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

Sisteme de criptare bloc - observații

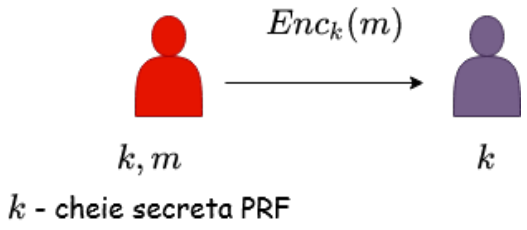
- Sistemele de criptare bloc sunt instanțieri sigure ale PRP
  Pentru n suficient de mare, un PRP este indistinctibil de un PRF
- reamintim că pentru PRP avem nevoie și de invertibilitate, dar pentru un n suficient de mare, un PRP este și un PRF

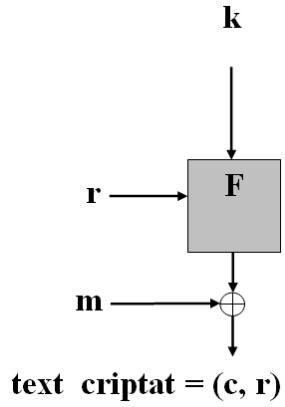
Sisteme de criptare bloc - observații

- 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

Sistem de criptare CPA-sigur

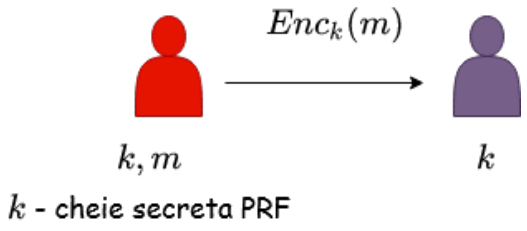
- Sistemele de criptare bloc sunt instanțieri sigure ale PRP

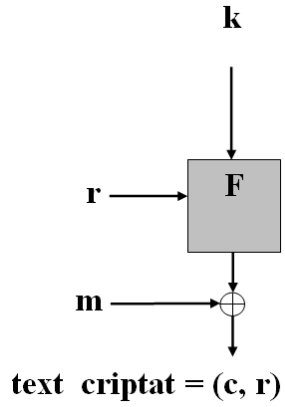




Sistem de criptare CPA-sigur

- Sistemele de criptare bloc sunt instanțieri sigure ale PRP

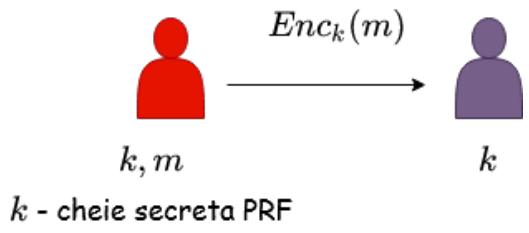


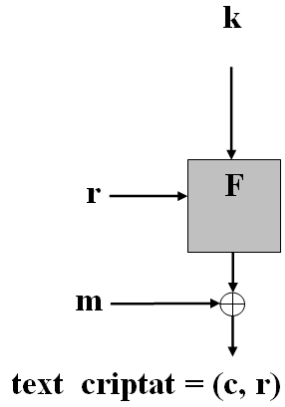


- Fie F_k o funcție cu cheie

Sistem de criptare CPA-sigur

- Sistemele de criptare bloc sunt instanțieri sigure ale PRP

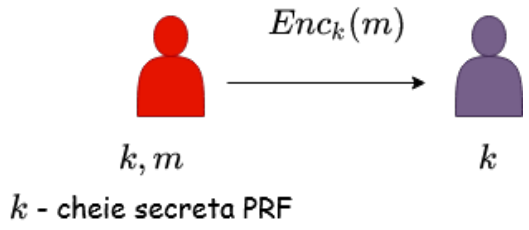


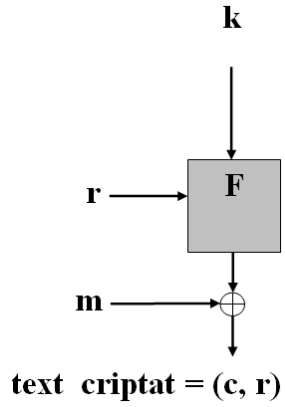


- Fie F_k o funcție cu cheie
- $\mathrm{Gen}(1^n)$: alege uniform cheie $k \in \{0,1\}^n$

