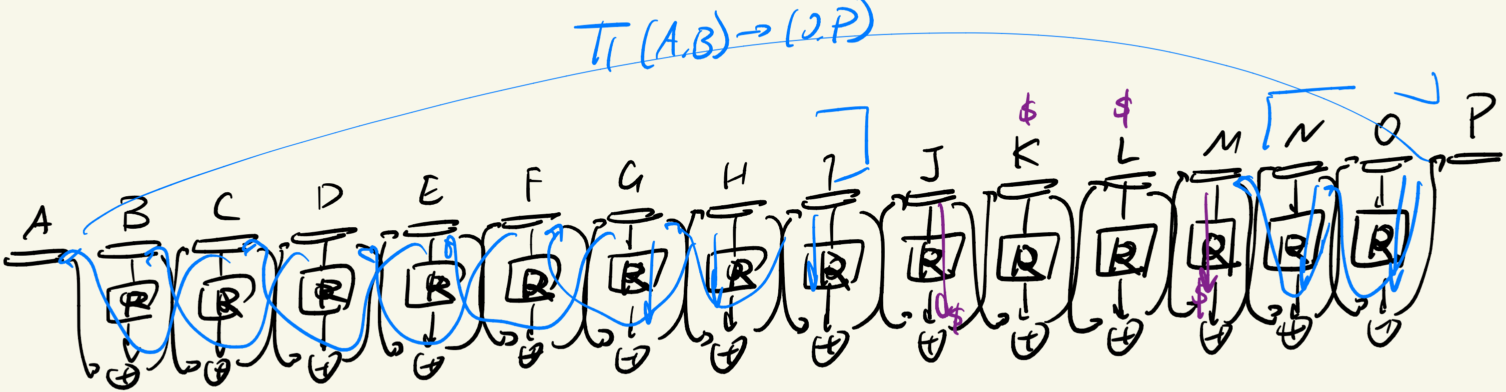
14-round Feistel is an indifferentiability secure construction of RP in RO model



Ideal World

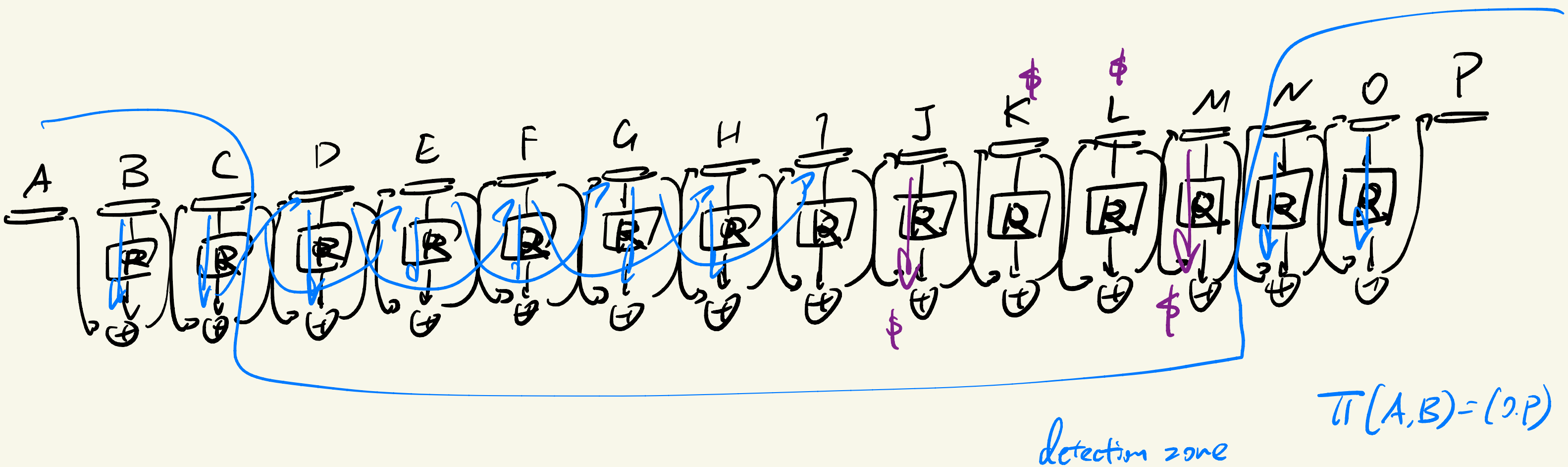
$\Pi : \{0,1\}^{2\lambda} \to \{0,1\}^{2\lambda}$

