Criptografie și Securitate

- Prelegerea 10 -
Securitate CPA și CCA

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Scenarii de atac

- Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
  - Atac cu text criptat: Atacatorul știe doar *textul criptat* - poate încerca un atac prin forță brută prin care se parcurg toate cheile până se găsește cea corectă;

Scenarii de atac

- Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
  - Atac cu text criptat: Atacatorul știe doar *textul criptat* - poate încerca un atac prin forță brută prin care se parcurg toate cheile până se găsește cea corectă;
  - Atac cu text clar: Atacatorul cunoaște una sau mai multe perechi *(text clar, text criptat)*;

Scenarii de atac

- Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
  - Atac cu text criptat: Atacatorul știe doar *textul criptat* - poate încerca un atac prin forță brută prin care se parcurg toate cheile până se găsește cea corectă;
  - Atac cu text clar: Atacatorul cunoaște una sau mai multe perechi *(text clar, text criptat)*;
  - Atac cu text clar ales: Atacatorul poate obține criptarea unor texte clare alese de el;

Scenarii de atac

- Reamintim câteva dintre scenariile de atac pe care le-am mai întâlnit:
  - Atac cu text criptat: Atacatorul știe doar *textul criptat* - poate încerca un atac prin forță brută prin care se parcurg toate cheile până se găsește cea corectă;
  - Atac cu text clar: Atacatorul cunoaște una sau mai multe perechi *(text clar, text criptat)*;
  - Atac cu text clar ales: Atacatorul poate obține criptarea unor texte clare alese de el;
  - Atac cu text criptat ales: Atacatorul are posibilitatea să obțină decriptarea unor texte criptate alese de el.

Scenarii de atac

- Ultimele 2 scenarii de atac oferă adversarului putere crescută;

Scenarii de atac

- Ultimele 2 scenarii de atac oferă adversarului 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

- Ultimele 2 scenarii de atac oferă adversarului 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;

Noțiuni de securitate

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

Securitate CPA

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

Securitate CPA

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

Securitate CPA

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

Securitate CPA

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

Securitate CPA

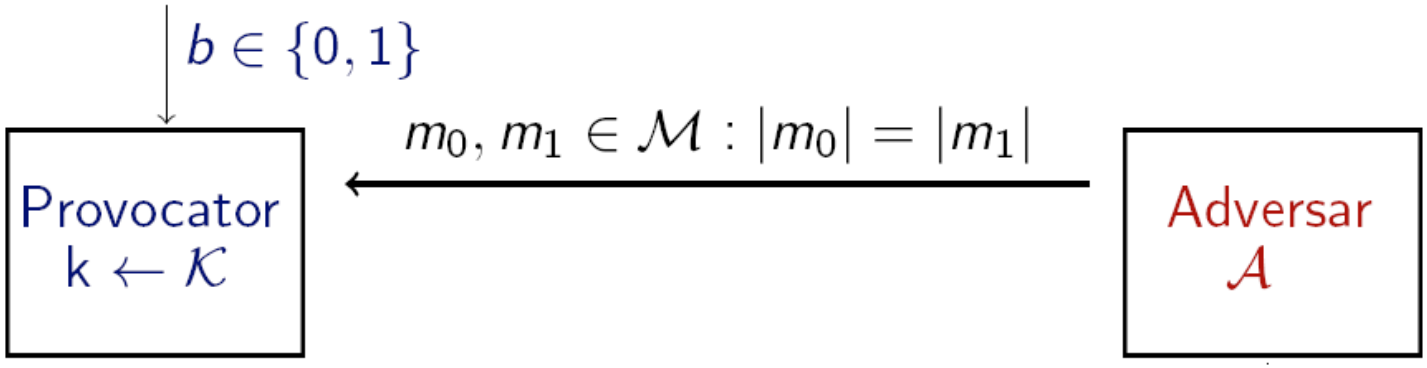
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CPA pe baza unui experiment de indistinctibilitate $Priv^{cpa}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

Securitate CPA

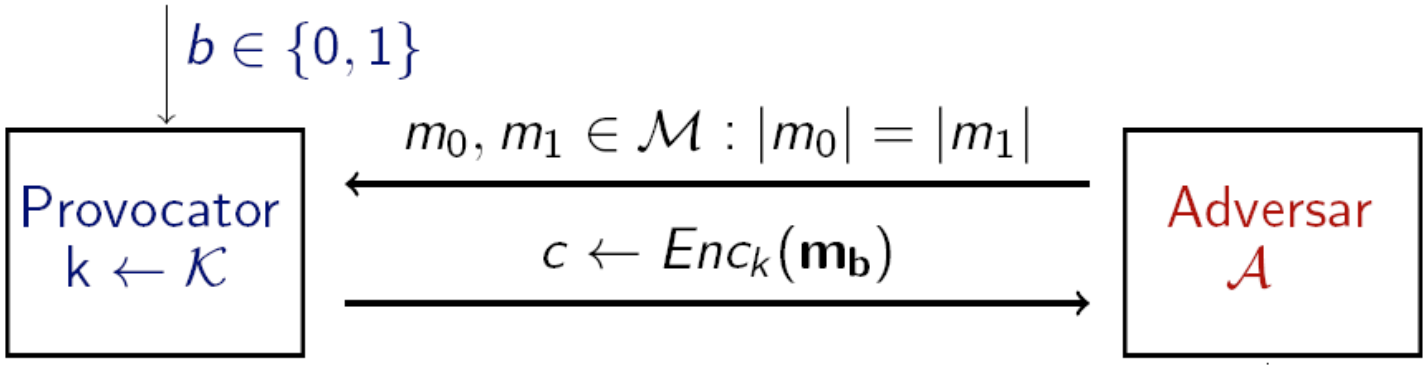
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CPA pe baza unui experiment de indistinctibilitate $Priv^{cpa}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

