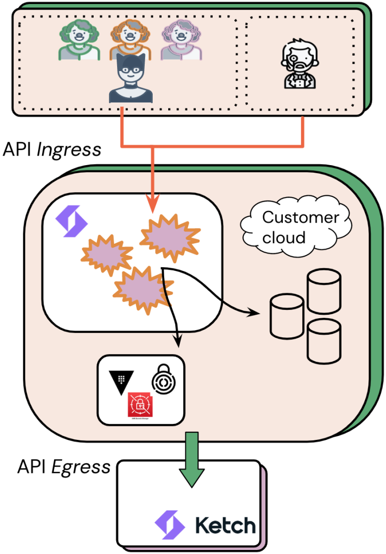
Toward a Unifying Information-Theoretic Framework for Re-identification Risk Quantification

Tayler Blake
taylerablake.github.io
Ketch, Inc.

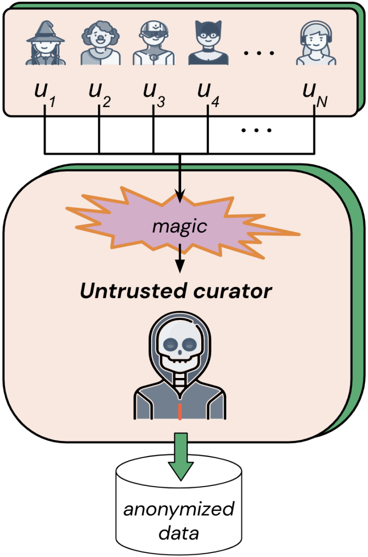
December 13, 2022

Introduction

Re-identification probabilities: elusive requisites



Re-identification probabilities: elusive requisites



The anonymization framework

$$\overset{\text{Subject}}{U \in \mathcal{U}} \xrightarrow[p_{X|U}]{} \overset{\text{Personal Data}}{X \in \mathcal{X}} \longrightarrow \boxed{\text{Anonymization mechanism } \mathcal{Q}} \xrightarrow[p^{\mathcal{Q}}_{Y|X}]{} \overset{\text{Anonymized Data}}{Y \in \mathcal{Y}}$$

The anonymization framework

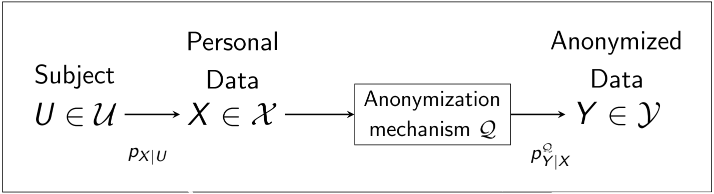
Subject | Personal Data | | Anonymized Data

$$U \in \mathcal{U} \xrightarrow[p_{X|U}]{} X \in \mathcal{X} \longrightarrow \boxed{\text{Anonymization mechanism } \mathcal{Q}} \xrightarrow[p^{\mathcal{Q}}_{Y|X}]{} Y \in \mathcal{Y}$$

$\mathcal{U} = \{u_1, \ldots, u_N\}$

The anonymization framework

$\mathcal{X} = \{x_1, \ldots, x_N\}$



$\mathcal{U} = \{u_1, \ldots, u_N\}$

The anonymization framework

$\boxed{\mathcal{Q} : \mathcal{X} \to \mathcal{Y}}$

$\boxed{\mathcal{X} = \{x_1, \dots, x_N\}}$ $\boxed{y_i = \mathcal{Q}(x_i)}$

Subject | Personal Data | | Anonymized Data

$$U \in \mathcal{U} \xrightarrow[p_{X|U}]{} X \in \mathcal{X} \longrightarrow \boxed{\text{Anonymization mechanism } \mathcal{Q}} \xrightarrow[p^{\mathcal{Q}}_{Y|X}]{} Y \in \mathcal{Y}$$

