영지식 증명

Zero-Knowledge Proof

Zero-Knowledge

- 정의

  명제의 참, 거짓을 증명할 때
  참, 거짓 여부 이외의 어떠한 정보도 노출하지 않는 것

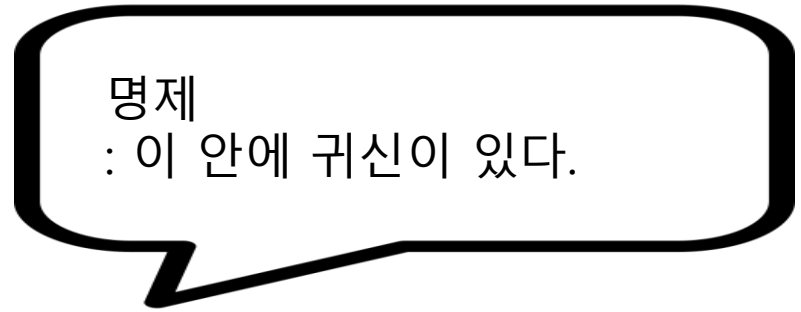
Zero-Knowledge

- 용어

  명제 (statement) : 증명하려는 사실, 참 혹은 거짓임
  증명자 (prover) : 참임을 증명하는 사람
  검증자 (verifier) : 참임을 검증하는 사람

Zero-Knowledge

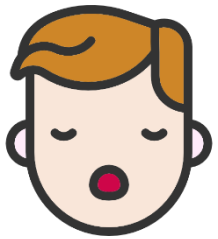
- 쉬운 예제



Zero-Knowledge

- 쉬운 예제

명제
: 이 안에 귀신이 있다.

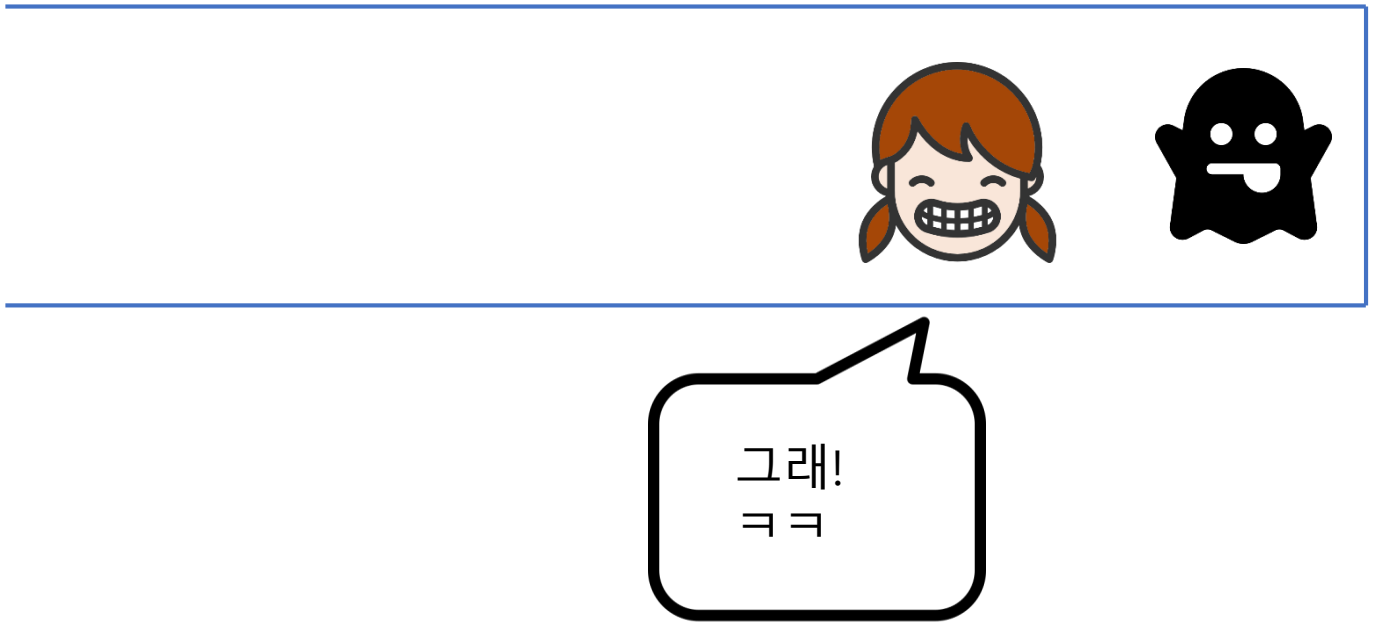


Zero-Knowledge

- 쉬운 예제
- #1

Zero-Knowledge

- 쉬운 예제
- #2



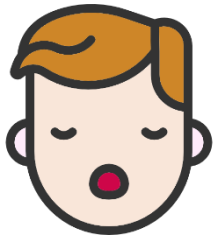
Zero-Knowledge

- 쉬운 예제
- #3~∞

명제
: 이 안에 귀신이 있다.

