

Du suppressif au perturbatif, comment paramétrer les méthodes de bruitage ? Une première démarche utilisant la méthode des clés aléatoires

Julien Jamme, Département des Méthodes Statistiques

JMS 2025

27 novembre 2025

Paris



Des diffusions de tableaux parfois complexes:

- Nombreux zonages géographiques
- Diffusions asynchrones
- Tableaux de grandes tailles
- Intrication très complexe des tableaux entre eux

Éléments de contexte

Rendant leur protection difficile à traiter avec les méthodes classiques:

- Nombreux zonages géographiques ⇒ Risques accrus de différenciation

Rendant leur protection difficile à traiter avec les méthodes classiques:

- Nombreux zonages géographiques \Rightarrow Risques accrus de différenciation
- Diffusions asynchrones \Rightarrow Non prises en compte par les méthodes suppressives

Rendant leur protection difficile à traiter avec les méthodes classiques:

- Nombreux zonages géographiques \Rightarrow Risques accrus de différenciation
- Diffusions asynchrones \Rightarrow Non prises en compte par les méthodes suppressives
- Tableaux de grandes tailles \Rightarrow Limites des outils de pose du secret secondaire

Rendant leur protection difficile à traiter avec les méthodes classiques:

- Nombreux zonages géographiques \Rightarrow Risques accrus de différenciation
- Diffusions asynchrones \Rightarrow Non prises en compte par les méthodes suppressives
- Tableaux de grandes tailles \Rightarrow Limites des outils de pose du secret secondaire
- Intrication très complexe des tableaux entre eux \Rightarrow Complexité des analyses préalables des liens entre tableaux.

Un exemple concret

La diffusion de données aux Quartiers prioritaires de la politique de la ville (QPV):

- Données diffusées au QPV, à l'IRIS, à la commune, etc. et sur deux millésimes des zonages QPV
- ⇒ Complexité des traitements de la différenciation
- ⇒ Suppressions secondaires importantes pour gérer ces risques de différenciation
- ⇒ Une perte d'utilité importante des tableaux

Le choix de méthodes perturbatrices

Face aux limites des méthodes suppressives pour traiter ces cas complexes, tournons-nous vers des méthodes perturbatrices.

Les critères d'une bonne méthode

- Perturber tous les comptages \Rightarrow Réduction automatique des risques de différenciation

Les critères d'une bonne méthode

- Perturber tous les comptages \Rightarrow Réduction automatique des risques de différenciation
- Perturber une case toujours de la même manière \Rightarrow Conserver une cohérence des tableaux entre eux

Les critères d'une bonne méthode

- Perturber tous les comptages \Rightarrow Réduction automatique des risques de différenciation
- Perturber une case toujours de la même manière \Rightarrow Conserver une cohérence des tableaux entre eux
- Facilité d'implémentation \Rightarrow Gagner en efficacité et en efficience.

- Comment s'adapter aux règles de confidentialité conçues à l'origine pour une approche suppressive ?
 - Règle de fréquence pour les tableaux de comptages = toute case en-dessous d'un seuil fixé est considérée comme sensible.
- Comment calibrer le bruit injecté le plus objectivement possible ?

Le choix de la méthode des clés aléatoires

La méthode des clés aléatoires ou *Cell Key Method* (CKM) consiste à **dévier tous les comptages** d'un tableau tout en assurant, par l'utilisation de clés aléatoires individuelles, qu'**une même case est toujours perturbée de la même manière**. Proposition originale dans [Fraser and Wooton, 2005]

Présentation de la méthode Cell Key

Les ingrédients nécessaires:

- Des clés individuelles aléatoires uniformes
- Une matrice de transition définissant les distributions de probabilités du bruit injecté
- Une table de perturbation déterminant le bruit à injecter en fonction des clés et de la matrice de transition.

Méthode Cell Key – 1 – Tirage des clés individuelles

Table 1: Tirage des clés d'enregistrement à partir d'une distribution uniforme

id	Commune	Âge	Clé d'enregistrement
1	Amiens	25	0.9177275
2	Paris	20	0.8850062
3	Marseille	45	0.6266963
4	Amiens	45	0.1117820
5	Marseille	20	0.6496634
6	Marseille	20	0.2813433

Méthode Cell Key – 2 – Construction des tableaux et des clés de chaque case

Table 2: Fréquences et agrégation des clés d'enregistrement

Comm.	ids	X	\sum clés	Clé de cellule
Amiens	{1,4}	2	1.0295095	0.0295095
Marseille	{3,5,6}	3	1.5577030	0.5577030
Paris	{2}	1	0.8850062	0.8850062
Total	{1,2,3,4,5,6}	6	3.4722187	0.4722187

Méthode Cell Key – 3 - La matrice de transition

Quelques notations:

- N : nombre d'enregistrements
- $X \in \llbracket 0; N \rrbracket$: décompte initial de la cellule \mathcal{C}
- $Z \in \llbracket -D; +D \rrbracket$: variable aléatoire du bruit injecté dans \mathcal{C}
- $X' = X + Z \in \mathbb{N}$: décompte perturbé
- Mécanisme de bruit défini par les probabilités de transition :
 - $p_{ij} = \mathbb{P}(X' = j | X = i)$
 - Distributions non biaisées et à variance constante
 - $M = [p_{ij}]$ construit avec le package `ptable` [Enderle, 2023]

Méthode Cell Key – 3 - La matrice de transition

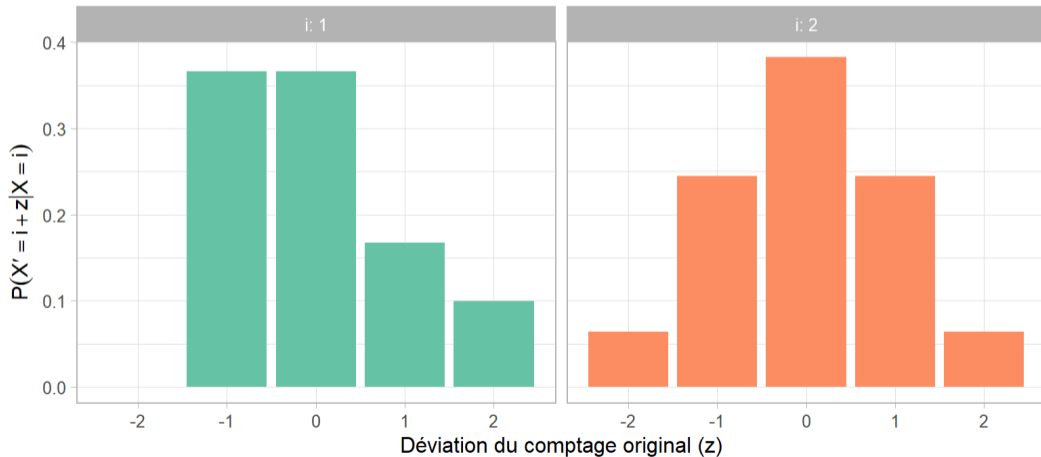
Table 3: Matrice des probabilités de transition: $p_{ij} = \mathbb{P}(X' = j | X = i)$

		$X' = j$				
		0	1	2	3	4
$X = i$	0	1.0000	0.0000	0.0000	0.0000	0.0000
	1	0.3665	0.3665	0.1676	0.0995	0.0000
	2	0.0638	0.2447	0.3830	0.2447	0.0638

Méthode Cell Key – 3 - La matrice de transition

Distributions du bruit injecté selon la valeur original de la case

Pour $D=2$ et $V=1$



Méthode Cell Key – 4 – La table de perturbation

Table 4: Perturbation du tableau pour $D = 2$ et $V = 1$

$X = i$	$X' = j$	ρ_{ij}	$Z = z$	ρ_{lb}	ρ_{ub}
0	0	1	0	0	1
1	0	0.366	-1	0	0.366
1	1	0.366	0	0.366	0.733
1	2	0.168	+1	0.733	0.901
1	3	0.099	+2	0.901	1
$i \geq 2$	$i - 2$	0.064	-2	0	0.064
$i \geq 2$	$i - 1$	0.245	-1	0.064	0.309
$i \geq 2$	i	0.383	0	0.309	0.691
$i \geq 2$	$i + 1$	0.245	+1	0.691	0.936
$i \geq 2$	$i + 2$	0.064	+2	0.936	1