$\boxed{\mathcal{U} = \{u_1, \dots, u_N\}}$

The anonymization framework

$\mathcal{Q} : \mathcal{X} \to \mathcal{Y}$

$\mathcal{X} = \{x_1, \ldots, x_N\}$

$y_i = \mathcal{Q}(x_i)$

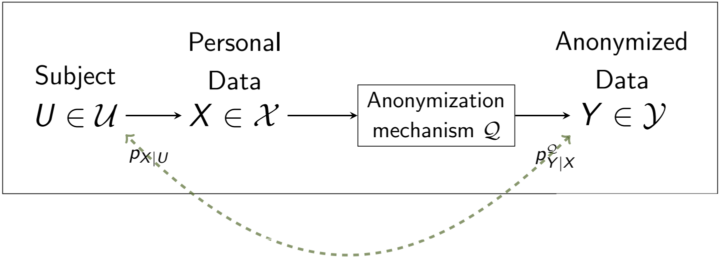
Subject | Personal Data | Anonymized Data

$$\underset{\text{Subject}}{U \in \mathcal{U}} \xrightarrow[p_{X|U}]{} \underset{\text{Personal Data}}{X \in \mathcal{X}} \longrightarrow \boxed{\text{Anonymization mechanism } \mathcal{Q}} \xrightarrow[p^{\mathcal{Q}}_{Y|X}]{} \underset{\text{Anonymized Data}}{Y \in \mathcal{Y}}$$

$\mathcal{Y} = \{y_1, \ldots, y_N\}$

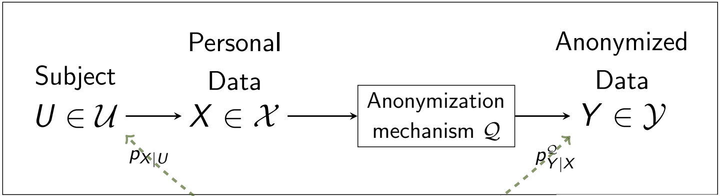
$\mathcal{U} = \{u_1, \ldots, u_N\}$

Evaluating re-identification risk



$$E_Y\left[\max_{u_i \in \mathcal{U}} P\left(U = u_i | Y\right)\right]$$

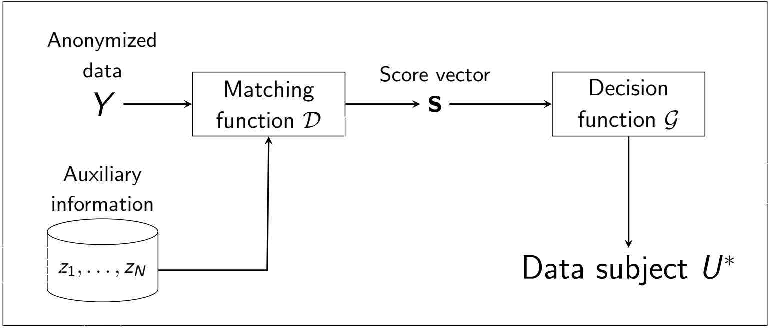
Evaluating re-identification risk



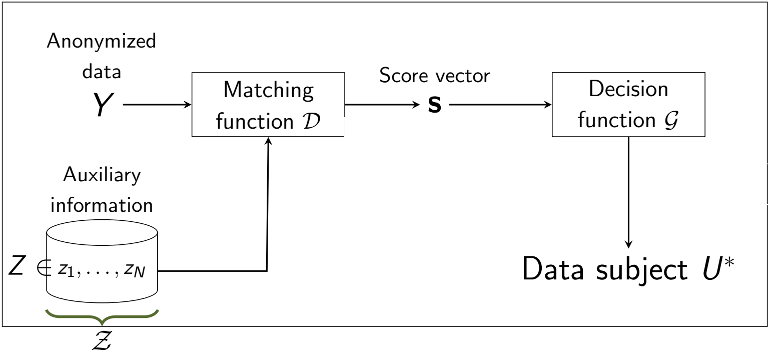
$$\text{PIE} = \boxed{I\left(U,Y\right) = \sum_{\mathcal{U}} \sum_{\mathcal{Y}} p_{U,Y}\left(u,y\right) \log \frac{p_{U,Y}\left(u,y\right)}{p_U\left(u\right) p_Y\left(y\right)}}$$

