# apprentissage automatique préservant la confidentialité basé sur le chiffrement homomorphique

Serigne Saliou Gueye

March 29, 2021

# R E M E R C I E M E N T S

Acknowledgement goes here

# RESUMÉ

# INTODUCTION GÉNÉRALE

# ABSTRACT

# CONTENTS

# PART I

# CONTEXTE ET INTRODUCTION

# CHAPTER 1

# NOTION PRÉLIMINAIRES DE LA CRYPTOGRAPHIE

Avant de passer à la définition du chiffrement homomorphe, nous allons revenir sur quelques notions cryptographiques à savoir les différents systèmes cryptographique (systèmes à clés secrètes et à clés privés) et aussi parler de la sécurité prouvée en cryptographie. Pour des traitements beaucoup plus approfondis de ces concepts nous renvoyons le lecteur sur [références](Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (Chapman Hall/Crc Cryptography and Network Security Series). Chapman Hall/CRC, 2007.)

## 1.1 Introduction

La cryptographie est une discipline des maths incluant des principes et méthodes permettant de garantir les services de sécurité de l'information .Sa principale mission est de garantir la sécurité des communications c'est-à-dire de permettre à des entités qui ne se font pas confiance en général de communiquer en toute sécurité en présence de potentiels adversaires (susceptibles entre autres d'accéder à des secrets en violant la confidentialité, d'intercepter et de modifier les informations échangées ou d'usurper des identités lors d'une communication).
La cryptographie ne prend en charge que les 4 premiers sur les 5 services de

sécurité fondamentaux que sont la Confidentialité, l'intégrité, l'authentification, la Non Répudiation et la Disponibilité.Elle est composée des systèmes à clé secrète et des systèmes à clés publiques.
Dans un système à clés secrètes les entités se partagent la même clé pour le chiffrement et le déchiffrement (on parle de cryptographie symétrique)

Dans le cas du système à clé publique, on utilise deux clés dont l'une soit k' est difficile à déduire de l'autre soit k (on parle aussi de cryptographie asymétrique). La clé k est appelée clé publique et est utilisée pour le chiffrement ou la vérification de signature selon le système ; la clé k' est appelée clé privée et est utilisée pour le déchiffrement ou la signature selon le système.

Les algorithmes de chifffrements et les protocoles cryptographique sont impliqués dans une variété d'applications critiques: : les banques en ligne, le vote électronique, la vente aux enchères électroniques... En tant que tels, leurs securités doivent donc être formellement vérifiées et prouvées

## 1.2 Sécurité inconditionelle

### 1.2.1 Notion de sécurité parfaite

Un cryptosytéme est parfois définis par trois algorithmes :Algorithme de génération des clés ,de chiffrement et de déchiffrement ainsi qu'une specification d'un espace de message M avec #M > 1
L'algorithme de génération des clés que nous notons GEN est un algorithme probabiliste qui produit une clé k choisit selon une certaine distribution. Nous désignons par K l'espace des clés c'est à dire l'ensemble de toutes les clés possibles qui peuvent être sortis par GEN
L'algorithme de chiffrement que nous allons noté par ENC prend en entré une clé $\kappa \in$ K et un messsage m $\in$ M produit un chiffré c .Nous considérons que l'algorithme de chiffrement est probabiliste donc ENC(k,m)peut alors générer des chiffrés différents lorsque le même message est utilisé.On note c $\mapsto ENC_{\kappa}(m)$.On note C l'ensemble de tous les chiffrés possibles
L'algorithme de déchiffrement noté par DEC prend en entré une clé $\kappa$ et un chiffré c et produit le message initial m. Contrairement à ENC l'algorithme de déchiffrement est déterministe puisque $\mathrm{DEC}_{\kappa}(c)$donne la même sortie à chaque exécution on notera donc m:=$\mathrm{DEC}_{\kappa}(c)$pour designer le caractére deterministe

Il est évident que si l'attaquant détient la clé alors il pourra déchiffrer tous les messages échangés par les entités. Alors qu'en est-il de ENC ? N'est-il pas mieux de garder tous les deux (l'algorithme et la clé) secret?
Auguste Kerckhoffs a soutenu le contraire à la fin du 19e siècle lors de l'élucidation de plusieurs principes de conception de chiffrements militaires. L'un des plus important d'entre eux, désormais simplement connu sous le nom de principe de Kerckhoff.

