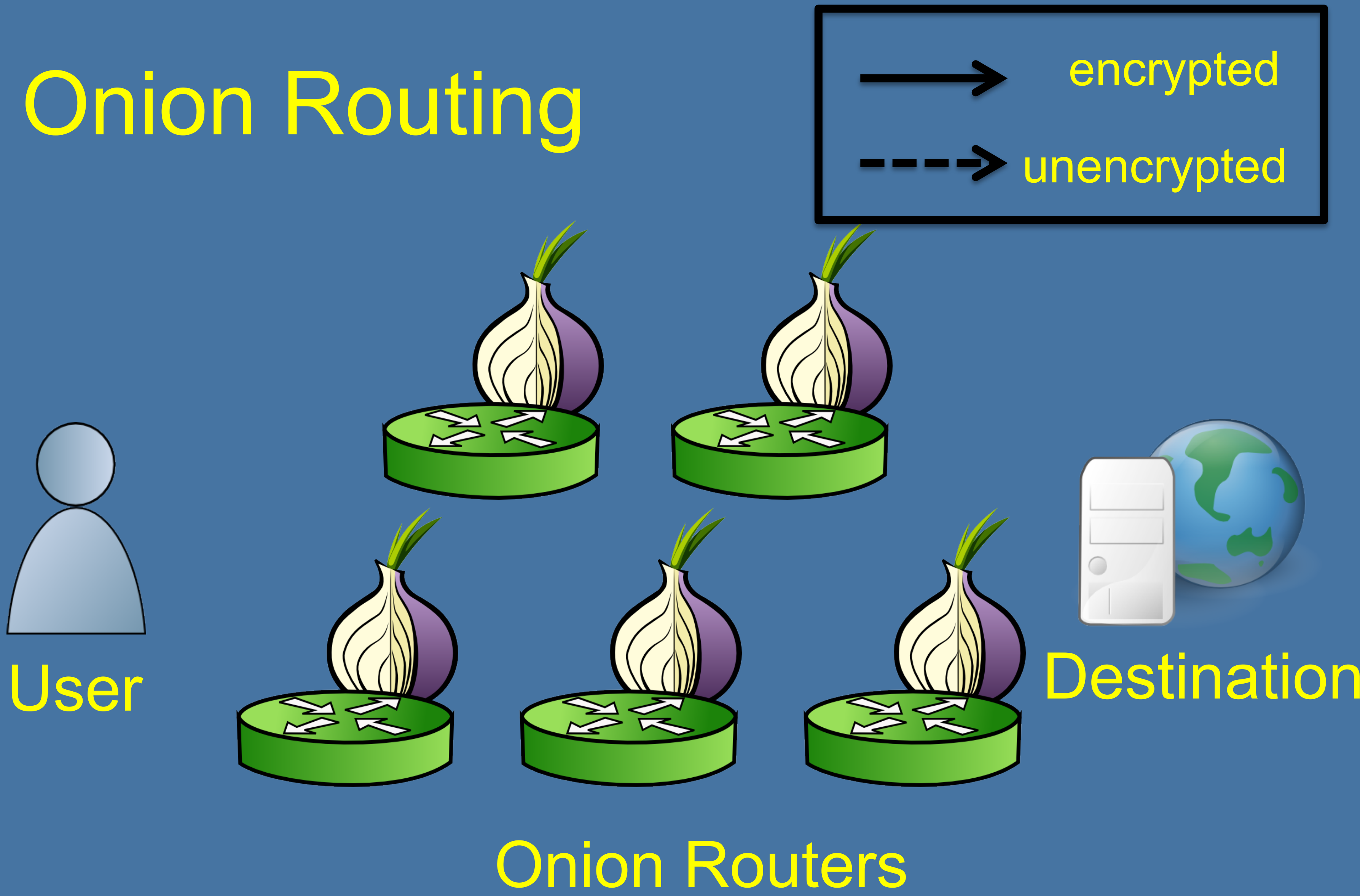
LIRA: Lightweight Incentivized Routing for Anonymity

20th Annual Network & Distributed System Security Symposium
February 27, 2013

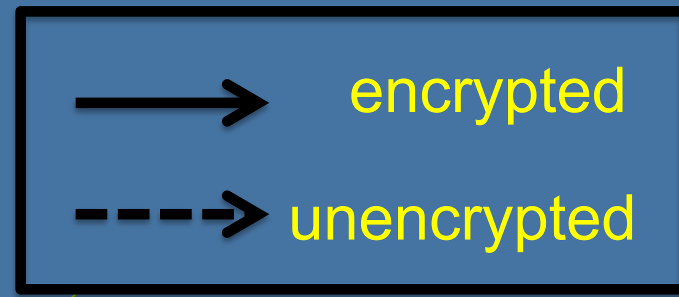
Rob Jansen
Aaron Johnson
Paul Syverson
U.S. Naval Research Laboratory