A general adversarial re-identification framework

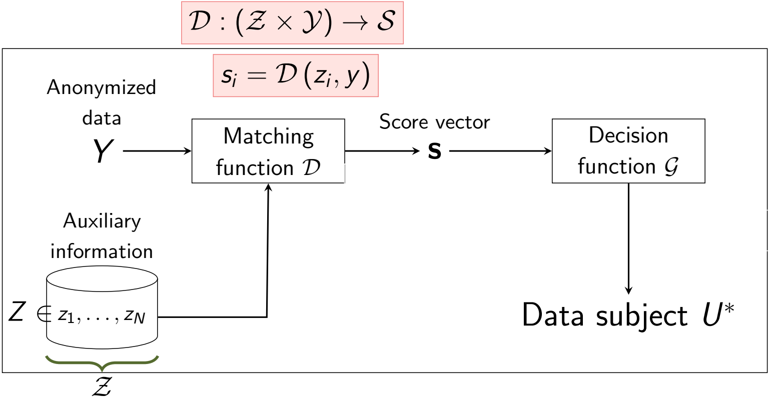
Re-identification framework



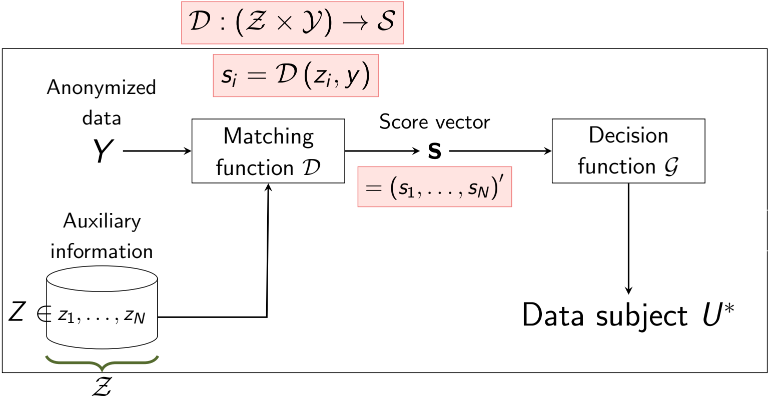
Re-identification framework



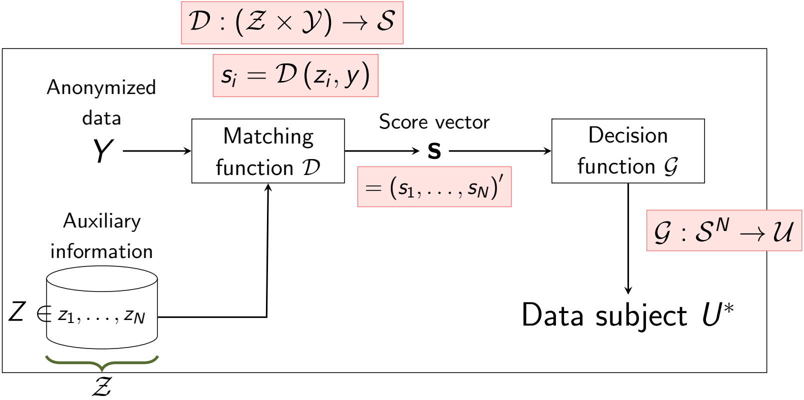
Re-identification framework



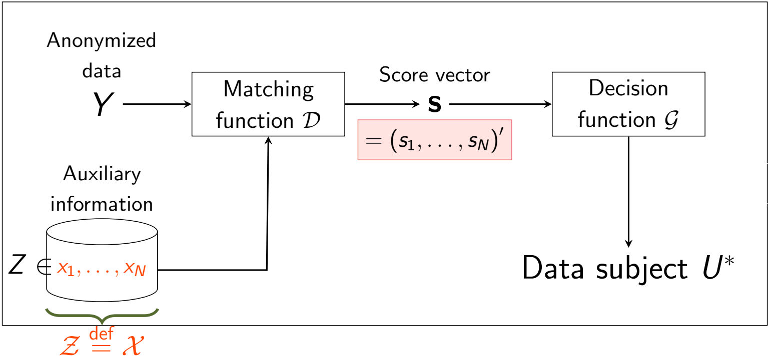
Re-identification framework



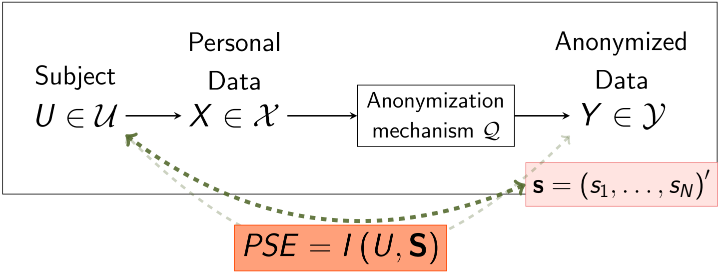
Re-identification framework



The maximum-knowledge intruder



Evaluating re-identification risk



Bounding posterior re-identification probabilities

Personal System Entropy (PSE)

The *personal system entropy* $\mathrm{PSE} = I(U, \mathbf{S})$ is a lower bound for the PIE.

