DIFFERENTIAL PRIVACY FOR FREE?

HARNESSING THE NOISE IN APPROXIMATE HOMOMORPHIC ENCRYPTION

TALK PLAN

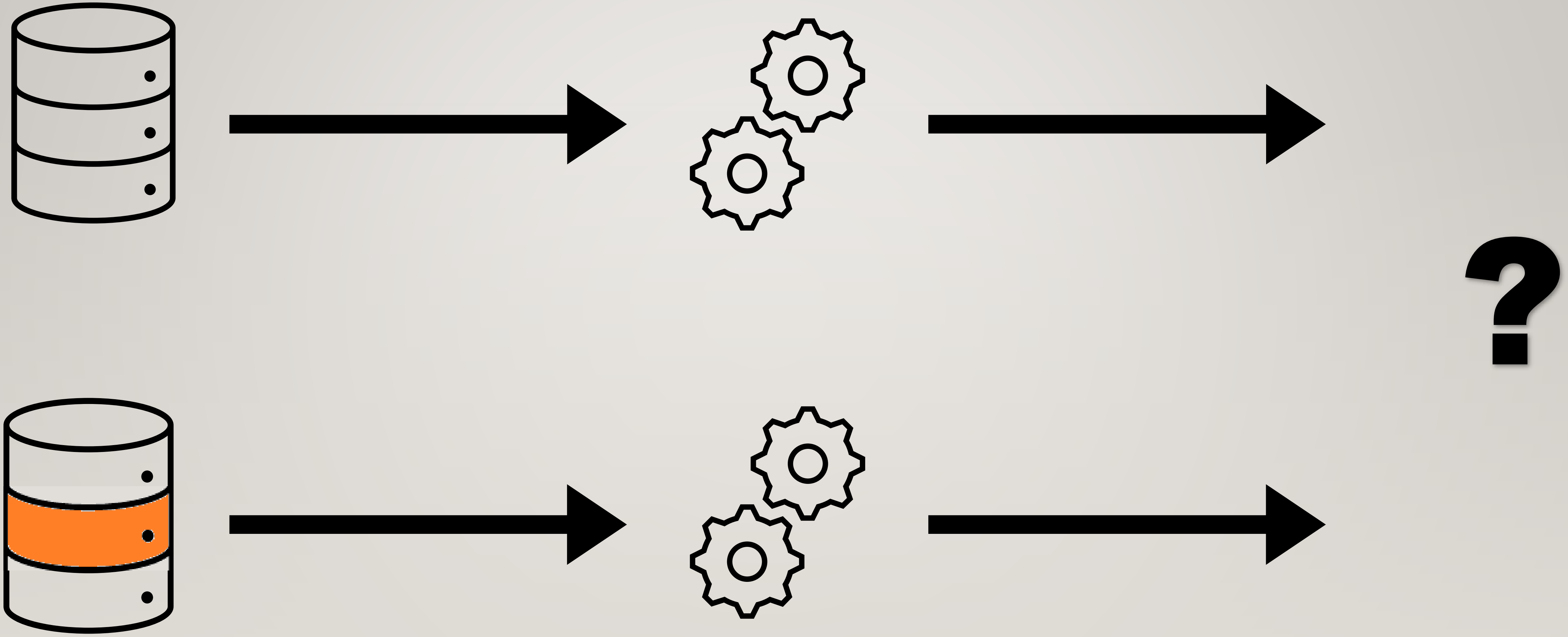
- Motivation
- What is Differential Privacy?
- Noise in Homomorphic Encryption
- Differential Privacy for Free?
- Analysis
- Case Study Results
- Further Work

