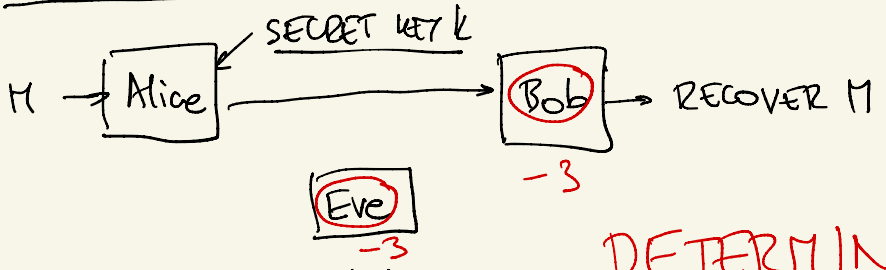
ENCRYPTION



hello → khoor

DETERMINISTIC

EVE CAN DO EVERYTHING BOB CAN DO.

- ADD RANDOMNESS

$+t \bmod 26$ WHERE t IS A RANDOM NUMBER

hello → ____

26

- FOR EVE TO ATTACK SHE HAS TO DO 26× AMOUNT OF WORK.

- INCREASE RANDOMNESS
  ① PERMUTE LETTERS RANDOMLY

Alice → Bob

buy, sell, sell, buy, buy

tpa tpa tpa

RANDOM SHIFT BY BLOCK

hello world
+ tuphtuphtu...

① RANDOMNESS IS NEEEDED ← SECRET KEY

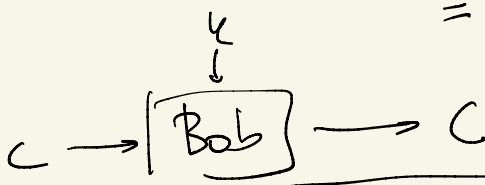
② NOT ENOUGH

CAN WE "HIDE" THE MESSAGE EVEN IF Eve HAS PARTIAL INFO?

$M \in \{0,1\}^m$ $\quad k = \{0,1\}^l$ RANDOM

ASSUME $m = k$: $\quad C = M + K \mod 2$

$= (M_1 + K_1, \ldots, M_2 + K_2)$.



$$M + K = C$$

FIXED RANDOM RANDOM

(Enc, Dec) IS PERFECTLY IND-SECURE IF $\forall M, M'$, $Enc(K, M)$ AND $Enc(K, M')$ ARE IDENTICALLY DISTRIBUTED. ✓

SIM-SECURE: Eve CAN SAMPLE C WITHOUT KNOWING M. ✓ UNIFORMLY RANDOM.

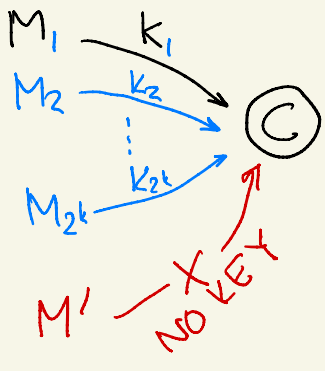
ISSUE? $k = m$ UNREALISTIC IF m IS LARGE ✗

IS $k < m$ POSSIBLE? NO.

$M \longrightarrow C = Enc(k, M)$

Eve

$M' \longrightarrow C' = Enc(k, M')$



M', M_1 DISTINGUISHABLE ← THERE EXISTS SOME OTHER

RELAXATION 1. $Enc(k, M)$ AND $Enc(k, M')$ NOT I.D. BUT MERELY "CLOSE".

X, X' ARE ε-STATISTICALLY CLOSE IF FOR ANY POSSIBLE TEST D THAT OUTPUTS yes OR no

$$\left| Pr[D(X) = yes] - Pr[D(X') = yes] \right| \leq \varepsilon$$

$\varepsilon = 0 \longrightarrow$ PERFECTLY INDISTINGUISHABLE

$\varepsilon = 1\% \longrightarrow$ 99% OF THE TIME CANNOT TELL APART.

EVEN $\varepsilon = \frac{1}{2}$ IMPOSSIBLE AS LONG AS $k < m$. ✗ BUT MAY BE COMPUTATIONALLY EXPENSIVE TO DO SO.

