Présentation ICAR

Intégration de codes anti-collusion dans le tatouage de seconde génération

Mathieu Desoubeaux
Orange Labs Cesson-Sévigné, LIRMM Montpellier
Le 10/12/2010

Sommaire

- Introduction
- Codes anti-collusion
- Travaux réalisés
- Travaux futurs

Introduction

- Contexte
  - Distribution légale de contenus vidéo
    - VOD, Blu-ray, Live Broadcasting
    - DRM, CAS : utilisation de la cryptographie
    - Distribution de clés, vérification de droits

Introduction

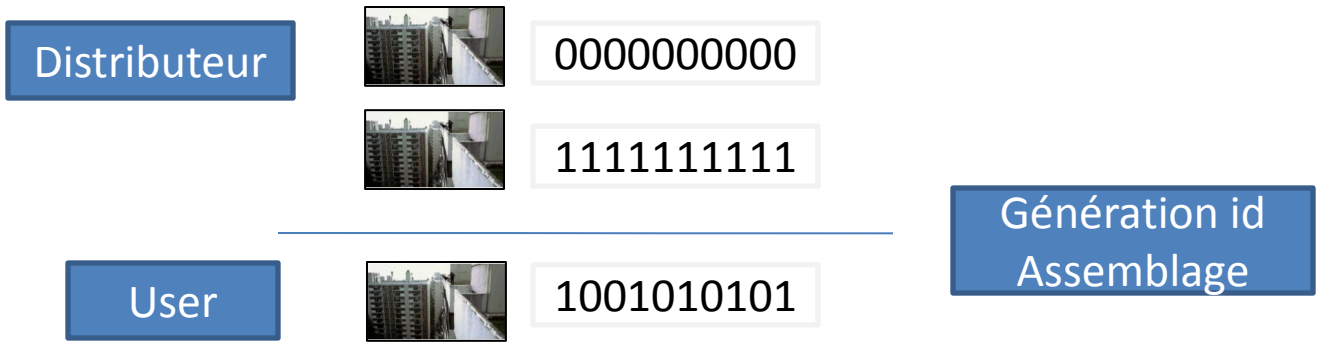
- Contexte
  - Distribution légale de contenus vidéo
    - VOD, Blu-ray, Live Broadcasting
    - DRM, CAS : utilisation de la cryptographie
    - Distribution de clés, vérification de droits
  - Points faibles
    - Le secret est donné à l'utilisateur
    - Possibilité d'attaques (reverse engineering, memory dumping)

Introduction

- Tatouage transactionnel
  - Insertion d’un identifiant dans les copies distribuées aux utilisateurs (découpage en blocs et aiguillage côté serveur)

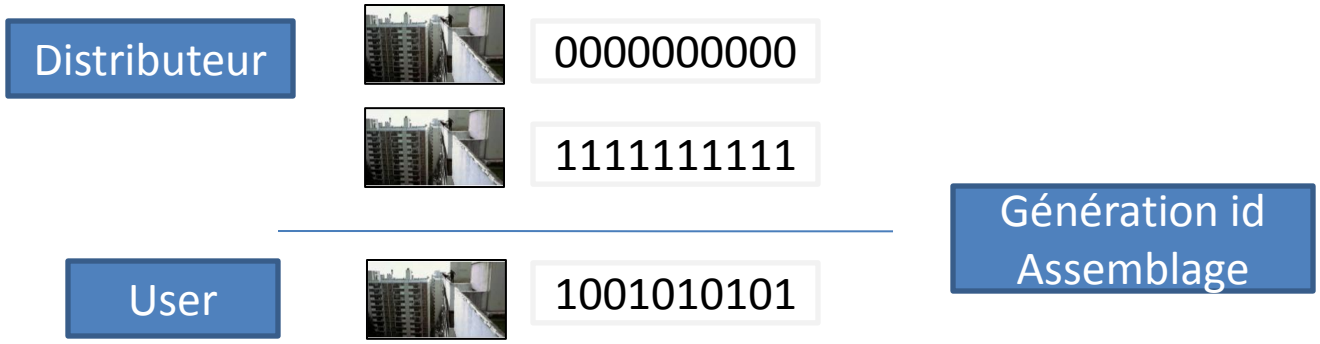
Introduction

- Tatouage transactionnel
  - Insertion d'un identifiant dans les copies distribuées aux utilisateurs (découpage en blocs et aiguillage côté serveur)