Simulator: $(S_1 \cdots S_{14})$

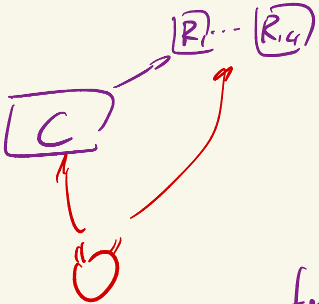


Set $R_0(K) = J \oplus L$

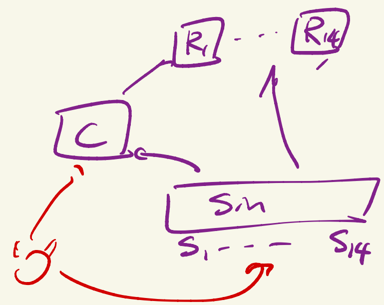
Set $R_1(L) = K \oplus M$



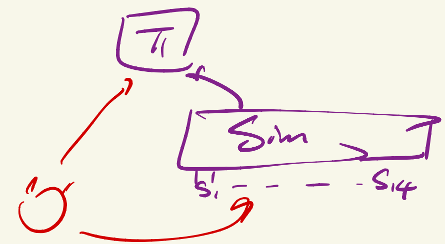
Real World



Hybrid World



Ideal World



footprint = (queried $R_1 \cdots R_{14}$)
$q_1 \cdots q_{14}$

footprint (queried $\overset{q}{\pi}$,
queried-and-randomly-sampled $R_1 \cdots R_{14}$)
$q_1' \cdots q_{14}'$

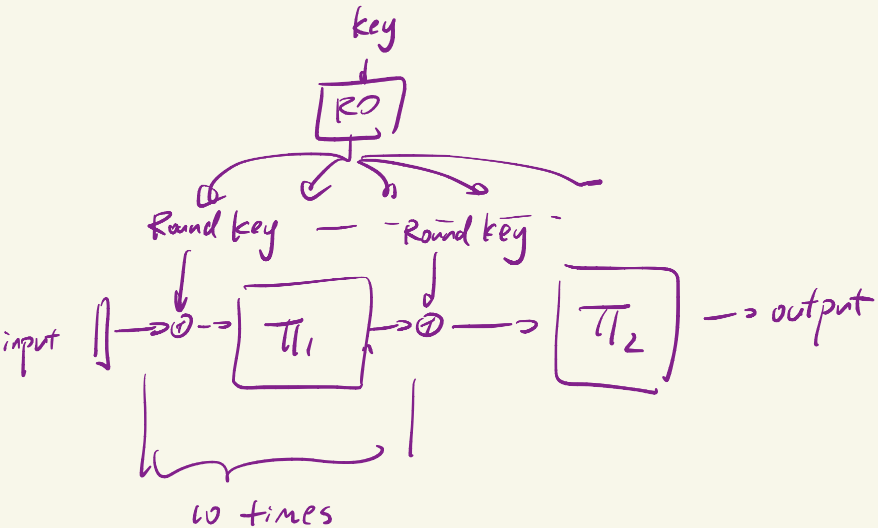
$$\Pr[\text{footprint}] = \frac{1}{2^{(q_1 + \cdots + q_{14})\lambda}} = \Pr[\text{footprint}] = \frac{1}{2^{(q_1' + \cdots + q_{14}')\lambda + q \cdot 2\lambda}}$$

$$(q_1 + \cdots + q_{14}) - (q_1' + \cdots + q_{14}') = 2q$$

Given Random Permutation / Random Oracle

Construct Idealized Cipher

10-round KAC is indifferentiability secure construction of IC in RO/RP model



Key-alternating cipher (KAC)