IDEAL: PERFECT SECURITY

RELAXED: STATISTICAL, COMPUTATIONAL ✓

CRYPTOGRAPHIC

$k = m-1 \quad \varepsilon = \frac{1}{2}$

$k = m-2 \quad \varepsilon = \frac{3}{4}$

$k \ll m \rightarrow \varepsilon = 1 - 2^{-(m-k)}$

CIRCUITS : MODEL OF EFFICIENT COMPUTATION

CIRCUIT = DIRECTED ACYCLIC GRAPH

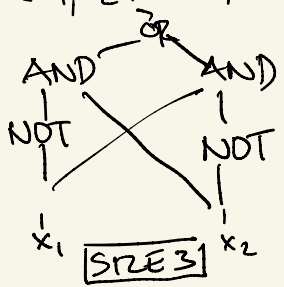
SOURCES : INPUTS

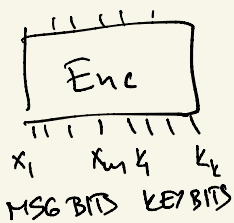
SINKS : OUTPUTS

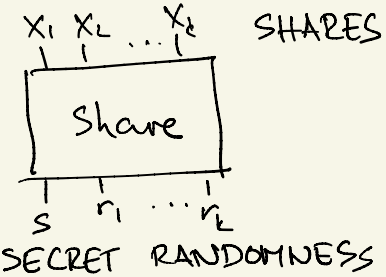
INTERNAL NODES : AND, OR, NOT GATES

$f(x_1, x_2) = x_1 \text{ XOR } x_2$

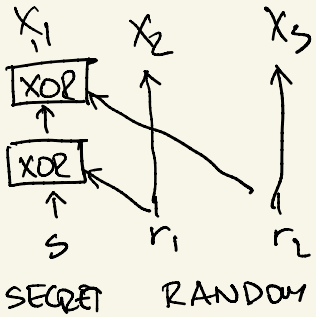
SIZE = NUMBER OF AND+OR GATES







Ex. Share(s): SAMPLE $X_1, X_2, X_3 \mid X_1 + X_2 + X_3 = s$



SIZE $= 2 \cdot$ SIZE (XOR)
$= 6.$

MEASURE OF EFFICIENCY

PROGRAMS VS. CIRCUITS

SIZE	RUNTIME		SIZE
s	t	$\rightarrow$	$O(st)$
$O(s)$	$O(s)$	$\leftarrow$	s

- C THAT TAKES NO REAL INPUT, ONLY RANDOMNESS IS A SAMPLER
- C THAT TAKES NO RANDOMNESS IS DETERMINISTIC

X AND X' OVER $\{0,1\}^k$ ARE (s,ε)-COMPUTATIONALLY INDISTINGUISHABLE IF FOR EVERY CIRCUIT $D:\{0,1\}^k \to \{0,1\}$ OF SIZE AT MOST s,

$$\left|\Pr[D(X)=1] - \Pr[D(X')=1]\right| \leq \varepsilon.$$

ε-STAT $\leftrightarrow$ (∞,ε)-COMP $\leftarrow$ $(2^k,\varepsilon)$-COMP

A CKT OF SIZE 2^k CAN COMPUTE ANY FUNCTION ON k BITS.

$s < 2^k/k$ $\rightarrow$ THERE EXIST FUNCTIONS THAT CANNOT BE COMPUTED BY CKTS OF SIZE s.

(Enc, Dec) IS (s,ε)-MESSAGE INDISTINGUISHABLE IF $\forall M M'$, $Enc(k,M)$ AND $Enc(k,M')$ ARE (s,ε)-COMPUTATIONALLY IND.

WHAT ARE REASONABLE VALUES FOR s AND ε?

k = "SECURITY PARAMETER"

THEORY: Alice, Bob RUN IN TIME POLYNOMIAL IN k
MAKE Eve DO "WORK" EXPONENTIAL IN k.
Ex. $s = 2^{k/3}$ OR $2^{\sqrt{k}}$.

s = AMOUNT OF WORK
ε = LUCK $K \in \{0,1\}^k$
Eve CAN ALWAYS RANDOMLY GUESS K.
GETS LUCKY WITH PROB 2^{-k}.
WANT ε NOT MUCH LARGER THAN THIS
Ex. $\varepsilon = 2^{-k/3}$ OR $2^{-\sqrt{k}}$.

RULE OF THUMB $\varepsilon \approx 1/s$ CAN CONVERT LUCK INTO WORK

Eve BREAKS 1 Enc w/p ε
t Enc w/p $1-(1-\varepsilon)^t \approx t\varepsilon$

PRACTICE $\varepsilon \approx \frac{1}{2^{80}}$ $s \approx 2^{80}$

SIMULATION-BASED DEFINITION

(Enc, Dec) IS (s,ε)-SIMULATABLE IN SIZE t IF THERE EXISTS A SAMPLER Sim OF SIZE t S.T. $\forall M$, OUTPUT OF Sim IS (s,ε)-INDISTINGUISHABLE FROM $Enc(k,M)$.