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

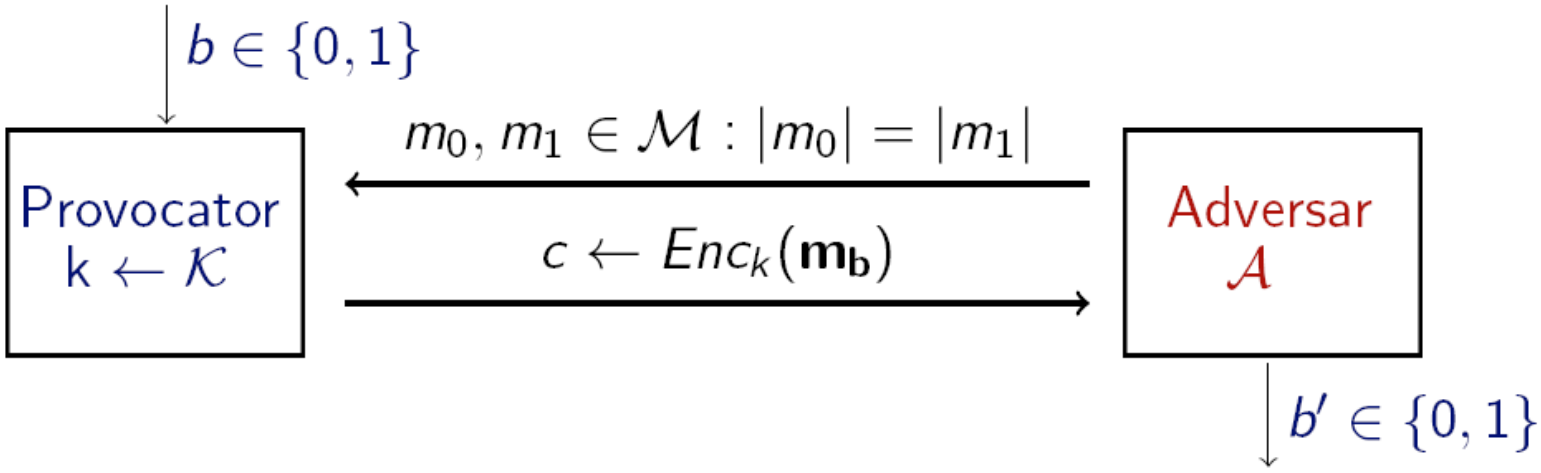
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



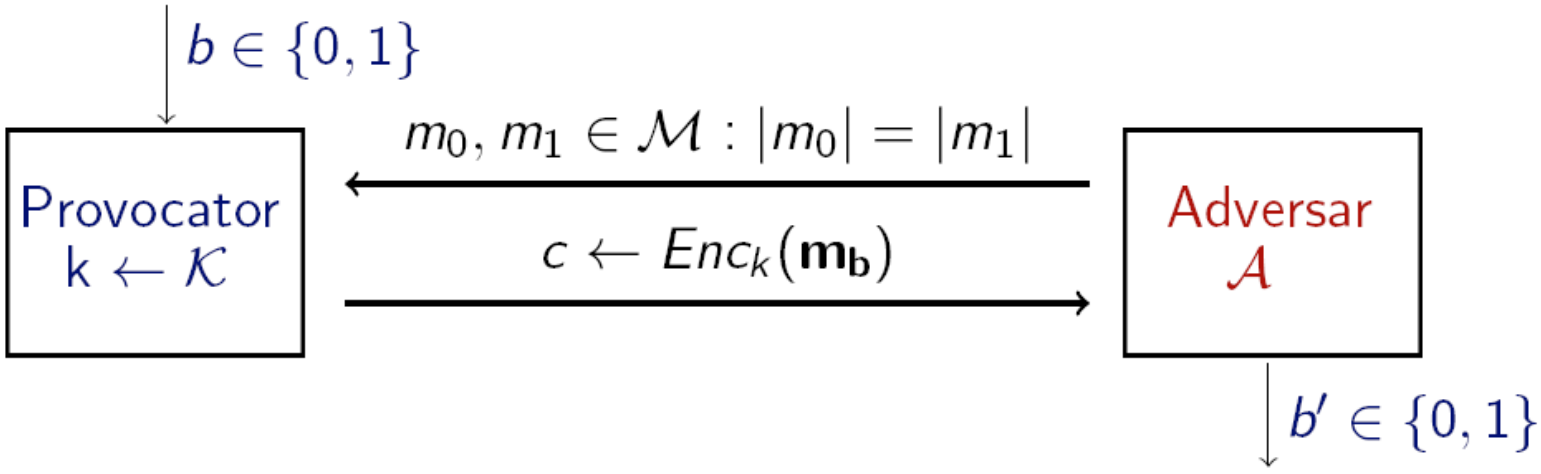
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



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

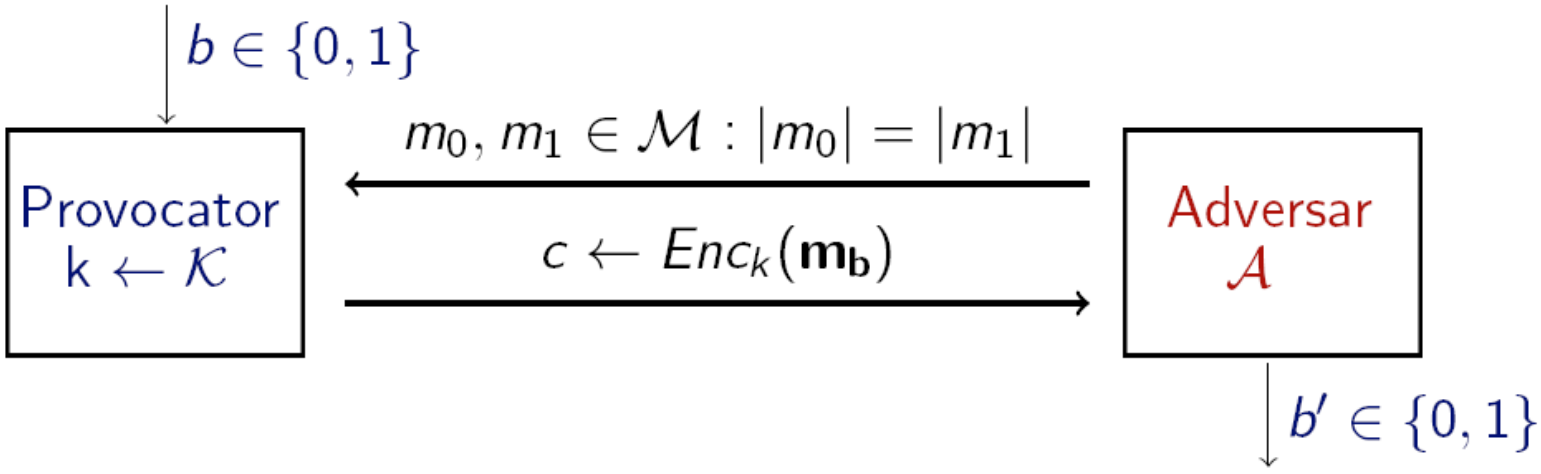


Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



- Pe toată durata experimentului, $\mathcal{A}$ are acces la oracolul de criptare $Enc_k(\cdot)$!

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



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

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

Definiție

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

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

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

Definiție

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

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

- 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 oracolul de criptare.

Securitate CPA

- Întrebare: Un sistem de criptare CPA-sigur este întotdeauna semantic sigur?

Securitate CPA

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

Securitate CPA

- Întrebare: Un sistem de criptare CPA-sigur este întotdeauna semantic sigur?
- Răspuns: DA! Experimentul $Priv^{eav}_{\mathcal{A},\pi}(n)$ este $Priv^{cpa}_{\mathcal{A},\pi}(n)$ în care $\mathcal{A}$ nu folosește oracolul de criptare.
- Întrebare: Un sistem de criptare determinist poate fi CPA-sigur?

