Anonymous Communication Networks

no address
(hide ip)

Oct 31, 2024

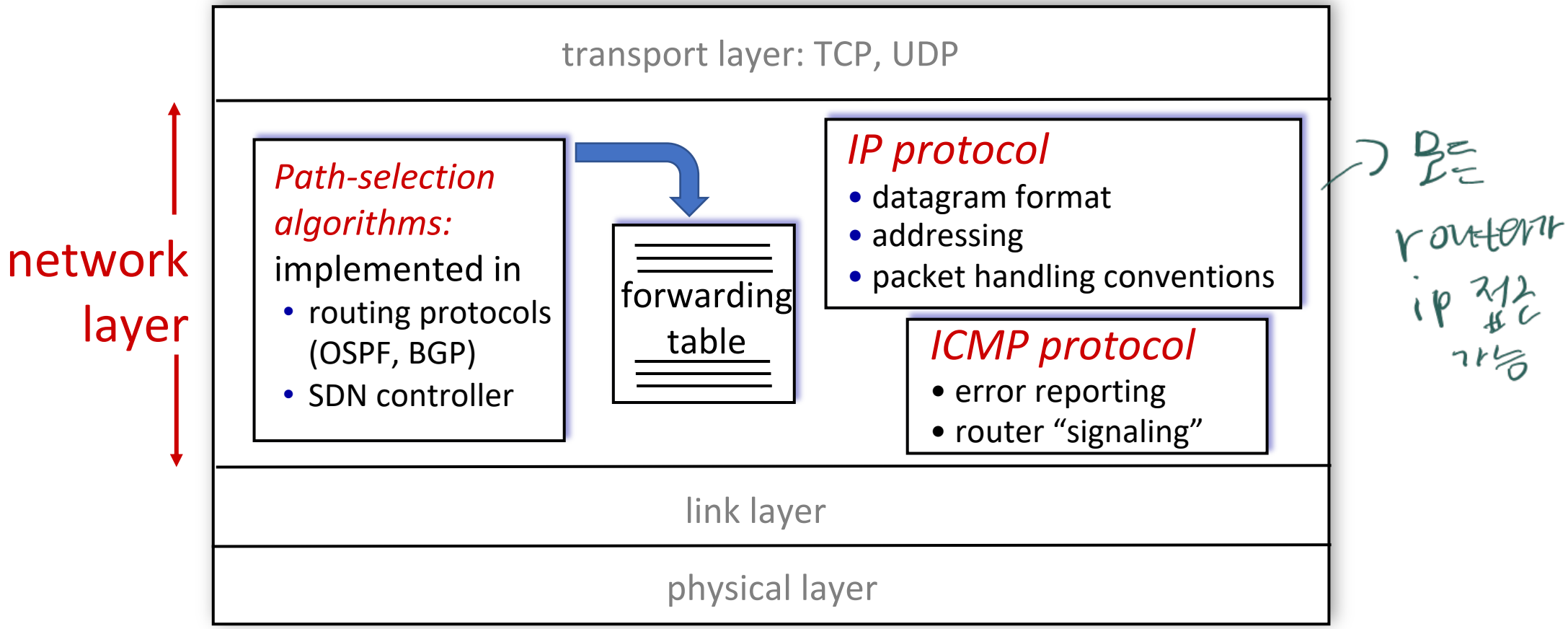
Min Suk Kang
Associate Professor
School of Computing/Graduate School of Information Security

