Constructions de protocoles efficaces de récupération confidentielle d'information (PIR)

Julien Lavauzelle

équipe projet GRACE
LIX & INRIA Saclay

Journées Codage et Cryptographie 2017, La Bresse
27/04/2017

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

5. Instances et généralisation

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

5. Instances et généralisation

Problématique — Private Information Retrieval (PIR)

Après le dépôt d'un fichier F sur un système distant,

comment accéder à la donnée F_i de manière confidentielle

(c'est-à-dire, sans donner d'information sur la valeur de i) ?

Définition

Soit F un fichier déposé sur un système distant S.

Un utilisateur U cherche à retrouver le symbole F_i.

Protocole de récupération confidentielle d'information (*Private Information Retrieval*, PIR) :

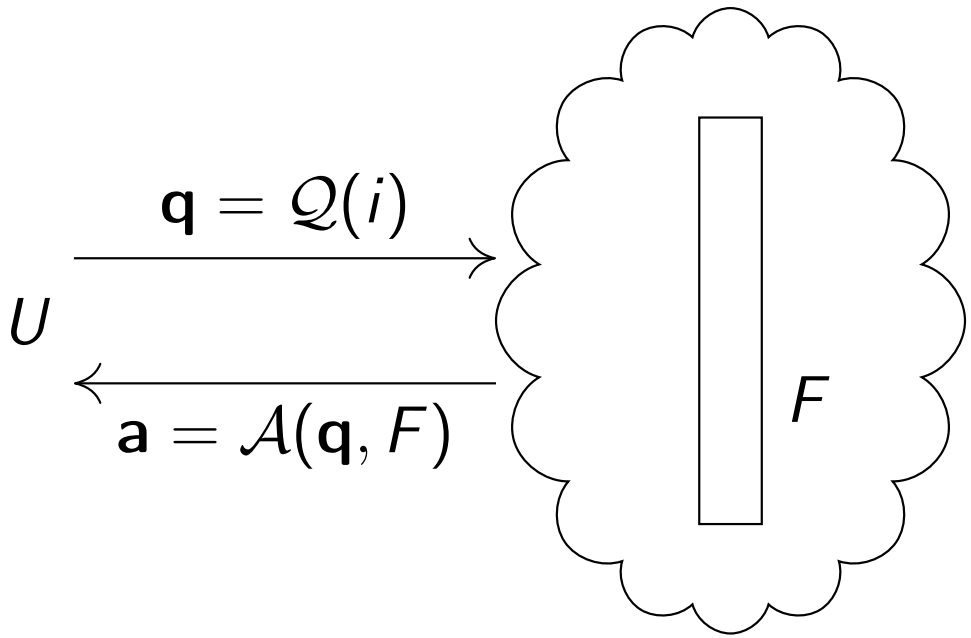
Définition

Soit F un fichier déposé sur un système distant S.

Un utilisateur U cherche à retrouver le symbole F_i.

Protocole de récupération confidentielle d'information (*Private Information Retrieval*, PIR) :

1. U engendre un ensemble de requêtes $\mathbf{q} = \mathcal{Q}(i)$ et l'envoie à S
2. S calcule une réponse $\mathbf{a} = \mathcal{A}(\mathbf{q}, F)$ et la renvoie à U
3. U reconstruit $F_i = \mathcal{R}(\mathbf{q}, \mathbf{a}, i)$.



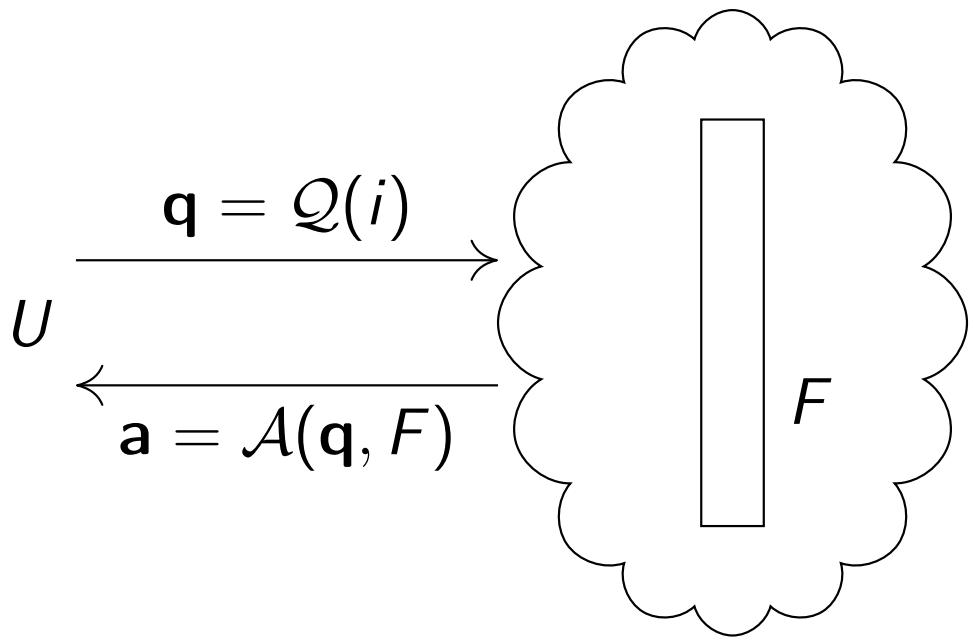
Définition

Soit F un fichier déposé sur un système distant S.

Un utilisateur U cherche à retrouver le symbole F_i.

Protocole de récupération confidentielle d'information (*Private Information Retrieval*, PIR) :

1. U engendre un ensemble de requêtes $\mathbf{q} = \mathcal{Q}(i)$ et l'envoie à S
2. S calcule une réponse $\mathbf{a} = \mathcal{A}(\mathbf{q}, F)$ et la renvoie à U
3. U reconstruit $F_i = \mathcal{R}(\mathbf{q}, \mathbf{a}, i)$.



Sécurité : on veut que $\mathbb{P}(\mathbf{q}|i) = \mathbb{P}(\mathbf{q})$.

Objectifs

Caractéristiques attendues :

- Faible complexité de communication (nombre de bits échangés).
- Faible complexité des algorithmes
  - de réponse $\mathcal{A}$,
  - de reconstruction $\mathcal{R}$.
- Faible redondance de stockage (si encodage).

Impact direct pour l'utilisateur : coût (financier) de la confidentialité.

Objectifs

Caractéristiques attendues :

- Faible complexité de communication (nombre de bits échangés).
- Faible complexité des algorithmes
  - de réponse $\mathcal{A}$,
  - de reconstruction $\mathcal{R}$.
- Faible redondance de stockage (si encodage).

Impact direct pour l'utilisateur : coût (financier) de la confidentialité.

Une approche triviale : télécharger entièrement le fichier...

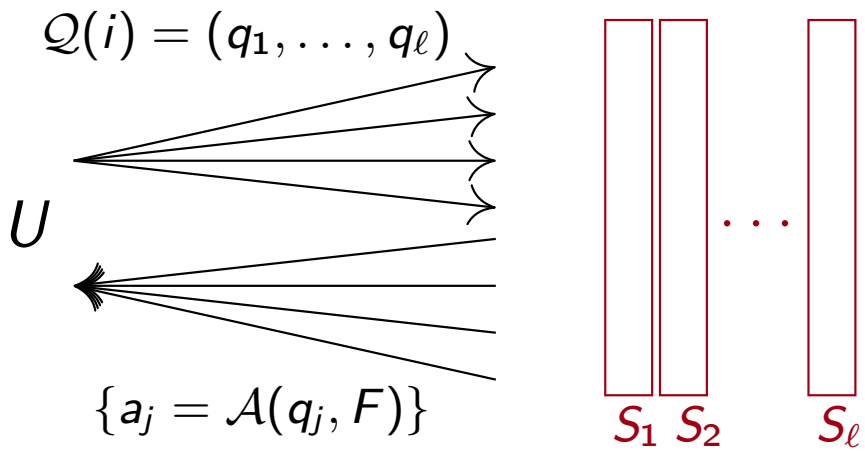
... mais c'est essentiellement la meilleure solution pour une sécurité inconditionnelle, lorsqu'un seul serveur est utilisé [CGKS95]

Définition

Soit F un fichier déposé **sur ℓ serveurs** $S_1, \ldots, S_\ell$.