Sistem de criptare CPA-sigur

- Sistemele de criptare bloc sunt instanțieri sigure ale PRP



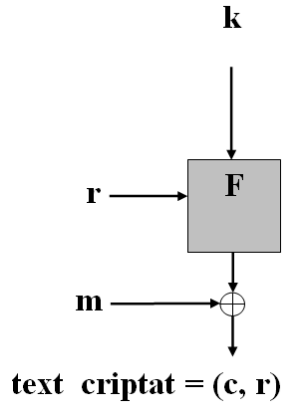


- Fie F_k o funcție cu cheie
- $\mathrm{Gen}(1^n)$: alege uniform cheie $k \in \{0,1\}^n$
- $\mathrm{Enc_k(m)}$: pentru $|m| = |k|$, alege r uniform în $\{0,1\}^n$

$$Enc_k(m) = (r, F_k(r) \oplus m)$$

Sistem de criptare CPA-sigur

- Sistemele de criptare bloc sunt instanțieri sigure ale PRP



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

$$Enc_k(m) = (r, F_k(r) \oplus m)$$

- $\mathrm{Dec_k(c = (c_0, c_1))}$: întoarce $c_1 \oplus F_k(c_0)$

Observații

- cheia este la fel de lungă precum mesajul - la fel ca la OTP

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

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 $(\overline{\Pi} = \overline{\mathrm{Gen}}, \overline{\mathrm{Enc}}, \overline{\mathrm{Dec}})$ *care se obține din schema anterioară* $(\Pi = \mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ *unde* F_k *- PRF este înlocuită cu f aleatoare.*

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

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

1. $\mathcal{A}$ *nu poate distinge între* Π *si* $\overline{\Pi}$ *decât cu probabilitate neglijabilă adică: există o funcție neglijabilă* $\mathtt{negl}$ *așa încât:*

$$|Pr[Priv^{cpa}_{\mathcal{A},\pi}(n) = 1] - Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1]| \leq \mathtt{negl(n)}$$

Sistem de criptare CPA-sigur

2. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
   - la fiecare criptare a lui m - interogare la oracol sau ca provocare de la Challenger - se alege $r \in \{0,1\}^n$ iar $c = (r, f(r) \oplus m)$.

Sistem de criptare CPA-sigur

2. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
   - 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:

Sistem de criptare CPA-sigur

2. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
   - 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 $\Rightarrow Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] = \frac{1}{2}$

Sistem de criptare CPA-sigur

2. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
   - 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 $\Rightarrow Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] = \frac{1}{2}$
     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 $f(\tilde{r}) = s \oplus m$. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{q(n)}{2^n}$.

Sistem de criptare CPA-sigur

2. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$.
   - 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 $\Rightarrow Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] = \frac{1}{2}$
     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 $f(\tilde{r}) = s \oplus m$. $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{q(n)}{2^n}$.
   - Notăm cu Ev evenimentul de la 2. și cu $\neg Ev$ evenimentul de la 1. Atunci: $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] =$
   $= Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \wedge Ev + Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \wedge \neg Ev$

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

.

Sistem de criptare CPA-sigur

- Am obținut că $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{q(n)}{2^n} + \frac{1}{2}$.

Sistem de criptare CPA-sigur

- Am obținut că $Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1] \leq \frac{q(n)}{2^n} + \frac{1}{2}$.
- Am stabilit de asemenea că
  $|Pr[Priv^{cpa}_{\mathcal{A},\pi}(n) = 1] - Pr[Priv^{cpa}_{\mathcal{A},\overline{\pi}}(n) = 1]| \leq \mathtt{negl(n)}$

Sistem de criptare CPA-sigur

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