MOTIVATION

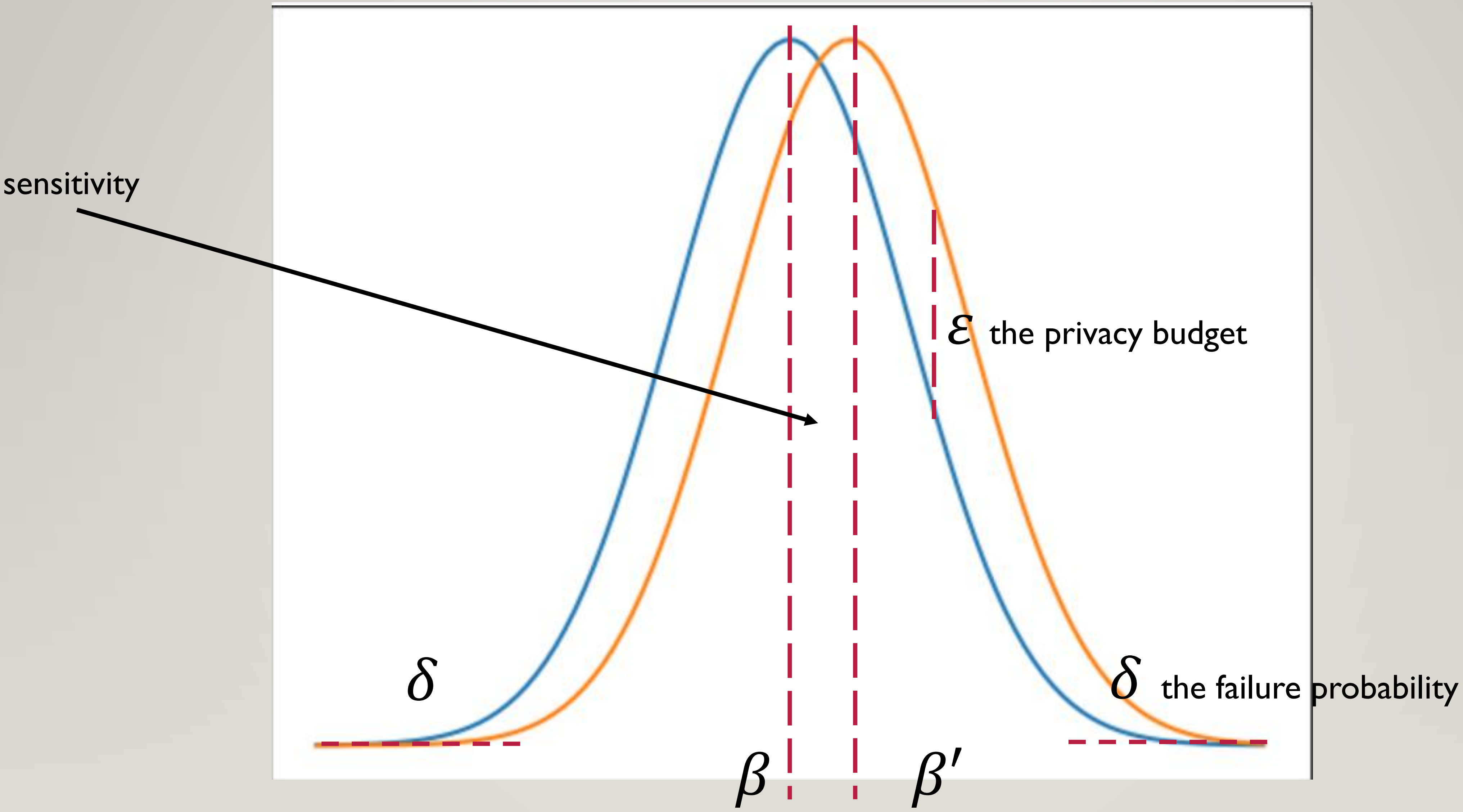
Homomorphic Encryption

Differential Privacy

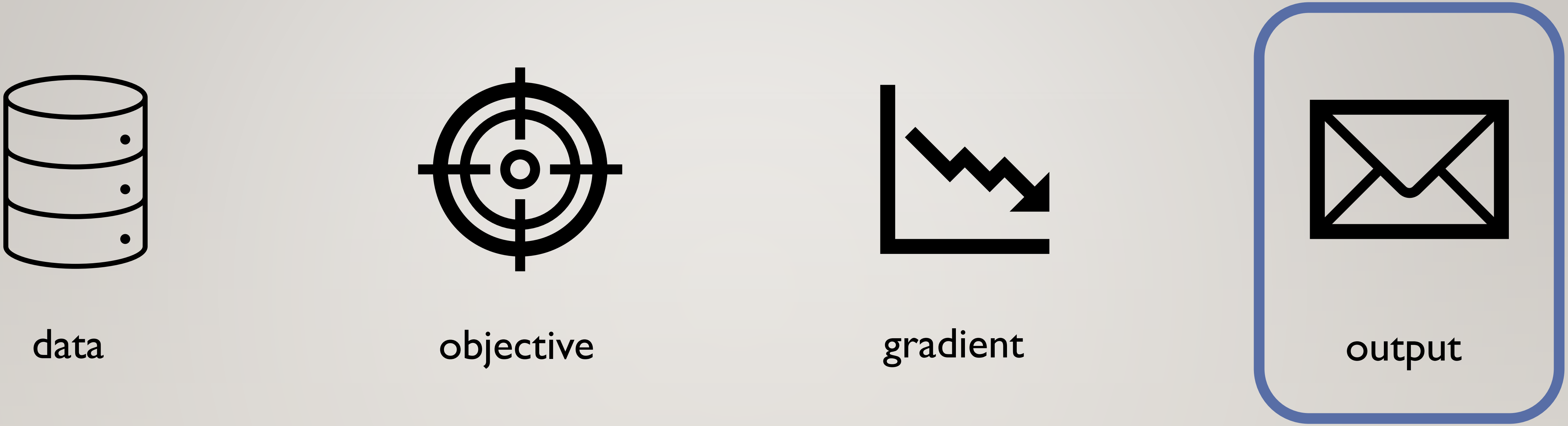
Image credit: https://www.xtivia.com/blog/data-science-pipeline-guidelines/



WHAT IS DIFFERENTIAL PRIVACY II



WHAT IS DIFFERENTIAL PRIVACY III



NOISE ANALYSIS I

$$(a, as + e)$$

- How large is the noise?
- How does the noise change when we perform homomorphic operations?
- Is the noise small enough to remove during decryption or bootstrapping?

NOISE ANALYSIS II

Worst Case

1. Bound fresh sources of noise using tail bounds
2. Update after each operation according to the "worst case" growth

- ✓ Very robust
- ✓ (Relatively) easy to implement
- ✗ Loose bounds
- ✗ Returns a bound on the noise only

Average Case

1. Analyse how the distribution of the noise changes over the course of a circuit
2. Use tail bounds to return a final upper bound on the noise

- ✓ Tight bounds
