rBridge: User Reputation Based Tor Bridge Distribution with Privacy Preservation

Qiyan Wang
Nikita Borisov

University of Illinois at Urbana-Champaign

Zi Lin
Nicholas J Hopper

University of Minnesota

The Internet helps political and social movements

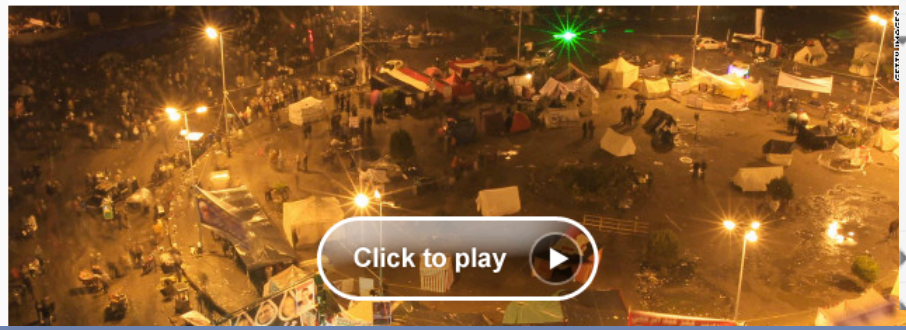
SET EDITION: U.S. | INTERNATIONAL | MÉXICO | ARABIC
TV: CNN | CNNi | CNN en Español | HLN

CNN

Home | TV & Video | NewsPulse | U.S. | World | Politics | Justice | Entertainment | Tech | Health

5 voices on Egypt's 'unfinished revolution'

updated 2:48 PM EST, Wed January 25, 2012



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Our updated Terms of Use will become effective on May 25, 2012. Find out more.

Falun Gong

From Wikipedia, the free encyclopedia
(Redirected from Falungong)

Falun Gong or **Falun Dafa** (literally means "*Law Wheel Practice*") is a spiritual discipline first introduced in China in 1992 through public lectures by its founder, Li Hongzhi.[1] It combines the practice of meditation and slow-

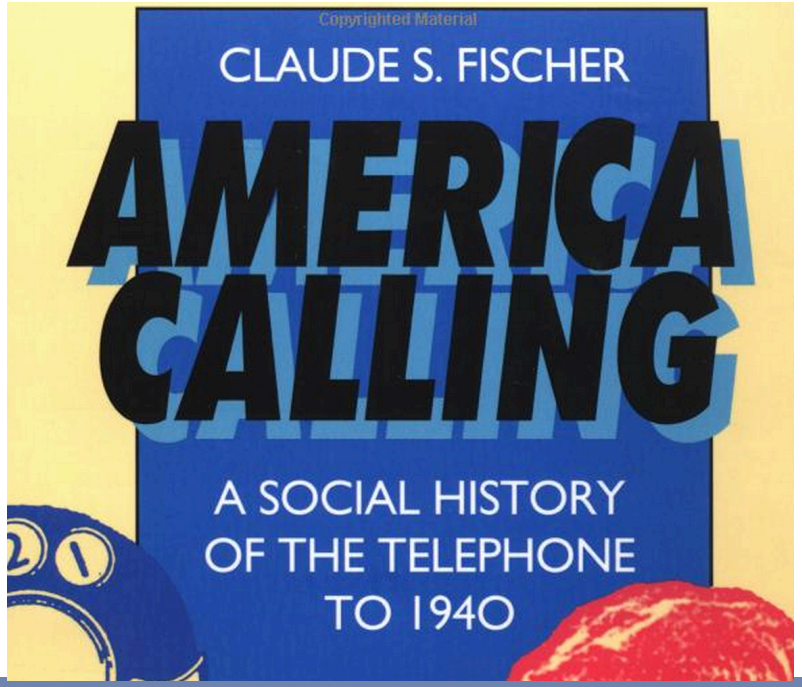
Falun Gong

The Falun Dafa emblem

of entering an upcoming bicycle race but do not really know how to start or how to get yourself

Utopian Dreams

"[It] is a force for democracy, because it permits citizens to communicate, to collaborate, and even to conspire uncontrolled by a central authority."



it with the desire to supply, in some degree, a

Internet censorship

- 7 out of top 10 non-Chinese sites[1] are blocked by the "Great Firewall of China".
- The Chinese government employs an Internet policy force of over 30,000 people[2] .

Top 10 non-Chinese sites	Blocked by GFW?
Google	**Partially**
Facebook	**Yes**
YouTube	**Yes**
Yahoo!	**Partially**
Wikipedia	**Yes**
Windows Live	No
Twitter	**Yes**
Amazon	No
Blogspot	**Yes**
LinkedIn	No

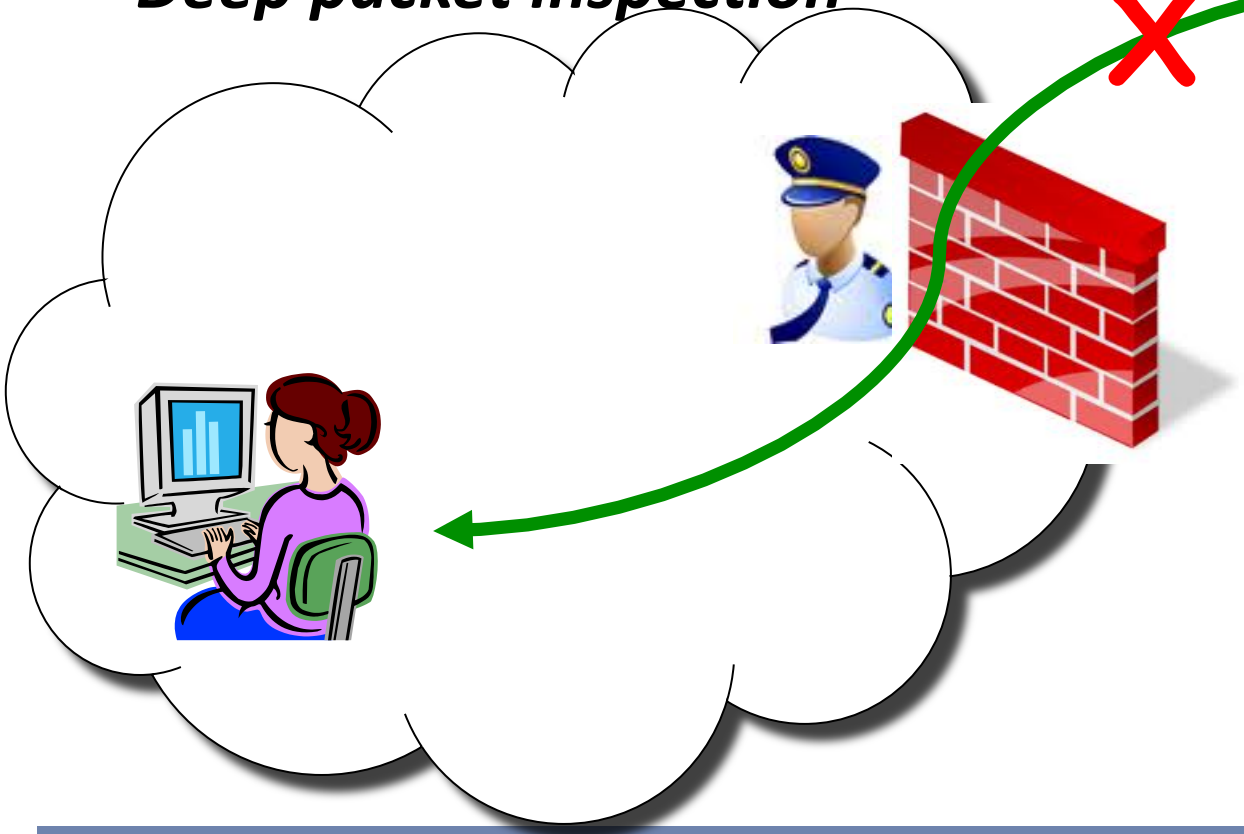
[1] Test report (Apr.3.2012-May.3.2012) from https://en.greatfire.org
[2] http://www.ibtimes.com/articles/113590/20110217/

Censorship techniques

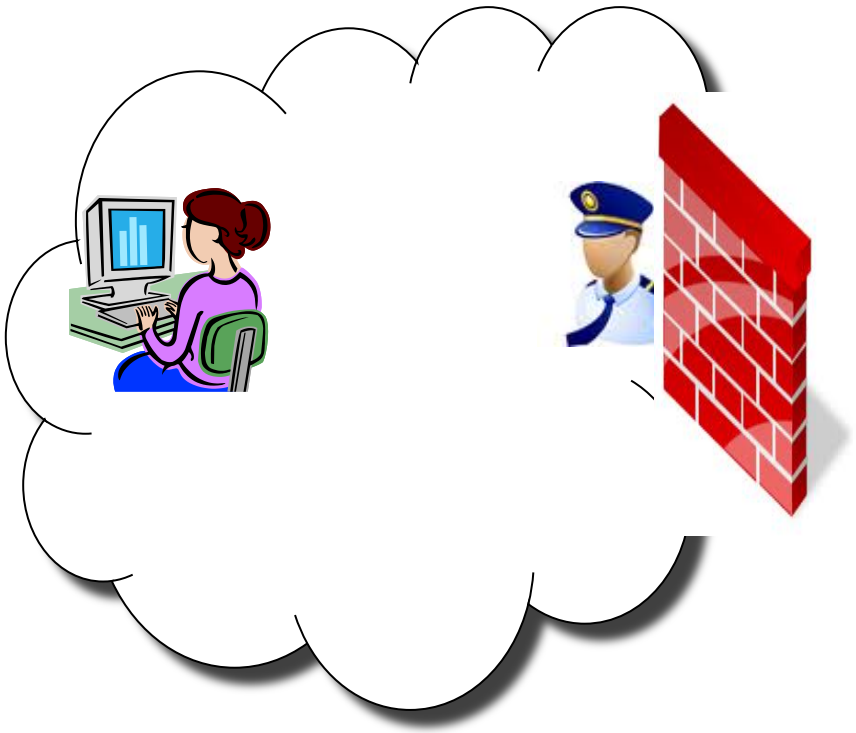
IP blocking

DNS hijiacking

Deep packet inspection

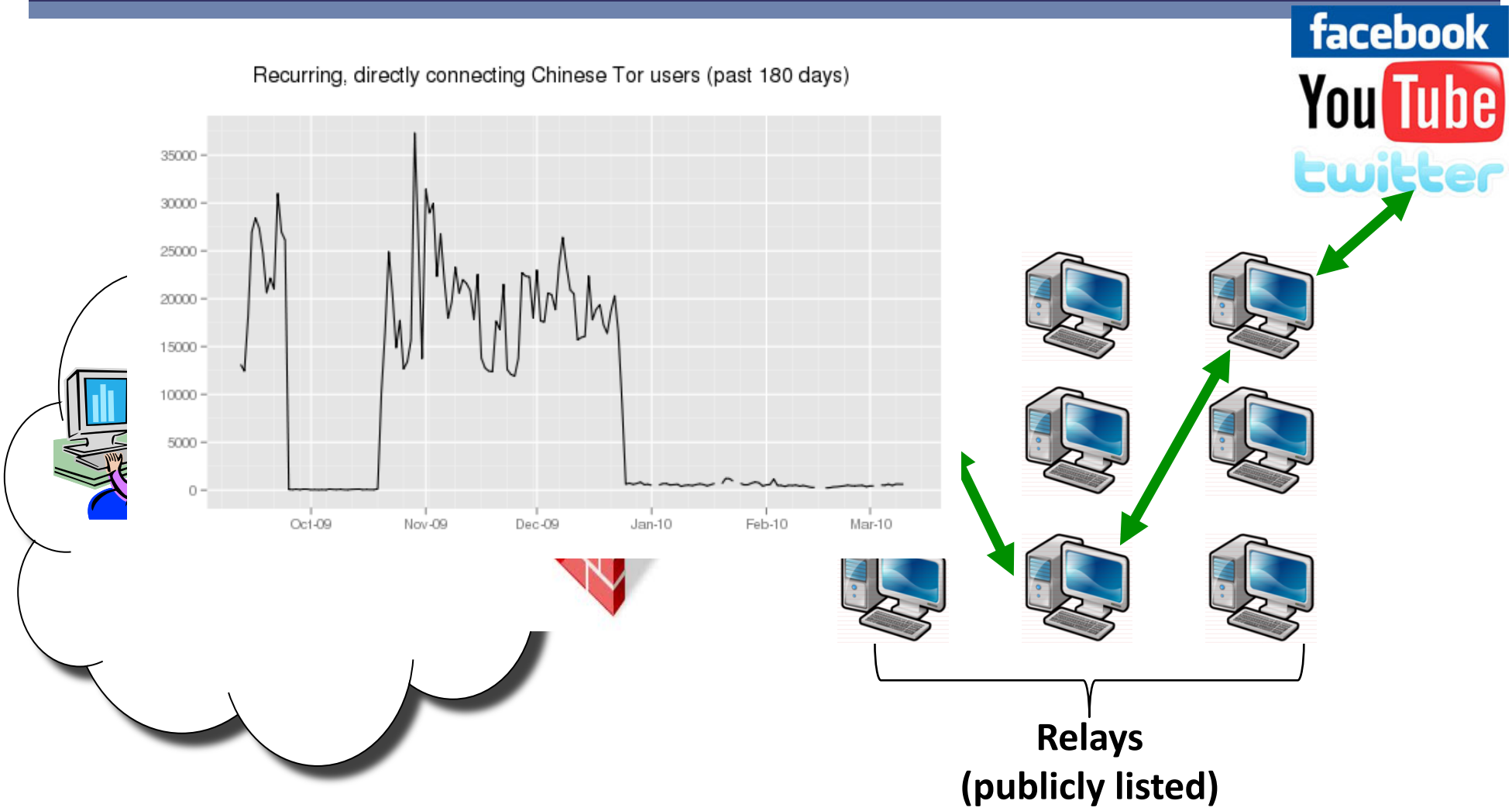


Censorship circumvention using Tor

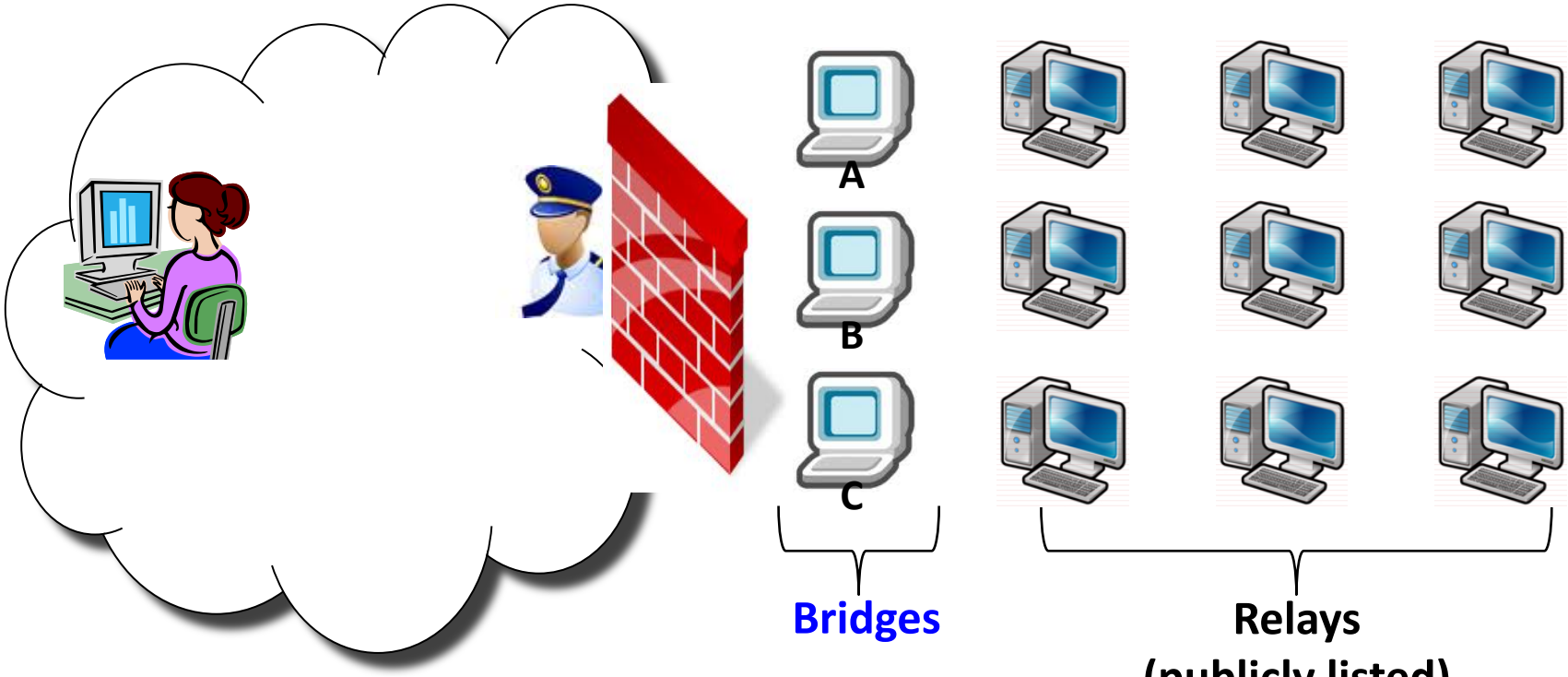


Relays
(publicly listed)

