

**ENCRYPTION**

\[ M \rightarrow \text{Alice} \xrightarrow{\text{SECRET KEY } K} \text{Eve} \xrightarrow{\text{RECOVER } M} \text{Bob} \]

\[ \text{hello} \rightarrow \text{khoor} \]

**DETERMINISTIC**

Eve can do everything Bob can do.

- **ADD RANDOMNESS**

  \[ t \mod 26 \]

  \[ \text{hello} \rightarrow \text{?} \]

  \[ \frac{?}{26} \]

- **INCREASE RANDOMNESS**

  1. **PERMUTE LETTERS RANDOMLY**

  Alice \rightarrow Bob

  \[
  \begin{align*}
  \text{buy, sell, sell, buy, buy} \\
  \text{tpa, tpa, tpa}
  \end{align*}
  \]
RANDOM SHIFT BY BLOCK

hello world
+ tupht uphtu...

1. RANDOMNESS IS NEEDED ← SECRET KEY
2. NOT ENOUGH

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

\( M \in \mathbb{Z}_n \quad \kappa = \mathbb{Z}_n \) RANDOM

ASSUME \( m = k \); \( C = M + \kappa \mod 2 \)

\[ \kappa = (M_1 + \kappa_1, \ldots, M_k + \kappa_k). \]

\( C \rightarrow \text{[Bob]} \rightarrow C + \kappa = \mathbb{M}. \)

\( M + \kappa = C \)

FIXED RANDOM RANDOM

\((\text{Enc, Dec})\) IS PERFECTLY IND-SECURE IF \( \forall M, M' \)
\( \text{Enc}(\kappa, M) \) AND \( \text{Enc}(\kappa, M') \) 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.

$M \rightarrow C = \text{Enc}(k, M)$

$M' \rightarrow C' = \text{Enc}(k, M')$

$M', M' \text{ Distinguishable} \leftarrow \text{THERE EXISTS SOME OTHER}$

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

$X, X'$ ARE $\varepsilon$-STATISTICALLY CLOSE IF FOR ANY POSSIBLE TEST $D$ THAT OUTPUTS YES OR NO

\[
|\Pr[D(X) = \text{yes}] - \Pr[D(X') = \text{yes}]| \leq \varepsilon
\]

$\varepsilon = 0 \quad \rightarrow \quad \text{PERFECTLY ININDISTINGUISHABLE}$

$\varepsilon = 1.1 \quad \rightarrow \quad 99\% \text{ OF THE TIME CANNOT TELL APART}$
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

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

$k < m$ $\Rightarrow$ $\varepsilon = 1 - 2^{-k-n}$

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

CIRCUITS: MODEL OF EFFICIENT COMPUTATION

CIRCUIT = DIRECTED ACYCLIC GRAPH

SOURCES: INPUTS
SINKS: OUTPUTS
INTERNAL NODES: AND, OR, NOT GATES

$\text{SIZE} = \text{NUMBER OF AND+OR GATES}$

$f(x_1, x_2) = x_1 \oplus x_2$
Ex. \( \text{Share}(s) \): SAMPLE \( X_1, X_2, X_3 | X_1 + X_2 + X_3 = s \)

\[
\begin{array}{c}
\text{SECRET RANDOM} \\
\downarrow \\
\text{XOR} \\
\uparrow \\
\text{XOR} \\
\uparrow \\
\text{SECRET RANDOM}
\end{array}
\]

\[
\begin{array}{c}
X_1 \\
\uparrow \\
\text{XOR} \\
\downarrow \\
X_2
\end{array}
\]

\[
\begin{array}{c}
X_3 \\
\uparrow \\
\text{XOR} \\
\downarrow \\
X_1
\end{array}
\]

\[
\begin{array}{c}
X_2 \\
\uparrow \\
\text{XOR} \\
\downarrow \\
X_3
\end{array}
\]

\[\text{SIZE} = 2 \cdot \text{SIZE}(\text{XOR}) = 6.\]