### 1.2.2 principe de Kerckhoff

La méthode de chiffrement ne doit pas être tenue secrète, et elle doit pouvoir tomber entre les mains de l'attaquant sans inconvénient.
Pour pouvoir bien comprendre ce principe et voir l'importance de garder la clé secrète nous pouvons considérer l'exemple suivant
Soit m un message $\in \{0,1\}^n$ . On definit notre algorithme de chiffrement (ENC) en faisant la somme directe entre m et $\kappa \in$ K c = m $\oplus$ $\kappa$ .On peut voir dans cet algorithme de chiffrement que si $\kappa$ est fixé alors ce cryptosystéme ne sera pas sur et l'attaquant obtenir le massage initial à partir du chiffré en faisant m = c $\oplus$ $\kappa$.
Par contre si $\kappa$ est choisit de façon uniformément aléatoire dans l'espace des clés $\{0,1\}^n$ et gardé secret pour l'attaquant alors le résultat du chiffré sera uniformément distribué dans l'espace des chiffrés $\{0,1\}^n$ et la sécurité sera atteinte

### 1.2.3 Principe de Shannon

Un chiffré doit apporter de la confusion et de la diffusion, c'est-à-dire :

Confusion
Il n'y a pas de relation algébrique simple entre le clair et le chiffré. En particulier, connaître un certain nombre de couples clair-chiffré ne permet pas d'interpoler la fonction de chiffrement pour les autres messages.
Diffusion
La modification d'une lettre du clair doit modifier l'ensemble du chiffré. On ne peut pas casser le chiffre morceau par morceau.

### 1.2.4 Théoréme du secret parfait

Avant d'énoncer ce théoréme,nous allons considérer les deux exemples ci-dessous

**exemple 1**

Considérons l'exemple simple du chiffrement de césar suivant
Soit $\kappa \in \{0,.....25\}$ avec $\Pr[K=\kappa]$ la probabilité que la clé soit k (on considère que les clés sont équiprobable) donc $\Pr[K=\kappa]=\frac{1}{26}$ . Supposons que nous avons la distribution suivante sur M:$\Pr[M=a]=0,7$ et $\Pr[M=z]=0,3$. ($\Pr[M=a]$ probabilité que le message soit a et $\Pr[M=z]$ probabilité que le message soit z ).Ainsi on cherche alors la probabilité que le message chiffré soit B
On peut voir qu'il n'y a deux possibilités :soit M=a et K=1 ,soit m=z et k= 2 .Par indépendance de M et K nous avons $\Pr[M=a\wedge K=1]$ =$\Pr[M=a]$*$\Pr[K=1]$,de même $\Pr[M=z\wedge K=2]$ =$\Pr[M=z]$*$\Pr[K=2]$.
Par conséquent,
$\Pr[C=B]=\Pr[M=a\wedge K=1]+\Pr[M=z\wedge K=2]=0,7\ \frac{1}{26}+0,3\ \frac{1}{26}=\frac{1}{26}$ donc
$\Pr[C=B]=\frac{1}{26}$
Nous pouvons également calculer la probabilité conditionnelle par exemple calculer la probabilité que le chiffré B soit issu de a ,$\Pr[a\mid B]$.En utilisant le théoréme de Bayes nous obtenons :

$$Pr[M=a\mid C=B]=\frac{Pr[C=B\mid M=a].Pr[M=a]}{Pr[C=B]}$$

Notons que $Pr[C=B\mid M=a]=\frac{1}{26}$ , puisque si M = a alors la seule voie C = B peut se produire si $\kappa$ = 1 ce qui se produit avec une probabilité de $\frac{1}{26}$

$$\text{Donc } Pr[M=a\mid C=B]=\frac{Pr[C=B\mid M=a].Pr[M=a]}{Pr[C=B]}=\frac{\frac{1}{26}.O,7}{\frac{1}{26}}$$

$$Pr[M=a\mid C=B]=0,7$$

Conclusion
on a $\Pr[M=a]=Pr[M=a\mid C=B]=0,7$ .
Ce résultat montre que la probabilité d'avoir une information claire sur le claire a ne varie pas même si on connait son chiffré B

**exemple 2**

Considérez à nouveau le chiffre de décalage, mais avec la distribution suivante sur M:

