Securing multimedia content delivery

Digital watermarking part. II

gaetan.leguelvouit@b-com.com

b com

Notations

- Signal hôte : $\mathbf{x} \in \mathbb{R}^m$
- Message : $\mathbf{m} \in \{0,1\}^n$
- Marque : $\mathbf{w} \in \mathbb{R}^m$
- Attaque : $\mathbf{z} \in \mathbb{R}^m$

$$\mathbf{y} = \mathbf{x} + \mathbf{w}$$

$$\mathbf{r} = \mathbf{y} + \mathbf{z}$$

Communication numérique

Tatouage = communication sur un **canal bruité**
→ formalisation de P_e
→ notion de capacité
→ codes correcteurs

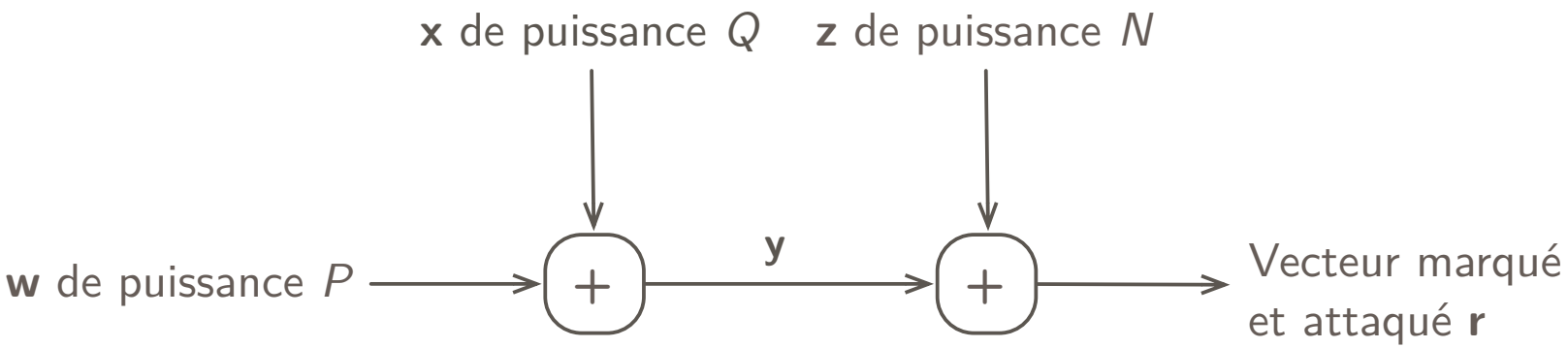
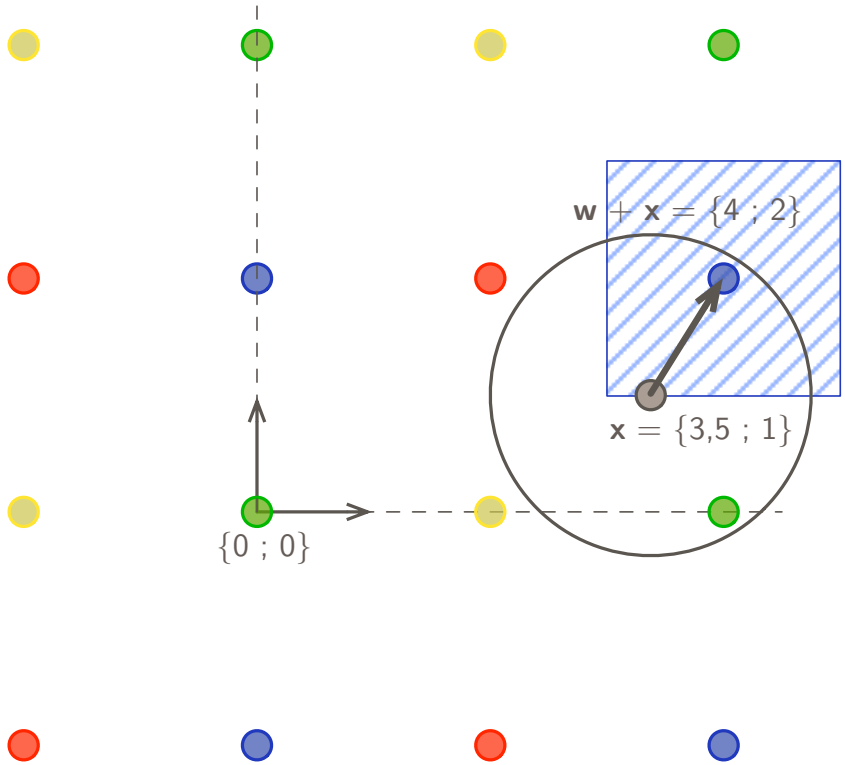


Schéma de Costa

- Information adjacente $\rightarrow$ pas d'impact sur la capacité du canal
- Schéma idéal de Costa impossible à mettre en pratique
- Utilisation de la quantification ou de codes correcteurs modifiés



Paradoxe

- Le tatouage doit être invisible/inaudible : il doit donc être inséré dans les zones perceptuellement peu importantes du document hôte
  - contours des images
  - fréquences $>$ 16 KHz
- Or ces zones sont les premières détruites par la compression avec perte

Consensus empirique

- La plupart des travaux s'accordent pour insérer la marque dans les **moyennes fréquences**
  - perceptuellement assez importantes pour ne pas être détruites par la compression
  - mais pas trop pour que les modifications liées au marquage ne soient pas gênantes

- Reprenons cela plus formellement : comment trouver le meilleur compromis possible ?

Distortion d'insertion

Mesure classique de l'erreur quadratique moyenne entre vecteur hôte et vecteur marqué :

$$\text{EQM} = \frac{1}{m}\sum_{i=1}^{m}(\mathbf{x}[i] - \mathbf{y}[i])^2$$

On y ajoute une pondération perceptuelle sous la forme d'un vecteur $\mathbf{p}$. Pour l'étalement de spectre, ça donne la distorsion d'insertion :

$$\mathrm{D}_{\mathbf{xy}} = \frac{1}{m}\mathbb{E}\left[\sum_{i=1}^{m}\mathbf{p}[i]^2(\mathbf{x}[i] - \mathbf{y}[i])^2\right] = \frac{n}{m}\sum_{i=1}^{m}\mathbf{p}[i]^2\mathbf{a}[i]^2$$

Distortion d'attaque

Reprenons la modélisation (très simplifiée) par ajout de bruit gaussien :

$$\mathbf{r}[i] = \mathbf{y}[i] + \mathbf{z}[i] \times \mathcal{N}(0, 1)$$

On mesure la distortion entre le vecteur tatoué $\mathbf{y}$ et le vecteur attaqué $\mathbf{r}$:

$$\mathrm{D}_{\mathbf{yr}} = \frac{1}{m} \sum_{i=1}^{m} \mathbf{p}[i]^2 \mathbf{z}[i]^2$$