- ✓ Description of the noise distribution
- ✗ Requires many assumptions
- ✗ Can be difficult to deploy

can homomorphic encryption noise give differential privacy *for free*?

DIFFERENTIAL PRIVACY FOR FREE? II

- Noise is removed during decryption ➡ *approximate* homomorphic encryption

- Noise remains small ➡ high depth circuit

- Need to know the noise distribution to accurately specify the privacy leakage ➡ use the heuristics of [1], which argues that noise in CKKS follows a normal distribution throughout a circuit

  * *Can only evaluate quadratic polynomials*

[1] Costache, A., Curtis, B.R., Hales, E., Murphy, S., Ogilvie, T., Player, R.: On the precision loss in approximate homomorphic encryption. Cryptology ePrint Archive (2022) 2022/162

DIFFERENTIAL PRIVACY FOR FREE? III

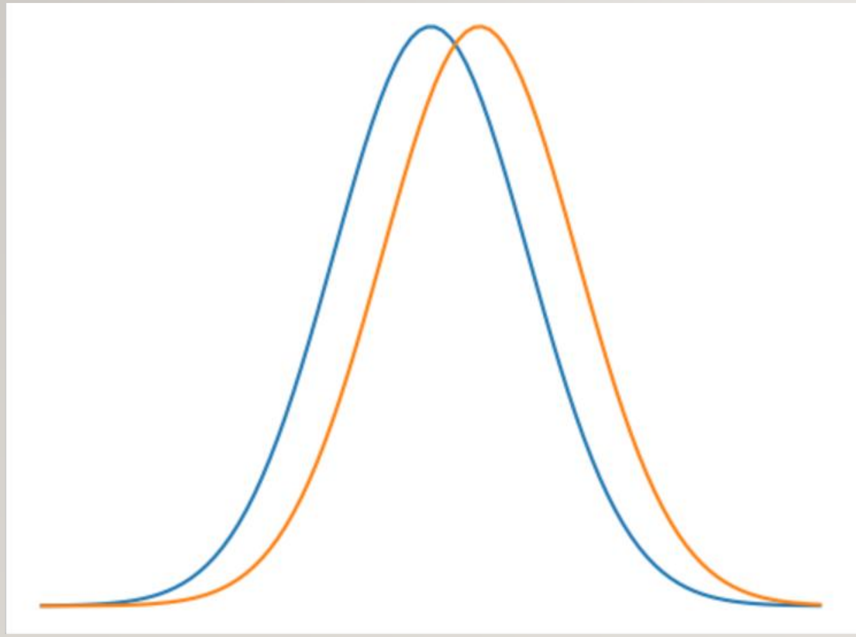
1. Use CKKS
2. Choose a high depth application
3. Allow the noise to grow large enough