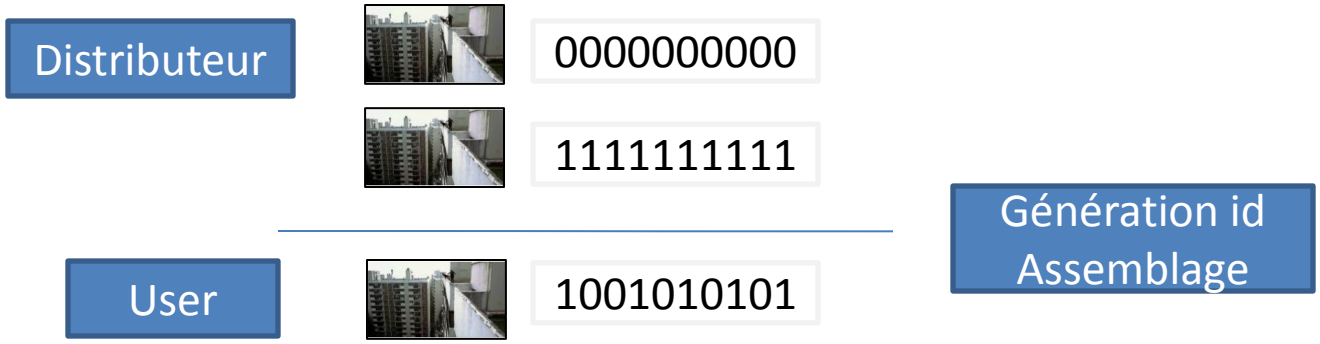
Introduction

- Tatouage transactionnel
  - Insertion d'un identifiant dans les copies distribuées aux utilisateurs (découpage en blocs et aiguillage côté serveur)
  - Répressif et Dissuasif

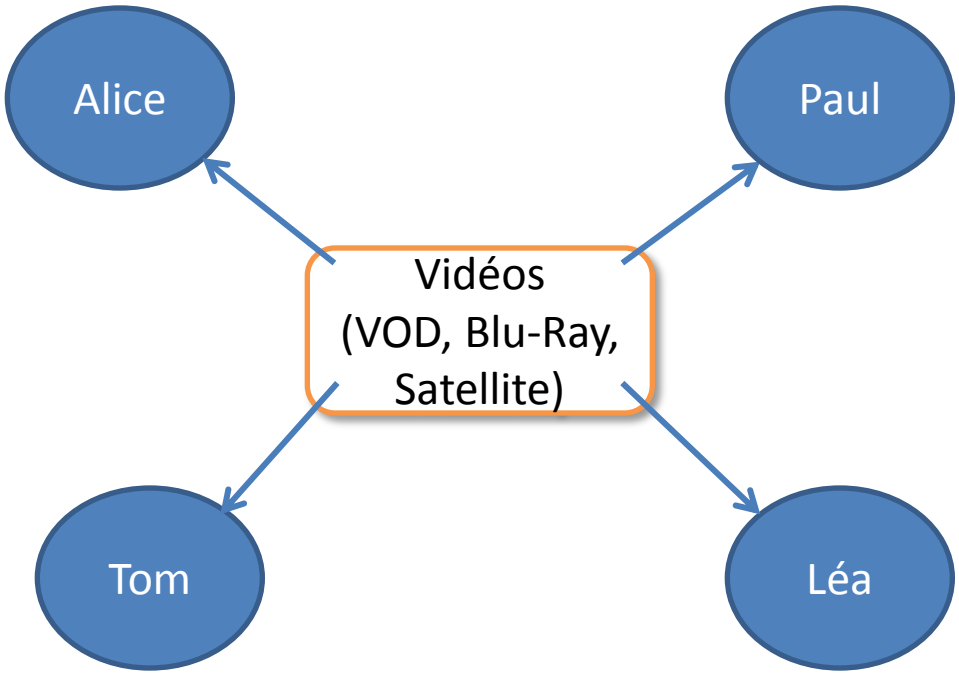


Introduction

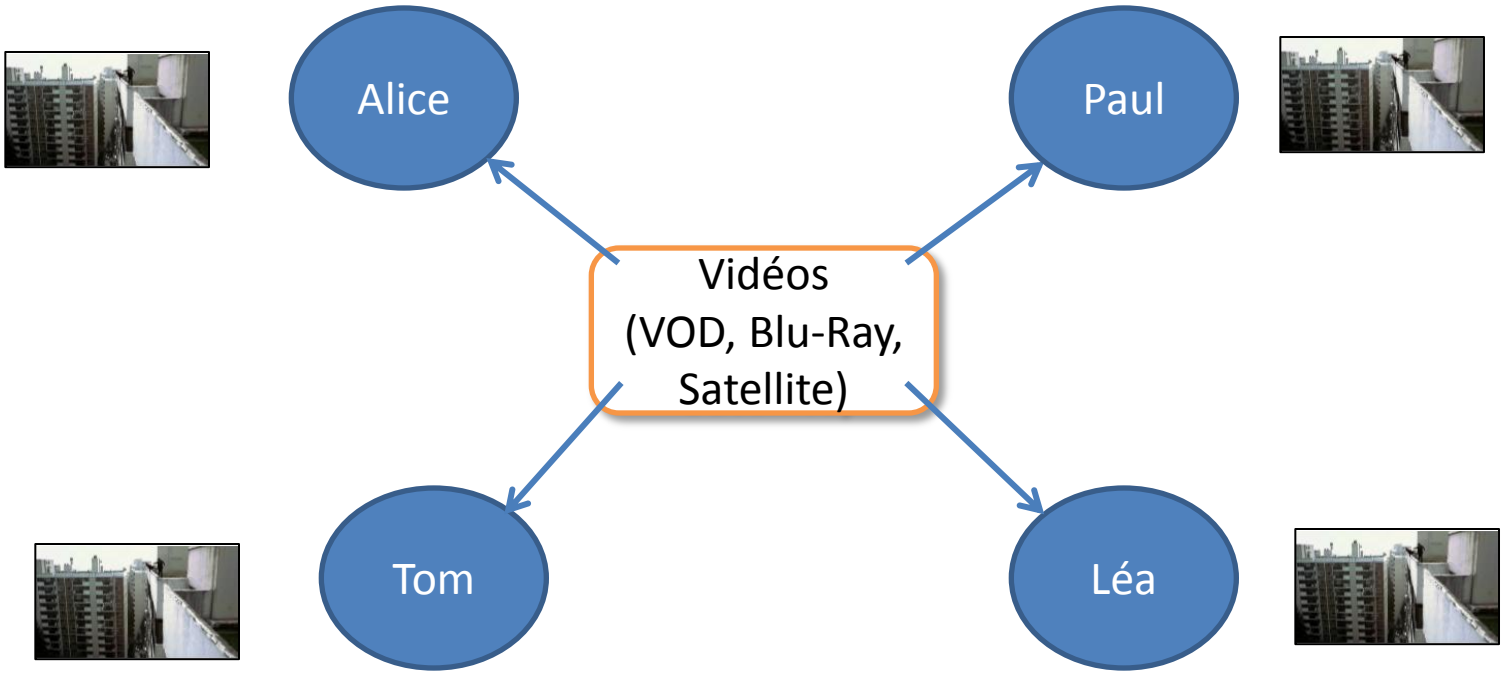
- Tatouage transactionnel
  - Insertion d'un identifiant dans les copies distribuées aux utilisateurs (découpage en blocs et aiguillage côté serveur)
  - Répressif et Dissuasif
  - Simplicité pour l'utilisateur