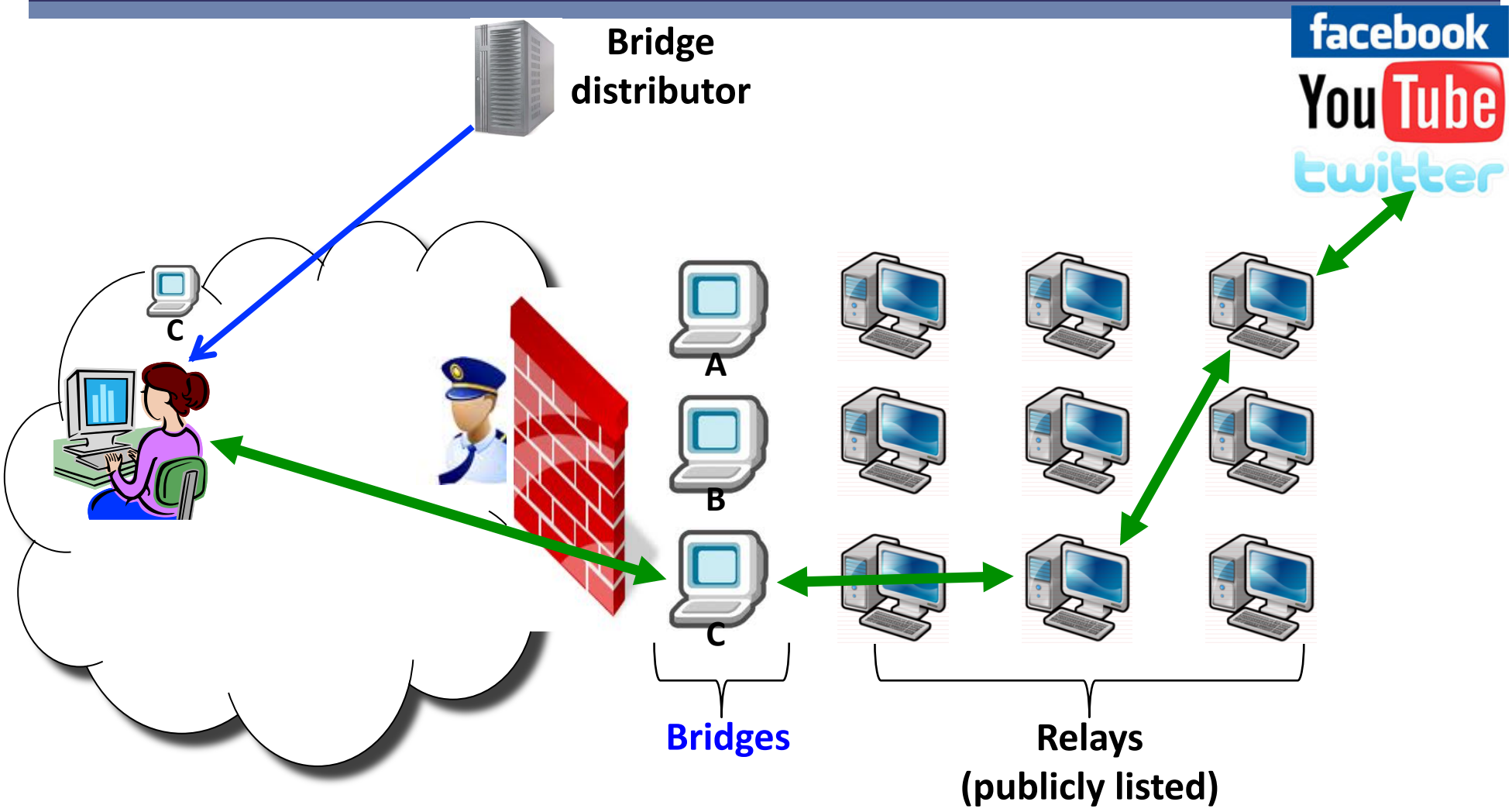
Censorship circumvention using Tor



Censorship circumvention using Tor bridges

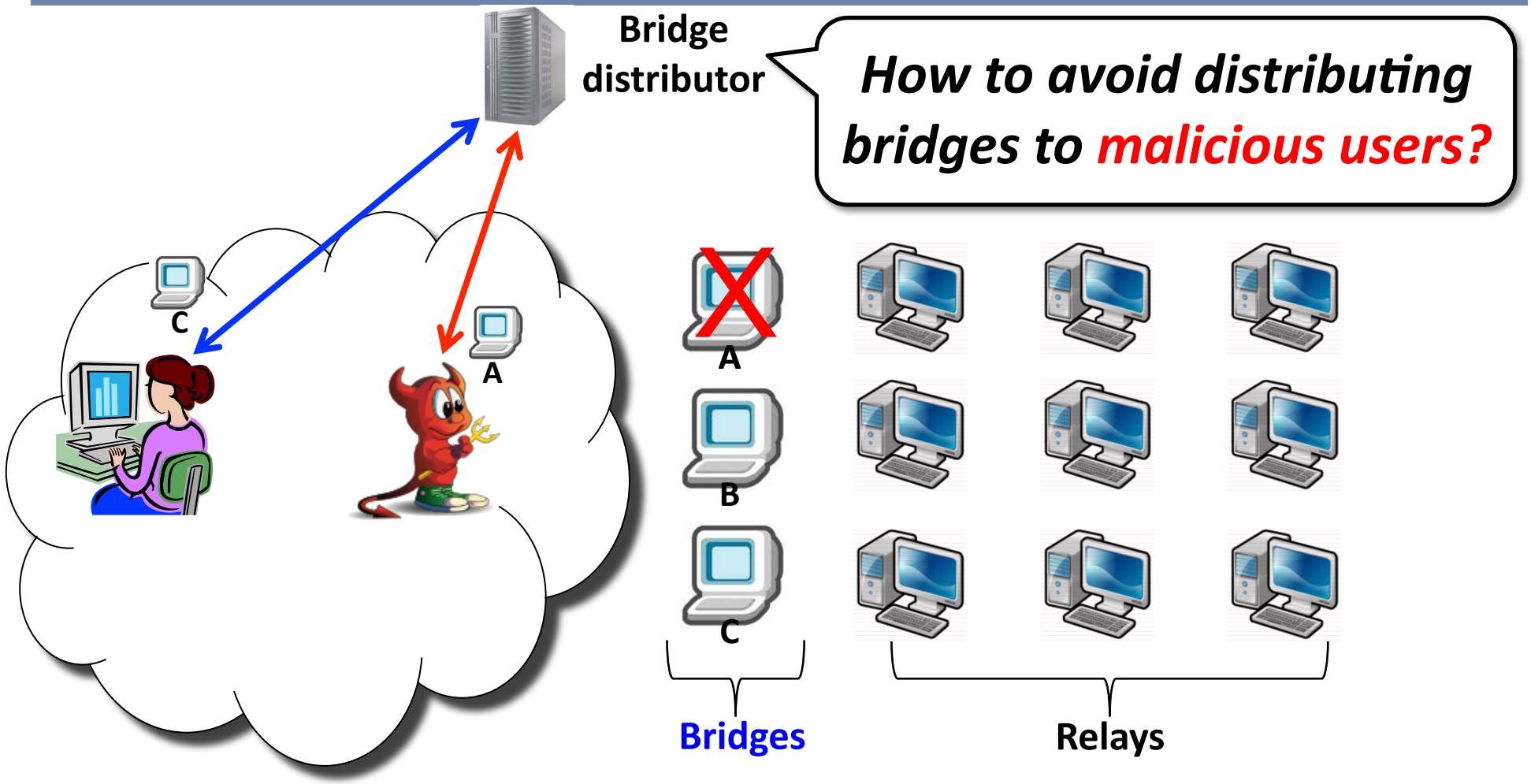


Censorship circumvention using Tor bridges



Tor via bridges

Censorship circumvention using Tor bridges



Rate limiting

One bridge per IP address / Gmail address

Bridge distributor

A

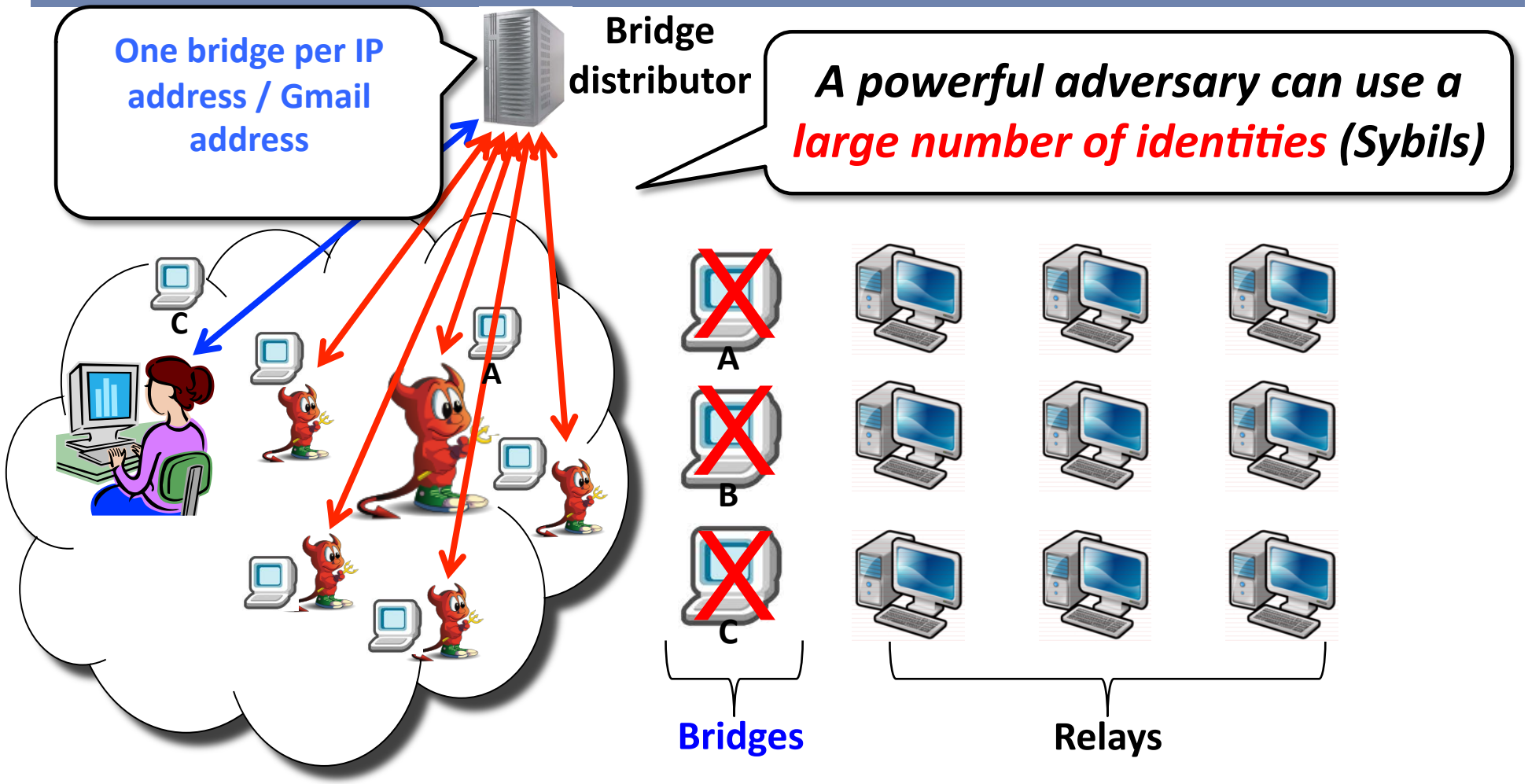
B

C

Bridges

Relays

Rate limiting

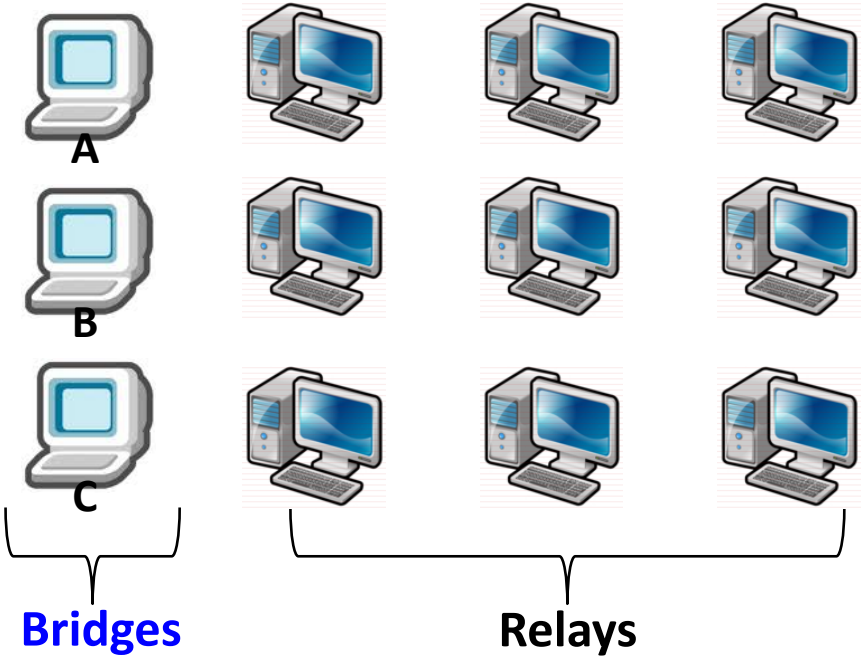


The Chinese government were able to enumerate all bridges in under a month in 2010.