ANALYSIS I

$$N\rho_1^2\rho_2^2 + \rho_1^2\underline{|m_2|}^2 + \rho_2^2\underline{|m_1|}^2$$

…the shape of the distribution depends on the input data

ANALYSIS II



Let κ = sensitivity/standard deviation, τ =standard deviation/standard deviation'

Standard case

$$\varepsilon \geq \sqrt{c}\kappa$$

Our case, 1D

$$\varepsilon \geq \tau^2\sqrt{c'}\kappa + \frac{1}{2}\tau^2\kappa^2 + \frac{1}{2}(\tau^2 - 1)c' + \ln\tau \Rightarrow \varepsilon \geq \sqrt{c'}\kappa + \frac{1}{2}\kappa^2$$

Our case, n-D

$$\varepsilon \geq \sqrt{c''\left(\tau^4\kappa^2 + \frac{n(\tau^2 - 1)}{2}\right)} + \frac{1}{2}\tau^2\kappa^2 + \frac{1}{2}(\tau^2 - 1)(c''+n) + \ln\tau \Rightarrow \varepsilon \geq \sqrt{c''}\kappa + \frac{1}{2}\kappa^2$$

case study requirements:

- CKKS
- (arbitrarily) high depth
- quadratic

→ Ridge regression training using gradient descent [2]

[2] Ogilvie, T., Player, R., Rowell, J.: Improved privacy-preserving training using fixed-hessian minimisation. In Michael Brenner, Tancrède Lepoint (Eds.), proceedings of the 8th Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC '20)

CASE STUDY II

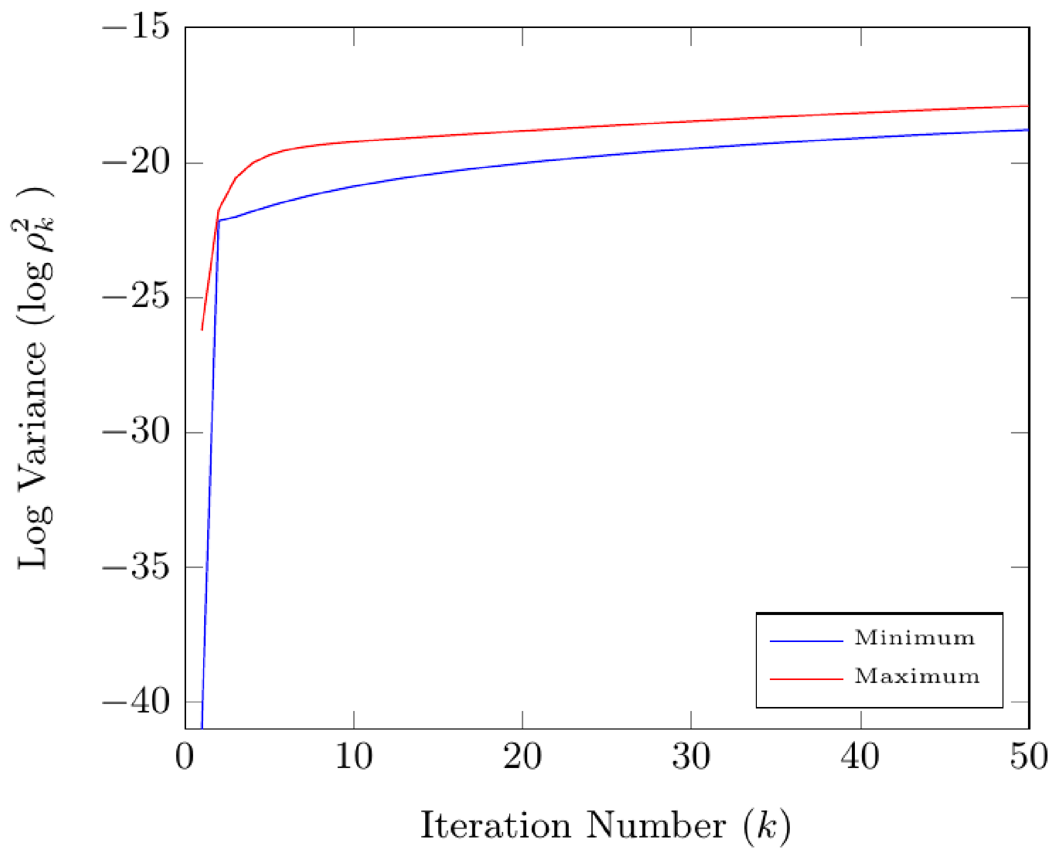


Fig. 2. Variance Growth with Iteration. $\log \Delta = 25$.

