PSEUDORANDOM PERMUTATIONS.

Quick summary: PRF implies everything in symmetric crypto. ← EFFICIENTLY

Sometimes need PRP (i.e. modes of operation).

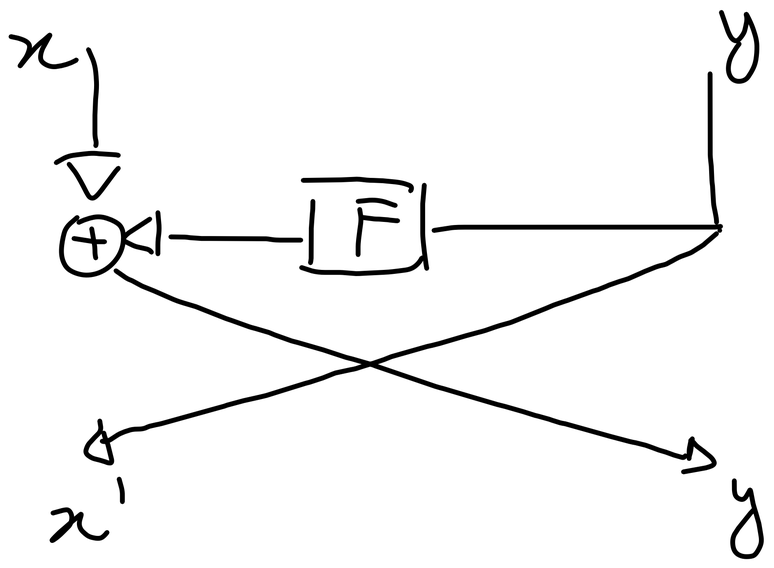
From theory: OWF ⇒ PRFs (⇒ PRP)

Practice: AES is a PRP. Make some "ad-hoc" PRF (only heuristic) and then use construction PRF ⇒ PRP.

LUBY-RACKOFF CONSTRUCTION:

$F: \{0,1\}^n \to \{0,1\}^n$

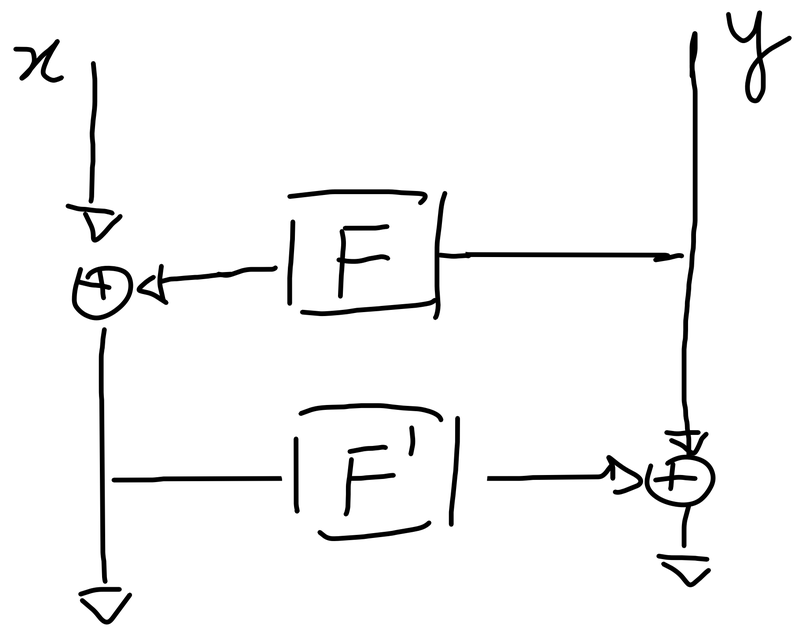
$$\psi_F(x,y) = (y, x \oplus F(y)) = (x', y')$$



FEISTEL (IBM) (1 ROUND)

$$\psi_F^{-1}(x',y') = (F(x') \oplus y', x') = (x, y)$$

Q: Is it PSEUDORANDOM? NO!