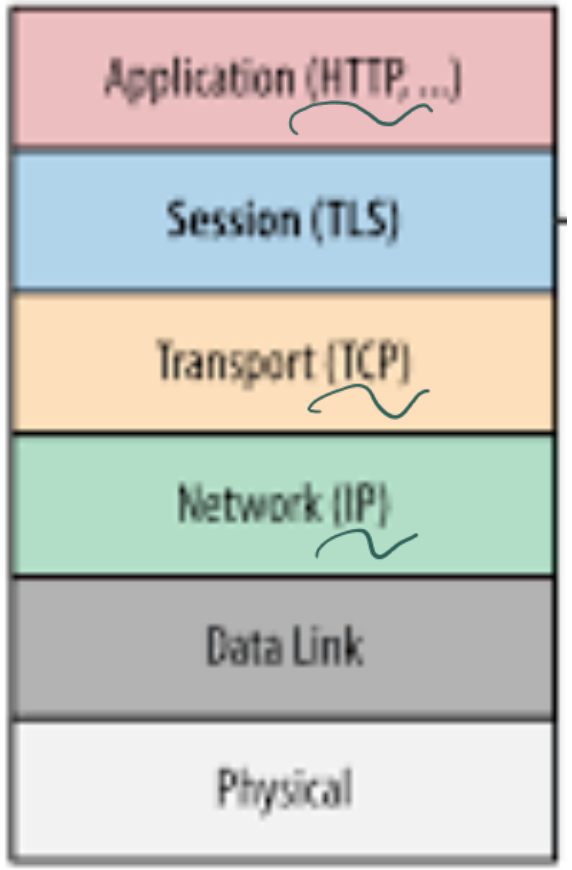
NetS&P
Research Lab @ KAIST

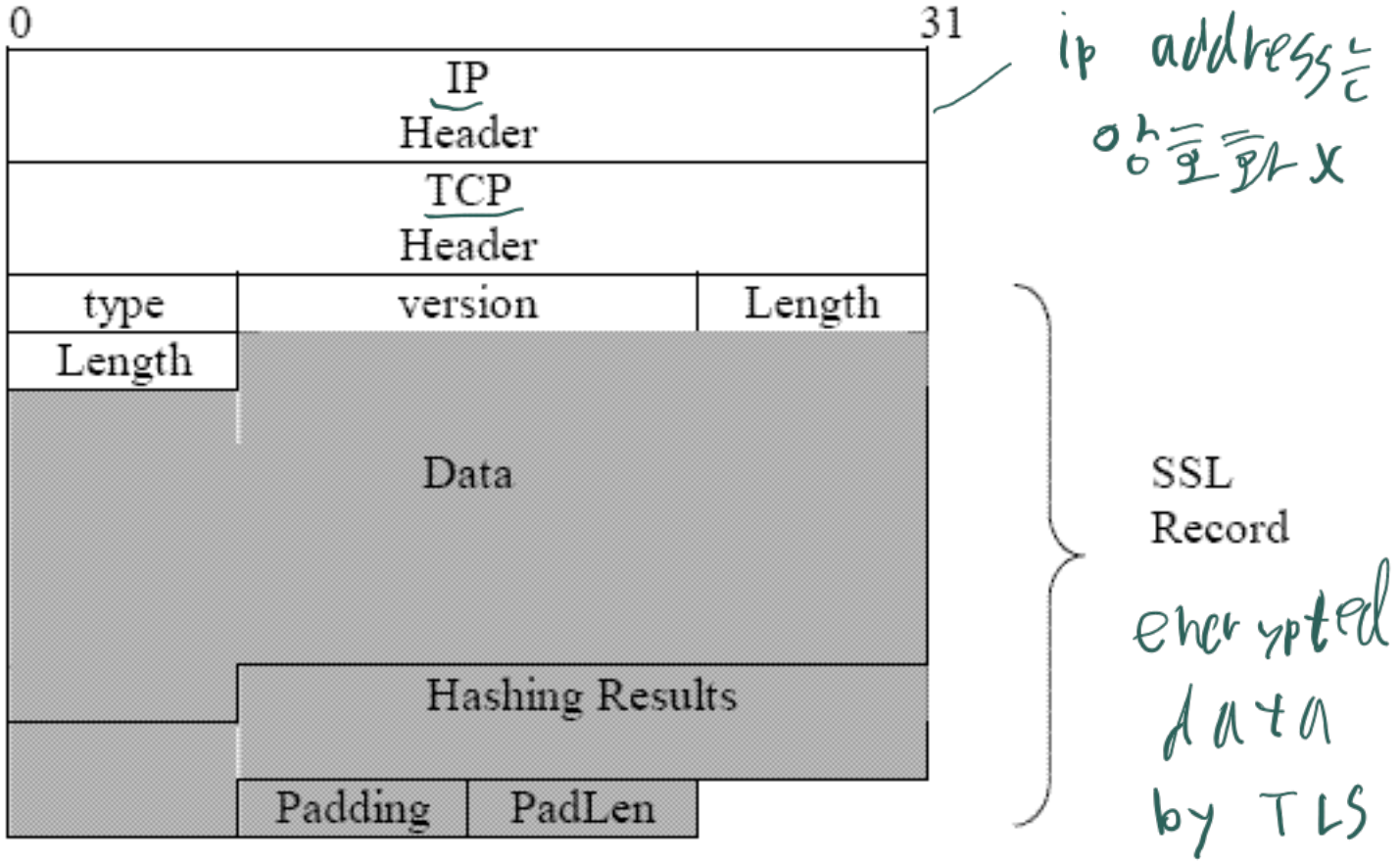
KAIST

Network Layer: Internet

host, router network layer functions:







