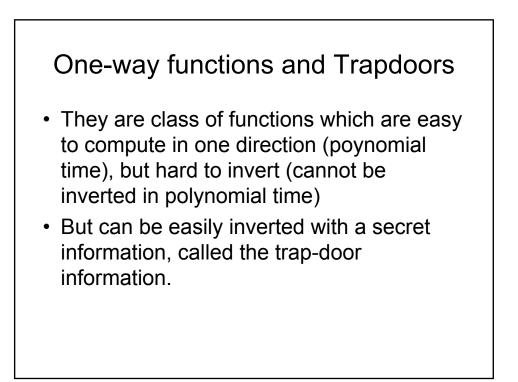
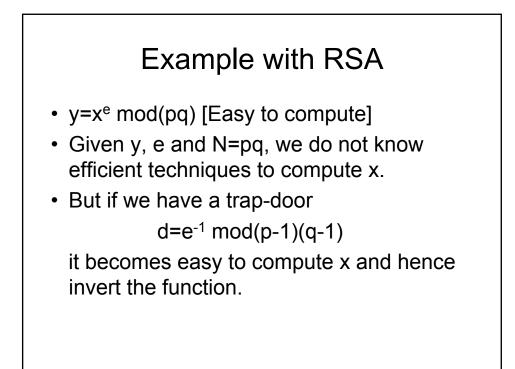


Hard Core Predicates

If $f : \{0,1\}^n \to \{0,1\}^n$, and bijective, a poly(n) computable $B : \{0,1\}^n \to \{0,1\}$ is $(t,\varepsilon) - hp$ for f if for every A with running time $\leq t(n)$, $\Pr_X [A(f(X))=B(X)] \leq \frac{1}{2} + \in (n)$





Hard Core Predicate of trapdoor permutations

(G, F, I) is a family of trapdoor permutations,

G chooses (k, t_k)

F(.,k) is bijective

 $I(.,t_k,k)$ is inverse of F(.,k)

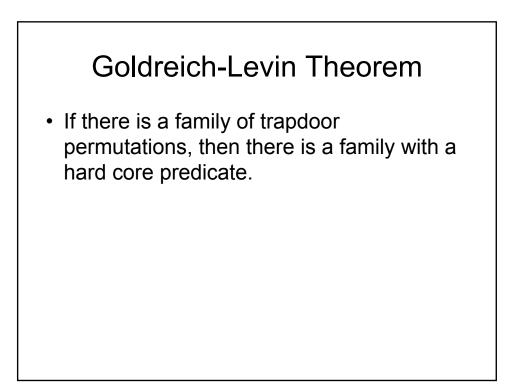
st, G,F,I can be done in poly(n) time and inverting

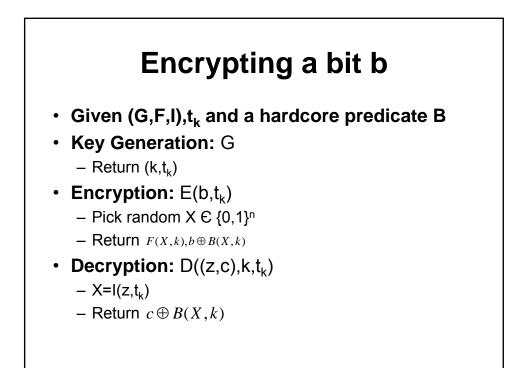
F without t_k is hard.

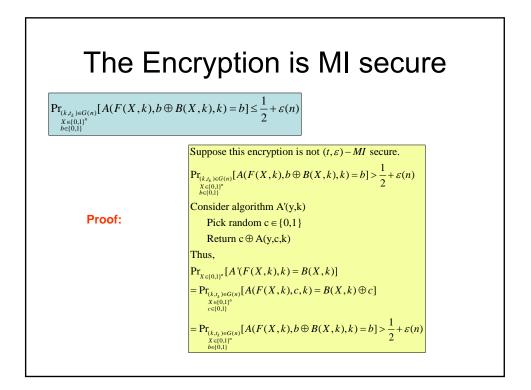
HP for trap-door permutations

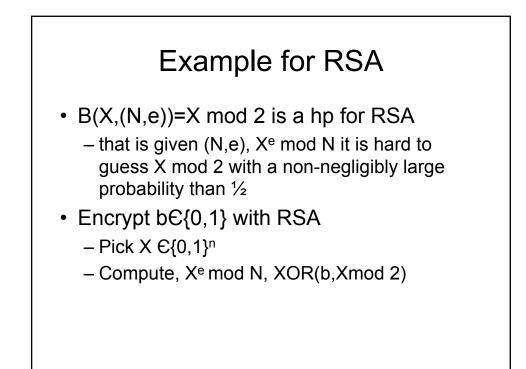
If (G, F, I) is a family of trapdoor permutations, then polynomial time one bit output B(X,k) is a hard-core predicate if for every A running in time $\leq t(n)$,