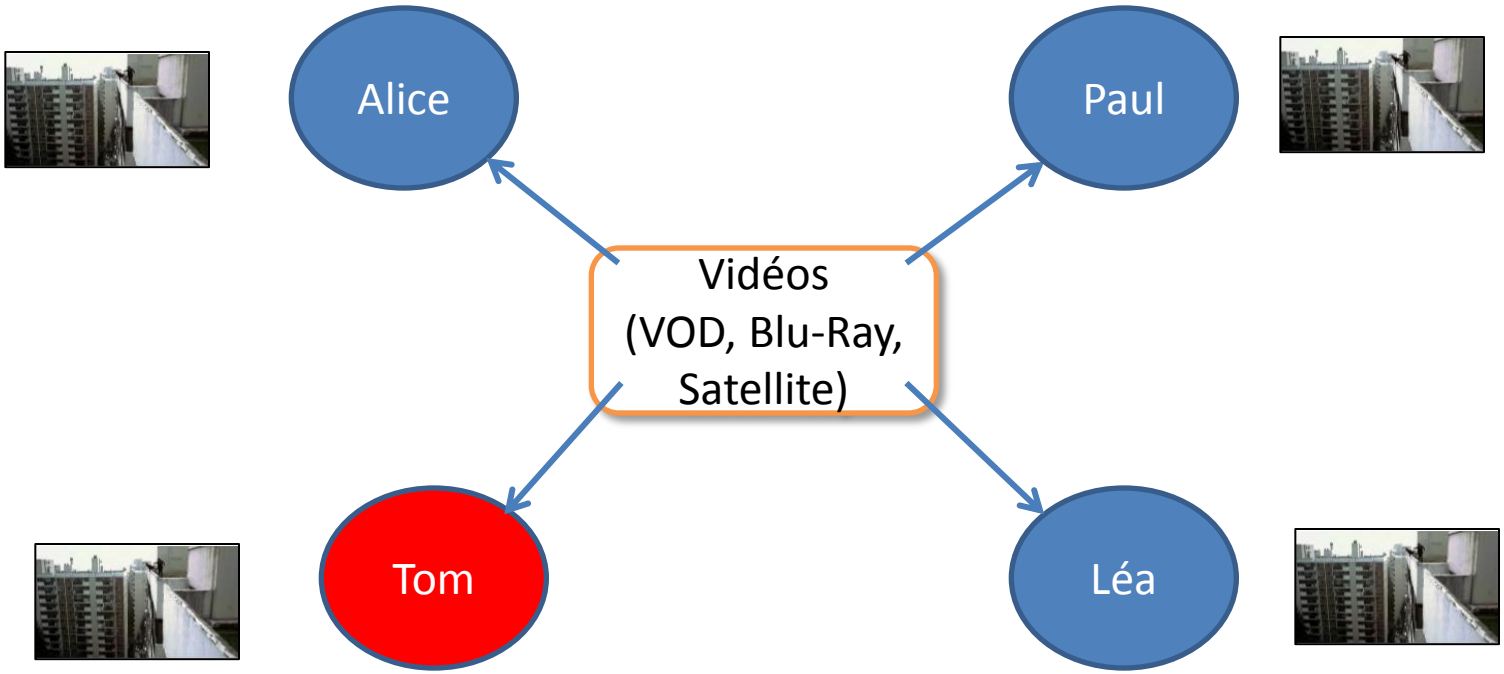
Scénario



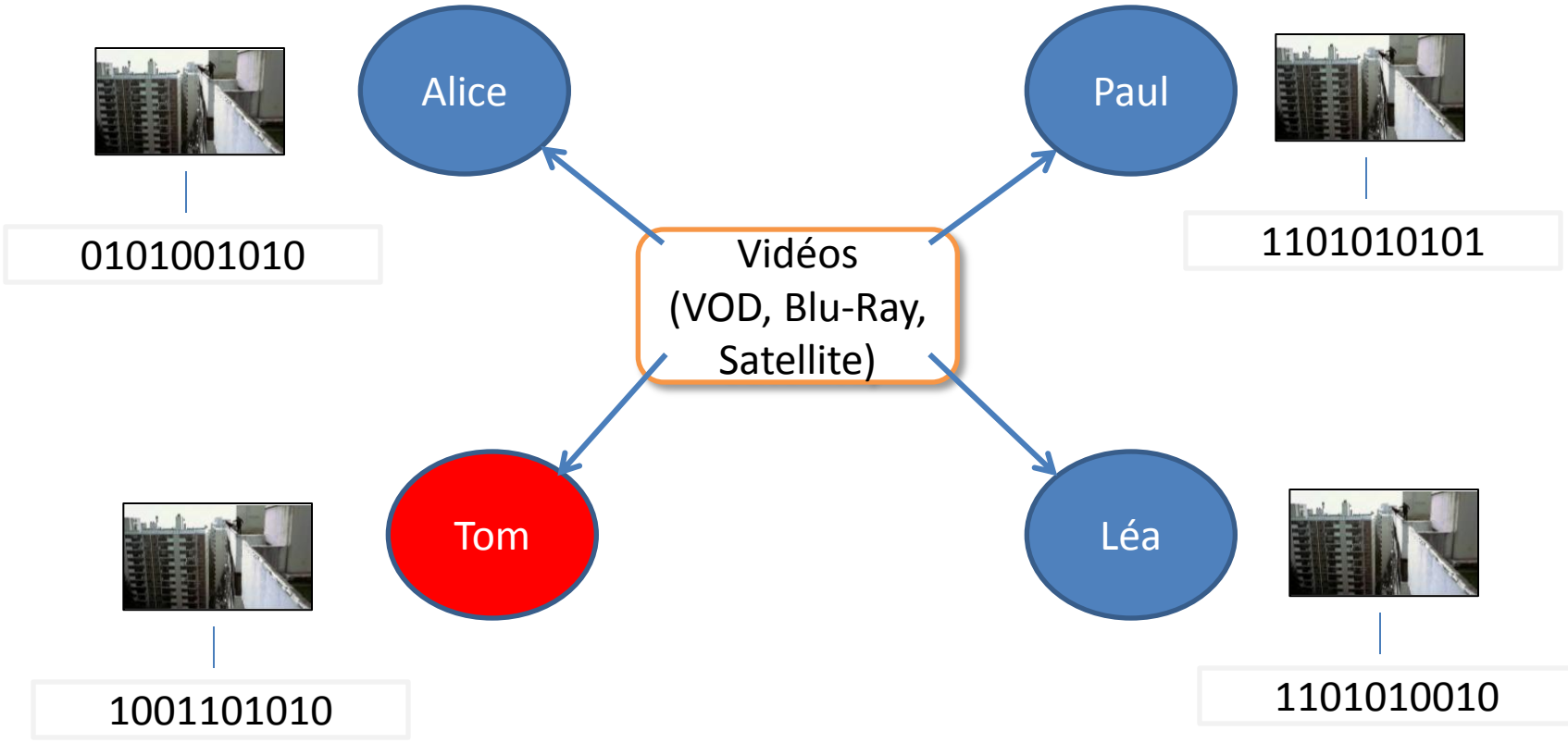
Scénario



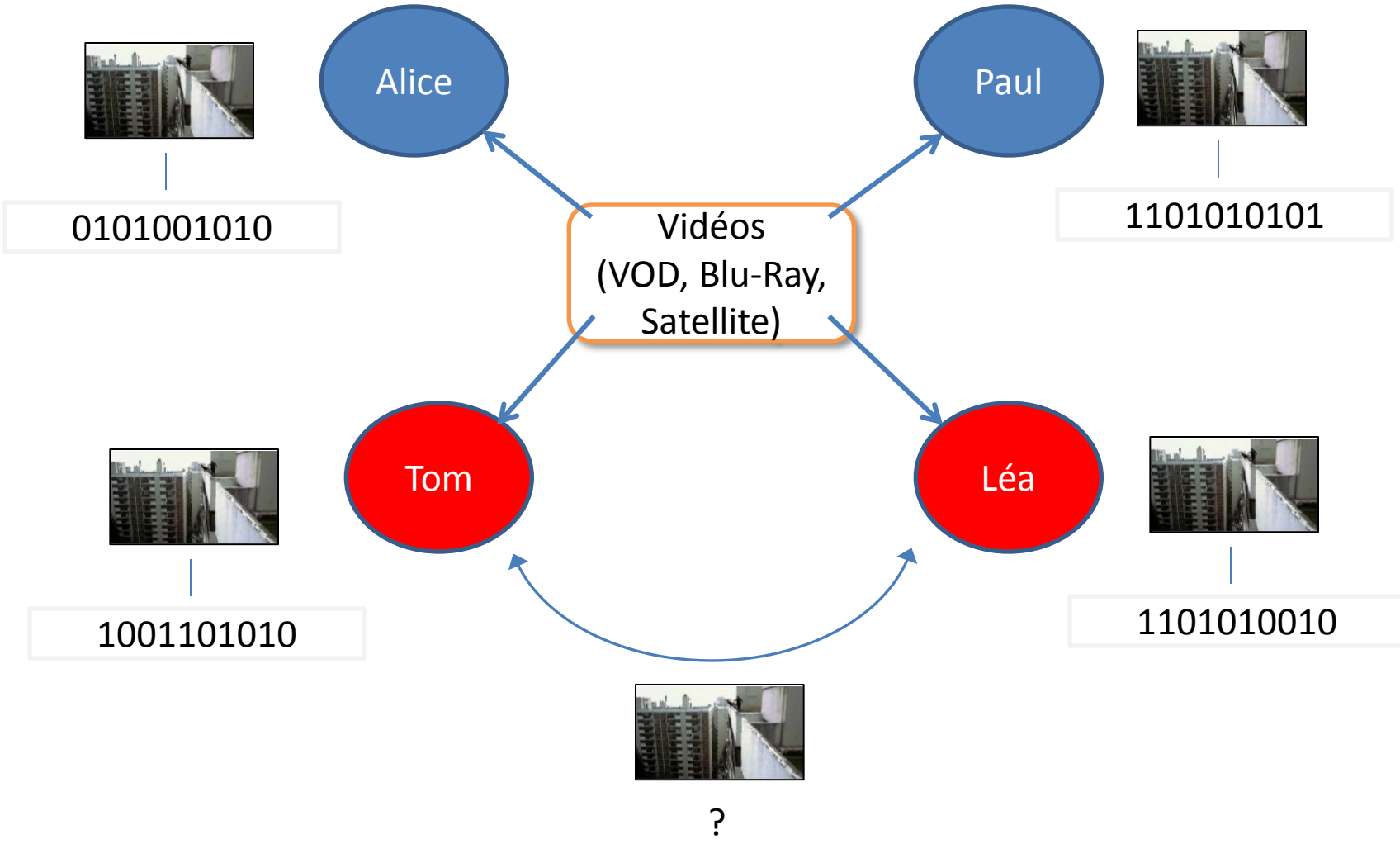
Scénario



Scénario


Alice
Paul
Vidéos
(VOD, Blu-Ray,
Satellite)
Tom
Léa
0101001010
1101010101
1001101010
1101010010

Scénario


Alice
Paul
Vidéos
(VOD, Blu-Ray,
Satellite)
Tom
Léa
0101001010
1101010101
1001101010
1101010010
?

Traçage de traitres

(Fingerprinting, user forensics, serialization, transactional watermarking…)

- Retrouver les sources d'une fuite
  - Début XXe s : valeurs des tables de log
  - 1980 : Les espaces de Ms. Thatcher
