Proof of Theorem 2

Theorem 2: For $b < \log n - \log\log n - 1$, there is an n-bit S which is $(b, 0)$-encryptable, but not $(1, \varepsilon)$-extractable, where

$$\varepsilon \geq \frac{1}{2} - 2^{\left(2b - \frac{n}{2^b}\right)} \geq \frac{1}{2} - \frac{1}{16n^2} = \frac{1}{2} - o(1)$$

Theorem 2': For $b < \log n - \log\log n - 1$, there is a b-bit $\mathcal{E}$ = (Enc,Dec) for which Good($\mathcal{E}$) is not $(1, \varepsilon)$-extractable, where

Good($\mathcal{E}$) = $\{K \mid \mathcal{E}$ is Shannon-secure under $K\}$

Our Encryption Scheme

- Let $N = 2^n$; $B = 2^b$; S s.t. $N \approx S(S-1)\ldots(S-B+1)$
- Note, $N < S^B$, so $S > N^{1/B}$ ($> B$ for our params)
- Message space M $= \{1,\ldots,B\}$
- Ciphertext space C $= \{1,\ldots,S\}$
- Key space K = {all B-tuples of ciphertexts}

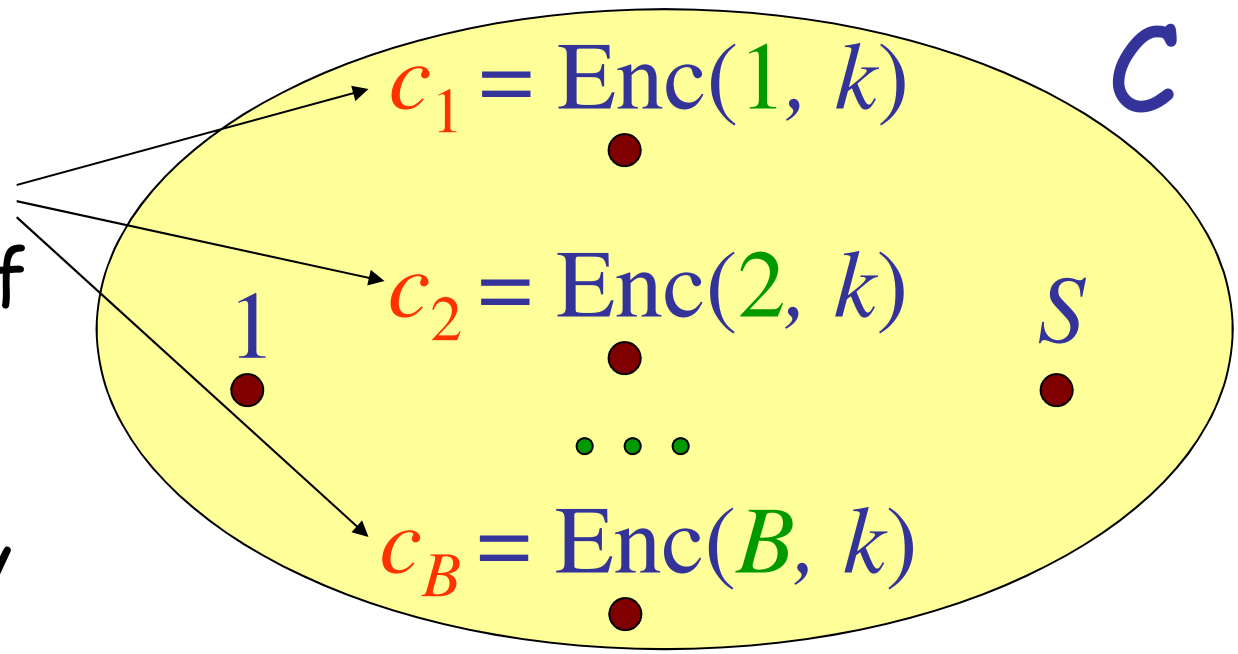
K = $\{\ k = (c_1\ldots c_B) \mid c_i \neq c_j \text{ for } i \neq j\ \}$