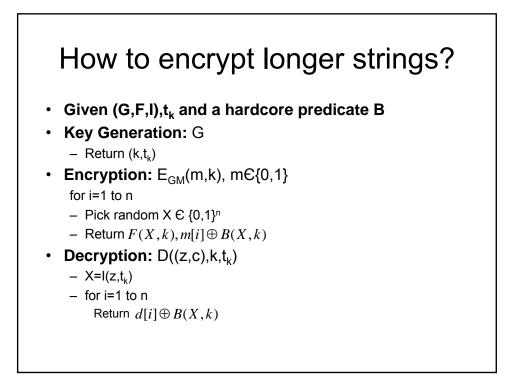
 $\operatorname{Pr}_{(k,t_k)\in G(n)}\left[A(F(X,k),k)=B(X,k)\right] \leq \frac{1}{2} + \varepsilon(n)$





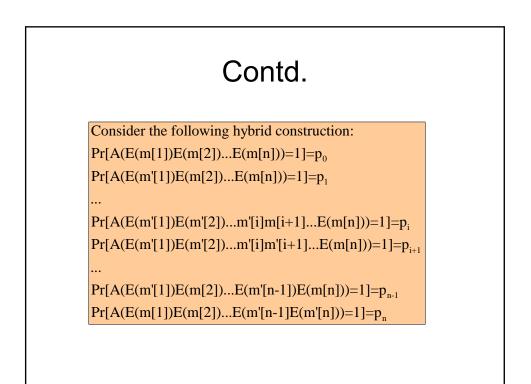


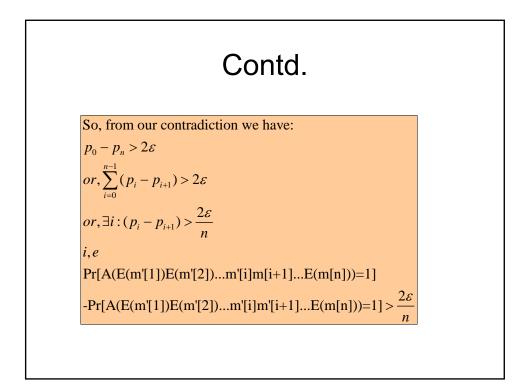


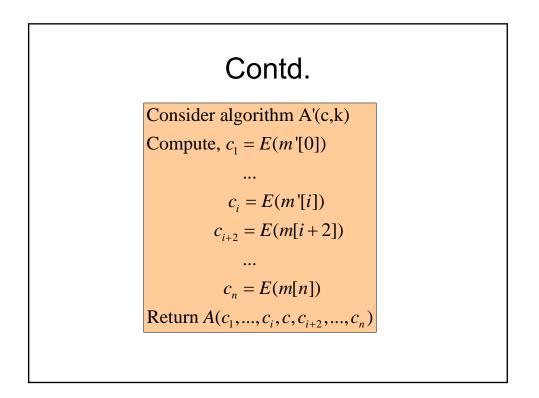


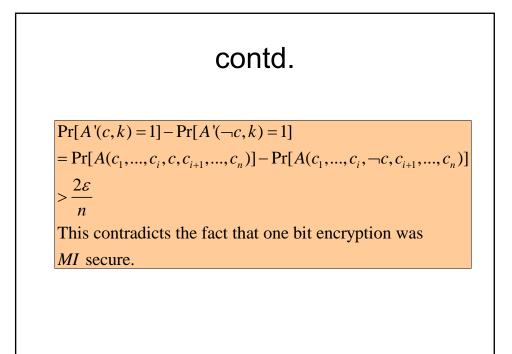
Proof of MI secured

For every m, m' for every A running in time $\leq t(n)$ $\Pr[A(E_{GM}(m,k),k) = 1] - \Pr[A(E_{GM}(m',k),k) = 1] \leq 2\varepsilon$ If we contradict this supposition, we have $\exists A, m, m$'s.t. $\Pr[A(E_{GM}(m,k),k) = 1] - \Pr[A(E_{GM}(m',k),k) = 1] > 2\varepsilon$









