1. □□□□

- □□□□□BERT-base-uncased
- □□□□GLUE/CoLA□□□□□□□□
- □□□□□epochs=3□□□□□=42□GPU□□
- □□□□□□□
  - □□□□□□□□□□□□PoisoningAttack□
  - □□□□□□□□□□

---

2. □□□□□□

- □□□□□□□□□□□□□□□ `normalTrain` □□□□□□□□□□□□□□□
- □□□□□BERT-base□GLUE/CoLA□□□□□□□□□80%-85%□□□□□□□□□□

---

3. □□□□□□

□□□□□□□**PoisoningAttack**□

- □□□□□□□□□10%□□□□□ `poisoning_rate=0.1` □□□□□□□□□□□□□□□□□□□□□□

- □□□□□

□□□□	□□□	**F1□□**	□□□□
□□□□-2□□□□	0.40	0.375	□
□□□□-2□□□□□□	0.40	0.375	□

- □□□□□

  1. □□□□□□□□□□□40%□□□□□□80%+□□□□50%□□□□□□□□□□□□□□
  2. □□
  3. **F1□□□□□□□**0.375□F1□□□□□□□□□□□□□□□□□□□

---

4. □□□□□□

- □□□□□**RLMI**□□□□□**FET**□□□□□□□□**ModelStealingAttack**□□□□□□□□□□□□□□

---

5. □□□□□□

□□□□□□□□

□□□□	□□□□
□□□□	□□□↓50%+□
□□□□	□□□□□□□□□
□□□□	□□□□□□□□

□□□□□

- □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□

1. □□□□□□□□□□□□□□□□□□□□□□□

2. [illegible]
3. [illegible]

---

6. [illegible]

- [illegible]
    - [illegible]
        - [illegible]
        - [illegible]
        - [illegible]
- [illegible]
    - [illegible]
    - [illegible]
- [illegible]

    > *[illegible]* `defenderEnabled` *[illegible]*

> *[illegible]*
>
> - *[illegible]**Accuracy**[illegible]*
> - ***F1**[illegible]*
> - *[illegible]**Poisoning Rate**[illegible]10%[illegible]*