$\Pr[M=kim]=0,5$, $\Pr[M=ann]=0,2$, $\Pr[M=boo]=0,3$
Calculons alors la probabilité pour que le chiffré C soit égale à DQQ.La seule façon dont ce chiffré peut se produire est si M = ann et K = 3, ou M = boo et K =

2, ce qui arrive avec la probabilité $0{,}2 \cdot \frac{1}{26} + 0{,}3 \cdot \frac{1}{26} = \frac{1}{52}$.
Nous pouvons également calculer la probabilité que le chifré DQQ soit isuu de ann.? Un calcul comme ci-dessus en utilisant le théorème de Bayes donne $Pr\left[M = ann \mid C = DQQ\right] = 0{,}4$
conclusion
On a $\Pr\left[M = ann\right] \neq \Pr\left[M = ann \mid C = DQQ\right]$ dans cette exemple nous avons vu avec cette distribution que la probabilité d'avoir une information claire ann varie si son chiffré DQQ est connu

**Commentaire**

Nous pouvons maintenant definir la notion de secret parfait .On imagine un adversaire qui connaît la distribution de probabilité de M c'est-à-dire que l'adversaire connaît la probabilité que différents messages soient envoyés.
L'adversaire connaît également le schéma de chiffrement utilisé. La seule chose Inconnue de l'adversaire est la clé partagée par les parties. Un message est choisi par l'une des parties et chiffré, et le texte chiffré résultant est transmis à l'autre partie. L'adversaire peut espionner la communication des parties, et ainsi observer ce texte chiffré. (Autrement dit, c'est un Attaque de texte chiffré uniquement « ciphertext-only attack », où l'attaquant ne voit qu'un seul texte chiffré.)
Dans un schéma parfaitement secret, l'observation de ce texte chiffré ne devrait avoir aucun effet sur la connaissance de l'adversaire concernant le message réel qui a été envoyé; autrement dit, la probabilité a posteriori qu'un message $m \in M$ ait été envoyé,conditionné par le texte chiffré qui a été observé, ne devrait pas être différente de la probabilité a priori que m serait envoyé. Cela signifie que le texte chiffré ne révèle rien sur le message envoyé sous-jacent et que l'adversaire n'apprend absolument rien sur le texte en clair qui a été chiffré. Formellement

**Definition 1**

Un cryptosystéme (GEN,ENC,DEC) avec M l'espace de messages est parfaitement secret si pour toute distribution de probabilité sur M et $\forall\ m \in M$ et $c \in C$ telque Pr[C=c]>0 on a ;

$$Pr\left[M = m \mid C = c\right] = Pr\left[M = m\right].$$

(L'exigence que Pr [C = c]> 0 est une condition nécessaire pour éviter le Conditionnement sur un événement à probabilité nulle.)
Nous pouvons voir que le chiffrement de césar n'est pas parfaitement secret

**Théorème du secret parfait, Shannon**

Soit (M,K,C, GEN,ENC,DEC) un cryptosytéme .On suppose que #M =#K =#C $<\infty$ et que Pr[M=m]>0 $\forall$ m $\in$ M . Alors ce cryptosytéme est à secert parfait Si seulement si

• La distribution des clés suit une loi uniforme

• pour tout clair m appartient à M

$$\phi_m = \begin{cases} K \longrightarrow \mathrm{C} \\ \kappa \longrightarrow \mathrm{ENC}_\kappa(m) \end{cases}$$

est une bijection

**Démonstration**

On suppose avoir secret parfait. On montre d'abord la bijectivité, puis l'équiprobabilité.
Bijectivité
S'il existe m tel que $\phi_m : k \mapsto \mathrm{ENC}_\kappa(m)$est non surjective, il existe c $\in$ C tel que $\forall$ $\kappa\in$ K, $ENC_\kappa(m) \neq c$. En particulier $\Pr[C = c \mid M = m]$=0, d'où l'on tire $\Pr[M = m \mid C = c]$=0$\neq$ $\Pr[M = m]$>0 impossible. Donc $\phi_m$ est surjective, et par égalité des cardinaux bijective.
Equiprobabilité
Soit c $\in$ C un chiffré fixé. Pour tout m $\in$ M, on note $\kappa$(m) l'unique clef telle que $ENC\ \kappa m$ [m]=c (d'après la bijectivité). On a $\Pr[M = m \mid C = c]$ = $\Pr[K = \kappa(\mathrm{m})]$

Puisque par hypothèse $\Pr[M = m \mid C = c]$=$\Pr[M = m]$, on obtient $\Pr[K = \kappa(\mathrm{m})]$=$\Pr[C = c]$.Or le chiffrement m$\mapsto\mathrm{ENC}_\kappa(m)$est injectif à clef fixé, donc bijectif. Donc pour toute clef $\kappa$, il existe m tel que $\kappa$=$\kappa$(m).