  - Bientôt avec Hadopi (chipset Mstar with civolution)

Traçage de traitres

(Fingerprinting, user forensics, serialization, transactional watermarking…)

- Retrouver les sources d'une fuite
  - Début XXe s : valeurs des tables de log
  - 1980 : Les espaces de Ms. Thatcher
  - Bientôt avec Hadopi (chipset Mstar with civolution)
- Le traçage de traitres s'appuie sur :
  - Un code anti-collusion, matrice n × m, qui associe à chaque utilisateur un identifiant de longueur m
  - Une technique d'insertion par tatouage pour cacher l'identifiant dans le document

Les attaques

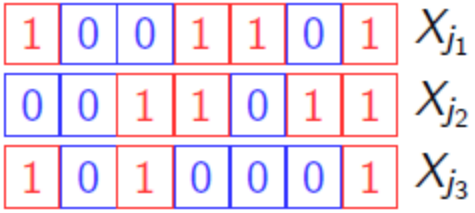
- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »

Les attaques

- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?

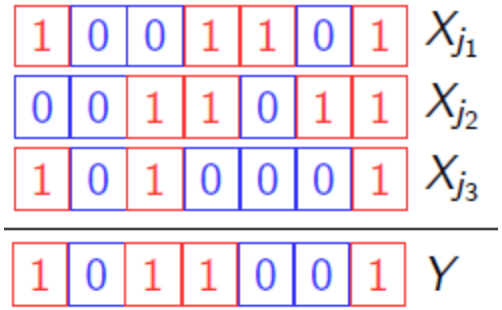
Les attaques

- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



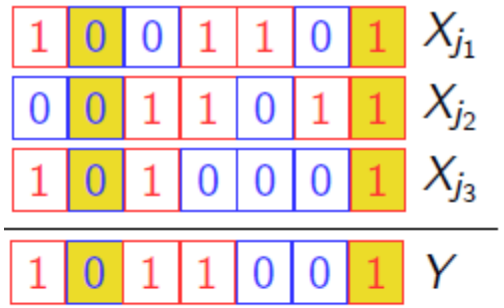
Les attaques

- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



Les attaques

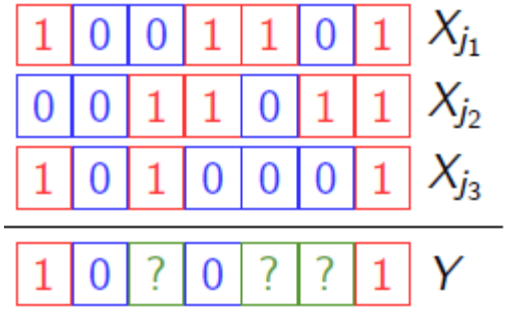
- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



- Marking assumption Xj1i = . . . = Xjc = a ⇒ Yi = a.