CASE STUDY III

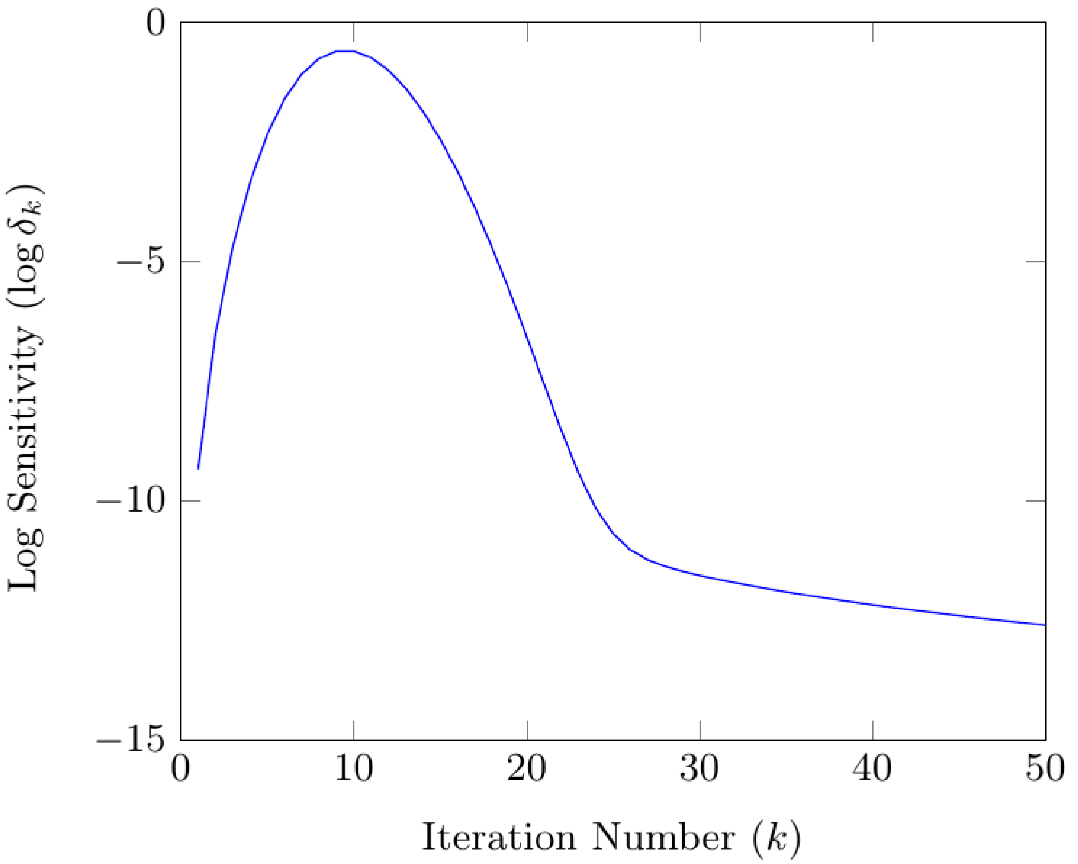


Fig. 2. Sensitivity Growth with Iteration.

