Confidentialité différentielle à risque : Relier les sources d'aléa et un budget de confidentialité

Ashish Dandekar
DI ENS, ENS, CNRS, Université PSL
& Inria & National University of Singapore
Paris, France & Singapour, Singapour
ashishd@comp.nus.edu.sg

Debabrota Basu
Chalmers University of Technology
& Inria
Göteborg, Suède & Lille, France
debabrota.basu@inria.fr

Pierre Senellart
DI ENS, ENS, CNRS, Université PSL
& Inria & Institut Universitaire de France
Paris, France
pierre@senellart.com

Stéphane Bressan
National University of Singapore

Singapour, Singapour
steph@nus.edu.sg

Dwork et al. [2] quantifient le niveau ε de confidentialité dans la *confidentialité ε-différentielle* comme une borne supérieure sur la perte de confidentialité, dans le pire des cas, obtenue par un mécanisme préservant la confidentialité. De manière générale, un mécanisme préservant la confidentialité perturbe les résultats en y ajoutant une certaine quantité de bruit aléatoire. La calibration du bruit dépend de la sensitivité de la requête et du niveau de confidentialité spécifié. Dans un scénario du monde réel, un coordinateur des données doit spécifier un niveau de confidentialité qui atteint un compromis entre les besoins des utilisateurs et les contraintes monétaires de l'entreprise. Par exemple, Garfinkel et al. [3] rapportent les difficultés rencontrées en déployant la confidentialité différentielle comme définition de confidentialité par le bureau du recensement des États-Unis. Ils insistent sur le manque de méthodes analytiques pour choisir le niveau de confidentialité. Ils fournissent également des études empiriques qui montrent la perte d'utilité obtenue en utilisant des mécanismes préservant la confidentialité.

Nous adressons le dilemme d'un coordinateur de données de deux manières. Premièrement, nous proposons une quantification probabiliste des niveaux de confidentialité. La quantification probabiliste des niveaux de confidentialité fournit au coordinateur des données une façon de prendre des risques quantifiés, en respectant un niveau d'utilité des données. Nous nous référons à cette quantification probabiliste par le terme de *confidentialité à risque* (Définition 1). Nous dérivons également un théorème de composition qui met en œuvre la confidentialité à risque. Deuxièmement, nous proposons un modèle de coût qui relie le niveau de confidentialité à un budget monétaire. Ce modèle de coût aide le coordinateur des données à choisir un niveau de confidentialité contraint par un budget estimé, et vice-versa. La convexité du modèle de coût proposé assure l'existence d'une confidentialité à risque unique qui minimise le budget. Nous montrons que la composition avec une confidentialité à risque optimale fournit des garanties de confidentialité plus fortes que le théorème classique de composition avancée [2]. Finalement, nous illustrons notre travail par un scénario réaliste qui démontre par l'exemple comment le coordinateur des données peut éviter de surestimer le budget en utilisant le modèle de coût proposé pour la confidentialité à risque. Pour plus de détails, se référer à la version longue de cet article [1].

La quantification probabiliste des niveaux de confidentialité dépend de deux sources d'aléa : l'*aléa explicite* induit par la distribution de bruit et l'*aléa implicite* de la distribution génératrice de données. Souvent, ces deux sources sont couplées l'une à l'autre. Nous imposons des formes analytiques des deux sources d'aléa ainsi qu'une représentation analytique de la requête pour dériver une garantie de confidentialité. Le calcul de la quantification probabiliste est, en général, une tâche difficile. Bien qu'il existe des définitions multiples de confidentialité probabiliste dans la littérature [4, 5], il manque une quantification analytique qui relie l'aléa et le niveau de confidentialité d'un mécanisme préservant la confidentialité.

Définition 1 (Confidentialité à risque). *Pour une distribution génératrice de données $\mathcal{G}$, un mécanisme préservant la confidentialité $\mathcal{M}$, équipé d'une requête f et de paramètres Θ, satisfait la confidentialité ε-différentielle avec une* confidentialité différentielle *$0 \leqslant \gamma \leqslant 1$ si, pour tous $Z \subseteq Image(\mathcal{M})$ et x, y échantillonés de $\mathcal{G}$ tels que $x \sim y$:*

$$\Pr\left[\left|\ln \frac{\Pr(\mathcal{M}(f,\Theta)(x) \in Z)}{\Pr(\mathcal{M}(f,\Theta)(y) \in Z)}\right| > \varepsilon\right] \leqslant \gamma, \tag{1}$$

où la probabilité externe est calculée par rapport à l'espace de probabilités $\text{Image}(\mathcal{M} \circ \mathcal{G})$ *obtenu en appliquant le mécanisme préservant la confidentialité $\mathcal{M}$ sur la distribution génératrice de données $\mathcal{G}$.*

Autant que nous en le sachions, nous sommes les premiers à dériver une confidentialité à risque pour le mécanisme de Laplace [2], largement utilisé. Nous dérivons également un théorème de composition pour la confidentialité à risque. C'est un cas particulier du théorème de composition avancée [2] qui traite d'un usage séquentiel et adaptatif de mécanismes préservant la confidentialité. Ces résultats et leurs preuves sont disponibles dans [1].

