Securitatea Sistemelor Informatice

- Curs 4.0 -

Noțiuni de securitate mai puternice

Adela Georgescu

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

Securitate computațională

In cursurile anterioare:

- Am definit securitate perfectă, am vazut OTP - perfect sigur și am evidențiat limitările practice

Securitate computațională

In cursurile anterioare:

- Am definit securitate perfectă, am vazut OTP - perfect sigur și am evidențiat limitările practice
- In practică, vrem chei mai scurte și refolosirea cheii

Securitate computațională

In cursurile anterioare:

- Am definit securitate perfectă, am vazut OTP - perfect sigur și am evidențiat limitările practice
- In practică, vrem chei mai scurte și refolosirea cheii
- Am slăbit noțiunea de securitate perfectă și am obținut securitate computațională, considerand un adversar polinomial cu probabilitate neglijabilă de succes

Securitate computațională

In cursurile anterioare:

- Am definit securitate perfectă, am vazut OTP - perfect sigur și am evidențiat limitările practice
- In practică, vrem chei mai scurte și refolosirea cheii
- Am slăbit noțiunea de securitate perfectă și am obținut securitate computațională, considerand un adversar polinomial cu probabilitate neglijabilă de succes
- Am construit un sistem de criptare computațional sigur (satisface indistinctibilitatea) pentru care cheia de criptare este mai scurtă

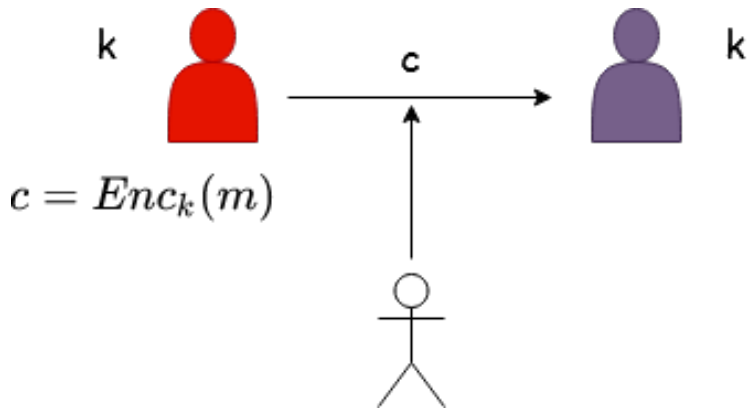
Securitate computațională

In cursurile anterioare:

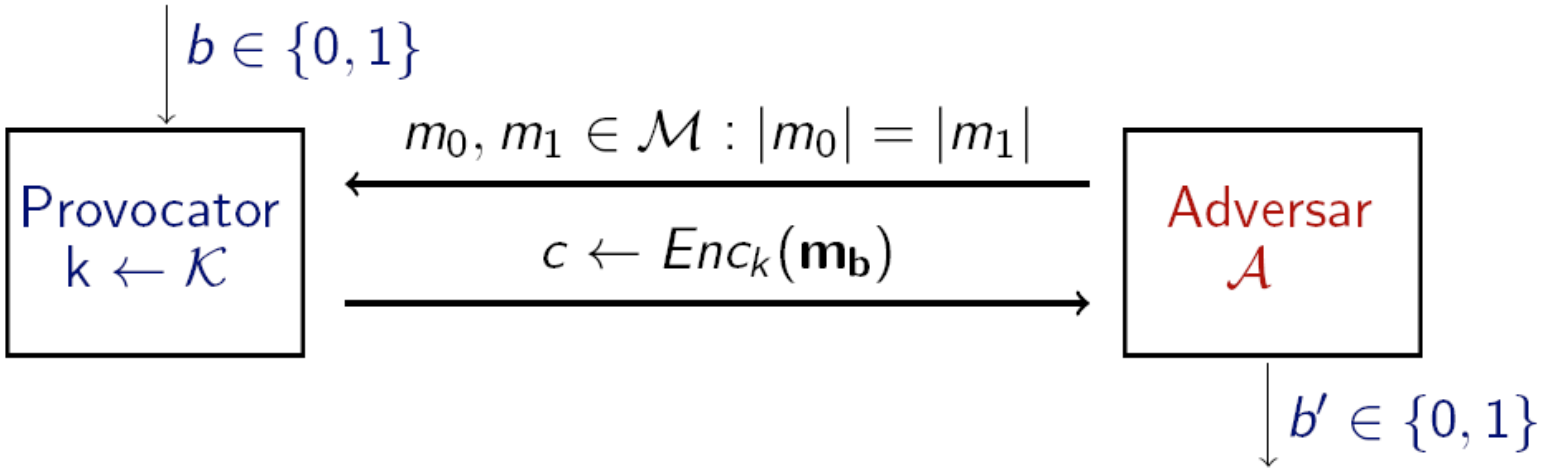
- Am definit securitate perfectă, am vazut OTP - perfect sigur și am evidențiat limitările practice
- In practică, vrem chei mai scurte și refolosirea cheii
- Am slăbit noțiunea de securitate perfectă și am obținut securitate computațională, considerand un adversar polinomial cu probabilitate neglijabilă de succes
- Am construit un sistem de criptare computațional sigur (satisface indistinctibilitatea) pentru care cheia de criptare este mai scurtă
- Insă acest sistem de criptare nu permite refolosirea cheii în siguranță

Securitate computațională

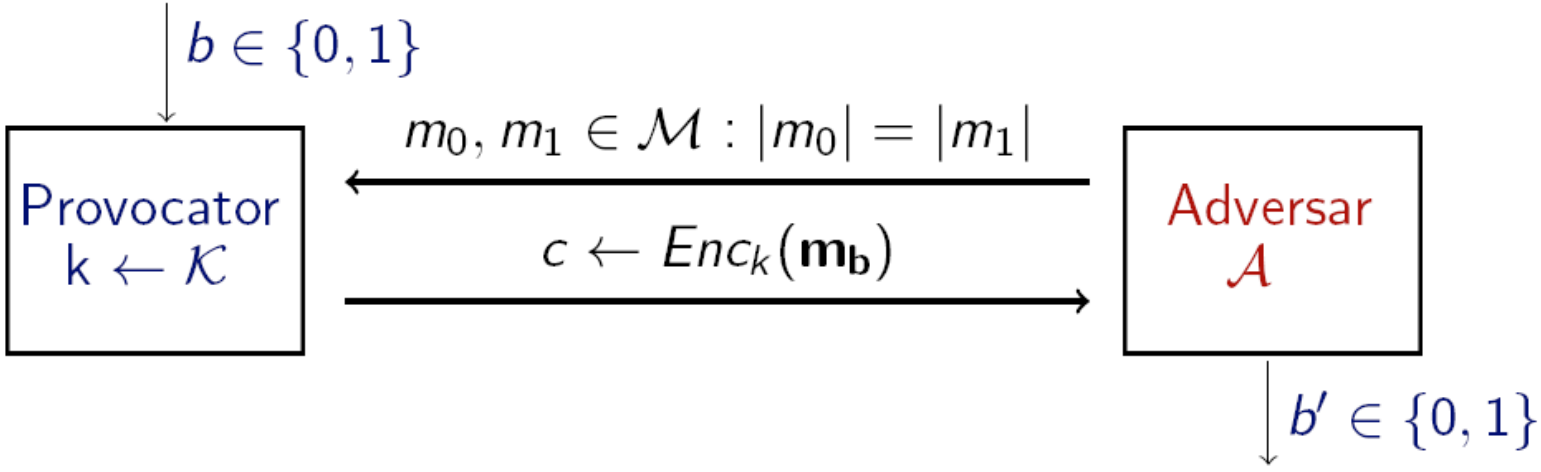
- In continuare considerăm noțiuni de securitate mai puternice care ne vor folosi pentru a obține refolosirea cheii
- Reamintim noțiunea de indistinctibilitate definită anterior, în cazul unui adversar care interceptează un singur mesaj criptat



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



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



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

Securitate - interceptare simplă

Definiție

O schemă de criptare $\pi = (Enc, Dec)$ este indistinctibilă în prezența unui atacator pasiv dacă pentru orice adversar $\mathcal{A}$ există o funcție neglijabilă negl așa încât

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

Securitate pentru interceptare multiplă

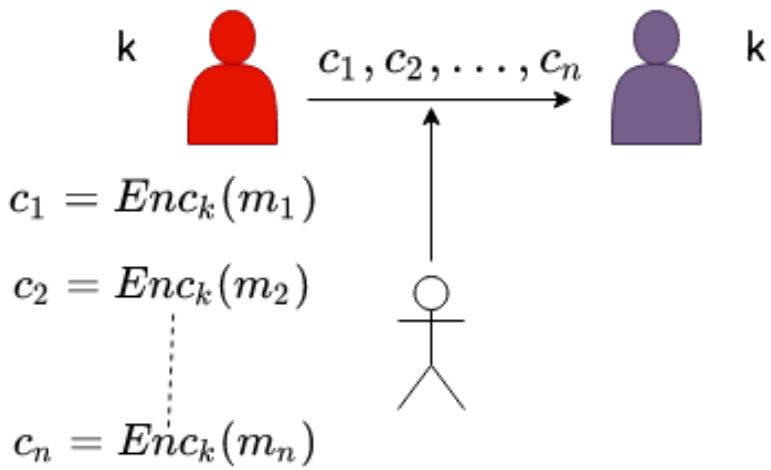
- In definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;