Méthode Cell Key – 5 – Injection du bruit

Table 5: Le tableau bruité

Comm.	Clé de cellule	X	Z	X'
Amiens	0.0295095	2	-2	0
Marseille	0.5577030	3	0	3
Paris	0.8850062	1	+1	2
Total	0.4722187	6	0	6

Évaluation du risque – Du suppressif au perturbatif

Approche suppressive :

- Règle de fréquence : tout décompte inférieur à un seuil est sensible et supprimé
- La suppression secondaire réduit la *perception* du risque à zéro

Approche perturbatrice :

- Les petits décomptes ne sont pas supprimés
- On cherche à limiter le risque de divulgation par inférence des petits comptages

Definition (Métrique de risque d'inférence I)

La capacité d'un attaquant à deviner la vraie valeur à partir de la valeur perturbée peut être évaluée par :

$$q_{ij} = \mathbb{P}(X = i \mid X' = j) = \frac{p_{ij} \times p_i}{q_j} \quad (1)$$

- $p_i = \mathbb{P}(X = i)$
- $q_j = \mathbb{P}(X' = j) = \sum_k p_{kj} p_k$

Remarque :

- Suivant [Enderle et al., 2020]
- Nécessité d'estimer les probabilités a priori p_k

Definition (Métrique de risque d'inférence II)

Soient I un ensemble de décomptes originaux et J un ensemble de décomptes perturbés. La mesure de risque peut s'évaluer comme :

$$q_{IJ} = \mathbb{P}(X \in I \mid X' \in J) \quad (2)$$

- Avec $I = \{1, \dots, s - 1\} \Rightarrow q_{IJ}$ = mesure du risque d'inférer un décompte sensible
- Métrique implémentée dans le package R `ckm`
<https://github.com/InseeFrLab/ckm>

Évaluation du risque – Exemple

Prenons un seuil de fréquence $s = 5$:

- $I = \{1, \dots, s - 1\} = \{1, \dots, 4\}$
- $J = \{1, \dots, s\} = \{1, \dots, 5\}$
- Évaluation du risque : $q_{IJ} = \mathbb{P}(X \in I \mid X' \in J)$
- Priors p_i : distributions empiriques des comptages originaux

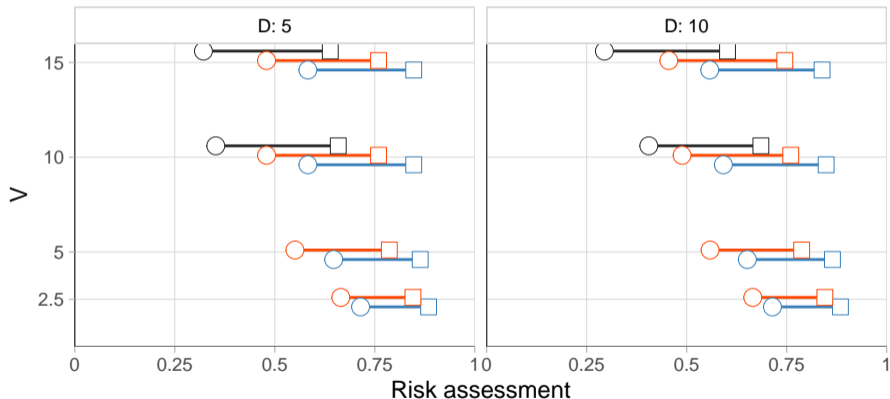
Évaluation du risque – Exemple

- Données de recensement
- Tableaux très détaillés : 5,3 millions de cellules
- Niveau le plus fin = commune \times sexe \times âge \times diplôme
- Tous les tableaux sont publiés en une seule fois
- Pour l'expérience, supposons $s = 5$.