Le niveau de confidentialité proposé par le cadre de la confidentialité différentielle est une quantité trop abstraite pour être intégrée dans un contexte d'affaires. Nous analysons et listons les conditions d'un modèle de coût qui transforme le niveau de confidentialité en un budget monétaire. Nous l'illustrons (équation (2))

en choisissant une fonction qui satisfait ces conditions. Dans l'équation (2), E dénote le budget de compensation qu'une entreprise doit payer à chaque partie prenante dans le cas d'une violation des données à caractère personnel quand les données sont traitées sans garantie de confidentialité prouvée, et E_ε^{cd} est le budget de compensation qu'une entreprise doit payer à chaque partie prenante dans le cas d'une violation des données à caractère personnel quand les données sont traitées par un mécanisme avec confidentialité ε-différentielle. $E_{\min}$ et c sont des hyper-paramètres réglables. Le lecteur pourra se référer à [1] pour plus d'explications.

$$E_\varepsilon^{cd} \triangleq E_{\min} + Ee^{-\frac{c}{\varepsilon}}. \quad (2)$$

La fonction choisie pour le modèle de coût pour la quantification probabiliste du modèle de coût est convexe en le niveau de confidentialité. Ainsi, elle conduit à un niveau de confidentialité probabiliste unique qui minimise le coût. Nous illustrons ceci par un scénario réaliste d'une entreprise respectant le RGPD qui a besoin d'une estimation du budget de compensation qu'elle devra payer aux parties prenantes dans le cas malheureux d'une violation de données personnelles. Cette illustration montre que l'usage des niveaux de confidentialité probabilistes évite de surestimer le budget de compensation sans sacrifier l'utilité.

Nous évaluons de plus les garanties de confidentialité en utilisant un calcul de la confidentialité à risque pour le mécanisme de Laplace. Nous comparons quantitativement la composition sous confidentialité à risque optimale, estimée avec les modèle de coût, avec les mécanismes traditionnels de composition – de base et avancé [2]. Nous observons de plus fortes garanties de confidentialité que celles obtenues par la composition avancée, sans sacrifier l'utilité du mécanisme. Nous adaptons également le système PATE [6], qui utilise la technique de comptabilité des moments de l'état de l'art, pour utiliser la confidentialité à risque. Nous montrons expérimentalement que la confidentialité à risque optimale fournit de meilleures garanties que la comptabilité des moments.

En conclusion, les bénéfices de la quantification probabiliste, c.-à-d., de la confidentialité à risque, sont doubles. Non seulement elle quantifie le niveau de confidentialité pour un mécanisme préservant la confidentialité donné, mais elle facilite également la prise de décision dans des problèmes qui se focalisent sur le compromis confidentialité–utilité et sur la minimisation du budget de compensation.

REMERCIEMENTS

Ce travail a été soutenu par la National Research Foundation (NRF) de Singapour, Corporate Laboratory@University Scheme, National University of Singapore et Singapore Telecommunications Ltd. Ces recherches ont également été financées par le projet BioQOP de l'ANR française (ANR-17-CE39-0006).

RÉFÉRENCES

[1] Ashish Dandekar, Debabrota Basu, and Stéphane Bressan. 2021. Differential Privacy at Risk : Bridging Randomness and Privacy Budget. *Proceedings on Privacy Enhancing Technologies* 1 (2021). https://doi.org/10.2478/popets-2021-0005

[2] Cynthia Dwork, Aaron Roth, et al. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science* 9, 3–4 (2014), 211–407.

[3] Simson L Garfinkel, John M Abowd, and Sarah Powazek. 2018. Issues Encountered Deploying Differential Privacy. *arXiv preprint arXiv :1809.02201* (2018).

[4] Rob Hall, Alessandro Rinaldo, and Larry Wasserman. 2012. Random Differential Privacy. *Journal of Privacy and Confidentiality* 4, 2 (2012), 43–59.

[5] Ashwin Machanavajjhala, Daniel Kifer, John Abowd, Johannes Gehrke, and Lars Vilhuber. 2008. Privacy : Theory meets practice on the map. In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on.* IEEE, 277–286.

[6] Nicolas Papernot, Martín Abadi, Úlfar Erlingsson, Ian J. Goodfellow, and Kunal Talwar. 2017. Semi-supervised Knowledge Transfer for Deep Learning from Private Training Data. In *5th International Conference on Learning Representations, ICLR 2017, Toulon, France, April 24-26, 2017, Conference Track Proceedings.*