Securitate pentru interceptare multiplă

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

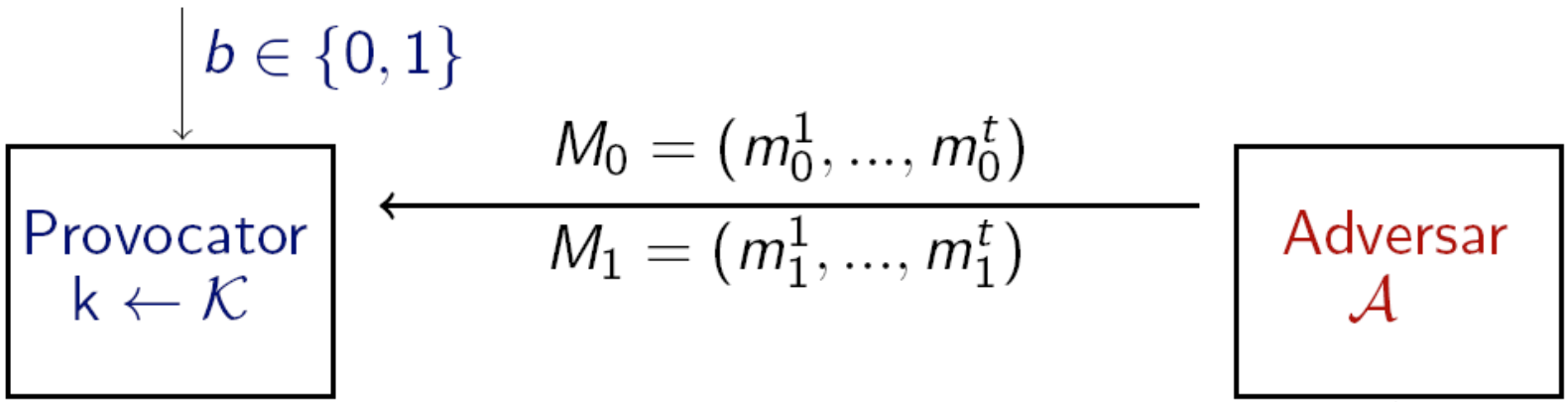
Securitate pentru interceptare multiplă

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

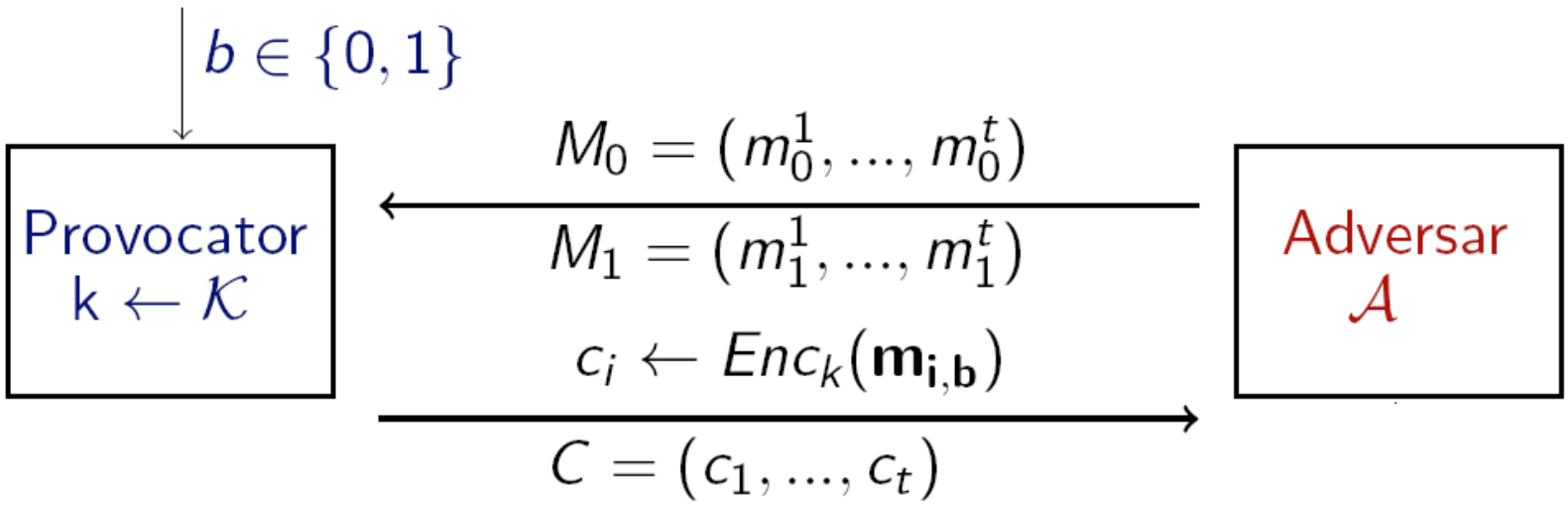


Experimentul $Priv^{mult}_{\mathcal{A},\pi}(n)$

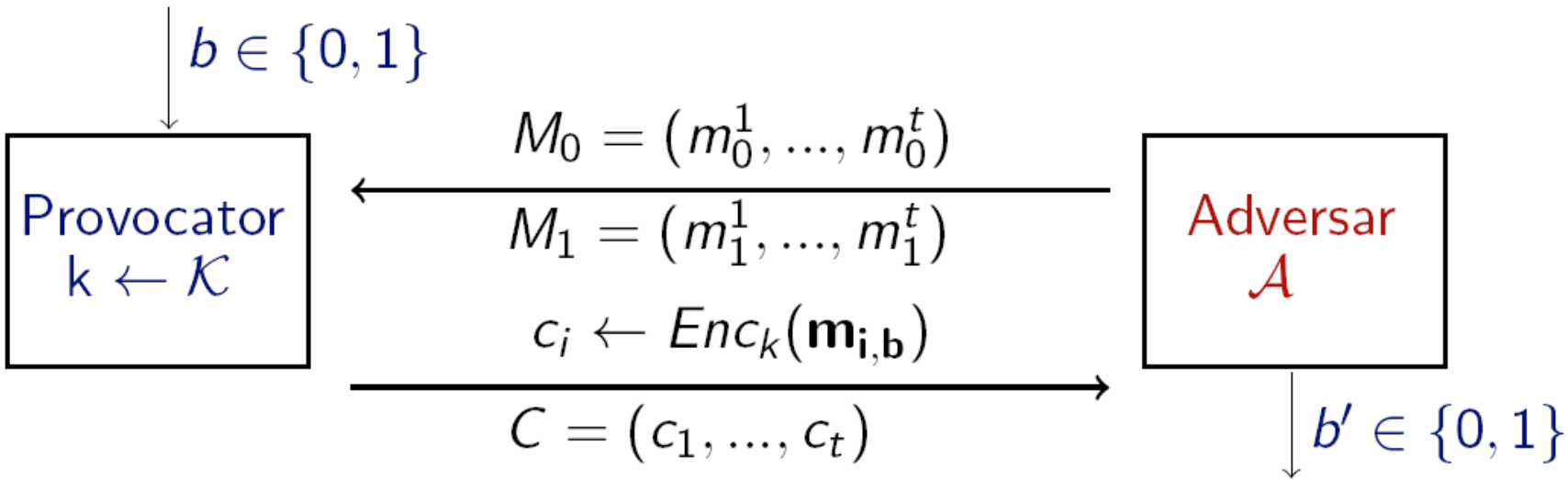
Experimentul $Priv^{mult}_{\mathcal{A},\pi}(n)$



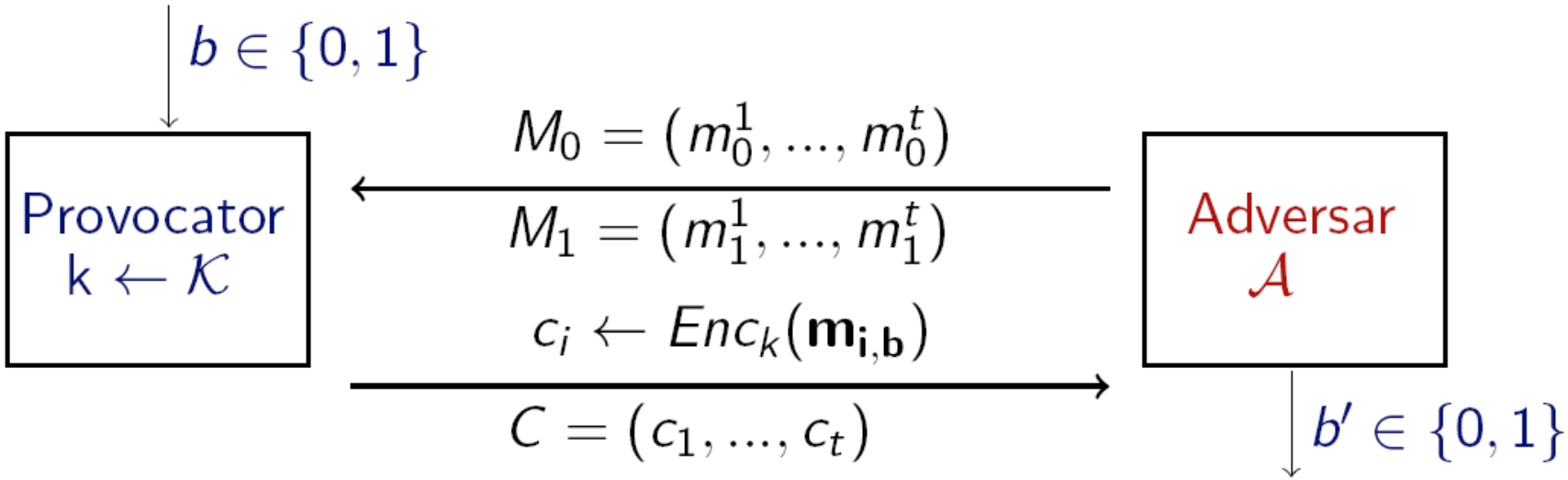
Experimentul $Priv^{mult}_{\mathcal{A},\pi}(n)$



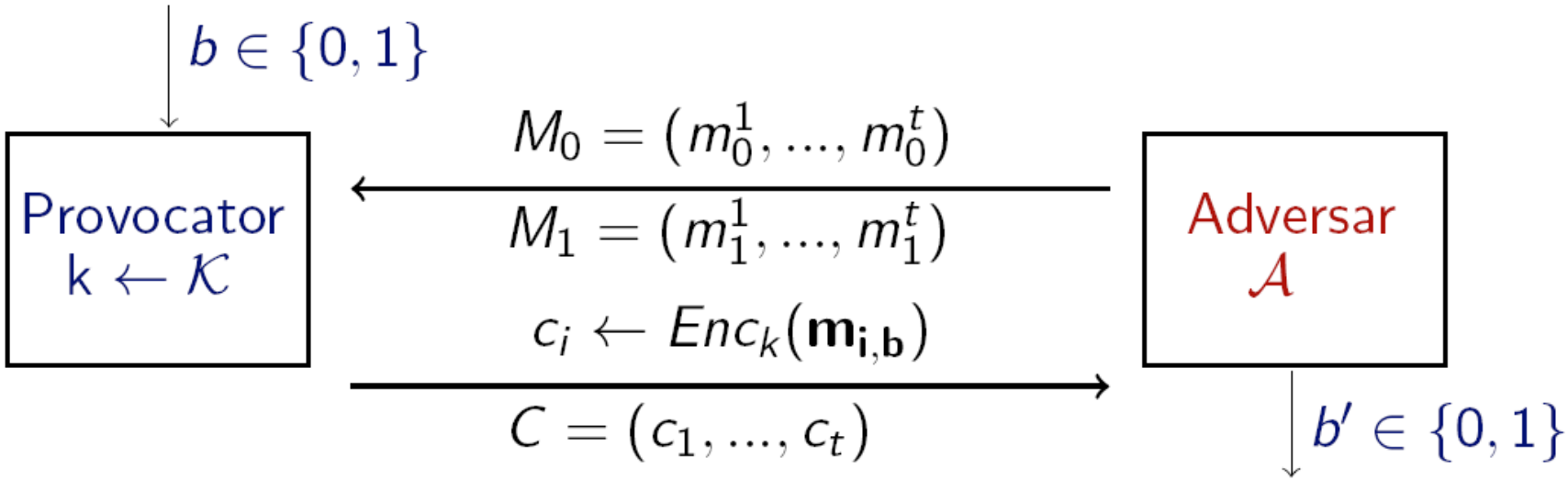
Experimentul $Priv_{\mathcal{A},\pi}^{mult}(n)$



