# A SUGGESTION

## OF ONE-WAY FUNCTIONS BASED ON EXPANDER GRAPHS

by

Oded GOLDREICH

WEIZMANN INSTITUTE

FILE AVAILABLE FROM

- ECCC
- CRYPTO' ePRINT
- Oded's homepage

# THE CONSTRUCTION

## PARAMETERS

$n$ = INPUT LENGTH (in practice 200 to 2000)

$\ell \geq 3$ S.T. $2^\ell$ IS FEASIBLE (in theory $\ell = o(\log n)$; in practice $\ell \in \{8, \dots, 16\}$)

## INGREDIANTS

- $\ell$-REGULAR $n$-VERTEX EXPANDER GRAPH

  $\Rightarrow S_1, \dots, S_n \subseteq [n]$ s.t. $|S_i| = \ell$

  "Expansion" $\equiv$ $\boxed{\exists k \text{ s.t. } \forall I \, (\text{with } |I| = k) \; \left|\bigcup_{i \in I} S_i\right| \geq k + \Omega(n)}$

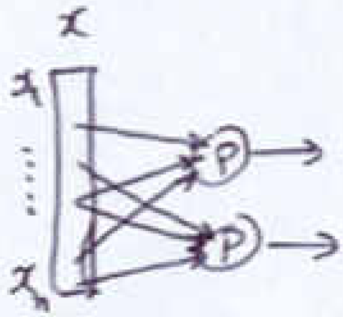
- A RANDOM (FIXED) PREDICATE $P : \{0,1\}^\ell \to \{0,1\}$

## THE FUNCTION

$f : \{0,1\}^n \to \{0,1\}^n$ $\left(f \equiv f_{S_1 \dots S_n, P}\right)$

$$f(x) = P(x[S_1]) \cdot P(x[S_2]) \cdots P(x[S_n])$$

where $x[\{i_1, \dots, i_\ell\}] = x_{i_1} \cdot x_{i_2} \cdots x_{i_\ell}$




$j^{th}$ output bit $= P(x_{i_1} \cdot x_{i_2} \cdots x_{i_\ell})$

where $S_j = \{i_1, i_2, \dots, i_\ell\}$

# MOTIVATION

- It is easy to invert P (i.e. find all $\approx \frac{1}{2} \cdot 2^{\ell}$ preimages)
- The difficulty should come from having to invert P on many related inputs.
- The expansion property prevents "length reduction" by divide-and-conquer (i.e., breaking the problem to unrelated sub-problems).

See role of expansion in the analysis of a natural algorithm (for inverting P)

# One Natural Inverting Algorithm

GIVEN $y \in \{0,1\}^n$, FIND $x$ S.T. $f(x) = y$.

IDEA: maintain a list of candidates that are consistent with some bits of $y$.

$$L_i = \left\{ x \in \{0,1,?\}^n : \begin{array}{ll} \forall j \in S_1 \cup \cdots \cup S_i & x_j \in \{0,1\} \\ \forall j \notin S_1 \cup \cdots \cup S_i & x_j = ? \\ \forall k = 1,\ldots,i & \underline{P(x[S_k]) = y_k} \end{array} \right\}$$

INITIALIZE: $L_0 = \{ ?^n \}$

ITERATE: from $L_i$ to $L_{i+1}$

For every $x \in L_i$
scan ~~check~~ all "extensions" of $x$ that may be in $L_{i+1}$
put such $x'$ in $L_{i+1}$ iff $\underline{P(x'[S_{i+1}]) = y_{i+1}}$

OUTPUT: $L_n \equiv$ list of all preimages of $y$ under $f$

---

ANALYSIS: $U_i \triangleq S_1 \cup \cdots \cup S_i$

expected size of $L_i$ $= \dfrac{2^{|U_i|}}{2^i} = \exp[\underbrace{|U_i| - i}_{\Omega(n)}]$

for some $i$ (by "expansion")