ㅠㅠ

야 이번엔
울면서 나와



Zero-Knowledge

- 명제 : “귀신이 존재한다”가 참일 경우
  검증자의 요구를 수행할 확률 50%에 근사
- 명제 : “귀신이 존재한다”가 거짓일 경우
  검증자의 요구를 수행할 확률 50%에 근사하지 않음

Zero-Knowledge

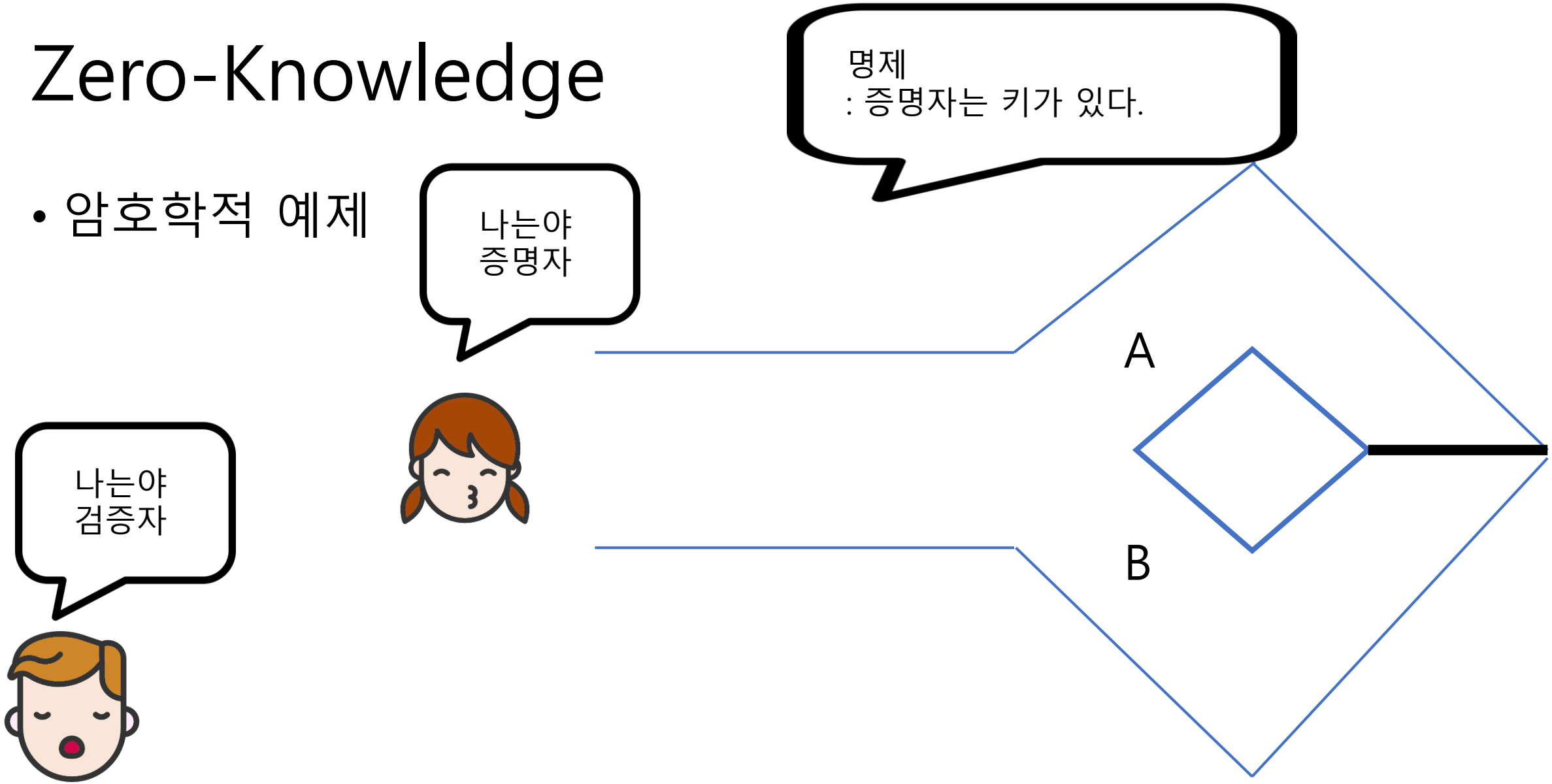
- 검증자의 시선
  검증자는 안에 귀신이 있는지 없는지 직접적인 정보없이 알 수 있음