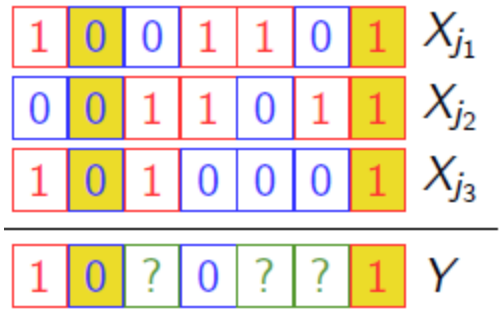
Les attaques

- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



Les attaques

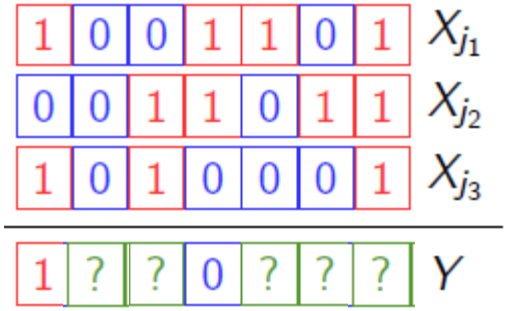
- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



Marking assumption Xj1i = . . . = Xjc = a ⇒ Yi = a.

Les attaques

- La collusion
  - « Entente secrète entre deux ou plusieurs personnes pour nuire à un tiers »
  - Attaques seulement théoriques, pourquoi s'y intéresser?
  - Echange de blocs, effacement, fusion.



Etat de l’art

- Codes anti-collusion
  - Traçabilité forte
    - ECC, longueur de codes trop long.

Etat de l’art

- Codes anti-collusion
  - Traçabilité forte
    - ECC, longueur de codes trop long.
  - Traçabilité faible
    - On accepte de commettre des erreurs.
    - Gabor Tardos (2003-2010).

Code de Tardos

- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.

Code de Tardos

- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.

	Indice 1	Indice 2	Indice 3	Indice 4	Indice 5	Somme
Suspect 1	+1	-1	+1	+1	+1	+3
Suspect 2	+1	+1	-1	-1	+1	+1
Suspect 3	-1	- 1	+1	-1	+1	- 1
Suspect 4	-1	-1	-1	+ 1	-1	-3

Code de Tardos

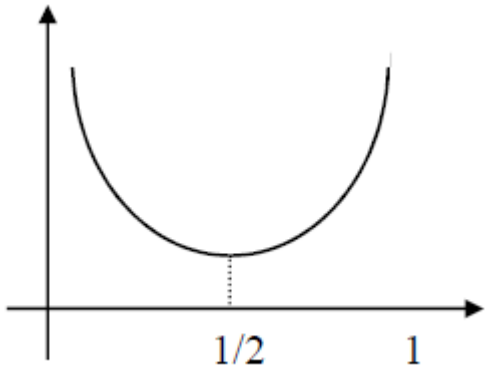
- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.

	$Y_1 = 1$	$Y_2 = 0$	$Y_3 = 0$	$Y_4 = 1$	$Y_5 = 1$	Somme
Suspect 1	+1	-1	+1	+1	+1	+3
Suspect 2	+1	+1	-1	-1	+1	+1
Suspect 3	-1	- 1	+1	-1	+1	- 1
Suspect 4	-1	-1	-1	+ 1	-1	-3

Code de Tardos

- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.
- La distribution des indices.

$$\text{Prob}(X_{ji} = 1) = p_i$$



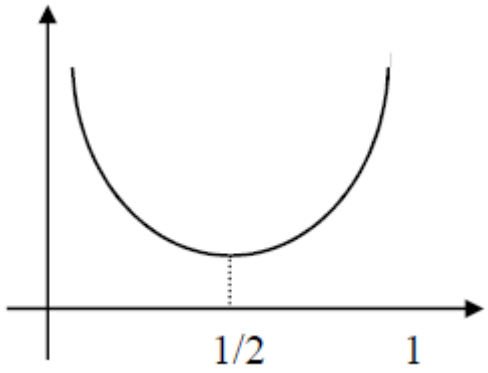
Code de Tardos

- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.
- La distribution des indices.

$$\text{Prob}(X_{ji} = 1) = p_i$$

- Taille du code (Tardos 2003)

$$m = 100c^2 \left\lceil \ln\left(\frac{1}{\varepsilon_1}\right) \right\rceil$$



Code de Tardos

- Intuitivement (jeu du Cluedo)
  - Qui a tué le docteur Lenoir ?
  - Mais il y a plusieurs coupables.
- La distribution des indices.

