

Securitatea Sistemelor Informatice



- Curs 5.2 - Securitate CCA

Adela Georgescu

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

Scenarii de atac activ

- ▶ Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
 - ▶ Atac cu text clar ales - chosen plaintext attack (CPA):
Atacatorul poate obține criptarea unor texte clare alese de el;

Scenarii de atac activ

- ▶ Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
 - ▶ Atac cu text clar ales - chosen plaintext attack (CPA):
Atacatorul poate obține criptarea unor texte clare alese de el;
 - ▶ Atac cu text criptat ales - chosen ciphertext attack (CCA):
Atacatorul are posibilitatea să obțină decriptarea unor texte criptate alese de el.

Scenarii de atac activ

- ▶ In aceste scenarii de atac adversarul are putere crescută;

Scenarii de atac activ

- ▶ In aceste scenarii de atac adversarul are putere crescută;
- ▶ Acesta devine un adversar **activ**, care primește abilitatea de a obține criptarea și / sau decriptarea unor mesaje, respectiv texte criptate alese de el;

Scenarii de atac activ

- ▶ În aceste scenarii de atac adversarul are putere crescută;
- ▶ Acesta devine un adversar **activ**, care primește abilitatea de a obține criptarea și / sau decriptarea unor mesaje, respectiv texte criptate alese de el;
- ▶ În plus, adversarul poate alege mesajele sau textele criptate în mod **adaptiv** în funcție de răspunsurile primite precedent.

Noțiuni de securitate

- ▶ Definim astfel 2 noțiuni de securitate:

Noțiuni de securitate

- ▶ Definim astfel 2 noțiuni de securitate:
 - ▶ CPA (Chosen-Plaintext Attack): adversarul poate să obțină criptarea unor mesaje alese de el; - discutată în cursul anterior

Noțiuni de securitate

- ▶ Definim astfel 2 noțiuni de securitate:
 - ▶ CPA (Chosen-Plaintext Attack): adversarul poate să obțină criptarea unor mesaje alese de el; - **discutată în cursul anterior**
 - ▶ CCA (Chosen-Ciphertext Attack): adversarul poate să obțină criptarea unor mesaje alese de el și decriptarea unor texte criptate alese de el.

Securitate CCA

- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de criptare** și cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;

Securitate CCA

- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de criptare** și cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;
- ▶ Adversarul poate transmite către oracolul de criptare orice mesaj m și primește înapoi textul criptat corespunzător sau poate transmite către oracolul de decriptare *anumite* mesaje c și primește înapoi mesajul clar corespunzător;

Securitate CCA

- ▶ Capabilitățile adversarului: el poate interacționa cu un **oracol de criptare** și cu un **oracol de decriptare**, fiind un adversar *activ* care poate rula atacuri în timp polinomial;
- ▶ Adversarul poate transmite către oracolul de criptare orice mesaj m și primește înapoi textul criptat corespunzător sau poate transmite către oracolul de decriptare *anumite* mesaje c și primește înapoi mesajul clar corespunzător;
- ▶ Dacă sistemul de criptare este nedeterminist, atunci oracolul de criptare folosește de fiecare dată o valoare aleatoare nouă și neutilizată anterior.

Securitate CCA

- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;

Securitate CCA

- ▶ Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- ▶ Vom defini securitatea CCA pe baza unui experiment de indistinctibilitate $Priv_{\mathcal{A}, \pi}^{cca}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de securitate al schemei π ;

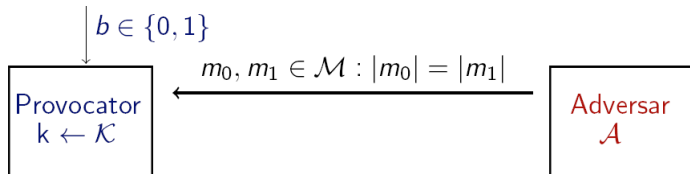
Securitate CCA

- ▶ Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- ▶ Vom defini securitatea CCA pe baza unui experiment de indistinctibilitate $Priv_{\mathcal{A}, \pi}^{cca}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de securitate al schemei π ;
- ▶ Personajele participante: **adversarul** \mathcal{A} care încearcă să spargă schema și un **provocator (challenger)**;

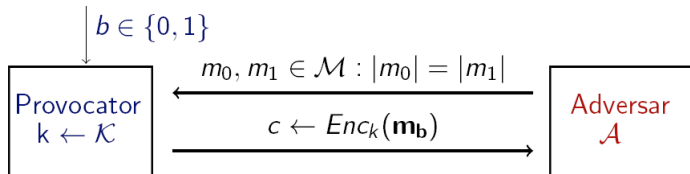
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



