Criptografie și Securitate

- Prelegerea 13 -
Scheme de criptare CCA sigure

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Securitate CCA

- In cursul precedent am introdus noțiunile de securitate CPA și securitate CCA;

Securitate CCA

- In cursul precedent am introdus noțiunile de securitate CPA și securitate CCA;
- Multe dintre schemele prezentate până acum sunt CPA sigure (sistemele bloc împreună cu modurile de utilizare CBC, OFB și CTR);

Securitate CCA

- In cursul precedent am introdus noțiunile de securitate CPA și securitate CCA;
- Multe dintre schemele prezentate până acum sunt CPA sigure (sistemele bloc împreună cu modurile de utilizare CBC, OFB și CTR);
- Insă nici una din schemele prezentate nu este CCA sigură;

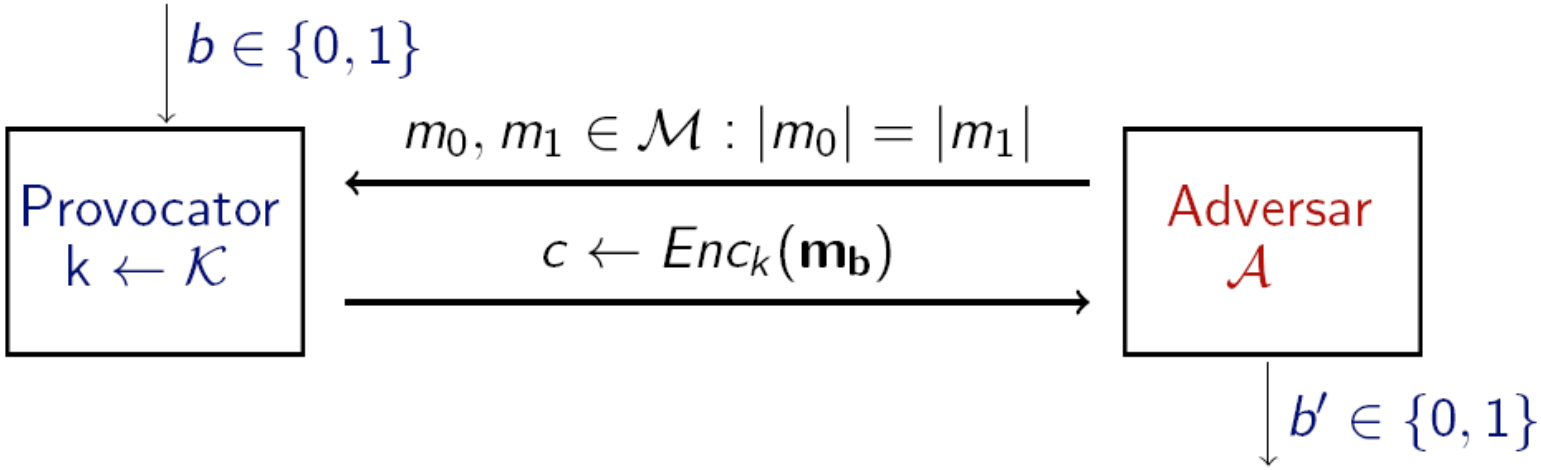
Securitate CCA

- In cursul precedent am introdus noțiunile de securitate CPA și securitate CCA;
- Multe dintre schemele prezentate până acum sunt CPA sigure (sistemele bloc împreună cu modurile de utilizare CBC, OFB și CTR);
- Insă nici una din schemele prezentate nu este CCA sigură;
- In acest curs vom folosi MAC-uri împreună cu scheme CPA sigure pentru a construi scheme CCA sigure;

Securitate CCA

- In cursul precedent am introdus noțiunile de securitate CPA și securitate CCA;
- Multe dintre schemele prezentate până acum sunt CPA sigure (sistemele bloc împreună cu modurile de utilizare CBC, OFB și CTR);
- Insă nici una din schemele prezentate nu este CCA sigură;
- In acest curs vom folosi MAC-uri împreună cu scheme CPA sigure pentru a construi scheme CCA sigure;
- Incepem prin a reaminti noțiunea de schemă CCA sigură;

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

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

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

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:
  - criptează m folosind schema CPA sigură, rezultând textul criptat c

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:
  - criptează m folosind schema CPA sigură, rezultând textul criptat c
  - calculează un tag MAC t pe textul criptat c

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:
  - criptează m folosind schema CPA sigură, rezultând textul criptat c
  - calculează un tag MAC t pe textul criptat c
  - rezultatul final al criptării este $\langle c, t \rangle$

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:
  - criptează m folosind schema CPA sigură, rezultând textul criptat c
  - calculează un tag MAC t pe textul criptat c
  - rezultatul final al criptării este $\langle c, t \rangle$
- Pentru un text criptat $\langle c, t \rangle$, Bob verifică validitatea tag-ului înainte de a decripta;

Schemă de criptare CCA sigură

- Cele două părți comunicante partajează două chei secrete, una pentru schema de criptare CPA sigură și încă una pentru un cod de autentificare a mesajelor (MAC).
- Pentru criptarea unui mesaj m, Alice procedează astfel:
  - criptează m folosind schema CPA sigură, rezultând textul criptat c
  - calculează un tag MAC t pe textul criptat c
  - rezultatul final al criptării este $\langle c, t \rangle$
- Pentru un text criptat $\langle c, t \rangle$, Bob verifică validitatea tag-ului înainte de a decripta;
- Un text criptat $\langle c, t \rangle$ este *valid* daca t este un tag valid pentru c.