CASE STUDY IV – variance only

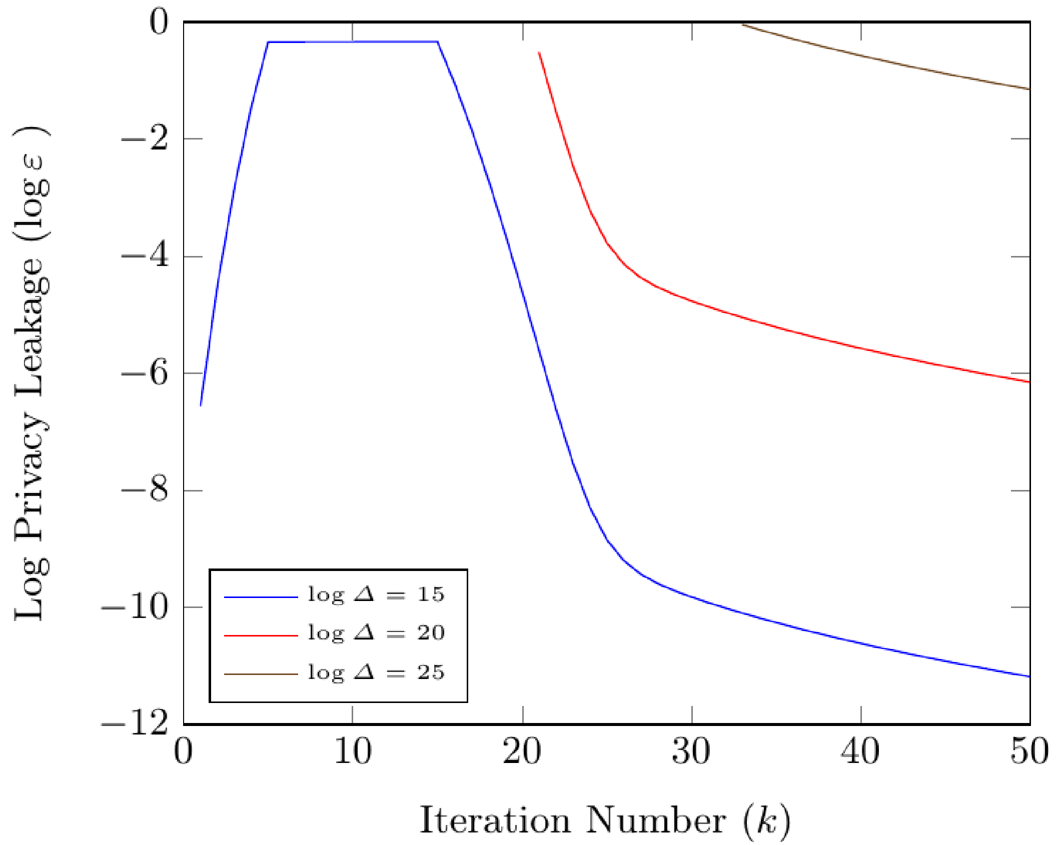


Fig. 3. ε Growth with Iteration for Varying Δ.

CASE STUDY V

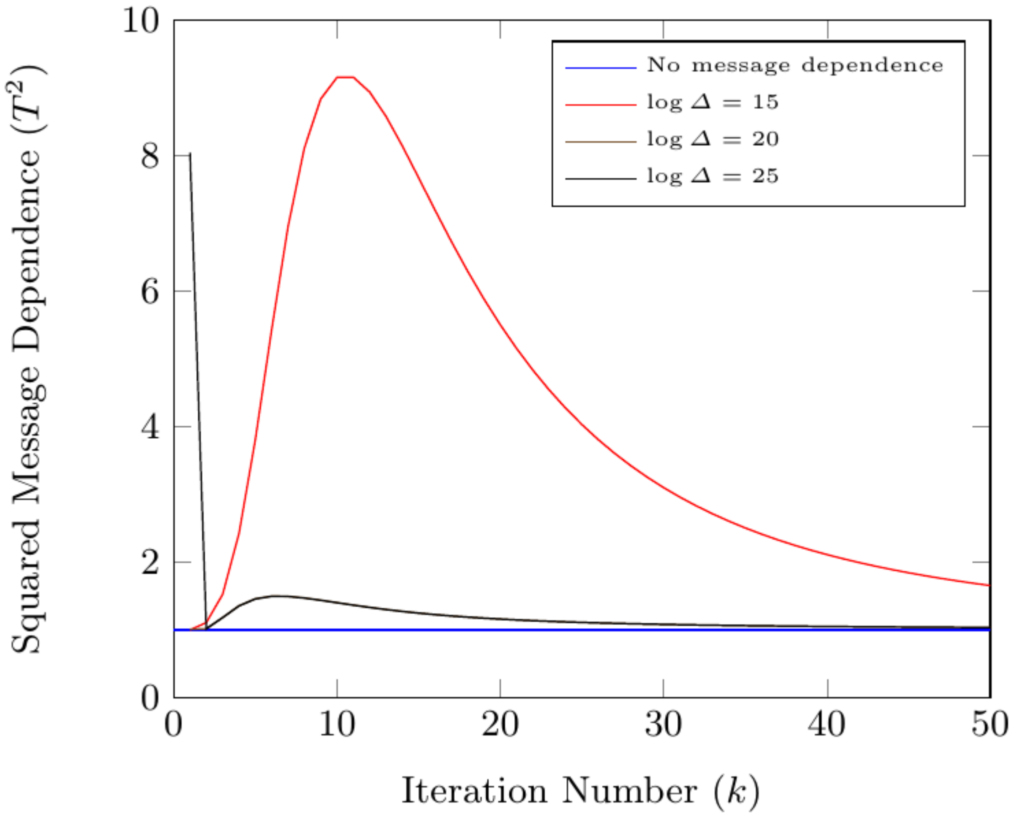


Fig. 6. Message Dependence Change with Iteration.

CASE STUDY VI

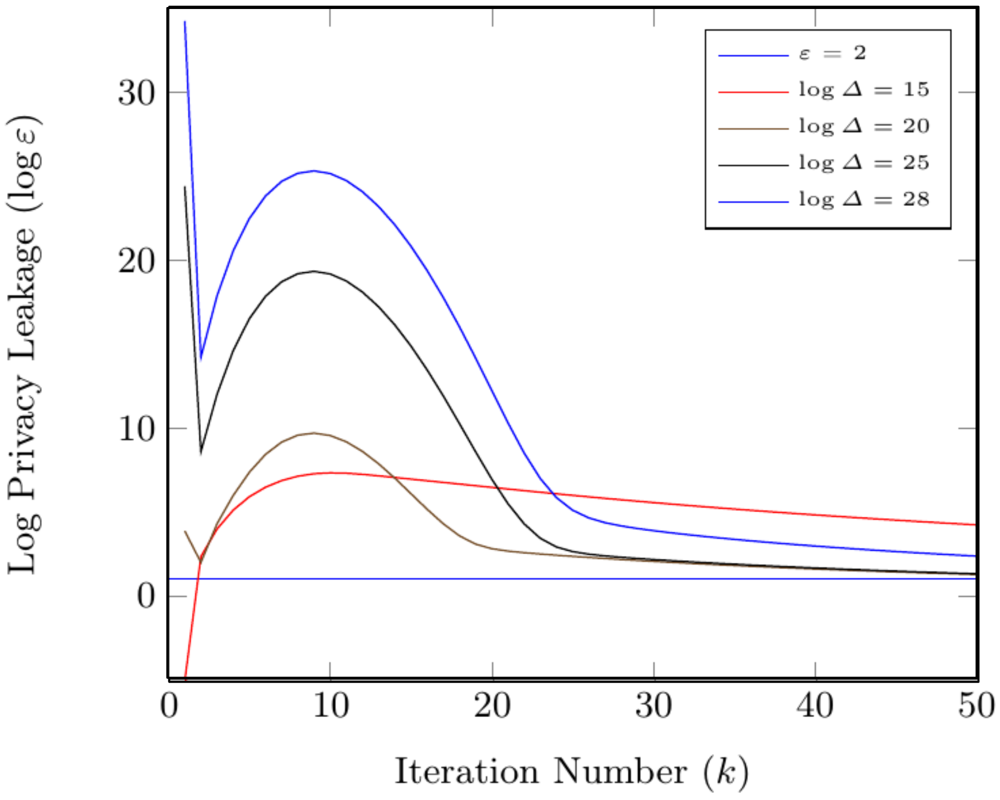


Fig. 7. Change in Log Privacy Leakage with Iteration.

CONCLUSION AND FURTHER WORK I

- We investigated the extent to which HE noise can provide differential privacy "for free"
- Identified message dependence as a key barrier
- Derived new results on the Differential Privacy in this setting
- Explored our results with a case study, and found a privacy budget of $\varepsilon \approx 2$ achievable with 50 iterations

further work

1. Further Noise Analysis
2. From Heuristic to Guarantee
3. Alternative Applications and Schemes
4. Beyond Output Perturbation
5. Differential Privacy "At A Discount"

Thanks for listening!

tabitha.l.ogilvie@gmail.com