IND	SIM
$\lvert Pr[D(Enc(k,M))=1] - Pr[D(Enc(k,M'))=1] \rvert \le \varepsilon$	$\lvert Pr[D(Sim)=1] - Pr[D(Enc(k,M))=1] \rvert \le \varepsilon$

$\forall D$ OF SIZE $\le s$

$(s,\frac{\varepsilon}{2})$-NON-SIM'LITY $\longrightarrow$ (s,ε)-~~INDIST'LITY~~

↑ COMES FROM PROOF

CONTRAPOSITIVE ←

Proof IN CONTRAPOSITIVE

SUPPOSE Eve CAN DISTINGUISH ENCRYPTIONS

$$Pr[D(Enc(k,M))=1] - Pr[D(Enc(k,M'))=1] > \varepsilon.$$

FOR SOME PAIR M AND M'.

EITHER $Pr[D(Enc(k,M))=1] - Pr[D(Sim)=1] > \frac{\varepsilon}{2}$

OR $Pr[D(Sim)=1] - Pr[D(Enc(k,M'))] > \frac{\varepsilon}{2}$.

→ SIM IS DIST FROM EITHER $Enc(k,M)$ OR $Enc(k,M')$ BY SIZE s AND ADV. $\varepsilon/2$.

EVEN IF SIZE(SIM) $= \infty$

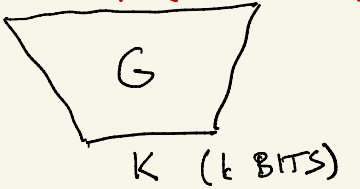
(s,ε) - INDIST'LITY → (s,ε) - SIM'LITY

SIM OUTPUTS $Enc(k, M_0)$ FOR SOME FIXED M_0 (E.G. M_0 = ALL ZEROS) AND RANDOM k.

size(Sim) = size($Enc(\cdot, M_0)$)

PSEUDORANDOM GENERATORS

OTP: $Enc(Y, M) = M+Y$ $Dec(Y, C) = C+Y$



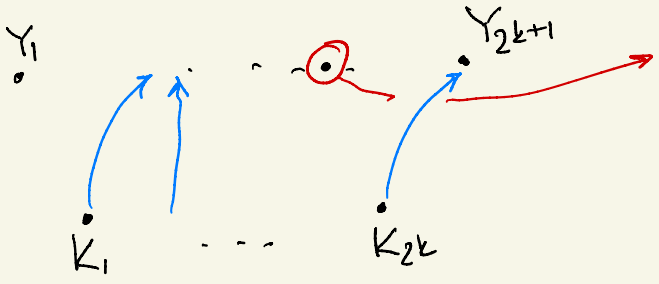
REPLACE KEY WITH SOMETHING THAT "LOOKS" PERFECTLY RANDOM

G IS AN (s,ε)-PSEUDORANDOM GENERATOR IF $G(K)$ (K RANDOM) IS (s,ε)-C.I. FROM A UNIFORM m-BIT STRING Y FOR $m > k$.

WHERE DO WE GET A PRG?
DO THEY EVEN EXIST? NOT SURE.

$$P \stackrel{?}{=} NP$$

$m = k+1$: 2^k KEYS $\longrightarrow$ 2^{k+1} OUTPUTS



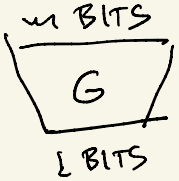
$\Pr[\exists K \text{ s.t. } G(K)=Y] \leq \frac{1}{2}$

IF CAN ANSWER EFFICIENTLY
$\rightarrow$ CAN DISTINGUISH $G(K)$ FROM Y

ONE-WAY FUNCTION

THEOREM CAN BUILD A PRG FROM ANY OWF.

CANDIDATE EXAMPLES OF PRG IN Lecture 4



LARGER m SHOULD BE HARDER TO GET... ACTUALLY $m = k+1$ WILL BE ENOUGH.

(s,ε) - PRG $\longrightarrow$ (s,ε) - SIM ENCRYPTION

$$\text{Enc}(k,M) = G(k)+M$$
$$\text{Dec}(k,C) = G(k)+C$$

Sim : OUTPUT UNIFORMLY RANDOM Y.