Securitate CPA

- Întrebare: Un sistem de criptare CPA-sigur este întotdeauna semantic sigur?
- Răspuns: DA! Experimentul $Priv^{eav}_{\mathcal{A},\pi}(n)$ este $Priv^{cpa}_{\mathcal{A},\pi}(n)$ în care $\mathcal{A}$ nu folosește oracolul de criptare.
- Întrebare: Un sistem de criptare determinist poate fi CPA-sigur?
- Răspuns: NU! Adversarul cere oracolului criptarea mesajului m_0. Dacă textul criptat este egal cu c, atunci $b' = 0$, altfel $b' = 1$. În concluzie, $\mathcal{A}$ câștigă cu probabilitate 1.

Securitate CPA - Criptare multiplă

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

Securitate CPA - Criptare multiplă

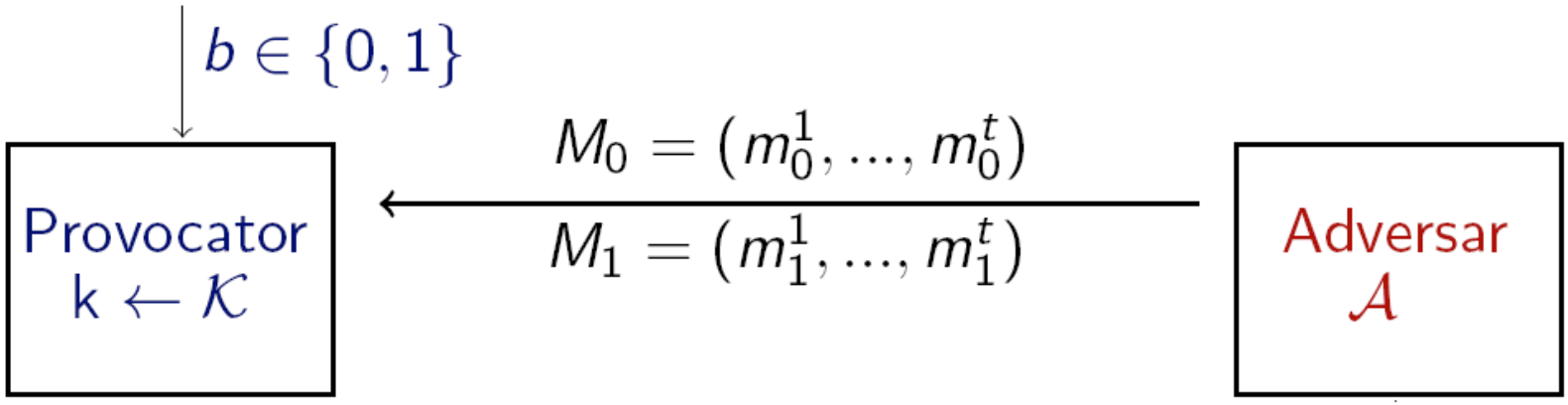
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;

Securitate CPA - Criptare multiplă

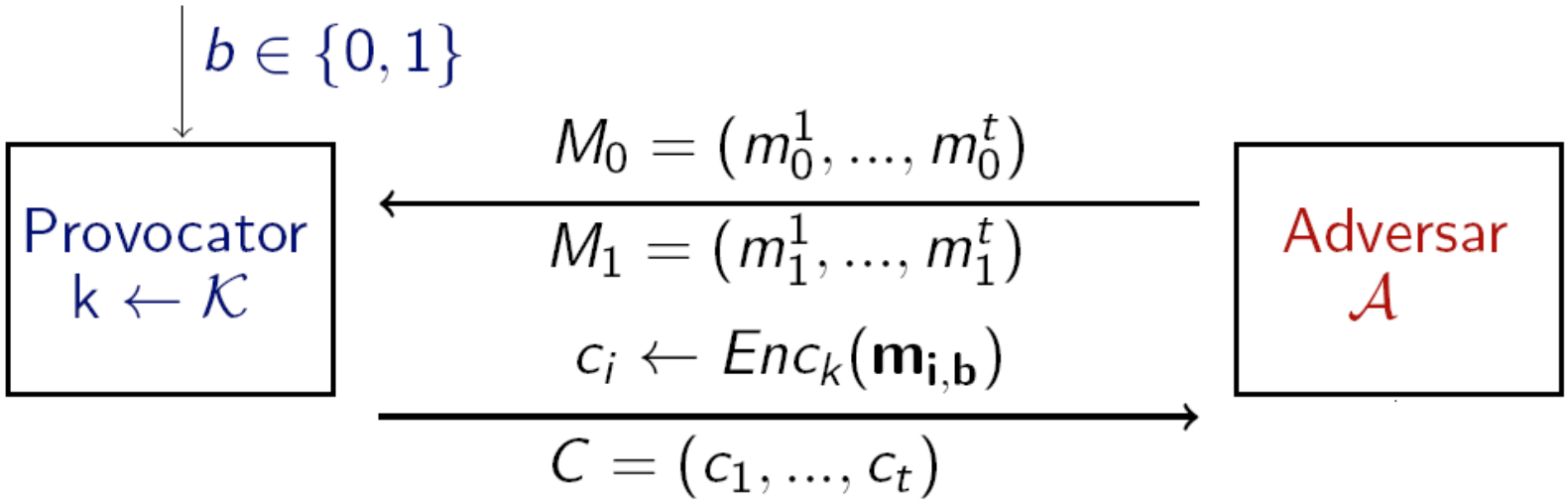
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;
- Definim ce înseamnă o schemă sigură chiar și în aceste condiții.