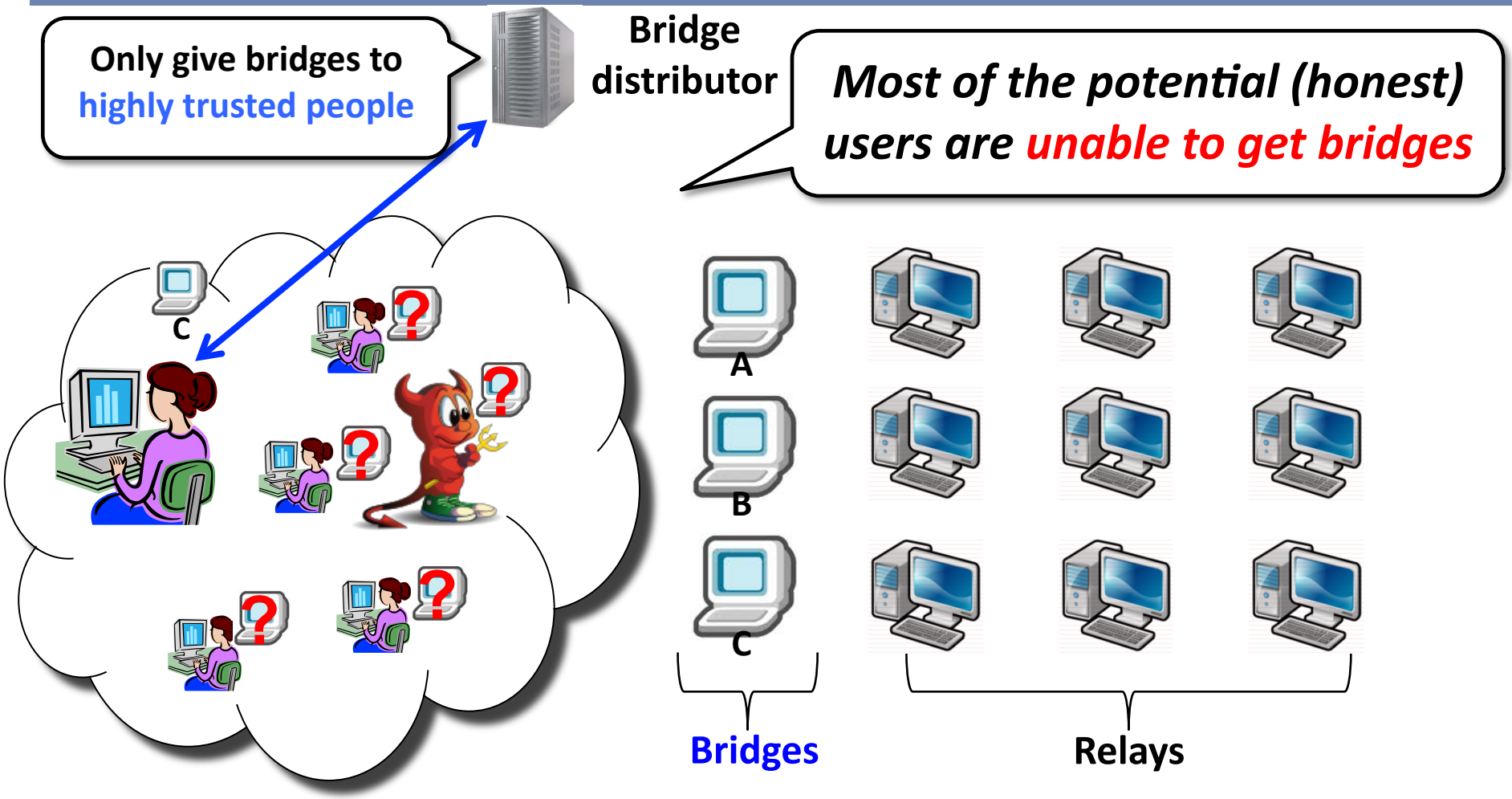
Limited access

Only give bridges to highly trusted people

Bridge distributor



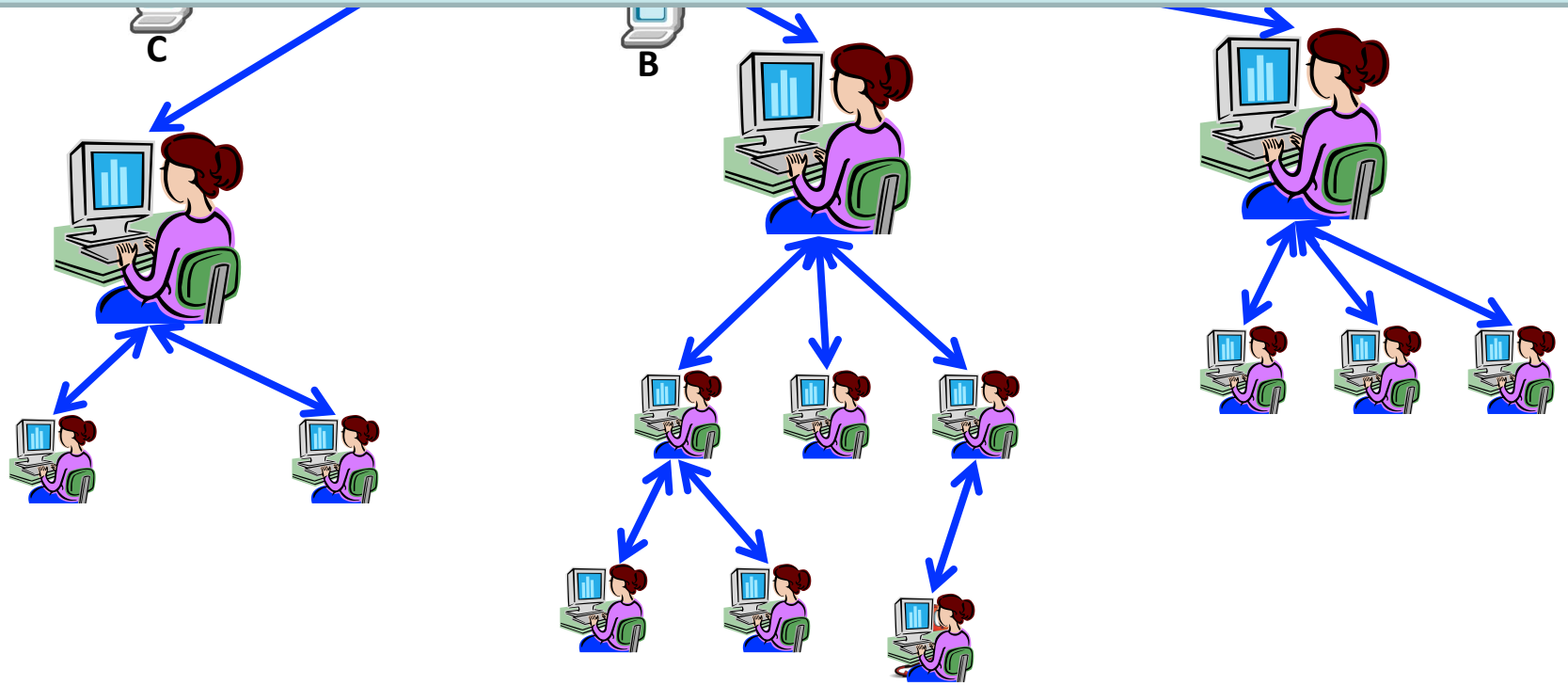
Limited Access



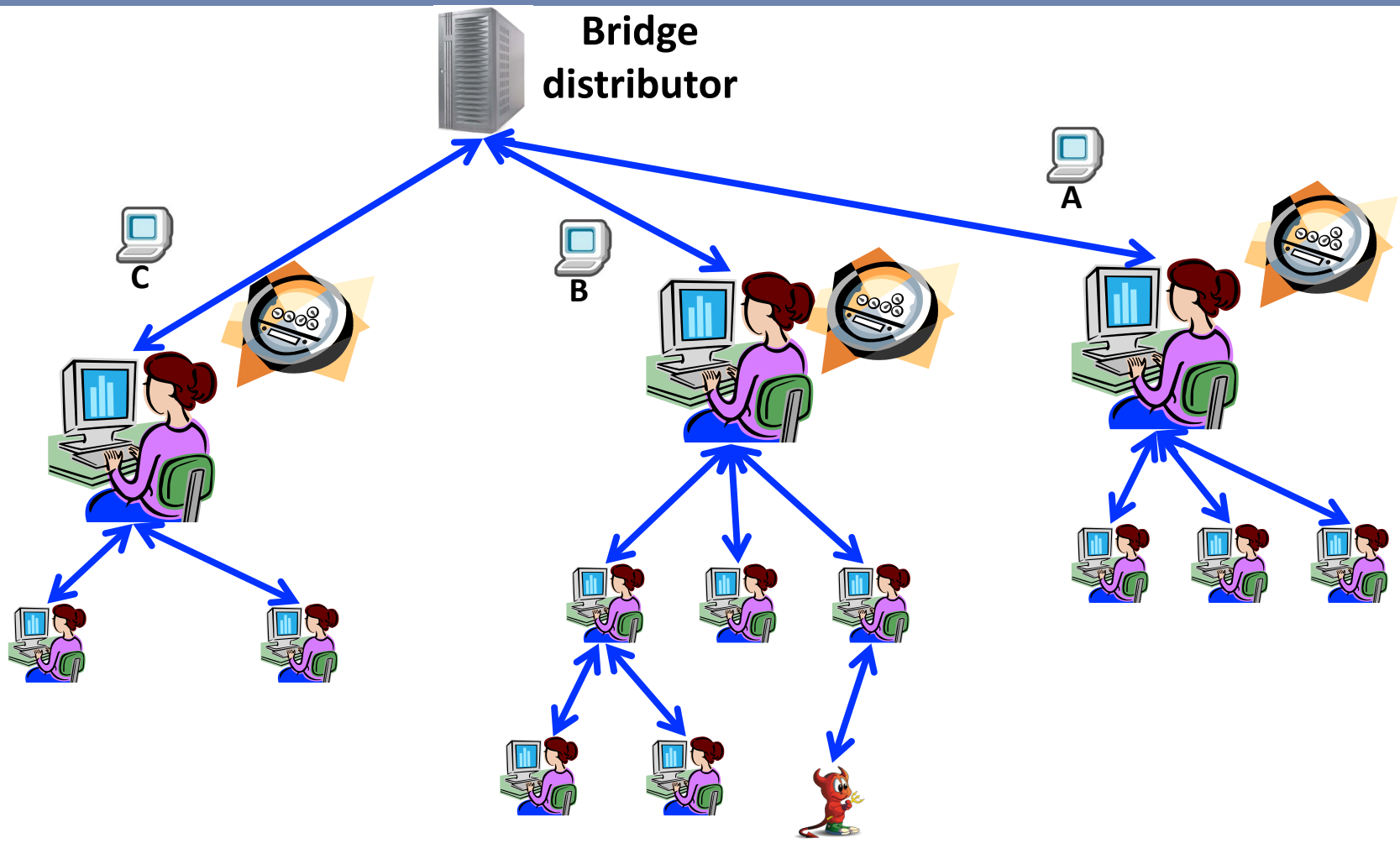
Social Distribution

Bridge distributor

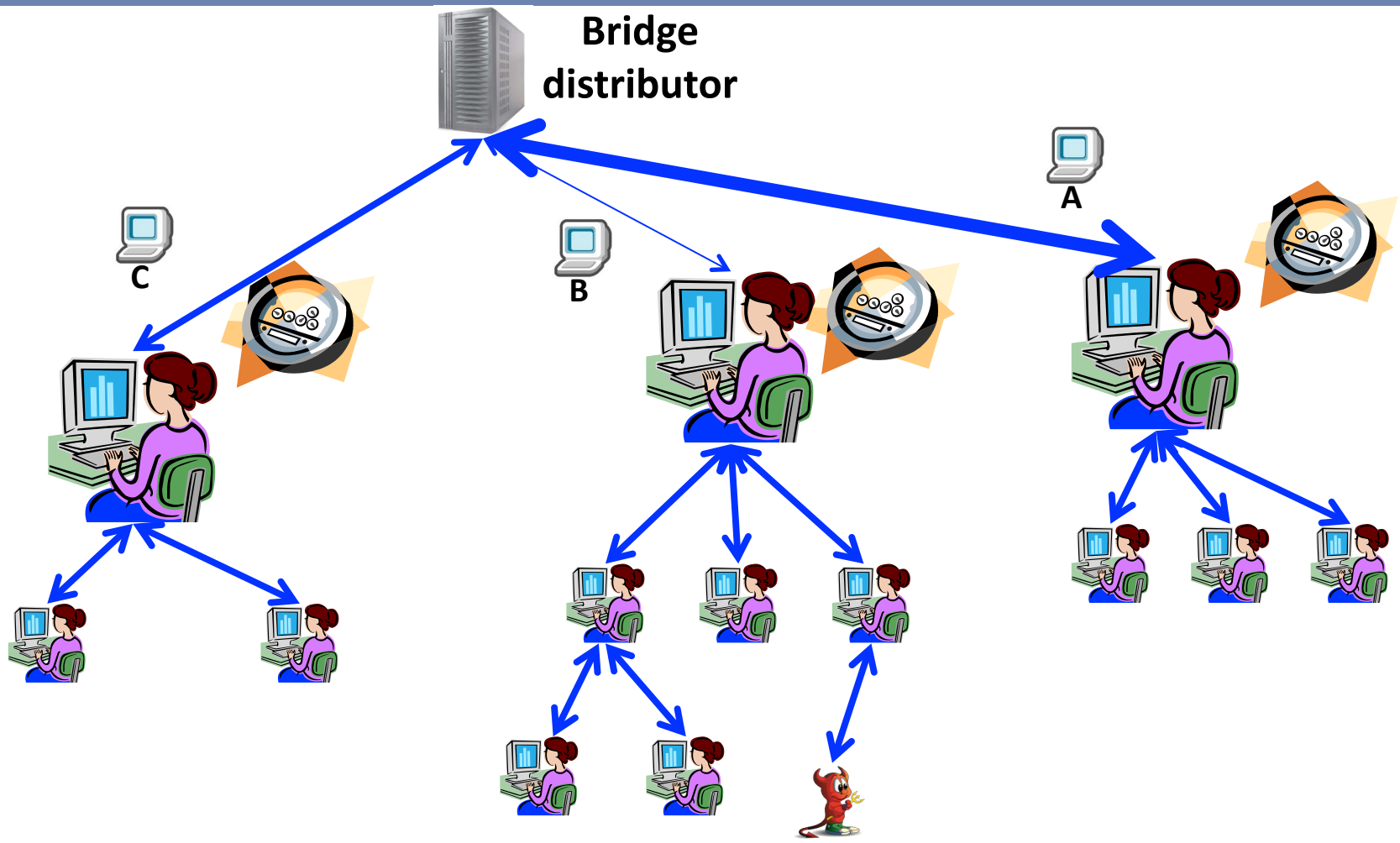
Conflict between robustness and openness!