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

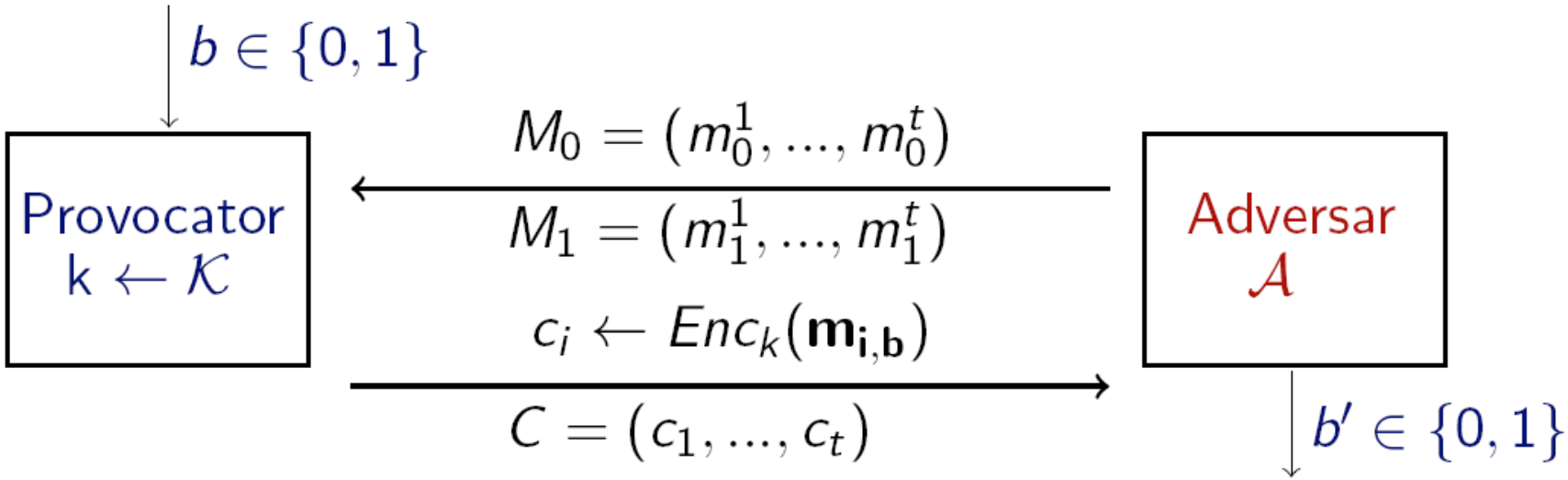


Experimentul $Priv^{mult}_{\mathcal{A},\pi}(n)$



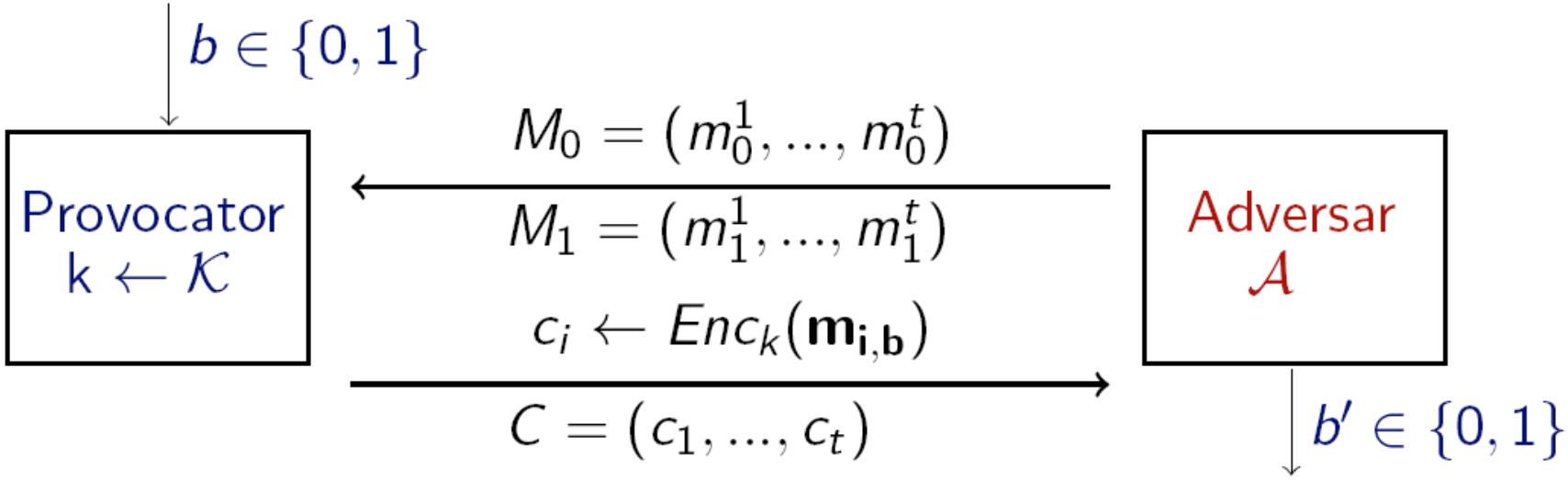
- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;

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



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



- 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 interceptare **simplă** nu implică securitate pentru interceptare **multiplă**!

Securitate pentru interceptare multiplă

Securitate pentru interceptare multiplă

Teoremă

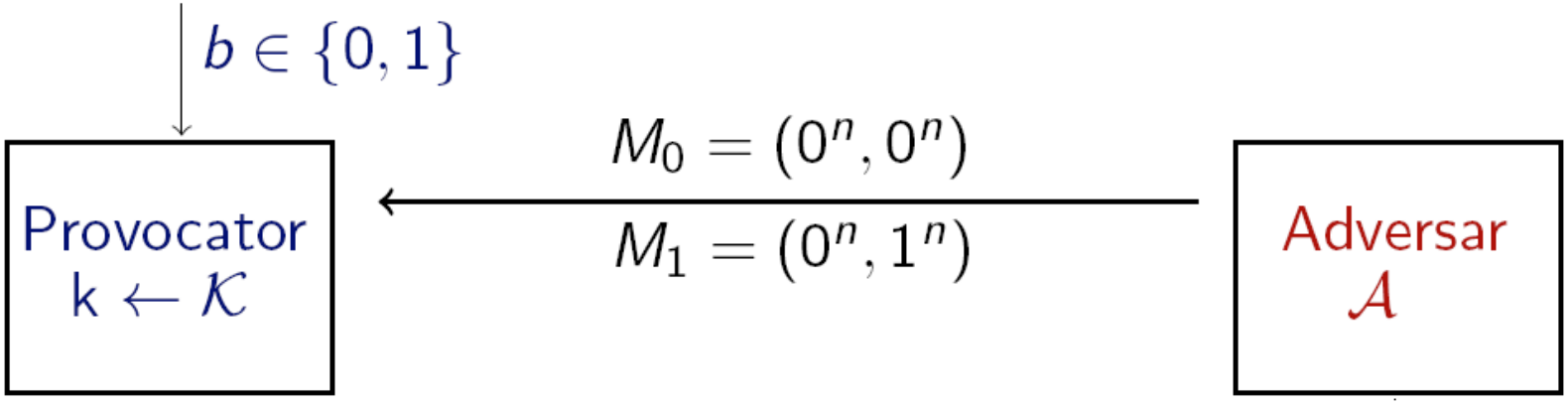
O schemă de criptare (Enc, Dec) unde funcția Enc este deterministă nu are proprietatea de securitate la interceptare multiplă conform cu definiția de mai sus.

Demonstrație

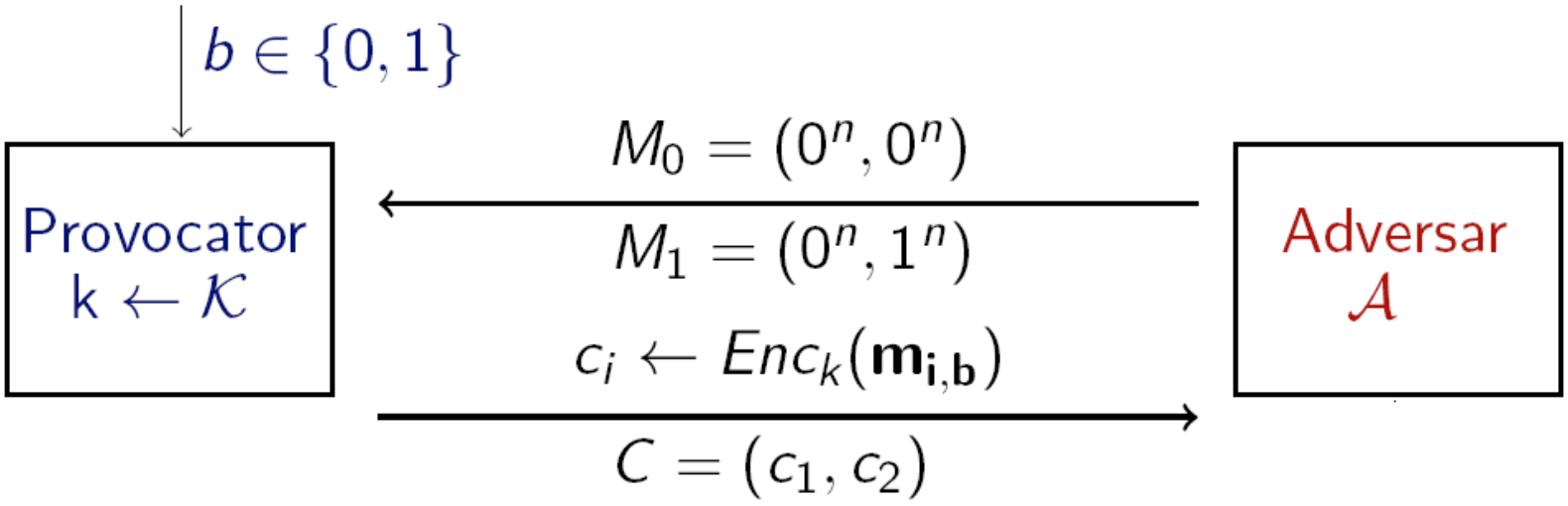
- Intuitiv, am vazut că schema OTP este sigură doar când o cheie este folosită o singură dată;
- La sistemul de criptare bazat pe PRG se întâmplă același lucru;
- Vom considera un adversar $\mathcal{A}$ care atacă schema (în sensul experimentului $Priv^{mult}_{\mathcal{A},\pi}(n)$)