Proposition

For any matching function $\mathcal{D}$ and any auxiliary information $z_1, \ldots, z_N$,

$$I(U, \mathbf{S}) \leq I(U, Y)$$

with equality if and only if U, $\mathbf{S}$, and Y form the Markov chain $U \to \mathbf{S} \to Y$ (i.e. $\mathbf{S}$ is a sufficient statistic for U).

e.g. if $\mathbf{s} = (q_1(y), \ldots, q_N(y))'$ where $q_i(y) = P(Y = y | U = u_i)$, then $\mathrm{PIE} = \mathrm{PSE}$.

Bayes re-identification error rate

Proposition (Bayes error, PIE and PSE)

$$\beta_{U|\mathbf{S}} \geq 1 - \frac{I\left(U, \mathbf{S}\right) + 1}{\log\left(1 - \beta_U\right)} \geq 1 - \frac{I\left(U, Y\right) + 1}{\log\left(1 - \beta_U\right)}.$$

where

$$\beta_U = 1 - \max_{u_i \in \mathcal{U}} P\left(U = u_i\right) = \text{Bayes error probability before observing } \mathbf{S}$$

$$\beta_{U|\mathbf{S}} = 1 - E_{\mathbf{S}}\left[\max_{u_i \in \mathcal{U}} P\left(U = u_i | \mathbf{S}\right)\right] = \text{Bayes error probability after observing } \mathbf{S}$$

Bayes re-identification error rate

Then!

$$1 - \beta_{U|\mathbf{S}} \leq \underbrace{\frac{I(U, \mathbf{S}) + 1}{\log(1 - \beta_U)}}_{\substack{\text{we can estimate this} \\ \text{using the adorable} \\ \text{result on the next slide}}} \leq \frac{I(U, Y) + 1}{\log(1 - \beta_U)}$$

When p_U is Uniform, this becomes

$$1 - \beta_{U|\mathbf{S}} \leq \frac{I(U, \mathbf{S}) + 1}{\log N} \leq \frac{I(U, Y) + 1}{\log N}$$

Estimation of the PSE

$$\text{Let } \mathcal{D}(X_i, Y_i) \sim \underbrace{f_G}_{\substack{\text{genuine}\\\text{score}\\\text{distribution}}}, \quad \mathcal{D}(X_i, Y_j) \sim \underbrace{f_I}_{\substack{\text{imposter}\\\text{score}\\\text{distribution}}} \text{ for } i \neq j.$$

Theorem (1)

Let f_G be a one-dimensional genuine score distribution and f_I be a one-dimensional imposter score distribution. Then

$$I(U, \mathbf{S}) \to D(f_G || f_I) \text{ as } N \to \infty,$$

where $D(f_G||f_I)$ denotes the Kullback-Leibler divergence of f_G from f_I.

References

[1] Michele Bezzi. An entropy based method for measuring anonymity. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, pages 28–32. IEEE, 2007.

[2] Anil K Jain, Arun A Ross, and Karthik Nandakumar. *Introduction to biometrics*. Springer Science & Business Media, 2011.

[3] Paul Cuff and Lanqing Yu. Differential privacy as a mutual information constraint. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 43–54, 2016.

[4] Amir Dembo, Thomas M Cover, and Joy A Thomas. Information theoretic inequalities. *IEEE Transactions on Information theory*, 37(6):1501–1518, 1991.

[5] Josep Domingo-Ferrer, Krishnamurty Muralidhar, and Maria Bras-Amorós. General confidentiality and utility metrics for privacy-preserving data publishing based on the permutation model. *IEEE Transactions on Dependable and Secure Computing*, 2020.

[6] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality*, 7(3):17–51, 2016.

