Computational Differential Privacy for Encrypted Databases Supporting Linear Queries

Ferran Alborch Escobar [1,2,3]

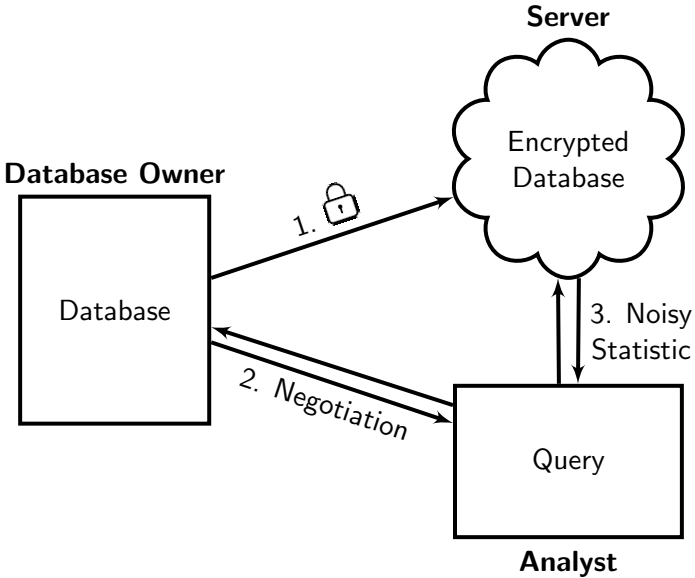
[1]Orange Innovation, Caen, France

[2]Télécom Paris, Palaiseau, France

[3]LIRMM, Montpellier, France

October 17th 2023

Motivation I



Motivation II: Previous works

- Agarwal *et al.* [AHKM19]
  - Histogram queries.
  - Based on Structured encryption.
- Bakas *et al.* [BMD22]
  - Summation queries.
  - Based on Homomorphic encryption.
- Either Server **or** Analyst are malicious.
  - For Server security of encryption scheme.
  - For Analyst standard (statistical) differential privacy.
  - Collusion?

(Randomized) Functional encryption [BSW11, GJKS15]

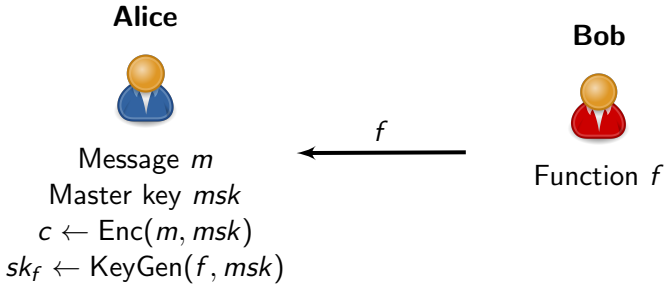
Alice

Message m
Master key msk

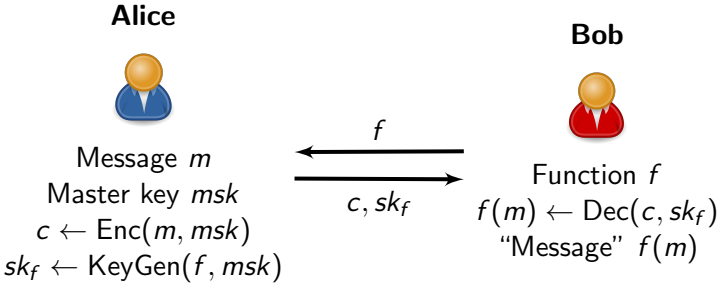
Bob

Function f

(Randomized) Functional encryption [BSW11, GJKS15]



(Randomized) Functional encryption [BSW11, GJKS15]

