2019-02-28

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

- IDASH2017-master代码

  Makefile C++工程项目　　添加注释

Logistic Regression Model Training based on the Approximate Homomorphic Encryption

Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.　　SNU 2018

$$L = \begin{cases} \text{ITERNUM} \cdot (3p + 2p_c + 3) + L_0 & g = g_3, \\ \text{ITERNUM} \cdot (4p + 2p_c + 3) + L_0 & g \in \{g_5, g_7\}, \end{cases}$$

$$\mathtt{ct}_z = \mathtt{Enc} \begin{bmatrix} z_{10} & z_{11} & \cdots & z_{1f} \\ z_{20} & z_{21} & \cdots & z_{1f} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n0} & z_{n1} & \cdots & z_{nf} \end{bmatrix}$$

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

- simplified fixed Hessian method

  C++编程实现

  Privacy-Preserving Logistic Regression Training

  Charlotte Bonte, and Frederik Vercauteren. [KU Leuven] 2018

  Fix-Hessian method : Dankmar Böhning and Bruce G Lindsay 1988

  Newton method： 海森矩阵不可逆，求海森矩阵的逆计算量大

  Böhning fix Hessian H⩾B（where “⩾” denotes the Loewner ordering）+ a lower bound

  Charlotte Bonte simplify lower bound

- 在明文上实现 simplified fixed Hessian method
  验证所实现算法代码的逻辑正确无误

- 在IDASH2017-maste的C++工程项目上
  实现经过验证的算法逻辑

- 并在密文上实现该算法逻辑

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab