2018-08-27

Nankai-Baidu
Joint Laboratory

Parallel and Distributed
Software Technology Lab

综述

1. 引言
2. 同态加密的相关知识
   起源、定义、发展、现状、应用
3. 两个实现方案
4. 在机器学习中的应用
5. 结论

综述

3. 两个实现方案
   - 3.0 符号定义
   - 3.1. BFV方案
   - 3.2 BGV方案
   - 3.3 自举法（Bootstrapping）

综述

自举法（Bootstrapping）

IDEA： We could refresh a ciphertext if we could completely decrypt it.

decrypt the ciphertext homomorphically

大部分解密算法是计算向量内积$\langle c, s\rangle = \sum_i c_i \cdot s_i$

综述

自举法（Bootstrapping）

Given: $\boldsymbol{c} = Encrypt(\boldsymbol{p}, m)$; $m = Decrypt(\boldsymbol{s}, c)$

$$m \cong \langle c, s \rangle = c_0 \cdot s_0 + c_1 \cdot s_1 + c_2 \cdot s_2 + \cdots$$

sk pk

$$\overline{c_i} = Encrypt(pk, c_i)\ ;$$
$$\overline{s_i} = Encrypt(pk, s_i)$$

$$\overline{c_0} \cdot \overline{s_0} + \overline{c_1} \cdot \overline{s_1} + \overline{c_2} \cdot \overline{s_2} + \cdots = ?$$

综述

自举法（Bootstrapping）

Given: $\boldsymbol{c} = Encrypt(\boldsymbol{p}, m)$; $m = Decrypt(\boldsymbol{s}, c)$

$$m \cong \langle c, s \rangle = c_0 \cdot s_0 + c_1 \cdot s_1 + c_2 \cdot s_2 + \cdots$$

$sk \quad pk$

$$\overline{c_0} \cdot \overline{s_0} + \overline{c_1} \cdot \overline{s_1} + \overline{c_2} \cdot \overline{s_2} + \cdots = Encrypt(pk, \langle c, s \rangle)$$

$$= Encrypt(pk, m) = ct$$

$$\boldsymbol{ct} = Encrypt(\boldsymbol{pk}, m)$$

综述

自举法（Bootstrapping）

Given: $\boldsymbol{c} = Encrypt(\boldsymbol{p}, m)$; $m = Decrypt(\boldsymbol{s}, c)$

$$m \cong \langle c, s \rangle = c_0 \cdot s_0 + c_1 \cdot s_1 + c_2 \cdot s_2 + \cdots$$

$sk \quad pk$

$$\overline{c_0} \cdot \overline{s_0} + \overline{c_1} \cdot \overline{s_1} + \overline{c_2} \cdot \overline{s_2} + \cdots = Encrypt(pk, \langle c, s \rangle)$$

$$= Encrypt(pk, m) = ct$$

$$\boldsymbol{ct} = Encrypt(\boldsymbol{pk}, m)$$

综述

4. 在机器学习中的应用
   - 4.1. ……
   - 4.2. 神经网络
   - 4.3. 逻辑回归

综述

4. 在机器学习中的应用

4.3. 逻辑回归

IDASH PRIVACY & SECURITY WORKSHOP 2017

secure genome analysis competition

- Logistic regression over encrypted data from fully homomorphic encryption
- Doing Real Work with FHE: The Case of Logistic Regression