O schemă de criptare CCA sigură

Construcție

Fie $\Pi_E = (\mathrm{Enc}, \mathrm{Dec})$ *o schemă de criptare cu cheie secretă și* $\Pi_M = (\mathrm{Mac}, \mathrm{Vrfy})$ *un cod de autentificare a mesajelor.*
Definim schema de criptare $(\mathrm{Enc}', \mathrm{Dec}')$ *astfel:*

- Enc*: pentru o cheie* (k_1, k_2) *și un mesaj* m*, calculează* $c = \mathrm{Enc}_{k_1}(m)$ *și* $t = \mathrm{Mac}_{k_2}(c)$ *și întoarce textul criptat* $\langle c, t \rangle$*;*
- Dec*: pentru o cheie* (k_1, k_2) *și un text criptat* $\langle c, t \rangle$*, verifică dacă* $\mathrm{Vrfy}_{k_2}(c, t) = 1$*. In caz afirmativ, întoarce* $\mathrm{Dec}_{k_1}(c)$*, altfel întoarce* $\perp$*.*

- Simbolul $\perp$ indică eșec;
- Corectitudinea schemei cere ca $Dec_{k_1,k_2}(Enc_{k_1,k_2}(m)) \neq \perp$.
- Spunem că $(\mathrm{Mac}, \mathrm{Vrfy})$ are *tag-uri unice* dacă $\forall m \, \forall k \, \exists$ un unic tag t a.î. $\mathrm{Vrfy}_k(m, t) = 1$.

O schemă de criptare CCA sigură

Teoremă

Dacă schema de criptare Π_E este CPA-sigură și Π_M este un MAC sigur cu tag-uri unice, atunci construcția precedentă reprezintă o schemă de criptare CCA-sigură.

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;
- Mesajele pe care adversarul $\mathcal{A}$ le trimite către oracolul de decriptare sunt de 2 feluri:

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;
- Mesajele pe care adversarul $\mathcal{A}$ le trimite către oracolul de decriptare sunt de 2 feluri:
  - texte criptate pe care $\mathcal{A}$ le-a primit de la oracolul de criptare (știe deja textul clar, deci nu îi sunt de folos);

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;
- Mesajele pe care adversarul $\mathcal{A}$ le trimite către oracolul de decriptare sunt de 2 feluri:
  - texte criptate pe care $\mathcal{A}$ le-a primit de la oracolul de criptare (știe deja textul clar, deci nu îi sunt de folos);
  - texte criptate pe care nu le-a primit de la oracolul de criptare;

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;
- Mesajele pe care adversarul $\mathcal{A}$ le trimite către oracolul de decriptare sunt de 2 feluri:
  - texte criptate pe care $\mathcal{A}$ le-a primit de la oracolul de criptare (știe deja textul clar, deci nu îi sunt de folos);
  - texte criptate pe care nu le-a primit de la oracolul de criptare;
- Insă, cum Π_M este un MAC sigur, cu probabilitate foarte mare textele criptate care nu au fost obținute de la oracolul de criptare sunt invalide, iar oracolul de decriptare va întoarce $\perp$ în acest caz;

Demonstrație intuitivă

- Un text criptat $\langle c, t \rangle$ este valid (în raport cu o cheie (k_1, k_2)) daca $\mathrm{Vrfy}_{k_2}(c, t) = 1$;
- Mesajele pe care adversarul $\mathcal{A}$ le trimite către oracolul de decriptare sunt de 2 feluri:
  - texte criptate pe care $\mathcal{A}$ le-a primit de la oracolul de criptare (știe deja textul clar, deci nu îi sunt de folos);
  - texte criptate pe care nu le-a primit de la oracolul de criptare;
- Insă, cum Π_M este un MAC sigur, cu probabilitate foarte mare textele criptate care nu au fost obținute de la oracolul de criptare sunt invalide, iar oracolul de decriptare va întoarce $\perp$ în acest caz;
- Cum oracolul de decriptare este inutil, securitatea schemei $(\mathrm{Enc}', \mathrm{Dec}')$ se reduce la securitatea CPA a schemei Π_E.

Important de reținut!

- Schemă de criptare CPA-sigură și MAC sigur aplicat pe textul criptat (*encrypt then MAC*) $\Rightarrow$ schemă de criptare CCA sigură