Pour retrouver le symbole F_i :

1. U engendre un ensemble de requêtes $\mathbf{q} = \mathcal{Q}(i)$ et envoie q_j à S_j
2. chaque S_j calcule une réponse $a_j = \mathcal{A}(q_j, F)$ et la renvoie à U
3. U reconstruit $F_i = \mathcal{R}(\mathbf{q}, \mathbf{a}, i)$



Sécurité : on veut que $\mathbb{P}(q_j|i) = \mathbb{P}(q_j)$, $\forall j = 1, \ldots, \ell$.

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

5. Instances et généralisation

Codes : rappels et notations

- Un code (linéaire) $\mathcal{C}$ de longueur n et dimension k sur $\mathbb{F}_q$ est un sous-espace vectoriel de $\mathbb{F}_q^n$ de dimension k
- Pour un mot $w \in \mathbb{F}_q^n$:
  - support $\mathrm{supp}(w) = \{i \in [1, n], w_i \neq 0\}$
  - poids $\mathrm{wt}(w) = |\mathrm{supp}(w)|$
- Distance minimale : $d(\mathcal{C}) = \min\{\mathrm{wt}(c), c \in \mathcal{C}, c \neq 0\}$
- Dual (= orthogonal) d'un code :

$$\mathcal{C}^\perp = \{w \in \mathbb{F}_q^n, \forall c \in \mathcal{C}, \sum_{i=1}^{n} c_i w_i = 0\}$$

- On va noter $c = \mathrm{Enc}_{\mathcal{C}}(F)$ l'encodage du fichier F par un code $\mathcal{C}$.

PIR avec un code localement décodable

Soit un code $\mathcal{C} \subseteq \mathbb{F}_q^n$ tel que $\forall i, j \in [1, n]$, il existe $h \in \mathcal{C}^\perp$ vérifiant :

$$\{i, j\} \subset \mathrm{supp}(h) \quad \text{et} \quad \mathrm{wt}(h) = \ell + 1.$$

On note $H_\ell(i, j)$ l'ensemble de tels mots h.

PIR avec un code localement décodable

Soit un code $\mathcal{C} \subseteq \mathbb{F}_q^n$ tel que $\forall i, j \in [1, n]$, il existe $h \in \mathcal{C}^\perp$ vérifiant :

$$\{i, j\} \subset \mathrm{supp}(h) \quad \text{et} \quad \mathrm{wt}(h) = \ell + 1.$$

On note $H_\ell(i, j)$ l'ensemble de tels mots h.

Protocole : Pour retrouver $F_i = c_i$:

1. L'utilisateur tire aléatoirement $h \in \cup_j H_\ell(i, j)$ qui "reconstruit" F_i.

$$\mathcal{Q}(i) = (q_1, \ldots, q_\ell) = \mathrm{supp}(h) \setminus \{i\}$$

PIR avec un code localement décodable

Soit un code $\mathcal{C} \subseteq \mathbb{F}_q^n$ tel que $\forall i, j \in [1, n]$, il existe $h \in \mathcal{C}^\perp$ vérifiant :

$$\{i, j\} \subset \mathrm{supp}(h) \quad \text{et} \quad \mathrm{wt}(h) = \ell + 1.$$

On note $H_\ell(i, j)$ l'ensemble de tels mots h.

Protocole : Pour retrouver $F_i = c_i$:

1. L'utilisateur tire aléatoirement $h \in \cup_j H_\ell(i, j)$ qui "reconstruit" F_i.

$$\mathcal{Q}(i) = (q_1, \ldots, q_\ell) = \mathrm{supp}(h) \setminus \{i\}$$

2. Chaque serveur S_j reçoit q_j et renvoie $a_j = c_{q_j}$.

PIR avec un code localement décodable

Soit un code $\mathcal{C} \subseteq \mathbb{F}_q^n$ tel que $\forall i, j \in [1, n]$, il existe $h \in \mathcal{C}^\perp$ vérifiant :

$$\{i, j\} \subset \mathrm{supp}(h) \quad \text{et} \quad \mathrm{wt}(h) = \ell + 1.$$

On note $H_\ell(i, j)$ l'ensemble de tels mots h.

Protocole : Pour retrouver $F_i = c_i$:

1. L'utilisateur tire aléatoirement $h \in \cup_j H_\ell(i, j)$ qui "reconstruit" F_i.

$$\mathcal{Q}(i) = (q_1, \ldots, q_\ell) = \mathrm{supp}(h) \setminus \{i\}$$

2. Chaque serveur S_j reçoit q_j et renvoie $a_j = c_{q_j}$.
3. Comme

$$h \in \mathcal{C}^\perp \quad \Rightarrow \quad \sum_{j \in \mathrm{supp}(h)} h_j c_j = 0\,,$$

l'utilisateur reconstruit $F_i = -\frac{1}{h_i} \sum_{j \neq i} h_j a_j$.

PIR avec un code localement décodable

Résultats :

- ℓ serveurs et communication en $\Theta(\ell \log(q))$ bits
- complexité algorithmique :
  - réponse $\mathcal{A}$ en $\Omega(|F|)$ pour chaque serveur
  - reconstruction $\mathcal{R}$ en $\mathcal{O}(\ell)$
- stockage : ℓ copies de $F \Rightarrow (\ell - 1)|F|$ bits de redondance

PIR avec un code localement décodable

Résultats :

- ℓ serveurs et communication en $\Theta(\ell \log(q))$ bits
- complexité algorithmique :
  - réponse $\mathcal{A}$ en $\Omega(|F|)$ pour chaque serveur **(à améliorer)**
  - reconstruction $\mathcal{R}$ en $\mathcal{O}(\ell)$
- stockage : ℓ copies de $F \Rightarrow (\ell - 1)|F|$ bits de redondance **(à améliorer)**

PIR avec un code localement décodable

Résultats :

- ℓ serveurs et communication en $\Theta(\ell \log(q))$ bits
- complexité algorithmique :
  - réponse $\mathcal{A}$ en $\Omega(|F|)$ pour chaque serveur **(à améliorer)**
  - reconstruction $\mathcal{R}$ en $\mathcal{O}(\ell)$
- stockage : ℓ copies de $F \Rightarrow (\ell - 1)|F|$ bits de redondance **(à améliorer)**

• 1ère idée : pré-calcul des réponses $\Rightarrow$ moins de calcul, plus de stockage

PIR avec un code localement décodable

Résultats :

- ℓ serveurs et communication en $\Theta(\ell \log(q))$ bits
- complexité algorithmique :
  - réponse $\mathcal{A}$ en $\Omega(|F|)$ pour chaque serveur **(à améliorer)**
  - reconstruction $\mathcal{R}$ en $\mathcal{O}(\ell)$
- stockage : ℓ copies de $F \Rightarrow (\ell - 1)|F|$ bits de redondance **(à améliorer)**

- 1ère idée : pré-calcul des réponses $\Rightarrow$ moins de calcul, plus de stockage
- 2nde idée [ALS14] : partager l'encodage de F sur les ℓ serveurs.

