

THEOREM

IF F IS A PSEUDORANDOM FUNCTION, THEN Π^F IS CPA-SECURE

PROOF

THE PROOF IS DIVIDED INTO TWO SUB-PROOFS

① IN THE FIRST ONE, WE INTRODUCE AND STUDY AN ENCRYPTION SCHEME $\tilde{\Pi}$ WHICH IS AN IDEALIZED VERSION OF Π^F . MORE SPECIFICALLY, $\tilde{\Pi} = (\text{Gen}, \text{Enc}, \text{Dec})$ WHERE

Gen , RATHER THAN GENERATING AN n -BIT STRING, IT GENERATES A RANDOM FUNCTION FROM $\{0,1\}^n$ TO ITSELF, NAMELY IT FILLS A TRUTH TABLE

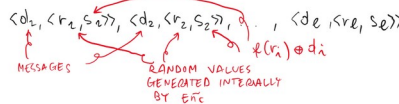


THIS MEANS Gen IS NOT EFFICIENTLY COMPUTABLE BUT THIS IS NOT A PROBLEM, BECAUSE $\tilde{\Pi}$ IS JUST AN IDEALIZED SCHEME, AND WON'T BE USED IN PRACTICE.

Enc IS DEFINED SIMILARLY TO Enc^F :

$r \leftarrow \{0,1\}^n$ THIS IS THE KEY NOW!
 return $\langle r, f(r) \oplus m \rangle$

SIMILARLY FOR Dec WE DO AS IN Enc^F . WE WANT NOW TO PROVE THAT $\tilde{\Pi}$ IS CPA-SECURE, WITHOUT ANY ASSUMPTION. TO DO THAT, WE JUST HAVE TO LOOK AT THE INTERACTION BETWEEN ANY ADVERSARY A AND $\tilde{\Pi}$ IN THE EXPERIMENT $\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}$. WHAT DOES A SEE ABOUT $\tilde{\Pi}$? IT CAN IN PARTICULAR QUERY THE ENCRYPTION ORACLE AND GET FROM IT SOME RESULTS, IN THE FOLLOWING FORM:



THE ADVERSARY, MOREOVER, ALSO RECEIVES THE "CHALLENGE CIPHERTEXT", NAMELY $\langle r, c \rangle$ SUCH THAT $s = f(r) \oplus mb$

THE REASONING WE ARE GOING TO DO IS BASED ON THE PROBABILISTIC EVENT $r = r_a$, THAT WE CALL Repeat.

- IF Repeat HOLDS, THEN THE ADVERSARY CAN EASILY WIN, BECAUSE (S)HE COULD DETERMINE $f(r) = f(r_a)$ AND THUS mb
- IF Repeat DOES NOT HOLD, THEN A CANNOT GUESS ANYTHING ABOUT b , BECAUSE $f(r)$ WOULD BE A GENUINELY RANDOM VALUE ABOUT WHICH A KNOWS NOTHING.

$$P(A) = Pr(B) \cdot Pr(A|B) + Pr(\neg B) \cdot Pr(A|\neg B)$$

NOW

$$Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n) = 1) = Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n) = 1 | \text{Repeat}) \cdot Pr(\text{Repeat}) + Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n) = 1 | \neg \text{Repeat}) \cdot Pr(\neg \text{Repeat})$$

$$= 1 \cdot Pr(\text{Repeat}) + \frac{1}{2} \cdot 1$$

THIS CANNOT BE TOO BIG BECAUSE $Pr(\text{Repeat}) \leq q(n)/2^n$ WHERE q IS A POLYNOMIAL AS A CONSEQUENCE $Pr(\text{Repeat})$ IS UPPER-BOUNDED BY $q(n)/2^n$, THANKS TO THE FACT THAT $r = r_a$ IS A FIXED STRING, AND EXPLOITING UNION BOUNDS $Pr(A|B) \leq Pr(A) + Pr(B)$

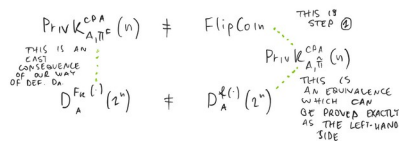
$$\leq \frac{q(n)}{2^n} + \frac{1}{2} = \frac{1}{2} + \epsilon(n)$$

NEGLIGIBLE

② THE SECOND PART IS A PROPER REDUCTION. IN PARTICULAR, WE ASSUME A BREAKS $\tilde{\Pi}$, NAMELY THAT $Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n))$ IS $\frac{1}{2} + \eta(n)$ WHERE η IS NOT NEGLIGIBLE, AND WE BUILD FROM A , A DISTINGUISHER D_A FOR F :

FUNCTION $D_A(2^n)$ // D_A HAS ACCESS TO AN ORACLE FOR EITHER $F_k(\cdot)$ OR $f(\cdot)$

- WE CALL $A(2^n)$ AND WAIT UNTIL IT PRODUCES m_1, m_2 .
- IF IN THE MEANTIME, A CALLS THE ORACLE FOR $\text{Enc}_k(\cdot)$ ON A VALUE m_i , WE PROCEED BY:
 - CREATING A RANDOM VALUE r
 - FEEDING A WITH r , OBTAINING s .
 - WE COMPUTE $s \oplus m_i$
 - WE RETURN $\langle r, s \rangle$
- WE DRAW b AT RANDOM
- WE COMPUTE THE ENCRYPTION OF m_b BY USING H THUS SIMULATING Enc_k
- WE FEED THE OBTAINED CIPHERTEXT TO A WHICH RETURNS b^* . IF A QUERIES $\text{Enc}_k(\cdot)$ WE HAVE TO PROCEED AS BEFORE.
- WE RETURN $\neg(b \neq b^*)$



IN OTHER WORDS

$$|Pr(D_A^{F_k(\cdot)}(2^n) = 1) - Pr(D_A^{f(\cdot)}(2^n) = 1)| = |Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n) = 1) - Pr(\text{PrivK}_{A,\tilde{\Pi}}^{\text{CPA}}(n) = 1)| = \frac{1}{2} + \eta(n) - \frac{1}{2} = \eta(n)$$

AND η IS NOT NEGLIGIBLE!