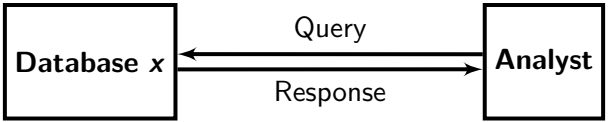


Security of (Randomized) Functional encryption

- Indistintinguishability vs. Simulation-based
  - Simulation-based stronger and more composable
  - Impossibility results for simulation-based
- Selective vs. (Semi)Adaptive
  - (Semi)Adaptive stronger
  - Impossibility results for (Semi)adaptive

Differential Privacy [DMNS06]

Usual data analysis:



Differential Privacy [DMNS06]

Private data analysis:

For example

$$\underbrace{\underbrace{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}_{\text{statistic}} + e}_{\text{noisy statistic}}$$

Differential Privacy [DMNS06]

Private data analysis:

For example

$$\underbrace{\underbrace{\langle \boldsymbol{x}, \boldsymbol{y} \rangle}_{\text{statistic}} + e}_{\text{noisy statistic}}$$

For $\boldsymbol{x}, \boldsymbol{x}'$ adjacent databases (statistical property)

$$\Pr\left[\mathcal{M}(\boldsymbol{x}) \in S\right] \leq \exp(\epsilon) \cdot \Pr\left[\mathcal{M}(\boldsymbol{x}') \in S\right] + \delta$$

Results I: Generic results

- Generic RFE scheme instantiating "statistical" private mechanism
  - $\mathcal{M}'(x, f) = f(x) + D$ a statistical DP mechanism
  - RFE such that $f(x) + D \leftarrow \mathsf{Dec}(c_x, sk_f)$

Results I: Generic results

- Generic RFE scheme instantiating "statistical" private mechanism
  - $\mathcal{M}'(x, f) = f(x) + D$ a statistical DP mechanism
  - RFE such that $f(x) + D \leftarrow \mathsf{Dec}(c_x, sk_f)$

- Result for generic functional encryption

Theorem

If the randomized functional encryption scheme RFE *instantiating* $\mathcal{M}'$ *(which is statistically* DP *for* Q *queries) holds simulation soundness for 1 database, it is computationally differentially private for 1* **encrypted database** *and* Q *queries.*

  - Proof intuition: Reduction to the "statistical" mechanism by using simulators from RFE

Results II: Randomized Inner-Product Functional Encryption

- Instantiation for Randomized Inner Product functional encryption
  - From generic (deterministic) Inner Product functional encryption and generic distribution.

$\mathbf{SetUp}^{\mathsf{RIPFE}}(1^\kappa)$:
$\boldsymbol{u} \xleftarrow{\$} \mathbb{G}^\ell$
$(\mathsf{msk}^{\mathsf{IPFE}}, \mathit{param}^{\mathsf{IPFE}}) \leftarrow \mathsf{SetUp}^{\mathsf{IPFE}}(1^\kappa)$
$\mathit{Output}\ (\mathsf{msk}^{\mathsf{RIPFE}}, \mathit{param}^{\mathsf{RIPFE}})$
$=((\boldsymbol{u}, \mathsf{msk}^{\mathsf{IPFE}}), \mathit{param}^{\mathsf{IPFE}})$

$\mathbf{KeyGen}^{\mathsf{RIPFE}}(\mathsf{msk}^{\mathsf{RIPFE}}, \boldsymbol{y})$:
$e_{\boldsymbol{y}} \leftarrow D$
$u'_{\boldsymbol{y}} \xleftarrow{\$} \mathbb{G}$
$d'_{\boldsymbol{y}} \leftarrow e_{\boldsymbol{y}} + u'_{\boldsymbol{y}}$
$sk_{\boldsymbol{y}} \leftarrow \mathsf{KeyGen}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{y})$
$zk_{\boldsymbol{y}} \leftarrow \langle \boldsymbol{u}, \boldsymbol{y} \rangle + u'_{\boldsymbol{y}}$
$\mathit{Output}\ sk_{\boldsymbol{y}}^{\mathsf{RIPFE}} = (d'_{\boldsymbol{y}}, sk_{\boldsymbol{y}}, zk_{\boldsymbol{y}})$