2 ROUND FEISTEL

$$\Psi_{F,F'}(x,y) = \Psi_{F'}(\Psi_F(x,y))$$

$x \oplus F(y)$

$y \oplus F'(x \oplus F(y))$

Q: Is it a PRP? NO

Look at 2 queries: (x,y) and (x',y) for $x \neq x'$.

$$\Psi_{F,F'}(x,y) \oplus \Psi_{F,F'}(x',y) = (x \oplus x', \text{———})$$

LUBY-RACKOFF: 3-ROUND WORKS!

THM Let F be a PRF. Then

$$\psi_F[3] = \psi_{F_{k_3}}\left(\psi_{F_{k_2}}\left(\psi_{F_{k_1}}(x,y)\right)\right)$$

for $k_1, k_2, k_3 \leftarrow\$ \{0,1\}^\lambda$

is a PRP.

Practice: F replaced by heuristic construct (SBOXES)

# of rounds: 18 times.

$k_1, \ldots, k_{18}$ all derived from single k.

Two steps:

1) If the queries are "y"-NIQUE, i.e. the y's are all distinct, then 7-ROUND FEISTEL is secure.

2) The first round makes queries "y"-NIQUE.

LEMMA. For every UNBOUNDED distinguisher STAT
asking $q(\lambda) = poly(\lambda)$ queries, the following are close:

→ S: $F, F' \leftarrow\$ \mathcal{R}(\lambda, n, n)$
and answer (x, y) with $\psi_{F'}(\psi_F(x, y))$

→ R: $R \leftarrow\$ \mathcal{R}(\lambda, 2n, 2n)$
and answer (x, y) with $R(x, y)$.

so long as $(x_1, y_1), \ldots, (x_q, y_q)$ are s.t. $y_i \neq y_j \quad \forall i \neq j$.

Proof. Hybrid argument : $H_i(\lambda)$ that answers the first i queries using S, and all other queries using R. $H_0 \equiv R$ and $H_q \equiv S$.

$\underline{H_i \approx_s H_{i-1}}$. The first i outputs of H_i:

$$\left(x_j \oplus F(y_j),\ y_j \oplus F'(x_j \oplus F(y_j))\right)_{j=1}^{i-1}$$

$$x_i \oplus F(y_i),\ y_i \oplus F'(x_i \oplus F(y_i)),\ \ldots,\ \ldots,\ \ldots$$

R

Proof. Hybrid argument : $H_i(1)$ that answers the first i queries using S, and all other queries using R. $H_0 \equiv R$ and $H_q \equiv S$.

$\underline{H_i \approx_s H_{i-1}}$. The first i outputs of H_i:

$$\left(x_j \oplus F(y_j),\ y_j \oplus F'(x_j \oplus F(y_j))\right)_{j=1}^{i-1}$$

$$x_i \oplus F(y_i),\ y_i \oplus F'(x_i \oplus F(y_i)),\ \ldots,\ \ldots,\ \ldots$$

R

By y-NIQUENESS, $F(y_i)$ IS RANDOM

and independent of the rest:

$$\left(x_i \oplus F(y_i),\ y_i \oplus F'\left(x_1 + F(y_1)\right)_{1=1}^{i-1}\right.$$

$$\left.\left(x_i \oplus r \quad ,\ y_i \oplus F'(x_i \oplus r)\right)\right)$$

What's the probability that $x_i \oplus r = x_j \oplus F(y_j)$?

For $j < i$ the prob. $\leq (i-1) \cdot 2^{-n}$. Assuming it does not happen:

$\rightarrow \left((x_i \oplus r),\ (y_i \oplus r')\right)$ which is $\equiv R(x_i, y_i)$.

By the lemma of game playing the distance between H_v and $H_{i-1} \leq (i-1) \cdot 2^{-m} = negl(\lambda)$.

$\hookrightarrow \Delta(S; R) \leq \sum (i-1) \cdot 2^{-m} \leq q^2 \cdot 2^{-m} = negl(\lambda)$ ∎

Proof (of THM). Consider:

- $T: (x, y) \mapsto \Psi_{F_{k_3}}(\Psi_{F_{k_2}}(\Psi_{F_{k_1}}(x, y)))$
- $S: (x, y) \mapsto \Psi_{F, F'}(\Psi_{F''}(x, y))$
- $R: (x, y) \mapsto R(x, y)$ $\quad R \leftarrow\$ \mathcal{R}(\lambda, 2m, 2m)$
- $P: (x, y) \mapsto P(x, y)$ $\quad P \leftarrow\$ \mathcal{P}(\lambda, 2m, 2m)$.