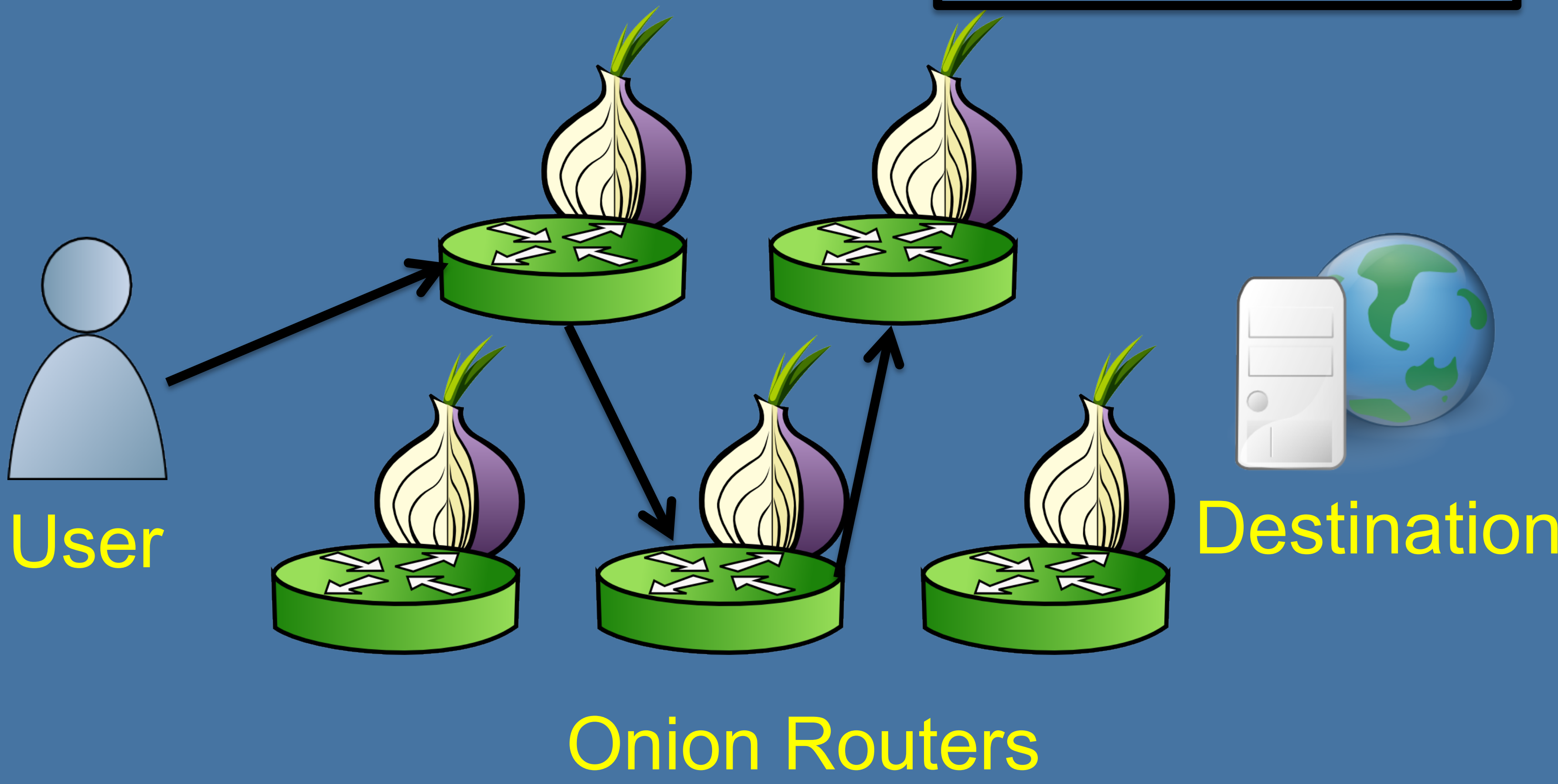
Problem

Onion Routing

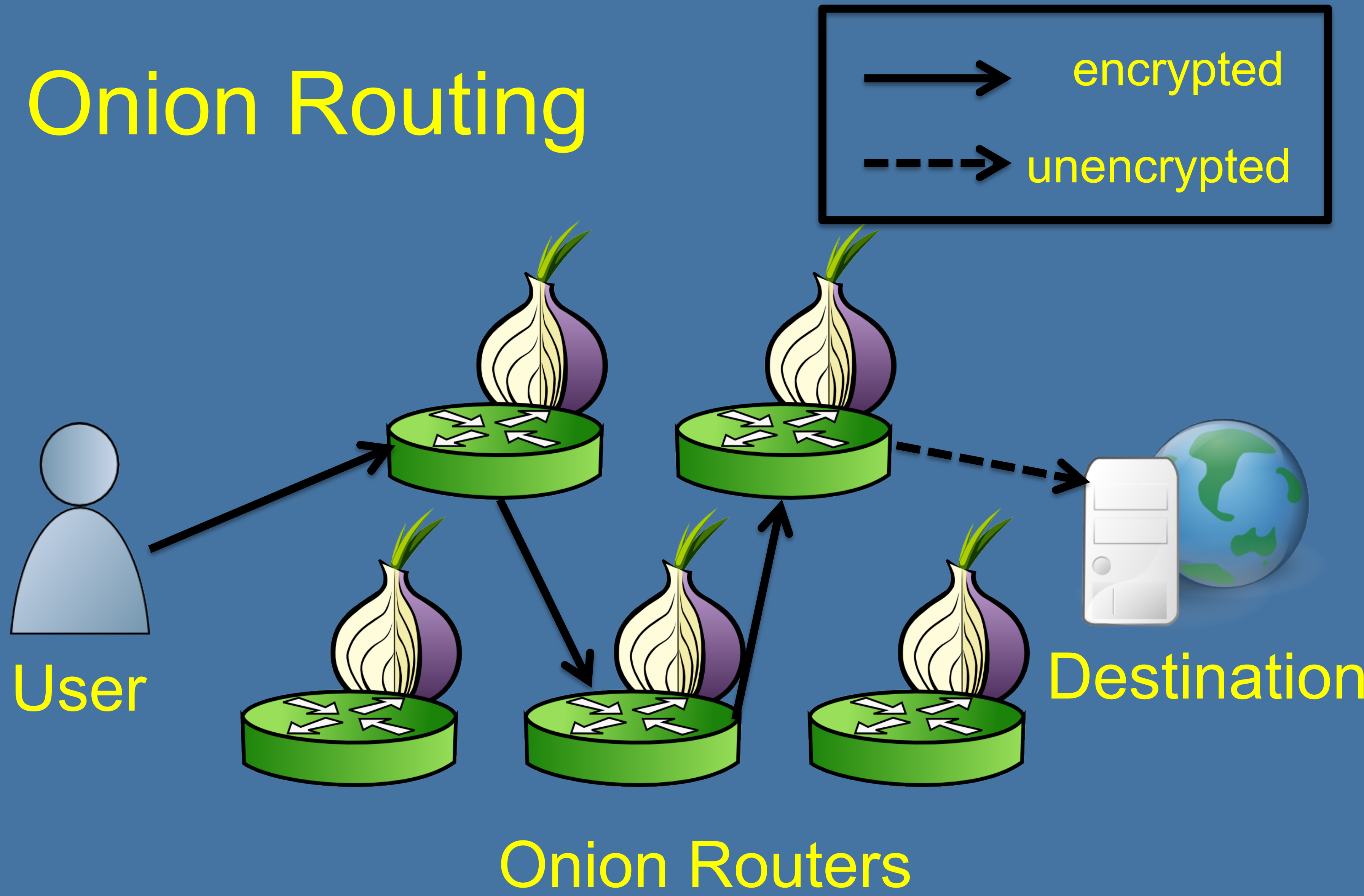


Onion Routing

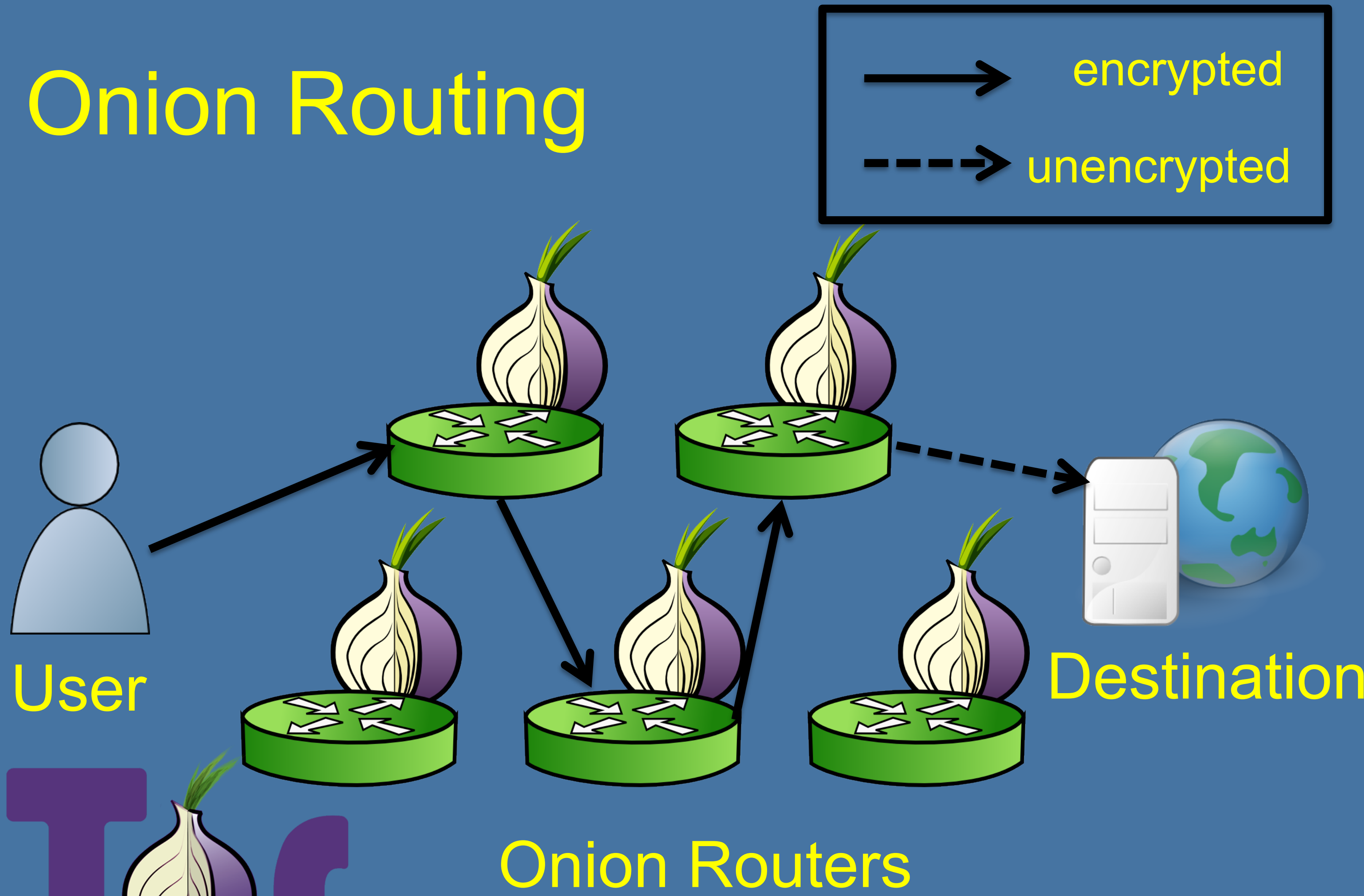




Onion Routing

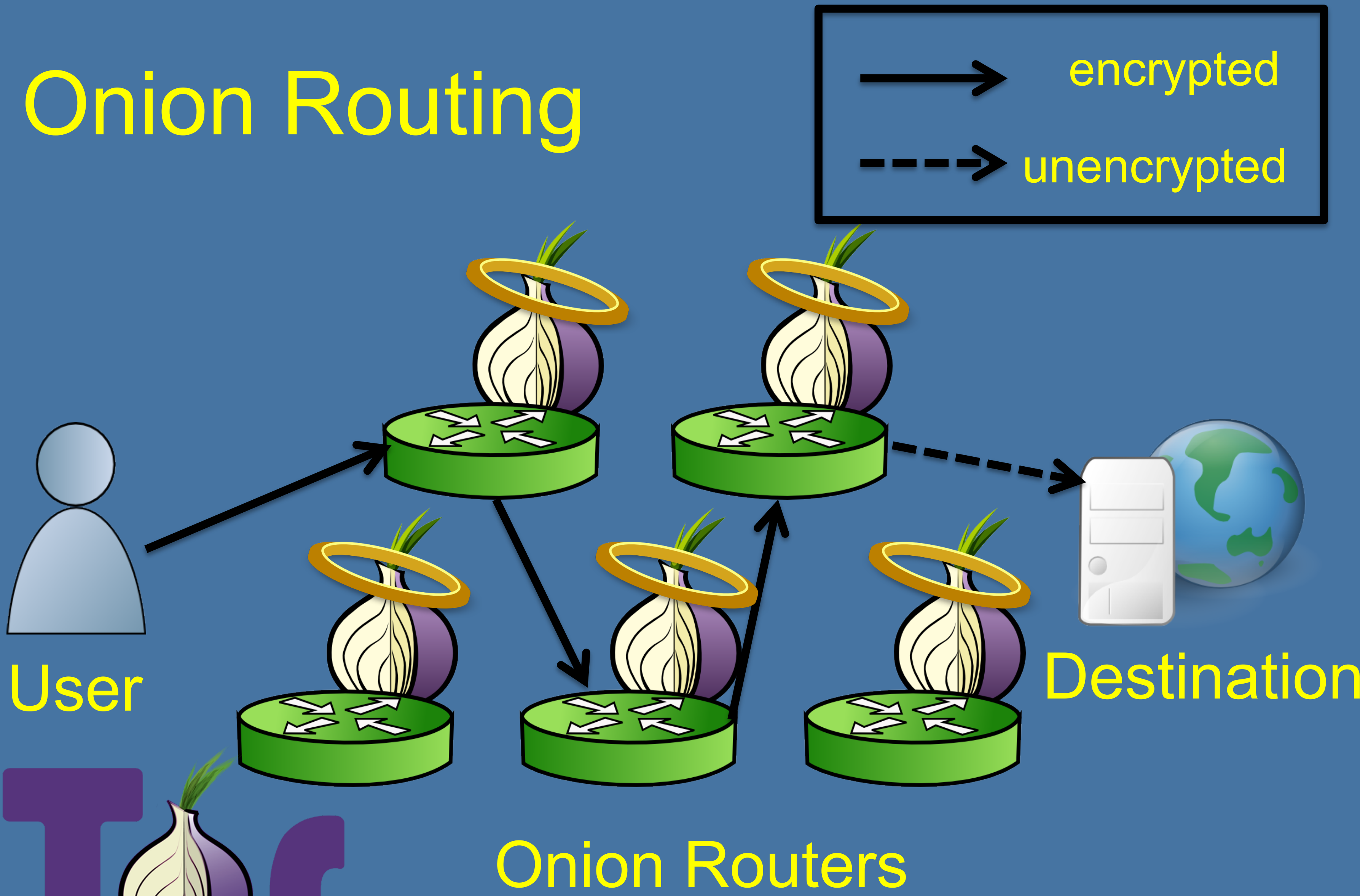