Évaluation du risque – Exemple

Range of risk assessment

Comparison of uniform prior and empirical frequencies (highly ventilated)



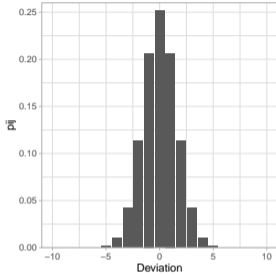
Prior □ Frequency ○ Uniform js ● 0 ● 2 ● 4

- Métriques a posteriori (distances entre données originales et perturbées)
- Métriques a priori basées sur la distribution du bruit :

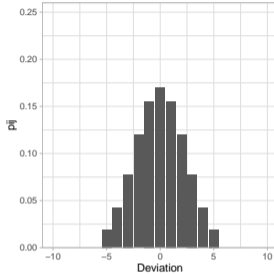
$$\text{pour } d < D, U(d) = \mathbb{P}(|Z| \leq d) \quad (3)$$

Évaluation de l'utilité – Exemple

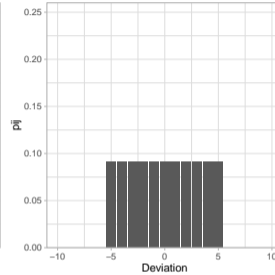
$D=5 - V=2.5 - P(|i-j| \leq 3) = 0.976$



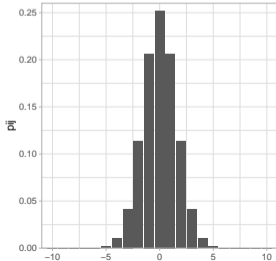
$D=5 - V=5 - P(|i-j| \leq 3) = 0.876$



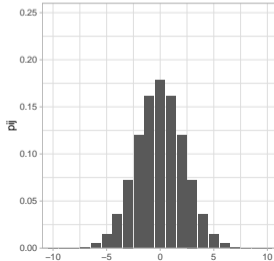
$D=5 - V=10 - P(|i-j| \leq 3) = 0.636$



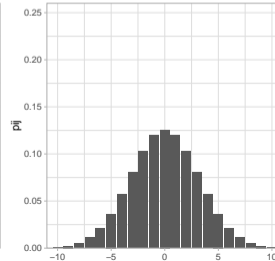
$D=10 - V=2.5 - P(|i-j| \leq 3) = 0.976$



$D=10 - V=5 - P(|i-j| \leq 3) = 0.886$



$D=10 - V=10 - P(|i-j| \leq 3) = 0.732$



Objectif

Appliquer une méthodologie respectant les critères suivants :

- Reproductibilité
- Métriques objectives et interprétables
- Compromis risque-utilité facilitant la prise de décision

Proposition détaillée dans [Jamme, 2025]

La calibration des paramètres: un enjeu important

Cinq étapes principales :

1. Définition des domaines des paramètres (D , V et js)
2. Sélection des données de calibration
3. Arbitrage risque-utilité

Étape 1 : Domaines des paramètres

- Paramètres à fixer :
 - $D \geq s$: écart maximal
 - $V > 0$: variance maximale du bruit
 - Seuil d'interdiction des petites valeurs js :
 - $js \in \llbracket 0; s - 1 \rrbracket$
 - $js = 0$: aucune sortie interdite
 - $js > 0$: réduit le risque de divulgation des petits décomptes
 - $js = s - 1$: proche d'une approche suppressive

Étape 1 : Domaines des paramètres – Expérience

Domaine de recherche des paramètres pour l'exemple ($s = 5$) :

- $D \in \{5; 10\}$
- $js \in \{0, 2, 4\}$
- V : variance maximale du bruit dépendant des paramètres précédents

Étape 2 : Sélection des tableaux

- Choisir un ensemble de tableaux pour la calibration
- Selon le type de diffusion :
 - **Diffusion synchrone** : toutes les données en une fois
 - **Diffusion asynchrone** : certaines données publiées plus tard

Étape 2 : Sélection des tableaux

Deux stratégies possibles :