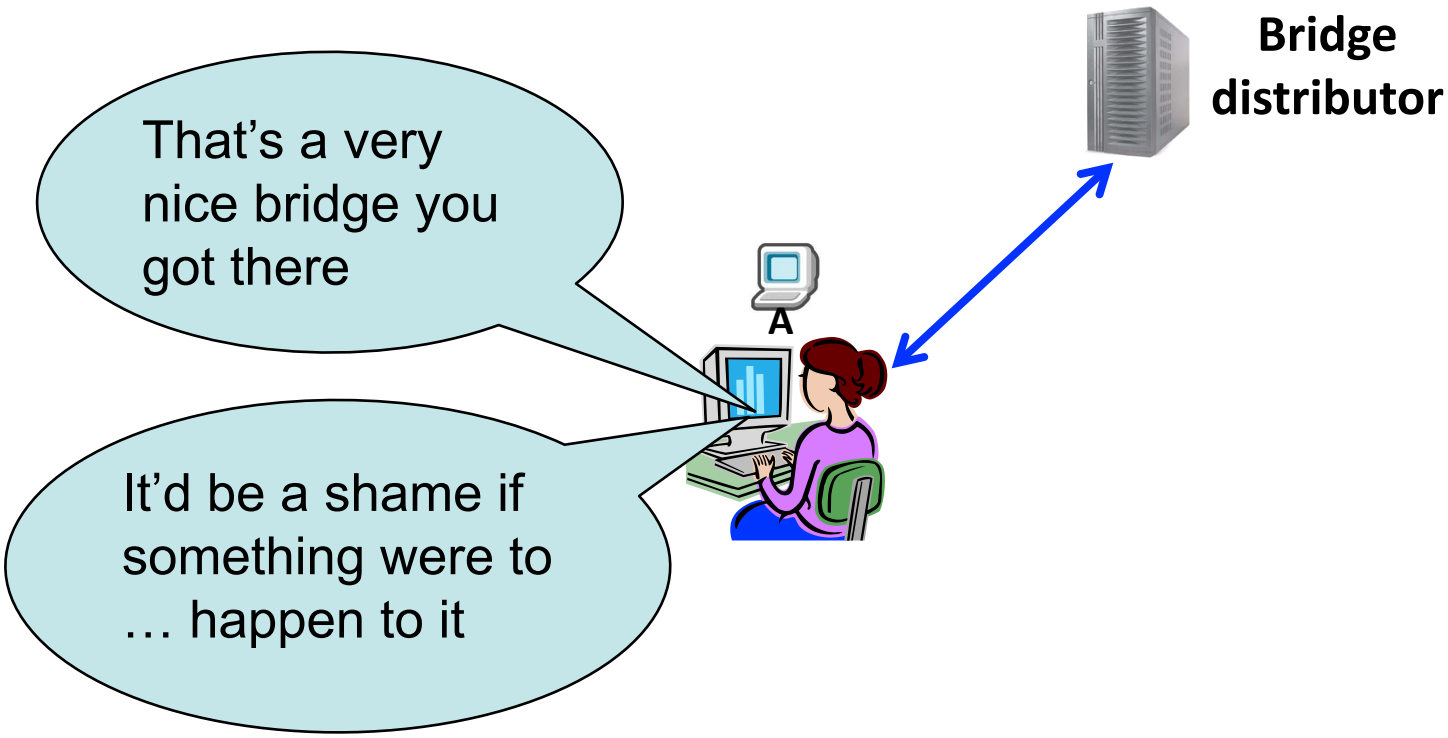
Proximax [McCoy et al., FC'11]



Proximax [McCoy et al., FC'11]



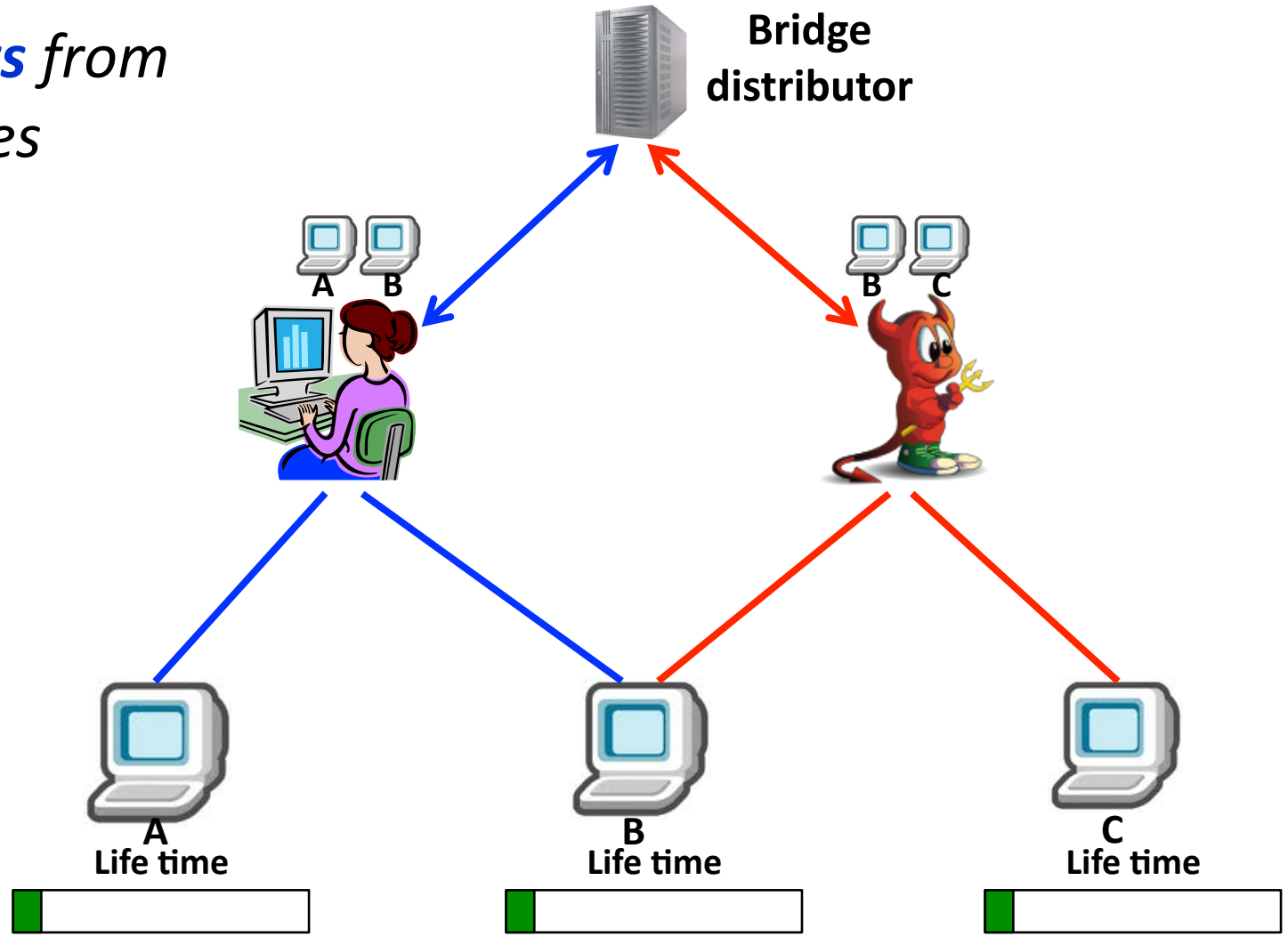
Our basic idea: Incentives



Pay users to keep bridges unblocked!

rBridge: user reputation

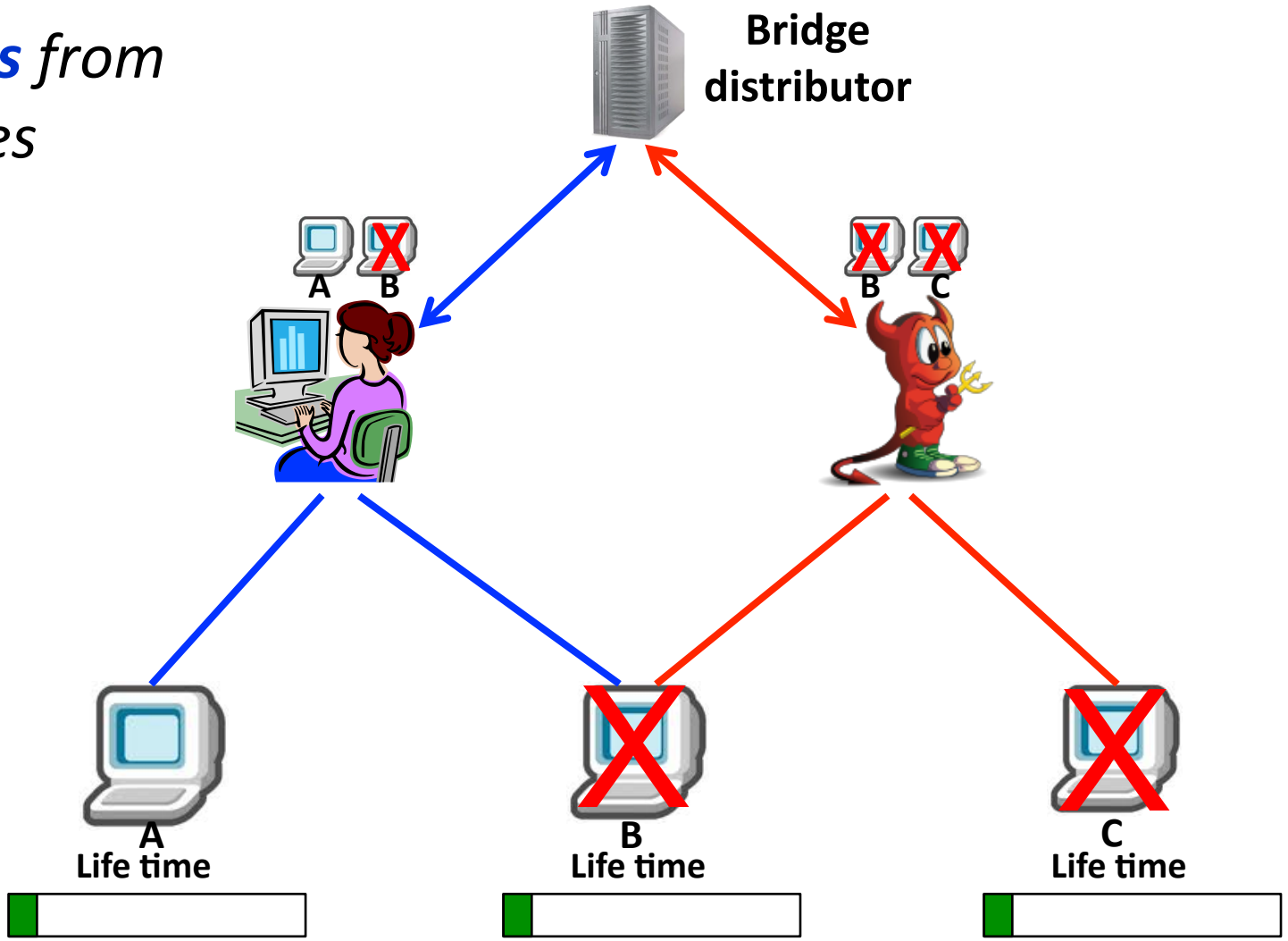
Earn credits *from alive bridges*



pyramid and a planet. Every step explained in detail including exactly

rBridge: user reputation

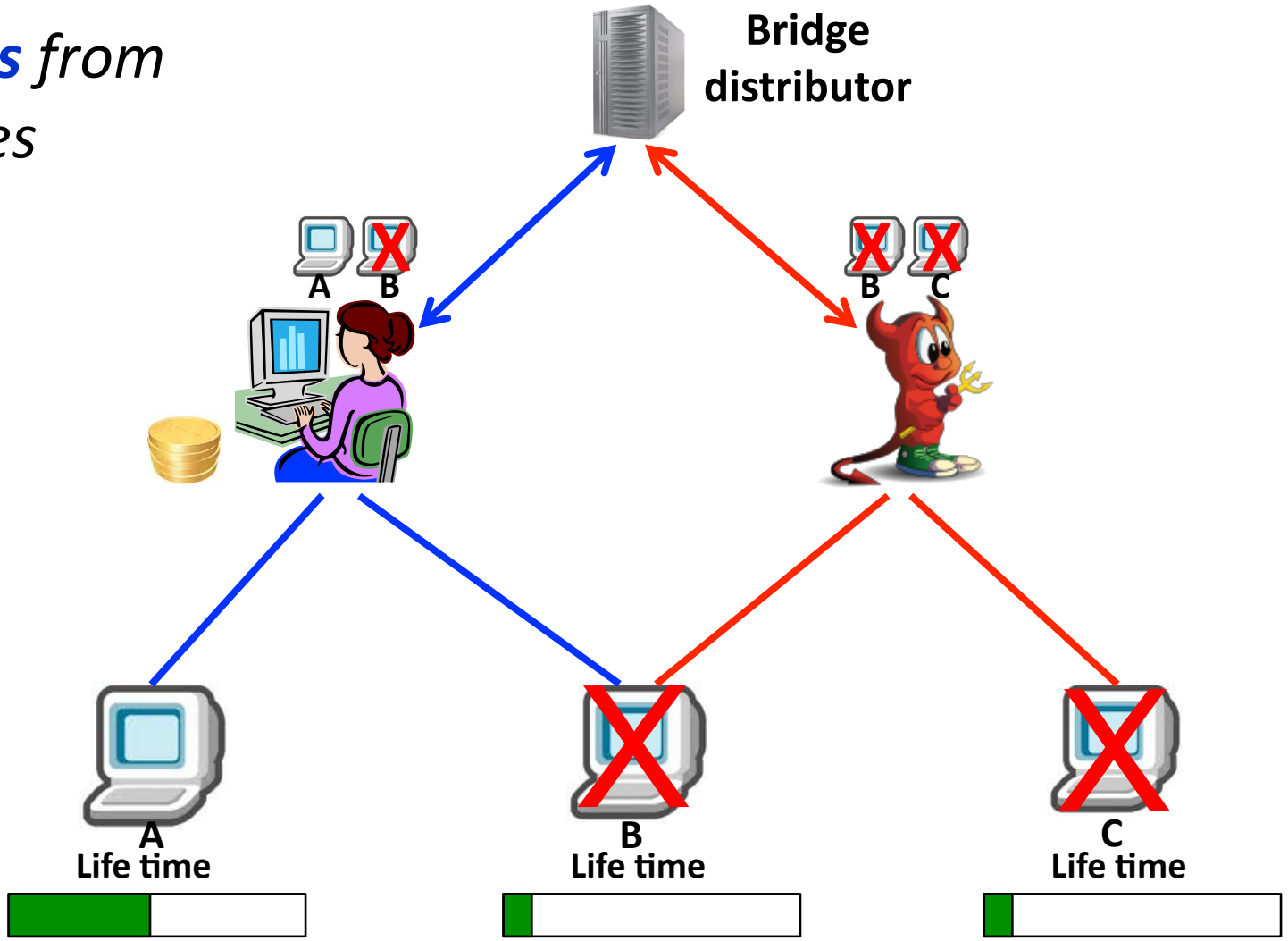
Earn credits *from alive bridges*



These are big promises! Why should

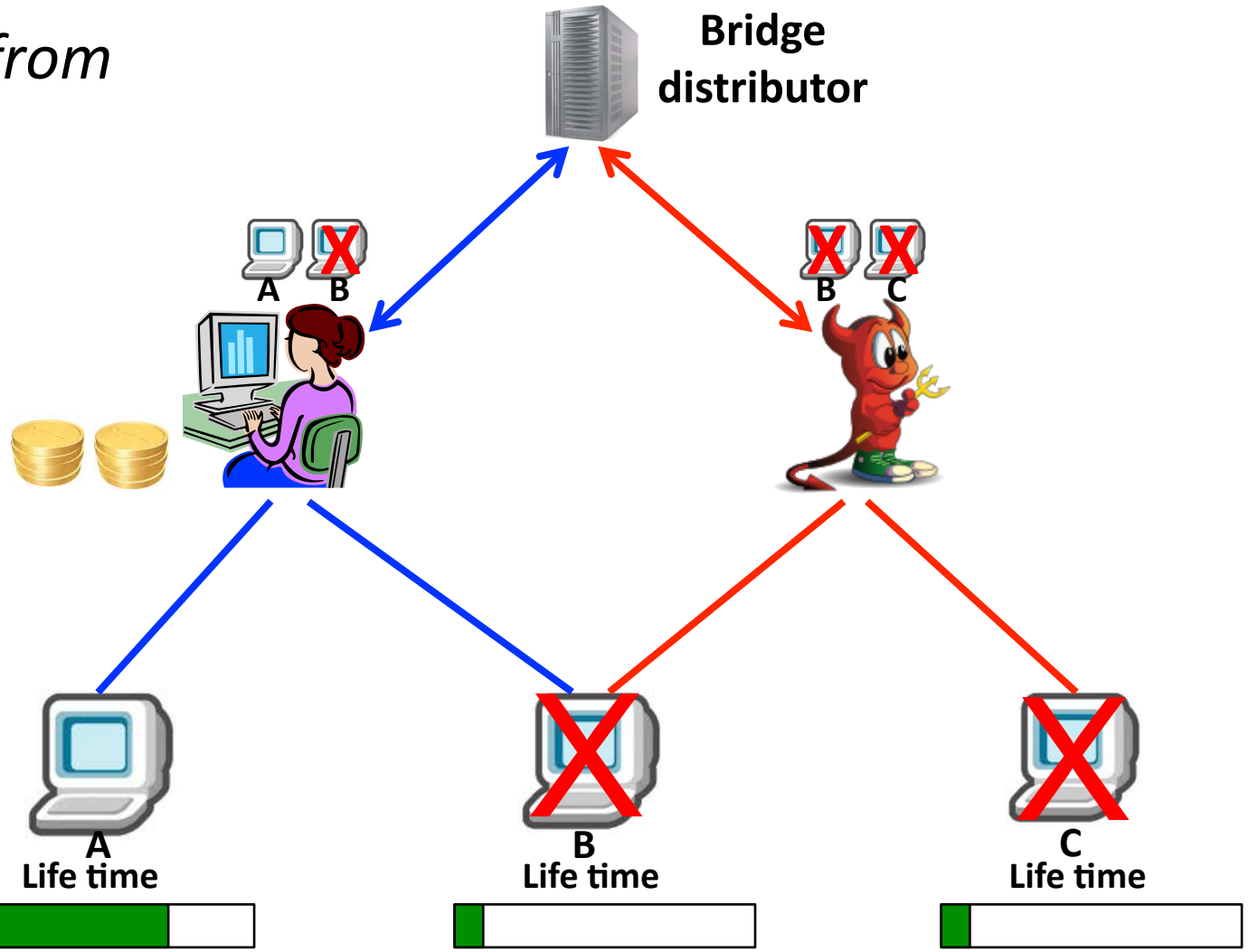
rBridge: user reputation

Earn credits *from alive bridges*



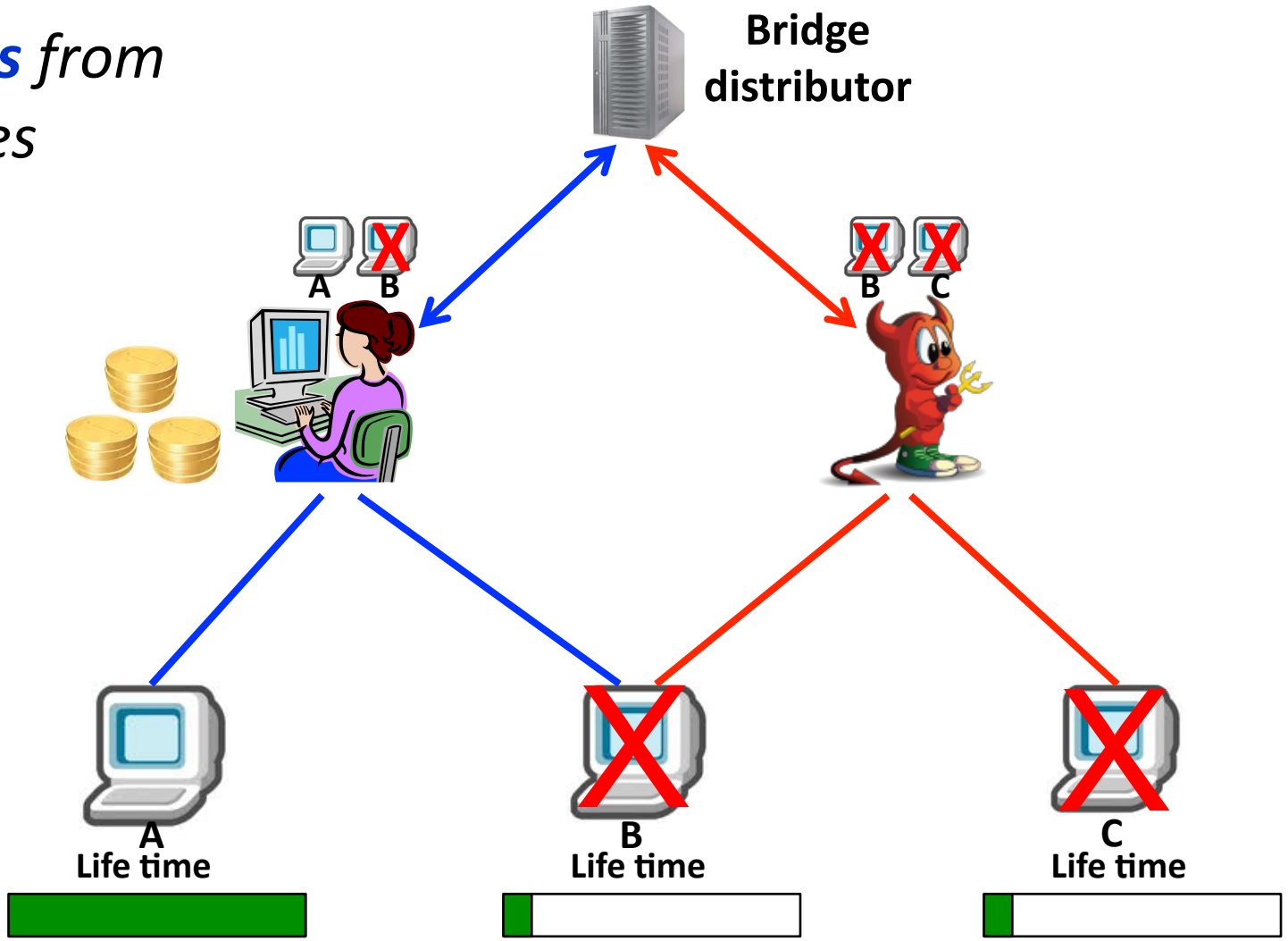
rBridge: user reputation

Earn credits *from alive bridges*



rBridge: user reputation

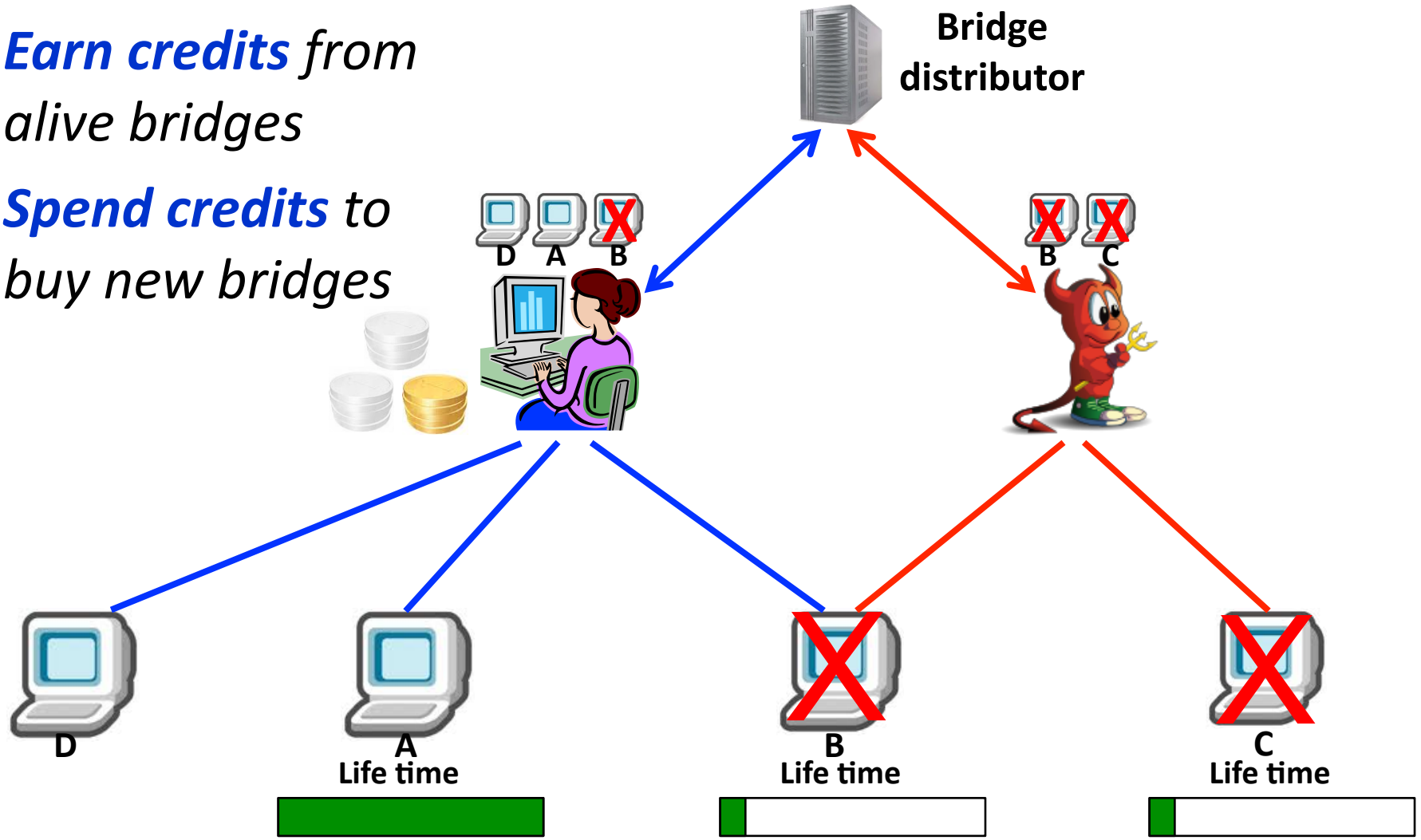
Earn credits *from alive bridges*



rBridge: user reputation

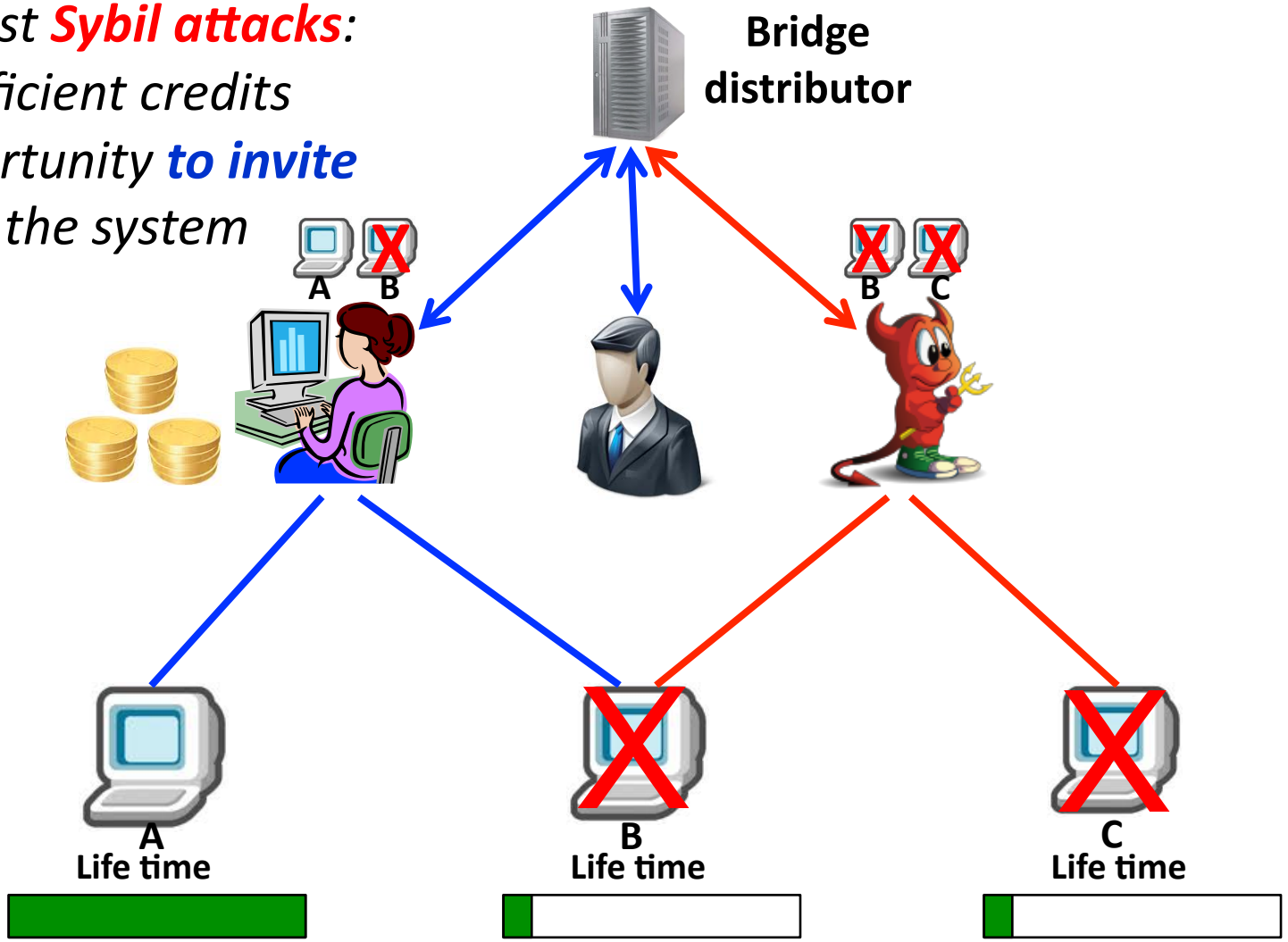
Earn credits *from alive bridges*

Spend credits *to buy new bridges*

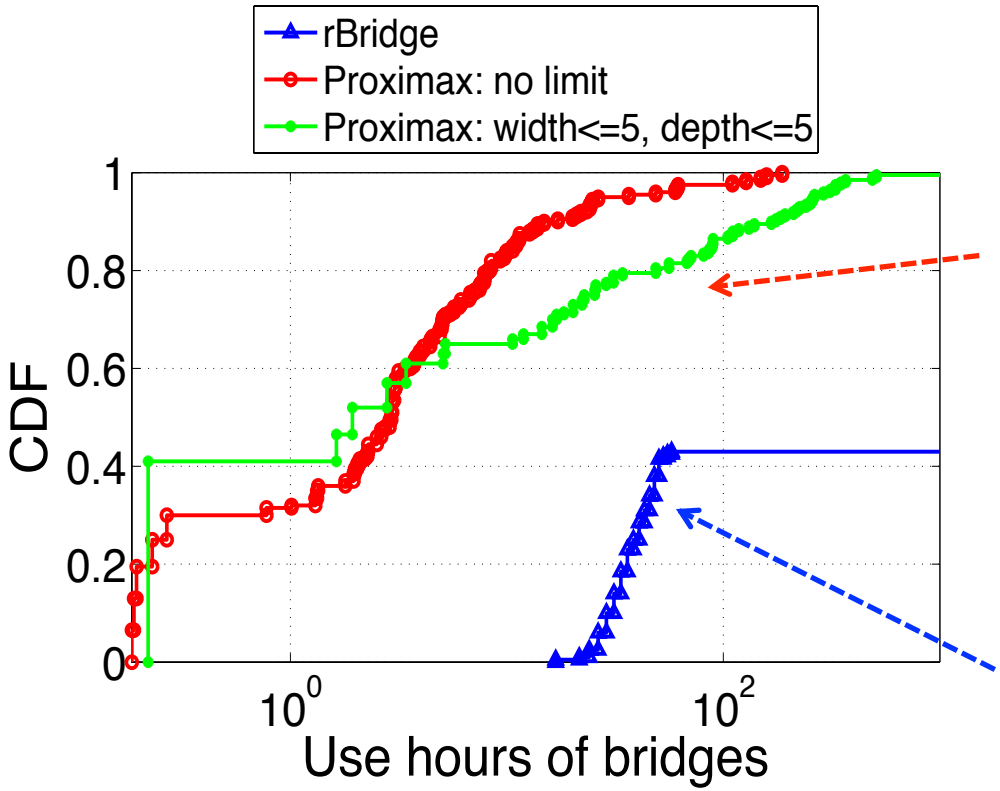


rBridge: user reputation

*Defense against **Sybil attacks**: users with sufficient credits have the opportunity **to invite friends** to join the system*



Comparison with Proximax (the state-of-the art scheme)



Proximax: less than **5% bridges** can serve more than **20 user-hours** before being blocked.

rBridge: over **80% bridges** can serve at least **60 user-hours** before being blocked, and about **60% bridges** are **never blocked**.

