THE BRIGHT SIDE OF HARDNESS

Oded GOLDREICH

WEIZMANN INST., ISRAEL

www.wisdom.weizmann.ac.il/~oded

/cc.html for COMPLEXITY THEORY (see CHAP. 1–2)

/foc.html for FOUNDATIONS OF CRYPTOGRAPHY (see primer)

/cc-book.html

/foc-sur04.html

P vs NP : search version

- Generic search problem for $R \subseteq \{0,1\}^* \times \{0,1\}^*$
  given x find y s.t. $(x,y) \in R$ [or declare that none exists]

P ~ class of search problems that can be solved in poly-time
i.e. efficiently/easily
(E.g. algs you saw.) (e.g. EULERIAN)

NP ~ class of search problems for which CORRECT INSTANCE-SOLUTION PAIRS are easy to recognize.
(e.g. FACTORING integers)
(+ HAMILTONIAN)

P≠NP ~ ABILITY TO EFFICIENTLY RECOGNIZE VALID SOLUTIONS DOES NOT IMPLY ABILITY TO EFF. FIND SOLUTIONS.

~ there exist "reasonable" search problems that are hard to solve.

NOTE: NP-COMPLETENESS.

ONE-WAY FUNCTIONS (OWF)

NOT EVERY EFFICIENT PROCESS CAN BE EFFICIENTLY REVERSED.

$$\begin{tikzcd} x \arrow[r, bend left, "\text{easy}"] & f(x) \arrow[l, bend left, squiggly, "\text{HARD}"] \end{tikzcd}$$

ON THE AVERAGE

THE SEARCH PROB. ASSOC. W. $\{ (f(x), x) : x \in \{0,1\}^n \}$ IS HARD TO SOLVE ON AVER.

[EX: $P \neq NP \Rightarrow$ WORST CASE HARD.]

EXAMPLE:

$$(p, q) \longmapsto p \cdot q \quad \text{(integer multiplication)}$$

$\longrightarrow O(n^2)$, $\tilde{O}(n)$ ALGS.

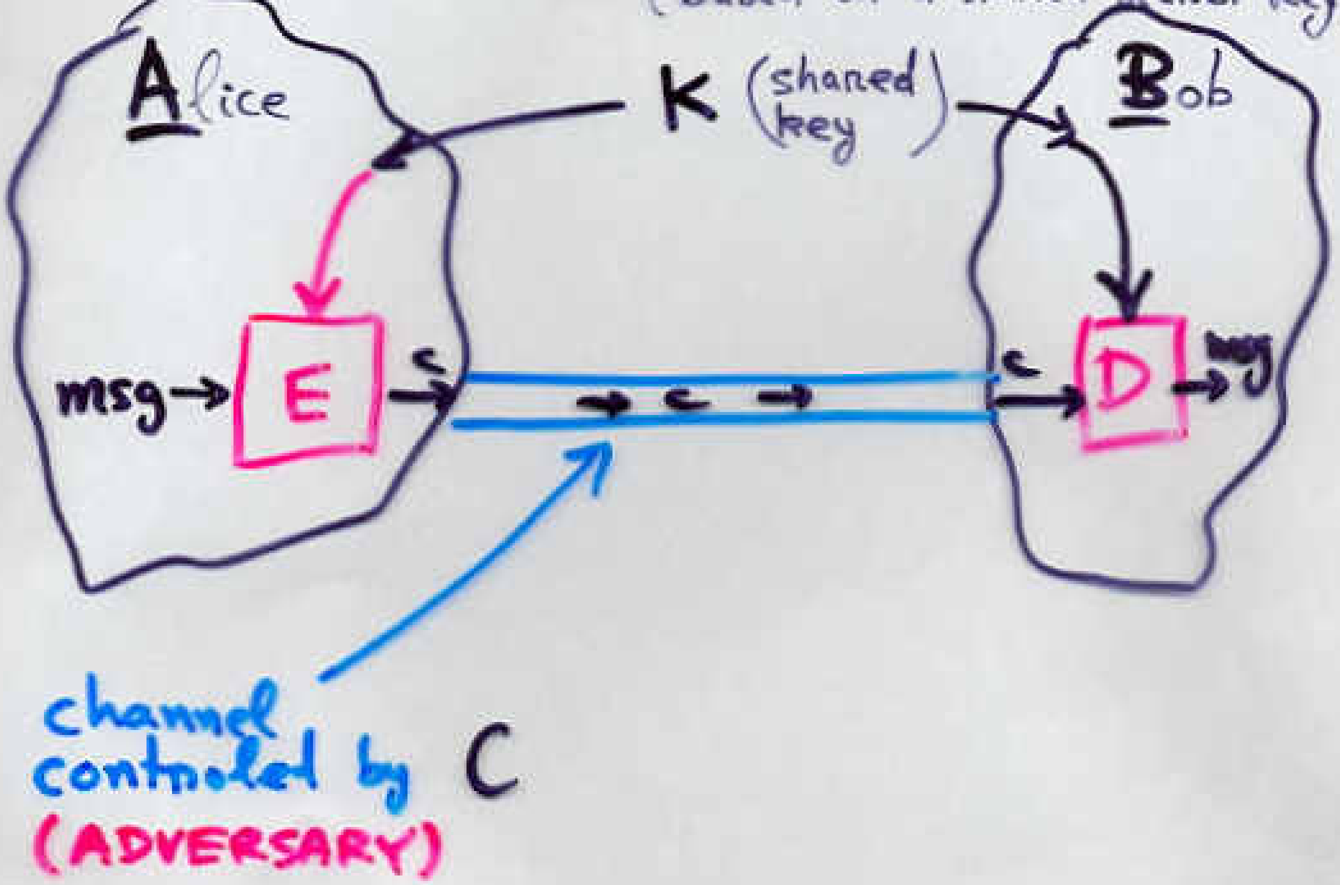
(integer FACTORIZATION) $\longleftarrow$

$O(\sqrt{2^n})$ ALG., $\exp(\tilde{O}(n^{1/3}))$ ALG.,

super-poly lowerbound $\Rightarrow P \neq NP$

USING OWF FOR SECURE COMMUNICATION

"private" & "authenticated"
(based on a shared secret key)



PRIVACY = C LEARNS NOTHING ABOUT msg

AUTHEN. = B ACCEPTS ONLY MESSAGES SENT BY A

} even if $|msg| > |k|$

THM: OWF ⟹ SECURE COMMUNICAT.

PRIVACY FOR SHORT MESSAGES

(single use!)

$$\begin{tikzcd} & k \arrow[d] & \\ \mathrm{msg} \arrow[r] & \boxed{E} \arrow[r] & \mathrm{msg}\oplus k \end{tikzcd}$$

$$\begin{tikzcd} & k \arrow[d] & \\ c \arrow[r] & \boxed{D} \arrow[r] & c\oplus k \end{tikzcd}$$

$(\mathrm{msg}\oplus k)\oplus k = \mathrm{msg}.$

(CORRECT.)

<u>PRIVACY</u>: not knowing k, $\mathrm{msg}\oplus k$ is uniformly dist.

AUTHENTICATION for ~~SHORT~~ MESSAGES (SINGLE USE!!!)

$$\begin{tikzcd} & K \arrow[d] & \\ msg \arrow[r] & \boxed{E/S} \arrow[r] & (msg, \underbrace{h_k(msg)}_{tag}) \end{tikzcd}$$

hashing function $\in$ FAMILY OF HASH FUNCTIONS
("Universal$_2$"
"pairwise indep.")

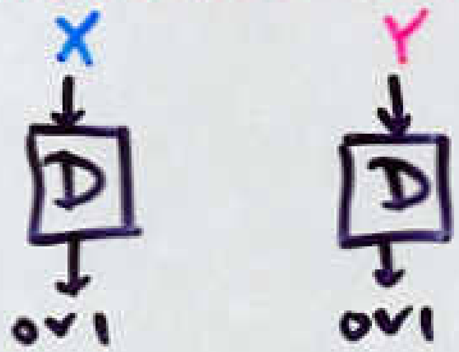
$$\begin{tikzcd} & K \arrow[d] & \\ (msg, t) \arrow[r] & \boxed{D/V} \arrow[r] & \begin{cases} msg & \text{IF } h_k(msg) = t \\ \perp & \text{OTHERWISE} \end{cases} \end{tikzcd}$$

CORRECTNESS ✓

SECURITY – IF C SEES ONLY <u>ONE</u> (msg, tag) THEN UNLIKELY TO GUESS A DIFF. VALID PAIR.

PSEUDORANDOM GENERATORS (PRG)

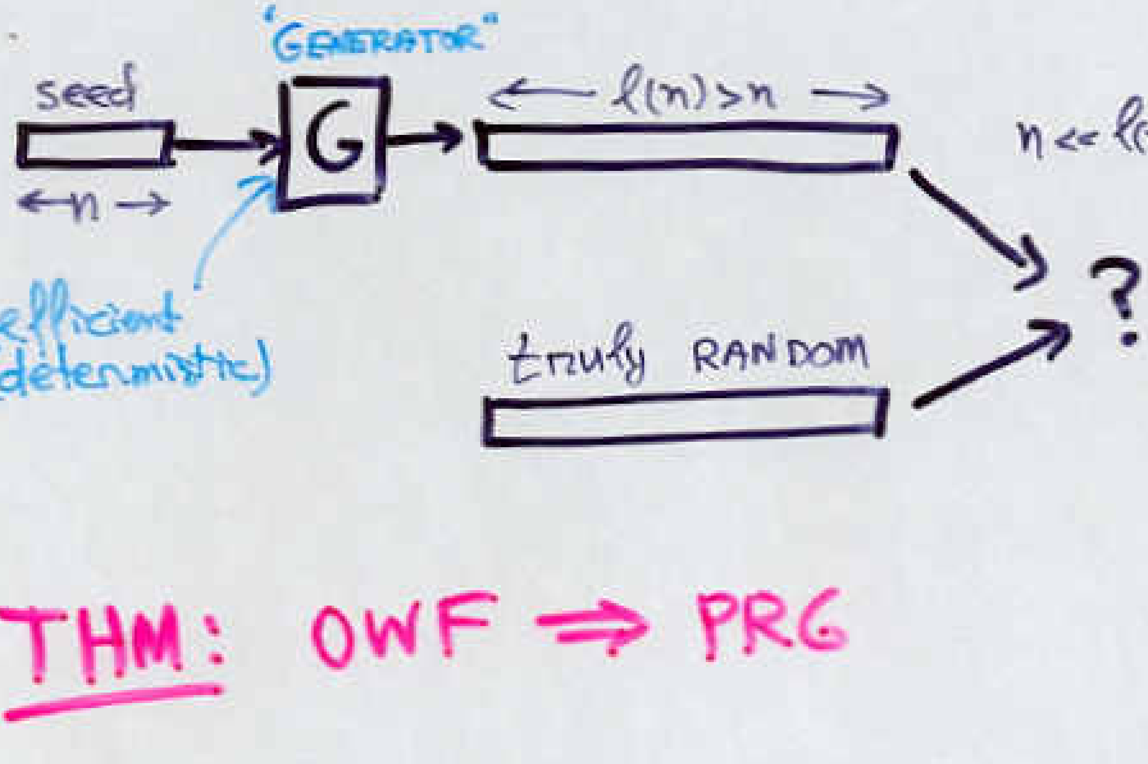
COMPUTATIONAL INDISTINGUISHABILITY (philo.)



$\text{Prob}[D(X)=1] \approx \text{Prob}[D(Y)=1]$

(strict) COARSING of STAT. INDIST.
[existance, constructability ⇔ OWF]

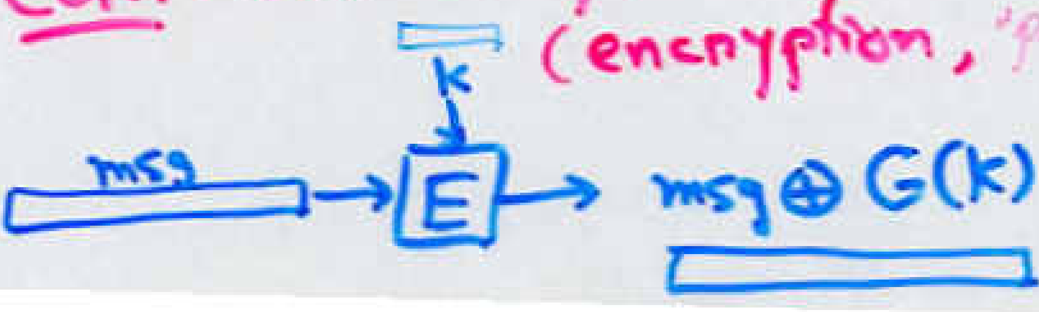
PSEUDORANDOM ≙ COMP. IND. from UNIFORM DIST.



$n \ll \ell(n) \leq \text{poly}(n)$

THM: OWF ⇒ PRG

COR.: OWF ⇒ private communicat. (encryption, "private-key")



OWF $\Longrightarrow$ PRG (special case)

f is OW**P** = OWF that induces a permutation on $\{0,1\}^n$ ($\forall n$).

$$G(\underbrace{s,r}_{2n \text{ BITS}}) = \underbrace{f(s), r}_{2n \text{ BITS}}, b(s,r)$$

INNER PRODUCT MOD 2 OF s and r.

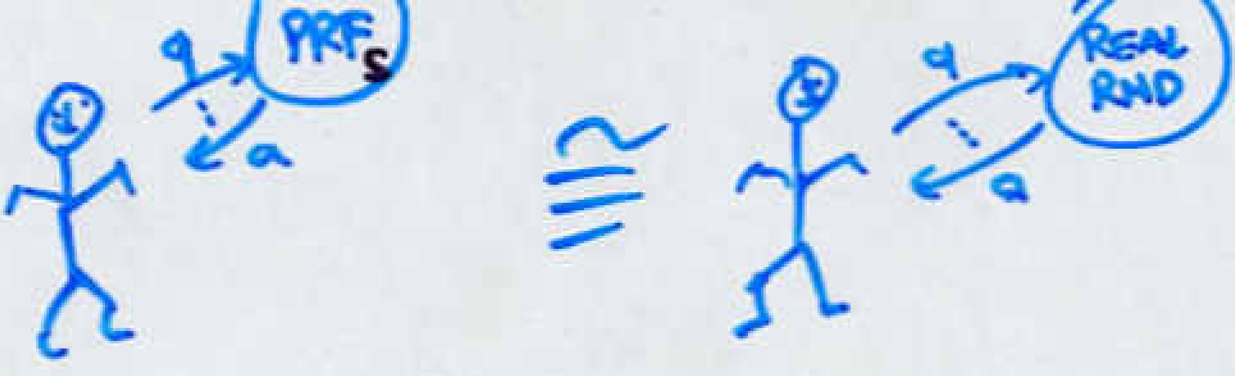
more bits — iterate or directly as →

$$G(s,r) = b(s,r), b(f(s),r)), \ldots, b(f^{\ell-1}(s), r)$$

PRG → AUTHENTIC.

VIA PRF (pseudorandom functions)

Replacing the HASHing functions



Even if f is a OWP
it may be easy to predict
the lsb of x given $f(x)$.

E.g. $f(x_1, \ldots, x_n) = (x_1, g(x_2 \ldots x_n))$.

Also, each bit may be easy to
predict (but not perfectly).

E.g. $f(x_1 \ldots x_n) = (x_1 \ldots x_\ell, x_i, g(x_1 \ldots x_n))$
$\ell = \log n,\ i = \mathrm{int}(x_1 \ldots x_\ell)$

But,

<u>THM:</u> If f is a OWF then
given $f(x)$ & r
it is infeasible to guess $b(x, r)$
SIGN. BETTER THAN w.p. $1/2$.

You may consider
$f'(x, r) \triangleq (f(x), r)$ as a new OWF
having a "bit" HARD to predict.