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

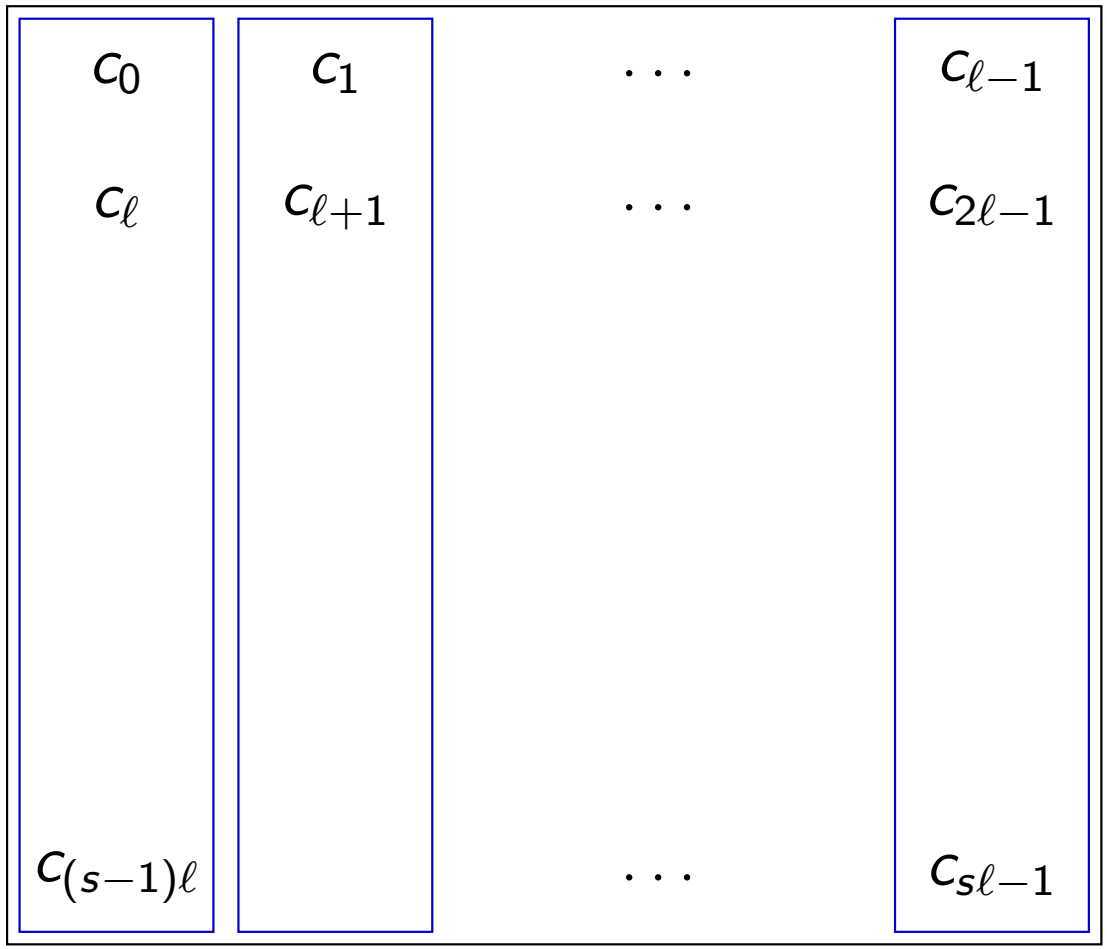
5. Instances et généralisation

Besoin d'un design transversal

$$\mathrm{Enc}_{\mathcal{C}}(F) = c = \begin{array}{|cccc|} \hline c_0 & c_1 & \cdots & c_{\ell-1} \\ c_\ell & c_{\ell+1} & \cdots & c_{2\ell-1} \\ & & & \\ & & & \\ & & & \\ c_{(s-1)\ell} & & \cdots & c_{s\ell-1} \\ \hline \end{array}$$