- **Diffusion synchrone** ⇒ calibration sur tous les tableaux publiés

Étape 2 : Sélection des tableaux

Deux stratégies possibles :

- **Diffusion synchrone** \Rightarrow calibration sur tous les tableaux publiés
- **Diffusion asynchrone** \Rightarrow calibration sur un tableau représentatif

Étape 3 : Évaluation du risque – De l'approche suppressive à perturbative

Approche suppressive :

- Règle de fréquence : tout décompte inférieur à un seuil est sensible et supprimé
- La suppression secondaire réduit la *perception* du risque à zéro

Approche perturbative :

- Les petits décomptes ne sont pas supprimés
- On cherche à limiter le risque de divulgation par inférence des petits comptages

Étape 3 : Compromis risque-utilité

- Visualiser le risque et l'utilité pour toutes les combinaisons de paramètres
- Utiliser des cartes risque-utilité pour la décision
- Sélectionner les paramètres optimaux conciliant confidentialité et perte d'information

Étape 3 : Compromis risque-utilité

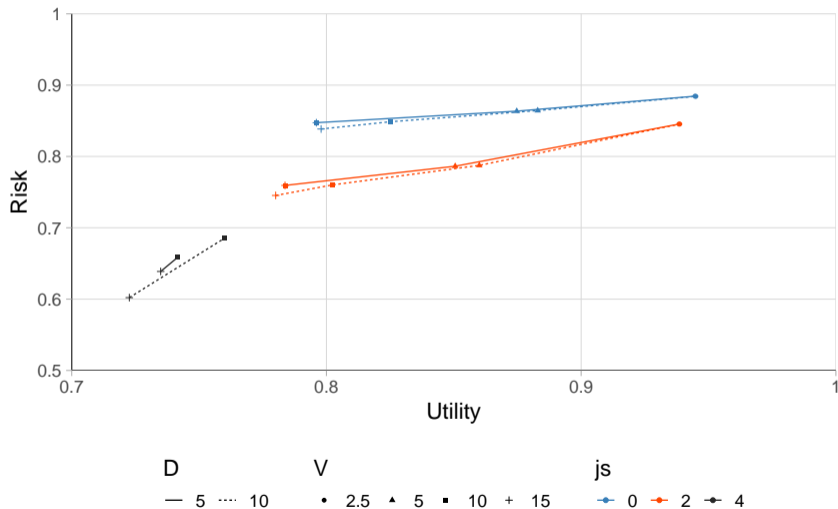






Figure 1: Carte risque-utilité pour le tableau du recensement

Conclusion

- Cadre objectif et transparent pour la calibration
- Aligne le niveau de protection avec la tolérance institutionnelle au risque
- Méthodologie reproductible pour la prise décision
- Implémentation des métriques et de la méthode dans le package ckm :
<https://github.com/InseeFrLab/ckm/tree/main/R>

- Une métrique de risque conservatrice (Hypothèses fortes sur les connaissances à la disposition de l'attaquant).
- Une métrique de risque sensible à la distribution originale des comptages (travaux en cours pour analyser cette sensibilité).

-  Enderle, T. (2023).
R package ptable : Generation of Perturbation Tables for the Cell-Key Method.
-  Enderle, T., Giessing, S., and Tent, R. (2020).
Calculation of Risk Probabilities for the Cell Key Method.
In Domingo-Ferrer, J. and Muralidhar, K., editors, *Privacy in Statistical Databases*, volume 12276, pages 151–165. Springer International Publishing, Cham.
Series Title: Lecture Notes in Computer Science.

-  Fraser, B. and Wooton, J. (2005).
A Proposed Method for Confidentialising Tabular Output to Protect against Differencing.
In *Monographs of Official Statistics: Work Session on Statistical Data Confidentiality*, pages 299–302.
-  Jamme, J. (2025).
A Framework for Cell Key Method Parameters Calibration based on a Risk-Utility trade-off.
In *Expert Meeting on Statistical Data Confidentiality*, Barcelona. UNECE.

Références et remerciements

- Contact : julien.jamme@insee.fr

Merci pour votre attention