- Encryption: $\mathrm{Enc}(m, (c_1\ldots c_B)) = c_m$
- Decryption: $\mathrm{Dec}(c, (c_1\ldots c_B)) = m \text{ s.t. } c_m = c$

Our Encryption Scheme

- <u>Our Goal</u>: show that the set of "perfect encryption distributions" on K is highly non-extractable

$k = (c_1 \ldots c_B)$: every subset of B ciphertexts is a possibility under some key



Proof of Theorem 2'

- Take any $\mathrm{Ext}: [N] \to \{0,1\}$
- Case 1: have 0-monochromatic perfect K
  - Fix Ext to 0 with K, done
- Case 2: no such 0-monochromatic perfect K
  - Main Lemma: if we cannot fix Ext to 0, then $\exists$ perfect K s.t. $\Pr[\mathrm{Ext}(K) = 0] < B^2/S < B^2/N^{1/B}$
    - Sublemma 1: certain condition implies $\mathrm{Ext}[k] = 1$
    - Sublemma 2: $\exists K$ uniform over S keys with at most B^2 keys not satisfying the condition of Sublemma 1

Sublemma 1

- Sublemma 1: certain condition $\Rightarrow$ $\mathrm{Ext}[k] = 1$
  - Step 1. No 0-monochromatic perfect $K \Rightarrow$ certain linear system has no solutions $x \geq 0$
  - Step 2. Use Farkas' Lemma: $Ax = e$ has no solutions $x \geq 0$ iff $\exists$ y s.t. $yA \geq 0$, $ye < 0$
    - Easy direction: $0 \leq (yA)x = y(Ax) = ye < 0$
  - Step 3. Deduce the condition using the y above

Step 1: Perfect Distributions

- Distribution $K = \{p_k\}$ is perfect for b-bit encryption iff $\mathrm{Vp} = \mathrm{e}$ and $\mathrm{p} \geq 0$
- V and e encode these constraints on p:
  - $\Sigma\, p_k = 1$
  - $p_k = \Pr[K = k] \geq 0$ for all k
  - $\forall\ (1 < m \leq \mathrm{B}, 1 \leq c \leq S)$, $\mathrm{Enc}_K(1) \equiv \mathrm{Enc}_K(\mathrm{m})$:

$$\sum_{k=(c_1,\ldots,c_B),c_1=c} p_k - \sum_{k=(c_1,..,c_B),c_m=c} p_k = 0$$

Step 1: Perfect Distributions

- Distribution $K = \{p_k\}$ is perfect for b-bit encryption iff $Vp = e$ and $p \geq 0$
- No 0-monochromatic perfect p

$$\Updownarrow$$

- No perfect p whose support is inside $Z = \{k\text{: Ext}(k) = 0\}$

$$\Updownarrow$$

- $Ax = e$ has no solutions $x \geq 0$
  - A and x - restrictions of V and p to Z

Steps 2 & 3: Apply Farkas Lemma

- (Farkas' Lemma) $Ax = e$ no solution $x \geq 0$ iff $\exists\, y$ such that $yA \geq 0$ and $ye < 0$.
  (A and x - restrictions of V and p to Z)
- Our situation:
  - For any k s.t. $\mathrm{Ext}(k) = 0$ (i.e., k in Z)

$$0 \leq (yA)_k = (yV)_k = y_1 + \Sigma_{m>1} (y_{m,c_1} - y_{m,c_m})$$

$-y_1 = ye < 0$. Thus, $0 < \Sigma_{m>1} (y_{m,c_1} - y_{m,c_m})$

- Thm: if $y_{m,c_1} - y_{m,c_m} \leq 0$ for all $m > 1 \Rightarrow \mathrm{Ext}[k]=1$