Ainsi, $\Pr[K = \kappa]$ = $\Pr[K = \kappa(\mathrm{m})]$ = $\Pr[C = c]$est constante, et vaut $\frac{1}{\#K}$

Dans le sens réciproque, il suffit d'effectuer le calcul : par équiprobabilité des clefs

## 1.3 définition de sécurité pour la cryptographie à clé privée

Avant de parler de la sécurité, nous allons définir formellement ce que signifie être sùr pou un système cryptographique .La sécurité d'un cryptosysteme est évaluée du fait qu'un adversaire efficace peut ou non différencier ou distinguer le chiffré de deux textes clairs dans une preuve par jeux donnée .

**Fonction négligeable**

Une fonction F de $N \longrightarrow R$ est dite negligeable si pout tout polynome P il existe $n_0 \in$ N telque pour tout n> $n_0$ on a:

$$F(n) < \frac{1}{P(n)}$$

Dans ce qui suit le terme on utilisera le terme « securité eav» pour désigner la sécurité du preuve par jeu en présence d'un espion comme noté dans la [référence]

### 1.3.1 sécurité EAV

**indistinguabilité**

On considère une expérience noté $\text{PrivK}^{eav}$ dans lequel un adversaire A émet deux messages $m_0, m_1$ et recoit le chiffré d'un de ces messages .La définition de l'indistinguabilité stipule qu'un schèma E est sûr si aucun adversaire A ne peut déterminer lequel des deux messages a été chiffre on dit alors que le cryptosysteme est indistinguable

**Définition de l'expérience**

L'expérience est définie pour un schéma de chiffrement à clé privée E = (GEN, ENC, DEC), un adversaire A, et une valeur n pour le paramètre de sécurité :
1 ) L'adversaire A émet deux messages $m_0, m_1 \in$ M

2)Une clé $\kappa$ est générée à l'aide de l'algorithme GEN, inconnue de l'adversaire de plus un bit aléatoire $b \in \{0,1\}$ est choisi pour sélectionner $m_0, m_1$ . On calcule c=$ENC_\kappa\left(m_b\right)$et on donne le chiffré c à A comme challenge

3)A émet alors un bit b ' dans le but d'avoir b'=b

4 ) Le résultat de l'expérience est 1 si b'=b et 0 sinon .Dans le cas ou le résultat est 1 on dit que A a réussi et on note PrivK$^{eav}_{A,E}$ =1
Ainsi formellement nous pouvons definir la « securité EAV » comme suit

**Définition 2**

Un schéma de chiffrement à clé privée E= (GEN, ENC, DEC) est indistinguable sous une attaque eav(attaque en présence d'espion) si pour tout algorithme probaliste ,il existe une fonction negligeable negl telle que

$$\Pr\left[PrivK^{eav}_{A,E}(\mathrm{n}) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(\mathrm{n})$$

Où la probabilité est prise aléatoirement et l'expérience également (c'est-à-dire le choix de la clé, du bit b ainsi que tout paramètre utilisé par ENC).

### 1.3.2 Attaque par texte choisi (Choosen plaintext Attack CPA)

Formellement, nous modélisons les attaques par texte choisi en donnant à l'adversaire A l'accès à un oracle de chiffrement, vu comme une boîte noire" qui chiffre les messages choisis par A à l'aide d'une clé k inconnue de lui. Autrement dit, nous imaginons que A a accès à un "oracle" ENC$\kappa$(-) ; lorsque A interroge cet oracle en lui fournissant un message m comme entrée, l'oracle renvoie un texte chiffré c $\leftarrow$ ENC$\kappa$(m) comme réponse. (Si ENC est randomisé, l'oracle oracle utilise un nouvel aléa chaque fois qu'il répond à une requête). L'adversaire peut interagir avec l'oracle de chiffrement de manière adaptative, autant de fois qu'il le souhaite.