Onion Routing



torproject.org

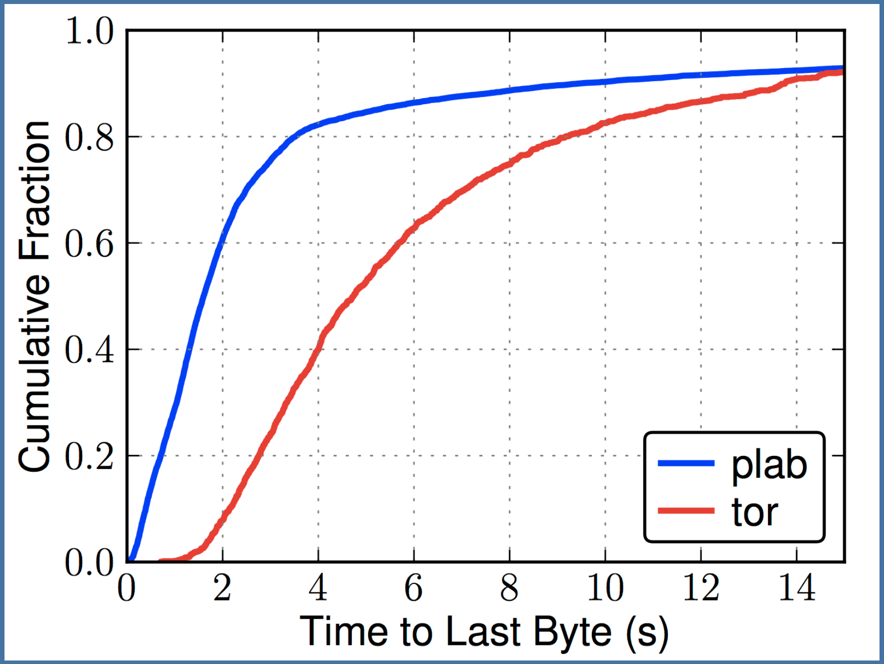
Onion Routing



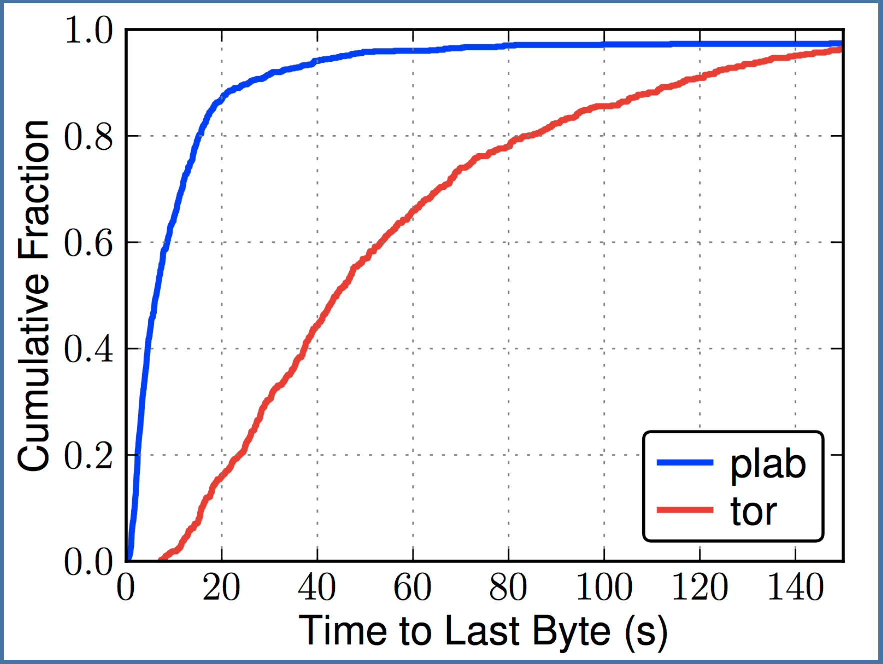
torproject.org

Tor is Slow

Web (320 KiB)

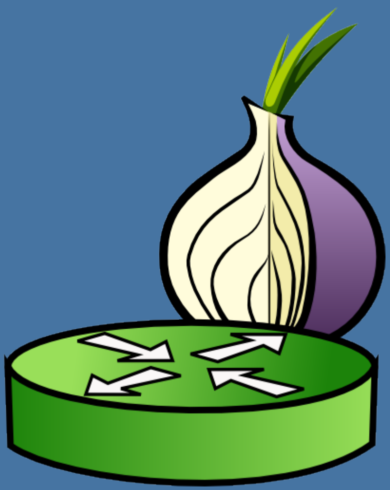


Bulk (5 MiB)