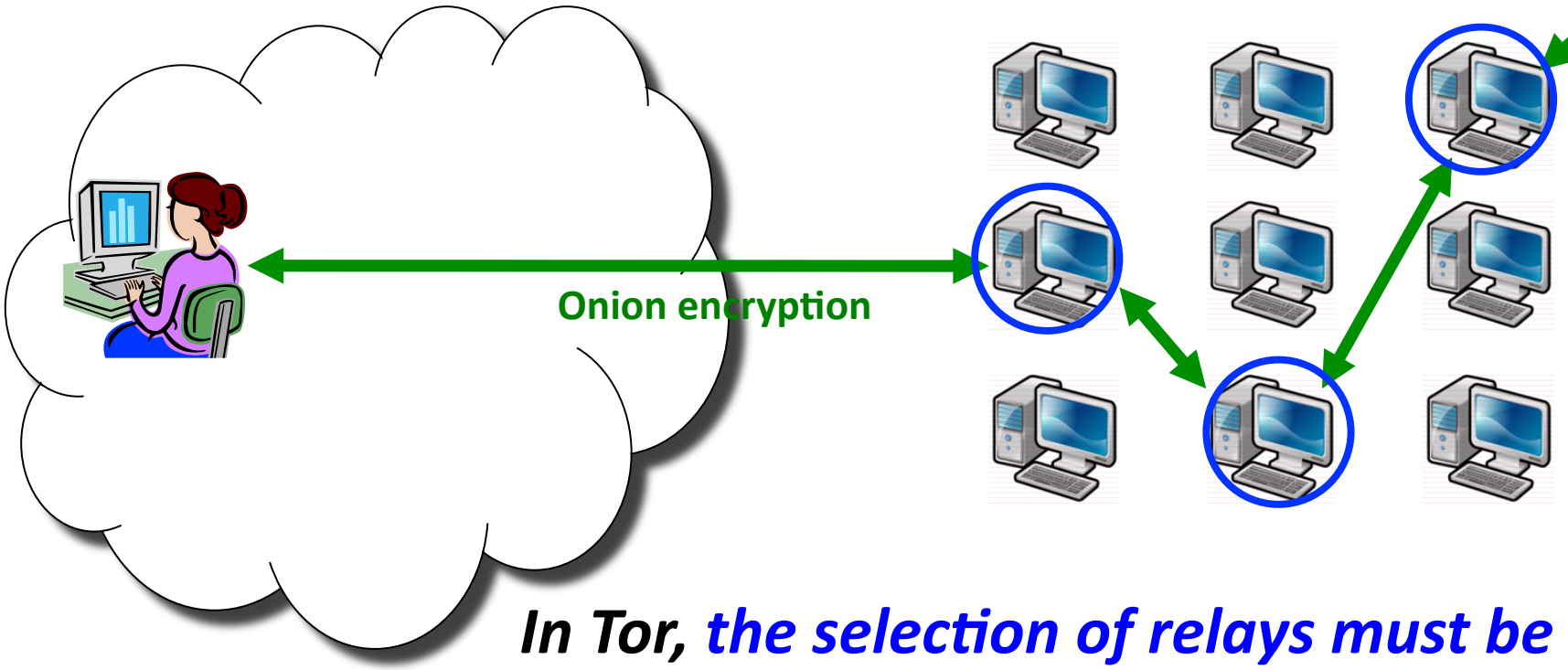
Privacy preservation

Directory authority

facebook

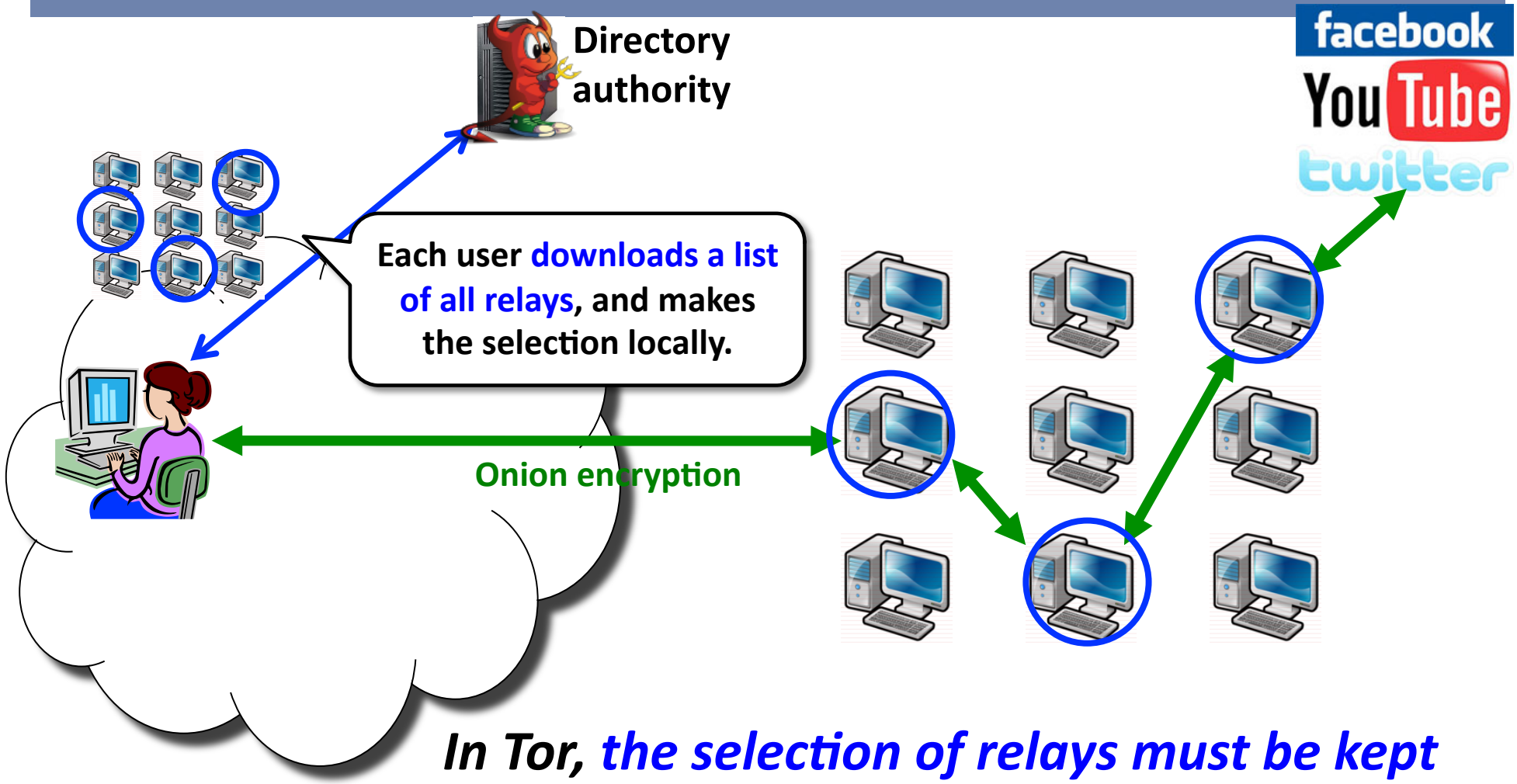
YouTube

twitter



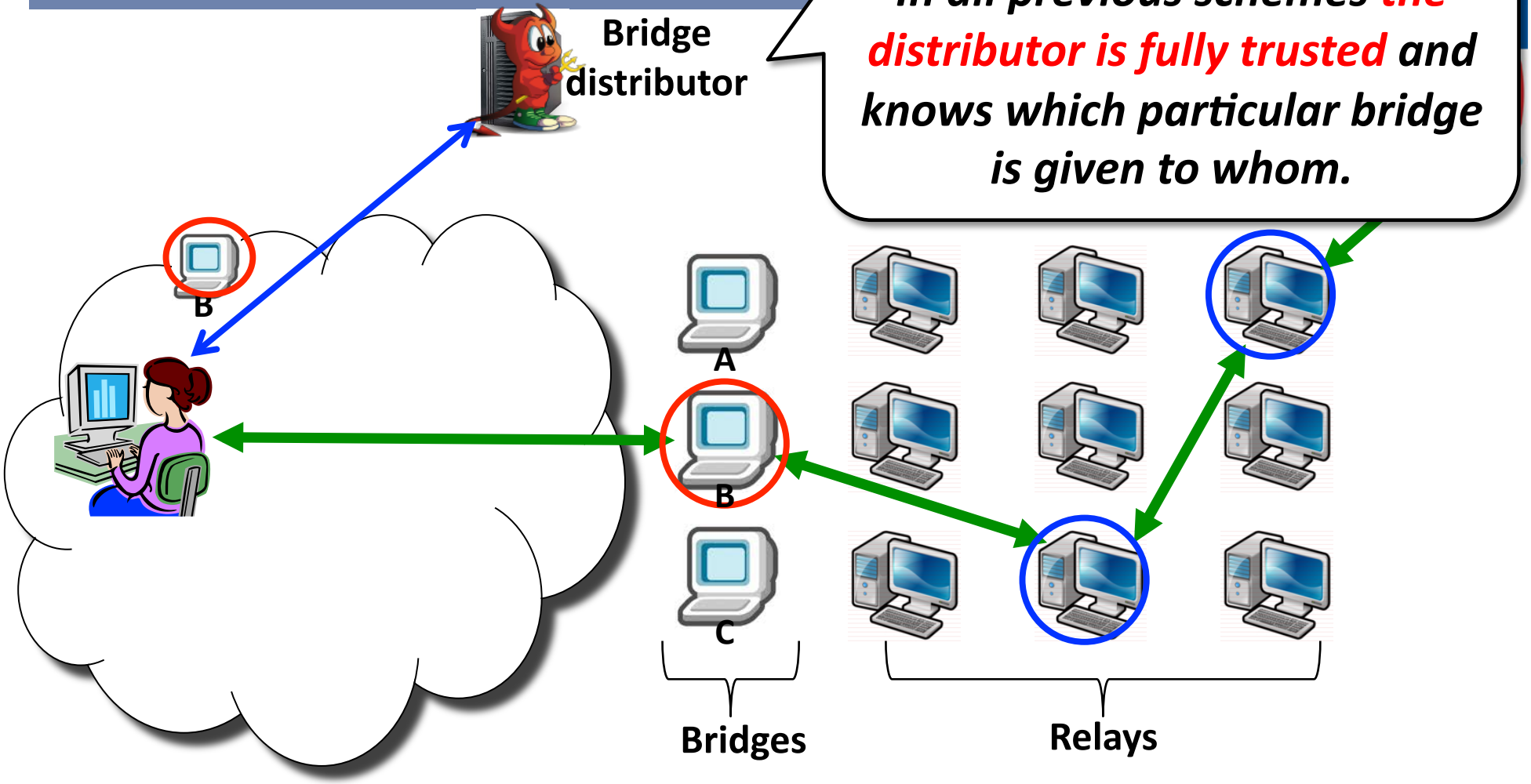
In Tor, the selection of relays must be kept secret, even from the directory authority!

Privacy preservation



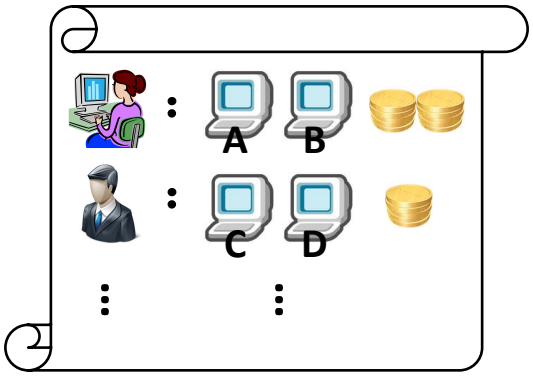
In Tor, the selection of relays must be kept secret, even from the directory authority!

Privacy preservation



rBridge: privacy preservation

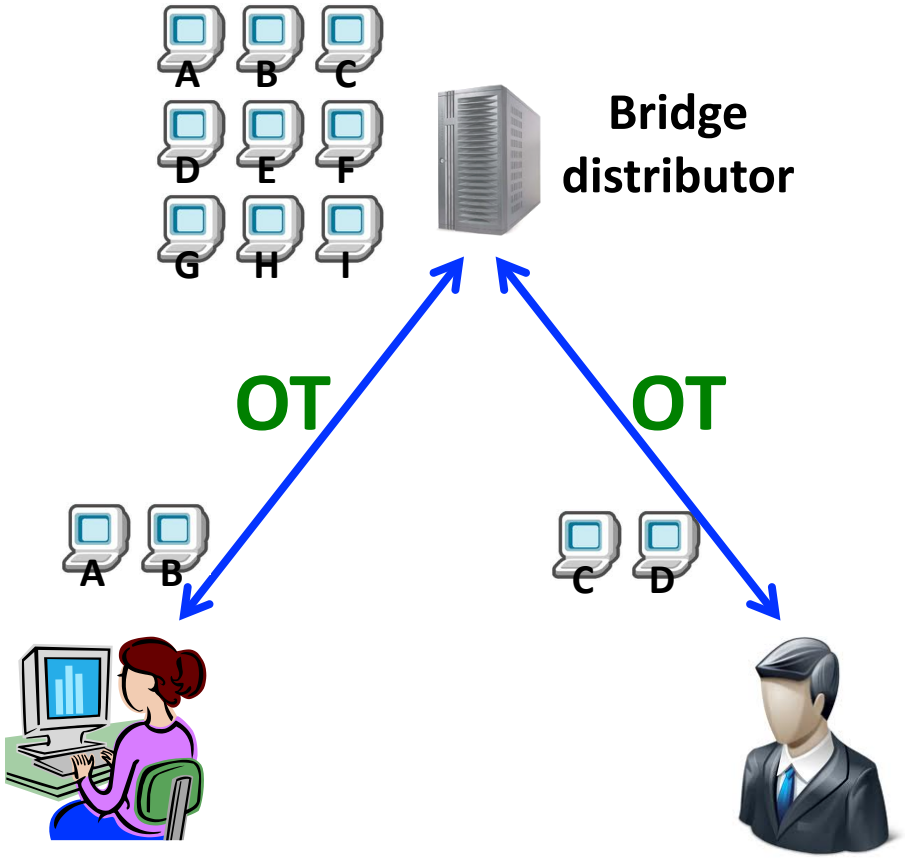
The basic rBridge scheme (without privacy preservation):