ip address는 암호화 X

encrypted data by TLS

Anonymous Communication on the Internet?

- Internet is designed as a public network
  - Machines on your LAN may see your traffic, network routers see all traffic that passes through them → 라우터 traffic 탐지 가능
- Routing information is public
  - IP packet headers identify source and destination
  - Even a passive observer can easily figure out **who is talking to whom**
- Encryption does not hide identities
  - Encryption hides payload, but not routing information

↳ 암호화는 payload만 숨기므로 ip 통해 알 수

↳ 언제 대상 쉽게 파악 가능

Anonymity… why?

- Def: anonymity is the state of being not identifiable within a set of subjects

- Do we need anonymity on the Internet?

hide ip address
(send anonymity)

freedom of speech
⇒ 강철, 김영철 등 회피

anonymity는 없애고 보강되어야 하는가? (too small: 표현의 자유 / too big: 범죄악용)

accountability?
(책임)

→ 국가마다 security level 다름

Applications of Anonymous Communication

- Privacy
  - Hide online transactions, Web browsing, etc., from intrusive governments, marketers and archivists
- Untraceable electronic mail
  - Corporate whistle-blowers
  - Political dissidents
  - Socially sensitive communications (online AA meeting)
- Digital cash
  - Electronic currency with properties of paper money (online purchases unlinkable to buyer's identity)
- Anonymous electronic voting
- Censorship-resistant publishing

What Is Anonymity?

- Anonymity is the state of being not identifiable within a set of subjects
  - You cannot be anonymous by yourself!
  - Hide your activities among others' similar activities
- Unlinkability of action and identity
  - For example, sender and his email are no more related after observing communication than they were before

Chaum's Mix

- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.

set a link system

암호화 + 재 전송

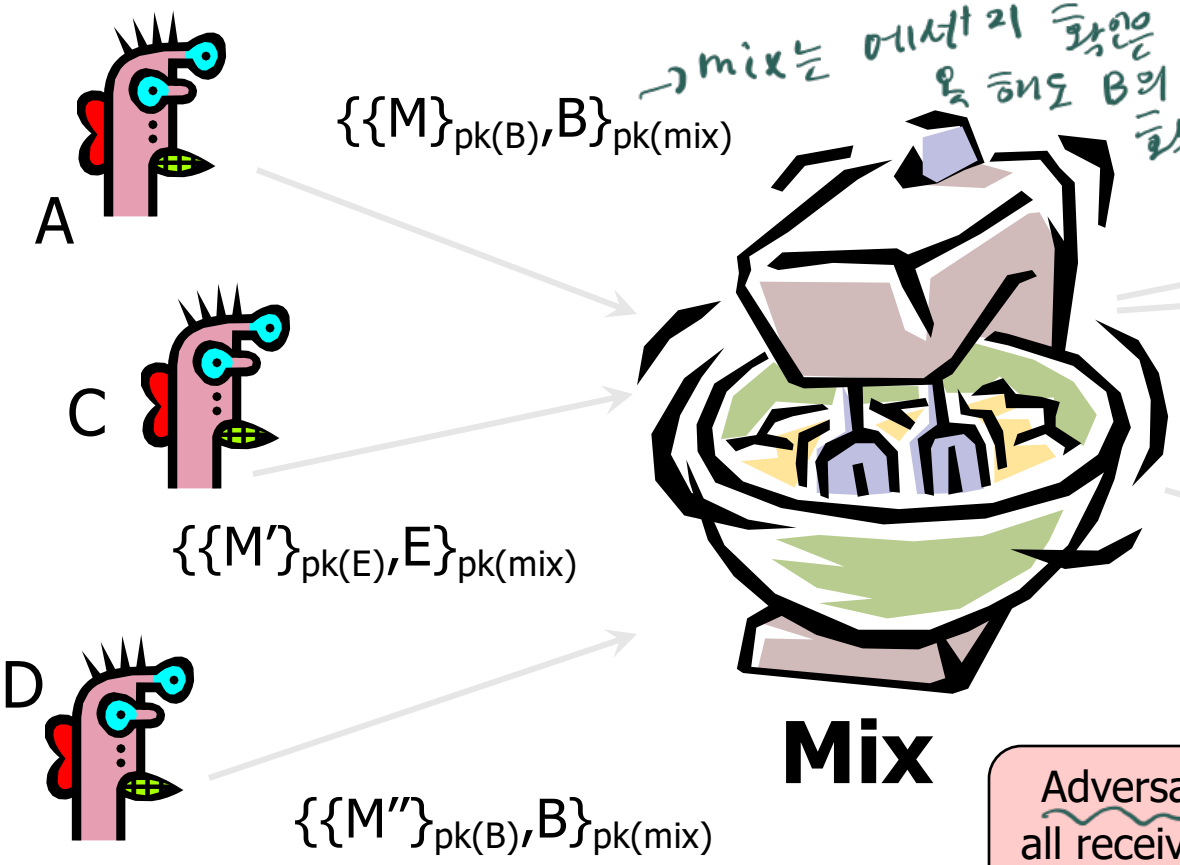
- Public key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms

신뢰받지못하는

가명

- Modern anonymity systems use Mix as the basic building block

Basic Mix Design

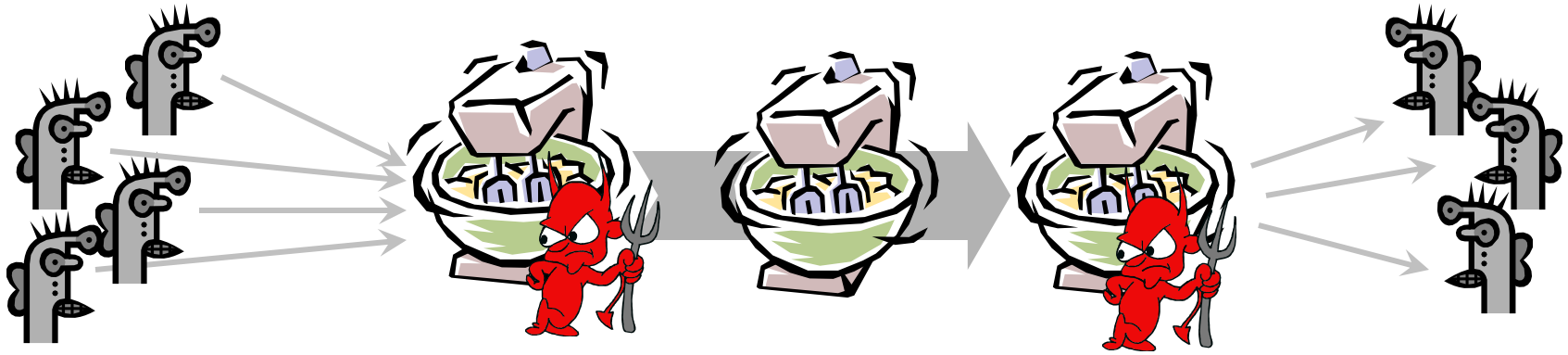


Does receiver know the sender?

What if M, M', M'' have different lengths?

Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Mix Cascade



- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes ("mixnet")
- Some of the mixes may be controlled by attacker, but even a single good mix guarantees anonymity
- Pad and buffer traffic to foil correlation attacks

Good enough?

