

# Securitatea Sistemelor Informatice



## - Curs 5.1 - Scheme de criptare CPA-sigure bazate pe PRF

Adela Georgescu

Facultatea de Matematică și Informatică  
Universitatea din București  
Anul universitar 2022-2023, semestrul I

## Sisteme de criptare bloc - observații

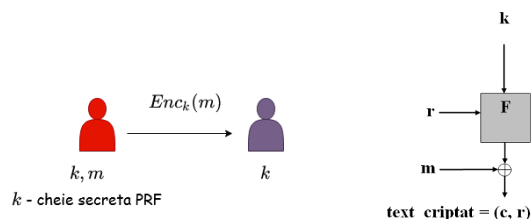
- ▶ Sistemele de criptare bloc sunt instanțieri sigure ale PRP  
Pentru  $n$  suficient de mare, un PRP este indistinctibil de un PRF
- ▶ reamintim că pentru PRP avem nevoie și de invertibilitate, dar pentru un  $n$  suficient de mare, un PRP este și un PRF
- ▶ în practică, sistemele de criptare bloc sunt și PRF bune, nu doar PRP-uri bune, deci le putem folosi oricând avem nevoie de una din cele două construcții

Securitatea Sistemelor Informatice

2/7

## Sistem de criptare CPA-sigur

- ▶ Sistemele de criptare bloc sunt instanțieri sigure ale PRP



- ▶ Fie  $F_k$  o funcție cu cheie
- ▶  $\text{Gen}(1^n)$ : alege uniform cheie  $k \in \{0, 1\}^n$
- ▶  $\text{Enc}_k(m)$ : pentru  $|m| = |k|$ , alege  $r$  uniform în  $\{0, 1\}^n$

$$\text{Enc}_k(m) = (r, F_k(r) \oplus m)$$

- ▶  $\text{Dec}_k(c = (c_0, c_1))$ : întoarce  $c_1 \oplus F_k(c_0)$

Securitatea Sistemelor Informatice

3/7

## Observații

- ▶ cheia este la fel de lungă precum mesajul - la fel ca la OTP
- ▶ dar, spre deosebire de OTP, se pot cripta **mai multe mesaje cu aceeași cheie** în siguranță

Securitatea Sistemelor Informatice

4/7

## Sistem de criptare CPA-sigur

### Teoremă

Dacă  $F$  este PRF, construcția anterioară este o schemă de criptare CPA-sigură pentru mesaje de lungime  $n$ .

### Schița demonstrației

Considerăm  $(\bar{\Pi} = \bar{\text{Gen}}, \bar{\text{Enc}}, \bar{\text{Dec}})$  care se obține din schema anterioară  $(\Pi = \text{Gen}, \text{Enc}, \text{Dec})$  unde  $F_k$  - PRF este înlocuită cu  $f$  aleatoare. Fie  $\mathcal{A}$  - adversar PPT și  $q(n)$  numărul maxim de interogări ale oracolului de criptare efectuate de  $\mathcal{A}$ . Arătăm:

1.  $\mathcal{A}$  nu poate distinge între  $\Pi$  și  $\bar{\Pi}$  decât cu probabilitate neglijabilă adică: există o funcție neglijabilă  $\text{negl}$  așa încât:

$$|Pr[Priv_{\mathcal{A}, \Pi}^{cpa}(n) = 1] - Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1]| \leq \text{negl}(n)$$

## Sistem de criptare CPA-sigur

$$2. Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}.$$

- ▶ la fiecare criptare a lui  $m$  - interogare la oracol sau ca provocare de la Challenger - se alege  $r \in \{0, 1\}^n$  iar  $c = (r, f(r) \oplus m)$ .
- ▶ fie  $(\tilde{r}, f(\tilde{r}) \oplus m_b)$  provocarea primită de  $\mathcal{A}$ . Există 2 variante:
  1. valoarea  $\tilde{r}$  nu este folosită niciodată ca răspuns de către oracolul de criptare  $\Rightarrow Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] = \frac{1}{2}$
  2. valoarea  $\tilde{r}$  este folosită cel puțin o dată ca răspuns la interogările oracolului de criptare  $\Rightarrow \mathcal{A}$  poate calcula  $m_b$ . El primește răspuns de la oracolul de criptare  $Enc(m) = (\tilde{r}, s)$  și calculează  $f(\tilde{r}) = s \oplus m$ .  $Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] \leq \frac{q(n)}{2^n}$ .
- ▶ Notăm cu  $Ev$  evenimentul de la 2. și cu  $\neg Ev$  evenimentul de la 1. Atunci:  $Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] = Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] \wedge Ev + Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] \wedge \neg Ev$

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

## Sistem de criptare CPA-sigur

- ▶ Am obținut că  $Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1] \leq \frac{q(n)}{2^n} + \frac{1}{2}$ .
- ▶ Am stabilit de asemenea că  $|Pr[Priv_{\mathcal{A}, \Pi}^{cpa}(n) = 1] - Pr[Priv_{\mathcal{A}, \bar{\Pi}}^{cpa}(n) = 1]| \leq \text{negl}(n)$
- ▶ Din ambele relații avem  $Pr[Priv_{\mathcal{A}, \Pi}^{cpa}(n) = 1] \leq \frac{q(n)}{2^n} + \frac{1}{2} + \text{negl}(n)$ , ceea ce încheie demonstrația.