Jouons au morpion

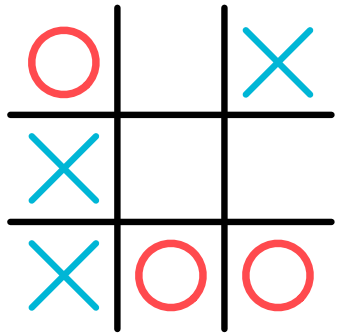
Jeu à plusieurs tours consécutifs, entre 2 joueurs

Considérons la fonction de gain suivante :

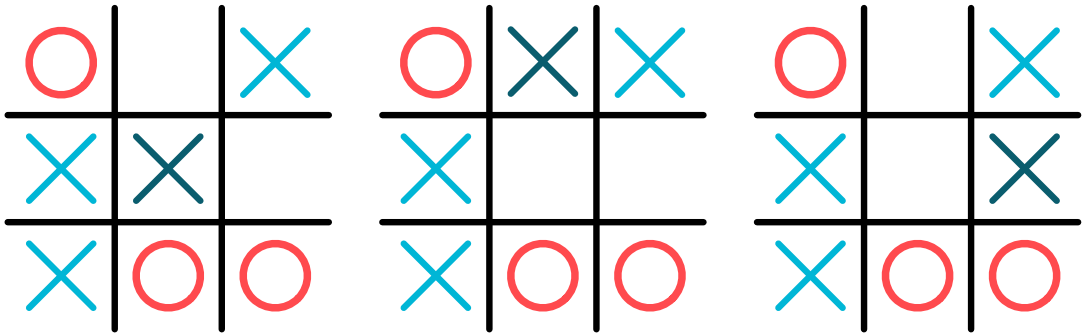
- j'ai gagné $\rightarrow +10$
- j'ai perdu $\rightarrow$ -10
- match nul $\rightarrow 0$

Jouons au morpion

Tour t



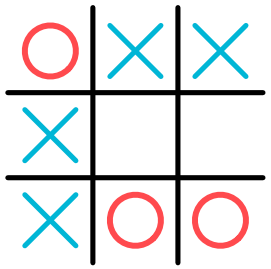
Tour $t+1$



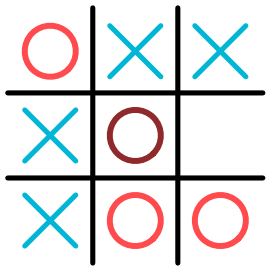
Gagné : $+10$

Jouons au morpion

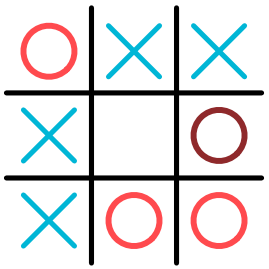
Tour t



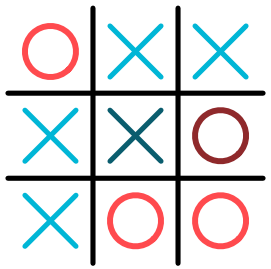
Tour $t+1$



Perdu : -10



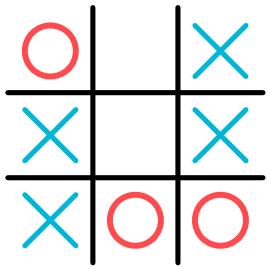
Tour $t+2$



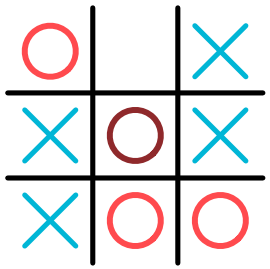
Gagné : +10

Jouons au morpion

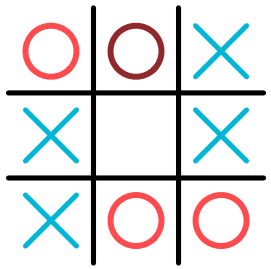
Tour t



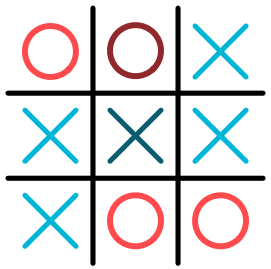
Tour $t+1$



Perdu : -10

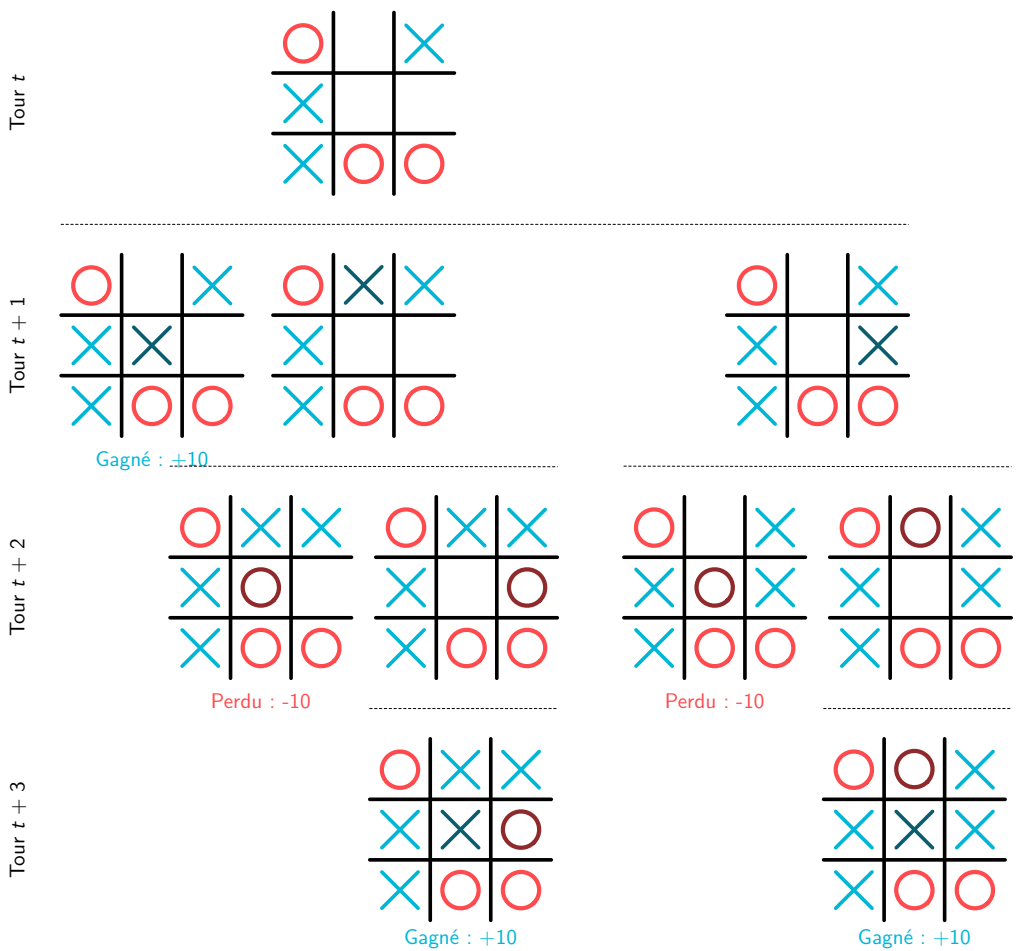


Tour $t+2$



Gagné : +10

Jouons au morpion



Algorithme min-max

1. **si** fin du jeu **alors** retourner le score

2. **sinon**
   - 2.1 faire la liste de tous les états possibles
   - 2.2 **pour** chaque état de liste, calculer min-max
   - 2.3 **si** c'est à mon tour **alors** retourner la valeur max
   - 2.4 **sinon** retourner la valeur min

Stratégie d'attaque

Le rapport signal-à-bruit SNR $= P/N$ du canal de tatouage mesure la performance du schéma

Pour une distorsion d'attaque maximale donnée, l'attaquant cherche à **minimiser la performance** (i.e. minimiser la capacité ou maximiser la probabilité d'erreur)

On résout ce type de compromis par une formulation Lagrangienne :

$$\mathbf{z}^\star = \arg_{\mathbf{z}} \min \{\mathrm{SNR}(\mathbf{a}, \mathbf{z}) + \lambda \mathrm{D}_{\mathbf{yr}}\}$$

Stratégie de défense

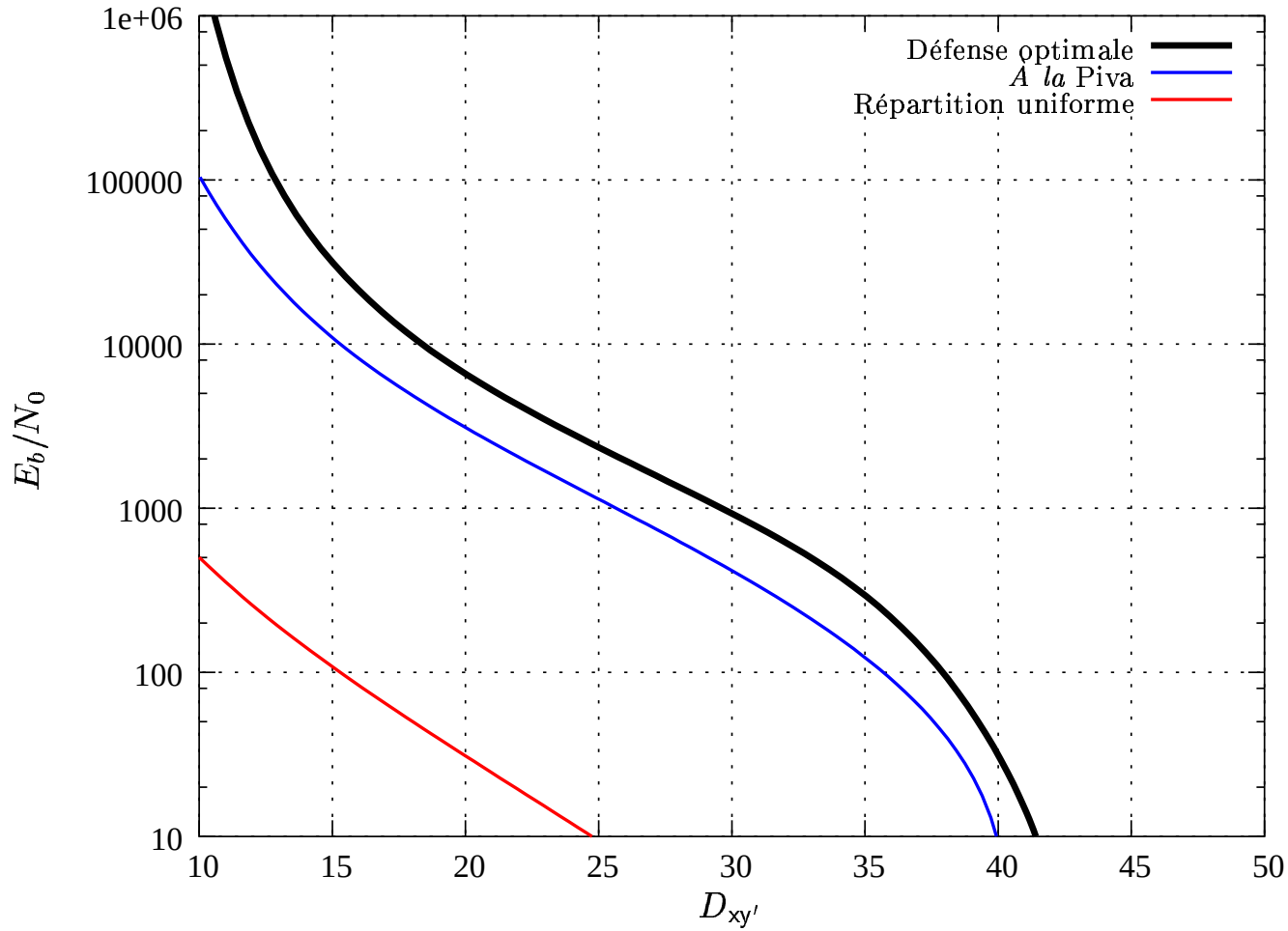
A contrario, le défenseur (qui insère la marque) souhaite **maximiser la performance** pour une distorsion d'insertion maximale donnée

Il doit prendre en compte la meilleure attaque possible, et y répondre par la meilleure défense :

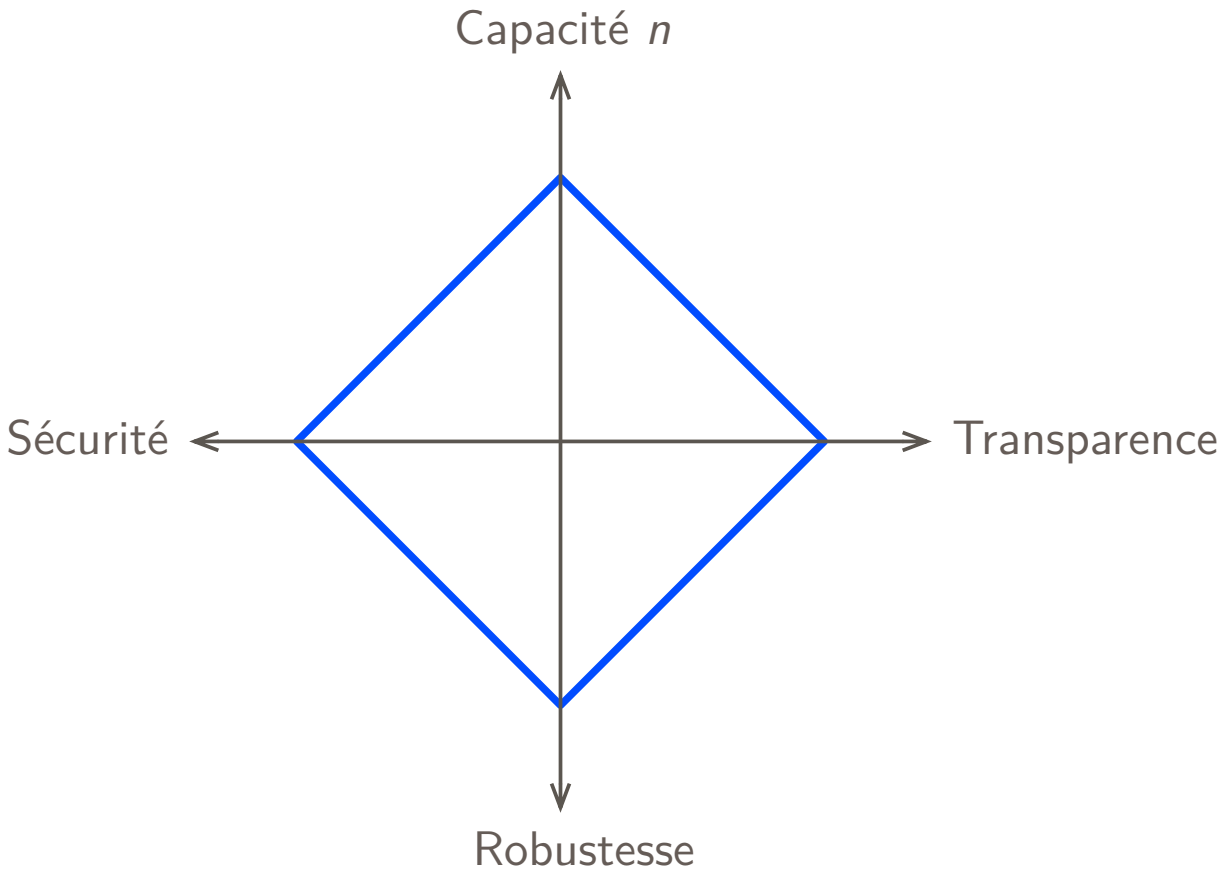
$$\mathbf{a}^\star = \arg_{\mathbf{a}} \max \{\mathrm{SNR}(\mathbf{a}, \mathbf{z}^\star) - \chi \mathrm{D}_{\mathbf{xy}}\}$$

On remarque une **stratégie de type min-max**, classique dans la théorie des jeux : elle assure un niveau de performance minimale
Les deux lagrangiens servent à ajuster les distorsions visées

Résultats


1e+06
100000
10000
1000
100
10
E_b/N_0
10
15
20
25
30
35
40
45
50
$D_{xy'}$
Défense optimale
A la Piva
Répartition uniforme

Nouveau compromis



Qu'est-ce que la sécurité ?

Définition ? pas simple, car souvent sécurité et robustesse sont très proches.

Robustesse	**Sécurité**
attaques non malicieuses	attaques intentionnelles
traitements usuels	attaques dédiées
une étape	plusieurs étapes itératives

Dissimulation d'information et sécurité

Principe de Kerckhoffs.

Steganographie : estimation de l'indétectabilité, avec des outils théoriques ou heuristiques ; depuis le début Cachin [98], Zollner [98], Mittelholzer [99], ...

Tatouage : estimation de la marque (e.g. attaque par oracle Cox [97], Linnartz [98], Kalker [98], ..., Comesana [06] , estimation des clefs Cayre [04,05], Pérez-Freire [06,07], ..., Bas [13,16] .

Sécurité vs. robustesse

La robustesse est la capacité à résister aux dégradations ou tentatives de suppression de la marque.

$\Rightarrow$ flou, compression, transformations géométriques, ...

La sécurité est la capacité à résister à l'estimation de la clef ou du message.

$\Rightarrow$ cryptanalyse

Méthodologie

N_o images : messages différents, mais clef secrète identique.

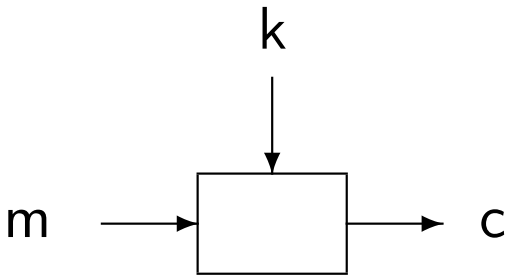
Nous suivons la méthodologie de Shannon [Sha49] :

- Possibilités théoriques ?
- Quels outils pour la mise en practique ?

et la classification de Diffie-Hellman [DH76] :

- Known Original Attack – KOA
- Known Messages Attack – KMA
- Watermark Only Attack – WOA

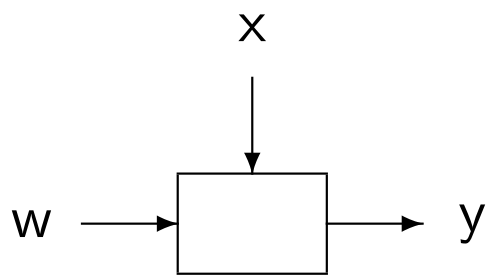
Perfect covering



chiffrement

m clair, k clef,

c chiffré



tatouage

w marque, x document hôte,

y document tatoué

Une technique de tatouage est perfect covering si

$$\mathbb{P}_W(w) = \mathbb{P}_W(w|y) \quad \forall (y, w) \in \mathcal{Y} \times \mathcal{W}$$

Fuite d'information Shannon [49]

Entropie : $H(\mathrm{K}) = -\sum_{\mathbf{k}} \mathbb{P}(\mathbf{k}) \log \mathbb{P}(\mathbf{k})$
Équivocation : $H(\mathrm{K}|\mathrm{Y}_1, \ldots, \mathrm{Y}_{N_o}) = H(\mathrm{K}) - I(\mathrm{K}; \mathrm{Y}_1, \ldots, \mathrm{Y}_{N_o})$

Les deux mesurent l'ignorance de la clef secrète.

L'équivocation est une fonctions non croissante, allant de $H(\mathrm{K})$ à 0 quand N_o croit.

La plus petite valeur de N_o donnant une équivocation nulle est notée $N_o{}^\star$, et est appelée la distance d'unicité. Elle correspond à un niveau de sécurité. Un schéma *perfect covering* correspond à $N_o{}^\star = +\infty$.

Tatouage substitutif e.g. Koch [95]

x, y : vecteurs binaires de dimension m
k : suite de n entiers, $1 \leq \mathbf{k}[j] \leq m$
m : vecteur binaire de dimension n

$$\begin{aligned} \mathbf{y}[i] &\leftarrow \mathbf{x}[i] \quad \forall\ 1 \leq i \leq m \\ \mathbf{y}[\mathbf{k}[j]] &\leftarrow \mathbf{m}[j] \quad \forall\ 1 \leq j \leq n \end{aligned}$$

$$\begin{aligned} \mathrm{m} &= (1101) & \mathrm{k} &= [2, 8, 5, 3] \\ \mathrm{x} &= (01001011) & \mathrm{y} &= (01100011) \end{aligned}$$

Tatouage substitutif e.g. Koch [95]

x, y : vecteurs binaires de dimension m
k : suite de n entiers, $1 \leq \mathbf{k}[j] \leq m$
m : vecteur binaire de dimension n

$$\begin{aligned} \mathbf{y}[i] &\leftarrow \mathbf{x}[i] \quad \forall\ 1 \leq i \leq m \\ \mathbf{y}[\mathbf{k}[j]] &\leftarrow \mathbf{m}[j] \quad \forall\ 1 \leq j \leq n \end{aligned}$$

$$\begin{aligned} \mathrm{m} &= (1101) & \mathrm{k} &= [2,8,5,3] \\ \mathrm{x} &= (01001011) & \mathrm{y} &= (01100011) \end{aligned}$$

Tatouage substitutif e.g. Koch [95]

x, y : vecteurs binaires de dimension m
k : suite de n entiers, $1 \leq \mathbf{k}[j] \leq m$
m : vecteur binaire de dimension n

$$\begin{aligned} \mathbf{y}[i] &\leftarrow \mathbf{x}[i] \quad \forall\ 1 \leq i \leq m \\ \mathbf{y}[\mathbf{k}[j]] &\leftarrow \mathbf{m}[j] \quad \forall\ 1 \leq j \leq n \end{aligned}$$

$$\begin{aligned} \mathrm{m} &= (1101) & \mathrm{k} &= [2, 8, 5, 3] \\ \mathrm{x} &= (01001011) & \mathrm{y} &= (01100011) \end{aligned}$$

Tatouage substitutif e.g. Koch [95]

x, y : vecteurs binaires de dimension m
k : suite de n entiers, $1 \leq \mathbf{k}[j] \leq m$
m : vecteur binaire de dimension n

$$\begin{aligned} \mathbf{y}[i] &\leftarrow \mathbf{x}[i] \quad \forall\ 1 \leq i \leq m \\ \mathbf{y}[\mathbf{k}[j]] &\leftarrow \mathbf{m}[j] \quad \forall\ 1 \leq j \leq n \end{aligned}$$

$$\begin{aligned} \mathrm{m} &= (1101) & \mathrm{k} &= [2,8,5,3] \\ \mathrm{x} &= (01001011) & \mathrm{y} &= (01100011) \end{aligned}$$

Tatouage substitutif e.g. Koch [95]

x, y : vecteurs binaires de dimension m
k : suite de n entiers, $1 \leq \mathbf{k}[j] \leq m$
m : vecteur binaire de dimension n

$$\begin{aligned} \mathbf{y}[i] &\leftarrow \mathbf{x}[i] \quad \forall\ 1 \leq i \leq m \\ \mathbf{y}[\mathbf{k}[j]] &\leftarrow \mathbf{m}[j] \quad \forall\ 1 \leq j \leq n \end{aligned}$$

$$\begin{aligned} \mathrm{m} &= (1101) & \mathrm{k} &= [2,8,5,3] \\ \mathrm{x} &= (01001011) & \mathrm{y} &= (01100011) \end{aligned}$$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]

WOA : $N_o^\star = +\infty$, perfect covering

KMA : $N_o^\star = \log_2 m$

$\mathbf{m}_1 = (1101)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{m}_2 = (1011)$ $\quad$ $\mathbf{y}_2 = (11101000)$

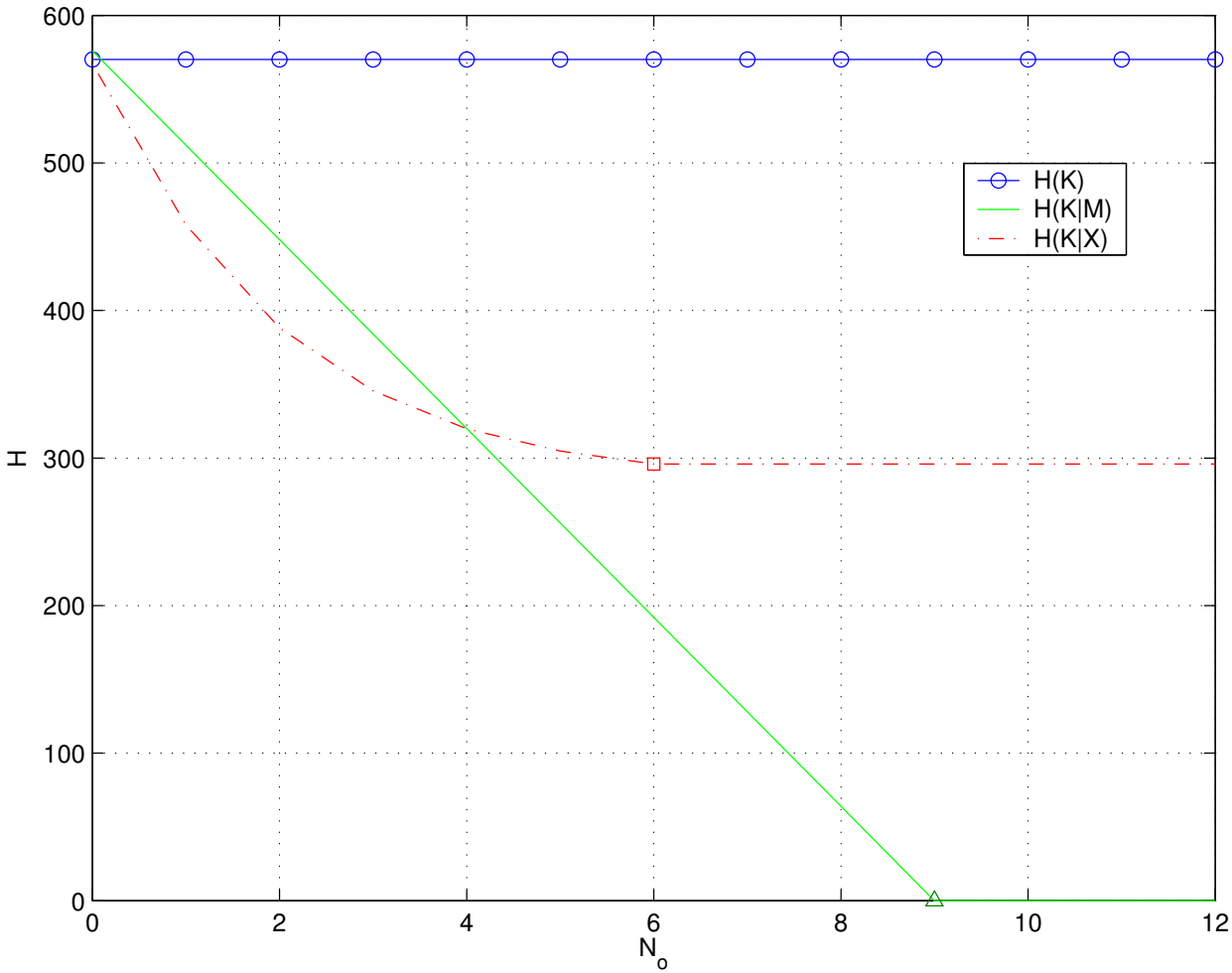
$\mathbf{m}_3 = (1000)$ $\quad$ $\mathbf{y}_3 = (11010010)$

KOA : $N_o^\star = \log_2 n$ (up to permutation of the indices)

$\mathbf{x}_1 = (01001011)$ $\quad$ $\mathbf{y}_1 = (01100011)$

$\mathbf{x}_2 = (10001001)$ $\quad$ $\mathbf{y}_2 = (11101000)$

Tatouage substitutif e.g. Koch [95]



Étalement de spectre

$$y = x + w, \qquad \text{avec } w = \alpha \sum_{j=1}^{n} \mathbf{m}[j] \times \mathbf{G}[j]$$

modulation de n porteuses privées $\mathbf{G}[j]$, $\|\mathbf{G}[j]\| = 1$;
$\alpha > 0$ règle la force du tatouage.

Les porteuses sont des vecteurs orthogonaux 2 à 2. Les symboles du message appartiennent à $\{-1, +1\}$ Pateux [03] .

Étalement de spectre

Premier résultat : pas de *perfect covering* !

Quelle est la fuite d'information ?

Comment mesurer la fuite ?

Problème : Les outils de Shannon ne sont pas adaptés aux valeurs réelles. L'information mutuelle est toujours valable, mais l'entropie n'a plus d'interprétation physique.

Les outils de Fisher sont plus adaptés.

Comment mesurer la fuite ?

Principe : estimation d'un paramètre inconnu (ici, la clef secrète).

Matrice d'information de Fisher :

$$\mathrm{FIM}(\theta) = E\psi\psi^{\mathsf{T}} \quad \text{avec} \quad \psi = \nabla_\theta \log \mathbb{P}_{\mathsf{X}}(\mathsf{y} - \mathsf{w}_\theta).$$

Le théorème de Cramér-Rao donne une borne inférieure sur les covariances relatives aux estimations conjointes des différents paramètres à partir des observations la matrice de covariance, quand la matrice de Fischer est inversible :

$$\mathcal{R}_{\hat{\theta}} \geq \mathrm{FIM}(\theta)^{-1},$$

Niveaux de sécurité théoriques

$\mathsf{X} \sim \mathcal{N}(0, \sigma_x^2 \mathcal{I}_m)$

KOA : $N_o^\star = \mathcal{O}(n)$, aux signes et permutations près

KMA : $N_o^\star = \mathcal{O}\left(\sigma_x^2/\alpha^2\right)$

WOA : $N_o^\star = \mathcal{O}\left(\sigma_x^2/\alpha^2\right)$, aux signes et permutations près

Et en pratique ?

Nous sommes en fade d'un problème de séparation de sources :

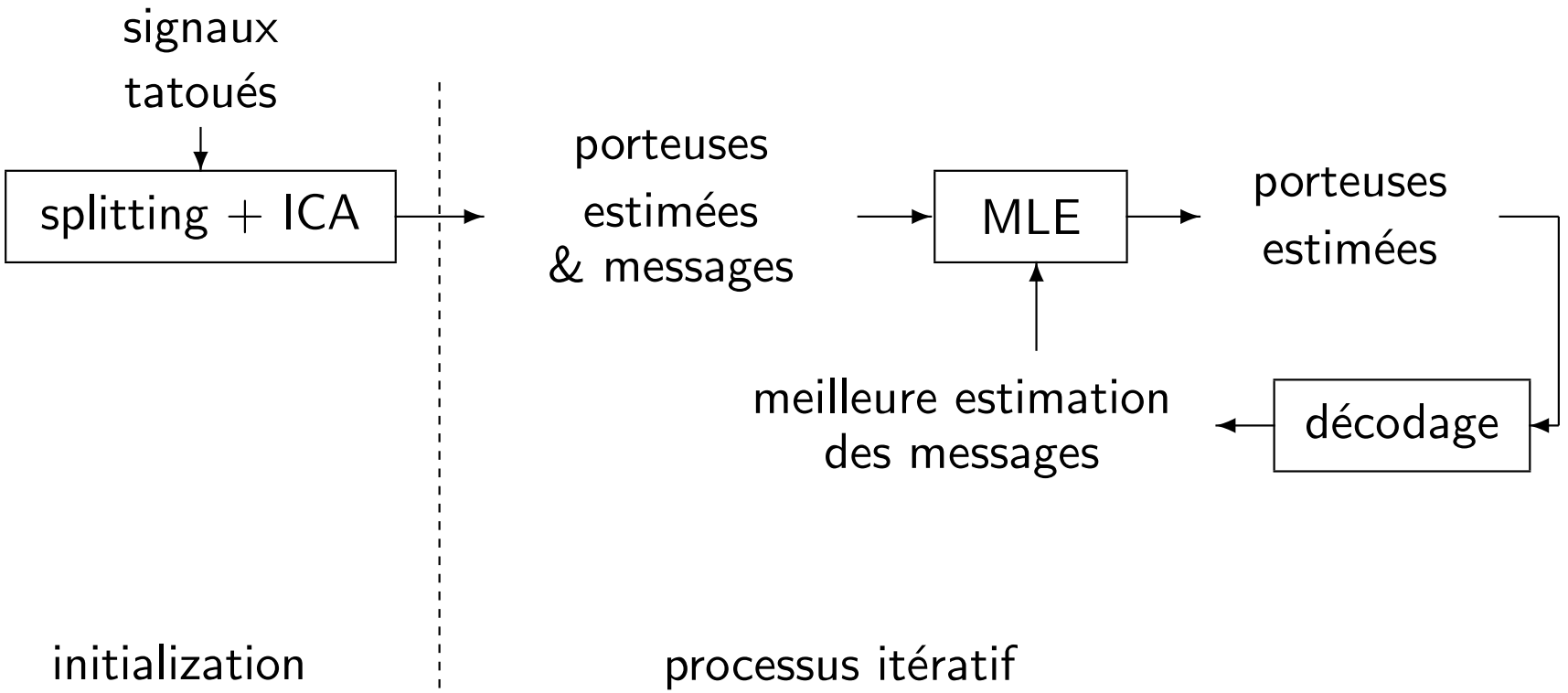
$$\mathrm{w} = \alpha \sum_{\mathrm{J}=1}^{n} \mathbf{m}[j] \times \mathbf{G}[j] \ (+ \text{ bruit})$$

KOA = pas de bruit, plus simple : une ICA donne une estimation correcte de $\mathbf{G}$, aux signes et permutations près ; $N_o > n$ observations.