Demonstrație

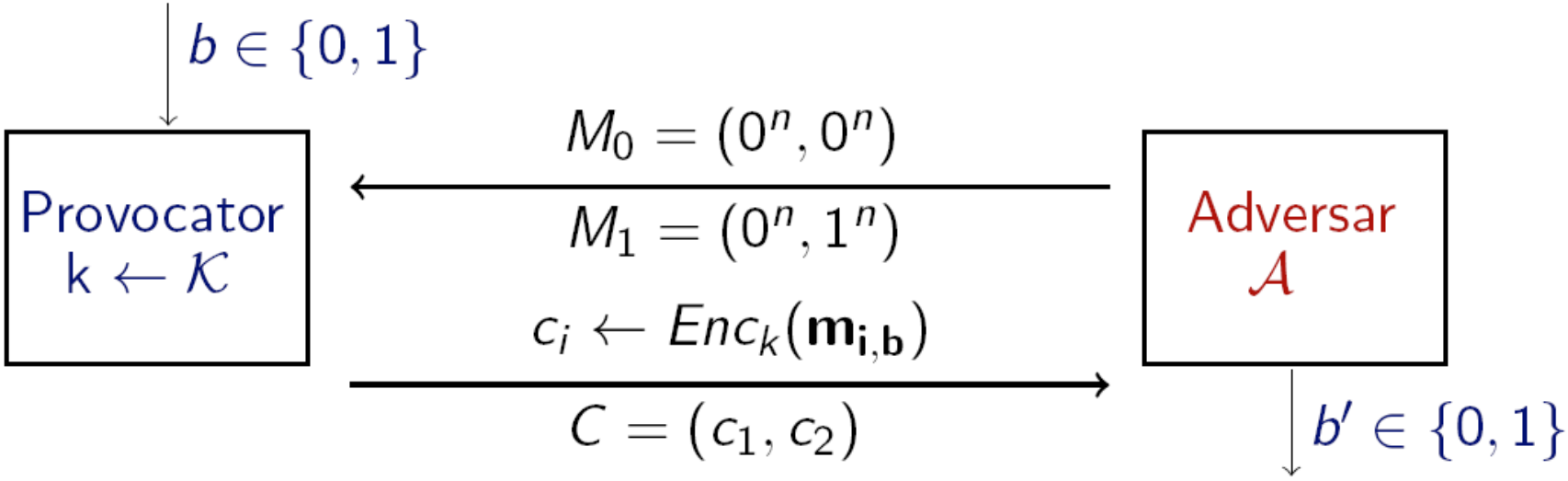
Demonstrație



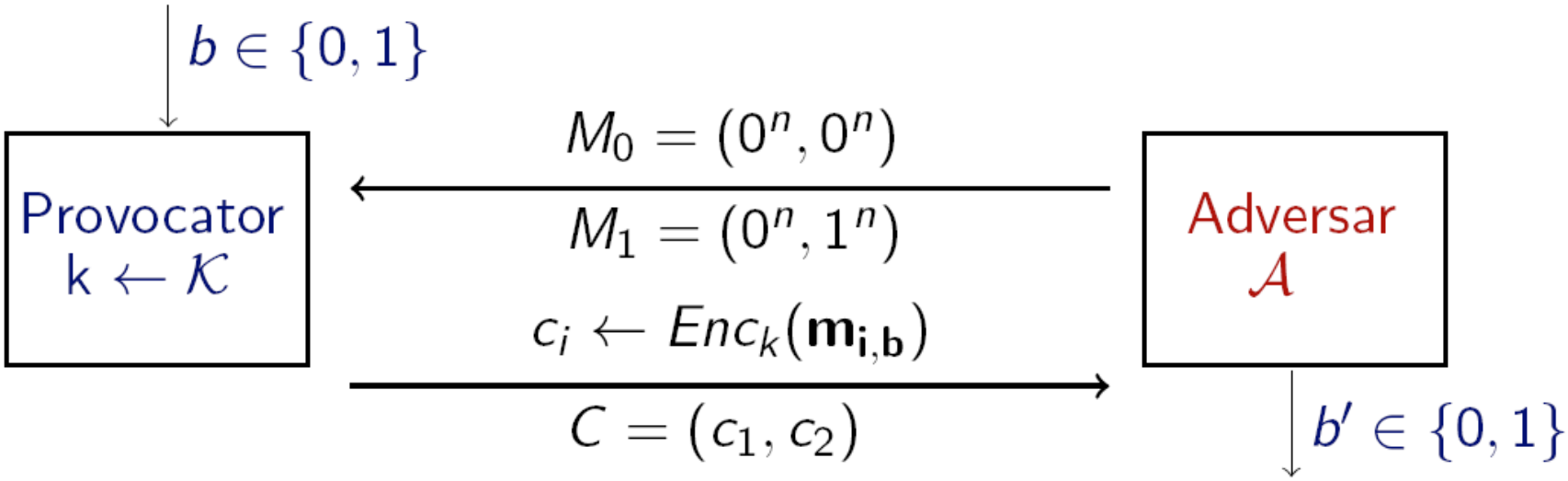
Demonstrație



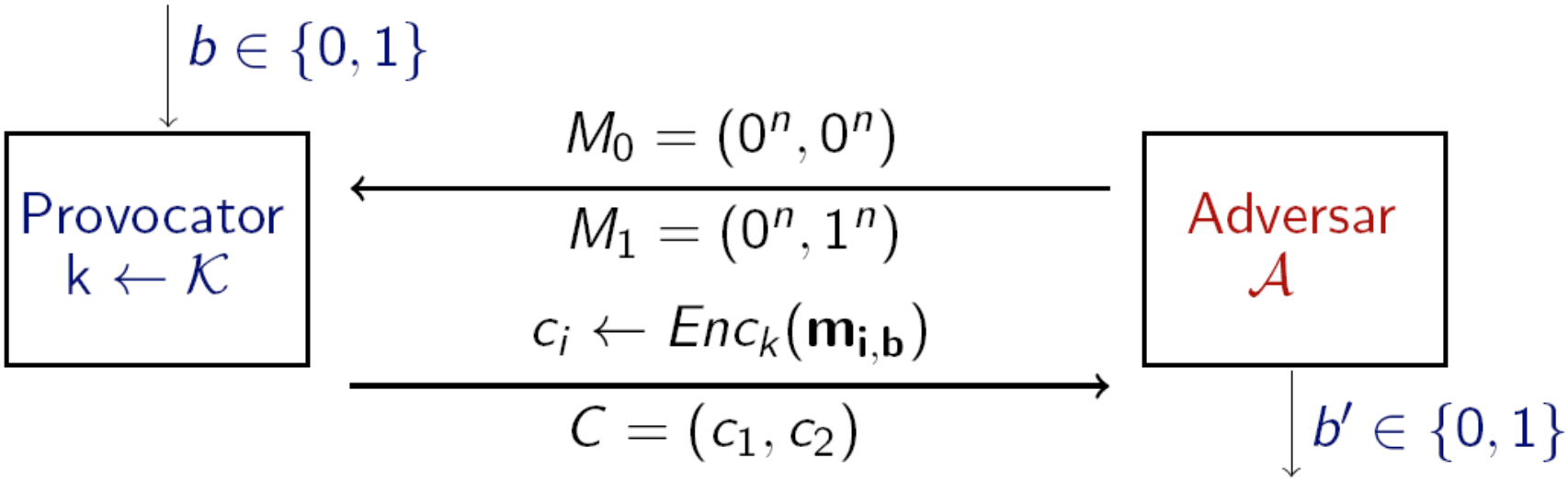
Demonstrație



Demonstrație

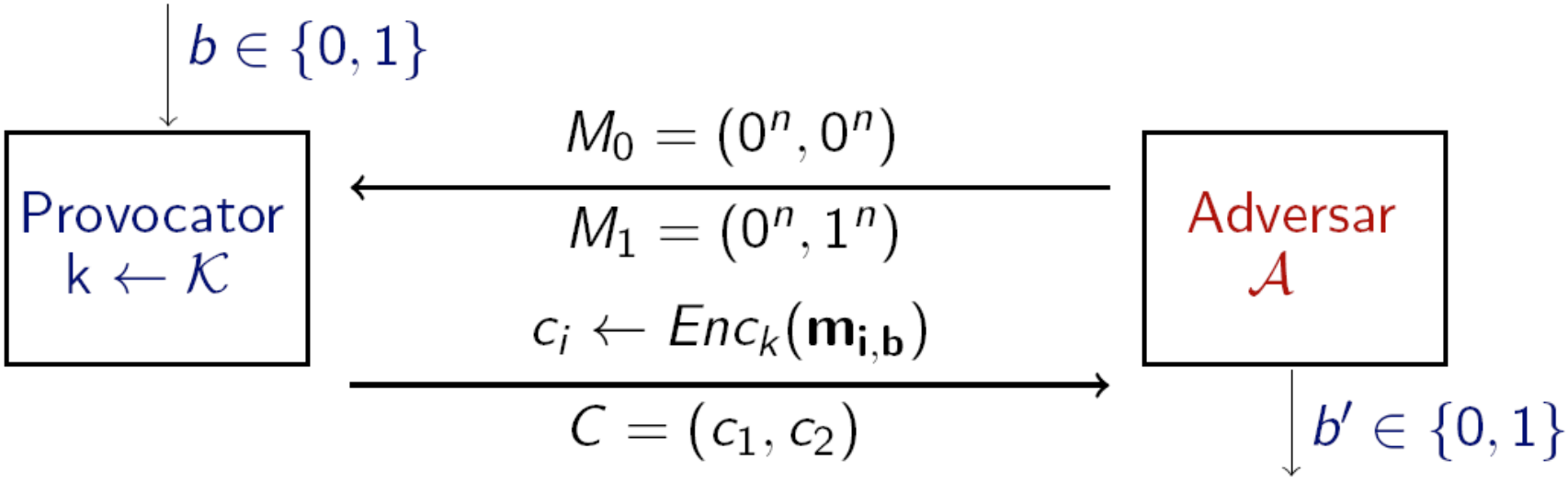


Demonstrație



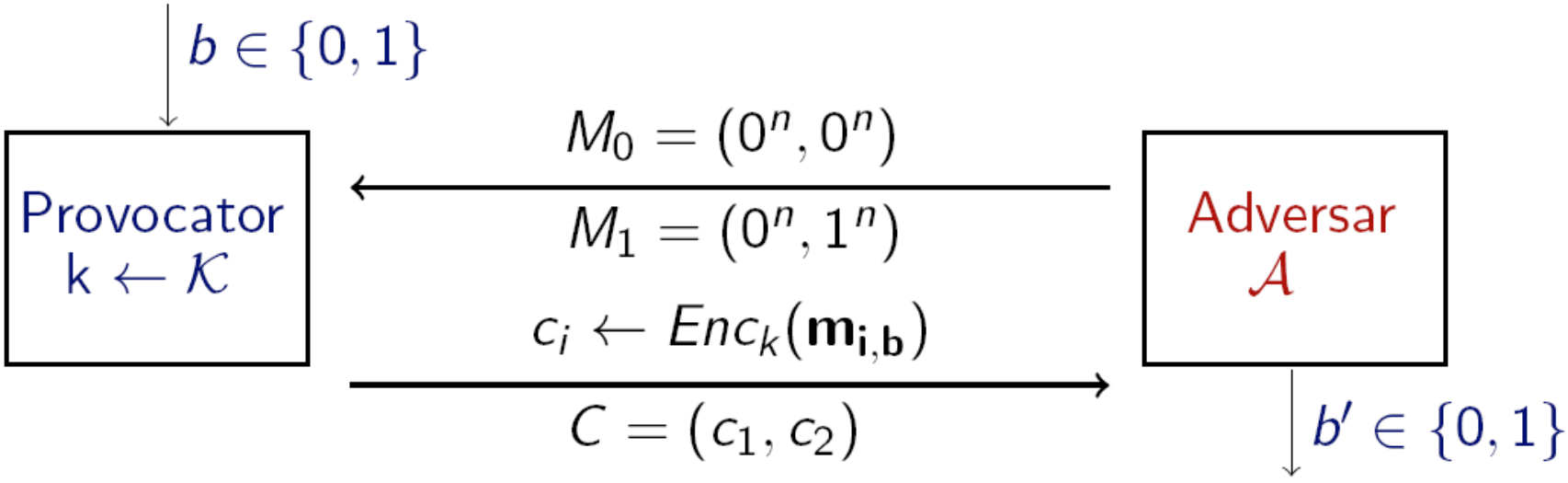
- Dacă $c_1 = c_2$, atunci $\mathcal{A}$ întoarce 0, altfel $\mathcal{A}$ întoarce 1.

Demonstrație



- Dacă $c_1 = c_2$, atunci $\mathcal{A}$ întoarce 0, altfel $\mathcal{A}$ întoarce 1.
- Analizăm probabilitatea ca $\mathcal{A}$ să ghicească b: dacă $b = 0$, același mesaj este criptat mereu ($m_0^1 = m_0^2$) iar $c_1 = c_2$ și deci $\mathcal{A}$ întoarce mereu 0;

Demonstrație



- Dacă $c_1 = c_2$, atunci $\mathcal{A}$ întoarce 0, altfel $\mathcal{A}$ întoarce 1.
- Analizăm probabilitatea ca $\mathcal{A}$ să ghicească b: dacă $b = 0$, același mesaj este criptat mereu ($m_0^1 = m_0^2$) iar $c_1 = c_2$ și deci $\mathcal{A}$ întoarce mereu 0;
- Dacă $b = 1$, atunci ($m_1^1 \neq m_1^2$) iar $c_1 \neq c_2$ și deci $\mathcal{A}$ întoarce mereu 1.

Concluzie

- $\mathcal{A}$ ghicește bitul b cu probabilitate 1 și deci schema nu este indistinctibilă la interceptare multiplă
- Pentru a obține *securitate la interceptare multipla*, avem nevoie de o schemă de criptare *probabilista*, așa încât la criptari succesive ale aceluiași mesaj să obținem texte criptate diferite

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.

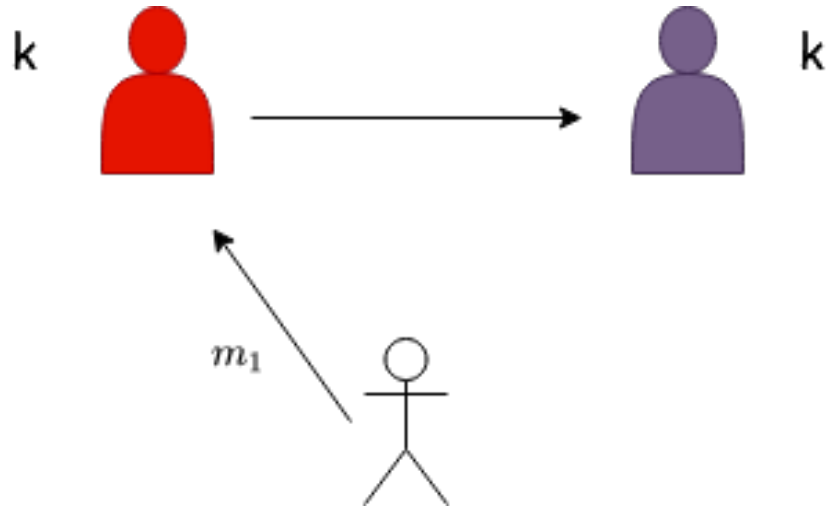
Securitate CPA

Securitate CPA

- CPA (Chosen-Plaintext Attack): adversarul poate să obțină criptarea unor mesaje alese de el;

