2018-12-04

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

Logistic Regression Based on Homomorphic Encryption

- Doing Real Work with FHE: The Case of Logistic Regression.

  Jack L.H. Crawford, Craig Gentry, Shai Halevi, Daniel Platt, and Victor Shoup.
- Logistic Regression Model Training based on the Approximate Homomorphic Encryption. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.
- Logistic regression over encrypted data from fully homomorphic encryption. Hao Chen, Ran Gilad-Bachrach, Kyoohyung Han, Zhicong Huang, Amir Jalali, Kim Laine, and Kristin Lauter.

- Privacy-Preserving Logistic Regression Training.

  Charlotte Bonte and Frederik Vercauteren.

Logistic Regression Based on Homomorphic Encryption

- Doing Real Work with FHE: The Case of Logistic Regression.

  Jack L.H. Crawford, Craig Gentry, Shai Halevi, Daniel Platt, and Victor Shoup.

  Craig Gentry

  Shai Halevi, and Victor Shoup. (HElib)

- Homomorphic binary comparisons.
- Unfortunately, our solution was not ready in time for the iDASH competition deadline, so we ended up not participating in the formal competition.

Logistic Regression Based on Homomorphic Encryption

Gradient Descent:

- Logistic Regression Model Training based on the Approximate Homomorphic Encryption. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.
- Logistic regression over encrypted data from fully homomorphic encryption. Hao Chen, Ran Gilad-Bachrach, Kyoohyung Han, Zhicong Huang, Amir Jalali, Kim Laine, and Kristin Lauter.

Logistic Regression Based on Homomorphic Encryption

Gradient Descent:

- Logistic Regression Model Training based on the Approximate Homomorphic Encryption. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.

- Homomorphic Encryption for Arithmetic of Approximate Numbers. Jung Hee Cheon et al.

  HEAAN

  It supports an approximate addition and multiplication of encrypted messages,

  together with a new ***rescaling*** procedure for managing the magnitude of plaintext.

rescaling **:** it seems similar to the modulus-switching method(Brakerski and Vaikuntanatan)

Logistic Regression: $weights[i] = weights[i] + \alpha \cdot (y_i - sigmoid(z)) \cdot data[i][j]$

Nankai-Baidu Joint Laboratory

Parallel and Distributed Software Technology Lab

Logistic Regression Based on Homomorphic Encryption

Gradient Descent:

- Logistic Regression Model Training based on the Approximate Homomorphic Encryption. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.

- Homomorphic Encryption for Arithmetic of Approximate Numbers. Jung Hee Cheon et al.

HElib + Logistic Regression

HElib + rescaling　　可能性　不可行

Logistic Regression Based on Homomorphic Encryption

Gradient Descent:

- Logistic Regression Model Training based on the Approximate Homomorphic Encryption. Andrey Kim, Yongsoo Song, Miran Kim, Keewoo Lee, and Jung Hee Cheon.

  We introduced HEAAN at a workshop for the standardization of HE hosted by Microsoft Research

- Logistic regression over encrypted data from fully homomorphic encryption. Hao Chen, Ran Gilad-Bachrach, Kyoohyung Han, Zhicong Huang, Amir Jalali, Kim Laine, and Kristin Lauter.

  We will use FHE.bscale(·,i) to denote the above bootstrapping plus scaling down by i digits in base p.

Logistic Regression Based on Homomorphic Encryption

Newton-Raphson

- Privacy-Preserving Logistic Regression Training.
  Charlotte Bonte and Frederik Vercauteren.

  近似简化 Hession matrix

  近似简化 sigmoid function ~ 0.5+0.25z （is enough to obtain good results.）

2018 iDASH

11/30/2018 Workshop paper submission due (postponed to 12/31, we will send CFP soon)