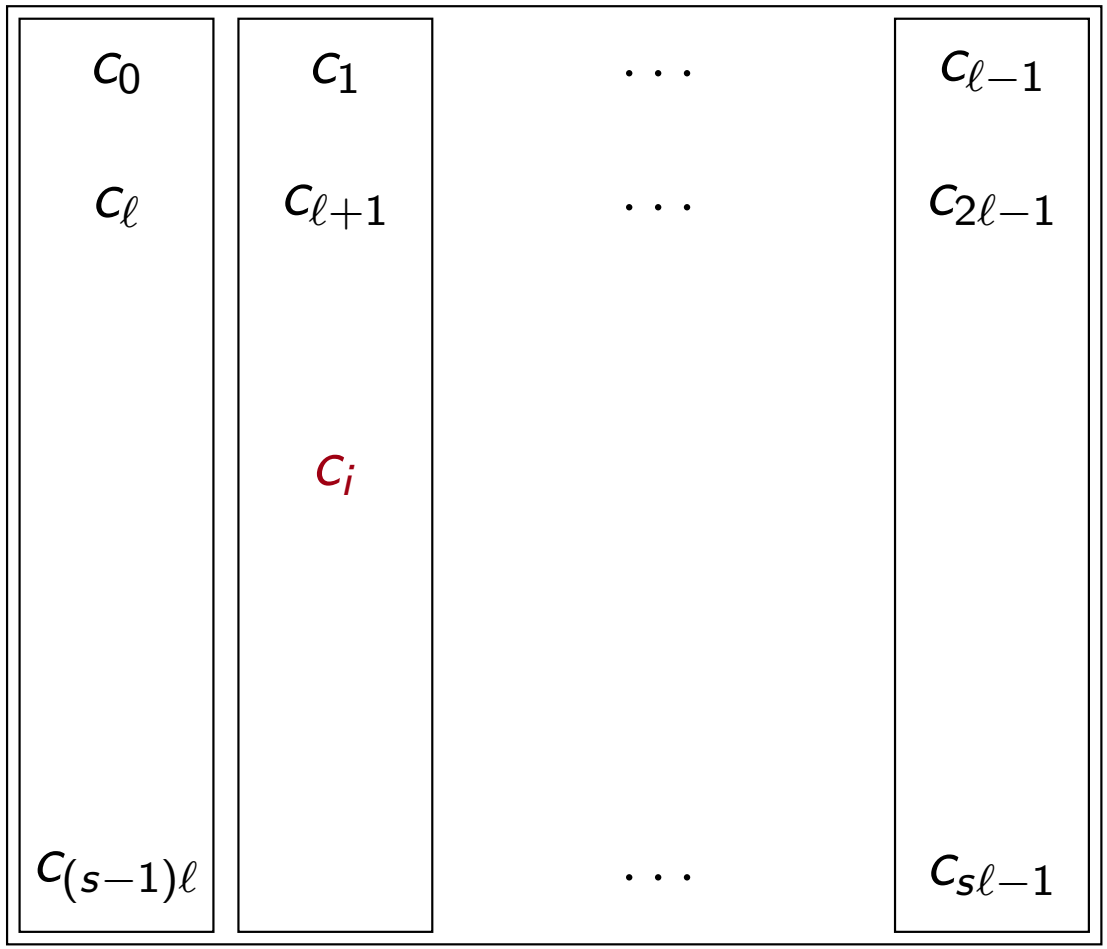
Besoin d'un design transversal

$\mathrm{Enc}_{\mathcal{C}}(F) = c =$

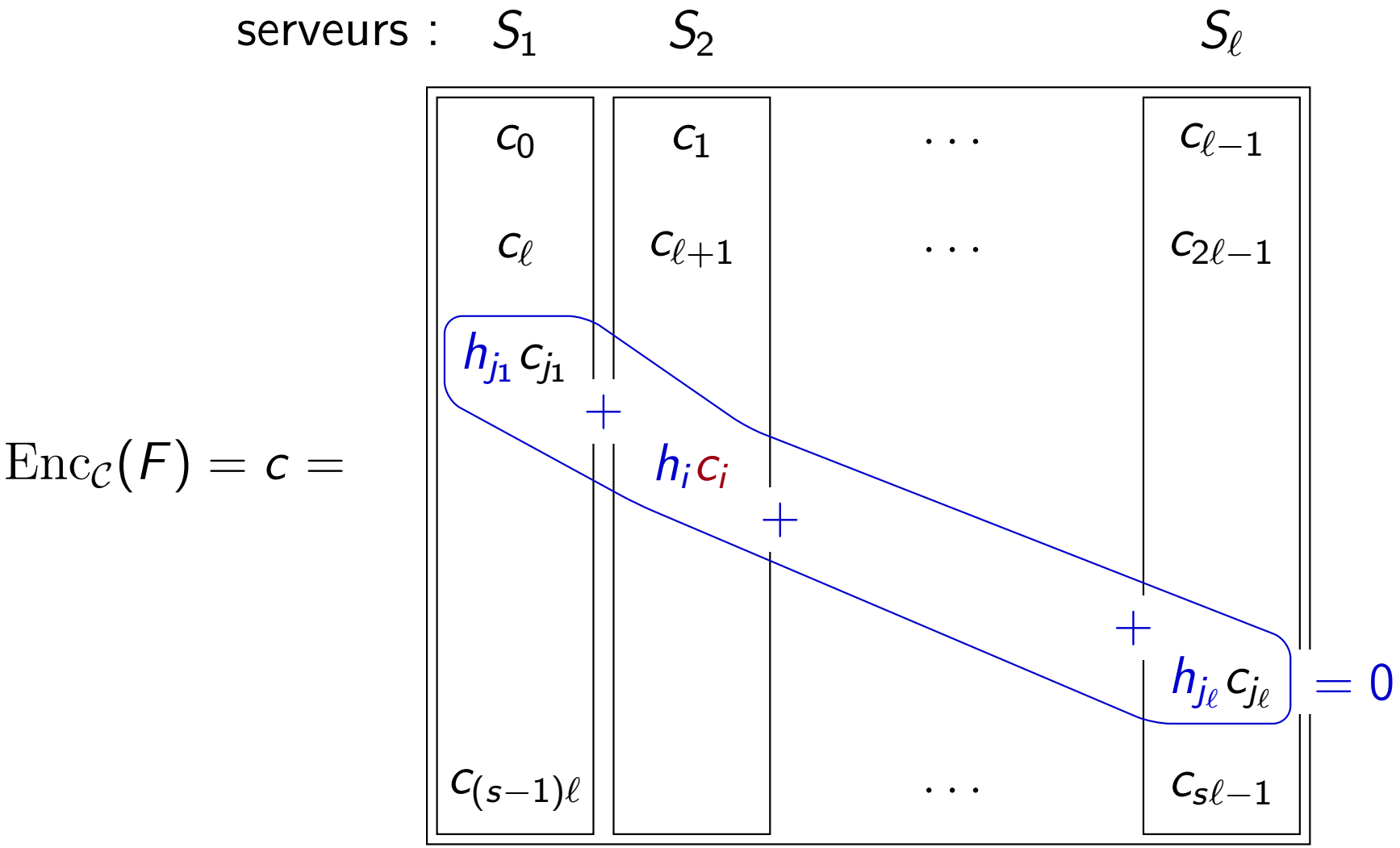


Besoin d'un design transversal

$\mathrm{Enc}_{\mathcal{C}}(F) = c =$

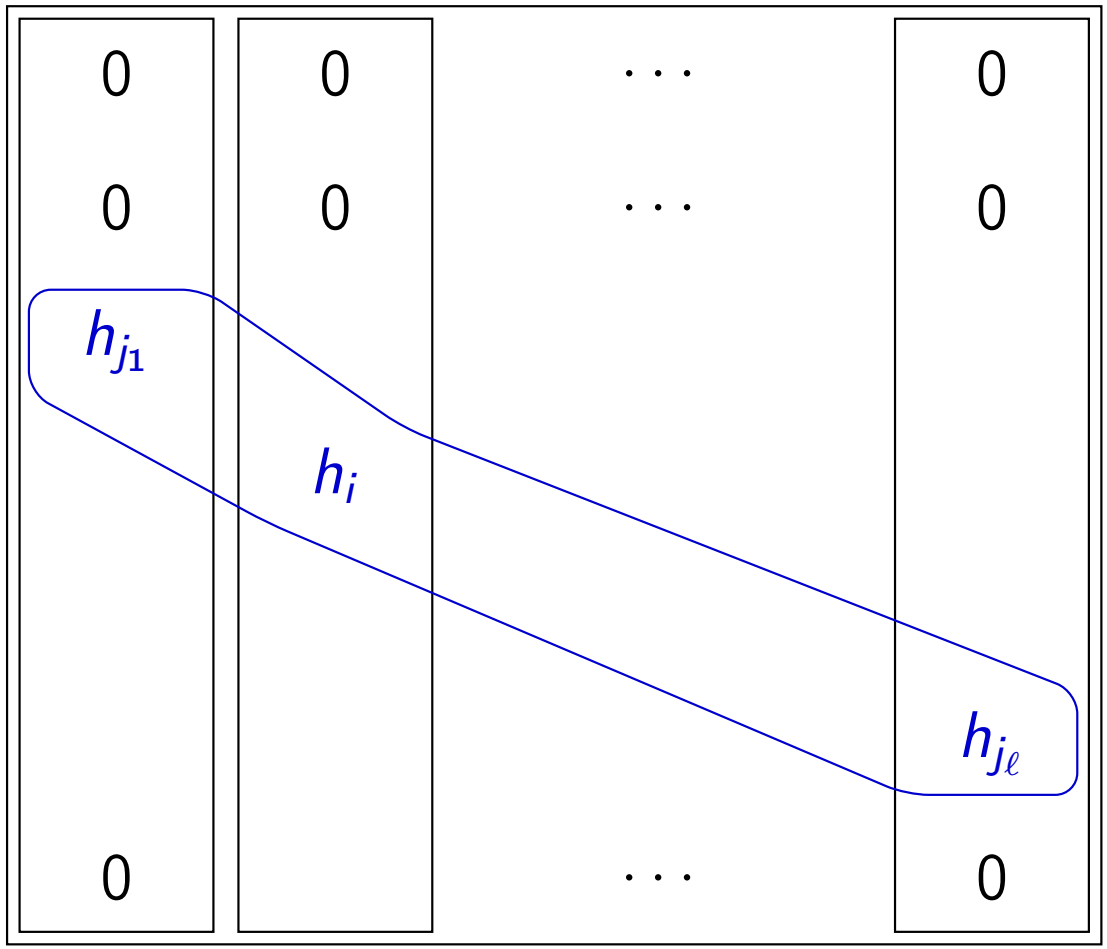


Besoin d'un design transversal



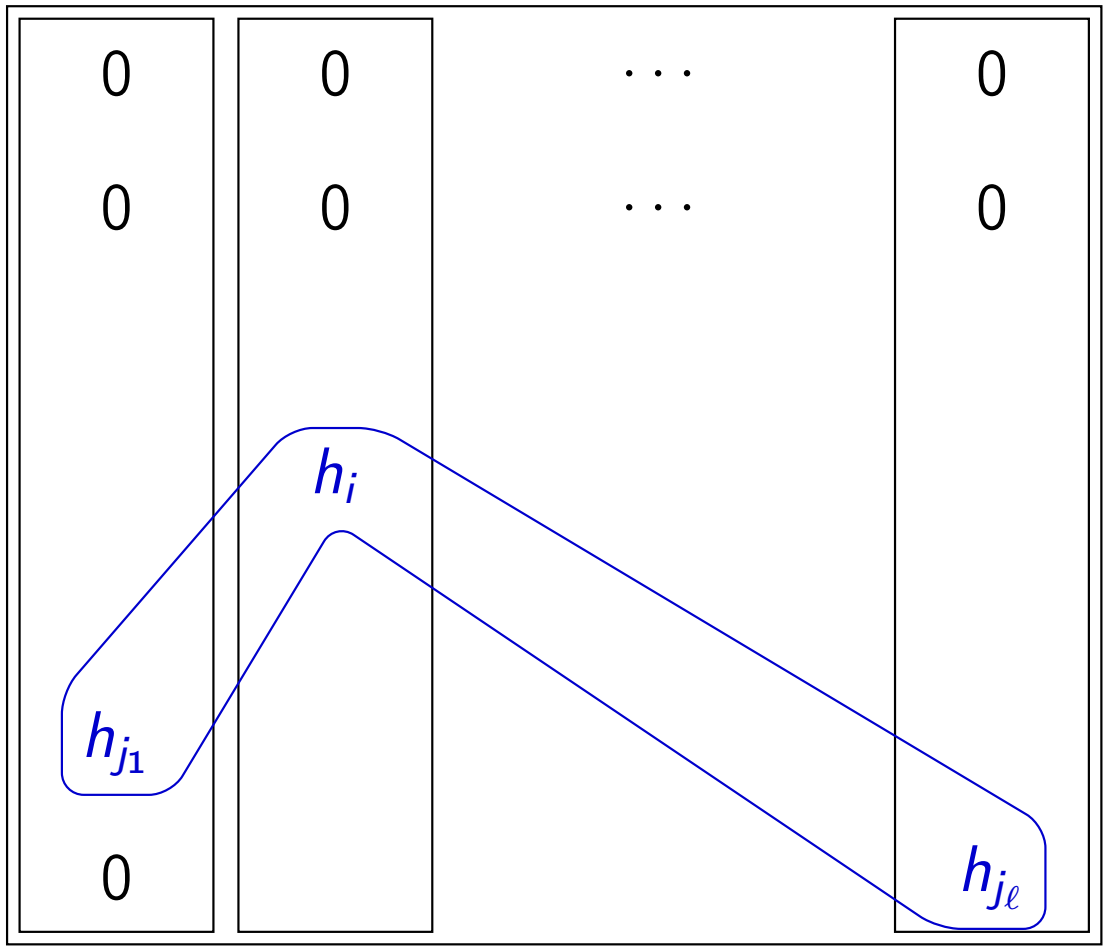
Besoin d'un design transversal

$\mathcal{C}^{\perp} \ni h =$



Besoin d'un design transversal

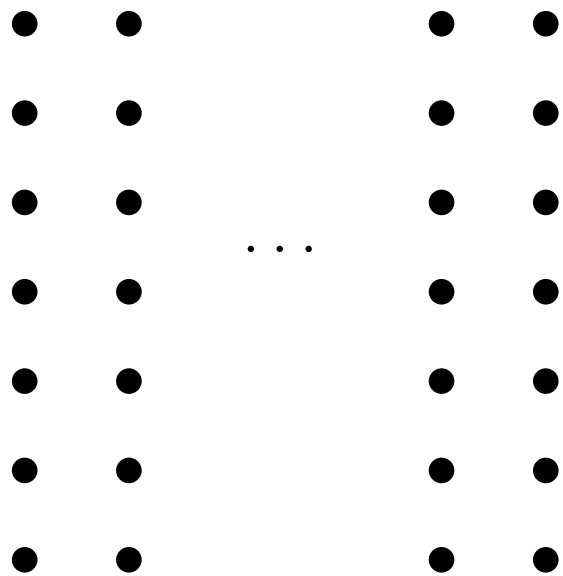
$\mathcal{C}^{\perp} \ni h =$