[7] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[8] Josep Domingo-Ferrer, Sara Ricci, and Jordi Soria-Comas. Disclosure risk assessment via record linkage by a maximum-knowledge attacker. In *2015 13th Annual Conference on Privacy, Security and Trust (PST)*, pages 28–35. IEEE, 2015.

[9] Josep Domingo-Ferrer and Vicenc Torra. A quantitative comparison of disclosure control methods for microdata. *Confidentiality, disclosure and data access: theory and practical applications for statistical agencies*, pages 111–134, 2001.

[10] Josep Domingo-Ferrer and Krishnamurty Muralidhar. New directions in anonymization: permutation paradigm, verifiability by subjects and intruders, transparency to users. *Information Sciences*, 337:11–24, 2016.

[11] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[12] Stephen E Fienberg and Paul W Holland. On the choice of flattening constants for estimating multinomial probabilities. *Journal of Multivariate Analysis*, 2(1):127–134, 1972.

[13] Anco Hundepool, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Eric Schulte Nordholt, Keith Spicer, and Peter-Paul De Wolf. *Statistical disclosure control*. John Wiley & Sons, 2012.

[14] Edwin T Jaynes. Information theory and statistical mechanics. *Physical review*, 106(4):620, 1957.

[15] Alexei Kounine and Michele Bezzi. Assessing disclosure risk in anonymized datasets. *Proceedings of FloCon*, 2008.

[16] Dennis V Lindley. The bayesian analysis of contingency tables. *The Annals of Mathematical Statistics*, pages 1622–1643, 1964.

[17] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pages 106–115. IEEE, 2007.

[18] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1):3–es, 2007.

[19] Takao Murakami, Atsunori Kanemura, and Hideitsu Hino. Group sparsity tensor factorization for re-identification of open mobility traces. *IEEE Transactions on Information Forensics and Security*, 12(3):689–704, 2016.

[20] Nicolas Ruiz, Krishnamurty Muralidhar, and Josep Domingo-Ferrer. On the privacy guarantees of synthetic data: a reassessment from the maximum-knowledge attacker perspective. In *International Conference on Privacy in Statistical Databases*, pages 59–74. Springer, 2018.

[21] Takao Murakami and Kenta Takahashi. Toward evaluating re-identification risks in the local privacy model. *arXiv preprint arXiv:2010.08238*, 2020.

[22] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125. IEEE, 2008.

[23] Arvind Narayanan and Vitaly Shmatikov. How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*, 2006.

[24] Jerome P Reiter. Estimating risks of identification disclosure in microdata. *Journal of the American Statistical Association*, 100(472):1103–1112, 2005.

[25] Lalitha Sankar, S Raj Rajagopalan, and H Vincent Poor. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security*, 8(6):838–852, 2013.

[26] Pierangela Samarati and Latanya Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. 1998.

[27] Gerard Salton and Christopher Buckley. Term-weighting approaches in automatic text retrieval. *Information processing & management*, 24(5):513–523, 1988.

[28] Latanya Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):571–588, 2002.

[29] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[30] Pang-Ning Tan, Michael Steinbach, and Vipin Kumar. *Introduction to data mining*. Pearson Education India, 2016.

[31] Vicenç Torra, John M Abowd, and Josep Domingo-Ferrer. Using mahalanobis distance-based record linkage for disclosure risk assessment. In *International Conference on Privacy in Statistical Databases*, pages 233–242. Springer, 2006.

[32] Article. General data protection regulation 2016, 4(1) GDPR.

[33] PIPEDA, S.C. 2000, c.5 2(1) (Can.). Personal information protection and electronic documents act, 2000.

[34] Sergio Verdú et al. Generalizing the fano inequality. *IEEE Transactions on Information Theory*, 40(4):1247–1251, 1994.

[35] Isabel Wagner and David Eckhoff. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)*, 51(3):1–38, 2018.

[36] Isabel Wagner and Eerke Boiten. Privacy risk assessment: from art to science, by metrics. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 225–241. Springer, 2018.

[37] Qing Wang, Sanjeev R Kulkarni, and Sergio Verdú. Divergence estimation for multidimensional densities via k-nearest-neighbor distances. *IEEE Transactions on Information Theory*, 55(5):2392–2405, 2009.

[38] D. Randall Wilson and Tony R. Martinez. Improved heterogeneous distance functions. *Journal of artificial intelligence research*, 6:1–34, 1997.