PROOF BY CONTRAPOSITIVE : SUPPOSE $\exists D$ OF SIZE s

$$\left|\Pr[D(G(k)+M)=1] - \Pr[D(Y)=1]\right| \geq \varepsilon$$

LET $D'(x) = D(x+M)$

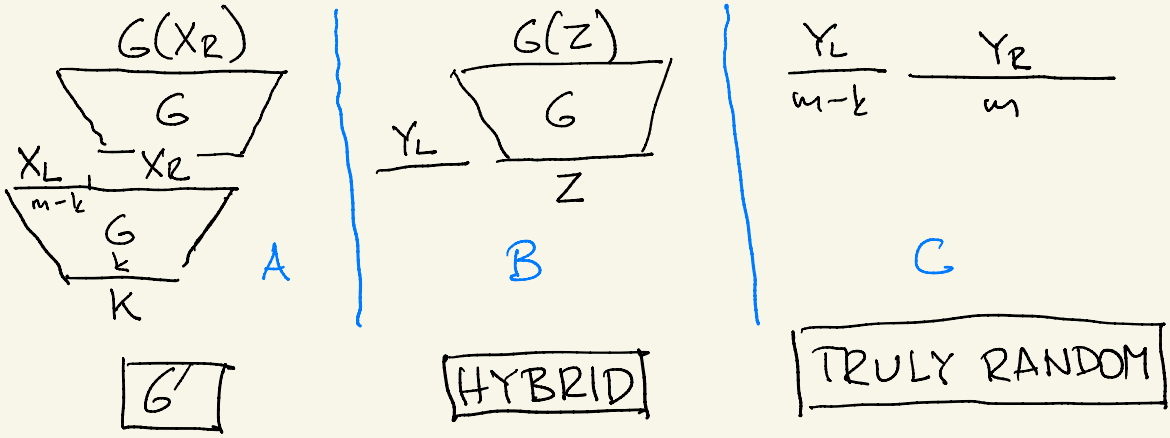
$$\Pr[D'(G(k))=1] = \Pr[D(G(k)+M)=1]$$
$$\Pr[D'(Y)=1] = \Pr[D(Y+M)=1]$$
$$= \Pr[D(Y)=1]$$

$\text{size}(D') = \text{size}(D) = s$ (M IS FIXED, ONLY ADDS SOME NOT GATES TO D)

$G : \{0,1\}^k \to \{0,1\}^m$ Ex. $k=500$, $m=2000$

STRETCH OF G $= m-k$

Theorem. IF G IS AN (s,ε)-PRG OF STRETCH $m-k$ THEN G' IS A (s',ε')-PRG OF STRETCH $2(m-k)$.



$(X_L, G(X_R))$ IS C.I. FROM (Y_L, Y_R).

Proof. SUPPOSE

$$\left| \Pr[D(X_L, G(X_R)) = 1] - \Pr[D(Y_L, Y_R) = 1] \right| > \varepsilon'$$

(A) (C)

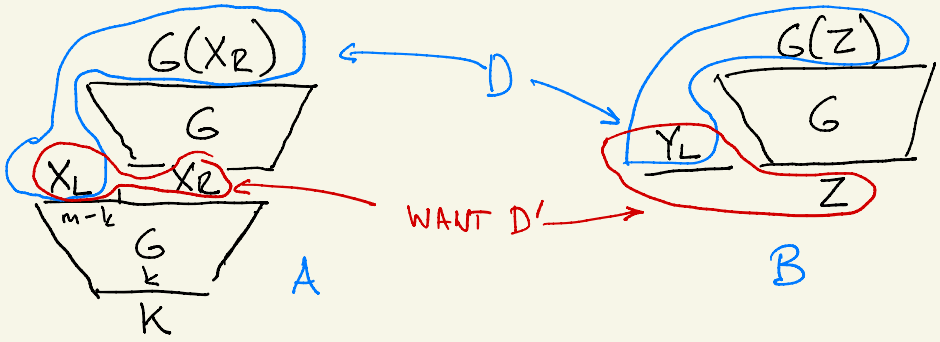
FOR SOME D OF SIZE s'. THEN

$\Pr[D(A)=1] - \Pr[D(B)=1] > \frac{\varepsilon'}{2}$ OR $\Pr[D(B)=1] - \Pr[D(C)=1] > \frac{\varepsilon'}{2}$

(1) (2)

CASE (2): $D'(y) = D(Y_L, y)$ DISTINGUISHES $G(Z)$ FROM Y_R FOR RANDOM Y_L $\rightarrow$ G IS NOT $(s, \varepsilon/2)$-P'RANDOM

CASE (1): NEXT TIME



G'

HYBRID

$$\left| P[D(A)=1] - P[D(B)=1] \right| \geq \frac{\varepsilon'}{2}$$

size $s'+t$ ← size s' size t

LET $D'(x) = D(x_1 \dots x_{m-k}, G(x_{m-k+1} \dots x_m))$

$D'(G(k)) = D(A)$ $\quad D'(R) = D(B)$

$$\left| P[D'(G(k))=1] - P[D'(R)=1] \right| \geq \frac{\varepsilon'}{2}$$

SO G IS NOT $(s'+t, \varepsilon'/2)$-P'RANDOM

IN EITHER ① OR ②, G IS NOT $(s'+t, \varepsilon'/2)$-P'RANDOM

SET $s' = s-t$, $\varepsilon' = 2\varepsilon$.