MEASURE OF EFFICIENCY

PROGRAMS VS. CIRCUITS

<table>
<thead>
<tr>
<th>SIZE</th>
<th>RUNTIME</th>
<th>SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s )</td>
<td>( t )</td>
<td>( O(st) )</td>
</tr>
<tr>
<td>( O(s) )</td>
<td>( O(s) )</td>
<td>( s )</td>
</tr>
</tbody>
</table>

- C THAT TAKES NO REAL INPUT, ONLY RANDOMNESS IS A SAMPLER
- C THAT TAKES NO RANDOMNESS IS DETERMINISTIC
$X$ AND $X'$ OVER $\mathcal{B}^k$ ARE $(s,\varepsilon)$-COMPUTATIONALLY INDISTINGUISHABLE IF FOR EVERY CIRCUIT $D: \mathcal{B}^k \to \{0,1\}$ OF SIZE AT MOST $s$,

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

$\varepsilon$ - STAT $\leftrightarrow$ $(\infty,\varepsilon)$-COMP $\leftrightarrow$ $(2^k,\varepsilon)$-COMP

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

$s < 2^{\frac{k}{2}}$ - THERE EXIST FUNCTIONS THAT CANNOT BE COMPUTED BY CUTS OF SIZE $s$.

$(\text{Enc}, \text{Dec})$ IS $(s,\varepsilon)$-MESSAGE INDISTINGUISHABLE IF $\forall M, M'$, $\text{Enc}(k,M)$ AND $\text{Enc}(k,M')$ ARE $(s,\varepsilon)$-COMPUTATIONALLY IND.
WHAT ARE REASONABLE VALUES FOR S AND \( \varepsilon \)?

\( k = " \text{SE\textit{curity PARAMETER}}" \)

\textbf{T\textit{HEORY}}: Alice, Bob \text{RUN IN TIME POLYNOMIAL IN } k \text{ MAKE Eve \textit{DO }"WORK" EXPONENTIAL IN } k.

\[ \text{Ex. } S = 2^{k/2} \text{ or } 2^{k/2}. \]

S = AMOUNT OF WORK

\( \varepsilon = \text{LUCK} \quad k \geq 90,13^k \)

Eve can always randomly guess \( k \).

\text{GETs LUCK with PROB } 2^{-k}.

\text{WANT } \varepsilon \text{ NOT MUCH LARGER THAN THIS}

\[ \text{Ex. } \varepsilon = 2^{-k/2} \text{ or } 2^{-k/2}. \]

\textbf{RULE OF THUMB} \( \varepsilon \approx \varepsilon \) \text{ CAN CONVERT}

\text{LUCK INTO WORK}

\text{Eve BREAKS } \text{ Enc w/ } \varepsilon

\[ \text{Enc w/ } \varepsilon \text{ Enc w/ } 1 - (1 - \varepsilon)^t \approx t \varepsilon. \]

\text{PRACTICE} \( \varepsilon \approx \frac{1}{2^{80}} \approx 2^{80} \)
**Simulation-Based Definition**

\((\text{Enc}, \text{Dec})\) is \((\frac{s}{2}, \epsilon)\)-simulatable in size \(s\) if there exists a sampler \(\text{Sim}\) of size \(s\) s.t. \(\forall M\), output of \(\text{Sim}\) is \((\frac{s}{2}, \epsilon)\)-indistinguishable from \(\text{Enc}(k, M)\).

\[
\begin{align*}
\text{IND} & \quad \text{SIM} \\
\Pr[\text{D}(\text{Enc}(k, M)) = 1] - \Pr[\text{D}(\text{Enc}(k, M')) = 1] & \leq \epsilon \quad \Pr[\text{D}(\text{Sim}) = 1] - \Pr[\text{D}(\text{Enc}(k, M)) = 1] & \leq \epsilon \\
\forall \text{D of size } s & \\
\end{align*}
\]

\((s, \frac{\epsilon}{2})\)-non-sim'ly \(\rightarrow (s, \epsilon)\)-indist'ly

**Proof in Contrapositive**

Suppose Eve can \(\epsilon\)-distinguish encryptions

\[
\Pr[\text{D}(\text{Enc}(k, M)) = 1] - \Pr[\text{D}(\text{Enc}(k, M')) = 1] > \epsilon.
\]

For some pair \(M\) and \(M'\).

