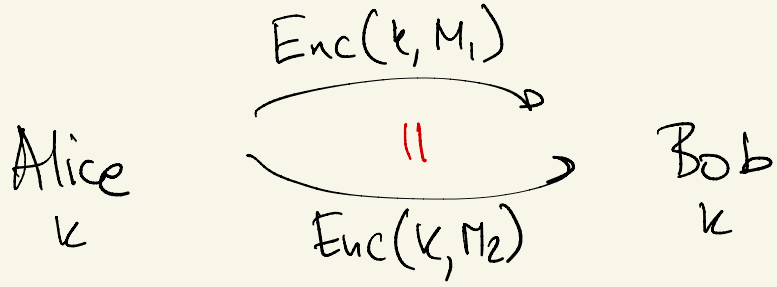
MULTIPLE ENCRYPTIONS

$Enc(k, M) = G(k) + M$ $\quad$ $Dec(k, C) = G(k) + C$

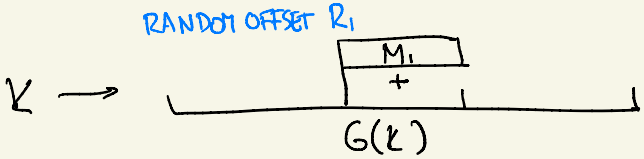
WHAT IF WE WANT TO ENCRYPT 2 MESSAGES?



$M_1 = M_2 = 0^m$ DISTINGUISHABLE FROM $0^m = M_1 \neq M_2 = 1^m$

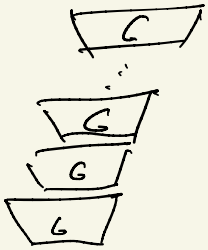
ENCRYPTION MUST BE RANDOMIZED

S. MICALI $\quad$ S. GOLDWASSER



$Enc(k, M) = (R, M + G(k)_{R+1 \text{ TO } R+m})$, R RANDOM.

$Pr[R_1 = R_2] = \frac{1}{n}$ $\longrightarrow$ $Enc(\ldots, \frac{1}{n})$ - DISTINGUISHABLE



TAKES $\Omega(n)$ WORK TO GET $\approx n$ BITS

WANT $\Omega(n) \ll \frac{1}{\varepsilon} = n$ ✗

WANT EXPONENTIALLY MANY PSEUDORANDOM BITS IN POLYNOMIAL TIME

↖ COMPUTE $G(k)_\ell$ DIRECTLY WITHOUT $G(k)_1, \ldots, G(k)_{\ell-1}$

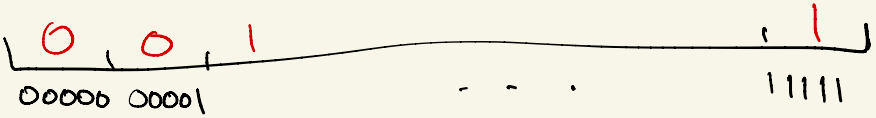
~~PSEUDO~~RANDOM FUNCTIONS

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

$F(00110) = 0$

$F(11011) = 0$

WHAT IS A RANDOM FUNCTION?

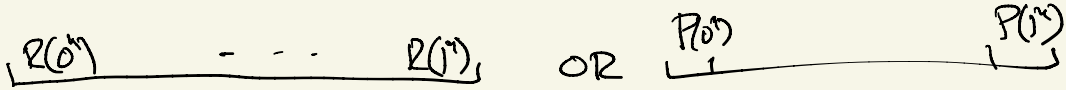


A RANDOM LIST OF 2^n VALUES

CIRCUIT FOR A RANDOM FUNCTION

ANY CIRCUIT THAT COMPUTES A RANDOM FUNCTION $\{0,1\}^n \to \{0,1\}$ MUST HAVE SIZE $\geq 2^n$. ← INFEASIBLE

P: INDISTINGUISHABLE FROM RANDOM BUT CAN BE COMPUTED BY A SMALL CIRCUIT.

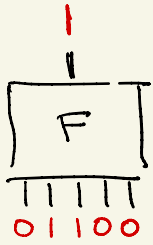


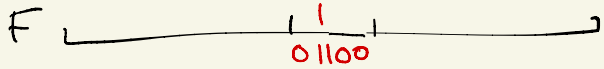
ALLOW DISTINGUISHER TO QUERY F

NEEDS TO DISTINGUISH F=R FROM F=P.