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

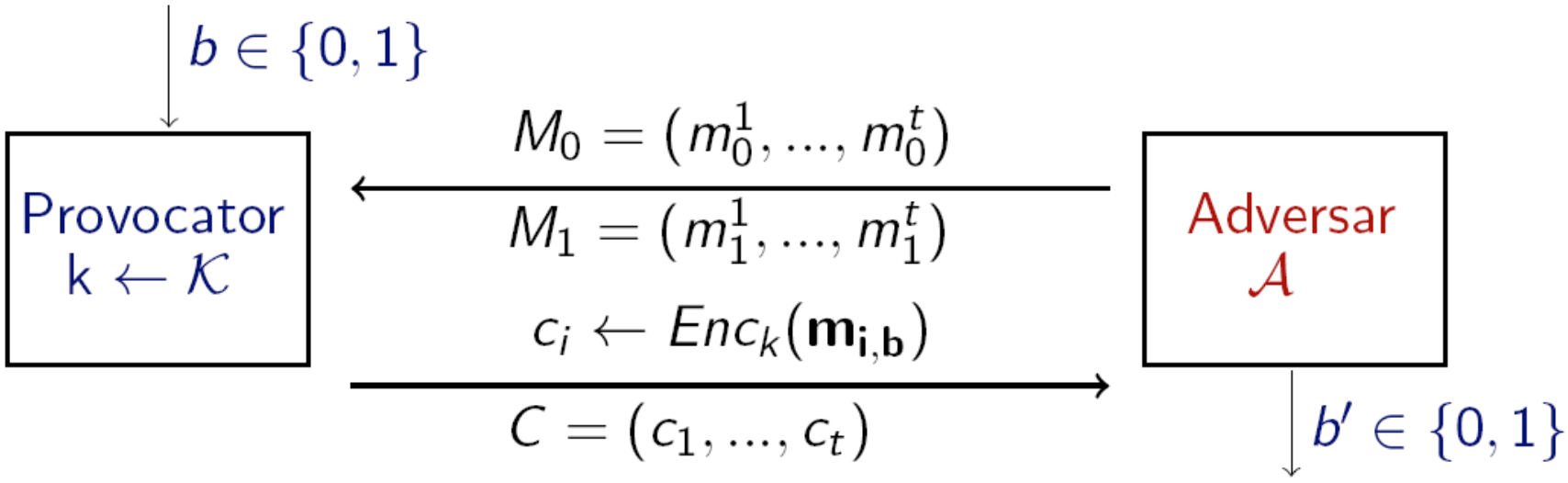
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



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

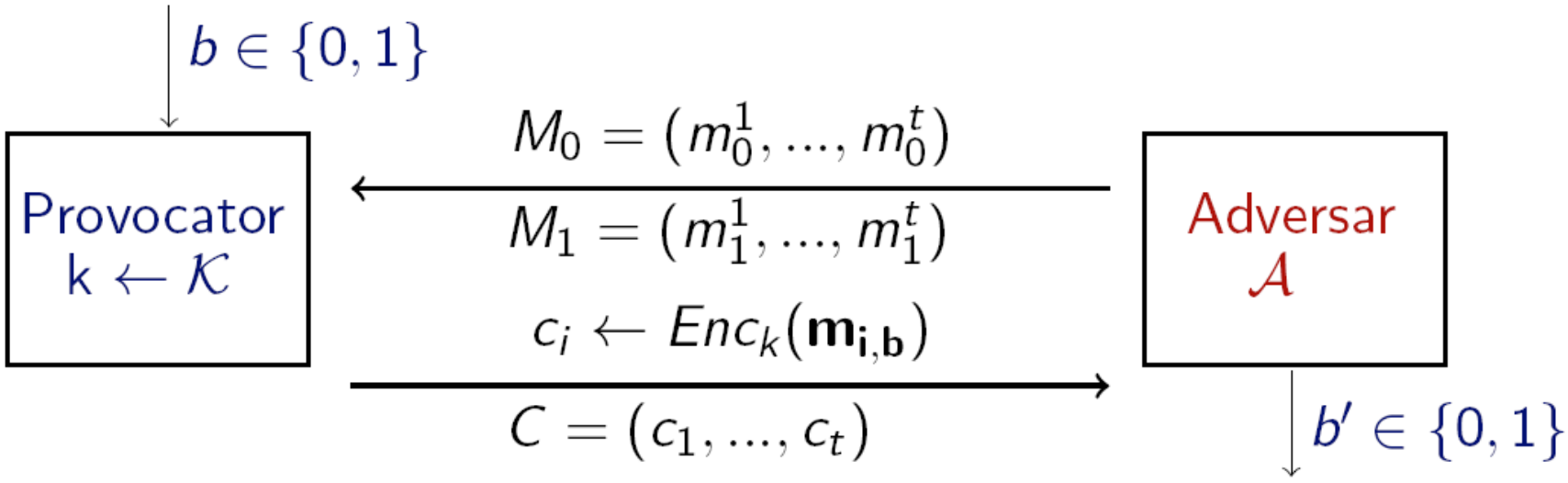


Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



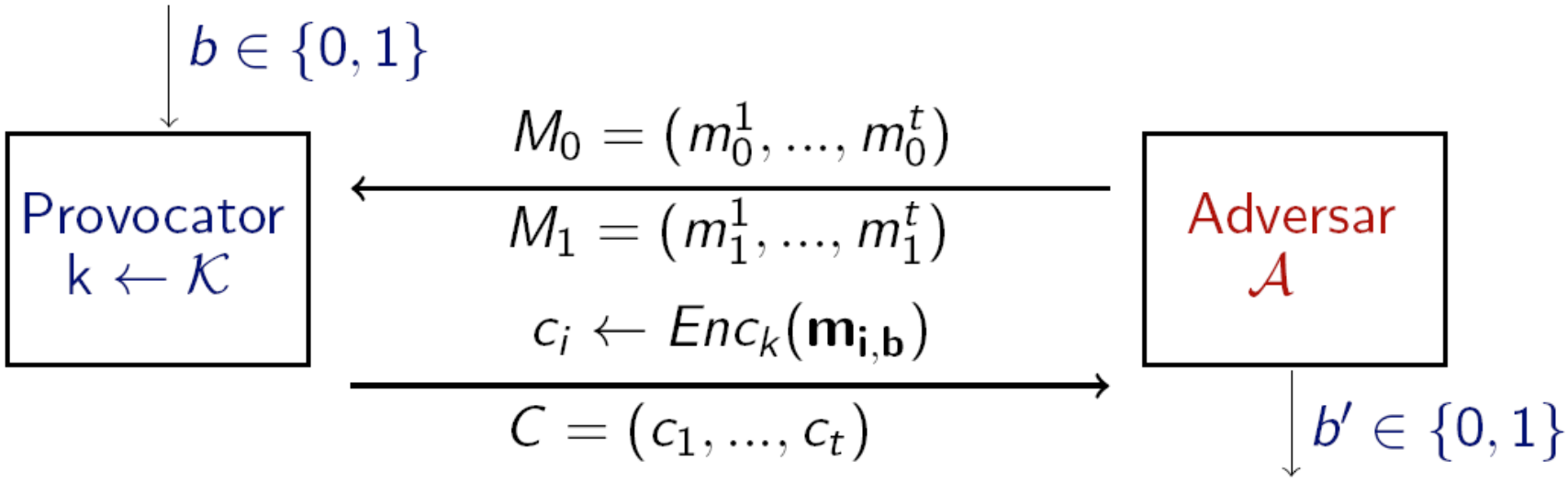
- Pe toată durata experimentului, $\mathcal{A}$ are acces la oracolul de criptare $Enc_k(\cdot)$!