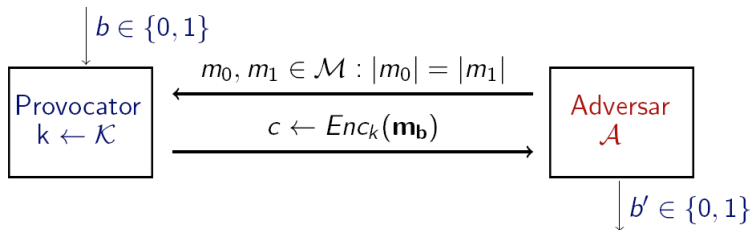
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



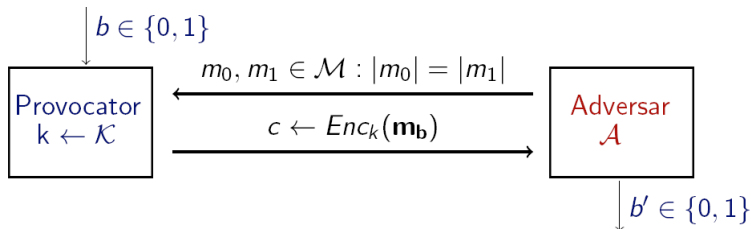
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$

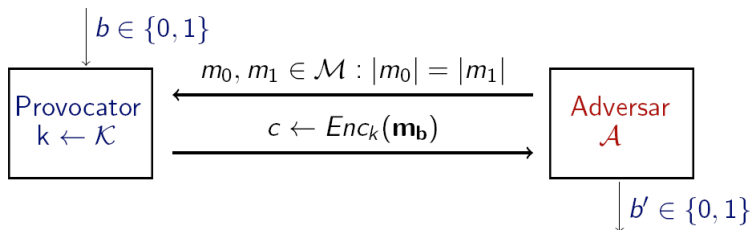


Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



- Pe toată durata experimentului, \mathcal{A} are acces la oracolul de criptare $\text{Enc}_k(\cdot)$ și la oracolul de decriptare $\text{Dec}_k(\cdot)$ cu restricția că nu poate decripta c !

Experimentul $\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n)$



- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel. Dacă $\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n) = 1$, spunem că \mathcal{A} a efectuat experimentul cu succes.

Experimentul $\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n)$

Definiție

O schemă de criptare $\pi = (\text{Enc}, \text{Dec})$ este **CCA-sigură** dacă pentru orice adversar PPT \mathcal{A} există o funcție neglijabilă negl așa încât

$$\Pr[\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

Experimentul $\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n)$

Definiție

O schemă de criptare $\pi = (\text{Enc}, \text{Dec})$ este **CCA-sigură** dacă pentru orice adversar PPT \mathcal{A} există o funcție neglijabilă negl așa încât

$$\Pr[\text{Priv}_{\mathcal{A},\pi}^{\text{cca}}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

- Un adversar nu poate determina care text clar a fost criptat cu o probabilitate semnificativ mai mare decât dacă ar fi ghicit (în sens aleator, dat cu banul), chiar dacă are acces la oracolele de criptare și decriptare.

Securitate CCA

- ▶ **Întrebare:** Un sistem de criptare CCA-sigur este întotdeauna CPA-sigur?

Securitate CCA

- ▶ **Întrebare:** Un sistem de criptare CCA-sigur este întotdeauna CPA-sigur?
- ▶ **Răspuns:** DA! Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cpa}}(n)$ este $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$ în care \mathcal{A} nu folosește oracolul de decriptare.

Securitate CCA

- ▶ **Întrebare:** Un sistem de criptare CCA-sigur este întotdeauna CPA-sigur?
- ▶ **Răspuns:** DA! Experimentul $Priv_{\mathcal{A}, \pi}^{cpa}(n)$ este $Priv_{\mathcal{A}, \pi}^{cca}(n)$ în care \mathcal{A} nu folosește oracolul de decriptare.
- ▶ **Întrebare:** Un sistem de criptare determinist poate fi CCA-sigur?

Securitate CCA

- ▶ **Întrebare:** Un sistem de criptare CCA-sigur este întotdeauna CPA-sigur?
- ▶ **Răspuns:** DA! Experimentul $\text{Priv}_{\mathcal{A},\pi}^{cpa}(n)$ este $\text{Priv}_{\mathcal{A},\pi}^{cca}(n)$ în care \mathcal{A} nu folosește oracolul de decriptare.
- ▶ **Întrebare:** Un sistem de criptare determinist poate fi CCA-sigur?
- ▶ **Răspuns:** NU! Sistemul nu este CPA-sigur, deci nu poate fi CCA-sigur.

Securitate CCA - Criptare multiplă

- ▶ În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;

Securitate CCA - Criptare multiplă

- ▶ În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- ▶ În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;

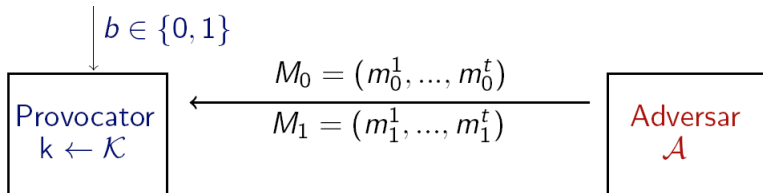
Securitate CCA - Criptare multiplă

- ▶ În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- ▶ În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;
- ▶ Definim ce înseamnă o schemă sigură chiar și în aceste condiții.

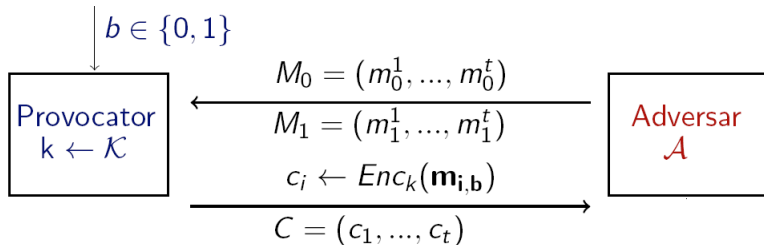
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



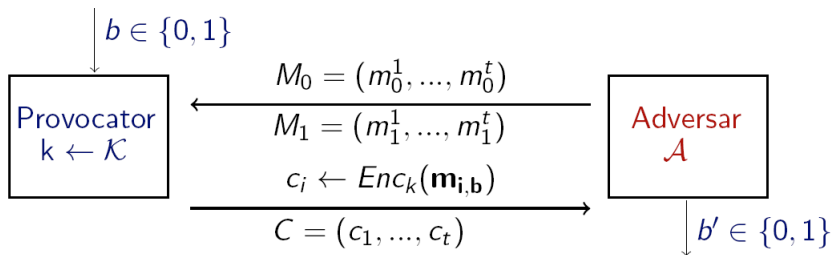
Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$

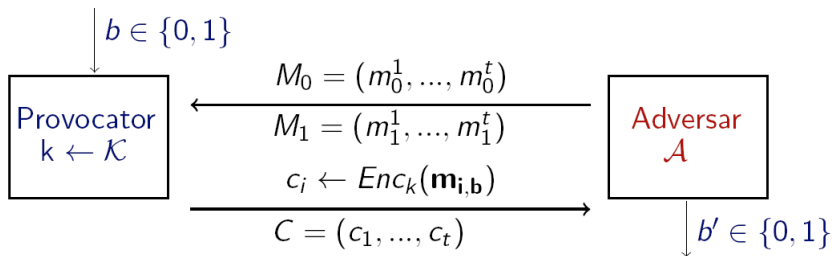


Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



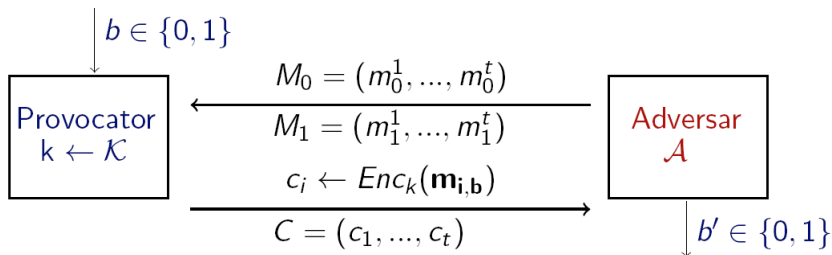
- Pe toată durata experimentului, \mathcal{A} are acces la oracolul de criptare $\text{Enc}_k(\cdot)$ și la oracolul decriptare $\text{Dec}_k(\cdot)$ cu restricția că nu poate decripta c_1, \dots, c_t !

Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



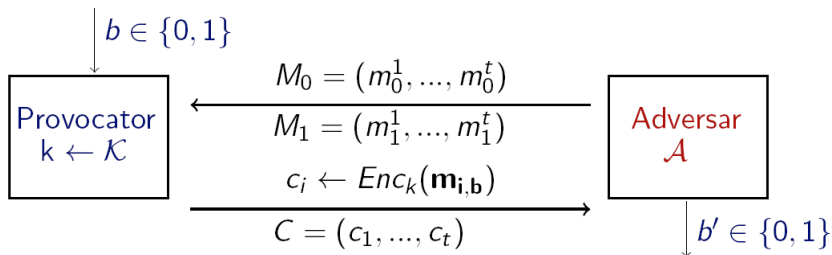
- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;

Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



- ▶ Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;
- ▶ Definiția de securitate este aceeași, doar că se referă la experimentul de mai sus.