Disadvantages of Basic Mixnets/Onion Routing

- Public-key encryption and decryption at each mix/router are computationally expensive ⇒ 매번 암호화/복호화로 cost↑ ⇒ 속도↓
- Basic mixnets have high latency
  - Ok for email, not ok for anonymous Web browsing → user submission 에서 문제
- Challenge: low-latency anonymity network

(한 번에 많은 메시지를 보낼수록 기밀성↑)

⇒ 검색에는 적합X

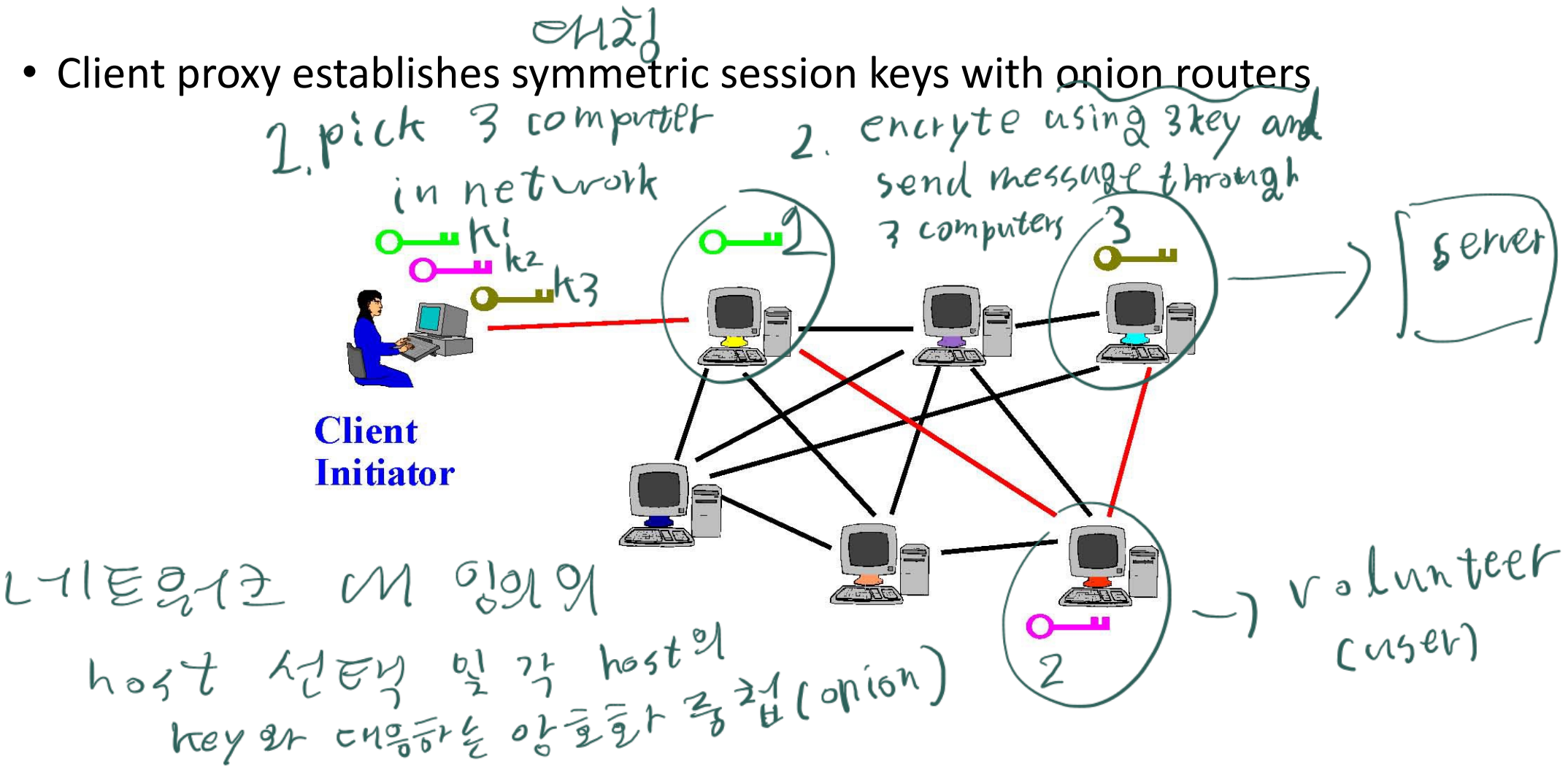
Tor (The Onion Routing)

- Second-generation onion routing network
  - Developed by Roger Dingledine, Nick Mathewson and Paul Syverson
  - Specifically designed for low-latency anonymous Internet communications
- Running since October 2003
- Around 2000 relays
- “Easy-to-use” client proxy

