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, $\tilde{\Pi} = (\tilde{Gen}, \tilde{Enc}, \tilde{Dec})$ WHERE

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

$$2^n \text{ ROWS} \left\{ \begin{array}{|c|c|} 000\ldots0 & \\ 000\ldots1 & \\ \vdots & \\ 111\ldots1 & \underbrace{\qquad\qquad}_{n \text{ BITS}} \end{array} \right. \quad \leftarrow \text{RANDOM BITS}$$

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

- $\tilde{Enc}$ 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 $\tilde{Dec}$: WE DO AS IN $\tilde{Enc}$

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 $PrivK^{CPA}$. WHAT DOES A <u>SEE</u> ABOUT $\tilde{\Pi}$? IT CAN IN PARTICULAR QUERY THE ENCRYPTION ORACLE AND GET FROM IT SOME RESULTS, IN THE FOLLOWING FORM:

$$\langle d_1, \langle r_1, s_1 \rangle\rangle, \langle d_2, \langle r_2, s_2 \rangle\rangle, \ldots, \langle d_\ell, \langle r_\ell, s_\ell \rangle\rangle$$

MESSAGES

RANDOM VALUES GENERATED INTERNALLY BY $\tilde{Enc}$

$f(r_i) \oplus d_i$

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

- THE REASONING WE ARE GOING TO DO IS BASED ON THE PROBABILISTIC EVENT $r = r_i$, THAT WE CALL Repeat.
  - IF Repeat HOLDS, THEN THE ADVERSARY CAN EASILY WIN, BECAUSE (S)HE COULD DETERMINE $f(r) = f(r_i)$ AND THUS m_b
  - 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.

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

NOW

$$Pr\left(PrivK^{CPA}_{A,\tilde{\Pi}}(n) = 1\right) = \overbrace{Pr\left(PrivK^{CPA}_{A,\tilde{\Pi}}(n) = 1 \mid Repeat\right)}^{1} \cdot Pr(Repeat) + \underbrace{Pr\left(PrivK^{CPA}_{A,\tilde{\Pi}}(n) = 1 \mid \neg Repeat\right)}_{1/2} \cdot \underbrace{Pr(\neg Repeat)}_{1}$$

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

THIS CANNOT BE TOO BIG BECAUSE $\ell \leq q(n)$ WHERE q IS A POLYNOMIAL. AS A CONSEQUENCE $Pr(Repeat)$ IS UPPER-BOUNDED BY $q(n)/2^n$, THANKS TO THE FACT THAT $Pr(r = r_i) = 1/2^n$ IF r IS A FIXED STRING, AND EXPLOITING UNION BOUNDS $Pr(A \cup B) \leq Pr(A) + Pr(B)$

$$\leq \underbrace{\frac{q(n)}{2^n}}_{\text{NEGLIGIBLE}} + \frac{1}{2} = \frac{1}{2} + \varepsilon(n)$$

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

function $D_A(1^n)$ // D_A HAS ACCESS TO AN ORACLE FOR EITHER $F_k(\cdot)$ OR $f(\cdot)$ CALL IT H

- WE CALL $A(1^n)$ AND WAIT UNTIL IT PRODUCES m_0, m_1.
  IF IN THE MEANTIME, A CALLS THE ORACLE FOR $Enc_k(\cdot)$ ON A VALUE m, WE PROCEED BY
  - CREATING A RANDOM VALUE r
  - FEEDING H WITH r, OBTAING s.
  - WE COMPUTE $s \oplus m = t$
  - WE RETURN $\langle r, t \rangle$
- 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 $Enc_k(\cdot)$ WE HAVE TO PROCEED AS BEFORE.
- WE return $\neg(b \oplus b^*)$

$$PrivK^{CPA}_{A,\Pi^F}(n) \quad \neq \quad FlipCoin$$

THIS IS STEP (1)

$$PrivK^{CPA}_{A,\tilde{\Pi}}(n)$$

THIS IS AN EASY CONSEQUENCE OF OUR WAY OF DEF. D_A

$$D_A^{F_k(\cdot)}(1^n) \quad \neq \quad D_A^{f(\cdot)}(1^n)$$

THIS IS AN EQUIVALENCE WHICH CAN BE PROVED EXACTLY AS THE LEFT-HAND-SIDE

IN OTHER WORDS

$$\left| Pr\left(D_A^{F_k(\cdot)}(1^n) = 1\right) - Pr\left(D_A^{f(\cdot)}(1^n) = 1\right) \right|$$

$$= \left| Pr\left(PrivK^{CPA}_{A,\Pi^F}(n) = 1\right) - Pr\left(PrivK^{CPA}_{A,\tilde{\Pi}}(n) = 1\right) \right|$$

$$= \left| \frac{1}{2} + \eta(n) - \frac{1}{2} \right| = \eta(n)$$

AND η IS NOT NEGLIGIBLE!