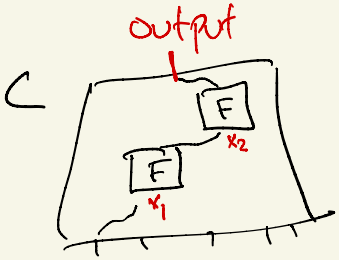
$F(10011) =$ 0 → $F(01000) = 0$; 1 → $F(11100) = 1$

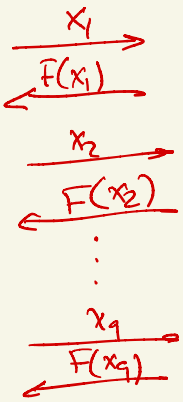
EXTEND DEF. OF CIRCUIT WITH SPECIAL ORACLE GATES





EACH ORACLE GATE COUNTS TOWARDS SIZE.





$F = P$ EFFICIENT

$F = R$ (RANDOM)

RANDOM COIN

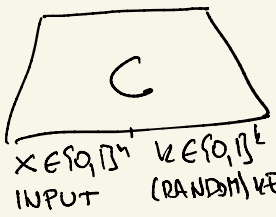
RANDOM COIN IF $x_2 \neq x_1$

VIEW OF C^F = $(F(x_1), \ldots, F(x_q))$ + C'S INPUT AND RANDOMNESS.

F RANDOMIZED $\longrightarrow$ VIEW IS A RANDOM VARIABLE

Definition $P : \{0,1\}^n \to \{0,1\}^m$ IS (S,ε)-PSEUDORANDOM IF FOR ANY ORACLE CKT D OF SIZE $\leq S$ THE VIEWS D^P AND D^R ARE (S,ε)-INDISTINGUISHABLE WHERE R IS A RANDOM FUNCTION.

P WILL BE IMPLEMENTED BY A EFFICIENT RANDOMIZED CIRCUIT C



$$P(x) = P_k(x) = C(k, x)$$

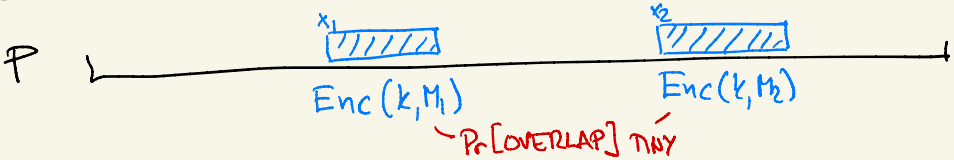
(EFFICIENT) IMPLEMENTATION OF P

(SHORT) DESCRIPTION OF P

DESCRIBE P USING k BITS ($k = \text{poly}(n)$)

IN CONTRAST R REQUIRES 2^n BITS

TO ENCRYPT SET X = RANDOM OFFSET



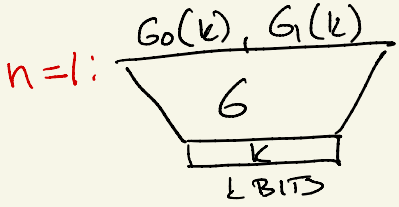
HOW TO CONSTRUCT A PRF

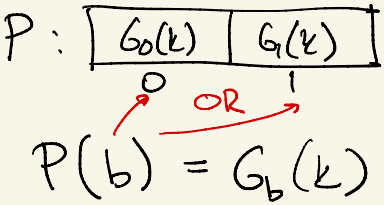
KEY $K = \{0,1\}^k$

INPUT $x \in \{0,1\}^n$

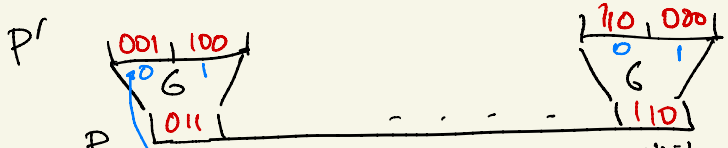
OUTPUT $P_k(x) \in \{0,1\}^k$

ASSUME I HAVE A PRG $G: \{0,1\}^k \to \{0,1\}^{2k}$





ASSUME $P : \{0,1\}^{n-1} \to \{0,1\}^k$ IS A PRF



$$P'(bx) = G_b(P(x))$$

NUMBER OF QUERIES $q \le s$.

Lemma. IF P IS (s, q, ε)-PRF AND G IS A (s', q', ε')-PRG THEN P' IS A $(s'', q'', \varepsilon'')$-PRF.