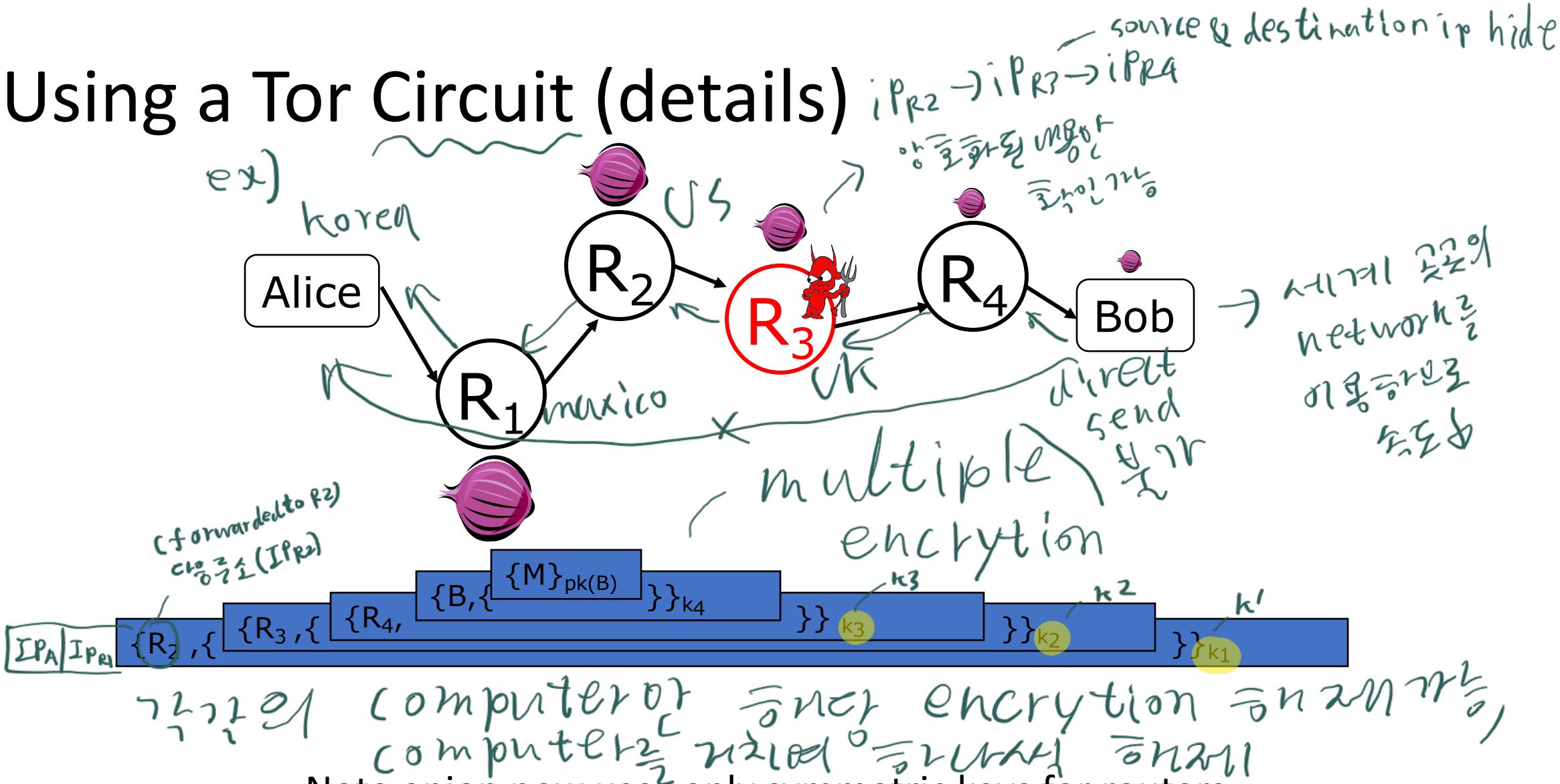
  - Freely available, can use it for anonymous browsing

Tor Circuit Setup

- Client proxy establishes symmetric session keys with onion routers



Using a Tor Circuit (details)



Note onion now uses only symmetric keys for routers

Tor's features

skip

- **Many applications** can share one circuit
  - Multiple TCP streams over one anonymous connection