Considérons l'expérience suivante définie pour tout schéma de chiffrement E = (GENC, ENC, DEC), l'adversaire A, et la valeur n pour le paramètre de sécurité :

1.) Une clé k est générée en utilisant GEN. L'adversaire A, qui ne connaît pas la clé, est autorisé à effectuer un nombre polynomial de requêtes à un oracle de chiffrement ENC$\kappa$.

2.)A émet deux messages $\mathrm{m}_0, m_1 \in \mathrm{M}$

3.) On choisit un bit aléatoire b $\in \{0,1\}$. On calcule c = ENC$\kappa$($\mathrm{m}_b$) et on donne le chiffré c à A comme le challenge

4.) A continue à avoir accès à l'oracle de chiffrement ENC$\kappa$.

5.) A sort un bit b' dans le but d'avoir b'= b

6.) La sortie de l'expérience est 1 si b'= b et 0 sinon. Nous appelons le premier cas le succès de A et le désignons par PrivK$^{cpa}_{A,E}$ =1
.

**Définition 3**

Un schéma de chiffrement à clé privée E = (GEN, ENC, DEC) est sûr en cas d'attaque par texte plat choisi (CPA) si, pour tous les adversaires probabilistes en temps polynomial A, il existe une fonction négligeable negl telle que

$$\Pr\left[PrivK^{cpa}_{A,E}(\mathrm{n}) = 1\right] \leq \frac{1}{2} + \mathrm{negl(n)}$$

**proposition 1**

Un schéma de chiffrement E dont l'algorithme de chiffrement ENC est déterministe ne peut pas être CPA-sûr

**Démonstration**

Considérons l'adversaire A suivant qui joue le jeu de sécurité CPA comme suit :
1.) Sélectionner deux messages aléatoires distincts $\mathrm{m}_0, m_1 \in \mathrm{M}$.
2.) Utiliser l'oracle de chiffrement pour obtenir les chiffrés $\mathrm{c}_0 = ENC\kappa(\mathrm{m}_0)$ et $\mathrm{c}_1 = ENC\kappa(\mathrm{m}_1)$.
3.) Sortir les deux messages $\mathrm{m}_1, m_1 \in \mathrm{M}$
4.) A la réception du texte chiffré c, si c = $\mathrm{c}_0$ , sortir le bit 0, sinon sortir le bit 1.
Comme ENC est déterministe, le texte chiffré du challenge c, étant un chiffrement de $\mathrm{m}_0$ ou $\mathrm{m}_1$ , sera égal à $\mathrm{c}_0$ ou $\mathrm{c}_1$ . Ainsi, A pourra réussir avec une probabilité non négligeable sur $\frac{1}{2}$ (en particulier,A réussira toujours). Ainsi, E ne peut pas être CPA-sûr

### 1.3.3 Attaque à chiffré choisi (Choosen Cipher text Attack)(CCA)

Qu'est-ce que cela signifie pour un schéma de chiffrement de résister contre les attaques à chiffre choisi ? Comme d'habitude pour définir une notion de sécurité appropriée, nous devons définir deux choses : la capacité supposé de l'attaquant

et ce qui constitue une attaque réussie .Pour ce dernier nous suivrons l'approche adoptée dans les définitions précédentes .Nous allons donc donner à l'attaquant un texte chiffré c comme challenge issu des messages $m_0$ ou $m_1$ (chacun choisi avec une probabilité égale )et on considère que le schéma est cassé si l'attaquant peut déterminer lequel des deux messages a été chiffre avec une probabilité significative meilleur que ½

L'attaque par chiffré choisi (CCA) permet à l'adversaire de disposer à la fois d'un oracle de chiffrement et de déchiffrement qu'il peut interroger à tout moment pendant le jeu.
D'autres textes distinguent les attaques par chiffré choisi non adaptative et les attaques par chiffres choisis adaptative .Les premières également appelé lunchtime permettent seulement à l'adversaire d'utiliser l'oracle de déchiffrement avant de recevoir le challenge (le chiffré) .La seconde un modèle d'attaque beaucoup plus puissant permet à l'adversaire de continuer d'utiliser l'oracle de déchiffrement après avoir reçu le challenge ,mais évidemment il n'est pas autorisé à interroger l'oracle de déchiffrement avec le challenge . Dans ce mémoire nous faisons allusion à la seconde cas lorsque nous parlerons d'attaque CCA Comme nous pouvons le voir la sécurité CCA est beaucoup plus forte que la sécurité CPA ou EAV et les implique tous les deux. Nous présenterons les définitions formelles ci-dessous