A Hard Core Predicate for any oneway function

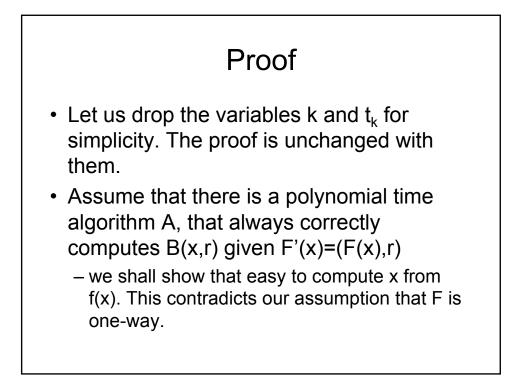
Let (G,F,I) be a family of trap-door permutations. Consider (G,F',I'), which is also a family of trap-door permutations.

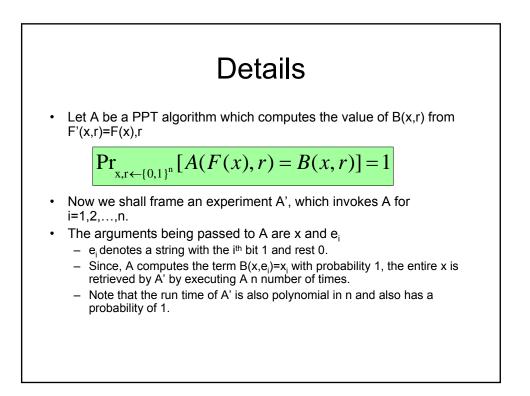
 $I'((z,r),t_k) = I(z,t_k), r$ and

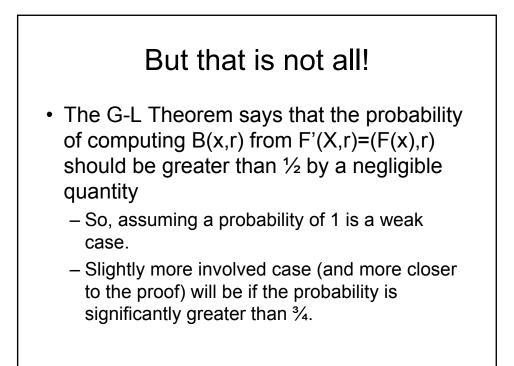
$$F'((x,r),k) = \langle F(x,k), r \rangle$$

Then $B(x,r) = \sum_{i} x_i \cdot r_i \mod 2$

is a hard core predicate for (G',F',I').

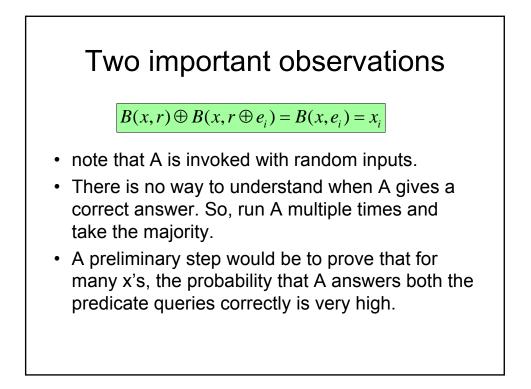


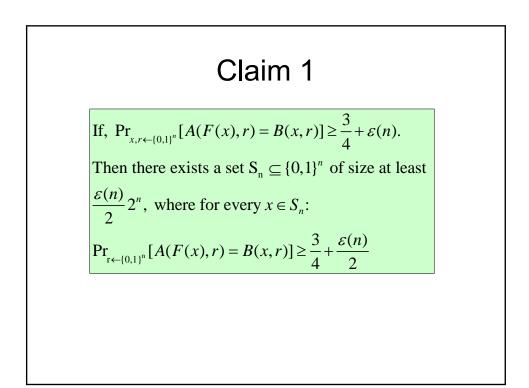


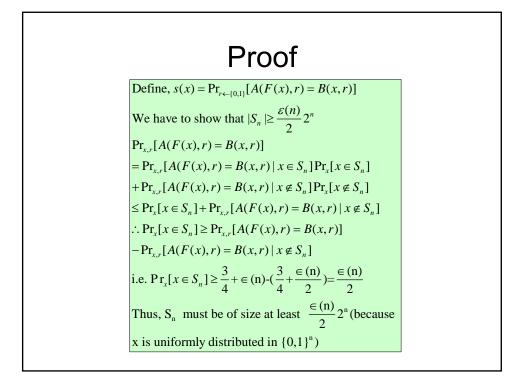


Why the previous proofs does not work?