Either \(\Pr[\text{D}(\text{Enc}(k, M)) = 1] - \Pr[\text{D}(\text{Sim}) = 1] > \frac{\epsilon}{2}\)

or \(\Pr[\text{D}(\text{Sim}) = 1] - \Pr[\text{D}(\text{Enc}(k, M'))] > \frac{\epsilon}{2}\).
\[ \text{Sim} \text{ is dist from either } \text{Enc}(k, \mathcal{M}) \text{ or } \text{Enc}(k, \mathcal{M}') \text{ by sizes } s \text{ and adv. } \varepsilon/2. \]

\[ \text{EVEN IF Size(Sim)} = \infty \]

\[ (s, \varepsilon) - \text{INDIST' LITY} \rightarrow (s, \varepsilon) - \text{SIM' LITY} \]

Sim outputs \( \text{Enc}(k, \mathcal{M}_0) \) for some fixed \( \mathcal{M}_0 \) (e.g. \( \mathcal{M}_0 = \text{all zeros} \)) and random \( k \).

Size(Sim) = Size(\text{Enc}(\cdot, \mathcal{M}_0))

**PSEUDORANDOM GENERATORS**

**OTP:** \( \text{Enc}(Y, \mathcal{M}) = \mathcal{M} + Y \quad \text{Dec}(Y, C) = C + Y \)

G is an \((s, \varepsilon) - \text{PSEUDORANDOM GENERATOR} \)

If G(k) (k random) is \((s, \varepsilon) - \text{C.I.}\)

From a uniform \( m \)-bit string \( Y \)

For \( m \geq k \).
**Where do we get a PRG?**

Do they even exist? Not sure.

\[ P \neq NP \]

\[ m = k + 1 : \quad 2^k \text{ keys} \rightarrow 2^{k+1} \text{ outputs} \]

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

If can answer efficiently

→ Can distinguish \( G(k) \) from \( Y \)

**One-way function**

\[ k \xrightarrow{\text{easy}} G(k) \]

\[ k \xleftarrow{\text{hard}} \]

**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.
$(s, \varepsilon)$-PRG $\rightarrow$ $(s, \varepsilon)$-SIM Encryption

\[
\begin{align*}
\text{Enc}(k, M) &= G(k) + M \\
\text{Dec}(k, C) &= G(k) + C
\end{align*}
\]

Sim: OUTPUT UNIFORMLY RANDOM $Y$.

Proof by CONTRAPOSITIVE: Suppose $3D$ of sizes

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

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

\[
\begin{align*}
\Pr[D'(G(k)) = 1] &= \Pr[D(G(k) + M) = 1] \\
\Pr[D'(Y) = 1] &= \Pr[D(Y + M) = 1] \\
&= \Pr[D(Y) = 1]
\end{align*}
\]

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

\[
G : \{0, 1\}^k \rightarrow \{0, 1\}^m \\
\text{Ex. } k = 500, \ m = 2000
\]

STRETCH OF $G$ = $m - k$
Theorem. If $G$ is an $(s, \varepsilon)$-PRG of stretch $m - 1$, then $G'$ is a $(s', \varepsilon')$-PRG of stretch $2(m - 1)$.

\begin{align*}
(X_L, G(X_2)) &\text{ is c.i. from } (Y_L, Y_R). \tag{1}
\end{align*}

Proof. Suppose
\begin{align*}
\left| P_r[D(X_L, G(X_2)) = 1] - P_r[D(X_L, Y_R) = 1] \right| > \varepsilon' \tag{2}
\end{align*}

for some $D$ of size $s'$. Then
\begin{align*}
P_r[D(A) = 1] - P_r[D(B) = 1] > \frac{\varepsilon'}{2} \quad \text{or} \quad P_r[D(B) = 1] - P_r[D(C) = 1] > \frac{\varepsilon'}{2}
\end{align*}

Case ②: $D'(y) = D(Y_L, y)$ distinguishes $G(Z)$ from $Y_R$ for random $Y_L \rightarrow G$ is not $(s', \varepsilon'/2)$-PRAND.

Case ①: Next time.