REPEAT n TIMES: $P: \{0,1\} \to \{0,1\}^k \longrightarrow$

$P': \{0,1\}^2 \to \{0,1\}^k \longrightarrow \dots \longrightarrow P'': \{0,1\}^n \to \{0,1\}^k$

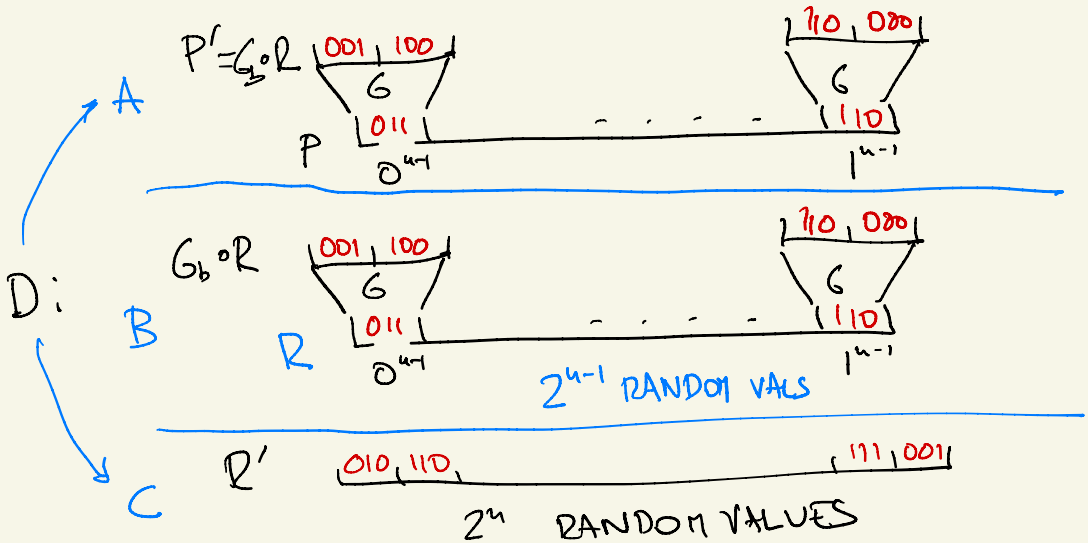
$$P'(x_1 x_2 \cdots x_n) = G_{x_1}(G_{x_2}(\cdots G_{x_n}(k)\cdots))$$

Goldreich-Goldwasser-Micali PRF

$$size(P') \approx n \cdot size(G)$$

O. GOLDREICH (WIKIPEDIA)

PROOF IDEA IF I CAN BREAK P' → I CAN BREAK P OR I CAN BREAK G.



$$\left| Pr[D^{P'} = 1] - Pr[D^{R'} = 1] \right| > \varepsilon''$$

A C

THEN EITHER

(1) $\left| Pr[D^{P'} = 1] - Pr[D^{G_b \circ R}] = 1 \right| > \varepsilon$

OR

(2) $\left| Pr[D^{G_b \circ R} = 1] - Pr[D^{R'} = 1] \right| > \varepsilon'$

$\varepsilon = \varepsilon' + \varepsilon''$

① D DISTINGUISHES $G_b \circ P$ AND $G_b \circ R$

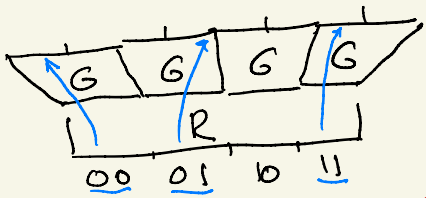
$D^{'F}$ $(F = P$ OR $R)$

WHEN D QUERIES ITS ORACLE AT (b,x), D' ANSWERS BY $D(G_b(F(x)))$.

IF D MAKES q QUERIES → D' MAKES q QUERIES → $q \cdot t$ EXTRA WORK

D' $(s''+qt, q, \varepsilon)$-DISTINGUISHES P FROM R.

② $n=3$



DEPENDENT

D: QUERIES AT 000, 101, 011, 100

OUTPUTS ARE INDEPENDENT B/C $R(00), R(01), R(11)$ ARE INDEPENDENT.

OBSERVES (PARTIAL) OUTPUTS OF G AT 3 INDEPENDENT INPUTS.

MODEL: D OBSERVES EITHER

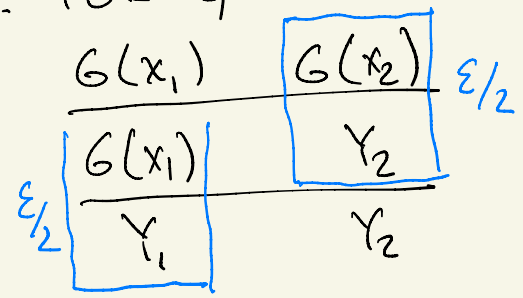
A': $G(x_1), \ldots, G(x_q)$ IND. RANDOM INPUTS

OR

B': $Y_1, \ldots, Y_q$ IND. UNIFORM

Lemma. IF A', B' ARE (s, ε) - DISTINGUISHABLE THEN $G(x), Y$ ARE $(s, \varepsilon/q)$ - DISTINGUISHABLE.