- It may be that A never succeeds in computing B(x,r) correctly when r=e_i
- The algorithm A' has no means of understanding that A has succeeded or not?
 - So, what does A' do in this case to increase his chance?
 - (repeat the experiment of A)

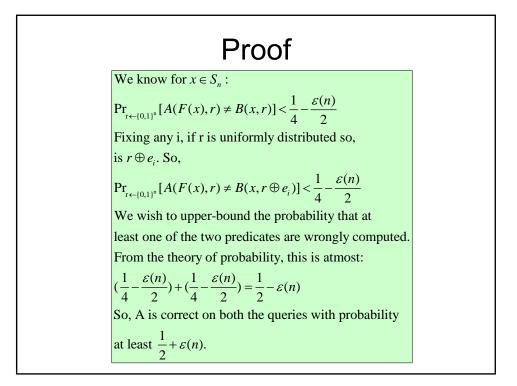


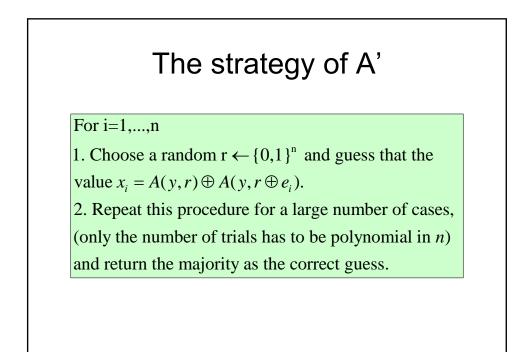




Claim 2
If,
$$\Pr_{x,r \leftarrow \{0,1\}^n} [A(F(x),r) = B(x,r)] \ge \frac{3}{4} + \varepsilon(n).$$

Then there exists a set $S_n \subseteq \{0,1\}^n$ of size at least
 $\frac{\varepsilon(n)}{2} 2^n$, where for every $x \in S_n$ and every *i* it holds
that:
 $\Pr_{r \leftarrow \{0,1\}^n} [A(F(x),r) = B(x,r) \land A(F(x),r \oplus e_i) = B(x,r \oplus e_i)]$
 $\ge \frac{1}{2} + \varepsilon(n)$





Can this proof be extended to the general case?

- Since it involves two computations of B(), the error probability is doubled.
- for the actual proof (and even when the error probability is exactly ¼ this will not help in inverting F with a significant prob)
- Instead, we guess one B and compute the other.
- m=poly(n) and set l=log₂(m+1)

Can this proof be extended to the general case?

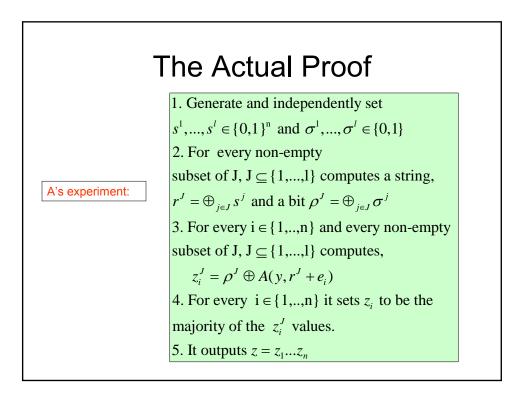
- Choose / strings uniformly and independently in {0,1}ⁿ and denote them by s₁,...,s_l.
- Then guess $B(x,s_1),\ldots,B(x,s_l)$ and call them $\sigma_1,\ldots,\sigma_l.$
- Probability that all of them are correct is 1/2ⁱ=1/poly(n)
- Fix J as a subset of {1,...,I} and define r^J = ⊕_{j∈J} s^j
 It may be shown that the r^J's are pairwise independent and uniformly distributed in {0,1}ⁿ

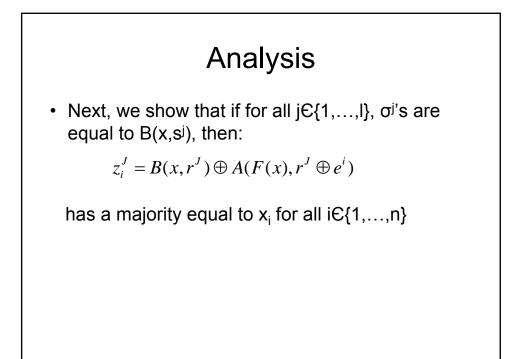
Can this proof be extended to the general case?

