IEEE Hong Kong 6G Wireless Summit

11-12 September 2024
Hong Kong, China

IEEE ComSoc IEEE Communications Society | IEEE

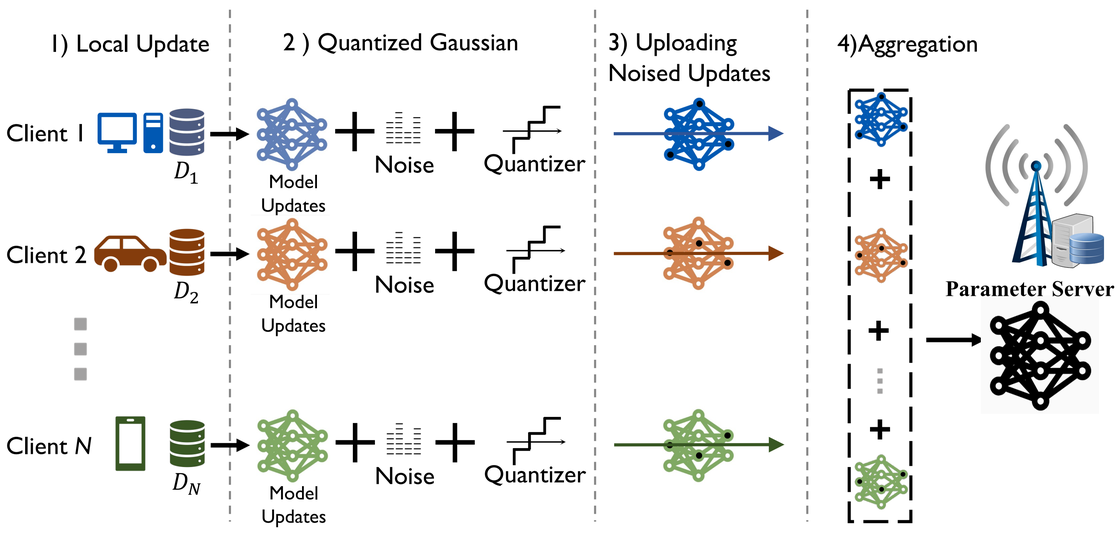
Department of Electronic and Computer Engineering, HKUST

The Effect of Quantization in Federated Learning: A Rényi Differential Privacy Perspective

Tianqu Kang, from Prof. Khaled B. Letaief's Research Group

Background

- **Federated Learning (FL):** A framework enabling multiple clients to collaboratively train a model without sharing their private data, but privacy risks remain due to model weight attacks.
- **Differential Privacy in FL:** Integrating Differential Privacy (DP) into adds noise to model weights to enhance privacy protection.
- **Communication Overhead:** A major challenge in FL is the large communication overhead due to the transmission of model weights.
- **Quantization for Efficiency:** Quantization is commonly employed to reduce the communication overhead in FL by compressing the model weights.



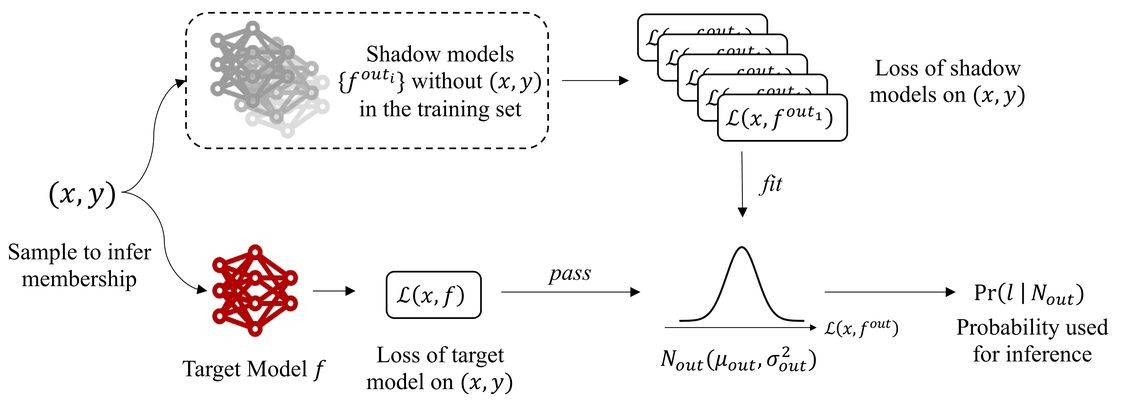
Federated Learning with quantized Gaussian mechanism applied. The weight of each client is first perturbed by Gaussian noise and then passed to the quantizer.

Motivations

- **Privacy vs. Communication Trade-off:** While quantization reduces communication costs, it introduces complexities in understanding and ensuring privacy protection

Contributions

- **Theoretical Analysis:** Provides a privacy budget analysis for quantized Gaussian mechanisms in FL using Rényi Differential Privacy (RDP), showing that lower quantization levels improve privacy.
- **Experimental Validation:** Empirical tests using Membership Inference Attacks (MIA) confirm the theoretical findings, where lower MIA accuracy refers to better privacy protection.



Working flow of the Membership Inference Attack.