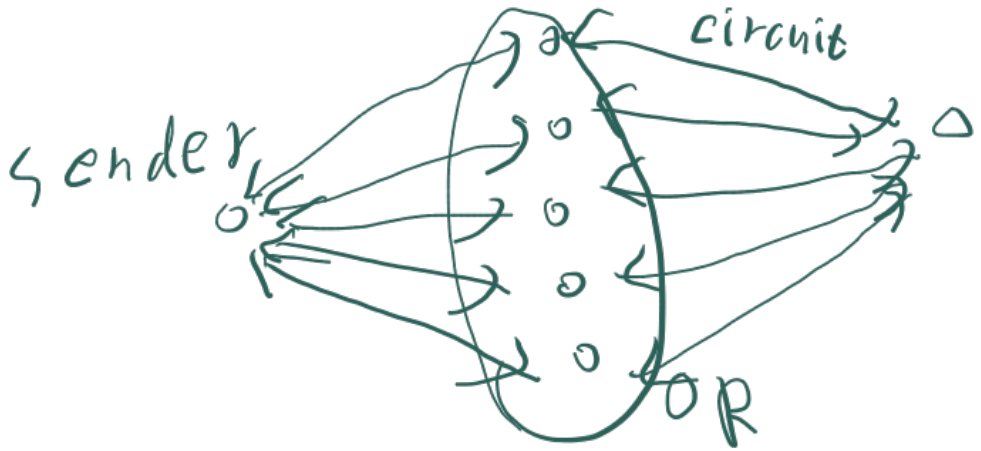
- Tor router **doesn't need root privileges**
  - Encourages people to set up their own routers
  - More participants == better anonymity for everyone

router에 필요한 특권이 없어 상대 자유로움

⇒ 기밀성↑

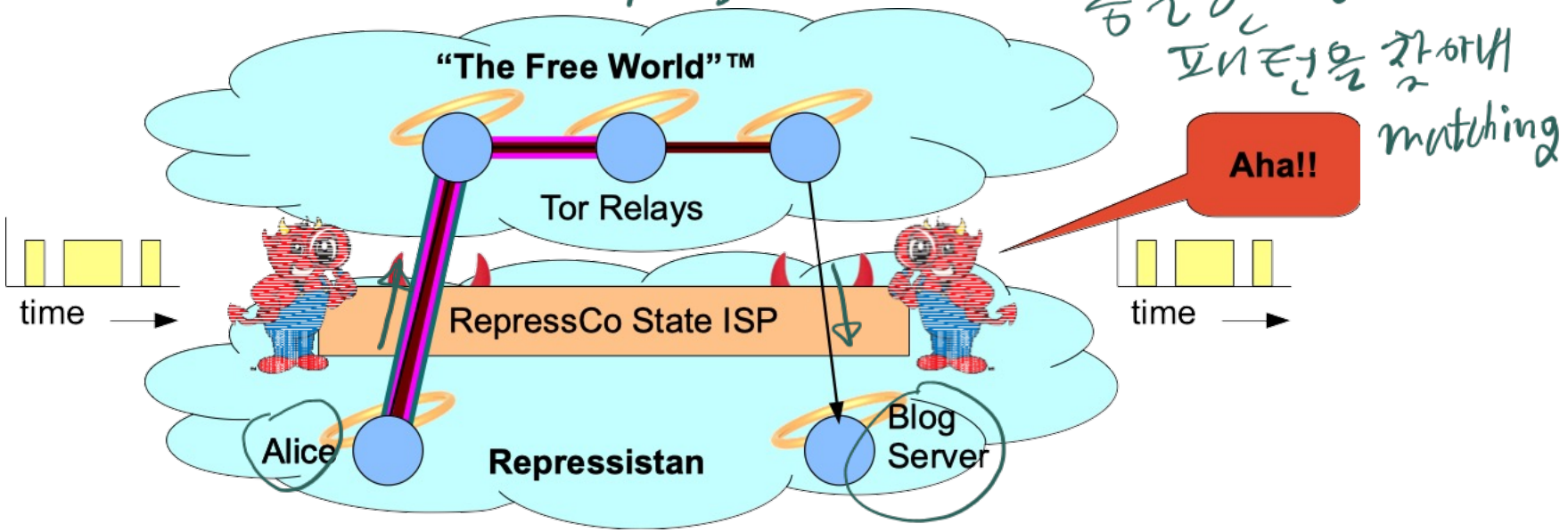
Hidden services

- Tor offers sender anonymity; how about responder anonymity?
- *Hidden services (.onion)* via *rendezvous points*
  - Hidden service selects and announces several ORs as its introduction points
  - Hidden service creates circuits to introduction points
  - Client picks one introduction point and construct a circuit
  - Stitched circuit maintains Tor circuit properties