WOA = avec bruit, plus complexe (voir slide suivant).

KMA = le plus facile : la MLE converge vers la borne de Cramér-Rao bound. Complexity = $\mathcal{O}(mn \times {N_o}^2) + \mathcal{O}(n^3)$.

Stratégie hybride pour le cas WOA

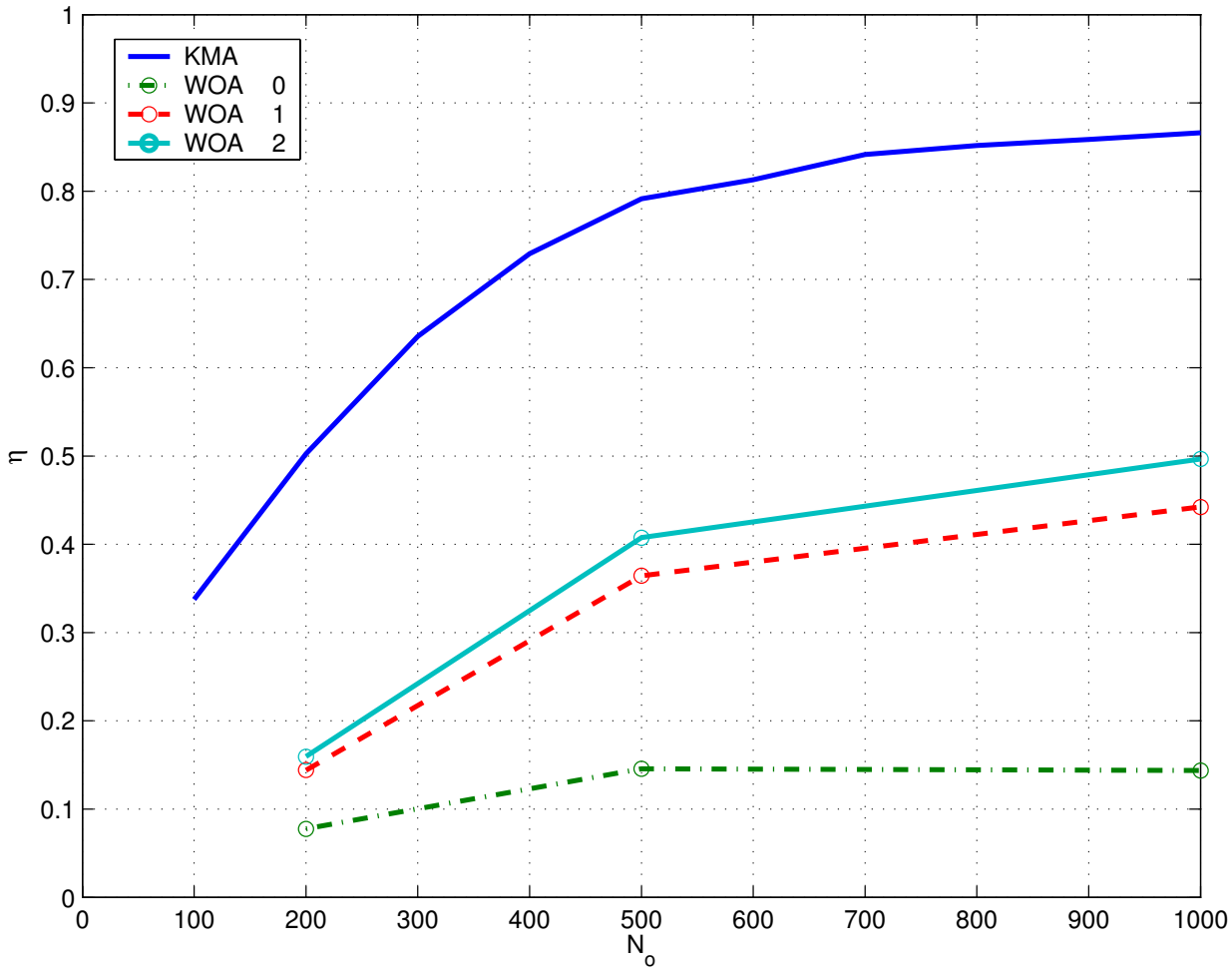


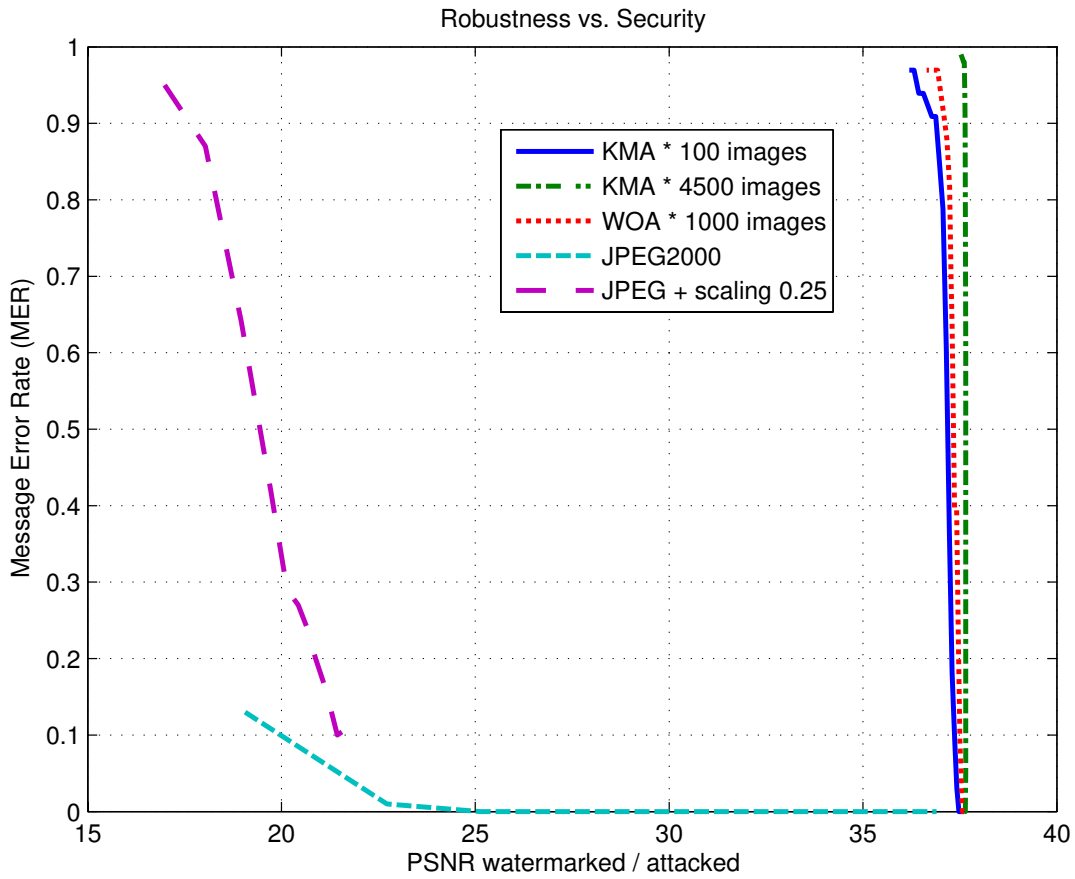
Application aux images

Insertion : tatouage proportionnel des coefficients ondelettes Pateux [03] .

Qualité : 38 dB.

Paramètres : $m = 258058, n = 8$


KMA
WOA 0
WOA 1
WOA 2
η
N_o
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
100
200
300
400
500
600
700
800
900
1000


Robustness vs. Security
Message Error Rate (MER)
PSNR watermarked / attacked
KMA * 100 images
KMA * 4500 images
WOA * 1000 images
JPEG2000
JPEG + scaling 0.25
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
15
20
25
30
35
40

(a) Meilleure qualité obtenue avec une attaque aveugle : PSNR=21,8 dB

(b) Meilleure qualité obtenue avec cryptanalyse : PSNR=35,8 dB

Conclusion

Première étude de cryptanalyse en tatouage Cayre [04,05]

Cela a conduit à de nouvelles recommandations :

- En pratique, il est plutôt simple de retrouver assez d'informations pour lancer une attaque efficace, en observant un nombre suffisant de documents tatoués
- Les clefs doivent être renouvelées souvent !

La menace de ce type d'attaque est réelle (d'autant plus en vidéo). Elle doit être prise en compte dans le design de systèmes de protection.

Liens entre tatouage et cryptographie

- gestion de clefs
- symétrique/asymétrique Van Schnydel [99], Eggers [99,00], Smith [99], Sylvestre [01], Stern [01], Furon [99,01,03],...
- authentification Craver [99], Lévy-dit-Véhel[04]
- intégrité, tatouage (semi-)fragile, robust hash Lefèbvre [04]
- cryptanalyse Cayre [04,05](SS), Peréz-Freire [06,07](QIM,lattices), Bas [13,16]
- tatouage-chiffrement joints Puech [04]
- traitement dans le domaine chiffré Kalker [06], He [16]

Liens entre tatouage et cryptographie

- gestion de clefs
- symétrique/asymétrique Van Schnydel [99], Eggers [99,00], Smith [99], Sylvestre [01], Stern [01], Furon [99,01,03],...
- authentification Craver [99], Lévy-dit-Véhel[04]
- intégrité, tatouage (semi-)fragile, robust hash Lefèbvre [04]
- cryptanalyse Cayre [04,05](SS), Peréz-Freire [06,07](QIM,lattices), Bas [13,16]
- tatouage-chiffrement joints Puech [04]
- traitement dans le domaine chiffré Kalker [06], He [16]

Mais le tatouage n'est pas de la cryptographie ! Cox [06]

Espace des clefs

1. Considérons une schéma de chiffrement à clef symétrique qui utilise une clef secrète **k** de longueur n.

Espace des clefs

1. Considérons une schéma de chiffrement à clef symétrique qui utilise une clef secrète **k** de longueur n.

