Anonymity and Privacy

Aggelos Kiayias

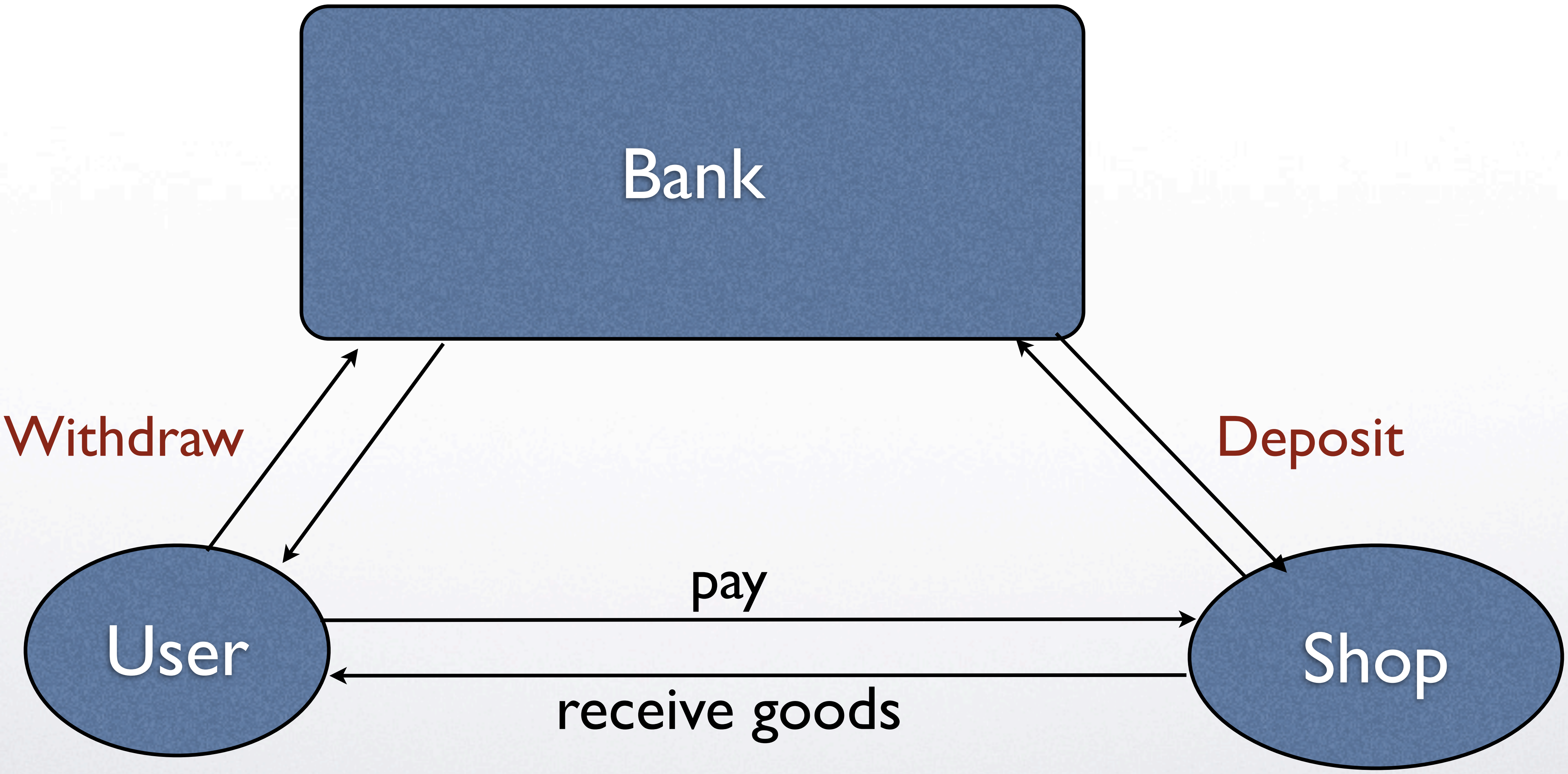
Anonymity in networks

- Anonymous Credentials
- Anonymous Payments
- Anonymous E-mail and Routing
- E-voting

E-payments

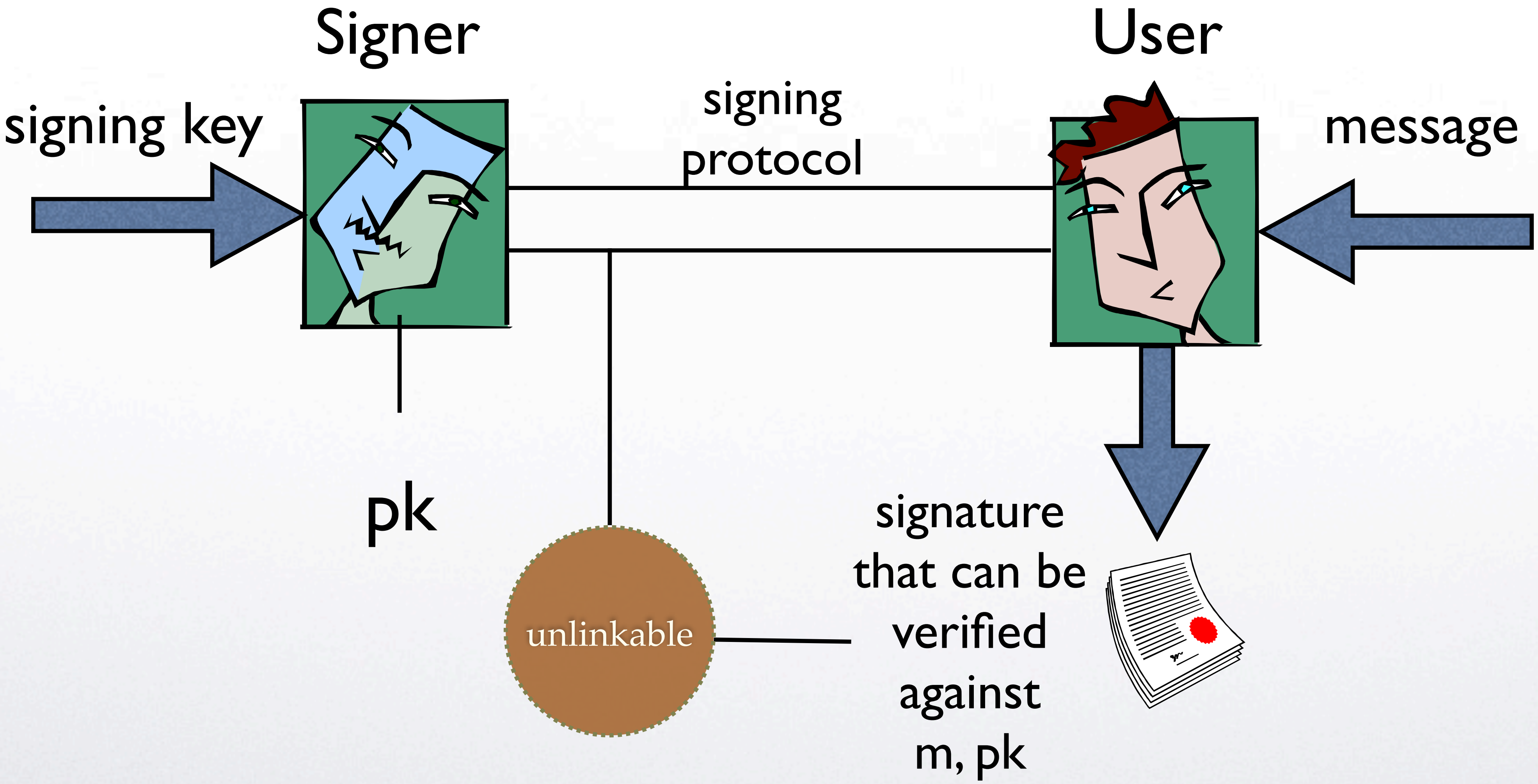
- How to simulate cash electronically?

(Electronic) Cash

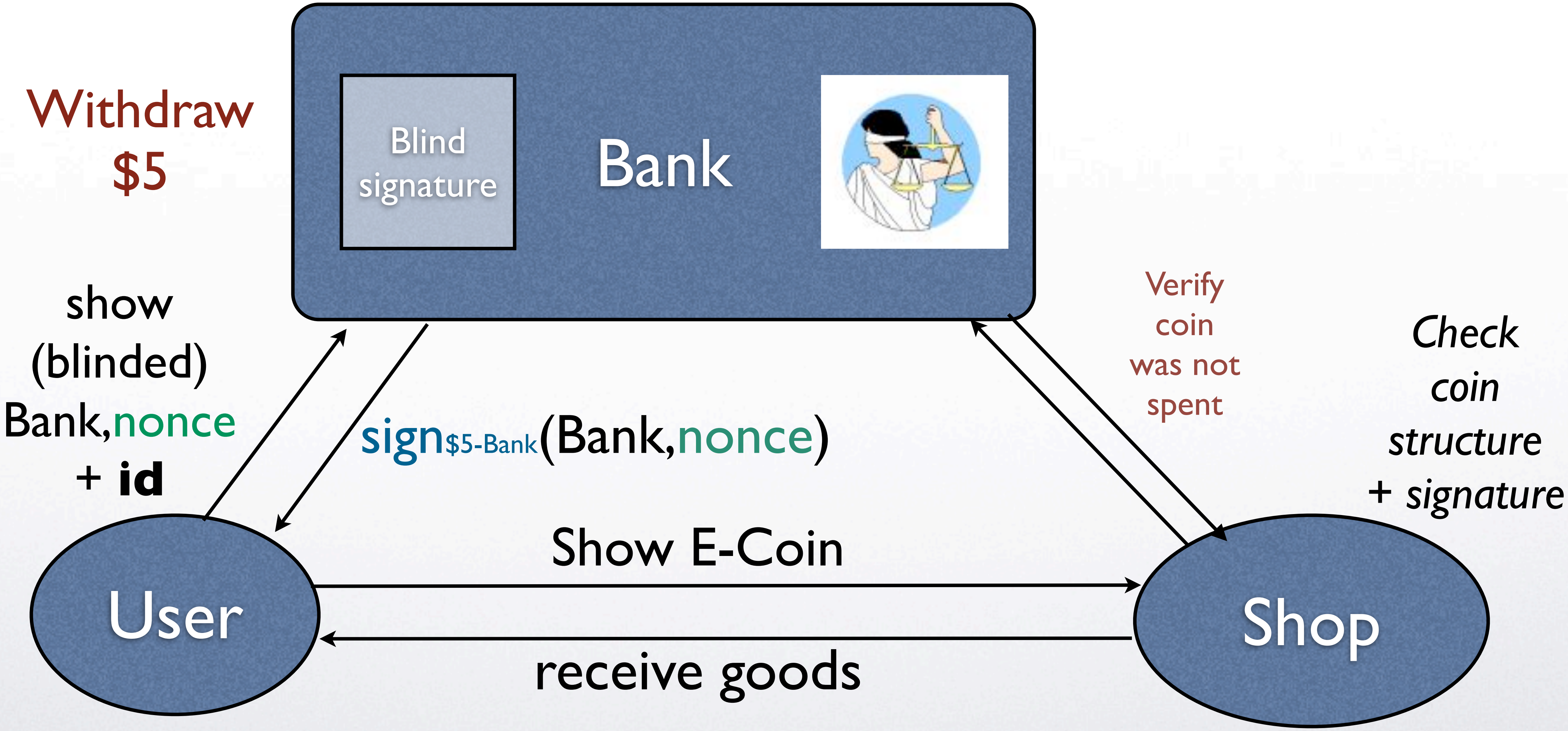


Blind Signatures

Chaum ‘82



Electronic Cash



Withdraw $5

Blind signature

Bank

show (blinded) Bank,nonce + **id**

$\text{sign}_{\$5\text{-Bank}}$(Bank,nonce)