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



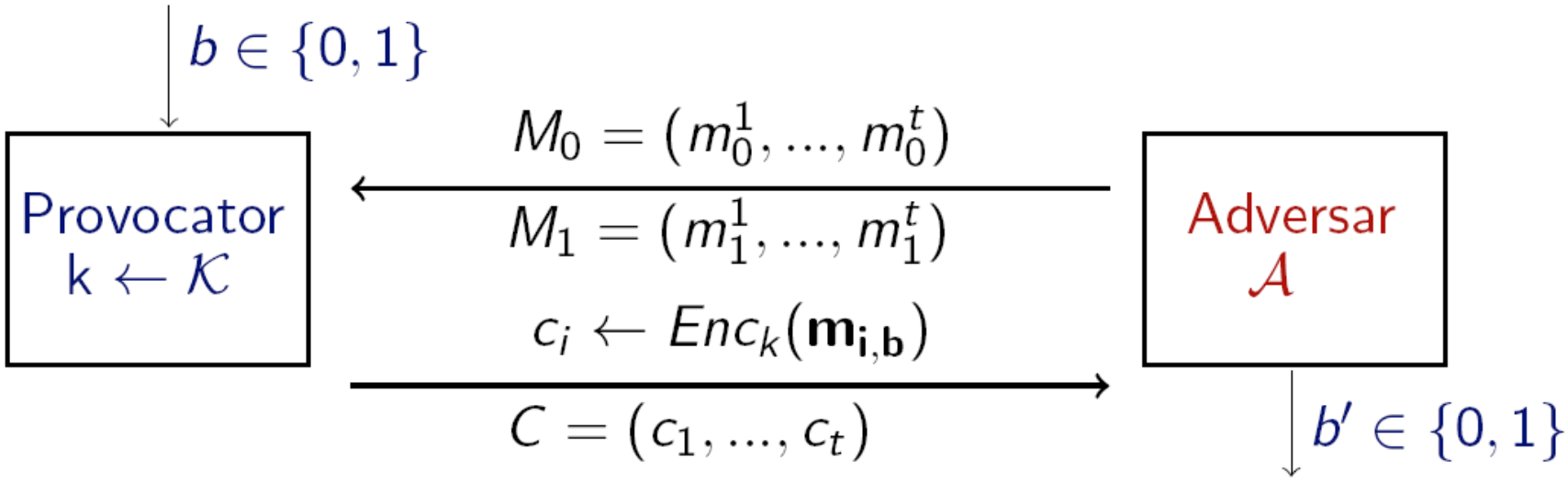
- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;

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



- 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 $Priv^{cpa}_{\mathcal{A},\pi}(n)$



- 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 **simplă** implică securitate pentru criptare **multiplă**!

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

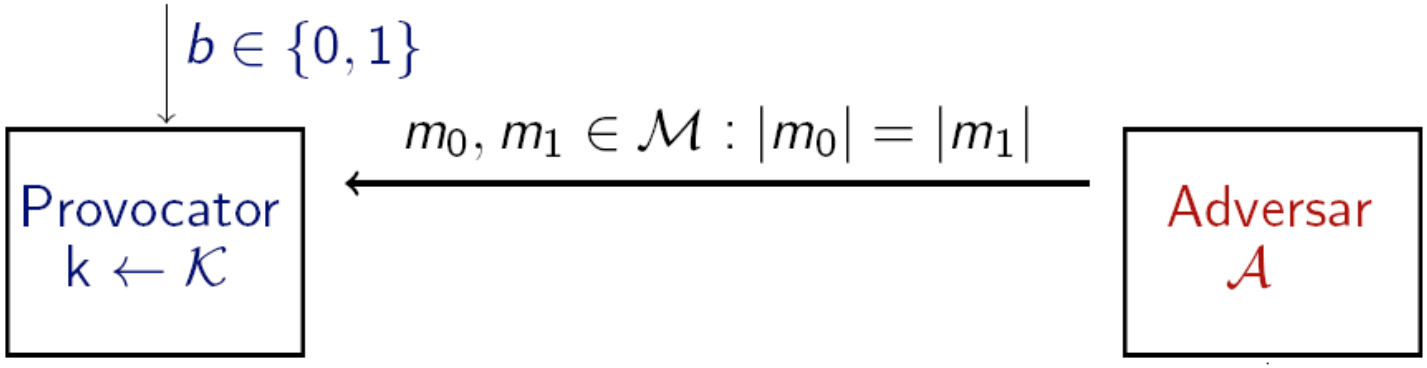
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CCA pe baza unui experiment de indistinctibilitate $Priv^{cca}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

Securitate CCA

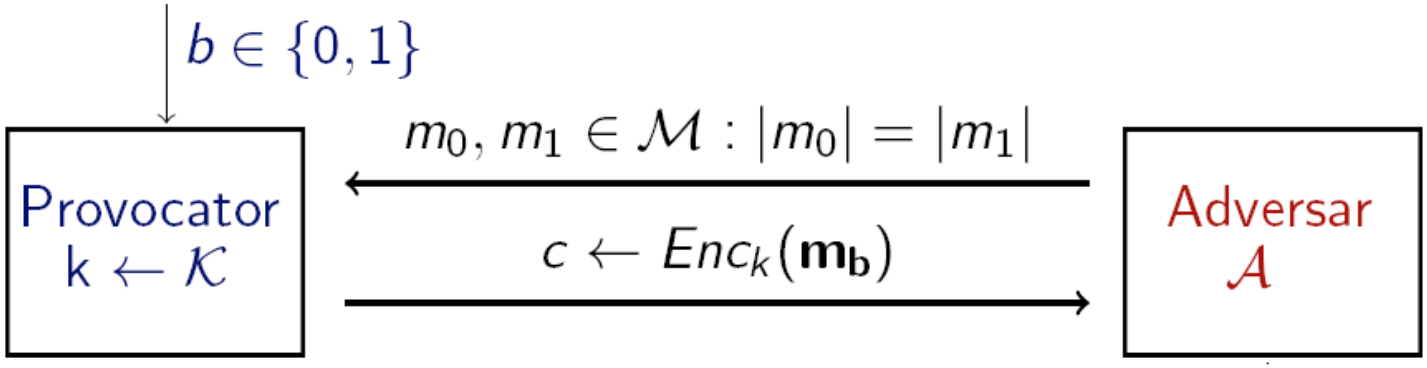
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CCA pe baza unui experiment de indistinctibilitate $Priv^{cca}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