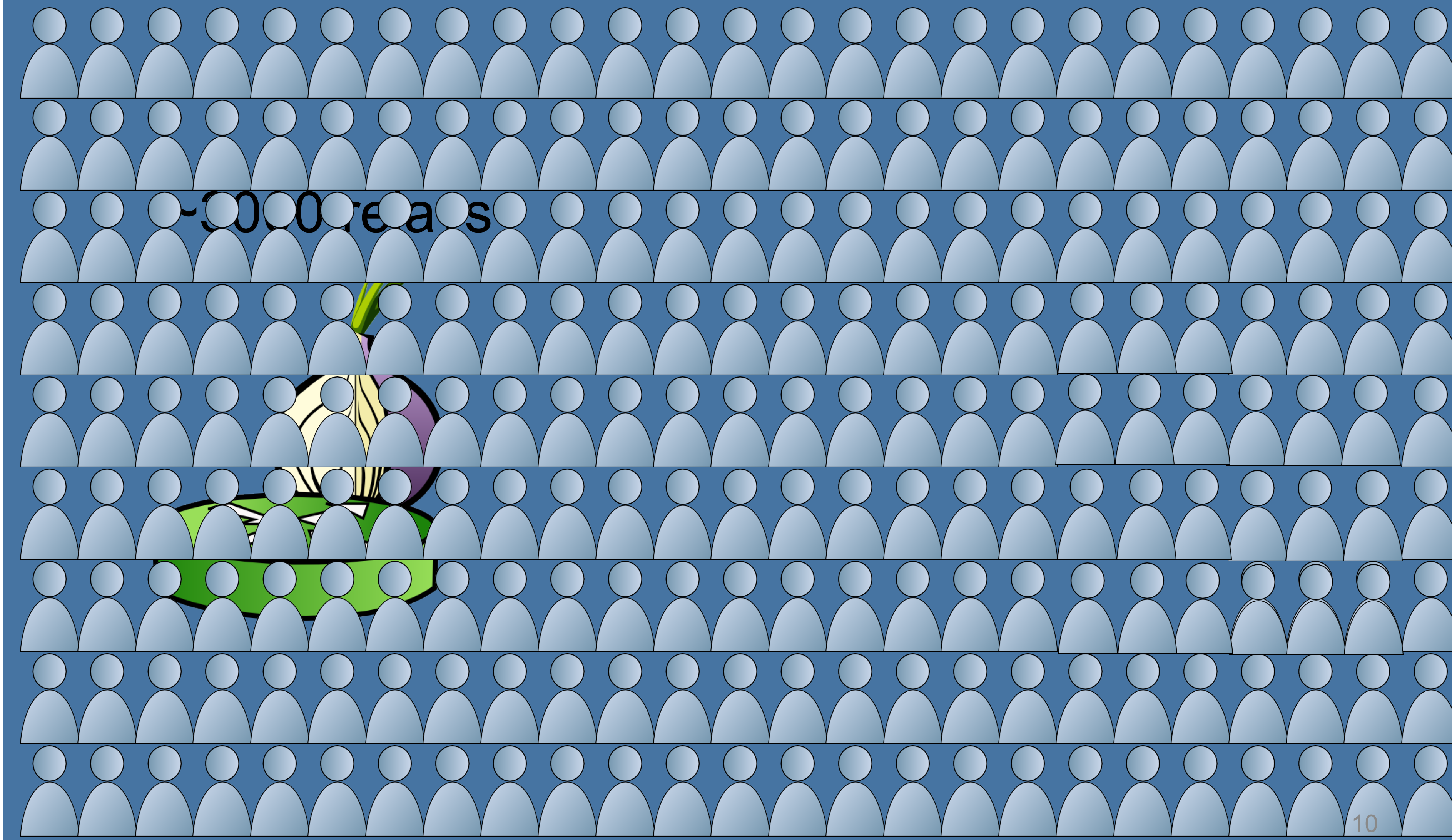
Tor Utilization

~3000 relays

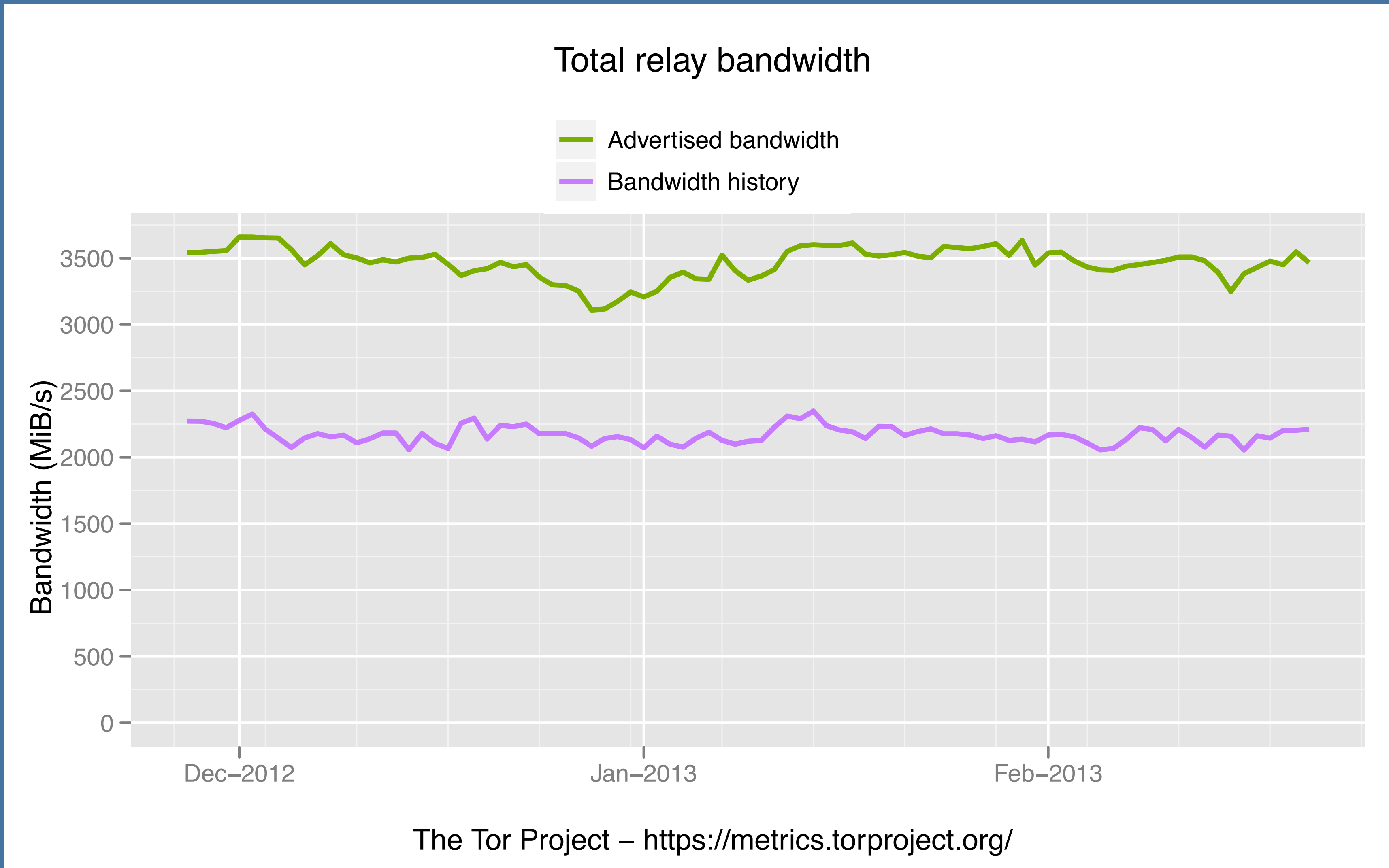


Tor Utilization

~500,000 users/day



Tor Utilization

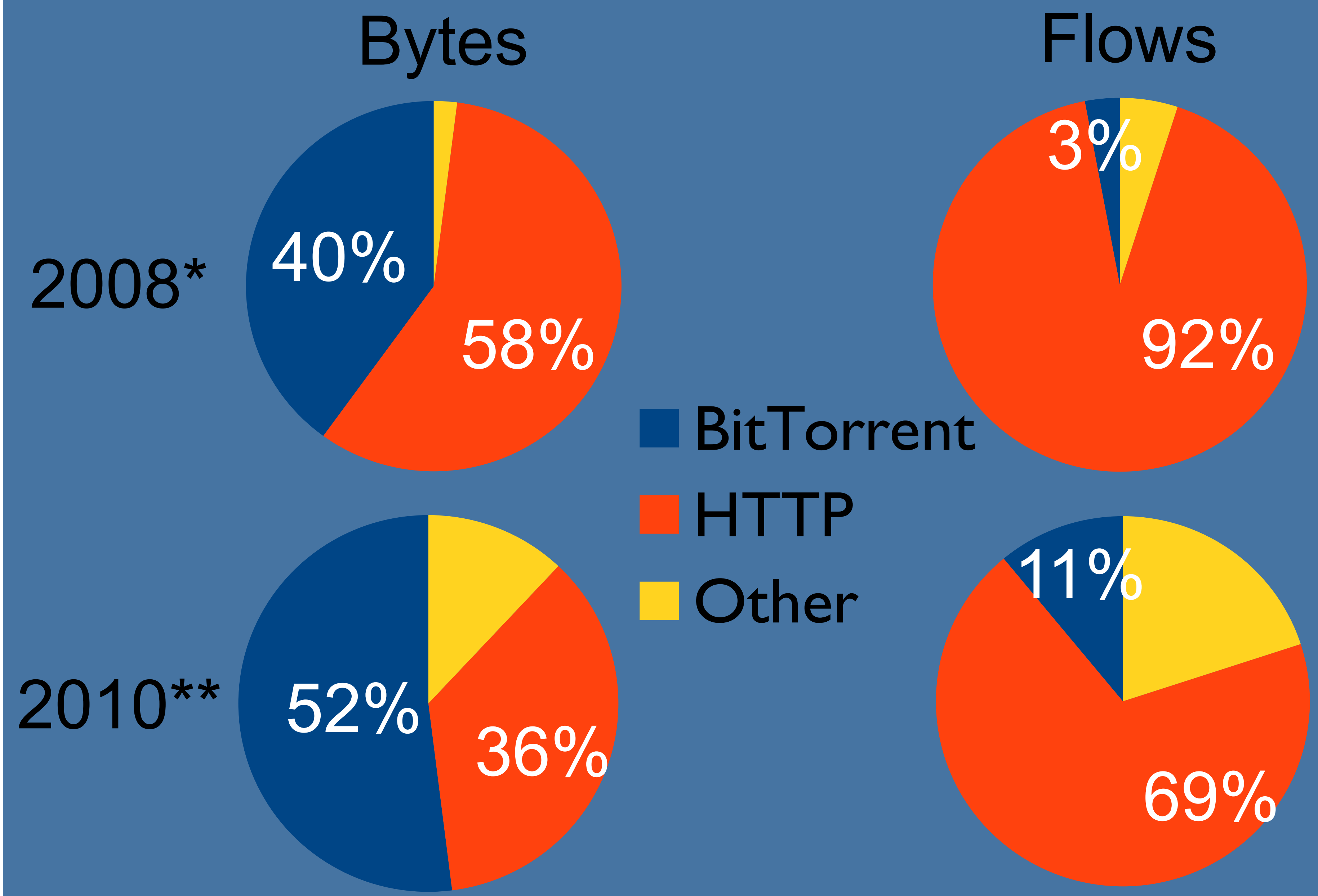


Tor's Top 20 Exit Relays

Exit Probability	Advertised Bandwidth	Nickname	Country
7.25%	0.87%	chaoscomputerclub18	DE
6.35%	0.93%	chaoscomputerclub20	DE
5.92%	1.48%	herngaard	US
3.60%	0.66%	chomsky	NL
3.35%	1.17%	dorrisdeebrown	DE
3.32%	1.18%	bolobolo1	DE
3.26%	0.65%	rainbowwarrior	NL
2.32%	0.36%	sdnettor01	SE
2.23%	0.69%	TheSignul	RO
2.22%	0.41%	raskin	DE
2.05%	0.40%	bouazizi	DE
1.93%	0.65%	assk	SE
1.82%	0.39%	kramse	DK
1.67%	0.35%	BostonUCompSci	US
1.53%	0.40%	bach	DE
1.31%	0.73%	DFRI0	SE
1.26%	0.31%	Amunet2	US
1.13%	0.27%	Amunet8	US
0.84%	0.27%	chaoscomputerclub28	DE
0.76%	0.37%	DFRI3	SE

