Skellam Mixture Mechanism: a Novel Approach to Federated Learning with Diferential Privacy —— 阅读心得

(南开大学网络空间安全学院 天津 300350)

(专业：信息安全 学号：2013921 姓名：周延霖)

一、动机

此篇论文是解决深度神经网络在训练过程中可能泄露敏感数据的问题。作者考虑了一种场景，即多个参与者拥有分布式的敏感数据，他们想要通过联邦学习（FL）的方式，共同训练一个模型。为了保证隐私，他们需要使用安全多方计算（MPC）来加密每次的梯度更新，同时使用差分隐私（DP）来给梯度注入随机噪声。然而，现有的 DP 机制大多数都是基于实数域的噪声，而 MPC 则是基于有限域的整数。这就导致了两者之间的不兼容性，以及噪声水平过高，从而影响了模型的效用。为了解决这个问题，作者提出了一种新的 DP 机制，叫做 Skellam 混合机制（SMM），它可以在不需要整数梯度的情况下，注入较小的噪声，并且可以进行紧密的隐私分析。

随着深度神经网络的发展和应用，它们的记忆能力也越来越强，但这也带来了一个严重的隐私问题，即它们可能会记住并泄露训练数据中的敏感信息。为了解决这个问题，一种有效的解决方案是使用差分隐私（DP）来训练模型，它可以通过给梯度注入随机噪声，来提供严格的隐私保证。然而，在一些场景中，敏感数据是分布在多个参与者之间的，他们想要通过联邦学习（FL）的方式，共同训练一个模型。在这种情况下，他们不仅需要使用 DP 来保护数据，还需要使用安全多方计算（MPC）来保护梯度更新。MPC 可以让参与者在不泄露自己的梯度的情况下，计算出所有梯度的加和。然而，MPC 和 DP 之间存在一个基本的不兼容性，即 MPC 是基于有限域的整数运算的，而 DP 则是基于实数域的噪声注入的。这就导致了现有的 DP 机制需要注入很高水平的噪声，从而影响了模型的效用。为了解决这个问题，文章提出了一种新的 DP 机制，叫做 Skellam 混合机制（SMM），它可以在不需要整数梯度的情况下，注入较小的噪声，并且可以进行紧密的隐私分析。

二、贡献

首先，此篇提出了一种新的 DP 机制，称为 Skellam 混合机制（SMM）。SMM 能够在无需整数梯度的情况下注入较小的噪声，同时实现紧密的隐私分析。其次，该论文

利用 Skellam 分布的特性，在不影响模型效用的前提下保证隐私。Skellam 分布具有良好的组合和子采样性质，可以用于精确的深度学习与 DP。此外，该论文对 SMM 进行了复杂而创新的理论分析，考虑了不同的场景和参数设置，并证明了 SMM 在隐私保证和效用方面的优势。最后，通过大量的实验，在多种实际设置下展示了 SMM 相比现有解决方案在模型效用方面的显著提升。

作者也提出了一种新的解决方案，为保护分布式敏感数据的隐私提供了方法。该方法可以在不降低模型效用的前提下，给梯度注入较小的噪声，并进行紧密的隐私分析。这对于涉及隐私数据的领域，如医疗、金融、教育等，具有重要的意义和价值。

此外，该文章为促进联邦学习和差分隐私的发展和应用提供了新的思路和方法。它利用了 Skellam 分布和 Skellam 混合分布的性质，解决了 MPC 和 DP 之间的不兼容性问题，并进行了复杂而创新的理论分析和实验评估。这对于涉及多方协作和数据共享的场景，如物联网、边缘计算、社交网络等，具有重要的影响和启发。

最后，该文章引入了 Skellam 分布和 Skellam 混合分布作为噪声分布，为推动差分隐私的理论研究和技术创新提供了新的工具和平台。这些分布具有良好的组合和子采样性质，以及复杂而有趣的数学特征。对于涉及差分隐私的问题，如敏感度计算、隐私损失估计、噪声方差优化等，该文章提供了重要的参考和借鉴。

三、方法

首先，它定义了一种新的噪声分布，叫做 Skellam 分布，它是由两个独立的泊松分布的差构成的。Skellam 分布的概率质量函数为：

$$P(X = x) = \frac{\lambda_1^x e^{-\lambda_1} \lambda_2^{-x} e^{-\lambda_2}}{x! \cdot I_x(2\sqrt{\lambda_1 \lambda_2})}$$