Verify coin was not spent

Check coin structure + signature

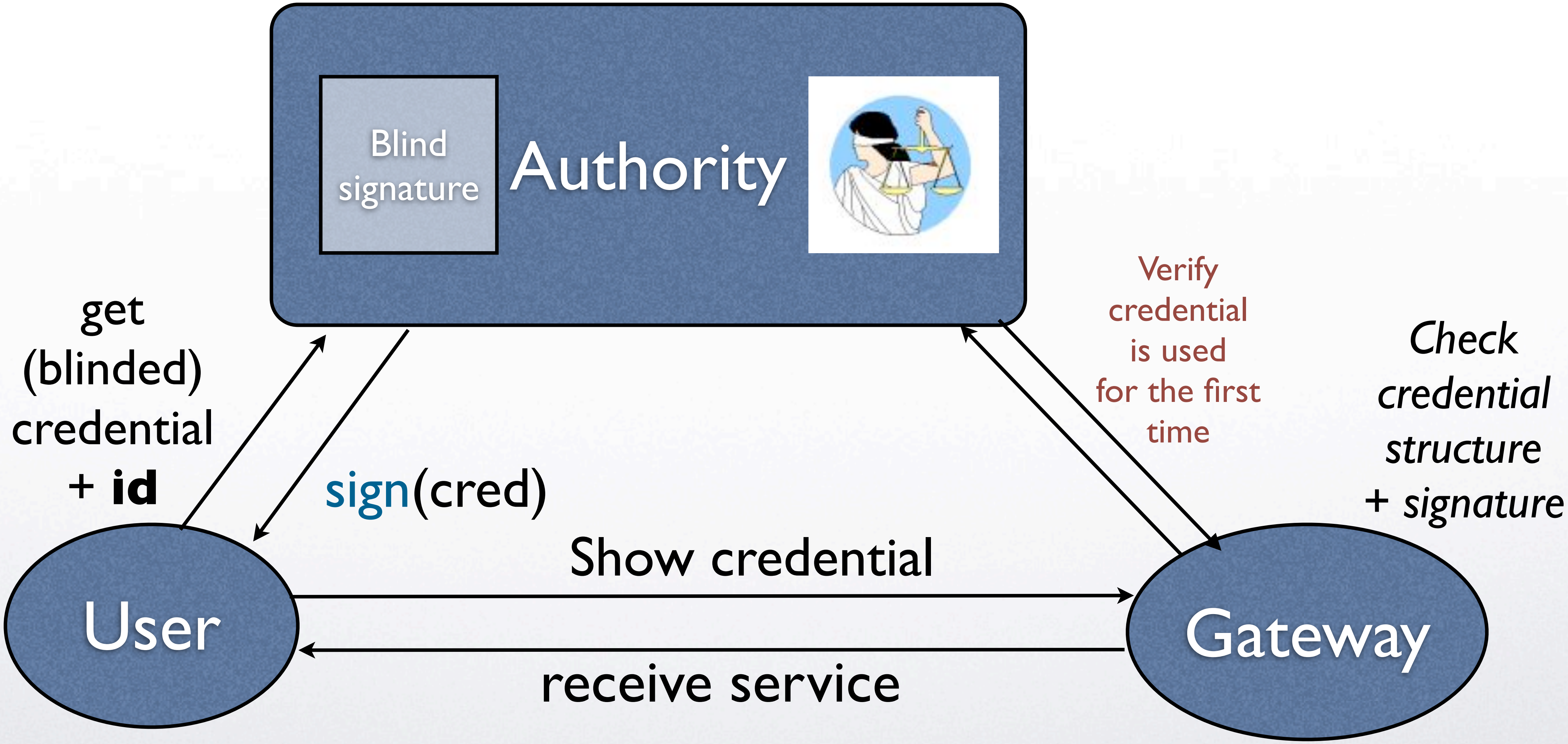
Show E-Coin

User

Shop

receive goods

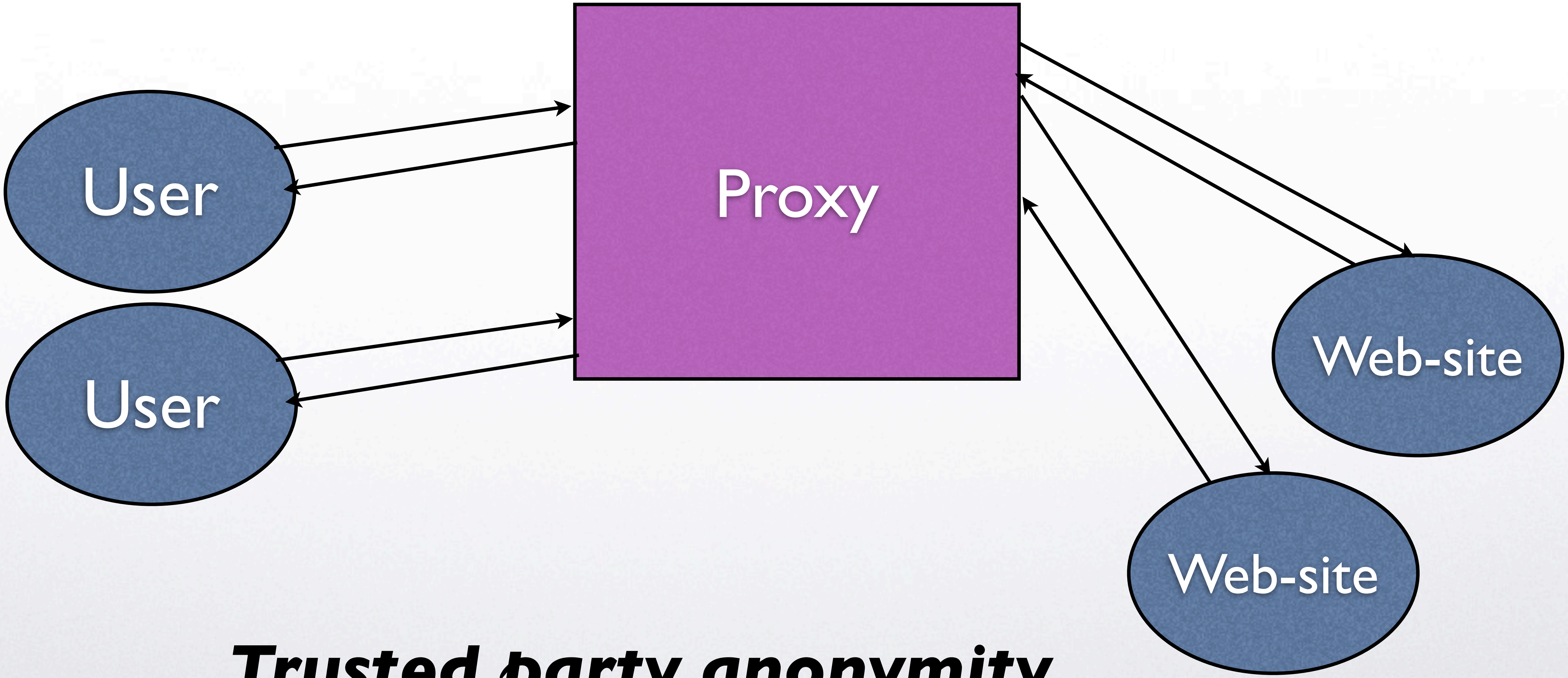
Anonymous Credentials


Blind signature
Authority
get (blinded) credential + **id**
sign(cred)
Verify credential is used for the first time
Check credential structure + signature
Show credential
receive service
User
Gateway

Applications

- Anonymous credentials: each credential can be used once and it is unlinkable to the act of showing the **id**.
- Can be used to disassociate the **id** from receiving the service.

Anonymous Communication



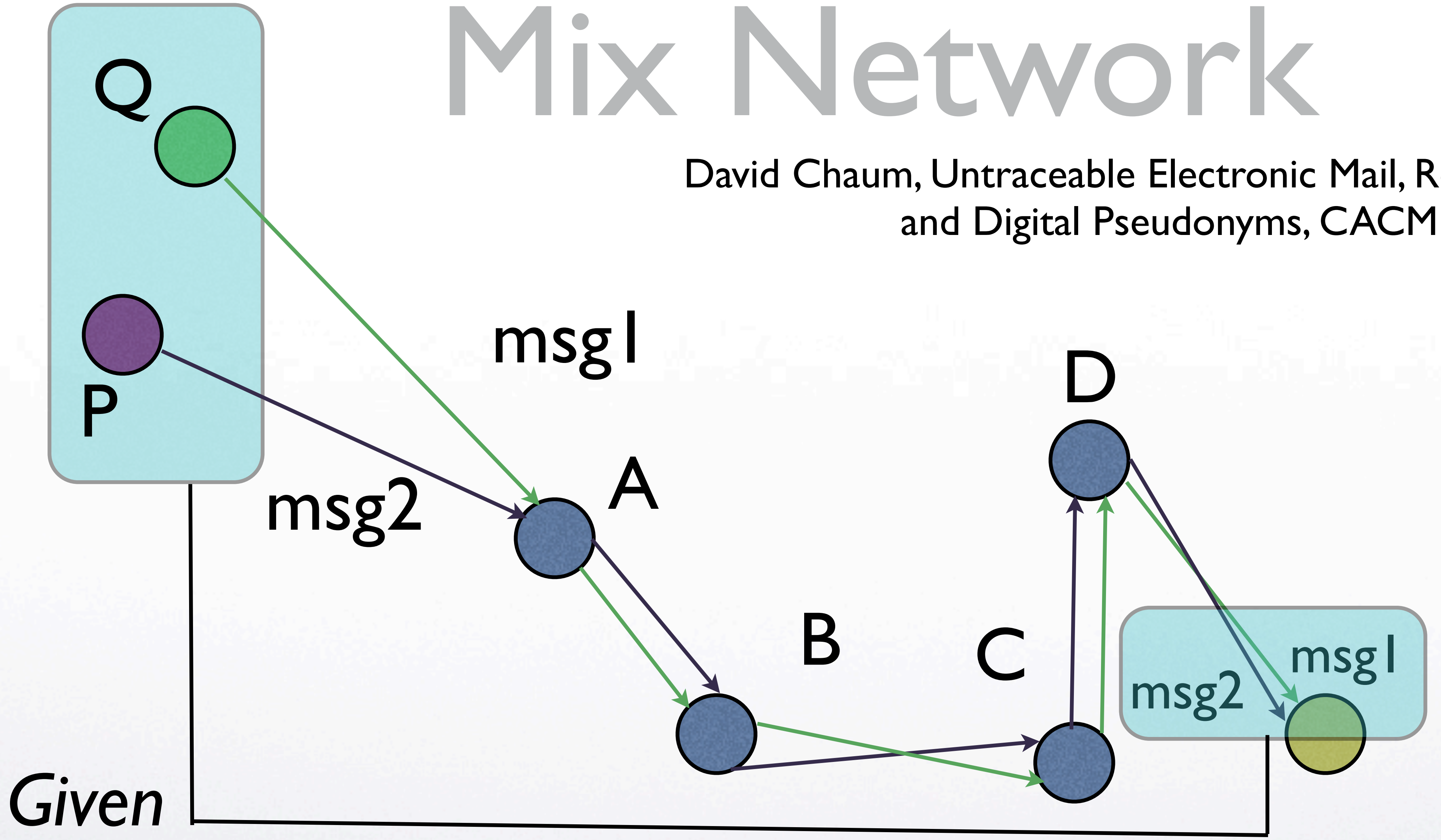
Trusted party anonymity

Anonymity and the Internet

- Whistle-blowing.
- Fear of censorship or prosecution.
- Communication regarding sensitive personal issues.

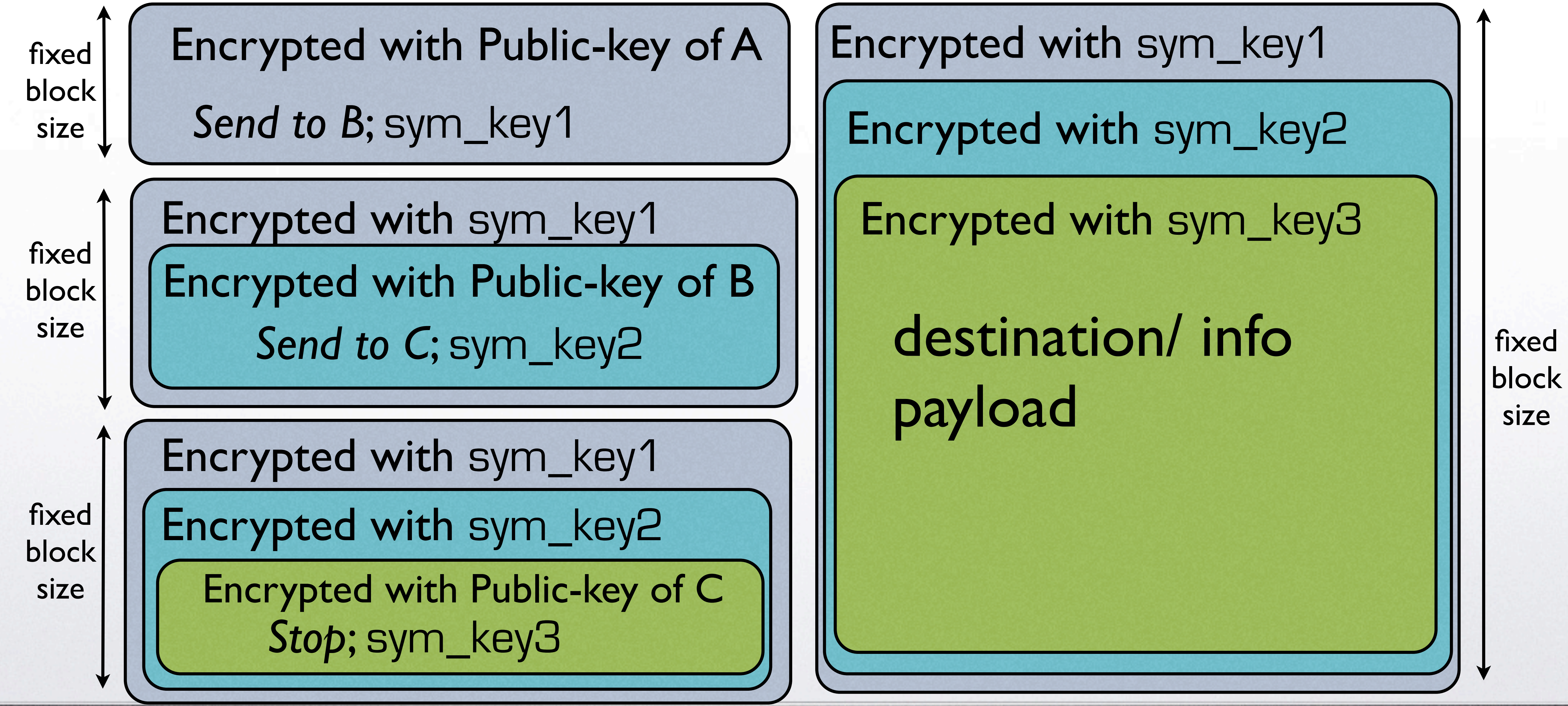
Mix Network

David Chaum, Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, CACM '81



Not possible to relate whether P send msg1 or msg2 and similarly for Q (as long as there is one honest mix)