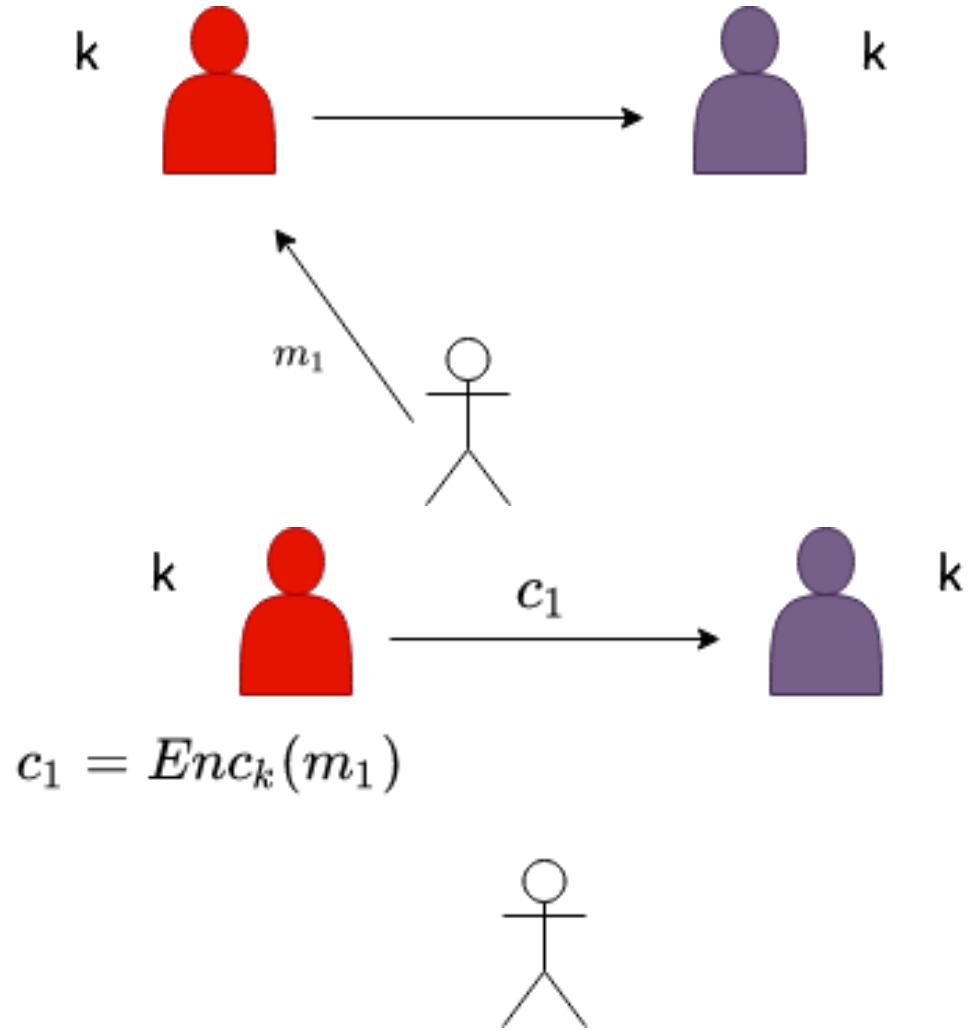
Securitate CPA

- CPA (Chosen-Plaintext Attack): adversarul poate să obțină criptarea unor mesaje alese de el;



Securitate CPA

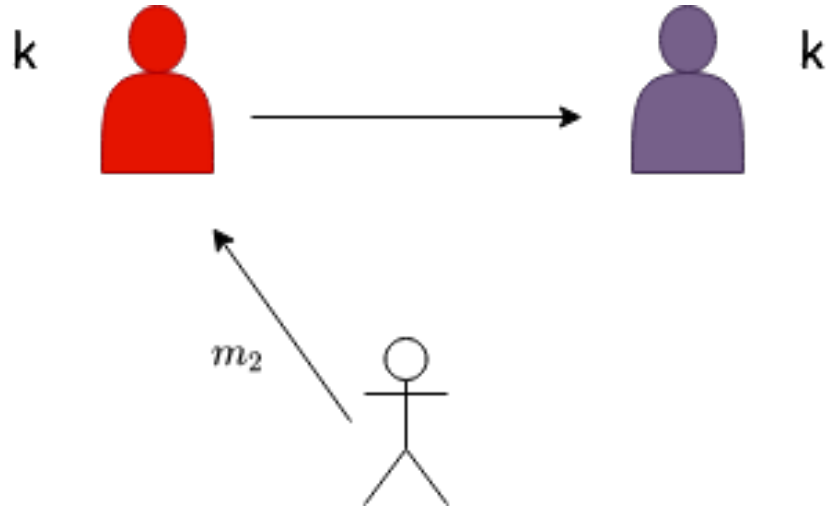
- CPA (Chosen-Plaintext Attack): adversarul poate să obțină criptarea unor mesaje alese de el;



Securitate CPA

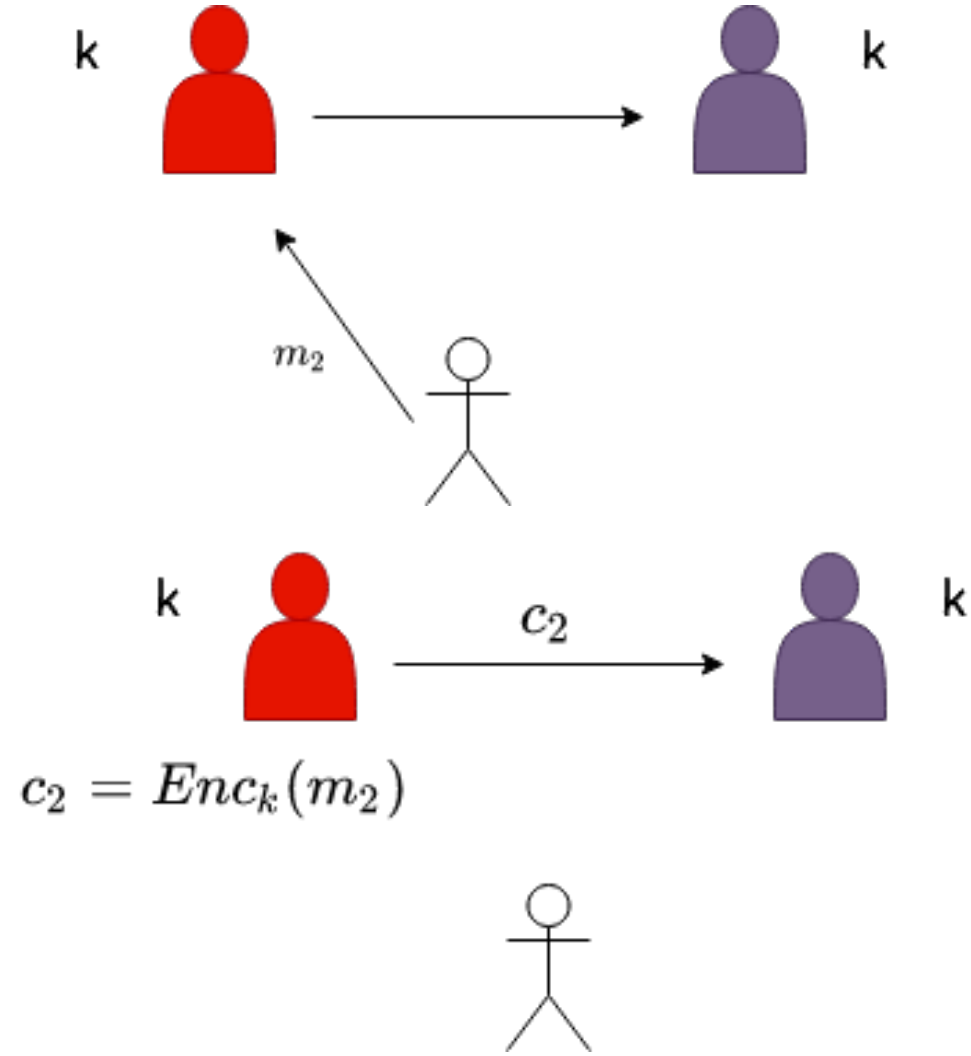
Securitate CPA

- adversarul poate cere criptarea unor mesaje alese de el repetitiv (polinomial de multe ori)



Securitate CPA

- adversarul poate cere criptarea unor mesaje alese de el repetitiv (polinomial de multe ori)



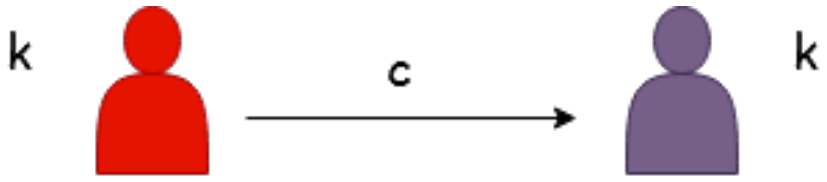
Securitate CPA

Securitate CPA

- mai tarziu adversarul observă criptarea unui mesaj necunoscut

Securitate CPA

- mai tarziu adversarul observă criptarea unui mesaj necunoscut

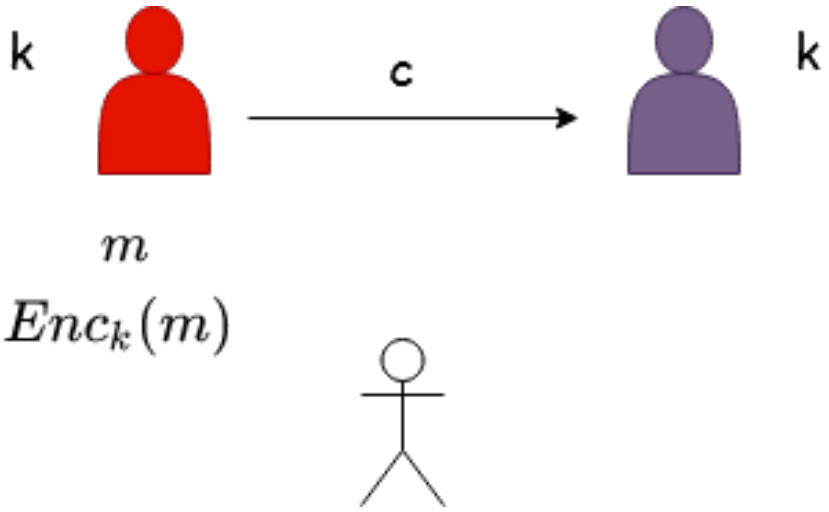


$$m$$

$$c = Enc_k(m)$$

Securitate CPA

- mai tarziu adversarul observă criptarea unui mesaj necunoscut



- dorim ca adversarul să nu afle nici un fel de informație despre mesajul m

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

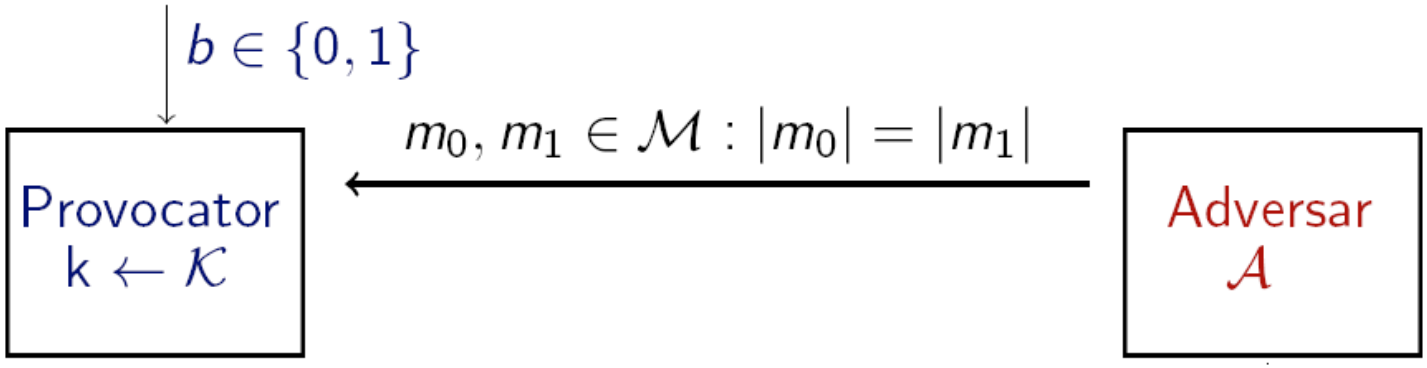
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CPA pe baza unui experiment de indistinctibilitate $Priv^{cpa}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