其中λ_1和λ_2是两个泊松分布的参数，I_x是第一类修正贝塞尔函数。

然后，它将 Skellam 分布扩展为 Skellam 混合分布，它是由两个 Skellam 分布的加权和构成的。Skellam 混合分布的概率质量函数为：

$$P(X = x) = p \cdot P_1(X = x) + (1 - p) \cdot P_2(X = x)$$

其中 p 是混合系数，P_1和P_2是两个 Skellam 分布。

接着，它设计了一种新的 DP 机制，叫做 Skellam 混合机制（SMM），它可以在不需要整数梯度的情况下，注入 Skellam 混合噪声，并且可以进行紧密的隐私分析。

SMM 的主要思想是将每个梯度分量分解为两个整数部分和一个小数部分，然后对每个整数部分注入一个 Skellam 噪声，对小数部分注入一个 Laplace 噪声，最后将三个部分重新组合起来得到最终的噪声梯度。

最后，它对 SMM 进行了复杂而创新的理论分析，证明了 SMM 的隐私保证和效用优势。它利用了 Skellam 分布的组合和子采样性质，以及 Skellam 混合分布的矩生成函数和尾部概率等性质，推导出了 SMM 的敏感度、隐私损失、噪声方差等重要指标，并且与现有的 DP 机制进行了比较。

四、思考

（一）未来想法

首先，进一步探索 Skellam 分布和 Skellam 混合分布的性质，并研究它们在其他场景下的应用。例如，是否可以将 Skellam 分布用于描述图像、文本、音频等其他类型的数据；是否可以利用 Skellam 混合分布构造更复杂的噪声分布，以适应更多样的数据分布。

其次，进一步优化 SMM 的性能，以提高模型的效用和隐私保护水平。例如，是否可以通过调整混合系数、噪声参数、梯度分解方式等因素，来降低噪声水平和隐私损失；是否可以引入其他技术，如梯度裁剪、梯度量化、梯度压缩等，以减少通信开销和计算开销。

此外，进一步扩展 SMM 的适用范围，以覆盖更多的场景和需求。例如，是否可以将 SMM 应用于非联邦学习的情况，如中心化的训练或分布式的训练；是否可以将 SMM 与其他类型的隐私保护技术结合，如同态加密、零知识证明、可验证计算等。

（二）当前不足

首先，文章未提供 SMM 的具体实现细节，如如何选择适当的 Skellam 分布参数、如何进行梯度分解和重组、如何在 MPC 中实现 Skellam 噪声的生成和加法等。这些实现细节对于 SMM 的实际应用和复现非常关键，但文章未提供足够的信息和指导。

其次，文章未对 SMM 的隐私保证和效用优势进行充分的理论证明和分析。尽管给出了一些定理和引理，但缺乏详细的证明和推导过程。这些证明和分析对于理解和评估 SMM 的性质非常重要，但文章未提供足够的细节和说明。

此外，文章未对 SMM 的性能进行充分的实验评估。仅仅在一些人工数据集和小规模数据集上进行了简单比较，未考虑到更多的场景和需求，如不同的数据类型、不

同的模型结构、不同的隐私需求等。这些实验评估对于验证和展示 SMM 的有效性非常重要，但文章未提供足够的结果和讨论。

（三）文章总结

文章的主题是关于联邦学习和差分隐私的研究，它提出了一种新的 DP 机制，叫做 Skellam 混合机制（SMM），它可以在保证隐私的同时提高模型的效用。文章的背景是，当多个参与者拥有分布式的敏感数据，他们想要通过联邦学习（FL）的方式，共同训练一个模型时，他们需要使用安全多方计算（MPC）来加密每次的梯度更新，同时使用差分隐私（DP）来给梯度注入随机噪声，以避免数据泄露。文章的挑战是，现有的 DP 机制大多数都是基于实数域的噪声，而 MPC 则是基于有限域的整数，这就导致了两者之间的不兼容性，以及噪声水平过高，从而影响了模型的效用。文章的方法是，利用 Skellam 分布和 Skellam 混合分布作为噪声分布，它们可以在不需要整数梯度的情况下，注入较小的噪声，并且可以进行紧密的隐私分析。文章的理论分析是非常复杂和创新的，它考虑了不同的场景和参数设置，并且证明了 SMM 的隐私保证和效用优势。文章的实验评估是在多种实际设置下进行的，它展示了 SMM 相比现有的解决方案，在模型效用方面的显著提升。