Design transversal

Un **design transversal** $\mathrm{TD}(\ell, s)$ est un triplet $(X, \mathcal{B}, \mathcal{G})$ tel que :

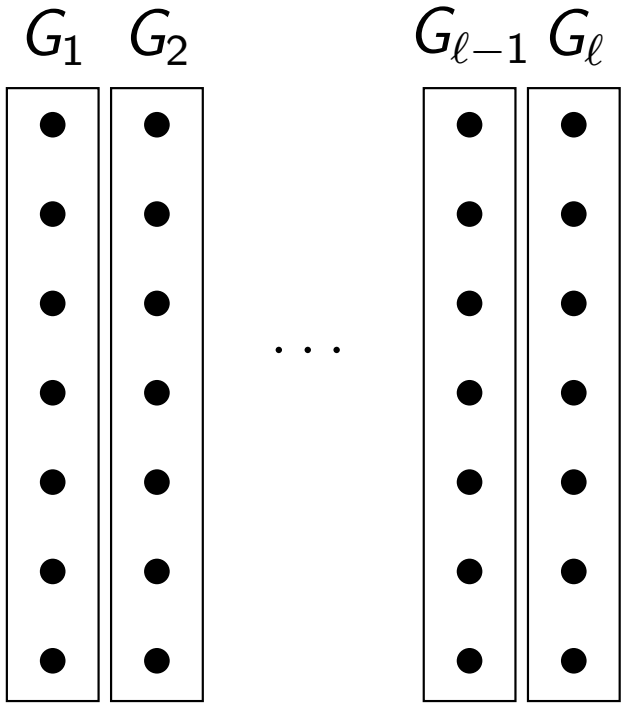
- X forme les *points*, $|X| = n = s\ell$,



Design transversal

Un **design transversal** $\mathrm{TD}(\ell, s)$ est un triplet $(X, \mathcal{B}, \mathcal{G})$ tel que :

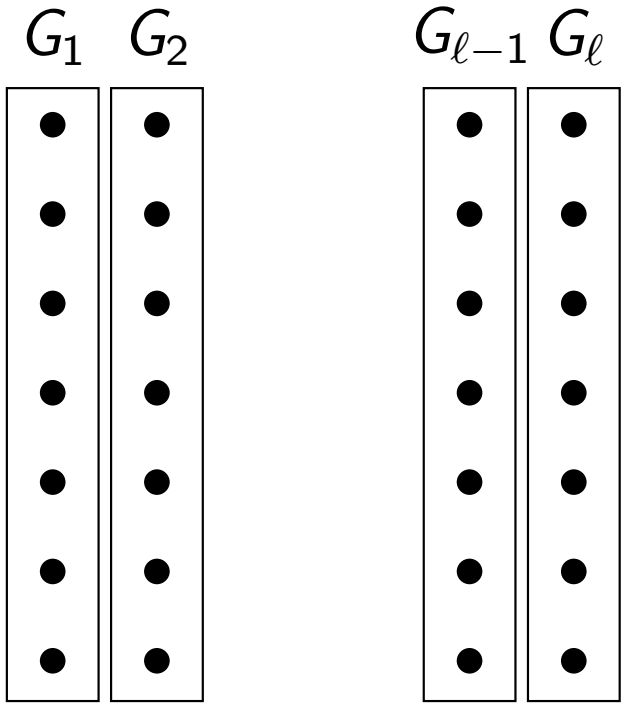
- X forme les *points*, $|X| = n = s\ell$,
- les *groupes* $\mathcal{G} = (G_1, \ldots, G_\ell)$ sont une partition de X, avec $|G_j| = s$;