Securitate CPA

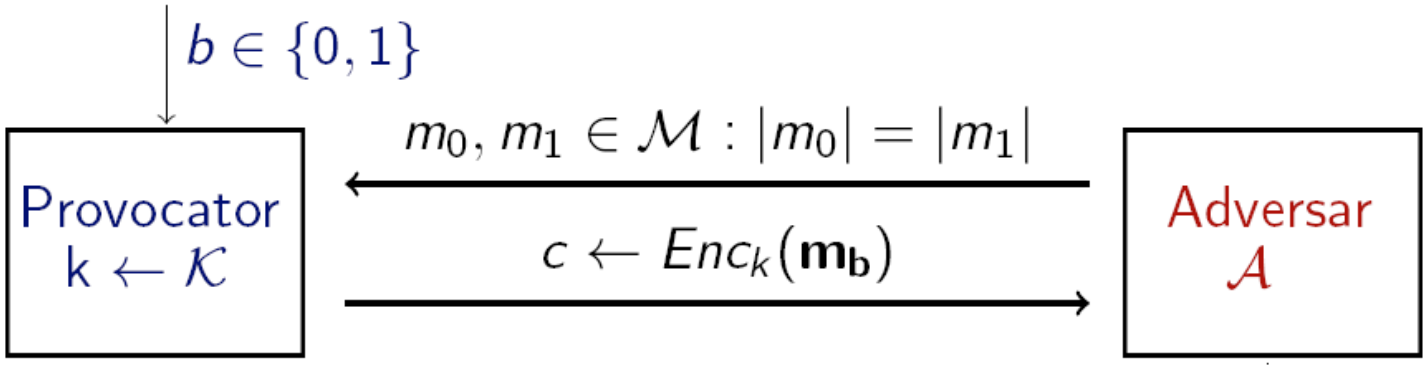
- Considerăm că securitatea este impactată dacă adversarul poate să distingă între criptările a două mesaje aleatoare;
- Vom defini securitatea CPA pe baza unui experiment de indistinctibilitate $Priv^{cpa}_{\mathcal{A},\pi}(n)$ unde $\pi = (Enc, Dec)$ este schema de criptare iar n este parametrul de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

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

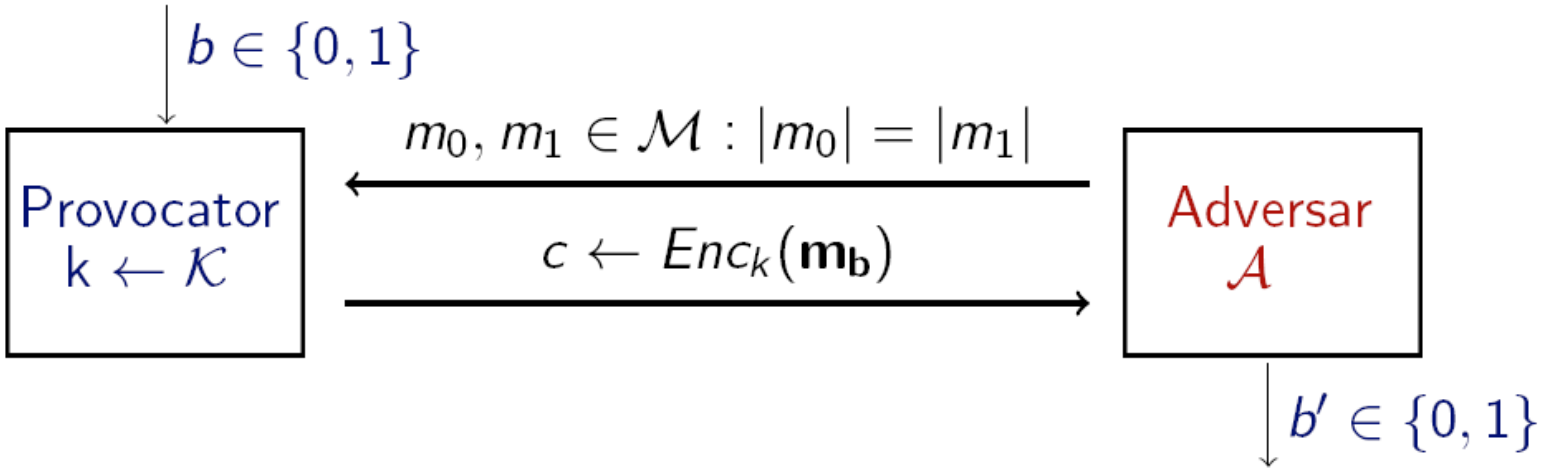
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



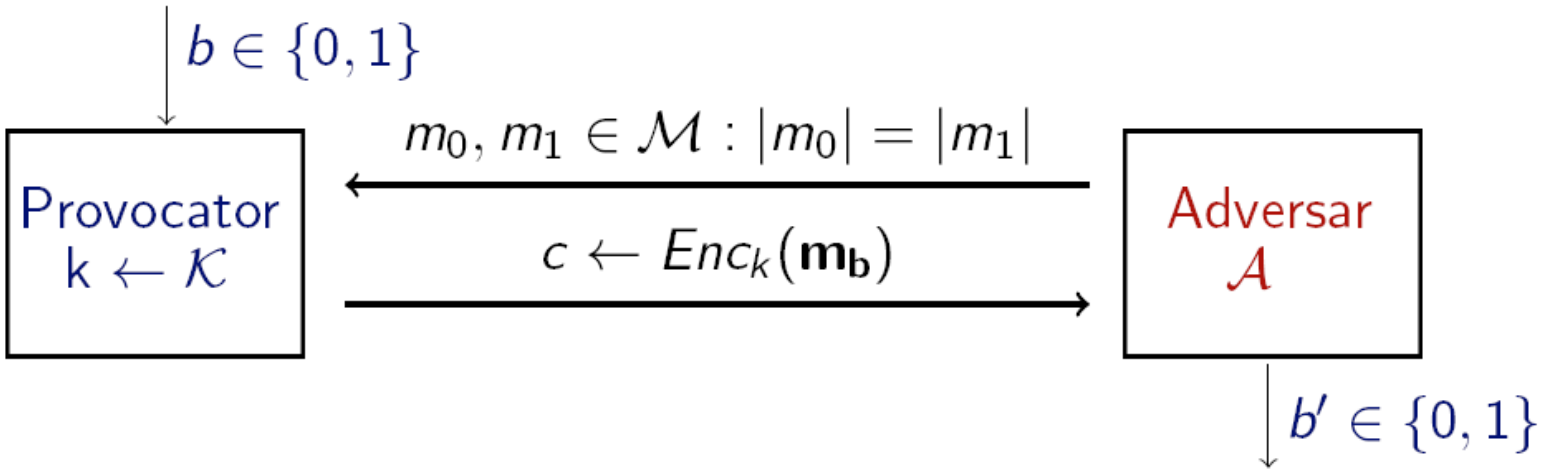
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



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

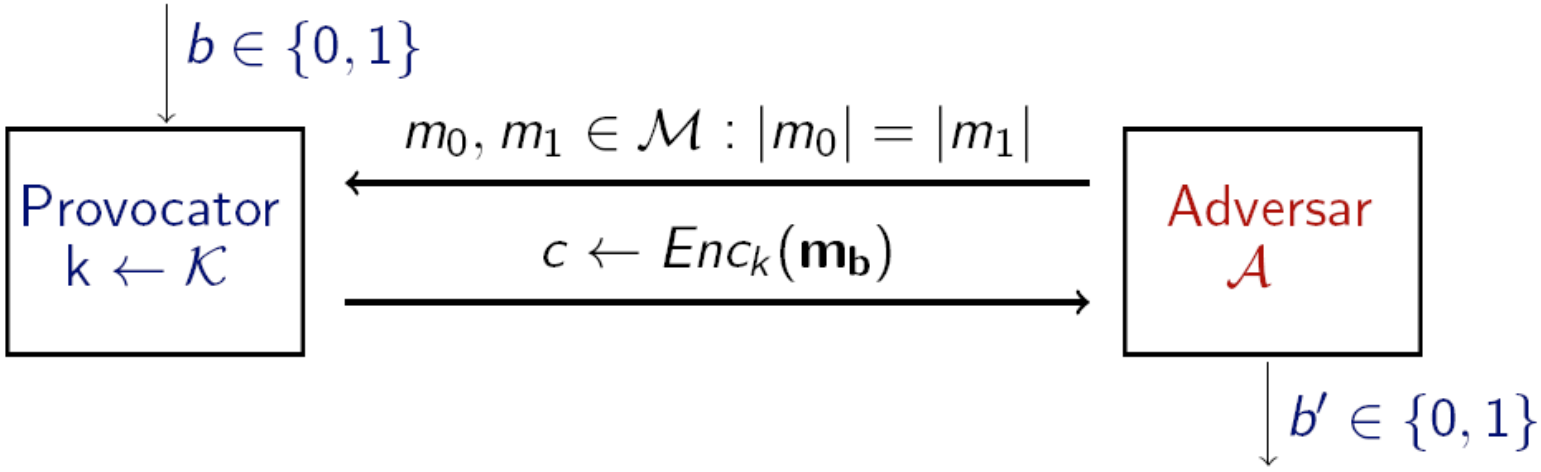


Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



- 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 - al doilea război mondial

criptanaliza sistemului de criptare german Enigma de către englezi

Puterile Aliate

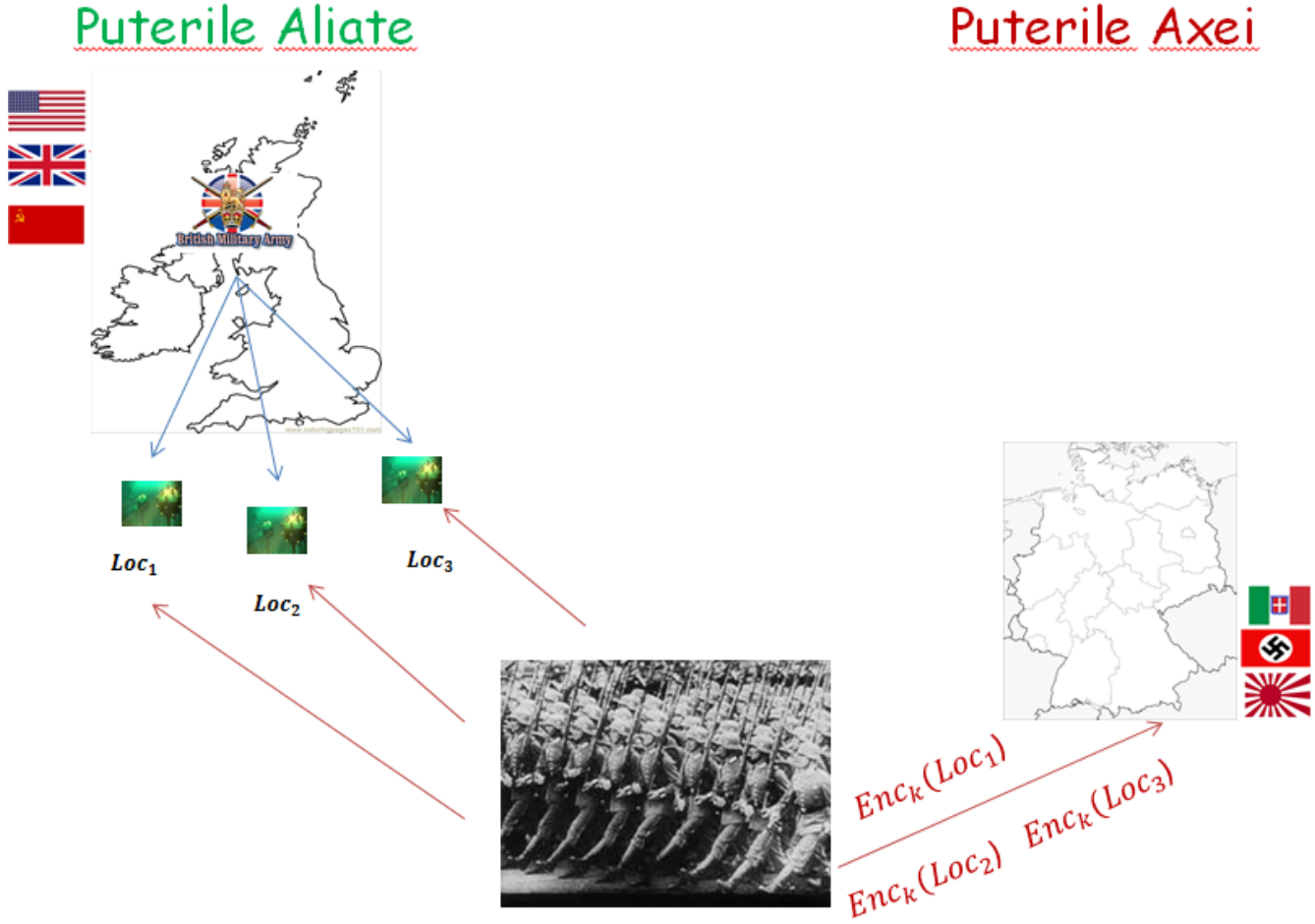
Puterile Axei

Securitate CPA - al doilea război mondial

armata engleză a plasat mine în anumite locații...

