Zero knowledge proof

甚麼是零知識證明

解釋

- 證明者向驗證者證明某命題的方法，且使驗證者能夠被說服
- 過程中不能洩漏除了該名題為真的事情
- 只有證明者知道內容
- 如何證明自己擁有該情報而不必透露情報內容。
- 驗證者需要能證明並無與證明者協調過，例如：現場以隨機事件作為驗證輸入
- 驗證者知道怎麼做輸入，但不知道其內容以及做法，只知道結果驗證後，確實符合命題
- 則在第三方完全不知情實驗命題以及內容

我的理解

- 宣告對方我擁有美味蟹堡秘方，但我並沒有公告內容為何

定義

- 完備 (complete)
  - 若證之事為真，誠實的證明者能直接說服誠實的驗證者
- 健全、合理 (sound)
  - 若證之事為假，作弊的證明者只有極小機率說服（騙過）誠實的驗證者
- 零知識 (zero-knowledge)
  - 若證之事為真，且驗證者在過程中不會知悉任何除命題為真之其他資訊
  - 在一交互情境下，每個驗證者可有相應的輸入，並且能夠證明事實