Traffic Analysis: Example

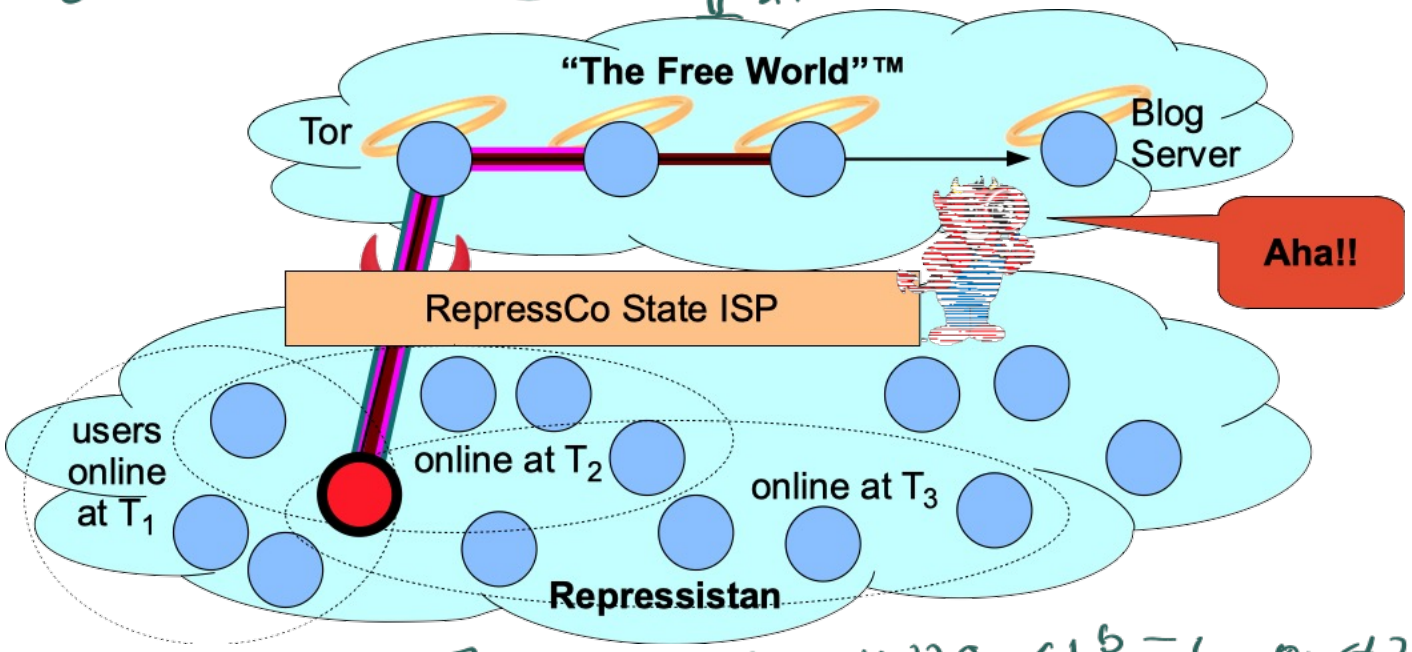
- Alice in Repressistan uses Tor to post onblog server hosted in Repressistan
- State ISP controls *both* entry and exit hops
- Fingerprint & correlate traffic to **deanonymize**



Intersection Attack: Example

skip

- Bob signs posts with pseudonym “AnoniBob”
  - Posts 3 signed messages at times T1, T2, T3
  - Police find sets of users online each time, **intersect**



ㄴ) 같은 익명(Anonibob)을 사용한 post가 올라온 시기의 이용자 집합의 교집합을 구해 사용자 특정

Next…

- *Chapter 5.1-5.3 Routing and Intra-AS Routing in the Internet: OSPF*