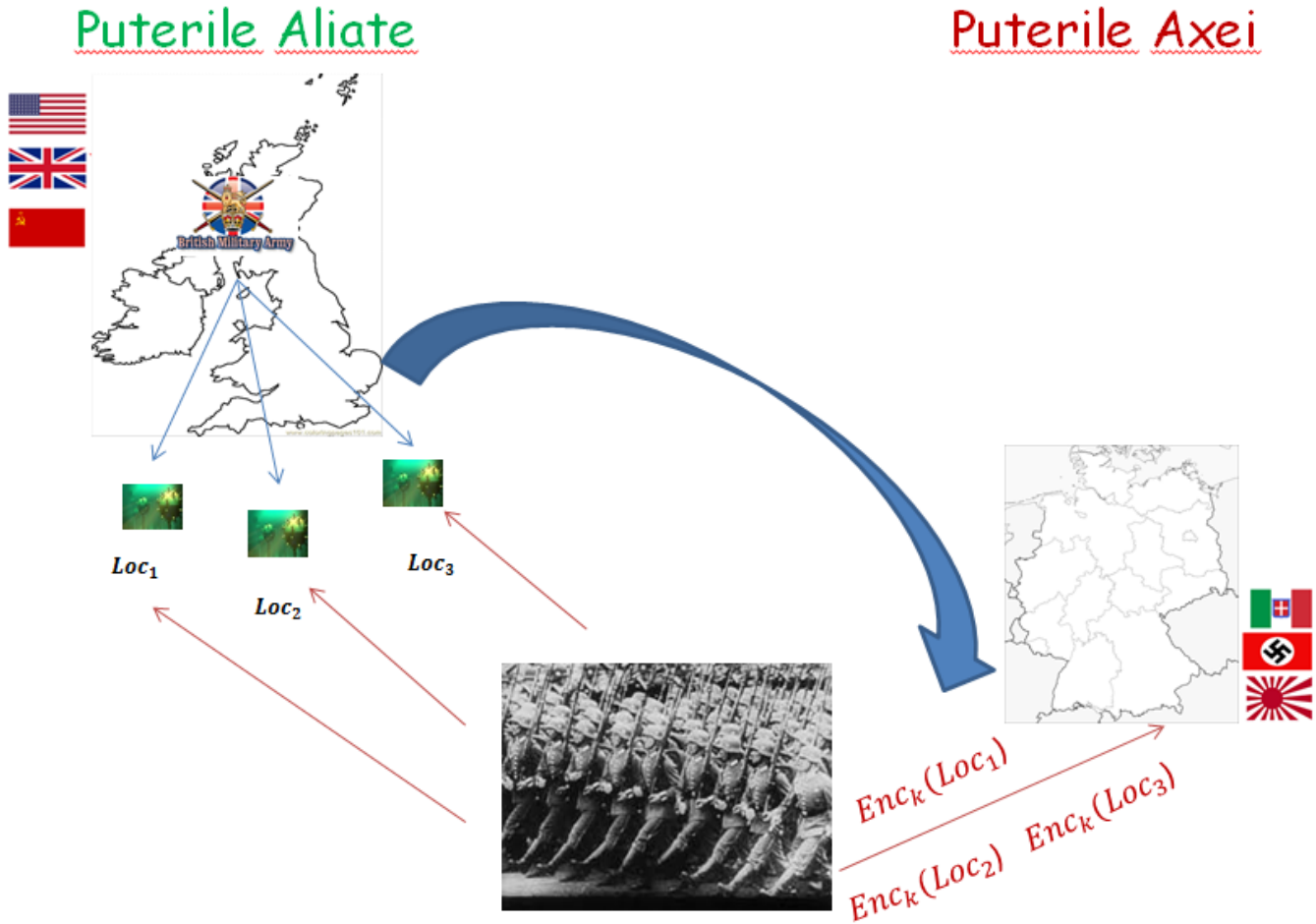
Securitate CPA - al doilea război mondial

...știind că armata germană le va găsi și va trimite locațiile lor criptate către sediu



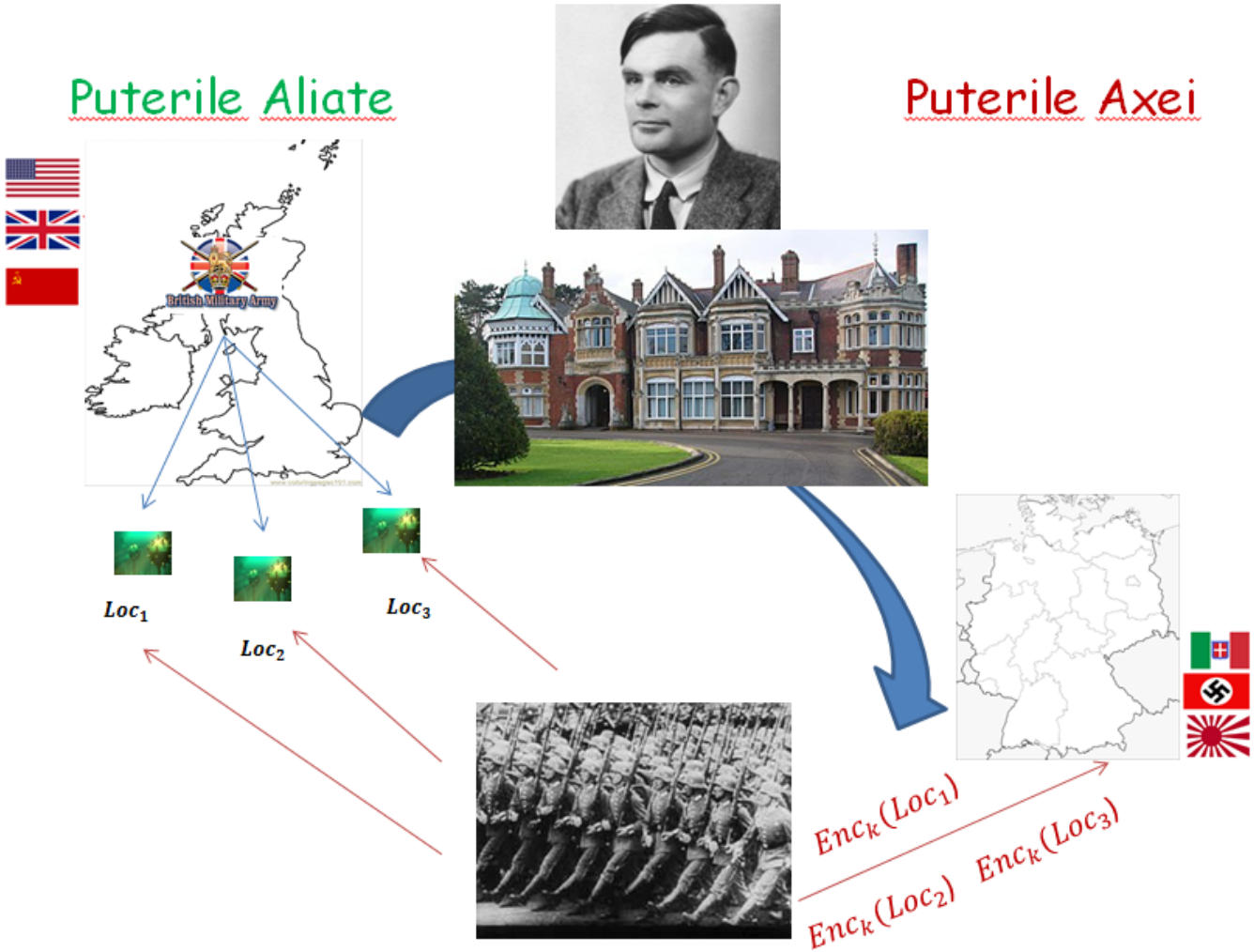
Securitate CPA - al doilea război mondial

aceste mesaje criptate au fost interceptate de către englezi ...



Securitate CPA - al doilea război mondial

... si folosite la Bletchely Park pentru criptanaliza mașinii Enigma



Securitate CPA

- Întrebare: Un sistem de criptare CPA-sigur are întotdeauna proprietatea de indistinctibilitate?

Securitate CPA

- Întrebare: Un sistem de criptare CPA-sigur are întotdeauna proprietatea de indistinctibilitate?
- 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 are întotdeauna proprietatea de indistinctibilitate?
- 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 are întotdeauna proprietatea de indistinctibilitate?
- 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

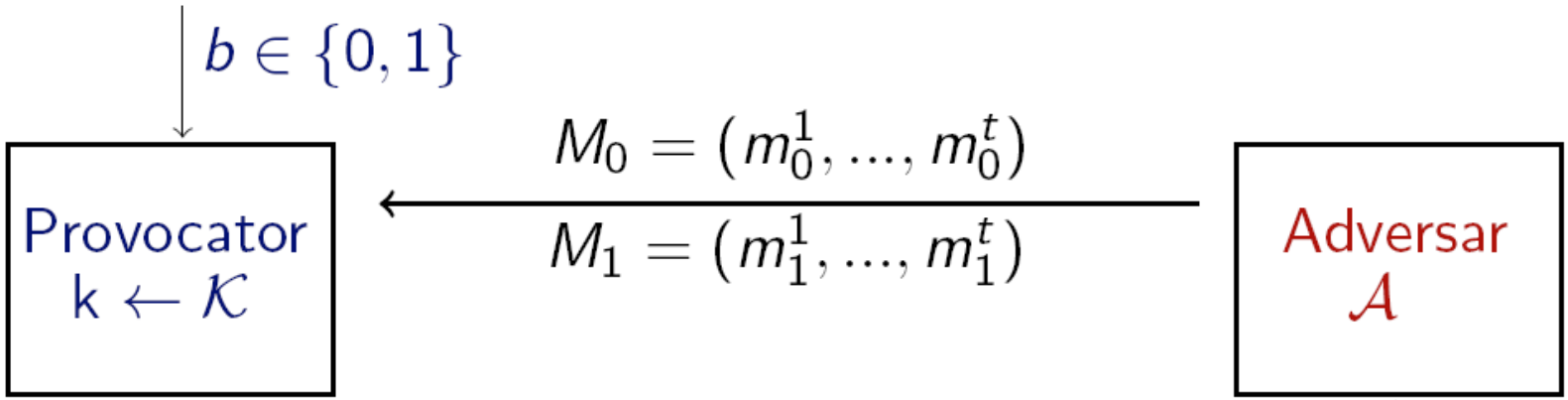
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;