Design transversal

Un **design transversal** $\mathrm{TD}(\ell, s)$ est un triplet $(X, \mathcal{B}, \mathcal{G})$ tel que :

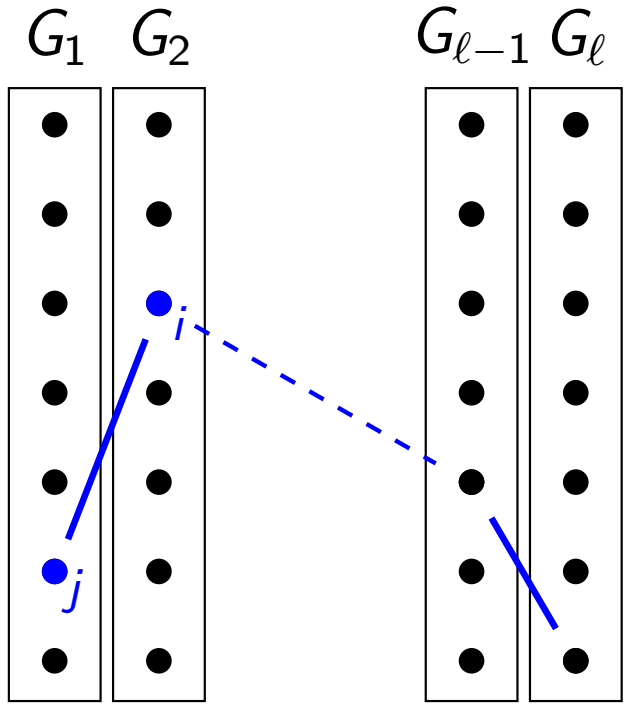
- X forme les *points*, $|X| = n = s\ell$,
- les *groupes* $\mathcal{G} = (G_1, \ldots, G_\ell)$ sont une partition de X, avec $|G_j| = s$;
- les *blocs* $B \in \mathcal{B}$ vérifient :
  - $B \subset X$ et $|B| = \ell$;
  - propriété d'incidence : si $\{i, j\} \subset X$ ne sont pas dans le même groupe, alors $\exists!$ bloc $B \in \mathcal{B}$ tel que $\{i, j\} \subset B$



Design transversal

Un **design transversal** $\mathrm{TD}(\ell, s)$ est un triplet $(X, \mathcal{B}, \mathcal{G})$ tel que :

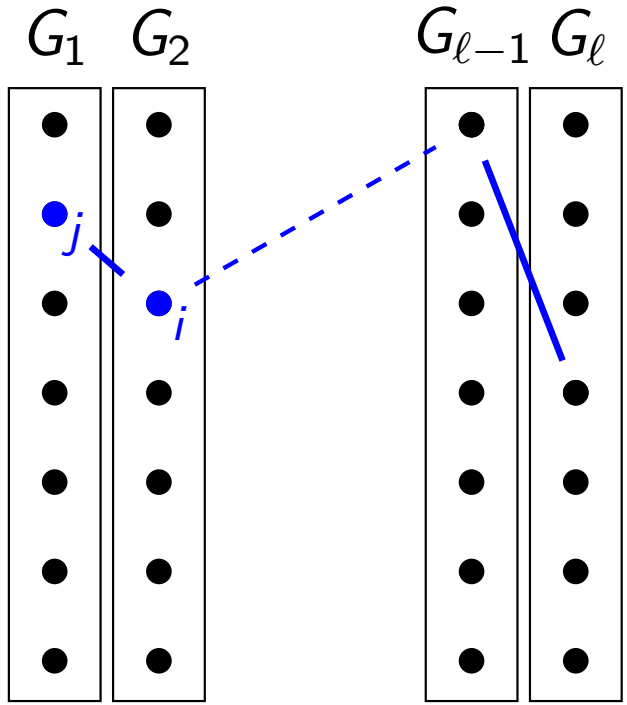
- X forme les *points*, $|X| = n = s\ell$,
- les *groupes* $\mathcal{G} = (G_1, \ldots, G_\ell)$ sont une partition de X, avec $|G_j| = s$;
- les *blocs* $B \in \mathcal{B}$ vérifient :
  - $B \subset X$ et $|B| = \ell$;
  - propriété d'incidence : si $\{i, j\} \subset X$ ne sont pas dans le même groupe, alors $\exists!$ bloc $B \in \mathcal{B}$ tel que $\{i, j\} \subset B$



Design transversal

Un **design transversal** $\mathrm{TD}(\ell, s)$ est un triplet $(X, \mathcal{B}, \mathcal{G})$ tel que :

- X forme les *points*, $|X| = n = s\ell$,
- les *groupes* $\mathcal{G} = (G_1, \ldots, G_\ell)$ sont une partition de X, avec $|G_j| = s$;
- les *blocs* $B \in \mathcal{B}$ vérifient :
  - $B \subset X$ et $|B| = \ell$;
  - propriété d'incidence : si $\{i, j\} \subset X$ ne sont pas dans le même groupe, alors $\exists!$ bloc $B \in \mathcal{B}$ tel que $\{i, j\} \subset B$



Code engendré par un TD

Soit $\mathcal{T} = (X, \mathcal{B}, \mathcal{G})$ un $\mathrm{TD}(\ell, s)$. On définit sa **matrice d'incidence** comme la matrice M de taille $|\mathcal{B}| \times |X|$ telle que:

$$M_{i,j} = \begin{cases} 1 & \text{si } x_j \in B_i \\ 0 & \text{sinon} \end{cases}$$

Code engendré par un TD

Soit $\mathcal{T} = (X, \mathcal{B}, \mathcal{G})$ un $\mathrm{TD}(\ell, s)$. On définit sa **matrice d'incidence** comme la matrice M de taille $|\mathcal{B}| \times |X|$ telle que:

$$M_{i,j} = \begin{cases} 1 & \text{si } x_j \in B_i \\ 0 & \text{sinon} \end{cases}$$

Le **code $\mathcal{C}$ engendré par $\mathcal{T}$ sur** $\mathbb{F}_q$ est le code sur $\mathbb{F}_q$ dont M est une matrice de parité.

Code engendré par un TD

Soit $\mathcal{T} = (X, \mathcal{B}, \mathcal{G})$ un $\mathrm{TD}(\ell, s)$. On définit sa **matrice d'incidence** comme la matrice M de taille $|\mathcal{B}| \times |X|$ telle que:

$$M_{i,j} = \begin{cases} 1 & \text{si } x_j \in B_i \\ 0 & \text{sinon} \end{cases}$$

Le **code $\mathcal{C}$ engendré par $\mathcal{T}$ sur** $\mathbb{F}_q$ est le code sur $\mathbb{F}_q$ dont M est une matrice de parité.

Propriété importante :

- pour tout $i \neq j \in [1, n]$, si i et j ne sont pas dans le même groupe, alors il existe un mot $h \in H_\ell(i, j)$.

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

5. Instances et généralisation

Définition du protocole de PIR

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ le code engendré par un $\mathrm{TD}(\ell, s)$.

Initialisation. L'utilisateur encode son fichier F avec $\mathcal{C}$, et distribue à chaque serveur S_j le sous-mot $c_{|G_j}$ associé au groupe G_j.

Définition du protocole de PIR

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ le code engendré par un $\mathrm{TD}(\ell, s)$.

Initialisation. L'utilisateur encode son fichier F avec $\mathcal{C}$, et distribue à chaque serveur S_j le sous-mot $c_{|G_j}$ associé au groupe G_j.

Pour retrouver $F_i = c_i$:

1. l'utilisateur tire aléatoirement un bloc $B \in \mathcal{B}$, et définit :

$$q_j = \mathcal{Q}(i)_j = \begin{cases} B \cap G_j & \text{si } i \notin G_j \\ \text{un point aléatoire de } G_j & \text{sinon} \end{cases}$$

2. chaque serveur S_j renvoie $a_j = \mathcal{A}(q_j, c_{|G_j}) = c_{q_j}$
3. l'utilisateur reconstruit

$$c_i = -\sum_{i \notin G_j} c_{q_j}$$

Propriétés du protocole de PIR

Théorème. Si les serveurs ne coopèrent pas, alors ce protocole de PIR est inconditionnellement sûr.

Propriétés du protocole de PIR

Théorème. Si les serveurs ne coopèrent pas, alors ce protocole de PIR est inconditionnellement sûr.

Preuve :

- le serveur qui détient i reçoit une requête aléatoire,
- pour un autre serveur S_j, le nombre de blocs passant par i et l'un des points de son groupe G_j est constant $(= 1) \Rightarrow$ aucune information sur i.

Propriétés du protocole de PIR

Théorème. Si les serveurs ne coopèrent pas, alors ce protocole de PIR est inconditionnellement sûr.
Preuve :

- le serveur qui détient i reçoit une requête aléatoire,
- pour un autre serveur S_j, le nombre de blocs passant par i et l'un des points de son groupe G_j est constant $(= 1) \Rightarrow$ aucune information sur i.

Propriétés. Pour un fichier de $k \log q$ bits, où $k = \dim_{\mathbb{F}_q} \mathcal{C} \leq n = s\ell$.

- communication : $\ell(\log s + \log q)$ bits
- calcul :
  - constant pour les réponses $\mathcal{A}$ (au lieu de $\Omega(k \log q)$)
  - une somme de $\ell - 1$ éléments de $\mathbb{F}_q$ pour la reconstuction $\mathcal{R}$
- stockage : $(n - k) \log q$ bits de redondance
  (au lieu de $(\ell - 1)k \log q$)

Propriétés du protocole de PIR

Théorème. Si les serveurs ne coopèrent pas, alors ce protocole de PIR est inconditionnellement sûr.
Preuve :

- le serveur qui détient i reçoit une requête aléatoire,
- pour un autre serveur S_j, le nombre de blocs passant par i et l'un des points de son groupe G_j est constant $(= 1) \Rightarrow$ aucune information sur i.

Propriétés. Pour un fichier de $k \log q$ bits, où $k = \dim_{\mathbb{F}_q} \mathcal{C} \leq n = s\ell$.

- communication : $\ell(\log s + \log q)$ bits
- calcul :
  - constant pour les réponses $\mathcal{A}$ (au lieu de $\Omega(k \log q)$)
  - une somme de $\ell - 1$ éléments de $\mathbb{F}_q$ pour la reconstuction $\mathcal{R}$
- stockage : $(n - k) \log q$ bits de redondance
  (au lieu de $(\ell - 1)k \log q$)

Question majeure : $k = \dim_{\mathbb{F}_q} \mathcal{C}$ en fonction de ℓ, n ?

1. Problématique et définitions

2. Protocoles de PIR avec des codes à propriétés locales

3. Designs transversaux et leurs codes

4. Protocoles de PIR fondés sur des designs transversaux

5. Instances et généralisation

L'instance classique : droites et hyperplans

Soient :

- $X = \mathbb{F}_q^m$,
- $\mathcal{G}$ un ensemble de q hyperplans qui partitionnent X,
- $\mathcal{B} = \{\text{droites affines non incluses dans un des hyperplans de } \mathcal{G}\}$.

L'instance classique : droites et hyperplans

Soient :

- $X = \mathbb{F}_q^m$,
- $\mathcal{G}$ un ensemble de q hyperplans qui partitionnent X,
- $\mathcal{B} = \{\text{droites affines non incluses dans un des hyperplans de } \mathcal{G}\}$.

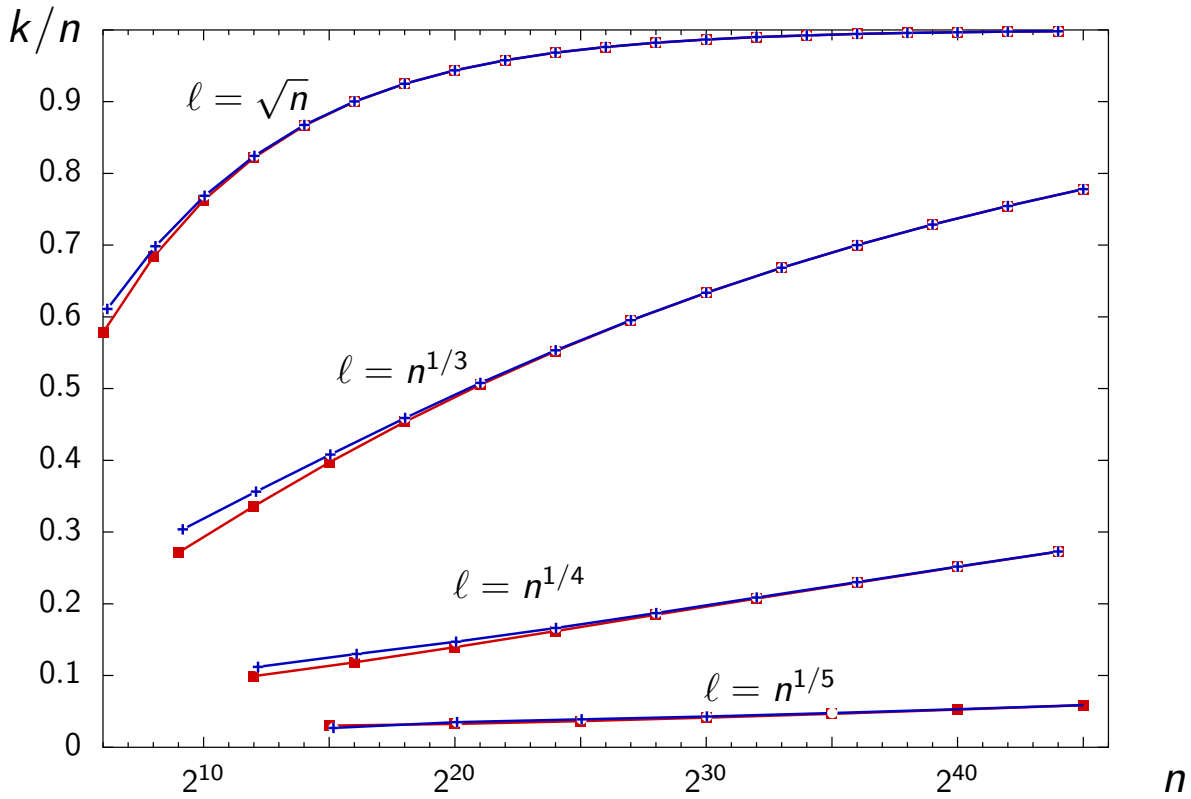
Code associé ?

- longueur $n = q^m$
- "localité" $\ell = q$
- dimension ?
  La matrice de parité a q^m colonnes et q^{2m-2} lignes, et on la veut de faible rang...

L'instance classique : droites et hyperplans

Exemple : pour $m = 2$ et $q = 4096$, on a $n/k \simeq 1,03$.

$\Rightarrow$ accès confidentiel à un fichier de $\simeq 2$ Mo, avec une communication de 6 ko, et seulement 3% de redondance sur les serveurs.



Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

$$OA = \begin{bmatrix} a & b & b \\ b & b & a \\ b & a & b \\ a & a & a \end{bmatrix}$$

Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

Construction OA $\rightarrow$ TD :

- $X = S \times [1, \ell]$
- $\mathcal{G} = \{S \times \{i\}, i \in [1, \ell]\}$

$$OA = \begin{bmatrix} a & b & b \\ b & b & a \\ b & a & b \\ a & a & a \end{bmatrix}$$

$(a,1)$ $(a,2)$ $(a,3)$

$(b,1)$ $(b,2)$ $(b,3)$

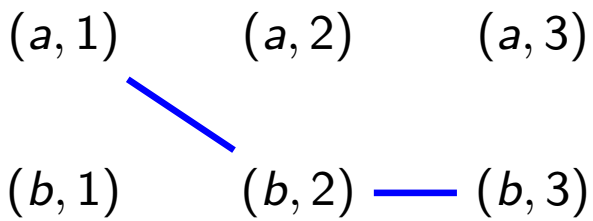
Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

Construction OA $\rightarrow$ TD :

- $X = S \times [1, \ell]$
- $\mathcal{G} = \{S \times \{i\}, i \in [1, \ell]\}$
- $\mathcal{B} = \{\{(c_i, i), 1 \leq i \leq \ell\}, c \in \mathrm{OA}\}$

$$OA = \begin{bmatrix} a & b & b \\ b & b & a \\ b & a & b \\ a & a & a \end{bmatrix}$$



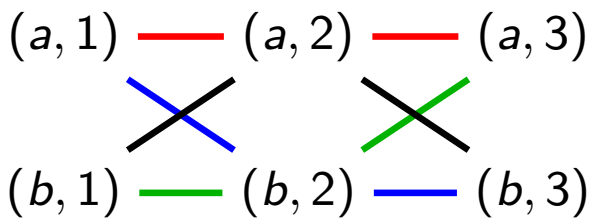
Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

Construction OA $\rightarrow$ TD :

- $X = S \times [1, \ell]$
- $\mathcal{G} = \{S \times \{i\}, i \in [1, \ell]\}$
- $\mathcal{B} = \{\{(c_i, i), 1 \leq i \leq \ell\}, c \in \mathrm{OA}\}$

$$OA = \begin{bmatrix} a & b & b \\ b & b & a \\ b & a & b \\ a & a & a \end{bmatrix}$$



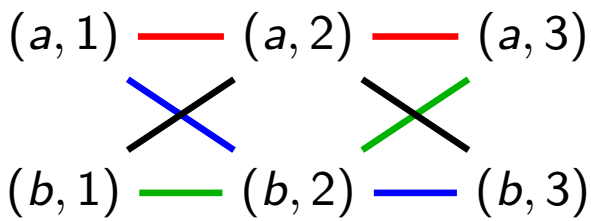
Une construction par tableaux orthogonaux

Un tableau orthogonal de force t (*orthogonal array* $\mathrm{OA}(t, \ell, s)$) est **un code sur S, $|S| = s$, de longueur ℓ, de cardinal N et de distance duale $d^\perp = t + 1$.**

$$OA = \begin{bmatrix} a & b & b \\ b & b & a \\ b & a & b \\ a & a & a \end{bmatrix}$$

Construction OA $\to$ TD :

- $X = S \times [1, \ell]$
- $\mathcal{G} = \{S \times \{i\}, i \in [1, \ell]\}$
- $\mathcal{B} = \{\{(c_i, i), 1 \leq i \leq \ell\}, c \in \mathrm{OA}\}$



Prop. Si $t = 2$, on obtient un $\mathrm{TD}(\ell, s)$.

Résistance aux collusions

Et pour $t > 2$?

Il existe un bloc passant par chaque t-uplet de positions appartenant à t groupes différents.

$\Rightarrow$ Le protocole de PIR résistera à la collusion de $t - 1$ serveurs.

Résistance aux collusions

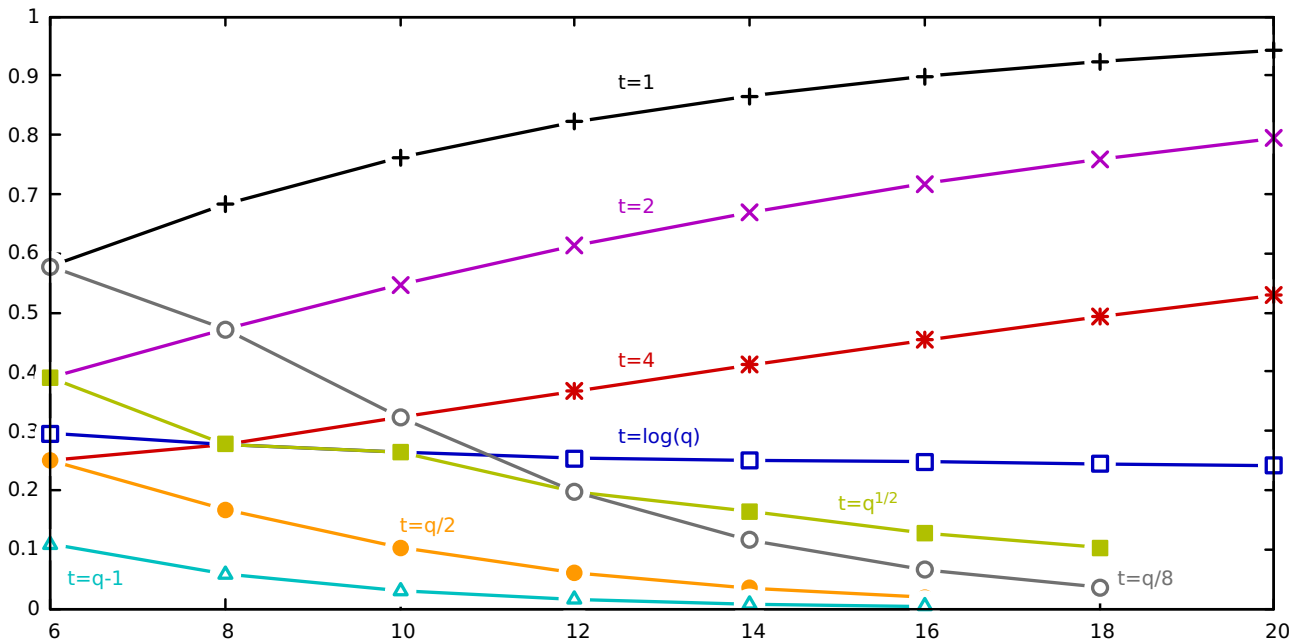
Et pour $t > 2$?

Il existe un bloc passant par chaque t-uplet de positions appartenant à t groupes différents.

$\Rightarrow$ Le protocole de PIR résistera à la collusion de $t - 1$ serveurs.

En pratique :

Le taux d'information du code construit décroît très vite avec t.



Conclusion

Contribution :

- La matrice d'incidence d'un design transversal fournit un encodage efficace pour un protocole de PIR.
- Une construction de TD à base de tableaux orthogonaux de force t donne une résistance à la collusion de $t - 1$ serveurs.

Conclusion

Contribution :

- La matrice d'incidence d'un design transversal fournit un encodage efficace pour un protocole de PIR.
- Une construction de TD à base de tableaux orthogonaux de force t donne une résistance à la collusion de $t-1$ serveurs.

Question (très) ouverte : peut-on caractériser les designs transversaux (ou les tableaux orthogonaux qui les définissent) donnant les meilleurs codes ?

Conclusion

Contribution :

- La matrice d'incidence d'un design transversal fournit un encodage efficace pour un protocole de PIR.
- Une construction de TD à base de tableaux orthogonaux de force t donne une résistance à la collusion de $t-1$ serveurs.

Question (très) ouverte : peut-on caractériser les designs transversaux (ou les tableaux orthogonaux qui les définissent) donnant les meilleurs codes ?

Merci !