Total: 54.14%

compass.torproject.org



*McCoy et al. PETS 2008, **Chaabane et al. NSS 2010

Our Solution

Incentive Scheme

- LIRA

Relays' own traffic gets better performance

Incentive Schemes

- LIRA
- Gold star
- Tortoise
- BRAIDS
- Freedom
- PAR
- XPay

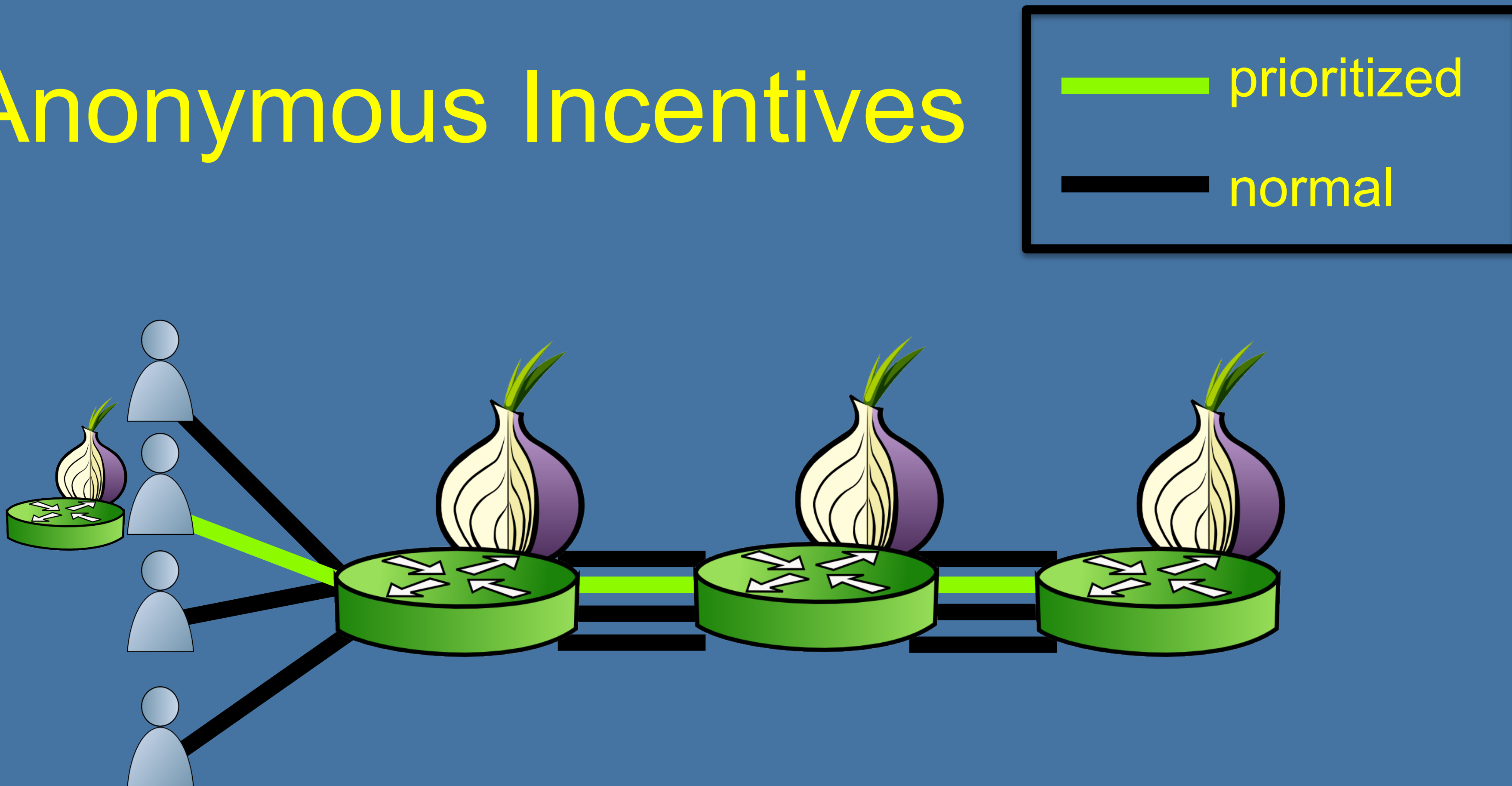
LIRA, Gold star, Tortoise, BRAIDS: Relays' own traffic gets better performance

Freedom, PAR, XPay: Charge users, pay relays

Incentive Schemes

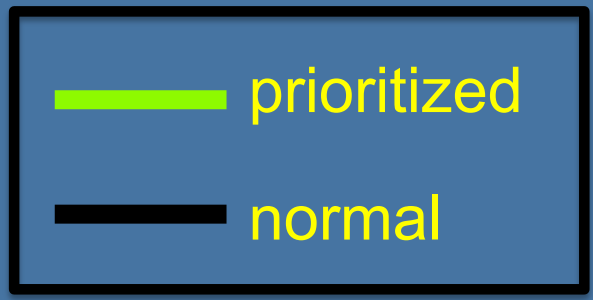
	External payment	Non-relays pay	Efficiency concerns	Anonymity concerns
Freedom	✖	✖		
PAR	✖	✖		
XPay	✖	✖		
Gold star				✖
Tortoise				✖
BRAIDS			✖	