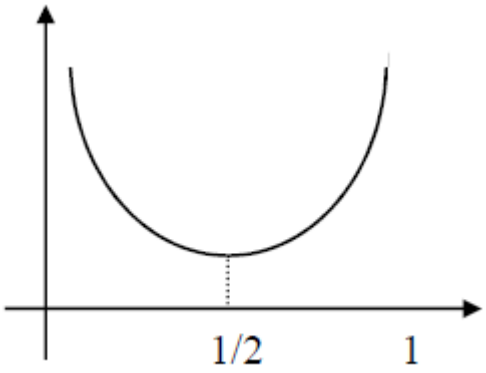
$$\text{Prob}(X_{ji} = 1) = p_i$$

- Taille du code (Tardos 2003)

$$m = 100c^2 \left\lceil \ln\left(\frac{1}{\varepsilon_1}\right) \right\rceil$$

- Décodage simple

$$S_j = \sum \text{ -/+ } \quad g(p_{yi})$$



Code de Tardos

- Théorie des jeux
  - Décodeur simple

$$max\, min\, E_p[I(Y;X|P)]$$

Code de Tardos

- Théorie des jeux
  - Décodeur simple

$$max\, min\, E_p[I(Y;X|P)]$$

  - Décodeur joint

$$max\, min\, E_p[I(Y;\{X_1,..,X_k\}|P)]$$

Code de Tardos

- Théorie des jeux
  - Décodeur simple

$$max\, min\, E_p[I(Y;X|P)]$$

  - Décodeur joint

$$max\, min\, E_p[I(Y;\{X_1,..,X_k\}|P)]$$

- Calcul du score
  - Décodeur simple (n scores)

$$S_j = \sum \text{ -/+ } \quad g(\, p_{yi}\,)$$

Code de Tardos

- Théorie des jeux
  - Décodeur simple

$$max\, min\, E_p[I(Y;X|P)]$$

  - Décodeur joint

$$max\, min\, E_p[I(Y;\{X_1,..,X_k\}|P)]$$

- Calcul du score
  - Décodeur simple (n scores)

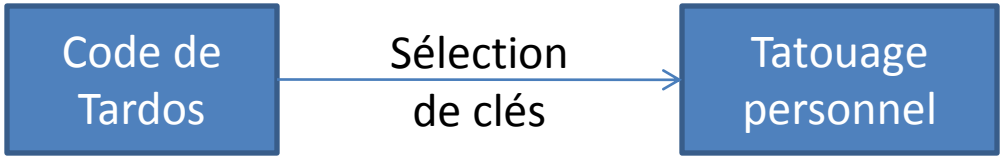
$$S_j = \sum \text{ -/+ } g(p_{yi})$$

  - Décodeur joint

$O(n^k)$ $\quad S_{\{j, \dots, k\}} = ?$

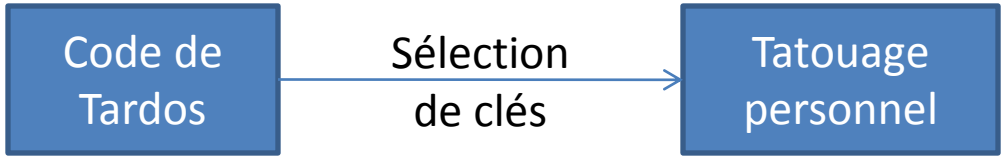
Probabilistic fingerprinting codes used to detect traitor zero-bit watermark

– Principe (Un code pour sélectionner, un tatouage pour accuser).



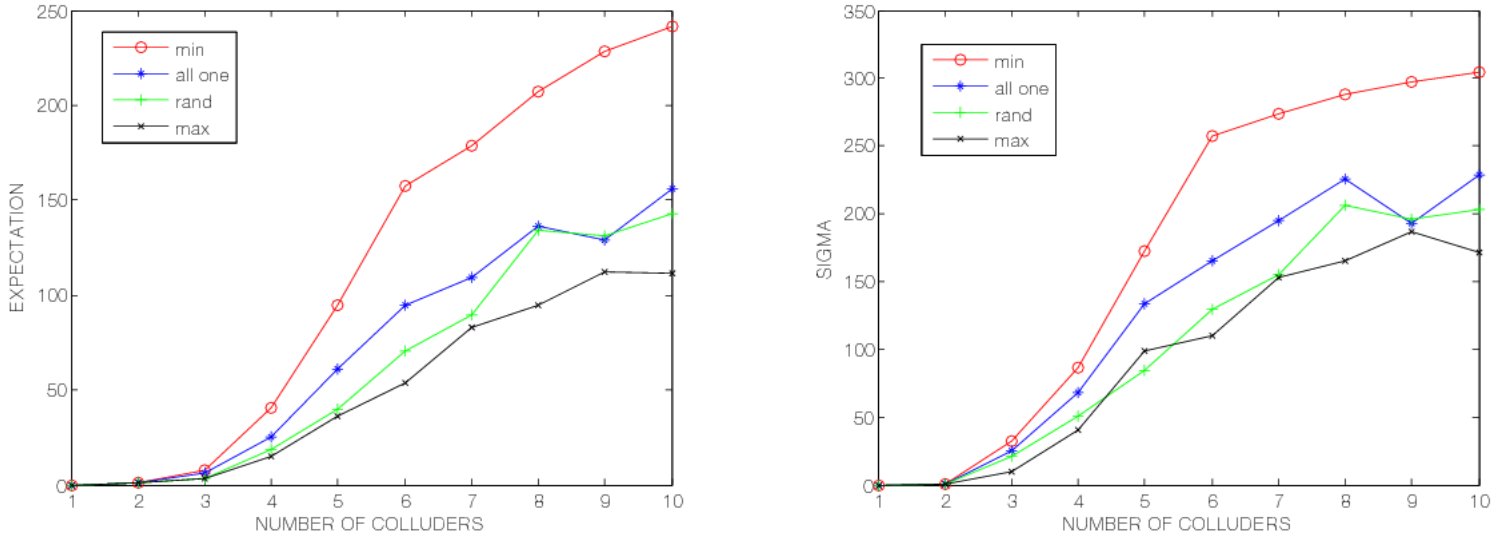
Probabilistic fingerprinting codes used to detect traitor zero-bit watermark