$\mathbf{Enc}^{\mathsf{RIPFE}}(\mathsf{msk}^{\mathsf{RIPFE}}, \boldsymbol{x})$:
$\boldsymbol{d} \leftarrow \boldsymbol{x} + \boldsymbol{u}$
$c_{\boldsymbol{d}} \leftarrow \mathsf{Enc}^{\mathsf{IPFE}}(\mathsf{msk}^{\mathsf{IPFE}}, \boldsymbol{d})$
$\mathit{Output}\ c_{\boldsymbol{d}}$

$\mathbf{Dec}^{\mathsf{RIPFE}}(c_d, sk_{\boldsymbol{y}}^{\mathsf{RIPFE}})$:
$\langle \boldsymbol{d}, \boldsymbol{y} \rangle \leftarrow \mathsf{Dec}^{\mathsf{IPFE}}(c_{\boldsymbol{d}}, sk_{\boldsymbol{y}})$
$\mathit{Output}\ \langle \boldsymbol{d}, \boldsymbol{y} \rangle + d'_{\boldsymbol{y}} - zk_{\boldsymbol{y}}$

Results III: Implementation

- Proof of concept implementation using the DDH-based IPFE scheme in [ALMT20] coded in C using the CiFEr library [BHTS21].

	Database entries	msk	c_x	sk_y
Sizes	100	150 KB	37 KB	1 KB
	1 000	1 MB	375 KB	1 KB
	10 000	14 MB	3 MB	1 KB
	100 000	146 MB	36 MB	1 KB

Table: Sizes of each element.

Results III: Implementation

- Proof of concept implementation using the DDH-based IPFE scheme in [ALMT20] coded in C using the CiFEr library [BHTS21].

	Database entries	SetUp	Encrypt	KeyGen	Decrypt
Comp. time	100	1.0236 s	0.9993 s	0.0001 s	0.5127 s
	1 000	9.9442 s	9.9193 s	0.0001 s	0.5799 s
	10 000	95.784 s	95.6347 s	0.0024 s	0.6206 s
	100 000	960.79 s	959.62 s	0.0252 s	2.211 s

Table: Times computed using ONE core i9-12900K (3.2Ghz).

Thank you for your attention

Questions?

Future works:

- Quadratic functionalities
- Dynamic databases
- Proof with Indistinguishability-based security


Archita Agarwal, Maurice Herlihy, Seny Kamara, and Tarik Moataz.
Encrypted databases for differential privacy.
Proceedings on Privacy Enhancing Technologies, 2019(3):170–190, 2019.


Shweta Agrawal, Benoît Libert, Monosij Maitra, and Radu Titiu.
Adaptive simulation security for inner product functional encryption.
In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 34–64, Cham, 2020. Springer.


Manca Bizjak, Jan Hartman, Marc Tilen, and Miha Stopar.
Cifer - functional encryption library, February 2021.


Alexandros Bakas, Antonis Michalas, and Tassos Dimitriou.
Private lives matter: A differential private functional encryption scheme.
In *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*, page 300–311, New York, NY, 2022. Association for Computing Machinery.


Dan Boneh, Amit Sahai, and Brent Waters.
Functional encryption: Definitions and challenges.

In Yuval Ishai, editor, *Theory of Cryptography*, pages 253–273, Berlin, Heidelberg, 2011. Springer.


Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith.
Calibrating noise to sensitivity in private data analysis.
In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 265–284, Berlin, Heidelberg, 2006. Springer.


Vipul Goyal, Abhishek Jain, Venkata Koppula, and Amit Sahai.
Functional encryption for randomized functionalities.
In Yevgeniy Dodis and Jesper Buus Nielsen, editors, *Theory of Cryptography*, pages 325–351, Berlin, Heidelberg, 2015. Springer.