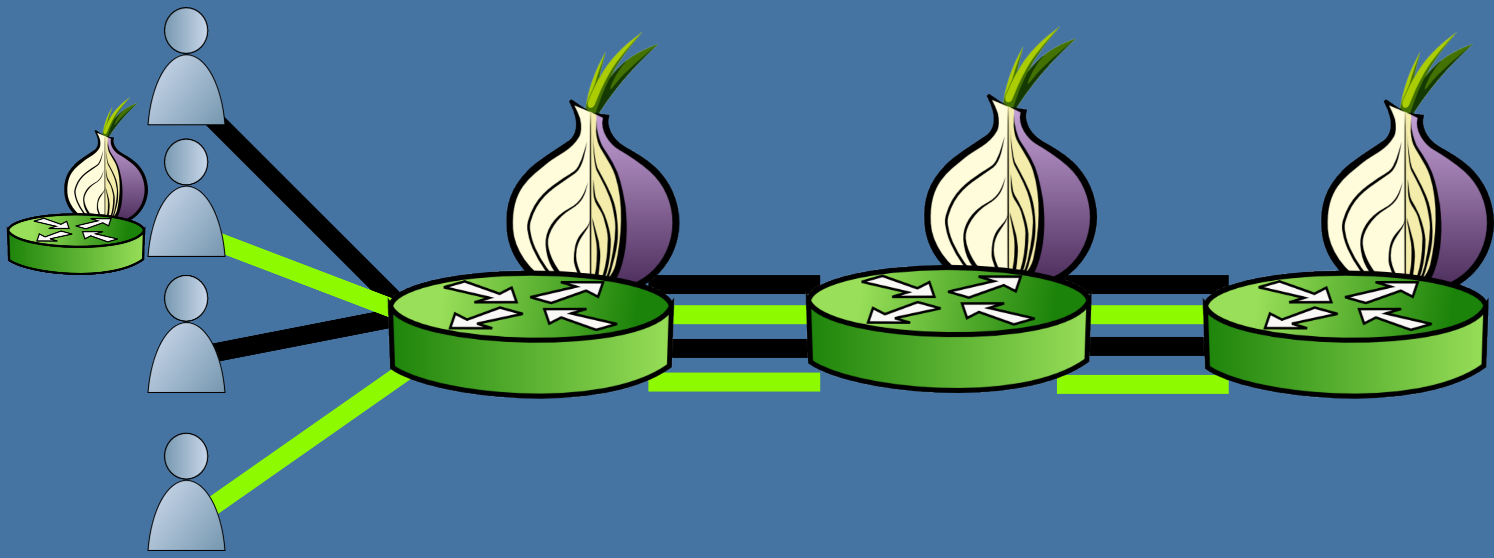
Anonymous Incentives



Problem: Priority identifies user as a relay

Anonymous Incentives



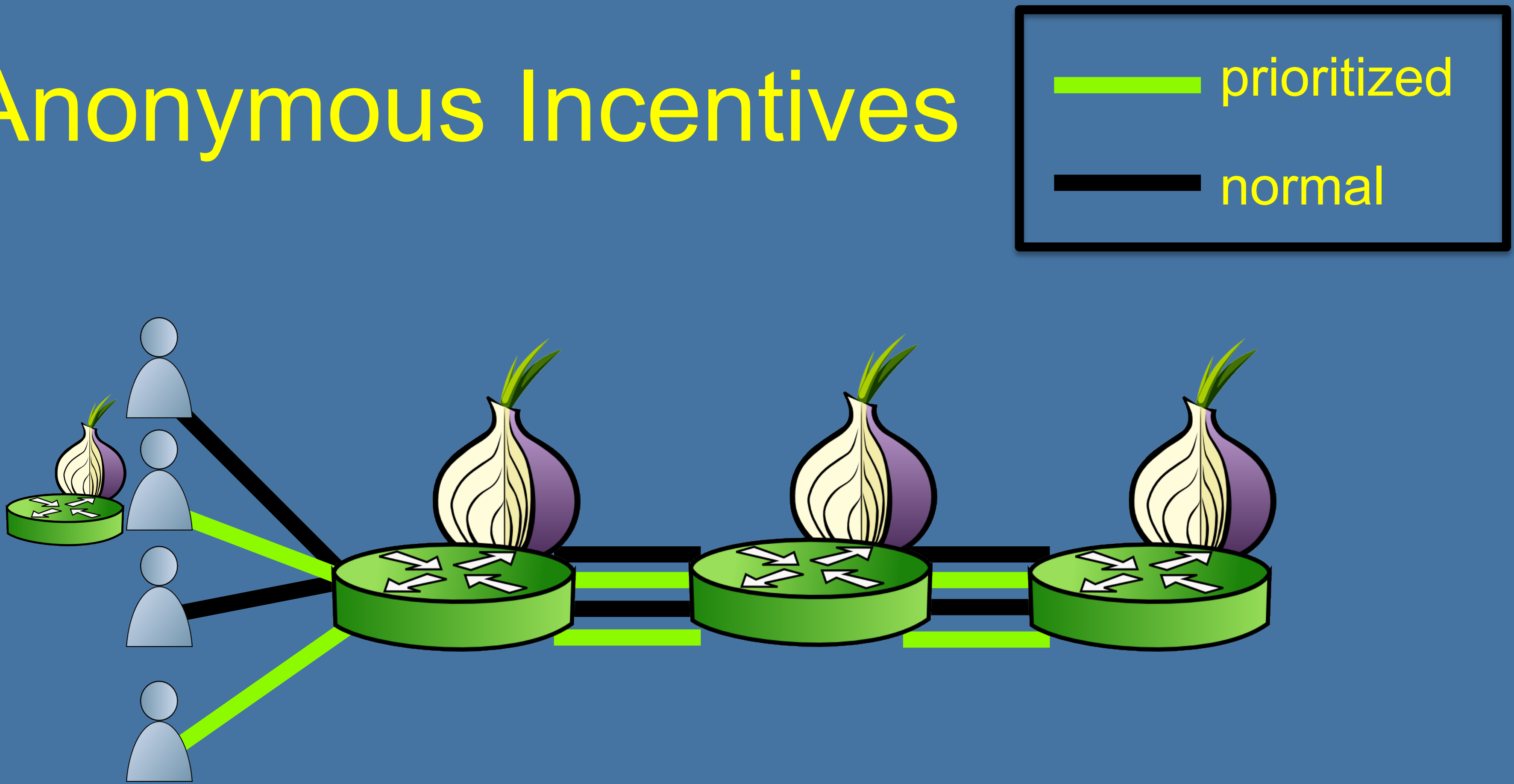


Problem: Priority identifies user as a relay

Solutions

1. Give some priority "tickets" to all users (BRAIDS).

Anonymous Incentives



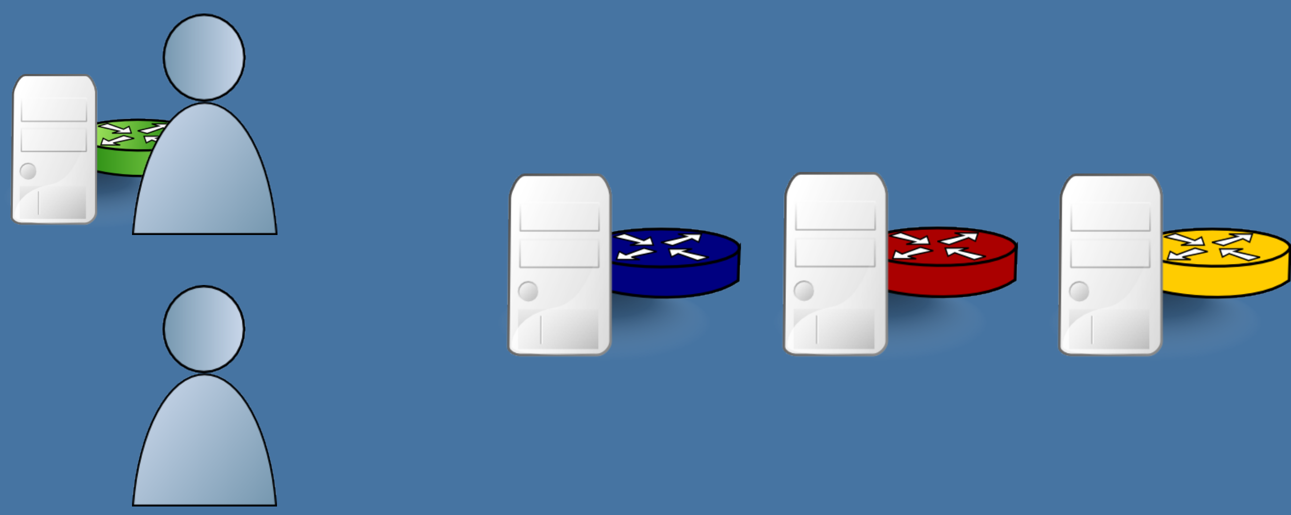
Problem: Priority identifies user as a relay

Solutions

1. Give some priority “tickets” to all users (BRAIDS).
2. Cryptographic lottery gives priority; winning tickets can be (secretly) bought (LIRA).