$\hookrightarrow P \in$ PERMUTATION

By the lemma of game playing the distance between H_N and $H_{i-1} \leq (i-1) \cdot 2^{-m} = negl(\lambda)$.

$\hookrightarrow \Delta(S; R) \leq \sum (i-1) \cdot 2^{-m} \leq q^2 \cdot 2^{-m} = negl(\lambda)$ ☑

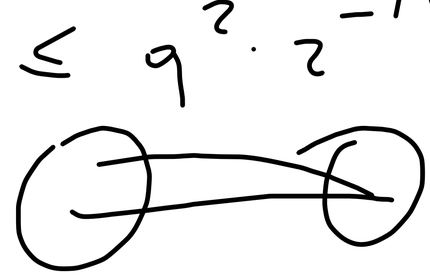
Proof (of THM). Consider:

- $T: (x, y) \mapsto \psi_{F_{k_3}}(\psi_{F_{k_2}}(\psi_{F_{k_1}}(x, y)))$
- $S: (x, y) \mapsto \psi_{F,F'}(\psi_{F''(x,y)})$ $\quad F, F', F'' \leftarrow\$ Q(n,n)$
- $R: (x, y) \mapsto R(x, y)$ $\quad R \leftarrow\$ \mathcal{R}(\lambda, 2n, 2n)$
- $P: (x, y) \mapsto P(x, y)$ $\quad P \leftarrow\$ \mathcal{P}(\lambda, 2n, 2n)$.

$\hookrightarrow P \in$ PERMUTATION

By the lemma of game playing the distance between H_N and $H_{i-1} \leq (i-1) \cdot 2^{-m} = negl(1)$.

$\hookrightarrow \Delta(S; R) \leq \sum (i-1) \cdot 2^{-m} \leq q^2 \cdot 2^{-m} = negl(1)$



Proof (of THM). Consider:

- $T: (x,y) \mapsto \Psi_{F_{k_3}}(\Psi_{F_{k_2}}(\Psi_{F_{k_1}}(x,y)))$
- $S: (x,y) \mapsto \Psi_{F,F'}(\Psi_{F''(x,y)})$, $F,F',F'' \leftarrow\$ Q(n,m)$
- $R: (x,y) \mapsto R(x,y)$ $\quad R \leftarrow\$ \mathcal{R}(\lambda, 2m, 2m)$
- $P: (x,y) \mapsto P(x,y)$ $\quad P \leftarrow\$ \mathcal{P}(\lambda, 2m, 2m)$.

$\hookrightarrow P \in$ PERMUTATION

LEMMA $T \approx_c S$.

Proof. Hybrid argument: $T \equiv H_0 \approx_c H_1 \approx_c H_2 \approx_c H_3 \equiv S$

H_1 : $\psi_{F_{k_3}}(\psi_{F_{k_2}}(\psi_{F''}(x,y)))$

H_2 : $\psi_{F_{k_3}}(\psi_{F'}(\psi_{F''}(x,y)))$

H_3 : S ; T : $\psi_{F_{k_3}}(\varphi_{F_{k_2}}(\varphi_{F_{k_1}}(\cdot,\cdot)))$