Using Encryption



fixed block size

Encrypted with Public-key of A

Send to B; sym_key1

fixed block size

Encrypted with sym_key1

Encrypted with Public-key of B

Send to C; sym_key2

fixed block size

Encrypted with sym_key1

Encrypted with sym_key2

Encrypted with Public-key of C

Stop; sym_key3

Encrypted with sym_key1

Encrypted with sym_key2

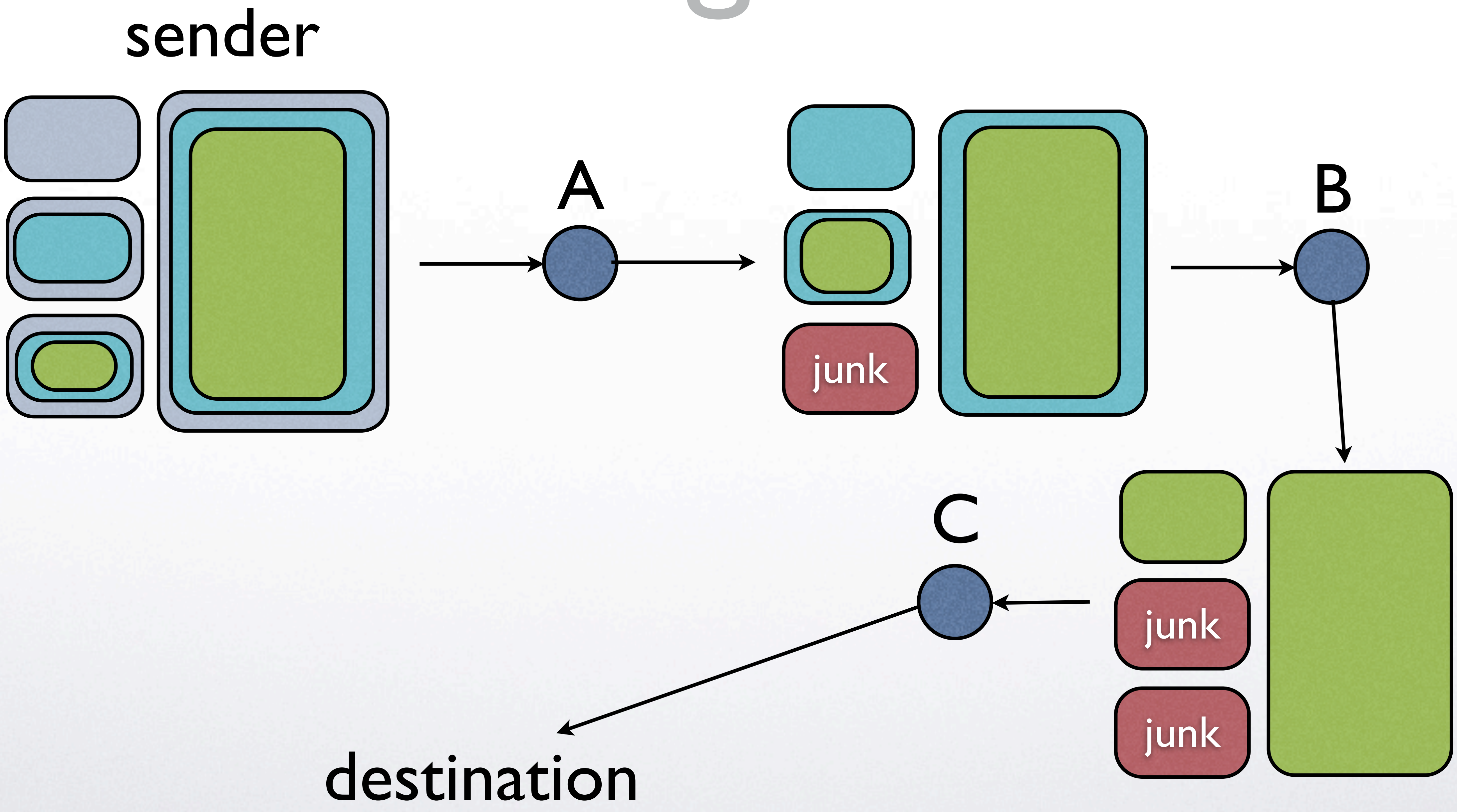
Encrypted with sym_key3

destination/ info

payload

fixed block size

Following the route



Mixmaster

- A mixnet implementation for anonymous remailing.
- Message may be split into packets and each packet is routed differently (but with the same final routing destination who should assemble).
- Each mix node relays messages in batches after randomly permuting them [consistent with the standard notion of mixnets].
- Payload can be either e-mail, or usenet posting or dummy message (why a dummy would be useful?).

http://www.abditum.com/mixmaster-spec.txt

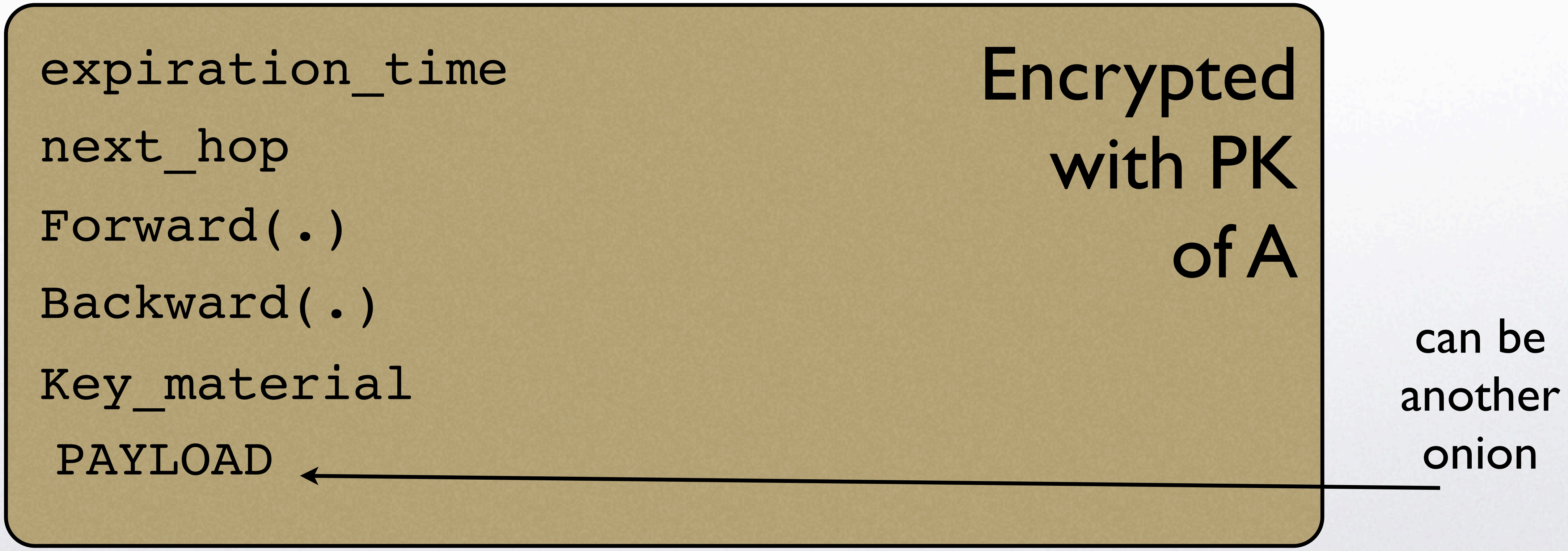
Limitations

- Lack of bidirectional communication: especially problematic if you want to use anonymity with bidirectional protocols.
- Possibility of replay attacks: can be handled by keeping a log of sent messages and compare.
- Abuse, flooding, etc.

Onion Routing

Hiding routing information, by D. M. Goldschlag, M.G.Reed, P.F. Syverson, Information Hiding Workshop 1996

- An onion directed to a node A is comprised of the following:

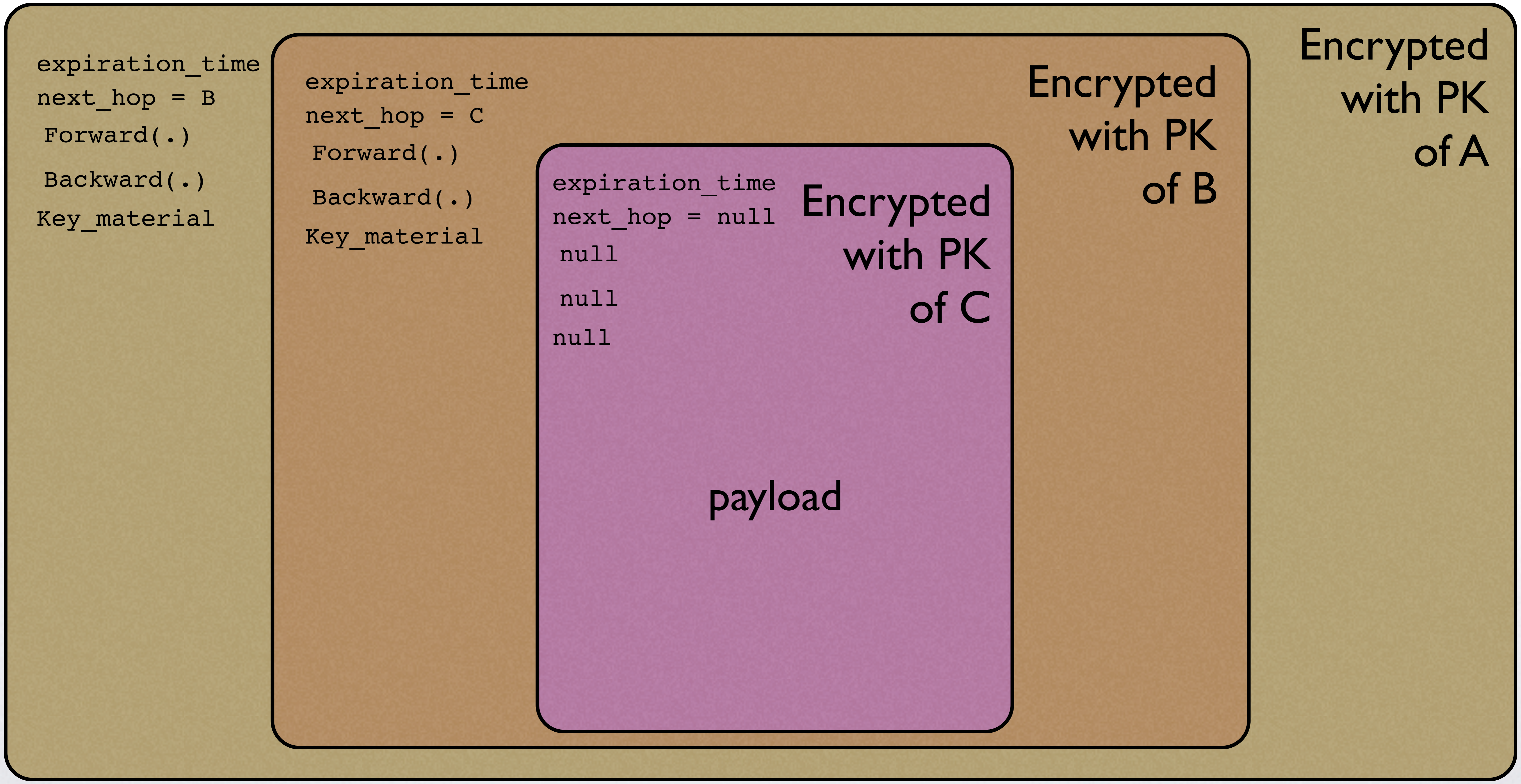


```
expiration_time
next_hop
Forward(.)
Backward(.)
Key_material
 PAYLOAD
```