Sublemma 2

- For any numbers $\{y_{m,c}\}$ $\exists$ perfect K which is uniform over S keys s.t. at most B^2 keys $k = (c_1,\ldots,c_B)$ do not satisfy the condition:

$$y_{m,c_1} - y_{m,c_m} \leq 0 \text{ for all } m > 1$$

- Special case $b=1$: for any numbers $\{y_c\}$ $\exists$ perfect K which is uniform over S keys s.t. at most 4 (we'll get 1, in fact) keys $k = (c,c')$ do not satisfy the condition:

$$y_c - y_{c'} \leq 0$$

Sublemma 2: Case b=1

- For any reals $\{y_c\}$ $\exists$ perfect K which is uniform over S keys s.t. at most 4 (we'll get 1, in fact) keys $k = (c,c')$ do not satisfy the condition:

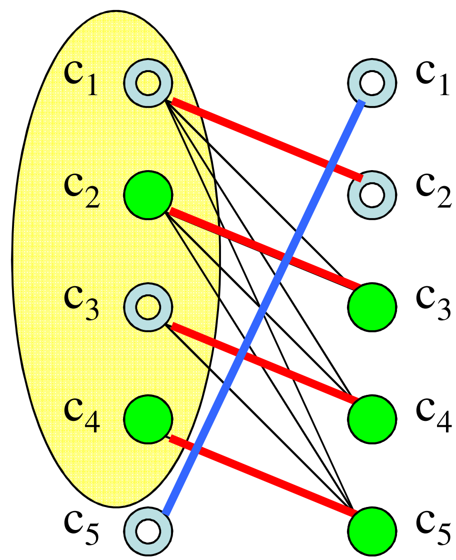
$$y_c - y_{c'} \leq 0$$

- Let $c_1 \ldots c_S$ be an ordering s.t. $y_{c_1} \leq y_{c_2} \leq \ldots \leq y_{c_S}$
- Define K uniform on $(c_1,c_2),\ldots,(c_{S-1},c_S),(c_S,c_1)$
  - Indeed a perfect distribution
- All $(y_{c_1} - y_{c_2})$, $(y_{c_2} - y_{c_3})$, …, $(y_{c_{S-1}} - y_{c_S})$ are ≤ 0. QED
- Could have found this using matchings

Sublemma 2: Case b=1

- Bipartite graph G with vertices labeled with $\{c\}$
- An edge runs from c to c' iff $y_c - y_{c'} \leq 0$ ($\Rightarrow$ Ext[(c,c')]=1)
- G has a matching of size $S - 1$
  - Hall's theorem: if every subset T of "left" set X has $|N(T)| \geq |T|$, then X is "matchable"
  - Here true for $X = \{c_1 \ldots c_{S-1}\}$:

    $N(\{c_i$, any other c_j's with $i < j < S\}) = \{c_{i+1},\ldots,c_S\}$
- Complete to get a perfect K (possibly using a 0-key)
  - All keys but the last one are "1-keys" (since they belong to G)



Sublemma 2: General Case

- Our K is uniform on S keys
- Instead of choosing $k_1, \ldots, k_S$,
- … we inductively choose $E(1), E(2), \ldots, E(B)$

	$E(1)$	$E(2)$	…	$E(m)$	…	$E(B)$
Key 1	$\pi_1(1)$	$\pi_2(1)$	…	$\pi_m(1)$	…	$\pi_B(1)$
Key 2	$\pi_1(2)$	$\pi_2(2)$	…	$\pi_m(2)$	…	$\pi_B(2)$
…	…	…	…	…	…	…
Key c	$\pi_1(c)$	$\pi_2(c)$	…	$\pi_m(c)$	…	$\pi_B(c)$
…	…	…	…	…	…	…
Key S	$\pi_1(S)$	$\pi_2(S)$	…	$\pi_m(S)$	…	$\pi_B(S)$