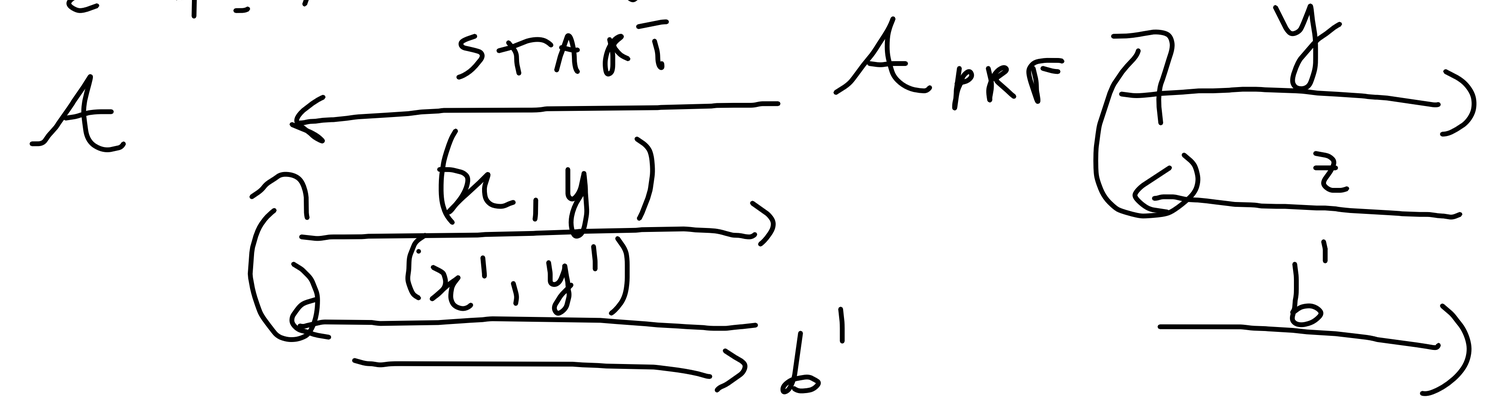
$n \to n$

$F''(\cdot)$

$\mathcal{C}_{PRF}$

$F_{k_1}(\cdot)$

$H_0 \approx_c H_1$. Assume not...



$(y, x \oplus z) \leftarrow \begin{cases} \psi_{F''}(x, y) \\ \psi_{F_{k_1}}(x, y) \end{cases}$

$\psi_{F''}(x, y) = (y, x \oplus F''(y))$

$\psi_{F_{k_1}}(x, y) = (y, x \oplus F_{k_1}(y))$

$k_2, k_3 \leftarrow\$ \{0,1\}^\lambda$

$(x', y') = \psi_{F_{k_3}}\left(\psi_{F_{k_2}}(y, (x \oplus z))\right)$ ☒

LEMMA $S \approx_c R$.

Proof. By the lemma we proved last time

$S \approx_c R$ if the inputs (x_i, y_i) are y-unique $\rightarrow$ to $\psi_F(\psi_{F'}(\cdot,\cdot))$

So, we show that for every A the prob. that $\psi_{F''}(x,y)$ is not "y"-unique is $negl(\lambda)$.

$\psi_{F''}(x_i, y_i)$ Take $(x_i, y_i) \neq_b (x_j, y_j)$ two queries.

$= (x_i'', y_i'')$ If $y_i = y_j$ then $x_i \neq x_j$:

$$y_i'' = x_i \oplus F''(y_i) = x_i \oplus F''(y_j) \neq x_j \oplus F''(y_j) = y_j''$$

Else $y_i \neq y_j$, then we are interested in the event:

$$x_i \oplus x_j = F''(y_i) \oplus F''(y_j) \leftarrow \text{RANDOM as } y_i \neq y_j$$

$$\Rightarrow \Pr[\, y_i'' = y_j'' \,] \leq 2^{-n}$$

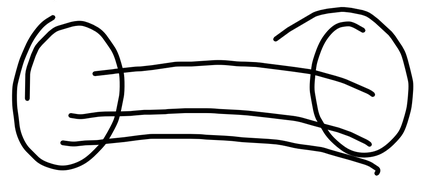
$$\Rightarrow \Pr[\neg\ y\text{-UNIQUE}] \leq \binom{q}{2} \cdot 2^{-n} = \mathrm{negl}(\lambda)$$

assuming $q = \mathrm{poly}(\lambda)$.

y-UNIQUE: $\forall\ (x_1, y_1), \ldots, (x_q, y_q)$ (distinct)

$$y_i'' \neq y_j''$$

where y_i'' is the y-part of $\psi_{F''}(x_i, y_i)$



LEMMA. $R \approx P$.

Proof. The only way to distinguish is to find $(x_i, y_i) \neq (x_j, y_j)$ s.t. $R(x_i, y_i) = R(x_j, y_j)$.

This only happens w.p. $\leq \binom{q}{2} \cdot \mathrm{negl}(\lambda) = \mathrm{negl}(\lambda)$. ∎