Considérons l'expérience suivante définie pour tout schéma de chiffrement E = (GENC, ENC, DEC), l'adversaire A, et la valeur n pour le paramètre de sécurité :

1)Une clé est généré à l'aide de l'algorithme de génération des clés GEN.L'adversaire A qui ne connait pas la clé ,peut effectuer un nombre polynomiale de requête à un oracle de chiffrement et de déchiffrement

2)A emet deux meaages $m_0$ , $m_1$

3)On choisit un bit aléatoire $b \in \{0,1\}$. On calcule c = ENC$\kappa(m_b)$et on donne c à A comme challenge

4)A continué à avoir accès à l'oracle de chiffrement et de déchiffrement mais avec la restriction que A ne peut pas exécuter l'oracle de déchiffrement sur le challenge c

5)A produit un bit b' dans le but d'avoir b'=b

6)Le resultat de l'experience est 1 si b'=b et 0 sinon Si b= b' nous disons que A a réussi et nous le désignons par PrivK$^{cca}_{A,E}$ =1
.

**Définition 3**

Un schéma de chiffrement à clé privée E = (KeyGen, Enc, Dec) est ,(CCA) sûr si, pour tous les adversaires probabilistes en temps polynomial A, il existe une fonction négligeable negl telle que

$$\Pr\left[PrivK^{cca}_{A,E}(\mathrm{n}) = 1\right] \leq \frac{1}{2} + \mathrm{negl(n)}$$

# 1.4 Cryptographie à clé publique

## 1.4.1 Fonction à sens unique

Une fonction f : A $\longrightarrow$ B est dite à sens unique s'il est facile à calculer f(x) pour tout x  A (complexité polynômiale)et est difficile (complexité exponentielle) pour presque tout y $\in$ B, de trouver x tel que y = f(x).

Une fonction est à sens unique avec trappe si l'on connaît un secret permettant de l'inverser

## 1.4.2 Fonction de hashage

$\{0,1\}^*$ ensemble des chaines de longueur quelconque, $\{0,1\}^l$ ensemble des chaines longueur fixe avec l≠0.

**définition 3**

Une fonction H $\{0,1\}^* \rightarrow \{0,1\}^l$ est dite fonction de hachage si :
1. Pour tout x, H(x) est facile à calculer, H(x) est appelé le hash ou l'empreinte de x
2. Étant donné H(x), il est difficile de trouver y tel que y = H(x) (fonction à sens unique) ;
3. Étant donné x, il est difficile de trouver x'tel que x ≠ x'et H(x) = H(x'), (collusions faibles) ;

4. Il est difficile de trouver x et x' (de son choix) x≠= x'tel que H(x) = H(x'), (collusions fortes) ;

### 1.4.3 Modélisation du chiffrement à clés publique

Un shéma de chiffrement à clé publique de E=(GEN,ENC,DEC) avec un espace de clés $K = K_{ks} \times K_{kp}$,un espace de message $M$ et un espace chiffré $C$ est un 3-tuple d'algorithme efficace dans lequel :
GEN : $\lambda \longrightarrow K$ algorithme de génération des clés
ENC$\kappa$ : $M \longrightarrow C$ est une fonction à sens unique (avec trappe qui est un inverse à gauche) appelée fonction de chiffrement et qui dépend d'un paramètre $\kappa$ appelé clé(publique)
DEC$\kappa$' : $C \longrightarrow M$ est la trappe et est appelée fonction de déchiffrement (dépendant de la clé $\kappa$') et on a DEC$\kappa$'(ENC$\kappa$(m)) = m

Il existe des définitions identiques pour la sécurité EAV, CPA et CCA pour les systèmes de chiffrements à clé publique. Nous renvoyons le lecteur à [référence] pour les détails.

**proposition 2**

Un cryptosystéme à clé publique est EAV-sùr si et seulement il est Cpa-sùr

**Démonstration**

Dans la version à clé publique du jeu de sécurité EAV, l'adversaire A a accès à la clé publique pk. Par conséquent, A peut calculer $\mathrm{Enc}_{pk}(m)$ lui-même pour tout message m, ce qui est équivalent à donner à A l'accès à un oracle de chiffrement. Par conséquent, pour les schémas de chiffrement à clé publique, la sécurité EAV est équivalente à la sécurité CPA.