# Lecture Notes 6.440 Lecture 23

Note Title 5/5/2013

## Today

## Codes in Cryptography

① Collision-free hashing

Often want hash family

$\mathcal{H} \subseteq \{h : U \to \Gamma\}$

s.t. w.h.p.

$\forall a, b \in U$

$$\Pr_{h \leftarrow \mathcal{H}} [h(a) \neq h(b)] \geq 1 - \epsilon$$

Given $|U|$ ; $\epsilon$

would like to minimize $|\Gamma|, |\mathcal{H}|$.

### Solution via Codes:

Let $C = (n, k, d)_\Sigma$ code

with coding function $E : \Sigma^k \to \Sigma^n$

Correspondence

$$\Gamma = \Sigma$$

$$U = \Sigma^k$$

$$\mathcal{H} = \{E_1, \ldots E_n : \Sigma^k \to \Sigma\}$$

Code has distance $(1-\epsilon)q$ $(E_i(x) - E(x)_i)$

$$\Rightarrow \Pr[h(a) \neq h(b)] \geq 1-\epsilon$$

---

## SECRET SHARING

### $(\ell, t, n)$ - scheme

- Given secret $s \in \Omega$
- find shares $S_1 \ldots S_n$ ; $S_i = f_i(S, R)$
- $\forall \; T \subseteq [n], \; |T| \geq t \quad \exists f_T$ (t people can find secret)

$$f_T(\{S_i \mid i \in T\}) = S$$

- $\forall \; T \subseteq [n], \; |T| \leq \ell \quad \forall f$ ($\leq \ell$ people have no clue)

$$\Pr_R[s = f(\{S_i \mid i \in T\})] = \frac{1}{|\Omega|}$$

# LINEAR SECRET SHARING SCHEMES

- Idea: Use linear codes with good distance of primal & dual
- Construction: Code given by
  - $E_1 \dots E_n : \mathbb{F}_q^k \to \mathbb{F}_q$
  - given $s \in \mathbb{F}_q^a$
  - find $x \in \mathbb{F}_q^k$ s.t.

    $(E_1(x), \dots E_a(x)) = s$
  - share $s_i = E_{a+i}(x)$
- Parameters:
  - $\ell = d^\perp - a - 1$ ($d^\perp$ = distance of $C^\perp$)
  - $t = n - d + 1$
  - $|\Omega| = q^a$

- Special Case: Perfect secret sharing

$t = l+1$

- Use MDS $(d = n-k+1)$ code & $a=1$.
- Dual of MDS = MDS
- $d^{\perp} = k+1$
- above parameters yield

$l = k-1$

$t = k$

## Hardcore Predicates

**Defn:** $f : \{0,1\}^m \to \{0,1\}^m$ is a one-way permutation if

1. $f$ is one-to-one
2. $f$ is easy to compute
3. $f$ is very hard to compute

$\forall$ circuits $C$ of size $\leq S$

$$\Pr_x [ C(f(x)) = x ] \leq \epsilon .$$

# Hard-core bits

- Does there exist $i$ s.t. $x$ remains very hard even given $f(x)$ & $x_i$ ?
- If it exists, it is very useful but many not exist.