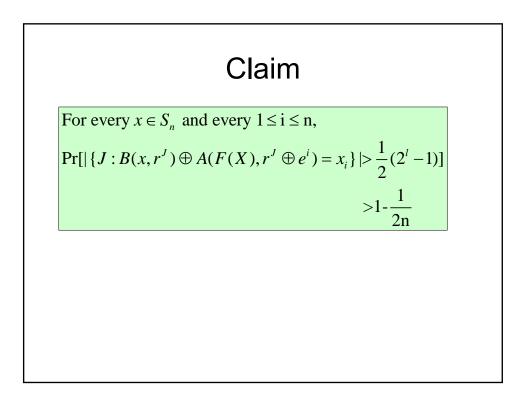
• Note that:

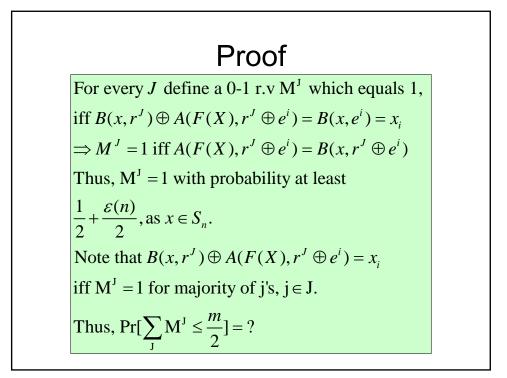
 $B(x,r^{J}) = B(x, \bigoplus_{j \in J} s^{j}) = \bigoplus_{j \in J} B(x, s^{j})$

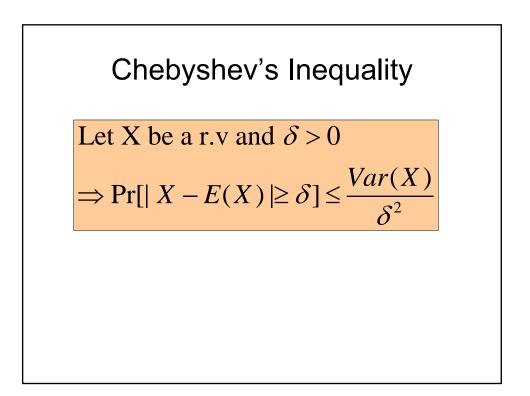
• So, our guess for B(x,r^J) is $\rho^{J} = \bigoplus_{j \in J} \sigma^{j}$











$$\Pr\left[\sum_{J} M^{J} \leq \frac{m}{2}\right] \leq \Pr\left[\left|\sum_{J} M^{J} - \left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right)m\right| \geq \frac{\varepsilon(n)}{2}m\right]$$
Note, $E\left(\sum_{J} M^{J}\right) = \left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right)m$

$$Var\left(\sum_{J} M^{J}\right) = m\left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right)\left(\frac{1}{2} - \frac{\varepsilon(n)}{2}\right) < \frac{m}{4}$$

$$\Pr\left[\sum_{J} M^{J} \leq \frac{m}{2}\right] \leq \Pr\left[\left|\sum_{J} M^{J} - \left(\frac{1}{2} + \frac{\varepsilon(n)}{2}\right)m\right| \geq \frac{\varepsilon(n)}{2}m\right]$$

$$\leq \frac{m/4}{(\varepsilon(n)/2)^{2}m^{2}} = \frac{1}{\varepsilon(n)^{2}m}$$
Let, $m = \frac{2n}{\varepsilon(n)^{2}}$, we have:
$$\Pr\left[\sum_{J} M^{J} \leq \frac{m}{2}\right] \leq \frac{1}{2n}$$

$$\therefore \Pr\left[\sum_{J} M^{J} > \frac{m}{2}\right] \geq 1 - \frac{1}{2n}$$
This completes the proof of the claim.