Securitate CPA - Criptare multiplă

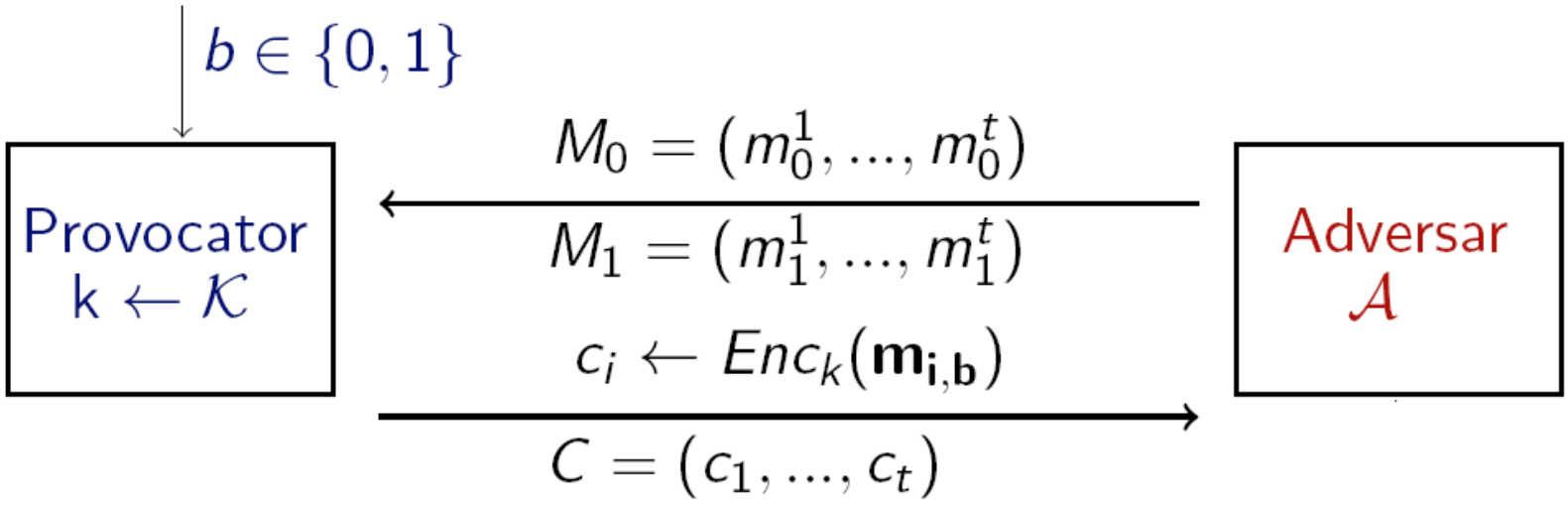
- În definiția precedentă am considerat cazul unui adversar care primește **un singur** text criptat;
- În realitate, în cadrul unei comunicații se trimit **mai multe mesaje** pe care adversarul le poate intercepta;
- Definim ce înseamnă o schemă sigură chiar și în aceste condiții.

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

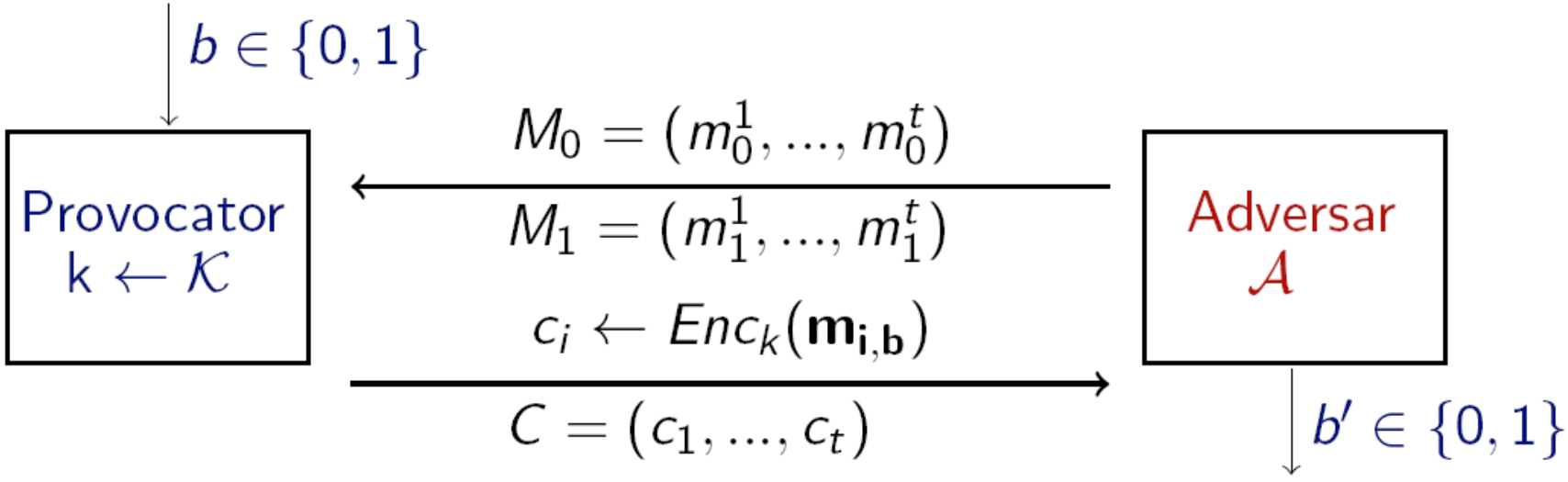
Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



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

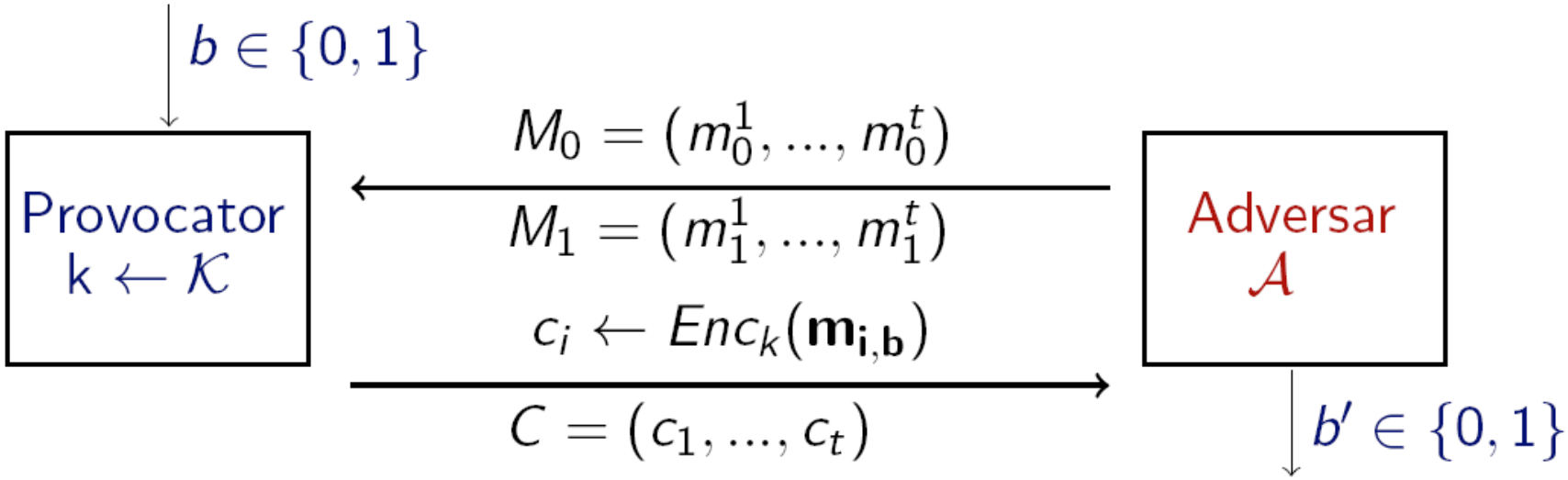


Experimentul $Priv^{cpa}_{\mathcal{A},\pi}(n)$



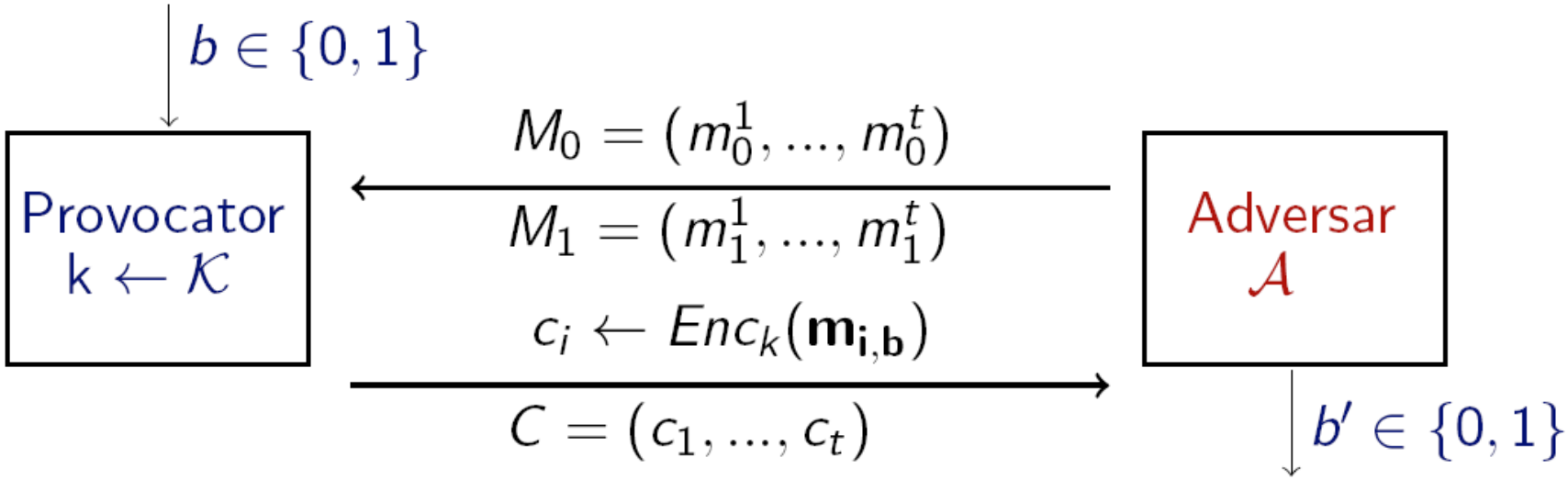
- Pe toată durata experimentului, $\mathcal{A}$ are acces la oracolul de criptare $Enc_k(\cdot)$!

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



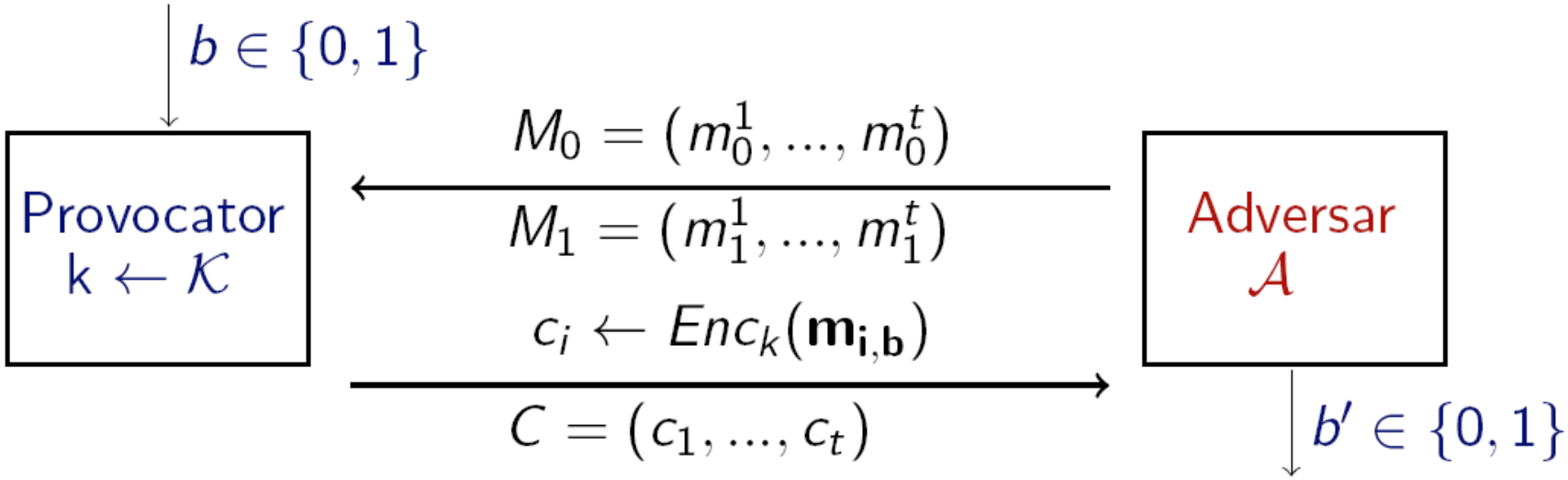
- Output-ul experimentului este 1 dacă $b' = b$ și 0 altfel;

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**!