Experimentul $\text{Priv}_{\mathcal{A}, \pi}^{\text{cca}}(n)$



- ▶ Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;
- ▶ Definiția de securitate este aceeași, doar că se referă la experimentul de mai sus.
- ▶ Securitatea pentru criptare **simplică** implică securitate pentru criptare **multiplă**!

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-signature.

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-secure.
- ▶ Arătăm pentru construcția anterioară, unde $Enc_k(m) = (r, F_k(r) \oplus m)$.

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-secure.
- ▶ Arătăm pentru construcția anterioară, unde $Enc_k(m) = (r, F_k(r) \oplus m)$.
- ▶ Considerăm că \mathcal{A} alege $m_0 = 0^n$ și $m_1 = 1^n$.

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-sigure.
- ▶ Arătăm pentru construcția anterioară, unde $Enc_k(m) = (r, F_k(r) \oplus m)$.
- ▶ Considerăm că \mathcal{A} alege $m_0 = 0^n$ și $m_1 = 1^n$.
- ▶ \mathcal{A} primește $c = (r, s)$, inversează primul bit al lui s și cere decriptarea textului rezultat c^* (permis deoarece $c^* \neq c$).

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-sigure.
- ▶ Arătăm pentru construcția anterioară, unde $Enc_k(m) = (r, F_k(r) \oplus m)$.
- ▶ Considerăm că \mathcal{A} alege $m_0 = 0^n$ și $m_1 = 1^n$.
- ▶ \mathcal{A} primește $c = (r, s)$, inversează primul bit al lui s și cere decriptarea textului rezultat c^* (permis deoarece $c^* \neq c$).
- ▶ Oracolul răspunde cu 10^{n-1} , și deci $b = 0$ sau cu 01^{n-1} , deci $b = 1 \Rightarrow Pr[Priv_{\mathcal{A}, \pi}^{cca}(n) = 1] = 1$.

Securitate CCA

- ▶ Nici una din schemele de criptare de până acum nu sunt CCA-sigure.
- ▶ Arătăm pentru construcția anterioară, unde $Enc_k(m) = (r, F_k(r) \oplus m)$.
- ▶ Considerăm că \mathcal{A} alege $m_0 = 0^n$ și $m_1 = 1^n$.
- ▶ \mathcal{A} primește $c = (r, s)$, inversează primul bit al lui s și cere decriptarea textului rezultat c^* (permis deoarece $c^* \neq c$).
- ▶ Oracolul răspunde cu 10^{n-1} , și deci $b = 0$ sau cu 01^{n-1} , deci $b = 1 \Rightarrow Pr[Priv_{\mathcal{A}, \pi}^{cca}(n) = 1] = 1$.
- ▶ Concluzie: orice schemă de criptare care permite ca textele criptate să fie modificate într-un mod controlat nu poate fi CCA-sigură.

Important de reținut!

- ▶ Securitate - interceptare simplă \Rightarrow securitate - interceptare multiplă
- ▶ Schemele deterministe nu sunt semantic / CPA / CCA sigure
- ▶ Securitate CCA \Rightarrow securitate CPA \Rightarrow securitate semantică

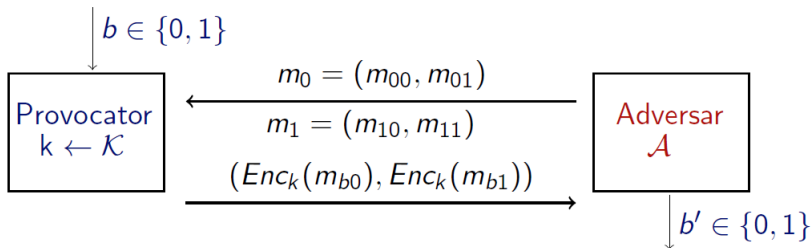
Exemplu

Fie (Enc, Dec) un sistem de criptare simetric. Se consideră sistemul de criptare (Enc', Dec') pentru mesaje de dimensiune dublă cu funcția de criptare definită astfel:

$$Enc'_k(m_1 || m_2) = (Enc_k(m_2), Enc_k(m_1))$$

Arătați că sistemul nu este CCA-sigur.

Rezolvare



\mathcal{A} transmite oracolului de decriptare $(Enc_k(m_{b0}), Enc_k(m_{b0}))$ și primește $m' = (m_{b0}, m_{b0})$, deci determină b' cu probabilitate 1.