Encrypted with PK of A

can be another onion

Onion Layers



expiration_time
next_hop = B
Forward(.)
Backward(.)
Key_material

expiration_time
next_hop = C
Forward(.)
Backward(.)
Key_material

expiration_time
next_hop = null
null
null
null

payload

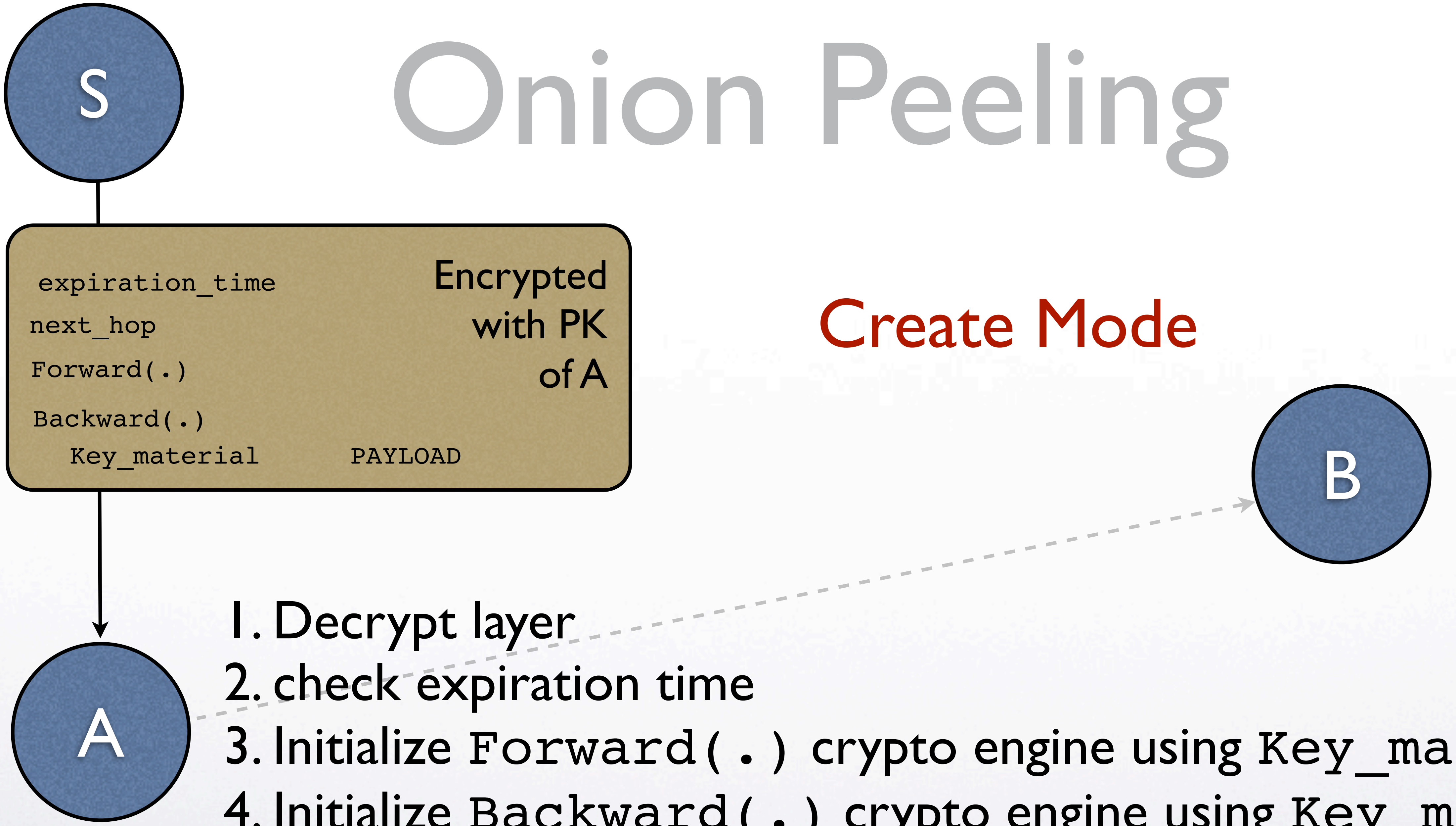
Encrypted with PK of C

Encrypted with PK of B

Encrypted with PK of A

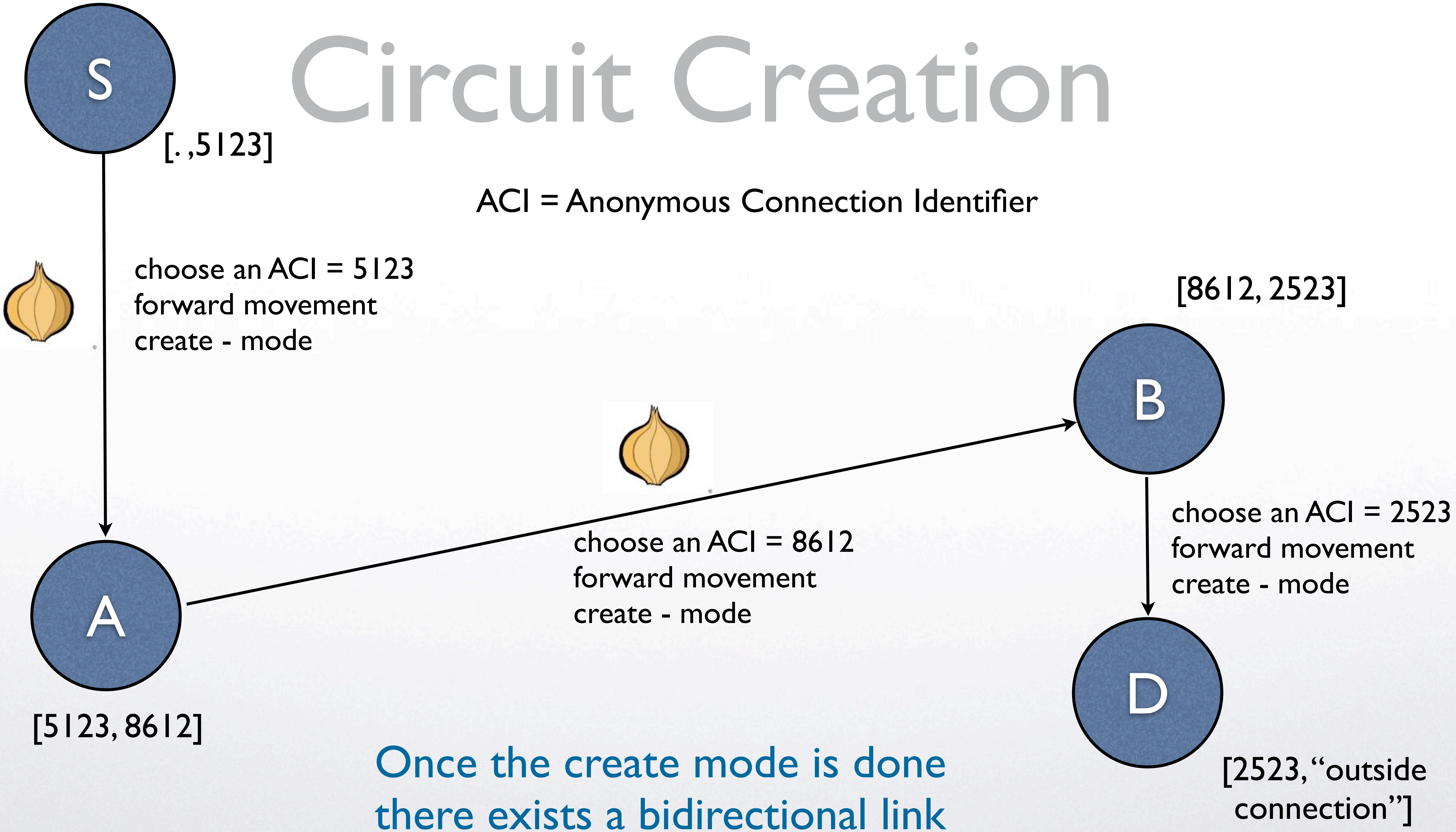
Onion Peeling

Create Mode



1. Decrypt layer
2. check expiration time
3. Initialize `Forward(.)` crypto engine using `Key_material`
4. Initialize `Backward(.)` crypto engine using `Key_material`
5. Pad `PAYLOAD` to maintain fixed size.
6. Forward `PAYLOAD` to `next_hop` node.

Circuit Creation



S

[. ,5123]

ACI = Anonymous Connection Identifier

choose an ACI = 5123
forward movement
create - mode

[8612, 2523]

B

choose an ACI = 8612
forward movement
create - mode

choose an ACI = 2523
forward movement
create - mode

A

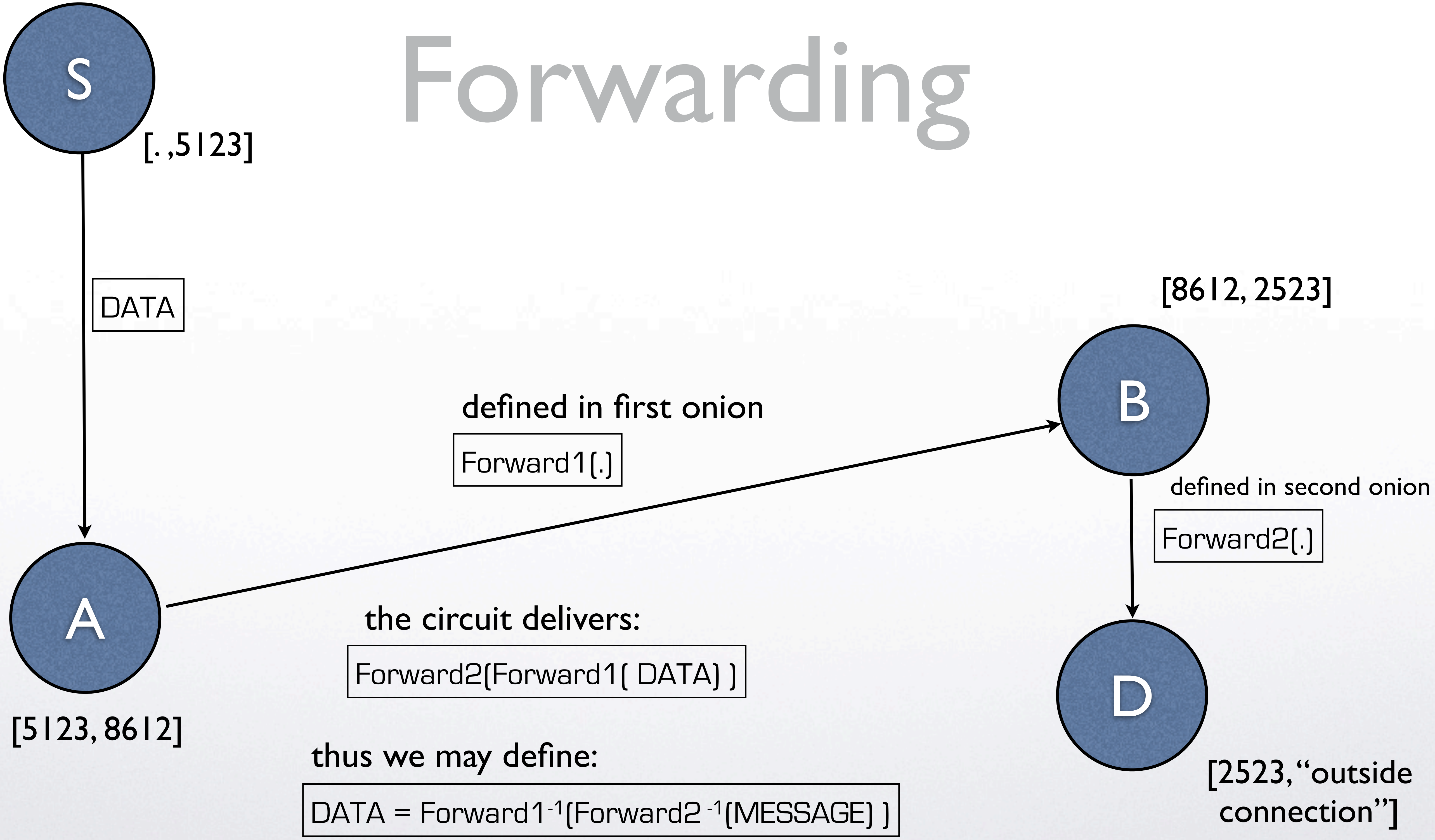
D

[5123, 8612]

[2523, "outside
connection"]

Once the create mode is done
there exists a bidirectional link

Forwarding



S

[.,5123]

DATA

A

[5123, 8612]

defined in first onion

Forward1(.)