– Principe (Un code pour sélectionner, un tatouage pour accuser).



– Avantages

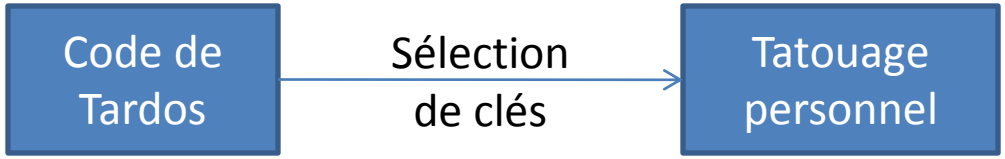
- On peut accuser plus tôt. pfa = pfa(tardos) x pfa(watermark)



Standard deviation and expectation for the number of search needed to find a colluder depending on collusion strategies for $n = 10000$ and $m = 200$.

Probabilistic fingerprinting codes used to detect traitor zero-bit watermark

- Principe (Un code pour sélectionner, un tatouage pour accuser).



- Inconvénients
  - Tatouage au moment de la distribution.
    - Niveau serveur ou client.
  - Dépend de la robustesse du tatouage à la collusion.

Robustesse tatouage

- Tatouage zéro-bit
  - une clé secrète par user.
  - Les porteuses sont supposées orthogonales.

	Expectation	Standard deviation
$c = 2$	0.1468	8.8e-004
$c = 4$	0.1468	1.00e-003
$c = 10$	0.1469	1.1186e-003

Expectation and standard deviation for 1000 innocent correlations and 3 sizes of collusion with JPEG QF = 10.

  - Faible Robustesse à la collusion

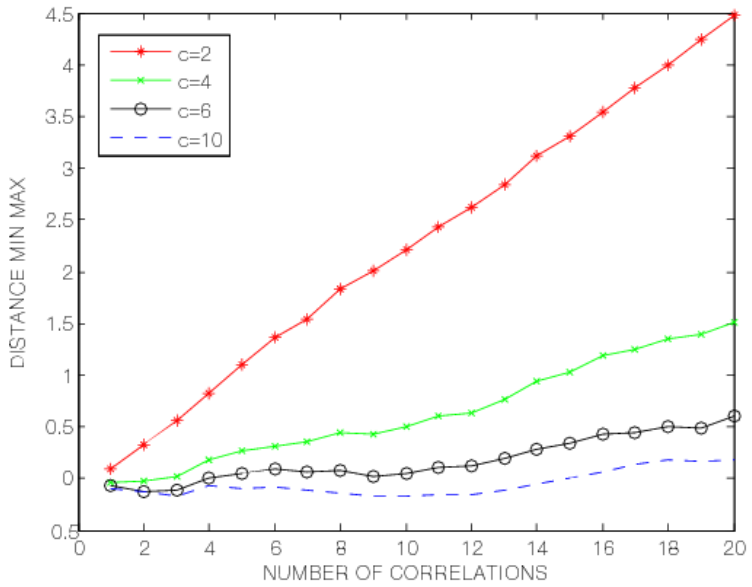
    C = 3 corrélation = 0.3770

    C = 5 corrélation = 0.2843

    C = 10 corrélation = 0.1873

Robustesse tatouage

- Corrélations successives $T_j = \sum_{i=1}^{p} t(j,i).$
  - Au récupère l'énergie du tatouage.



Distance between the minimum colluder correlation and the maximum innocent correlation for 100 innocents users and JPEG QF = 10.

  - Les corrélations des innocents n'ont pas la même variance que les corrélations des attaquants.
  - Difficile d'estimer la pfa du schéma de tatouage expérimentalement.

Travaux futurs

- Décodeur joint avec tatouage personnel
  - EM algorithme (on répète 2 étapes jusqu'à convergence)

    1 - On estime les colluders pour une stratégie fixée.

    2 - On estime la stratégie connaissant les colluders.
- Etude et réalisation d'un tatouage informé sûr
  - Schéma basé quantification robuste au camcording (brevet Orange).