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

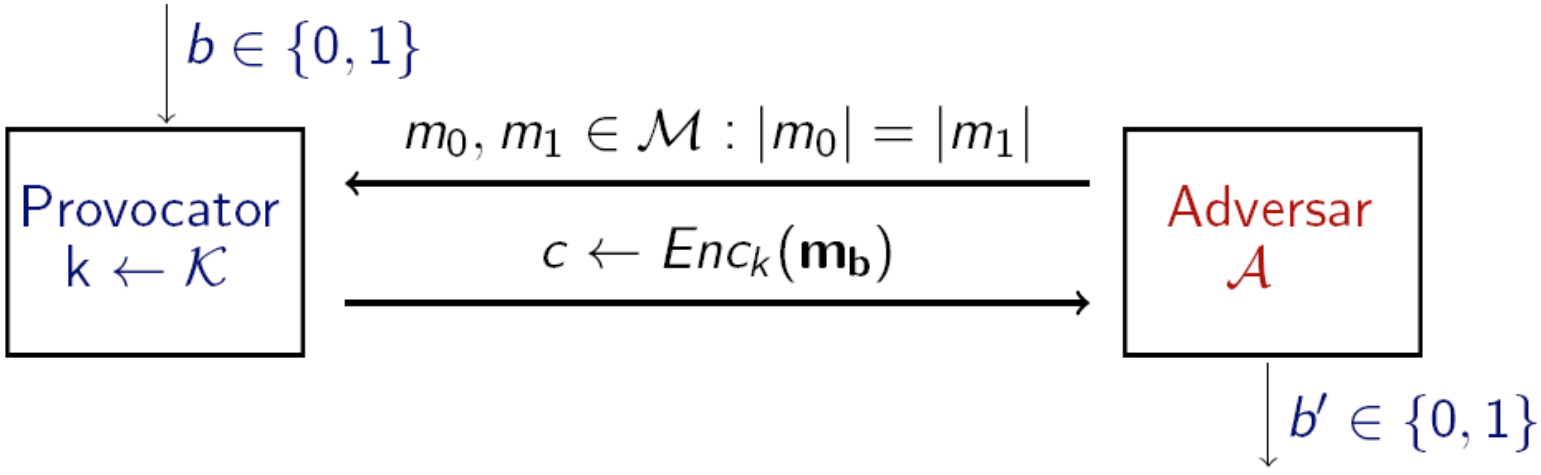
Experimentul $Priv^{cca}_{\mathcal{A},\pi}(n)$



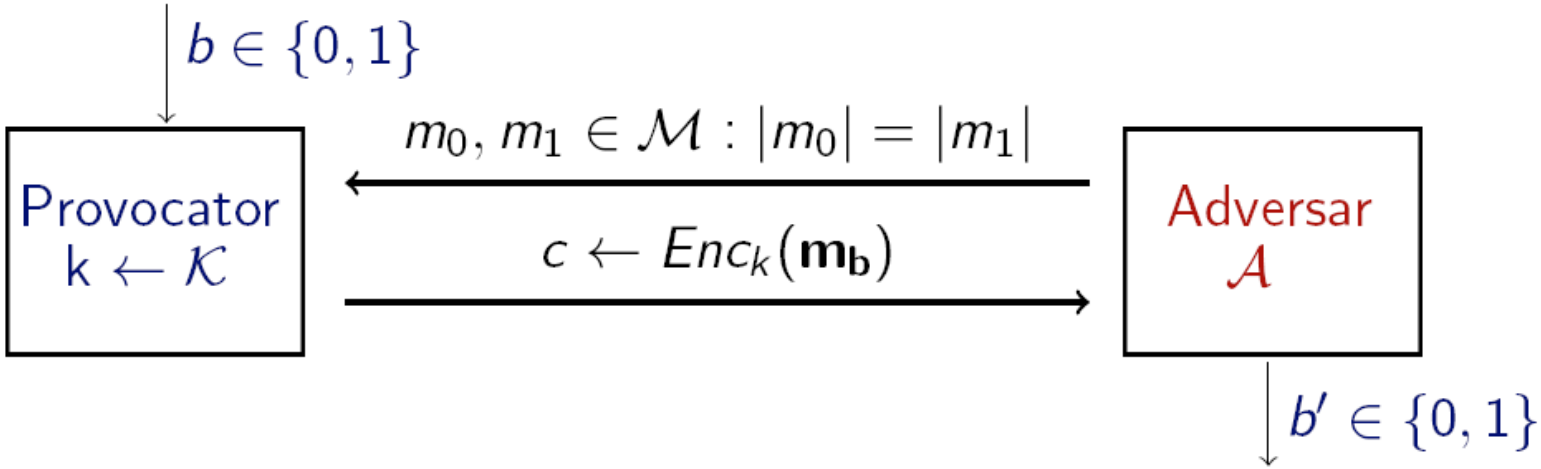
Experimentul $Priv^{cca}_{\mathcal{A},\pi}(n)$



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

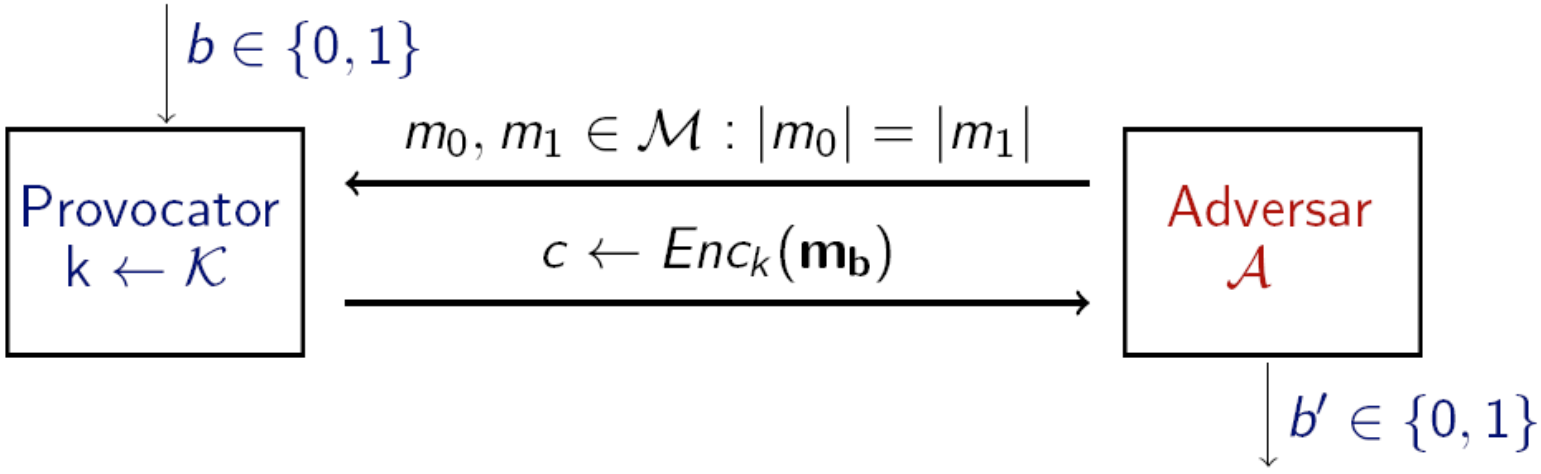


Experimentul $Priv^{cca}_{\mathcal{A},\pi}(n)$



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

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



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

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

Definiție

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

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

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

Definiție

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

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

- 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 $Priv^{cpa}_{\mathcal{A},\pi}(n)$ este $Priv^{cca}_{\mathcal{A},\pi}(n)$ 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 $Priv^{cpa}_{\mathcal{A},\pi}(n)$ este $Priv^{cca}_{\mathcal{A},\pi}(n)$ 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 $Priv^{cpa}_{\mathcal{A},\pi}(n)$ este $Priv^{cca}_{\mathcal{A},\pi}(n)$ 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

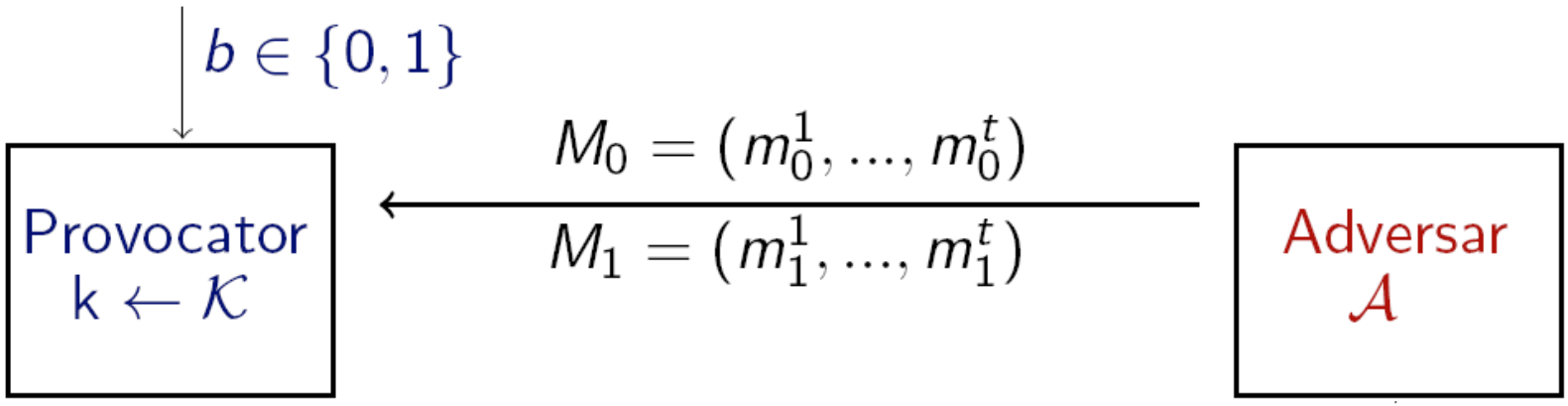
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;

Securitate CCA - Criptare multiplă

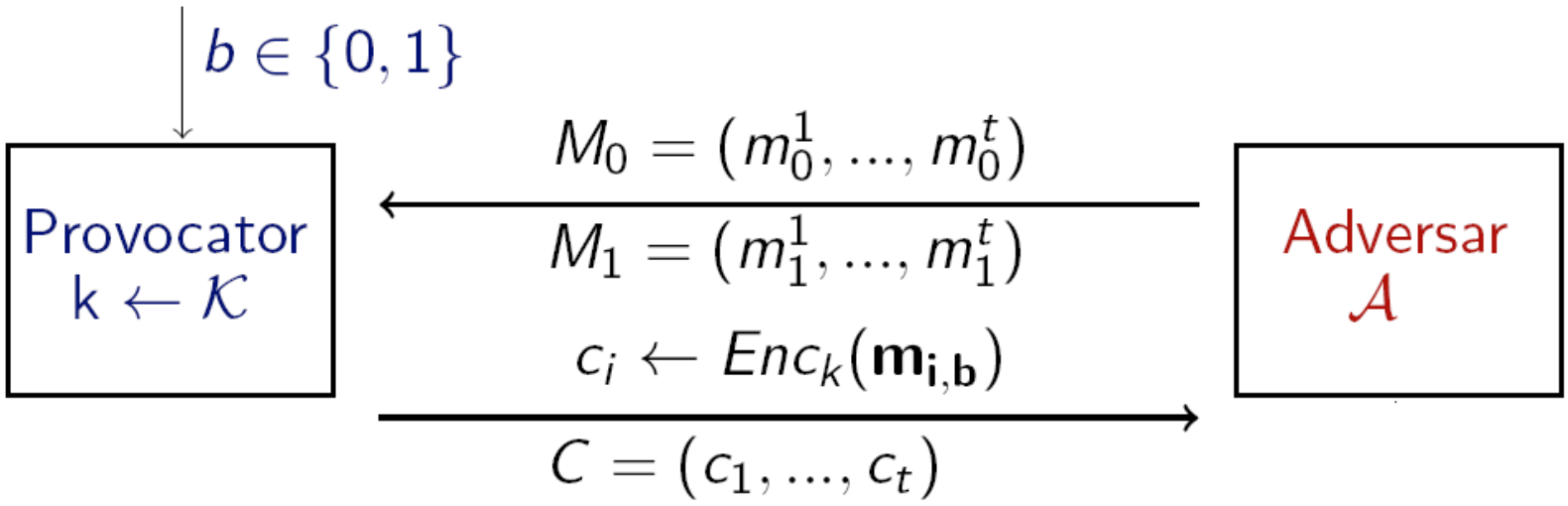
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;
- Definim ce înseamnă o schemă sigură chiar și în aceste condiții.

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

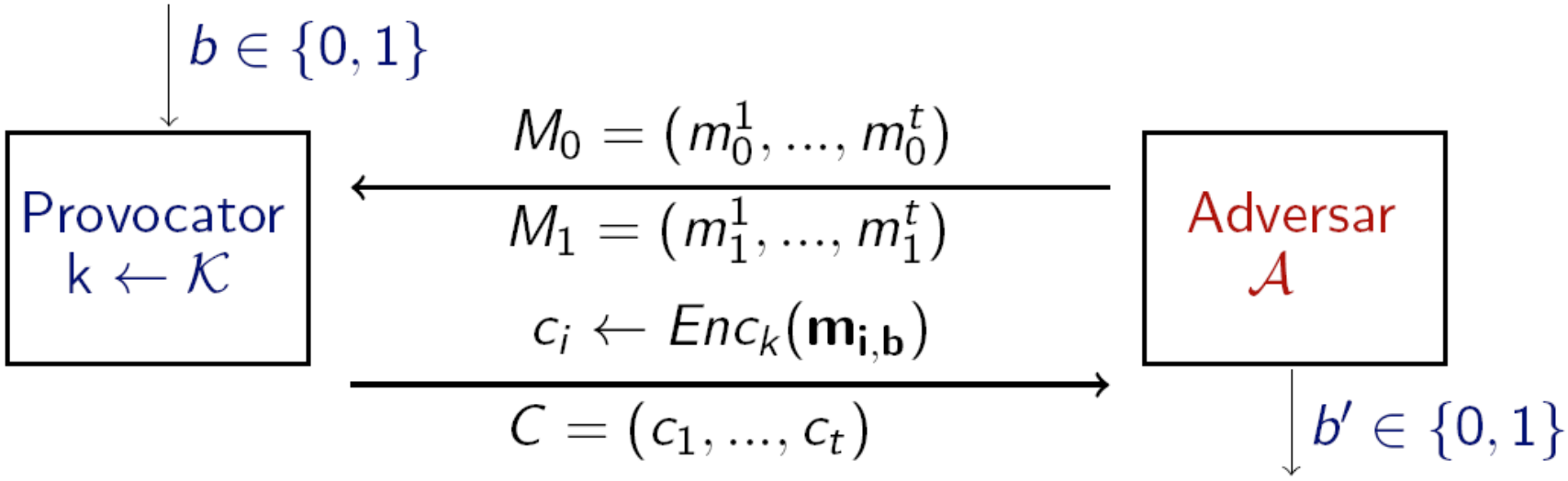
Experimentul $Priv^{cca}_{\mathcal{A},\pi}(n)$