B

[8612, 2523]

defined in second onion

Forward2(.)

D

[2523, "outside connection"]

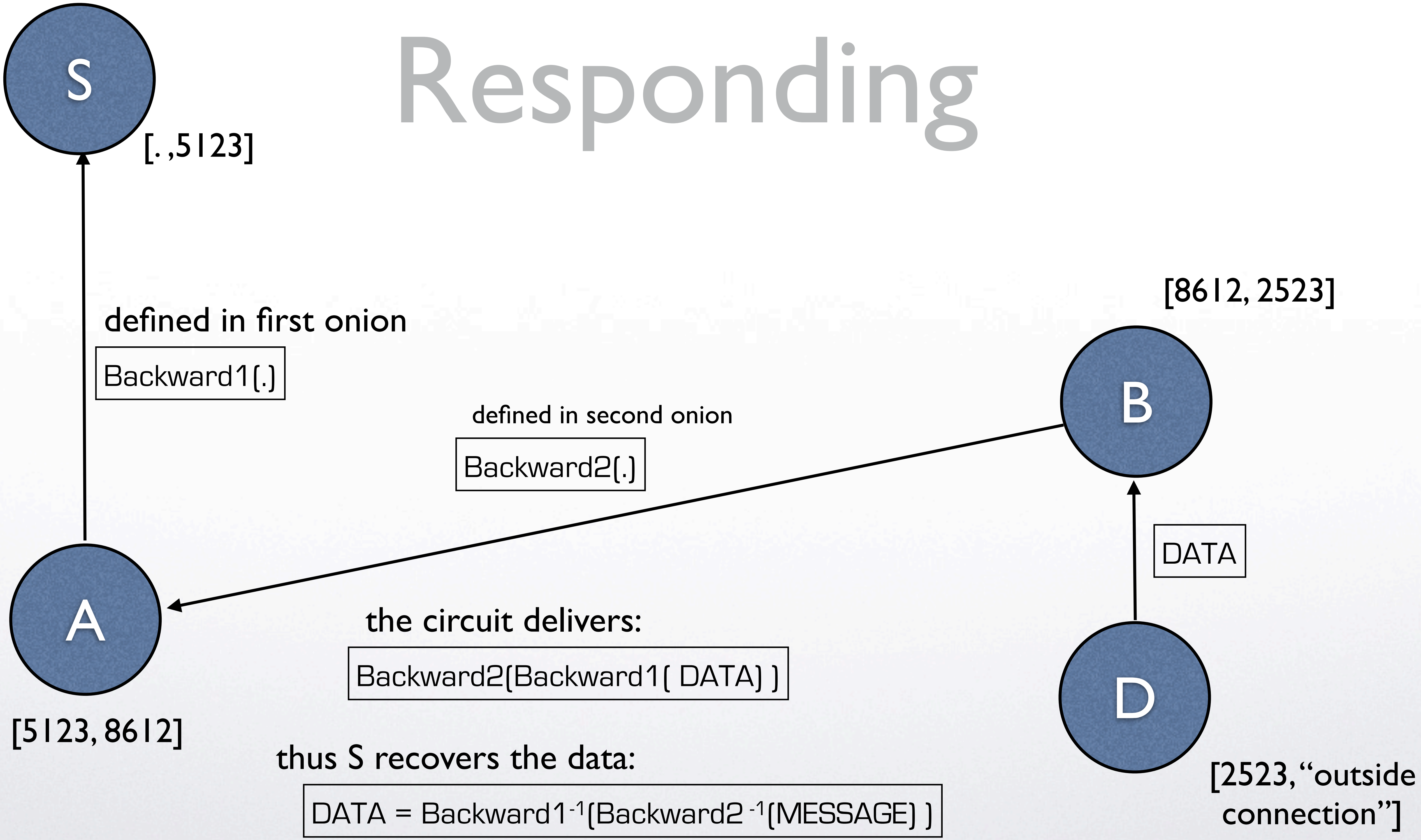
the circuit delivers:

Forward2(Forward1(DATA))

thus we may define:

DATA = Forward1^{-1}(Forward2 $^{-1}$(MESSAGE))

Responding



[. ,5123]

defined in first onion

Backward1(.)

defined in second onion

Backward2(.)

[8612, 2523]

DATA

the circuit delivers:

Backward2(Backward1(DATA))

[5123, 8612]

thus S recovers the data:

DATA = Backward1^{-1}(Backward2 $^{-1}$(MESSAGE))

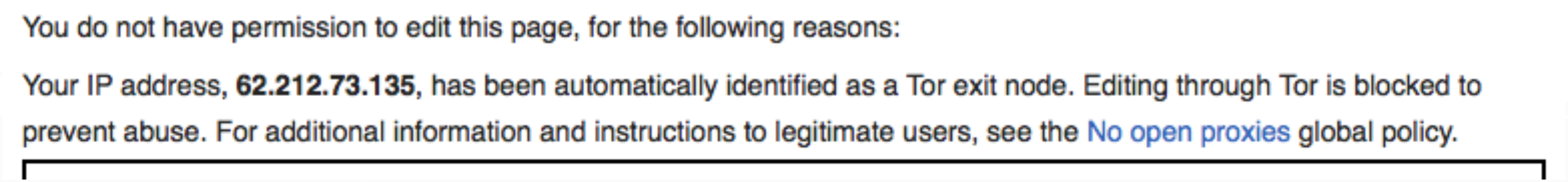
[2523, "outside connection"]

Implementing Onion Routing

Tor http://tor.eff.org/

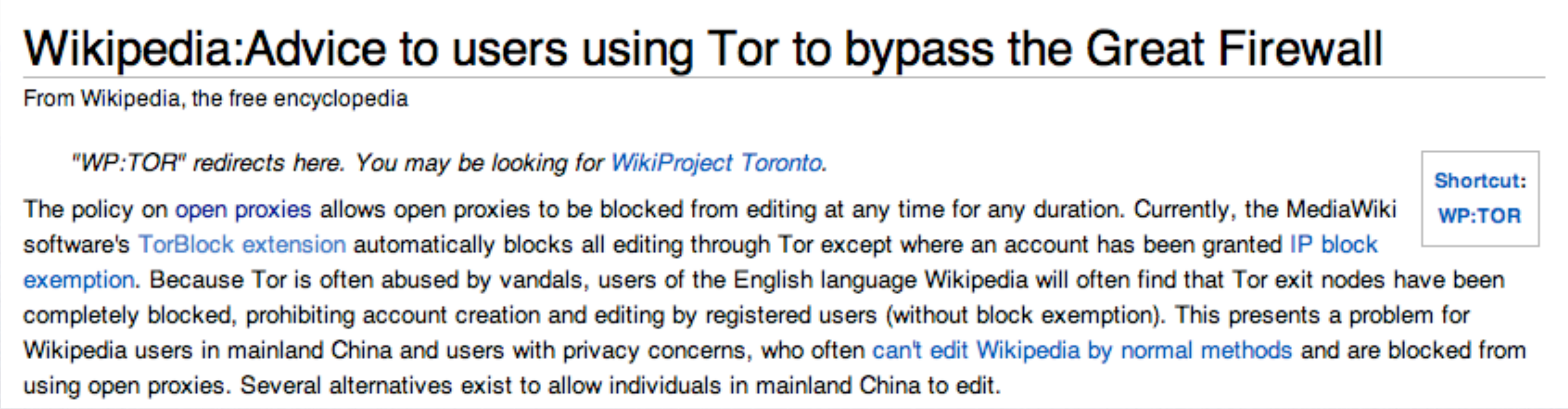
- Each host runs an onion proxy locally.
- TCP/IP traffic can be directed through virtual circuits created by onions.

Problems with Tor



You do not have permission to edit this page, for the following reasons:

Your IP address, **62.212.73.135**, has been automatically identified as a Tor exit node. Editing through Tor is blocked to prevent abuse. For additional information and instructions to legitimate users, see the No open proxies global policy.



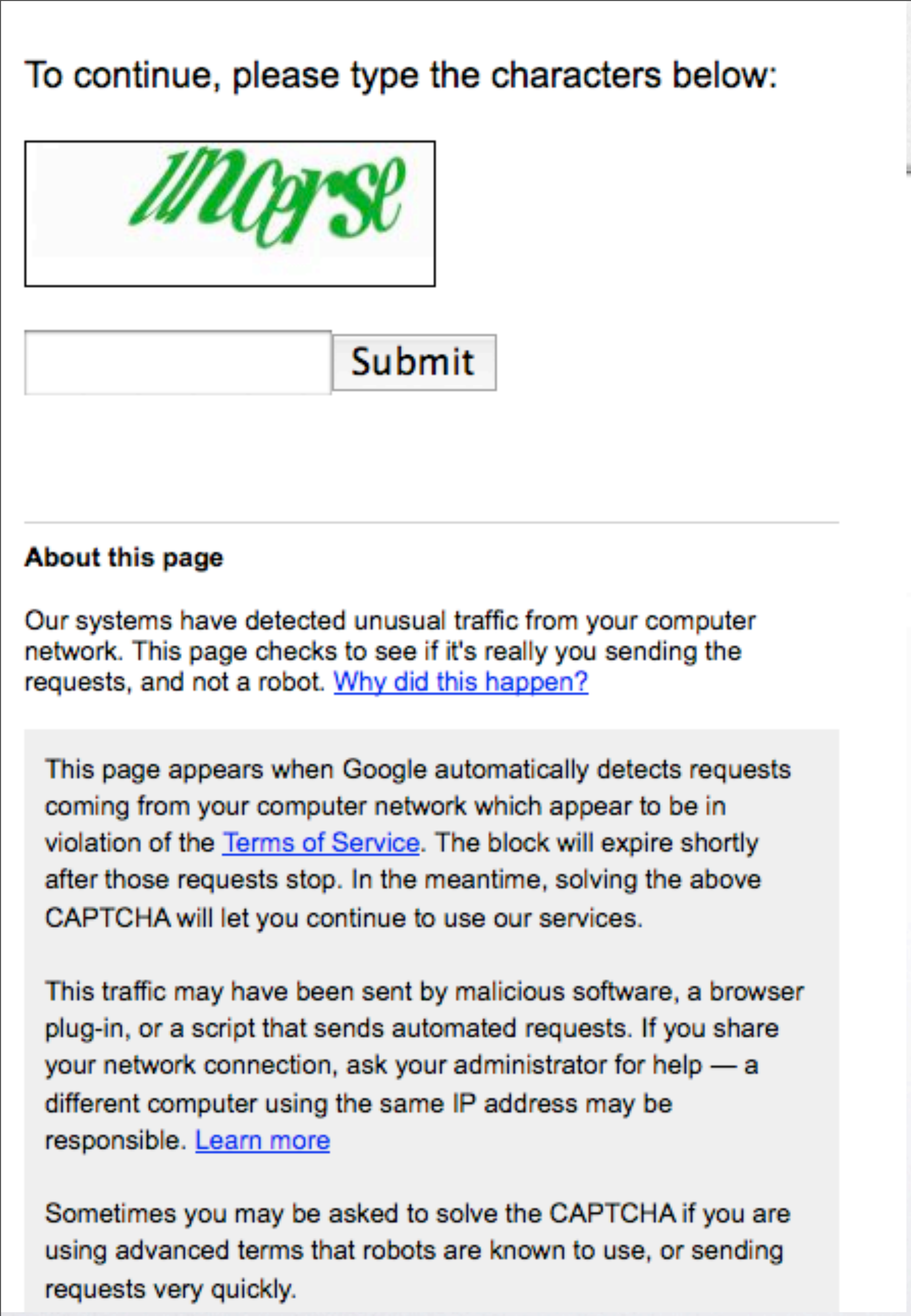
Wikipedia:Advice to users using Tor to bypass the Great Firewall

From Wikipedia, the free encyclopedia

"WP:TOR" redirects here. You may be looking for WikiProject Toronto.

The policy on open proxies allows open proxies to be blocked from editing at any time for any duration. Currently, the MediaWiki software's TorBlock extension automatically blocks all editing through Tor except where an account has been granted IP block exemption. Because Tor is often abused by vandals, users of the English language Wikipedia will often find that Tor exit nodes have been completely blocked, prohibiting account creation and editing by registered users (without block exemption). This presents a problem for Wikipedia users in mainland China and users with privacy concerns, who often can't edit Wikipedia by normal methods and are blocked from using open proxies. Several alternatives exist to allow individuals in mainland China to edit.

Google



To continue, please type the characters below:

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

This page appears when Google automatically detects requests coming from your computer network which appear to be in violation of the Terms of Service. The block will expire shortly after those requests stop. In the meantime, solving the above CAPTCHA will let you continue to use our services.