Theoretical Analysis

- **RDP:**

Definition 3 ((α, ϵ)-RDP)**.** *A randomized mechanism $f: \mathcal{D} \mapsto \mathcal{R}$ is said to have (α, ϵ)-RDP, if for any neighboring $D, D' \in \mathcal{D}$ it holds that*

$$D_\alpha\left(f(D) \| f(D')\right) \leq \epsilon, \tag{6}$$

$\epsilon \downarrow \Leftrightarrow$ Privacy Protection $\uparrow$

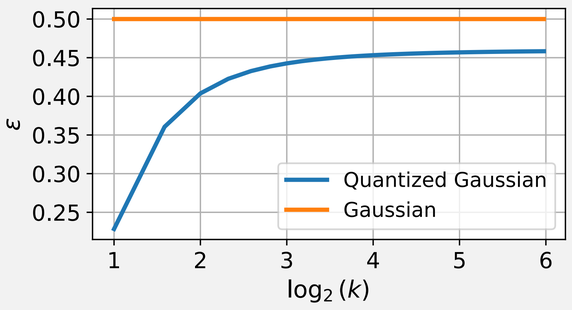
- **Theorem 2:** Provides an **upper bound** of the privacy budget of the quantized Gaussian

$$D_1(P_x || P_{x'}) \leq D_{KL}(P_{\frac{C_q}{2}} || P_{-\frac{C_q}{2}})$$

$$D_\alpha(P_x || P_{x'}) \leq D_\infty(P_x || P_{x'}) \leq \log\left(\frac{\delta}{\int_{B(k-2)}^{B(k-1)} f(x)\,(x - B(k-2))\,dx}\right)$$

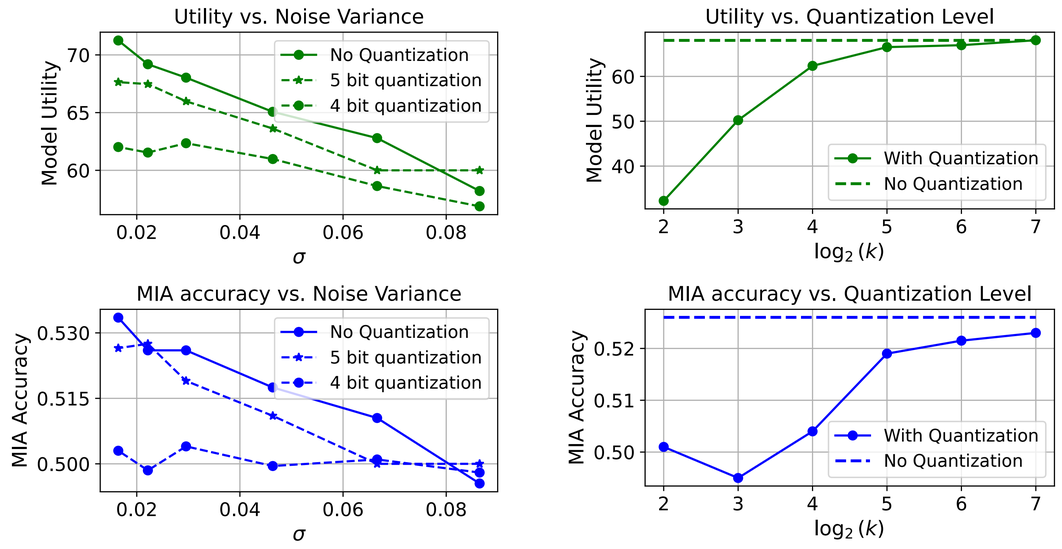
- **Lemma 3:** Proves that the upper bound in the previous theorem **increases monotonically** with quantization level

RDP bound of Gaussian and quantized Gaussian with α=1



Numerical sketch of RDP budgets for Gaussian and quantized Gaussian mechanisms at $\alpha = 1$, with varying quantization levels k from 2 to 64 while keeping $\sigma = 1$ and $\Delta_2 = 1$

Experiment result



Utility and MIA accuracy comparison varying the Gaussian noise variance during training.

Comparison of utility and MIA accuracy all with a noise variance of 0.03.

- **Lower Quantization, Better Privacy**: The experiments confirmed that models with lower quantization levels exhibited lower MIA accuracy, indicating better privacy protection.
- **Quantized Gaussian vs. Gaussian**: Quantized Gaussian mechanisms **consistently outperformed** standard Gaussian mechanisms in terms of providing a tighter privacy budget.

MIA accuracy $\downarrow$
$\Updownarrow$
Privacy Protection $\uparrow$

TABLE I
PARAMETERS FOR FL EXPERIMENTS

Parameter	Value
Architecture	ResNet-18
Dataset	Cifar-10
Client Number (N)	100
Communication Rounds (T)	150
Total training Samples	45,700 (i.i.d. among clients)
Client Optimizer	Adam [20]
Batch Size	128
Learning Rate (α)	0.001
Adam β_1	0.9
Adam β_2	0.999
Clipping Threshold (C_q)	1

Related Publication

- T. Kang, L. Liu, H. He, J. Zhang, S. Song and K. B. Letaief, "The Effect of Quantization in Federated Learning: A Renyi Differential Privacy Perspective," in Proc. IEEE Int. Mediterranean Conf. on Commun. and Netw. (MeditCOM), Madrid, Spain, 2024.

Acknowledgment

This work was supported in part by the Hong Kong Research Grants Council under the Areas of Excellence Scheme Grant AoE/E-601/22-R