Proof idea. FOR $q = 2$



IN GENERAL, CAN ELIMINATE DEPENDENCES BY "MEMORIZING" ANSWERS

D QUERIES 000 → { D' QUERIES F(00) AND REMEMBERS BOTH $G_0(F(00))$ AND $G_1(F(00))$

size $(D') \approx$ size $(D) + O(q^2)$.

G IS NOT $(s + O(q^2), \varepsilon'/q)$ - PSEUDORANDOM.

$P: \{0,1\}^n \to \{0,1\}^m$ IS A PRF

$Enc(k, M) = (X, M + P_k(X))$

FOR X RANDOM

$Dec(X, C) = C + P_k(X)$

CHOSEN PLAINTEXT SECURITY

Eve HAS Enc_k ORACLE

$M_1 \to [Enc_k] \to Enc_k(M_1)$

$M_2 \to [Enc_k] \to Enc_k(M_2)$ (COULD DEPEND ON $Enc_k(M_1)$)

$\vdots$

} CAN SIMULATE WITHOUT KNOWING K

(s,q,ε)-SIMULATABLE IF $\forall$ D OF SIZE s THAT MAKES q QUERIES TO Enc_k, $\exists$ SIMULATOR Sim THE VIEW D^{Enc_k} IS (s,q,ε)-IND. FROM VIEW D^{Sim}.

Claim. P IS A PRF $\to$ (Enc, Dec) IS SIMULATABLE.

A $Enc_k(M) = (X, P_k(X)+M)$ X RANDOM

B $Enc'_R(M) = (X, R(X)+M)$ R RANDOM FN

C $Sim = (X, Y)$ X, Y RANDOM, INDEPENDENT ON EVERY QUERY

A, B: $D'^F = D$ ⟵ Encrypt M, ⟶ $(X, F(X)+M)$

B: $(X_1, R(X_1)+M_1)$ ... $(X_q, R(X_q)+M_q)$

C: (X_1, Y_1) ... (X_q, Y_q)

$X_1, \dots, X_q$; $Y_1, \dots, Y_q$ INDEPENDENT

IDENTICAL UNLESS $X_i = X_j$ FOR SOME $(i \neq j)$

$$\Pr[\exists i,j : X_i = X_j] \leq \sum \Pr[X_i \neq X_j] = \binom{q}{2} \cdot 2^{-n}$$

SO B, C ARE $(\infty, q, \binom{q}{2}2^{-n})$ - INDISTINGUISHABLE.

LEARNABILITY

UNKNOWN $f : \{0,1\}^n \to \{0,1\}$

TRY TO LEARN BASED ON EXAMPLES

x_1	$f(x_1)$
x_2	$f(x_2)$
⋮	
x_m	$f(x_m)$

TRAINING PHASE

x	PREDICT $f(x)$

TEST

MINIMAL REQUIREMENT: $x \neq x_i$ FOR ALL i

IF PRFs EXIST, THERE EXIST EFFICIENT f THAT CANNOT BE LEARNED.

Thm. IF P_k IS A $(s, q+1, \varepsilon)$-PRF FOR EVERY LEARNER L OF SIZE $\leq s$

$$\Pr\left[L^{P_k}(x) = P_k(x)\right] \leq \frac{1}{2} + \varepsilon.$$

FOR ANY CHOICE OF $x_1, \ldots, x_q, x$ AS LONG AS $x \neq x_i$ FOR ALL i.

Proof. SUPPOSE $\Pr\left[L^{P_k}(x) = P_k(x)\right] \geq \frac{1}{2} + \varepsilon$

DISTINGUISH P_k FROM R

x_1 ... x_q	x	OUTPUT
$F(x_1)$ ... $F(x_q)$	$F(x)$	$\begin{cases} 1 \text{ IF } L^F(x) = F(x) \\ 0 \text{ IF NOT} \end{cases}$

$$F = P_k \rightarrow P\left[D^{P_k} = 1\right] \geq \frac{1}{2} + \varepsilon$$

$$F = R \rightarrow P\left[D^{R} = 1\right] = P\left[L^{R}(x) = R(x)\right] = \frac{1}{2}$$