This traffic may have been sent by malicious software, a browser plug-in, or a script that sends automated requests. If you share your network connection, ask your administrator for help — a different computer using the same IP address may be responsible. Learn more

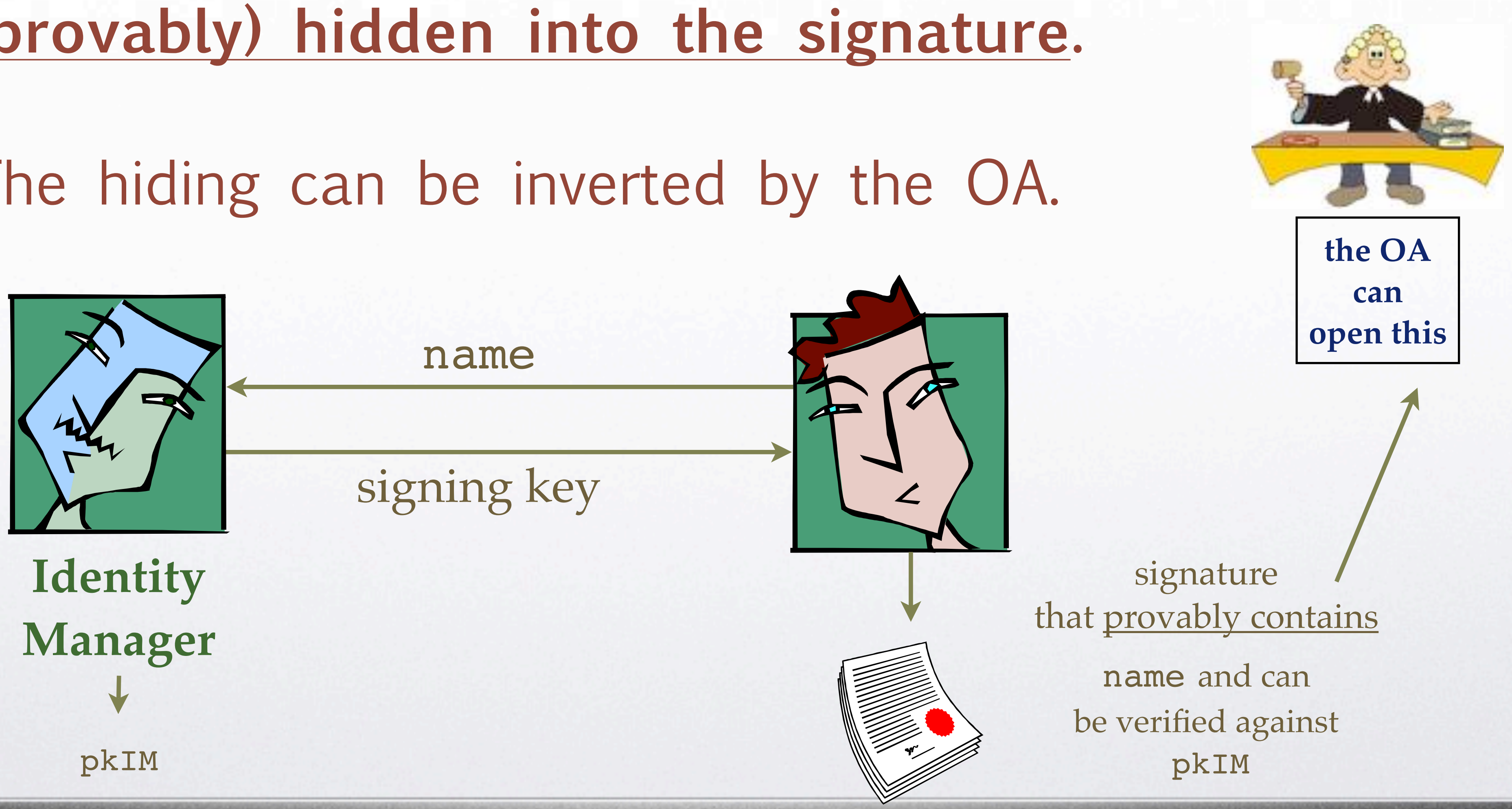
Sometimes you may be asked to solve the CAPTCHA if you are using advanced terms that robots are known to use, or sending requests very quickly.

An example where google "banned" a Tor exit point.

Hidden Identity Based Signatures

Kiayias - Zhou (2007)

- **Hidden ID-based signatures**: a digital signature where the corresponding public-key is your name & **is (provably) hidden into the signature**.
- The hiding can be inverted by the OA.



name

signing key

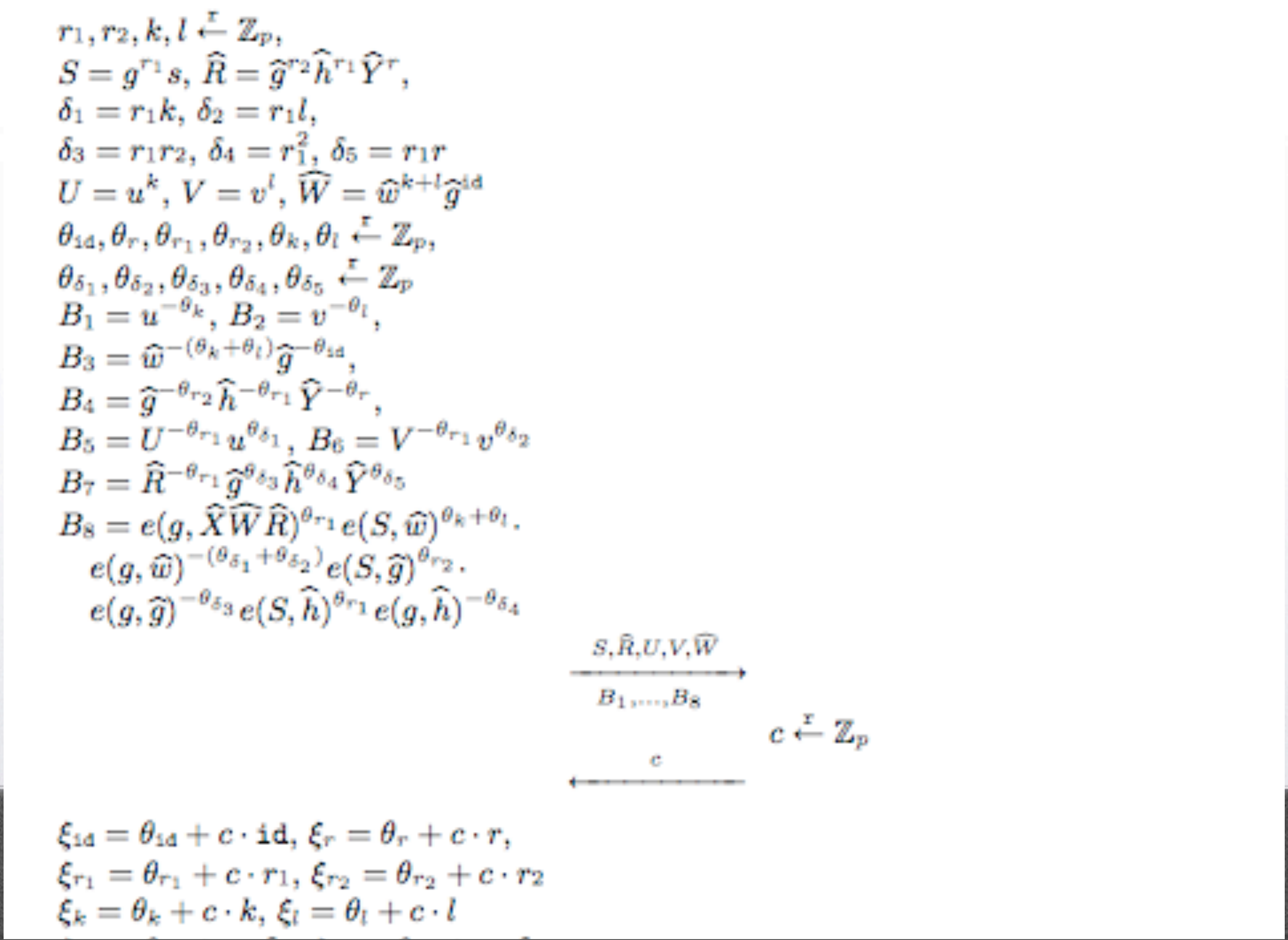
Identity Manager

pkIM

the OA can open this

signature that provably contains name and can be verified against pkIM

a glimpse



$r_1, r_2, k, l \xleftarrow{r} \mathbb{Z}_p,$

$S = g^{r_1} s,\ \widehat{R} = \widehat{g}^{r_2} \widehat{h}^{r_1} \widehat{Y}^{r},$

$\delta_1 = r_1 k,\ \delta_2 = r_1 l,$

$\delta_3 = r_1 r_2,\ \delta_4 = r_1^2,\ \delta_5 = r_1 r$

$U = u^k,\ V = v^l,\ \widehat{W} = \widehat{w}^{k+l} \widehat{g}^{\mathtt{id}}$

$\theta_{\mathtt{id}}, \theta_r, \theta_{r_1}, \theta_{r_2}, \theta_k, \theta_l \xleftarrow{r} \mathbb{Z}_p,$

$\theta_{\delta_1}, \theta_{\delta_2}, \theta_{\delta_3}, \theta_{\delta_4}, \theta_{\delta_5} \xleftarrow{r} \mathbb{Z}_p$

$B_1 = u^{-\theta_k},\ B_2 = v^{-\theta_l},$

$B_3 = \widehat{w}^{-(\theta_k + \theta_l)} \widehat{g}^{-\theta_{\mathtt{id}}},$

$B_4 = \widehat{g}^{-\theta_{r_2}} \widehat{h}^{-\theta_{r_1}} \widehat{Y}^{-\theta_r},$

$B_5 = U^{-\theta_{r_1}} u^{\theta_{\delta_1}},\ B_6 = V^{-\theta_{r_1}} v^{\theta_{\delta_2}}$

$B_7 = \widehat{R}^{-\theta_{r_1}} \widehat{g}^{\theta_{\delta_3}} \widehat{h}^{\theta_{\delta_4}} \widehat{Y}^{\theta_{\delta_5}}$

$B_8 = e(g, \widehat{X}\widehat{W}\widehat{R})^{\theta_{r_1}} e(S, \widehat{w})^{\theta_k + \theta_l} \cdot$
$\quad e(g, \widehat{w})^{-(\theta_{\delta_1} + \theta_{\delta_2})} e(S, \widehat{g})^{\theta_{r_2}} \cdot$
$\quad e(g, \widehat{g})^{-\theta_{\delta_3}} e(S, \widehat{h})^{\theta_{r_1}} e(g, \widehat{h})^{-\theta_{\delta_4}}$

$$\xrightarrow[B_1,\ldots,B_8]{S,\widehat{R},U,V,\widehat{W}}$$

$$c \xleftarrow{r} \mathbb{Z}_p$$

$$\xleftarrow{c}$$

$\xi_{\mathtt{id}} = \theta_{\mathtt{id}} + c \cdot \mathtt{id},\ \xi_r = \theta_r + c \cdot r,$

$\xi_{r_1} = \theta_{r_1} + c \cdot r_1,\ \xi_{r_2} = \theta_{r_2} + c \cdot r_2$

$\xi_k = \theta_k + c \cdot k,\ \xi_l = \theta_l + c \cdot l$

Applying HiddenIBS to TOR

- How to calibrate anonymity of Tor using Hidden-IBS
    - Add *three entities* in Tor:
    - Identity manager (IM)
    - A Disputes & Grievances (D&G) database
    - An opening authority (OA)