$$\begin{aligned} \#\mathcal{K} &= 2^n \\ \text{P(déchiffrer avec une clef au hasard)} &= 2^{-n} \end{aligned}$$

Espace des clefs

1. Considérons une schéma de chiffrement à clef symétrique qui utilise une clef secrète **k** de longueur n.

$$\begin{aligned} \#\mathcal{K} &= 2^n \\ \text{P(déchiffrer avec une clef au hasard)} &= 2^{-n} \end{aligned}$$

2. Considérons maintenant un tatouage symétrique de type WSS avec une clef secrète **k** de longueur n.

Espace des clefs

1. Considérons une schéma de chiffrement à clef symétrique qui utilise une clef secrète **k** de longueur n.

$$\begin{aligned} \#\mathcal{K} &= 2^n \\ \text{P(déchiffrer avec une clef au hasard)} &= 2^{-n} \end{aligned}$$

2. Considérons maintenant un tatouage symétrique de type WSS avec une clef secrète **k** de longueur n.

$$\begin{aligned} \#\mathcal{K} &\neq 2^n \\ \text{P(attaquer avec une clef au hasard)} &\neq 2^{-n} \end{aligned}$$

Analyse

Une clef génère un ensemble de porteuses, i.e. des séquences binaires. Souvent, les porteuses identifient la clef. Notons n la longueur de la secret sequence au complet.

Analyse

Une clef génère un ensemble de porteuses, i.e. des séquences binaires. Souvent, les porteuses identifient la clef. Notons n la longueur de la secret sequence au complet.

Toutes les séquences possibles ne sont pas adaptées pour un bon tatouage !

$$\#\{\text{séquences éligibles de longueur } n\} = 2^{n-\frac{1}{2}\log_2 n}$$

Analyse

Une attaque peut être réussie même si la séquence estimée n'est pas exactement la même que la séquence secrète ! Une corrélation of $\rho_{\text{min}} = 0.4$ suffit.

Si au moins

$$k_{\text{min}} = \lceil \frac{n(\rho_{\text{min}} + 1)}{2} \rceil$$

éléments de la porteuse estimée correspondent, l'attaque sera probante.

$$\text{P(attaquer avec une clef au hasard)}$$

$$= \sum_{k_{\text{min}} \leq k \text{ pair } \leq n} \frac{\binom{n/2}{k/2}^2}{\binom{n}{n/2}} \simeq 2^{-0.12n}$$

Analogie avec les clefs publiques

Clef publique en cryptographie : initialise une communication sécurisée sans avoir à partager un secret, ou pour permettre à quiconque de vérifier une signature sans être capable d'en forger une.

Clef publique en tatouage : pour permettre à quiconque de vérifier/lire une marque sans être capable de la supprimer.

Analogie avec les clefs publiques

Clef publique en cryptographie : initialise une communication sécurisée sans avoir à partager un secret, ou pour permettre à quiconque de vérifier une signature sans être capable d'en forger une.

Clef publique en tatouage : pour permettre à quiconque de vérifier/lire une marque sans être capable de la supprimer.

[Spoiler] C'est impossible.