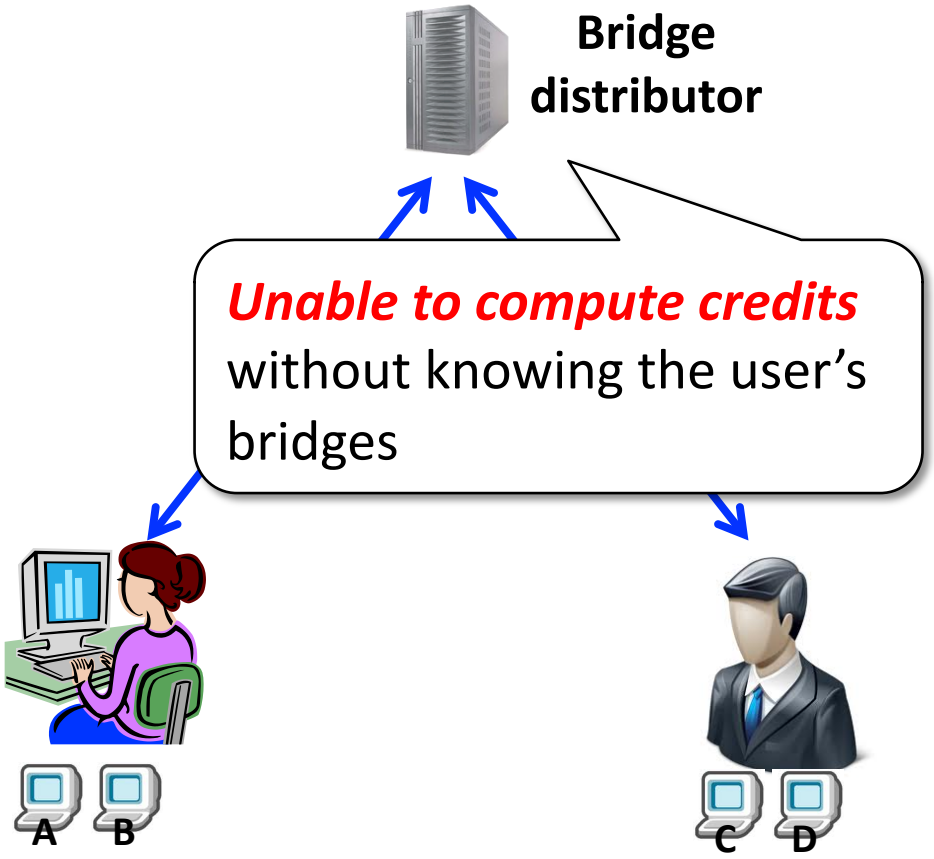
Bridge distributor

rBridge: privacy preservation

Use ***Oblivious Transfer (OT)*** to give out bridges, while ***hiding which bridges are received by the user***.

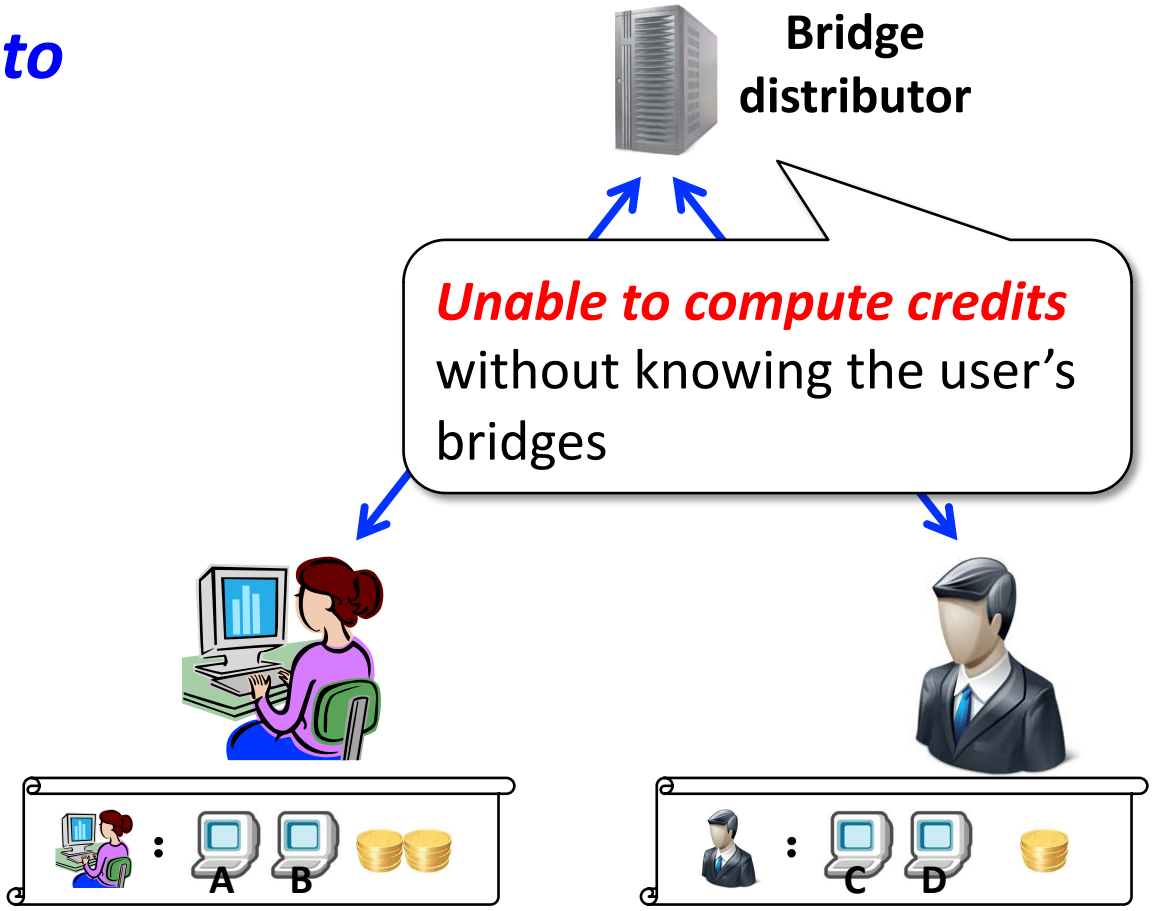


rBridge: privacy preservation



rBridge: privacy preservation

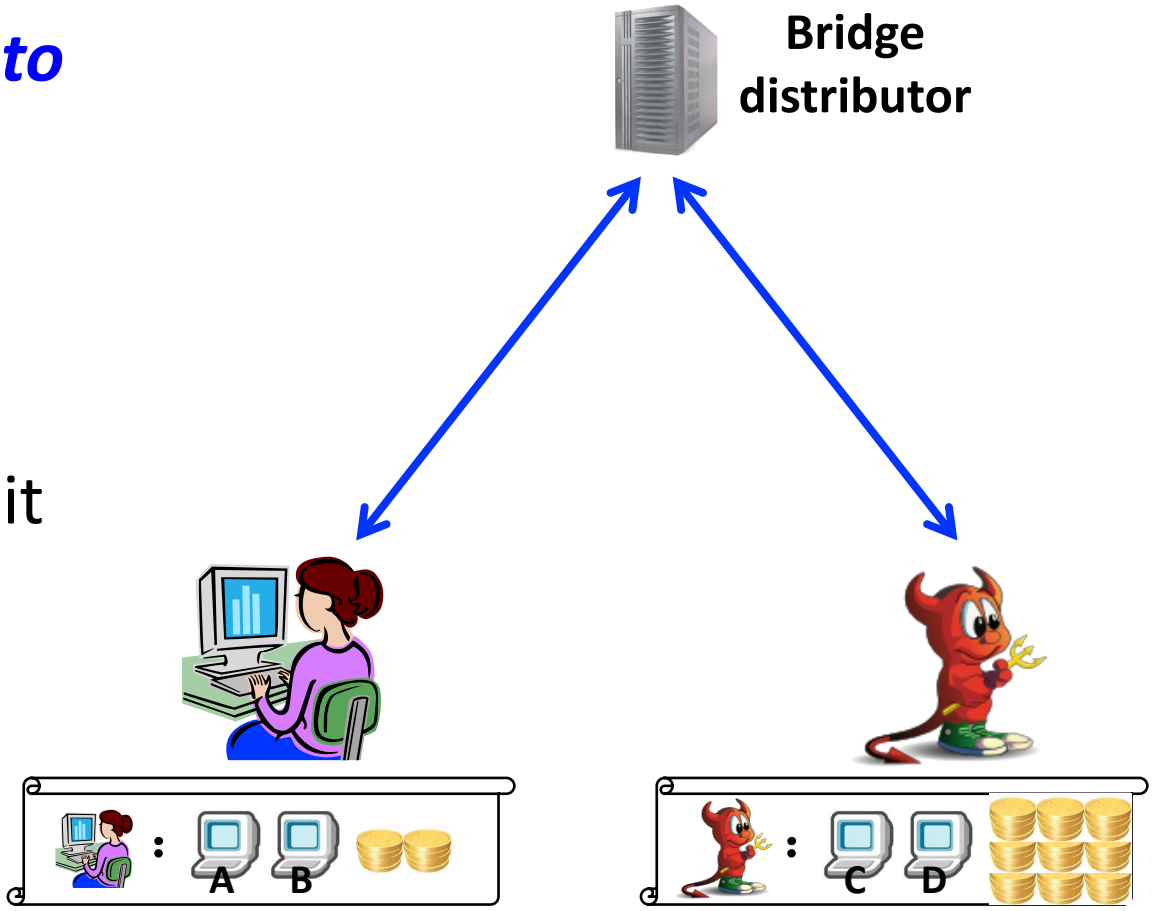
Delegate the task of computing reputation to users themselves.



rBridge: privacy preservation

Delegate the task of computing reputation to users themselves.

We need to prevent ***user misbehavior***, e.g., manipulating credit balance.



rBridge: privacy preservation

Anonymous Credential

: **Pseudonym X**

: **Credit balance Φ**

: ID of assigned **bridge B_i**,
time T_i when B_i was given to X,
#credits Φ_i earned from B_i

rBridge: privacy preservation

Anonymous Credential

: **Pseudonym X**

: **Credit balance Φ**

: ID of assigned **bridge B_i**, **time T_i** when B_i was given to X, **#credits Φ_i** earned from B_i

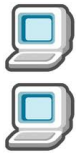
Use ***blind signature*** to sign each part of the credential to ***prevent manipulation***.

rBridge: privacy preservation

Anonymous Credential

: **Pseudonym X**

: **Credit balance Φ**

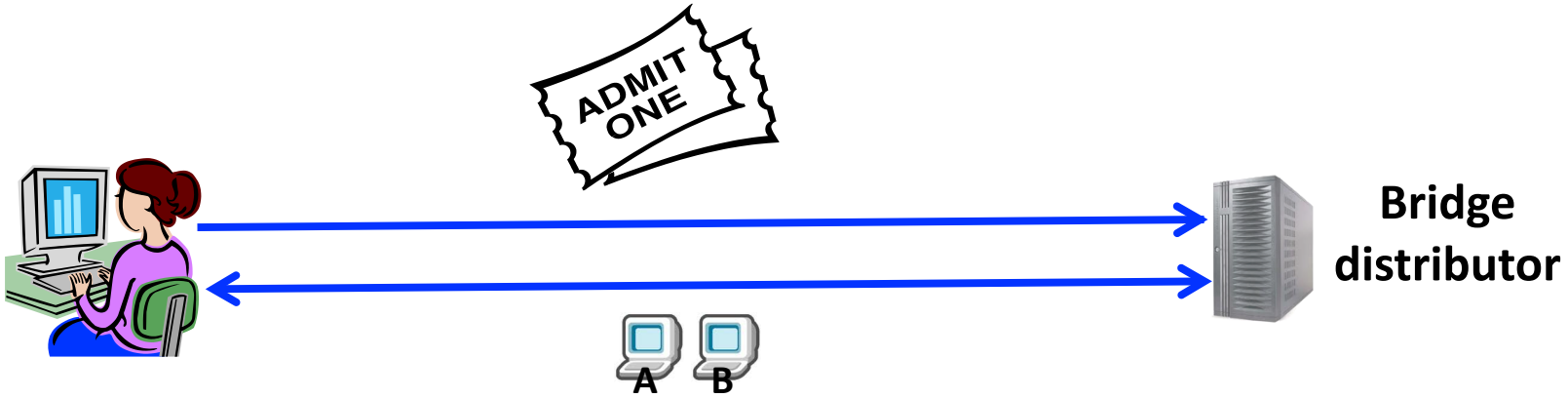


: ID of assigned **bridge B**
time T_i when B_i was gi
#credits Φ_i earned fro

Use ***blind signature*** to sign each part of the credential to ***prevent manipulation***.

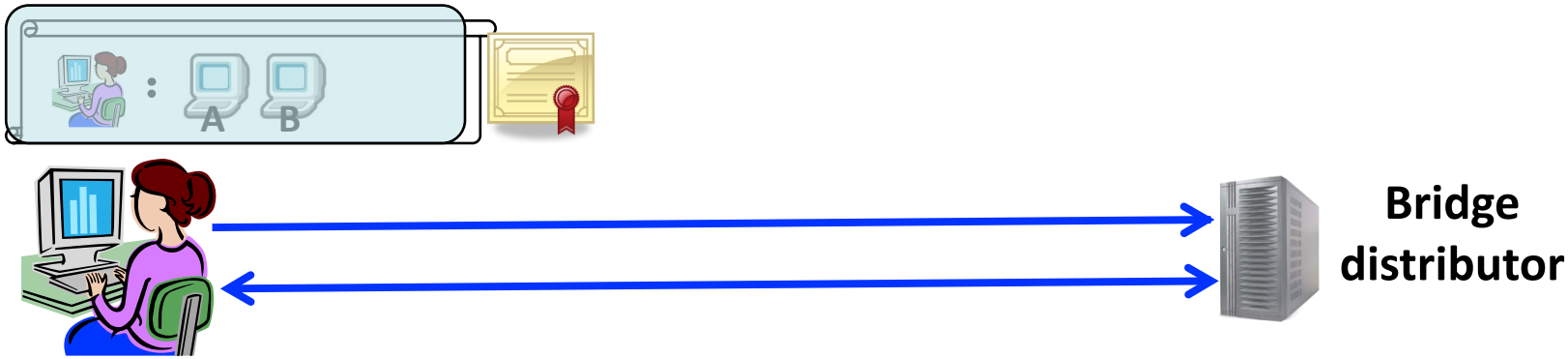
Use ***zero-knowledge proofs*** to prove the information on the credential is correct while ***hiding all the information from the bridge distributor***.