**Defn:** $b : \{0,1\}^m \to \{0,1\}$ is a hard core predicate for $f : \{0,1\}^m \to \{0,1\}^m$ if

(A) $b$ is easy to compute given $x$

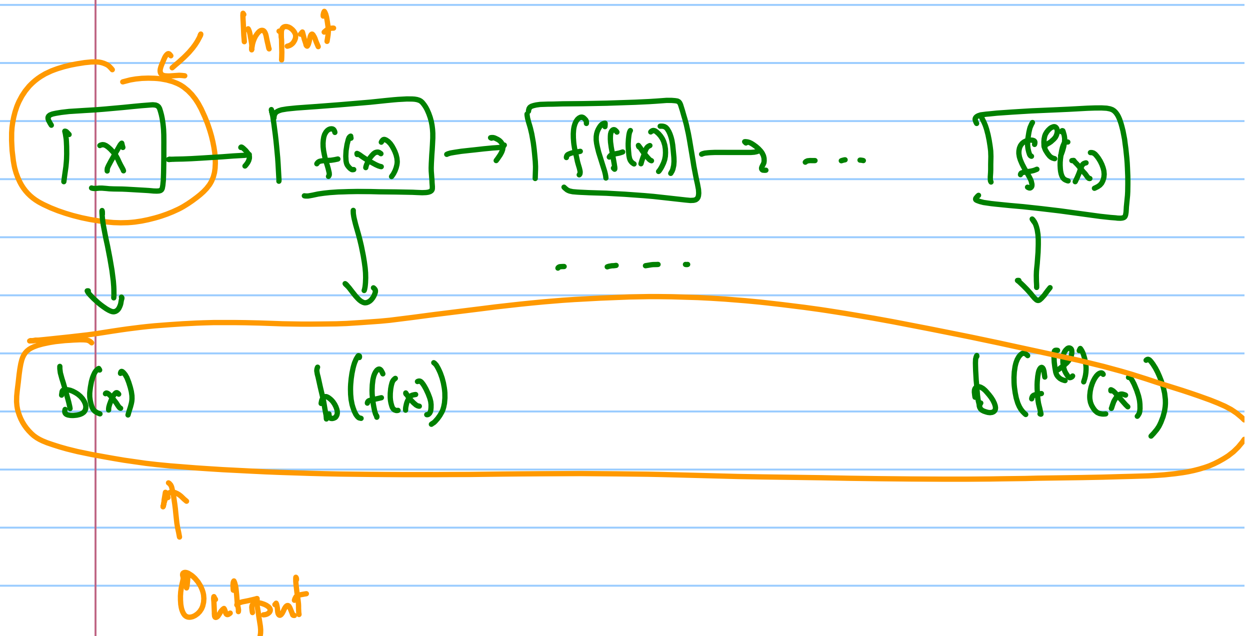
(B) $b$ is very hard given $f(x)$

$\forall$ circuits $C$ of size $\le S$

$$\Pr_x \left[ C(f(x)) = b(x) \right] \le \frac{1}{2} + \epsilon$$

[Blum Micali], [Yao], [Goldreich Levin]

# Pseudo random generator for size s circuits




## Analysis Sketch

Claim 1: if above not prg then

$\exists\, i, C$ s.t.

- $C$ guesses $b(f^{(i)}(x))$

  given $b(f^{(i+1)}(x)) \dots b(f^{(n)}(x))$

- But implies $\tilde{C}$ guesses above

  given $f^{(i+1)}(x)$.

- "Deterministically" hardcore bits may not exist

- Lemma: $\forall f \; \exists \tilde{f}, b$

  s.t. ① $f$ is OWP $\iff$ $\tilde{f}$ is OWP

  ② $b$ is hardcore for $\tilde{f}$.

- Construction:

  - let $f: \mathbb{F}_2^k \to \mathbb{F}_2^k$

    $E: \mathbb{F}_2^k \to \mathbb{F}_2^n$ be code

    that is list-decodable from

    $(\frac{1}{2}-\epsilon)$ fraction errors.

  - $\tilde{f}: \mathbb{F}_2^k \times [n] \to \mathbb{F}_2^k \times [n]$

    $\tilde{f}(x,i) = (f(x), i)$

  - $b(x,i) = E(x)_i$

## Analysis:

- Suppose

$$\Pr_{x,i}\left[C(f(x),i) = E(x)_i\right] \geq \frac{1}{2}+\epsilon$$

- By averaging

$$\Pr_x\left[\underbrace{\Pr_i\left[C(f(x),i) = E(x)_i\right] \geq \frac{1}{2}+\frac{\epsilon}{2}}_{(\ast)}\right] \geq \frac{\epsilon}{2}$$

- Fix $x$ s.t. $(\ast)$ holds

- Let $w_i = C(f(x),i)$,

- $\{x^{(1)} \dots x^{(L)}\} = \text{List-decode}(w)$

- Claim: $x \in \{x^{(1)} \dots x^{(L)}\}$