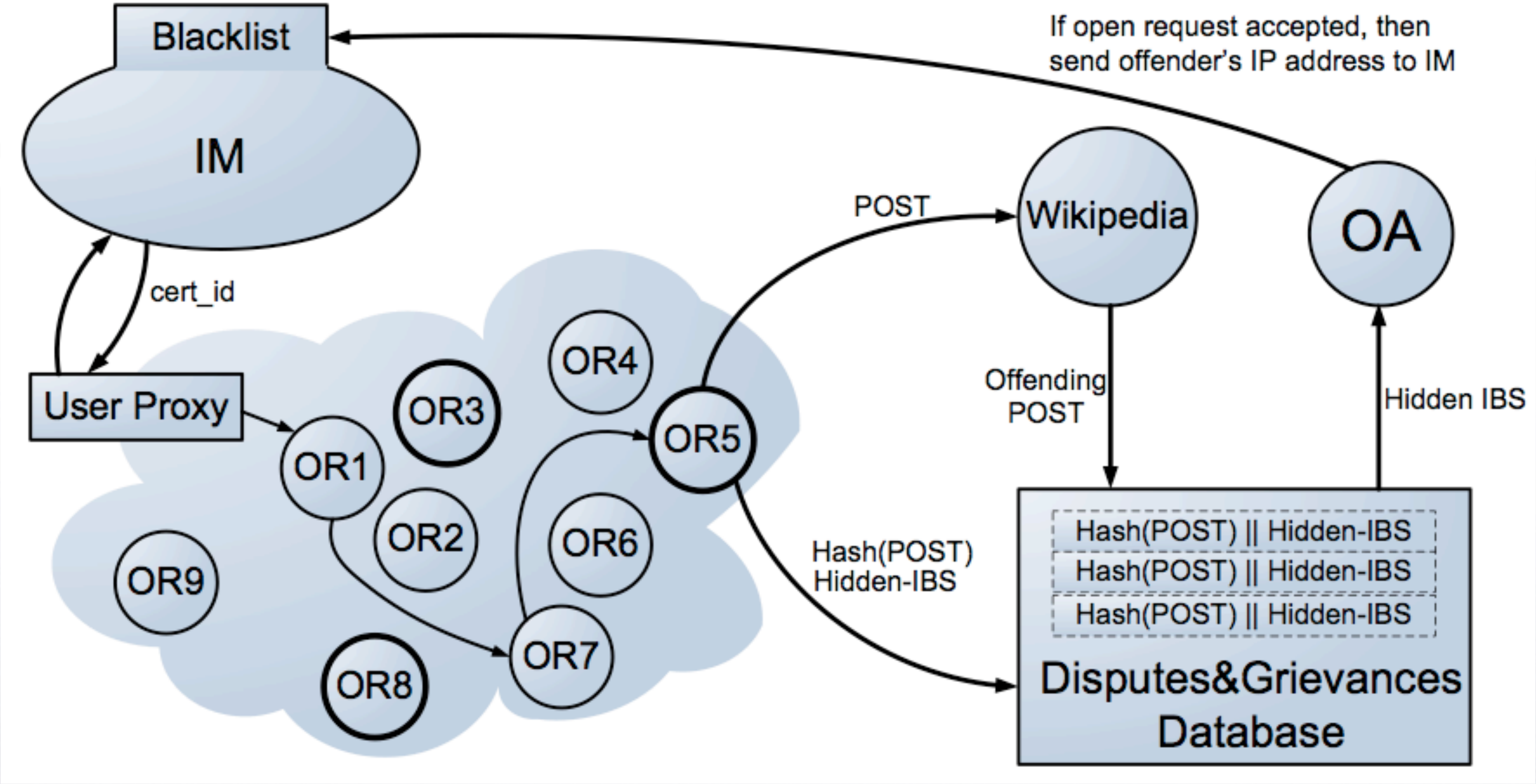
Goals

- **Minimal anonymity loss** if misbehavior does not occur.
- **Minimal efficiency impact** for services that do not require anonymity control.
- **Transparency** to service providers.
    - the service providers accepting Tor traffic should not have to **assist** the system [except providing the necessary forensic information]

HiddenIBS + Tor

- **Modify Tor Exit** policy: certain type of packets must be HiddenIBS'ed [e.g., **http POST requests**]
- **Modify user's onion proxy** : it catches such packets and signs them using user's HiddenIBS signing credential.
    - If user does not have a credential, the onion proxy directs user to IM to get one.
- **Modify exit point**: beyond forwarding the packet it registers it to the D&G database (only the hash + signature need to be registered).

Overview


Blacklist
IM
If open request accepted, then send offender's IP address to IM
cert_id
User Proxy
OR1
OR2
OR3
OR4
OR5
OR6
OR7
OR8
OR9
POST
Wikipedia
OA
Offending POST
Hidden IBS
Hash(POST) Hidden-IBS
Hash(POST) || Hidden-IBS
Hash(POST) || Hidden-IBS
Hash(POST) || Hidden-IBS
Disputes&Grievances Database

realization issues

- What is a user's identity and how does the Identity Manager verifies it?
  - IP address, e-mail address, id in a reputation system, etc.
- How to deal with misbehaving users?
  - black-listing. revocation of credentials, time-based or reactive.

anonymity scalability

- Disputes & Grievances database contains:
  - hashes of packets + HiddenIBS signatures. we include nonces in the packets to increase entropy.
- The D&G size is manageable:
  - using a SHA-256 hash + our bilinear map based scheme with a 10GB we can store ~ 27.3 million entries.

properties

- **Minimal anonymity loss** : D&G database leaks no information about Tor usage, if no misbehavior occurs.

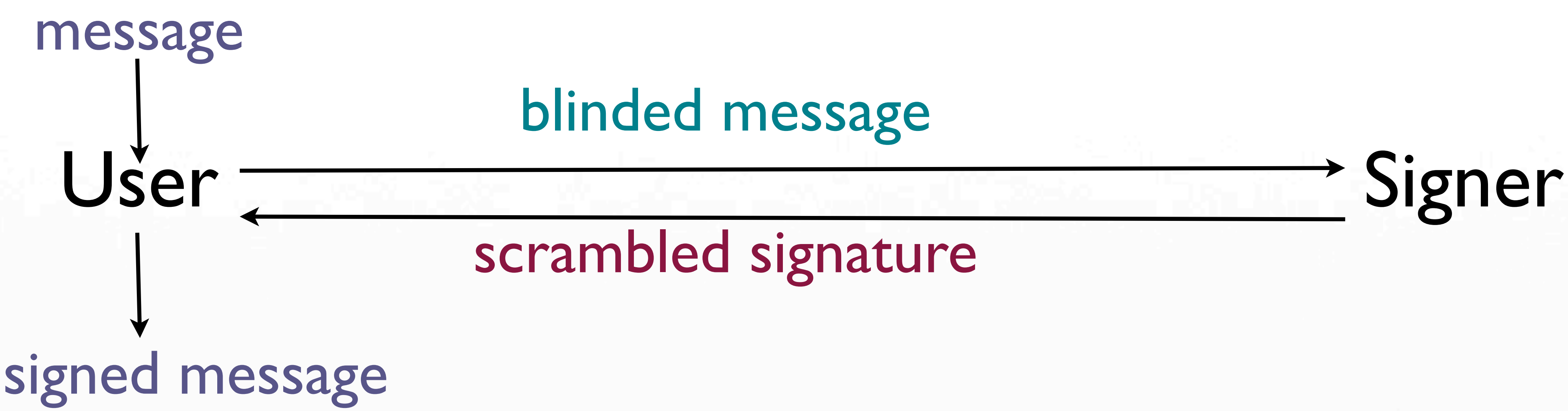
- **Minimal efficiency impact** for services that do not require anonymity control: only a few types of packets need to be signed.

- **Transparency** to service providers: a simple packet log is enough to make an abuse report resulting in blacklisting a user.

other applications

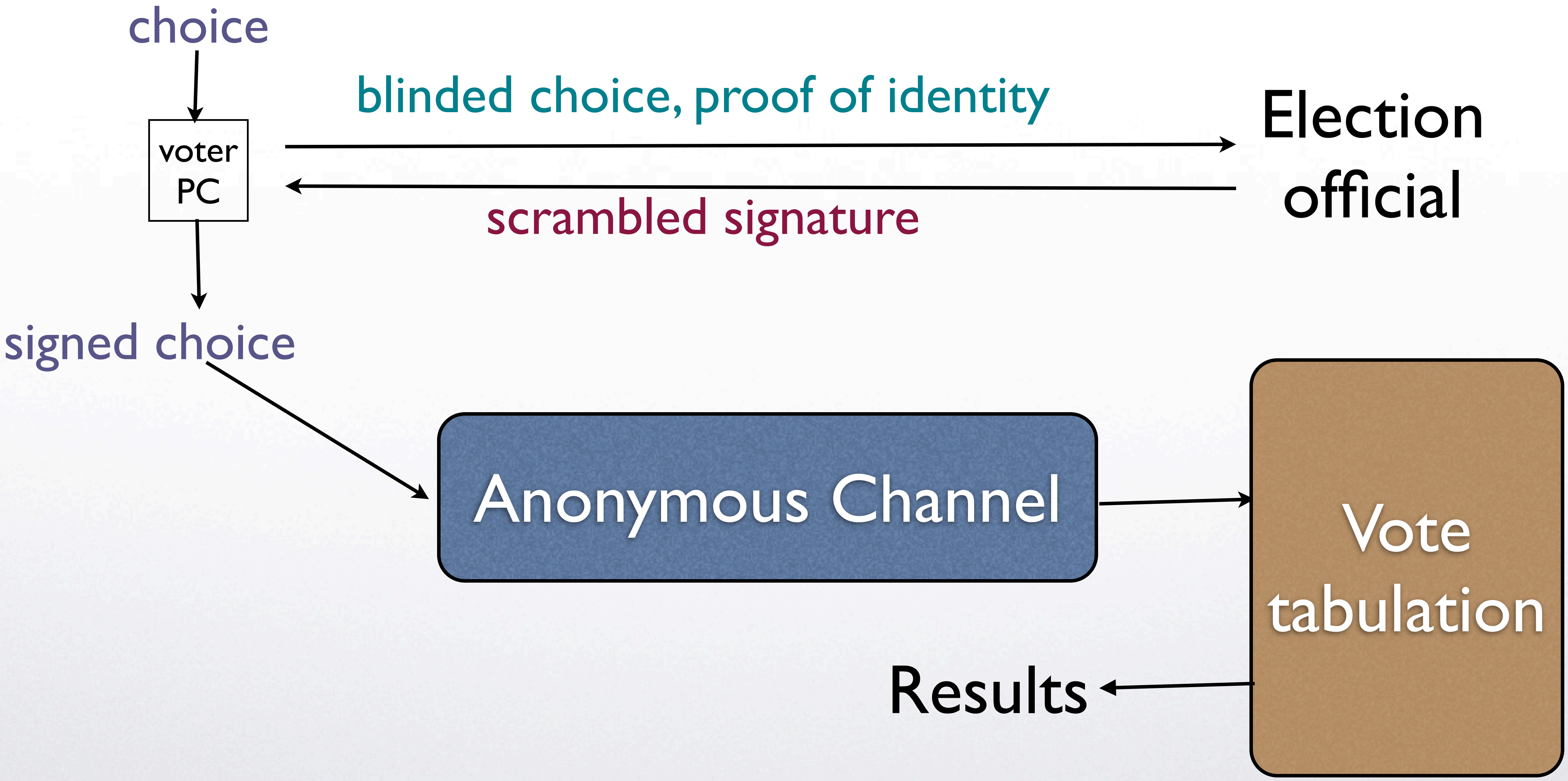
- Approach is fairly general.
  - application to other anonymous access systems is possible.
  - other web-sites than wikipedia need similar abuse protection; e.g. slashdot.
- More services: e.g., SMTP traffic is blocked. Using HiddenIBS it can be opened.

Blind Signatures



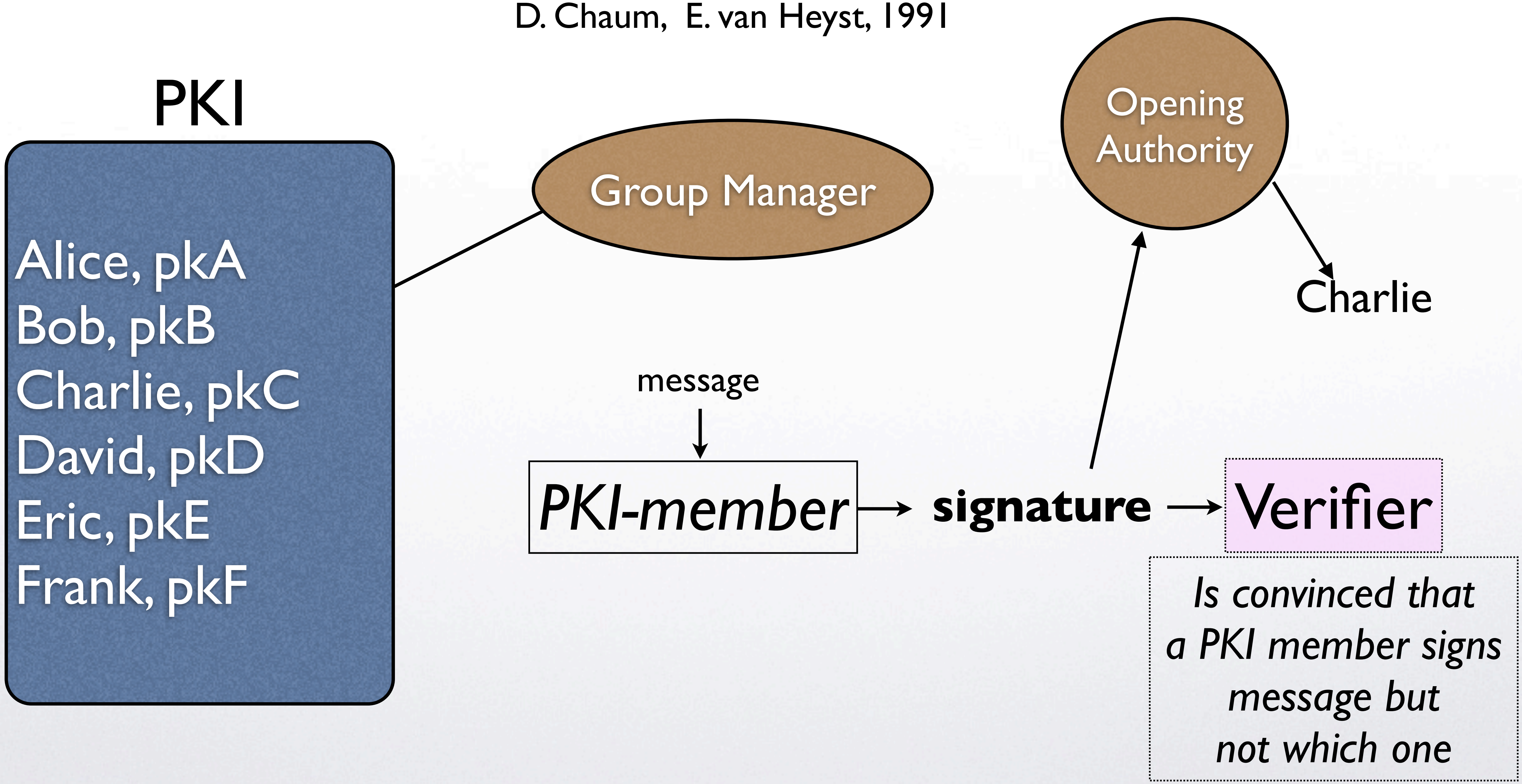
- we have seen already its application to e-cash and anonymous tokens.
- Another anonymity/privacy application : e-voting