1. Registration

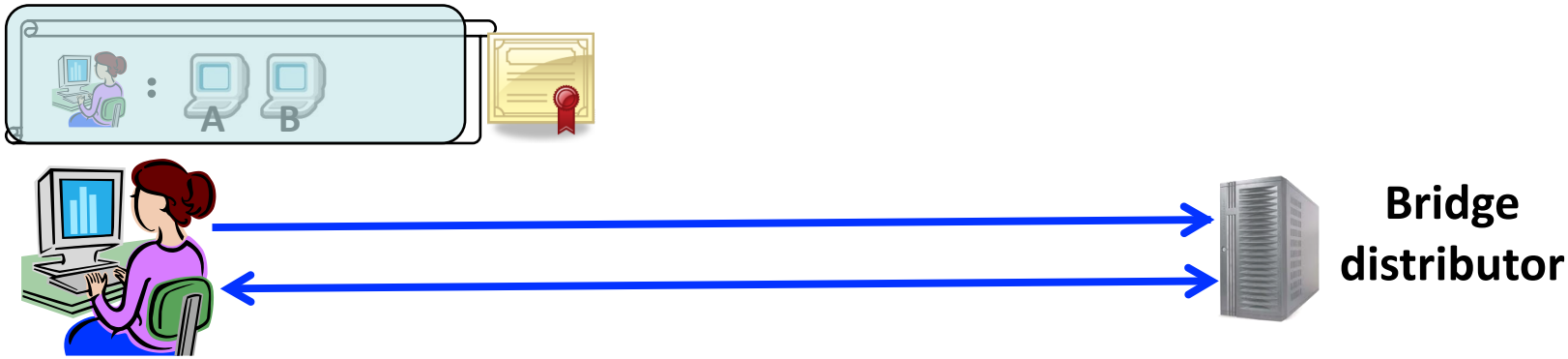


OT

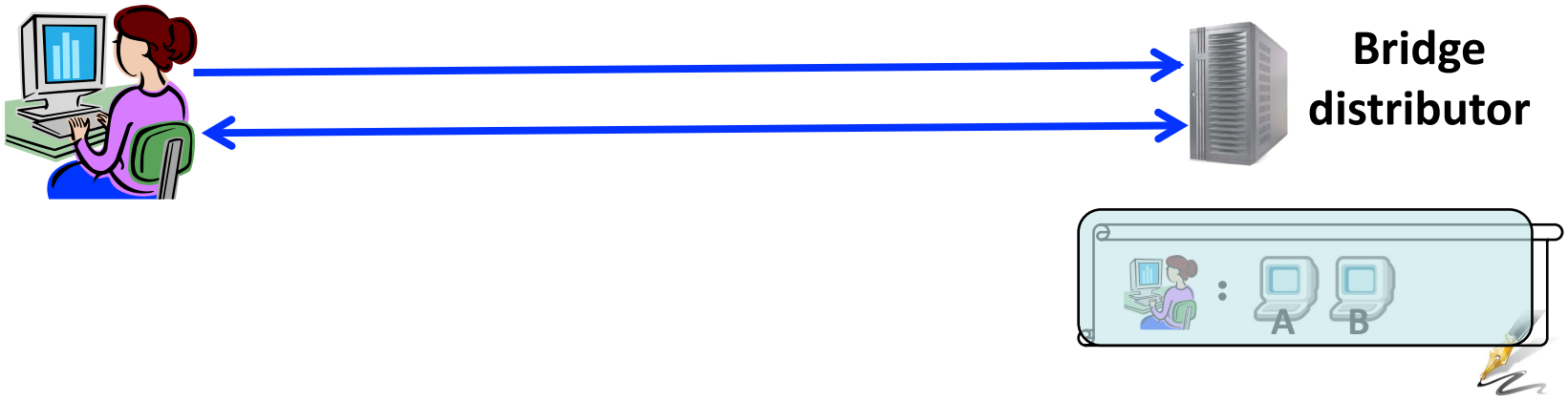
1. Registration



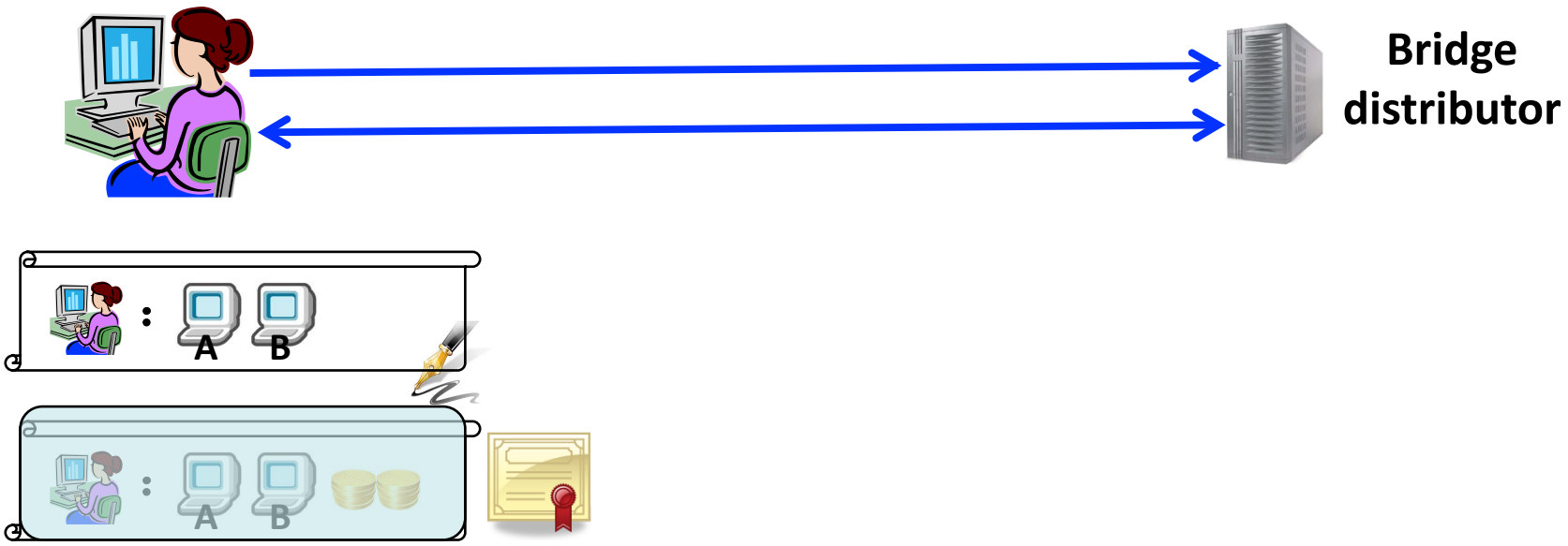
1. Registration



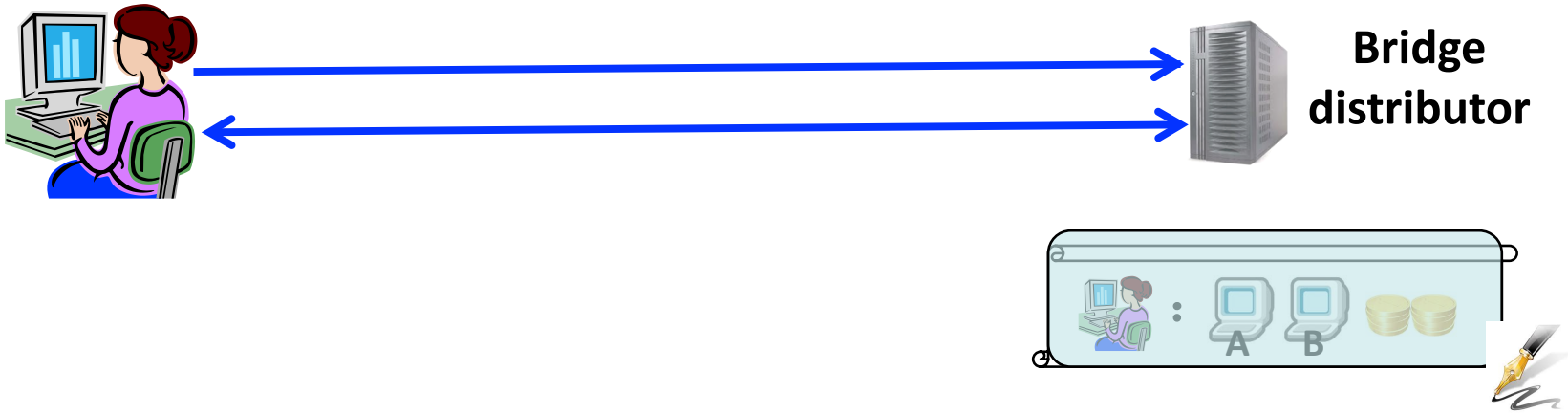
1. Registration



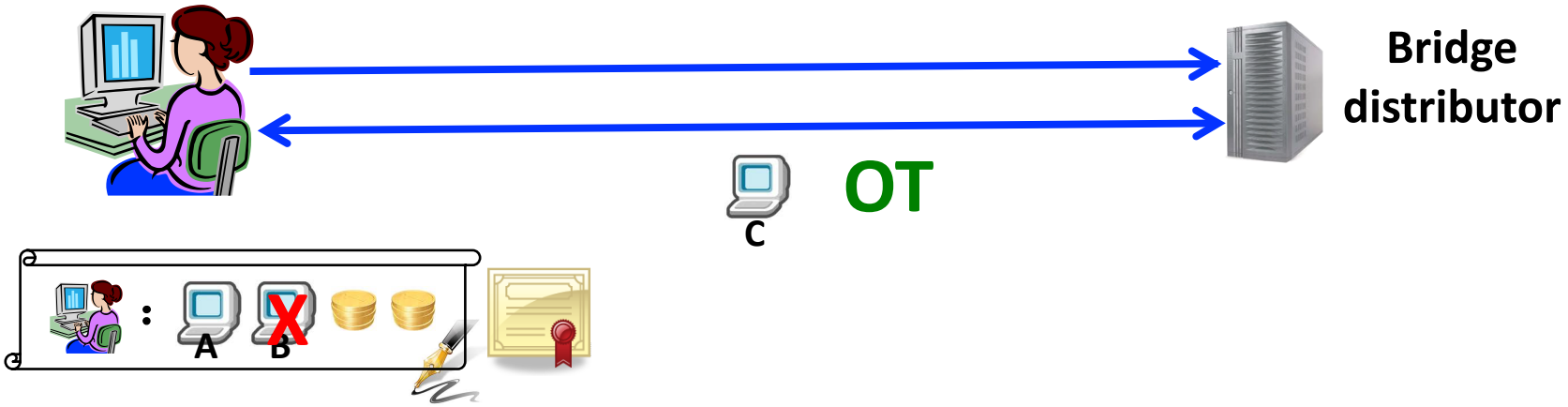
2. Update Credit Balance



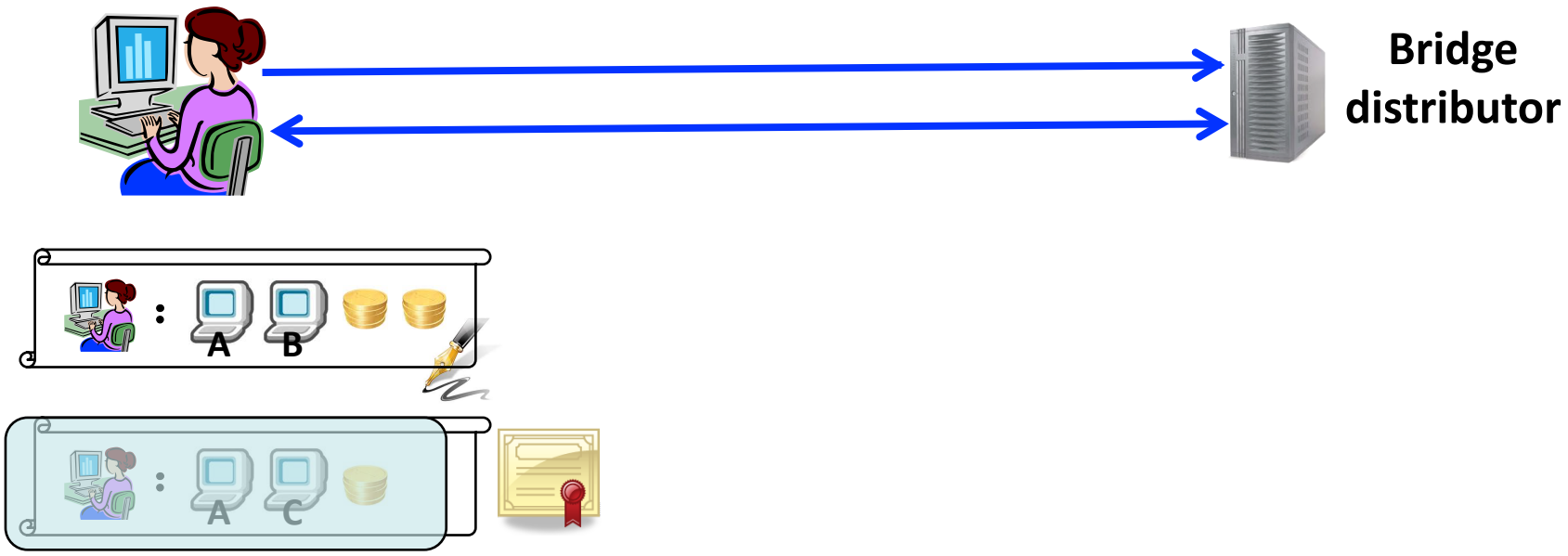
2. Update Credit Balance



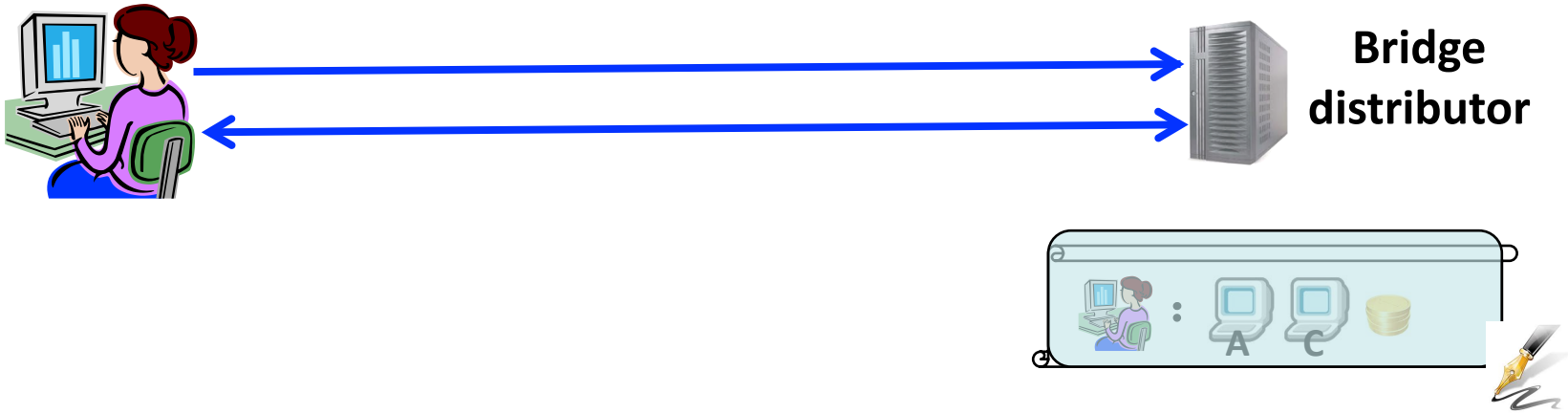
3. Bridge Exchange



3. Bridge Exchange



3. Bridge Exchange



Performance evaluation

Table 1: Performance (averaged over 100 runs)

Operation	Comp. (s) U	Comp. (s) D	Comm. (KB)
Registration	5.15	17.44	388.1
Updating credit balance	0.51	0.47	34.7
Getting a new bridge	5.35	17.62	340.1
Inviting new users	0.27	0.16	2.0

These operations are ***infrequent***!

Performance evaluation

Table 1: Performance (averaged over 100 runs)

Operation	Comp. (s) U	Comp. (s) D	Comm. (KB)
Registration	5.15	17.44	388.1
Updating credit balance	0.51	0.47	34.7
Getting a new bridge	5.35	17.62	340.1
Inviting new users	0.27	0.16	2.0

These operations are ***infrequent***!

In the current Tor network, each client needs to download 120 KB network-status file every 3 hours

Summary

- Leverage ***user reputation*** to bridge the gap between robustness and openness in Tor bridge distribution.
  - High-reputation users can ***buy*** bridges and ***invite*** new friends
  - Much higher ***robustness*** than previous work
- Design the first ***privacy-preserving*** bridge distribution scheme
  - Use Oblivious Transfer, Commitment, Zero-knowledge Proof, and Blind Signature as building blocks.

Thank you!

Question?