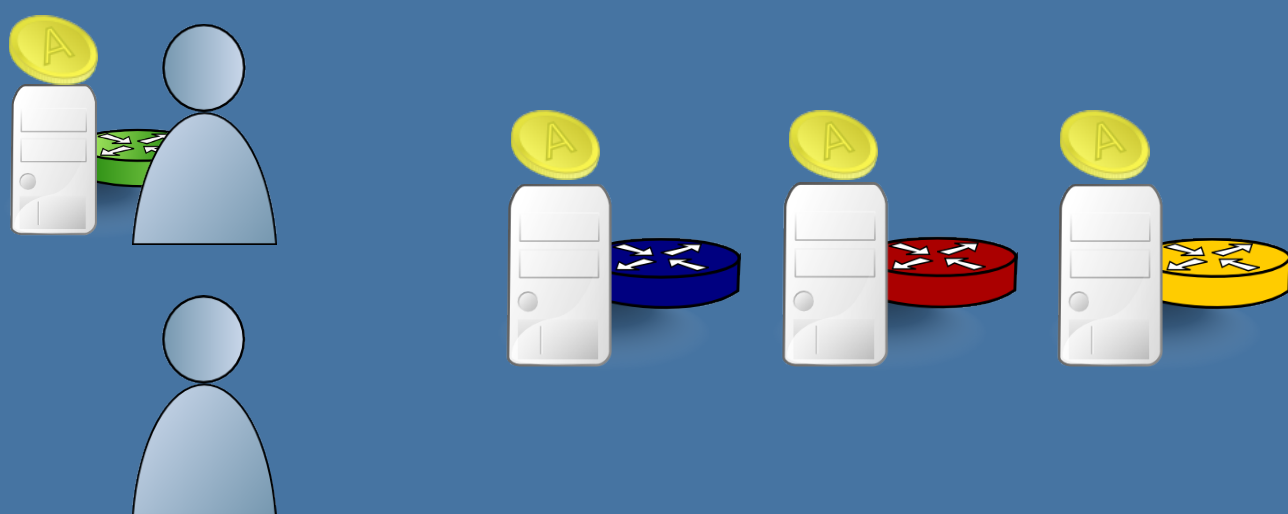
LIRA Design

Bank



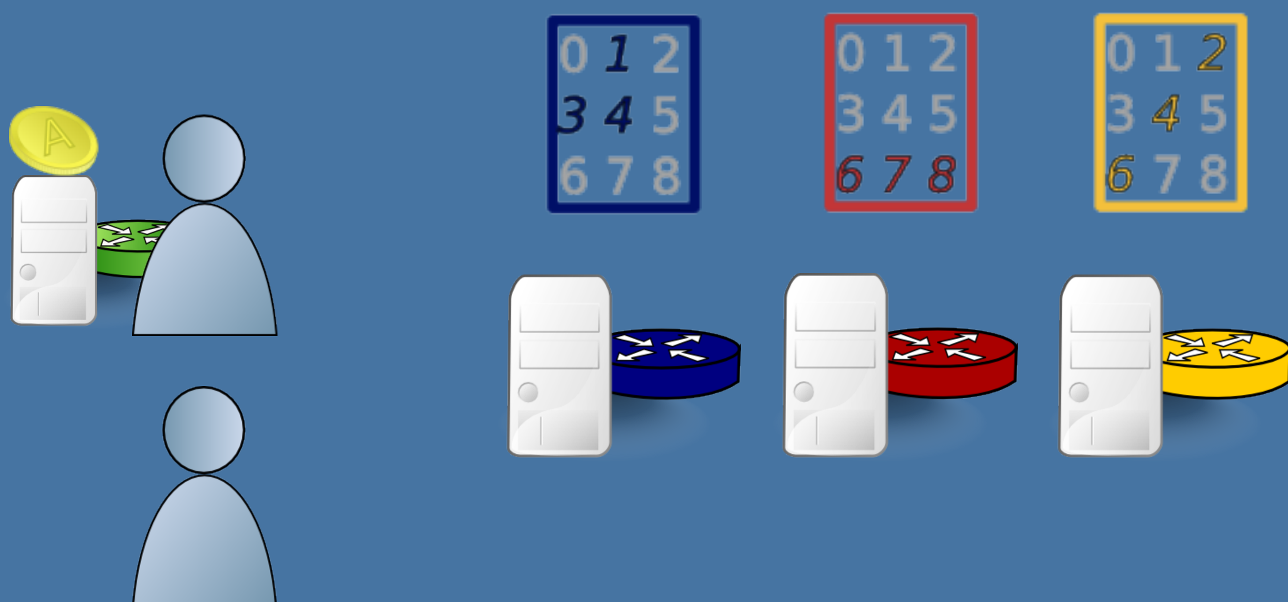
LIRA Design

Bank gives anonymous coins to relays based on amount of traffic forwarded



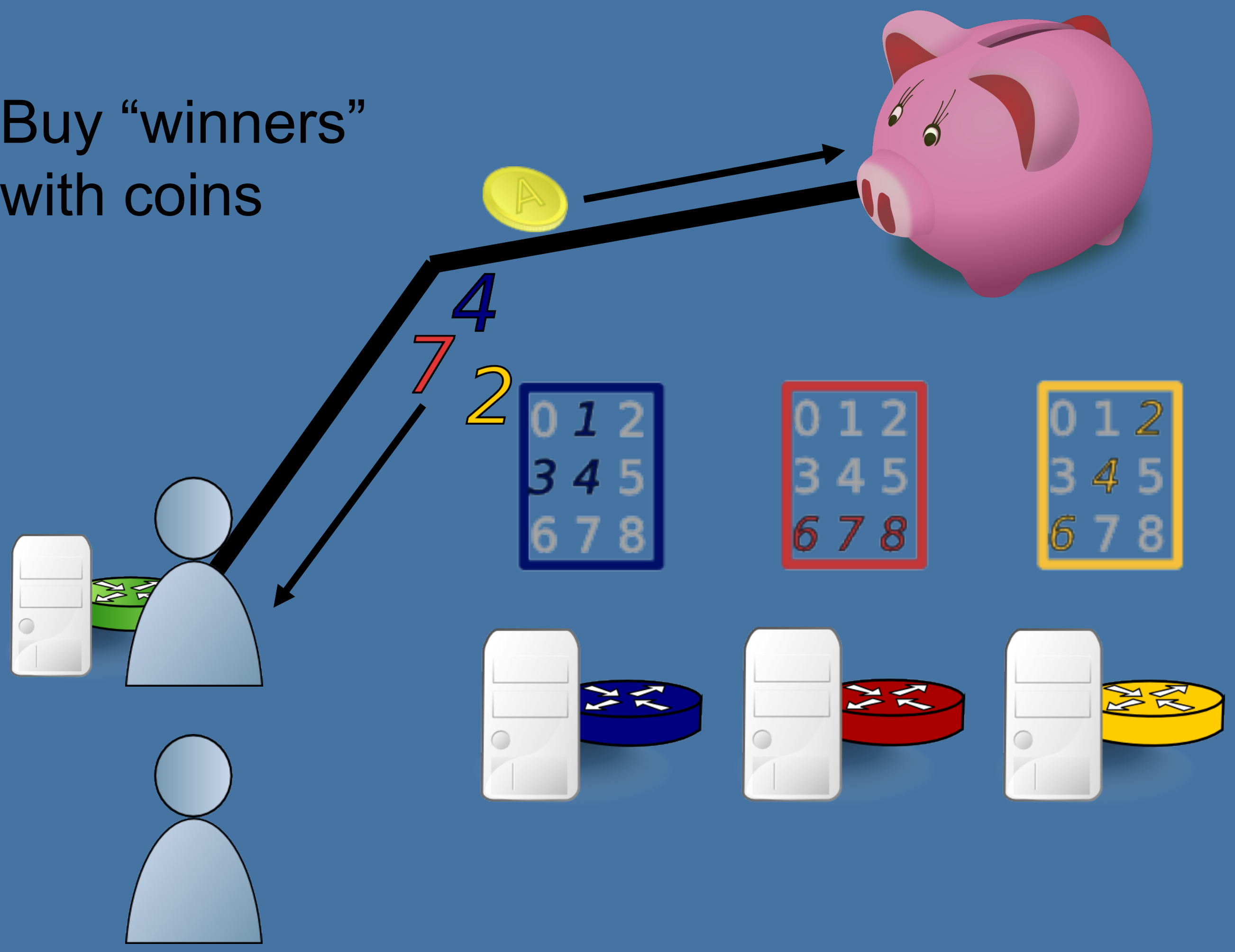
LIRA Design

Bank sets up lottery with each relay



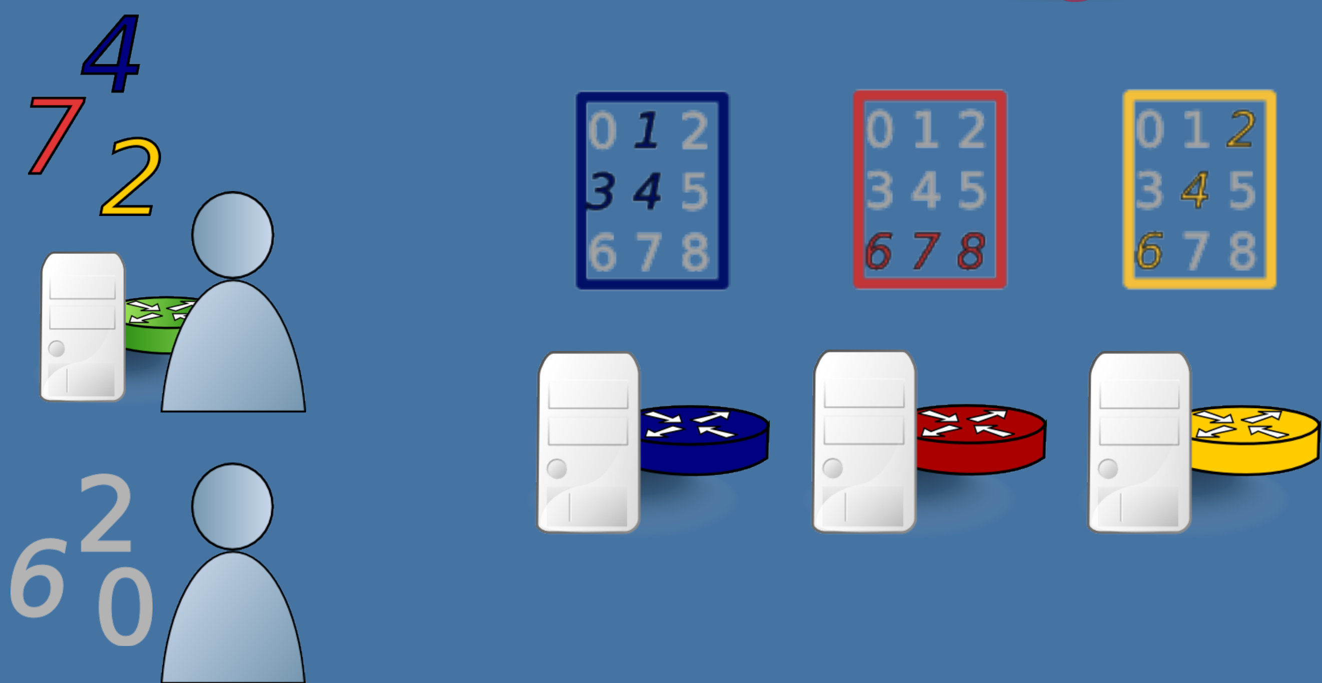
LIRA Design

Buy “winners”
with coins



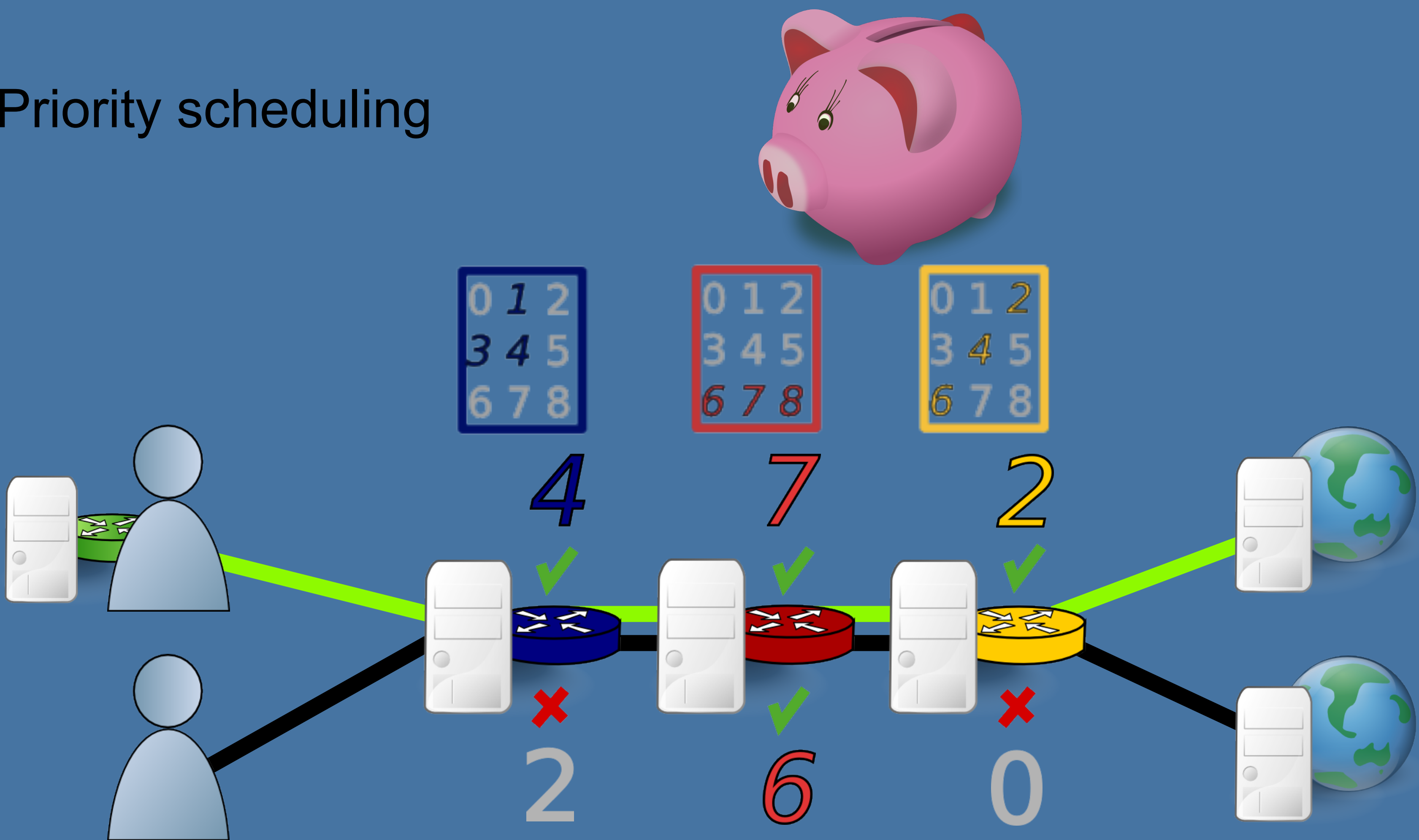
LIRA Design

Clients guess winners



LIRA Design

Priority scheduling



Cryptographic Lotteries

- Lottery at relay *r*
  $g_r: \{0,1\}^{2L} \rightarrow \{0,1\}^{2L}$
  x wins if
  - $g_r(x) = y_0 \,||\, y_1$
  - $0 \leq y_0 \oplus y_1 < p\, 2^L$

Cryptographic Lotteries

- Lottery at relay *r*
  g_r: $\{0,1\}^{2L} \rightarrow \{0,1\}^{2L}$
  x wins if
  - $g_r(x) = y_0 \,||\, y_1$
  - $0 \leq y_0 \oplus y_1 < p\, 2^L$
- g_r defined from PRF f_r using a Luby-Rackoff-like construction
  - $y_0 = f_r(x_1) \oplus x_0$
  - $y_1 = f_r(y_0) \oplus x_1$
  - $g_r(x) = y_0 \,||\, y_1$

Cryptographic Lotteries

- Lottery at relay *r*
  g_r: $\{0,1\}^{2L} \rightarrow \{0,1\}^{2L}$
  x wins if