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

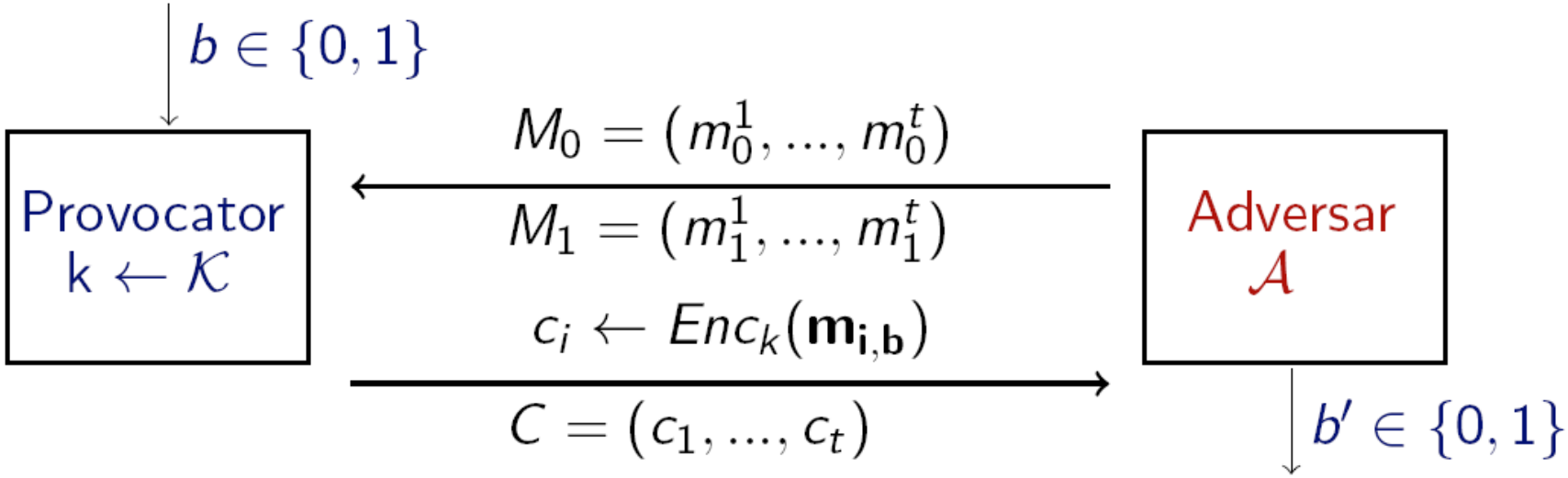


Experimentul $Priv^{cca}_{\mathcal{A},\pi}(n)$



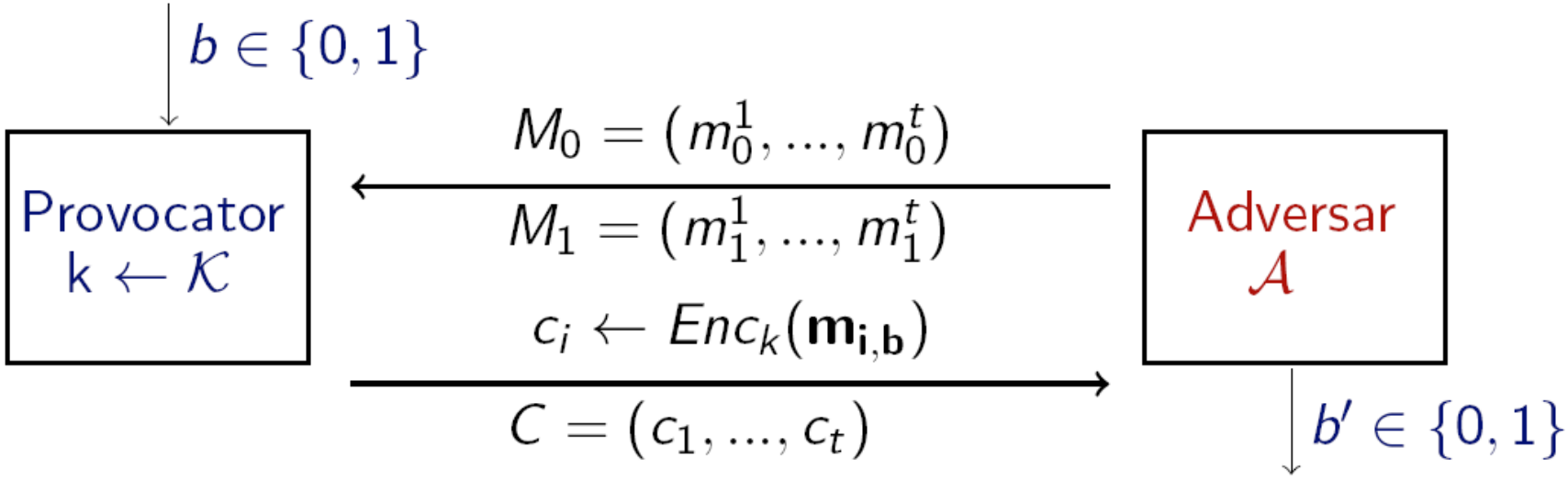
- Pe toată durata experimentului, $\mathcal{A}$ are acces la oracolul de criptare $Enc_k(\cdot)$ și la oracolul decriptare $Dec_k(\cdot)$ cu restricția că nu poate decripta $c_1, \ldots, c_t$!

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



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

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



- 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.

Important de reținut!

- Securitate CCA $\Rightarrow$ securitate CPA $\Rightarrow$ securitate semantică
- Schemele deterministe nu sunt semantic / CPA / CCA sigure