Sublemma 2: General Case

- Each column m is a *permutation* π_m of $\{1,\ldots,S\}$
  - Ensures the distribution is perfect ($E(m)$ is random !)
- Constraints:
  - $\pi_m(c) \neq \pi_{m'}(c)$ for all c, $m \neq m'$ (unique decodability for a fixed key)
  - Want many rows satisfying $y_{m,\pi_1(c)} - y_{m,\pi_m(c)} \leq 0$ for all $m > 1$

	$E(1)$	$E(2)$	...	$E(m)$	...	$E(B)$
Key 1	$\pi_1(1)$	$\pi_2(1)$	…	$\pi_m(1)$	…	$\pi_B(1)$
Key 2	$\pi_1(2)$	$\pi_2(2)$	…	$\pi_m(2)$	…	$\pi_B(2)$
…	…	…	…	…	…	…
Key c	$\pi_1(c)$	$\pi_2(c)$	…	$\pi_m(c)$	…	$\pi_B(c)$
…	…	…	…	…	…	…
Key S	$\pi_1(S)$	$\pi_2(S)$	…	$\pi_m(S)$	…	$\pi_B(S)$

Sublemma 2: General Case

- Constraints:
  - $\pi_m(c) \neq \pi_{m'}(c)$ for all c, $m \neq m'$ (unique decodability for a fixed key)
  - Want many rows satisfying $y_{m, \pi_1(c)} - y_{m, \pi_m(c)} \leq 0$ for all $m > 1$
- Call $\pi_m(c)$ red if $y_{m,\pi_1(c)} - y_{m, \pi_m(c)} \leq 0$ & $\pi_m(c) \neq \pi_{m'}(c)$, $\forall\, m' < m$
  - Note: $\pi_1(c) \ldots \pi_B(c)$ red implies $\mathrm{Ext}[c] = 1$

	E(1)	E(2)	…	E(m)	…	E(*B*)
Key 1	$\pi_1(1)$	$\pi_2(1)$	…	$\pi_m(1)$	…	$\pi_B(1)$
Key 2	$\pi_1(2)$	$\pi_2(2)$	…	$\pi_m(2)$	…	$\pi_B(2)$
…	…	…	…	…	…	…
Key c	$\pi_1(c)$	$\pi_2(c)$	…	$\pi_m(c)$	…	$\pi_B(c)$
…	…	…	…	…	…	…
Key *S*	$\pi_1(S)$	$\pi_2(S)$	…	$\pi_m(S)$	…	$\pi_B(S)$

Sublemma 2: Induction

- Call $\pi_m(c)$ red if $y_{m,\pi_1(c)} - y_{m,\,\pi_m(c)} \leq 0$ & $\pi_m(c) \neq \pi_{m'}(c),\ \forall\ m' < m$
- Key inductive step: can select a permutation column $\#m$ which has $\leq 2m$ non-red $\pi_m(c)$'s!
  - Generalizes the Hall's matching argument we saw for $b=1$

	E(1)	E(2)	…	E(m)	…	E(B)
Key 1	$\pi_1(1)$	$\pi_2(1)$	…	$\pi_m(1)$	…	$\pi_B(1)$
Key 2	$\pi_1(2)$	$\pi_2(2)$	…	$\pi_m(2)$	…	$\pi_B(2)$
…	…	…	…	…	…	…
Key c	$\pi_1(c)$	$\pi_2(c)$	…	$\pi_m(c)$	…	$\pi_B(c)$
…	…	…	…	…	…	…
Key S	$\pi_1(S)$	$\pi_2(S)$	…	$\pi_m(S)$	…	$\pi_B(S)$

Sublemma 2

- After iteration j, row c is still good if we have

$$y_{m,\pi_1(c)} - y_{m,\pi_m(c)} \leq 0 \text{ for } 1 < m \leq j$$

- Key Step: At iteration m, at most $2m$ rows become bad