E-Voting using Blind Signatures



Group Signatures

D. Chaum, E. van Heyst, 1991



PKI

Alice, pkA
Bob, pkB
Charlie, pkC
David, pkD
Eric, pkE
Frank, pkF

Group Manager

Opening Authority

Charlie

message

PKI-member → **signature** → Verifier

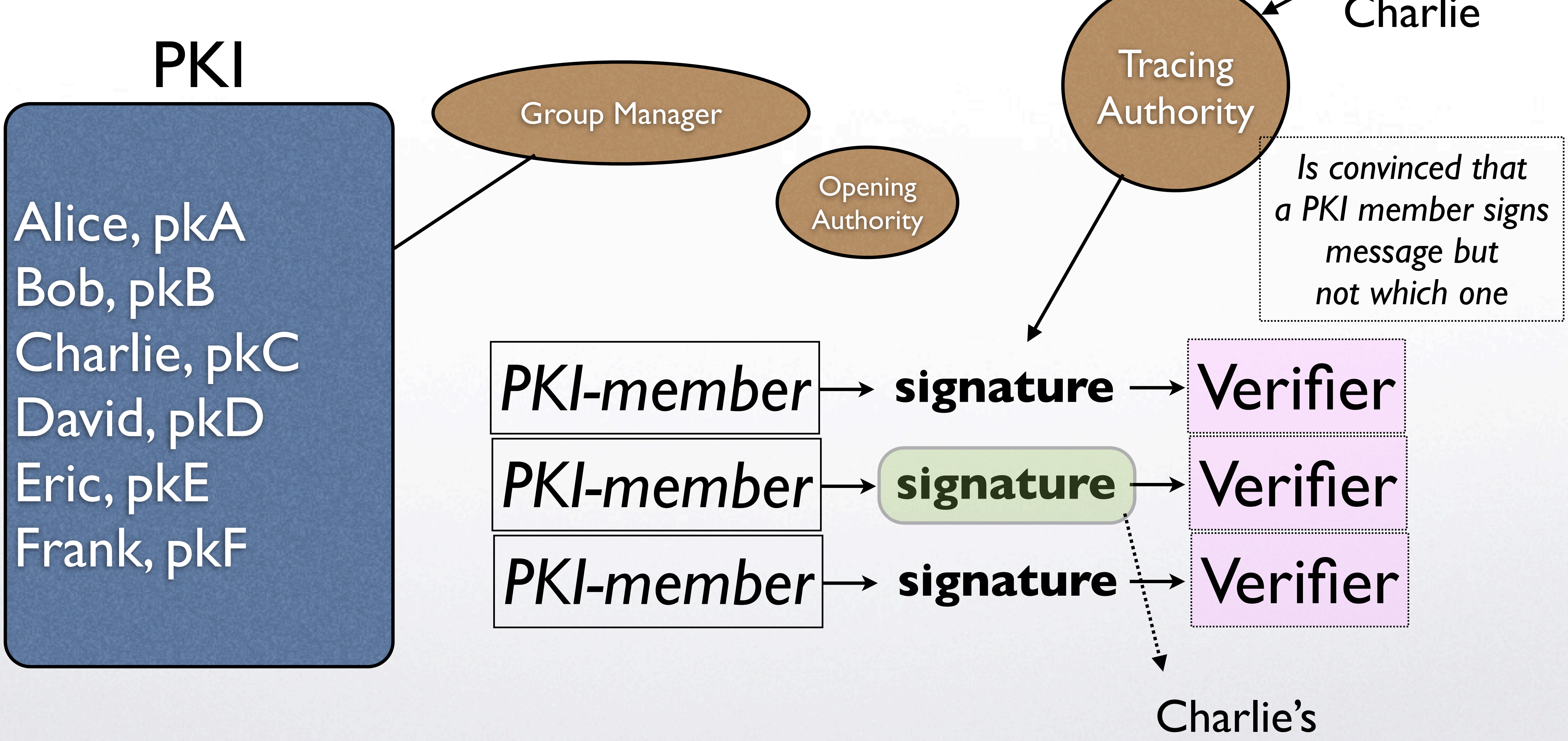
Is convinced that a PKI member signs message but not which one

Applications

- Can be used to hide the origin of a transaction.
- Prove that you belong in a group without showing who you are.
- They allow Opening Authority to reveal the identity in case of dispute.

Traceable Signatures

A. Kiayias, Y. Tsiounis M. Yung, 2004



PKI

Alice, pkA
Bob, pkB
Charlie, pkC
David, pkD
Eric, pkE
Frank, pkF

Group Manager

Opening Authority

Tracing Authority

Charlie

Is convinced that a PKI member signs message but not which one

PKI-member → **signature** → Verifier

PKI-member → **signature** → Verifier

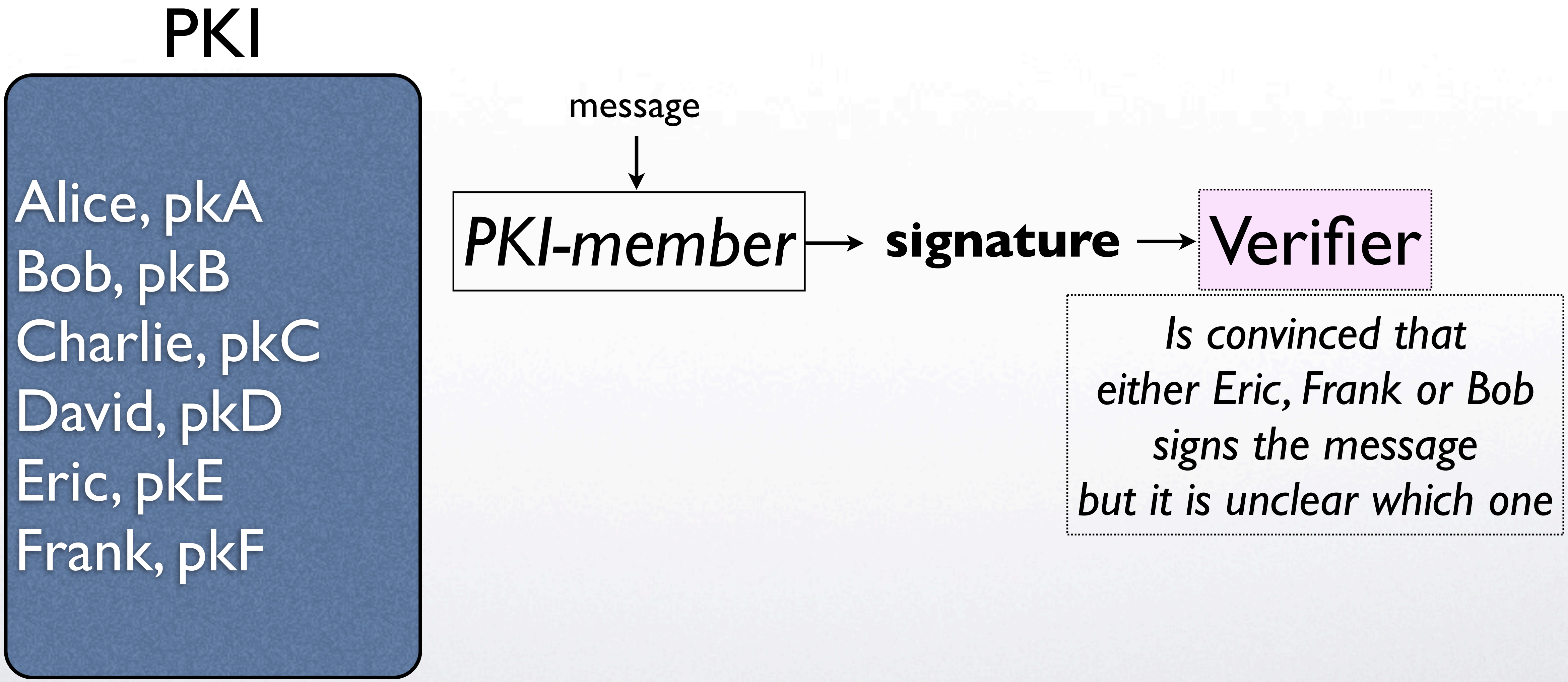
PKI-member → **signature** → Verifier

Charlie's

Applications

- As in group signatures but now it is possible to:
  - The tracing authority to find all signatures of a “wanted user”
  - A user to claim his signatures.

Ring Signatures



PKI

Alice, pkA
Bob, pkB
Charlie, pkC
David, pkD
Eric, pkE
Frank, pkF

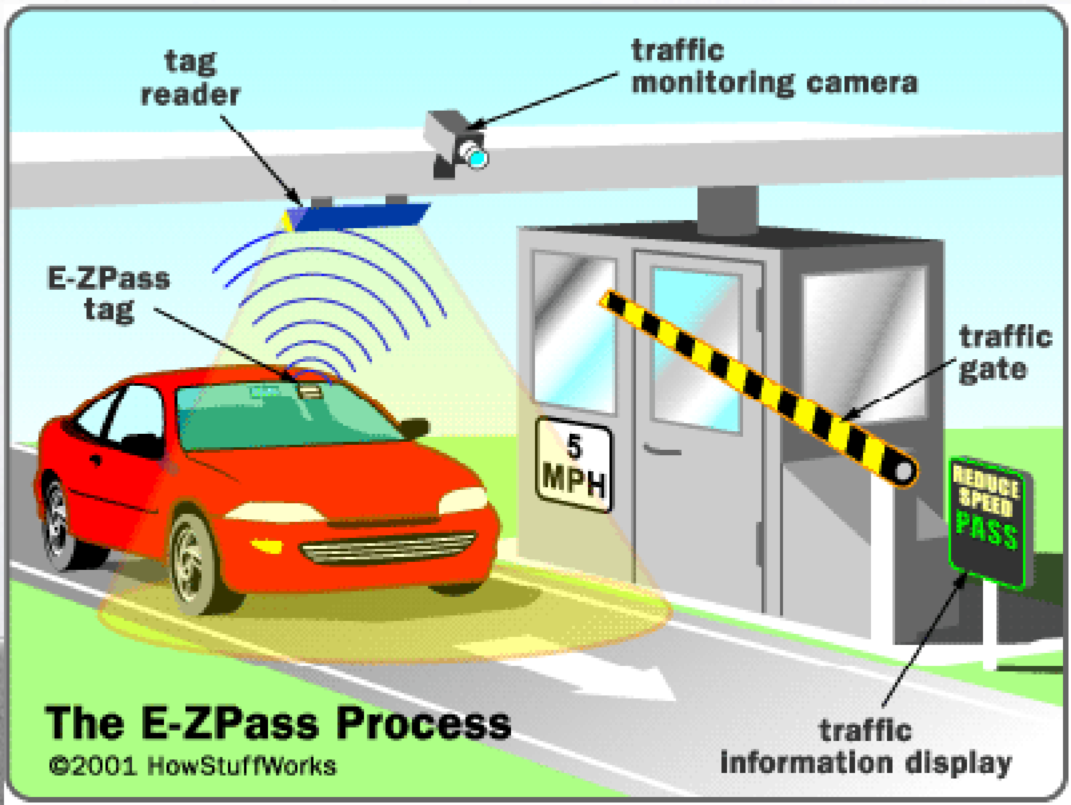
message

PKI-member → **signature** → Verifier

Is convinced that either Eric, Frank or Bob signs the message but it is unclear which one

Electronic Tolls

- As car approaches toll booth RF signal activates car transponder.
- Car transponder engages in identification.
- Toll access point (interacting with central database) grants access or denies it.



The E-ZPass Process

©2001 HowStuffWorks