Zero-Knowledge

- 제 3자의 시선
  증명자와 검증자는 어떤 요구를 할 것인가, 어떤 반응을 보일 것인가에 대하여 합의할 수 있음
  → 보여지는 정보로 어떠한 정보도 획득할 수 없음

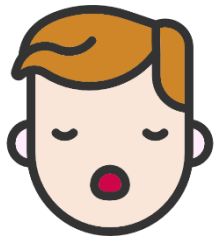
Zero-Knowledge

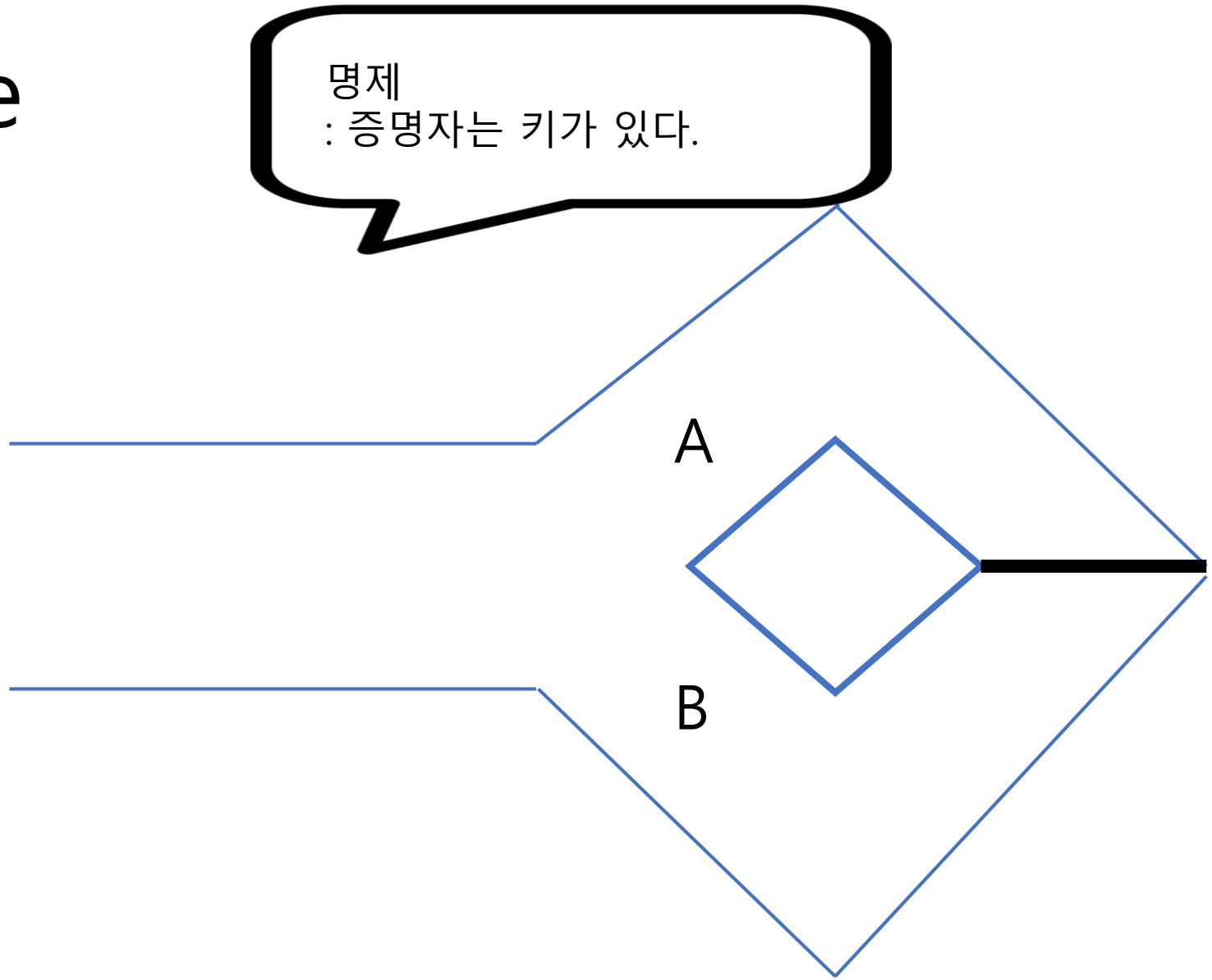
- 암호학적 예제



Zero-Knowledge

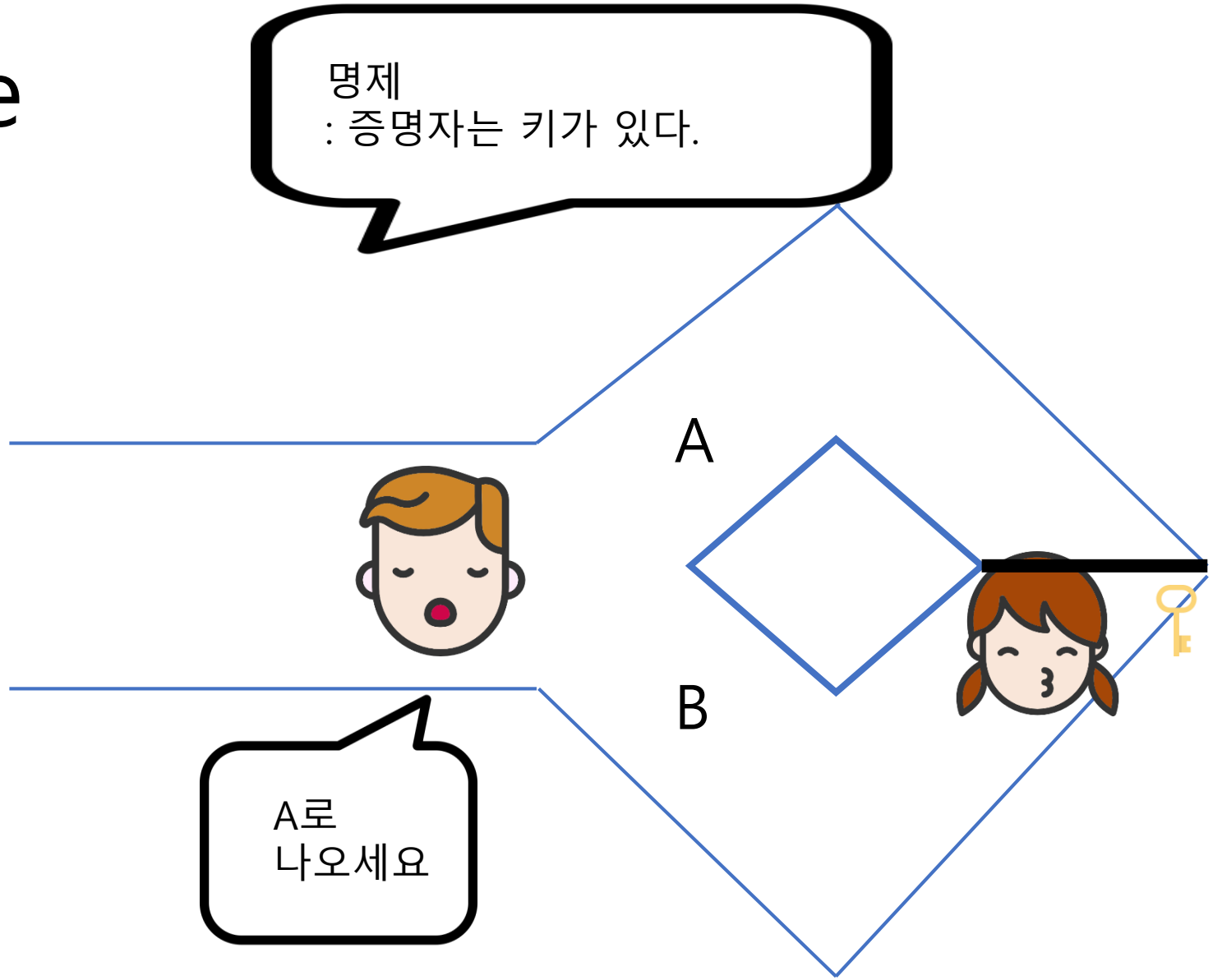
- 암호학적 예제





Zero-Knowledge

- 암호학적 예제



Zero-Knowledge in Blockchain

- 블록체인
  "가명화, 익명화, 프라이버시"를 보장하는가?
- 비트코인
  비트코인은 가명화된 트랜잭션 제공

  → 하지만, 분석을 통해 가명화를 풀 수 있음

Zero-Knowledge in Blockchain

- 접근법
  - 현존하는 블록체인 플랫폼에 익명성 추가
    화폐, 데이터 전송 트랜잭션 숨기기
  - 새로운 블록체인 플랫폼 개발
    Zero-Knowledge proof를 이용한 새로운 블록체인 개발 → ex) Zerocash

Zerocash

- Zero-Knowledge의 변형
  검증자 : 명제 해시
  검증자 : 해시, 난수를 이용하여 키 쌍 생성 (증명자 키, 검증자 키)
  증명자 : 증명자 키로 명제와 명제의 해시값을 암호화하여 보냄
  검증자 : 검증자 키로 명제의 해시값을 검증

  →Zero-Knowledge SNARKs
  (Succinct Non-interactive Argument of Knowledge)