
DU SUPPRESSIF AU PERTURBATIF, COMMENT PARAMÉTRER LES MÉTHODES DE BRUITAGE ? UNE PREMIÈRE DÉMARCHÉ UTILISANT LA MÉTHODE DES CLÉS ALÉATOIRES

Julien Jamme ()*

() Insee, Département des méthodes statistiques, Insee*

julien.jamme@insee.fr

Domaines : Confidentialité.

Résumé

À l'Insee, des méthodes suppressives (regroupement ou blanchiment de cases) sont majoritairement utilisées pour limiter les risques de divulgation d'informations confidentielles lors de la publication de tableaux statistiques. Aujourd'hui, ces méthodes atteignent certaines de leurs limites, en particulier lorsque les produits de diffusion deviennent complexes ([1]). Certaines méthodes perturbatrices, en particulier la méthode des clés aléatoires, permettent de combler ces lacunes. Or, les règles du secret statistique sont particulièrement adhérentes aux méthodes suppressives: une case est supprimée si elle ne respecte pas le critère choisi. Comment, en utilisant des méthodes perturbatrices, s'assurer, par exemple, de respecter la règle de fréquence, celle qui fixe un nombre de contributeurs minimal à une case pour pouvoir la diffuser ? Le bruit injecté par ce type de méthode est en général piloté par un ensemble de paramètres. Comment assurer un choix optimal de ces paramètres, c'est-à-dire un choix qui offre les garanties nécessaires de protection tout en assurant un qualité suffisante de l'information transmise au public ?

Nous nous attacherons ici à étudier le cas de l'application de la méthode des clés aléatoires ([2], [3]) à des comptages issus de sources exhaustives. Cette méthode repose sur deux éléments fondamentaux: des clés individuelles aléatoires qui introduisent l'aléa dans le processus tout en assurant une certaine cohérence des requêtes entre elles et une matrice de probabilités de transition qui définit la façon dont les comptages sont perturbés. Pour définir ces distributions de probabilité, il est nécessaire de fixer - a minima - deux paramètres: la déviation maximale des comptages et la variance de la distribution de probabilité. Le choix de ces paramètres est réalisé pour assurer le meilleur compromis entre protection et utilité, les deux termes nécessitant chacun une métrique permettant de les objectiver.

Les probabilités de transition qui définissent le mécanisme de perturbation peuvent servir à estimer les deux plateaux de la balance. Elles fournissent directement une mesure d'utilité et, en les inversant avec la formule de Bayes, elles nous permettent d'estimer la capacité qu'aurait un attaquant d'inférer une valeur sensible à partir d'un comptage diffusé.

Notre démarche consiste ainsi à comparer l'effet sur le niveau de protection et sur la qualité de l'information transmise d'un ensemble de paramètres appliqués sur un ou plusieurs tableaux représentatifs de la source étudiée. Les résultats montrent en particulier la nécessité d'utiliser un

paramètre supplémentaire permettant d'interdire l'apparition de petits comptages et ainsi limiter la capacité d'inférence des attaquants. Le choix de ce seuil d'interdiction est d'autant plus important qu'il a un impact non négligeable sur le niveau de variance injecté dans les données et donc sur la qualité des informations diffusées auprès du public.

Bibliographie

- [1] M. CHEVALIER, A. HACHID et J. JAMME, « Données sur les quartiers prioritaires de la politique de la ville (qpv): une nouvelle méthode pour protéger le secret statistique », jan. 2025.
- [2] B. FRASER et J. WOOTON, « A proposed method for confidentialising tabular output to protect against differencing », in *Monographs of Official Statistics: Work Session on Statistical Data Confidentiality*, p. 299–302, 2005.
- [3] J. JAMME, « La méthode des clés aléatoires (cell key method) », fév. 2025.