  - $g_r(x) = y_0 \,||\, y_1$
  - $0 \leq y_0 \oplus y_1 < p\, 2^L$
- g_r defined from PRF f_r using a Luby-Rackoff-like construction
  - $y_0 = f_r(x_1) \oplus x_0$
  - $y_1 = f_r(y_0) \oplus x_1$
  - $g_r(x) = y_0 \,||\, y_1$
- $f_r(x) = H(x(H(H(x)\ x_r^d)))$
  - H is a hash function
  - x_r is public; bank gives x_r^d to *r* during setup,
  - *d* is bank's private RSA key

Analysis

Efficiency

		LIRA	BRAIDS
Bank	Blind signatures/s	127.5+127.5f (256B/sig)	637.5 (488 B/sig)
Relay	Priority verification	6 hashes (18 us)	PBS verify (1500 us)
Normal Client	Tickets / connection	0	1

f is fraction of credit redeemed.
Entire network is transferring 1700 MiB/s.
Signature size: 1024 bits. Ticket size: 320 bits.
Linux OpenSSL benchmarks on Intel Core2 Duo 2.67 GHz

Anonymity

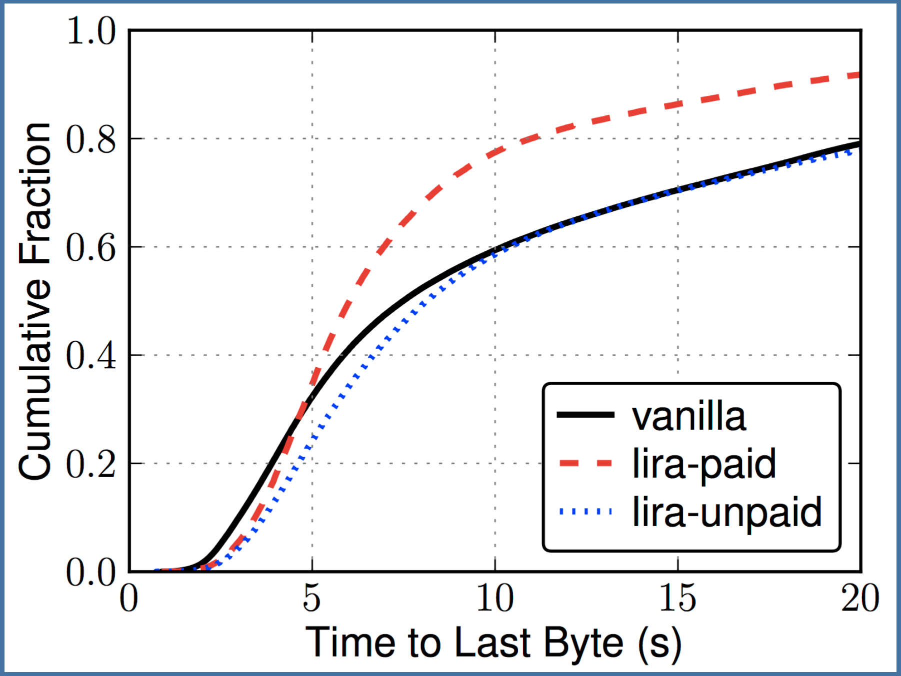
- With m buyers and n guessers, the probability that a prioritized circuit source is a given buyer is

$$1 / (m + np^3)$$

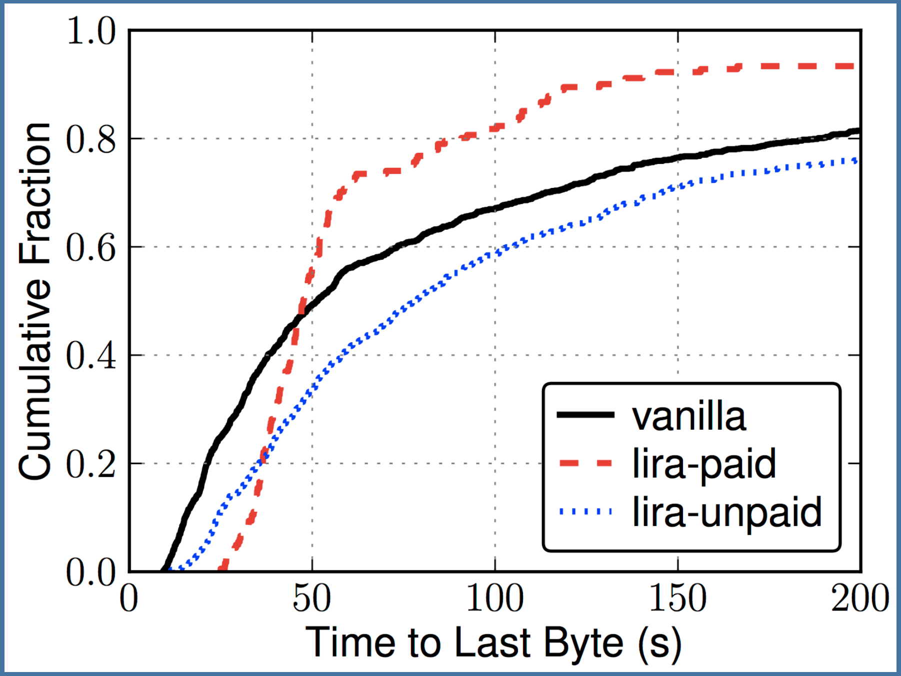
  compared to $1/(m+n)$ without priority.
- Linked priority degrades anonymity exponentially to $1/m$.

Performance

Web (320 KiB)

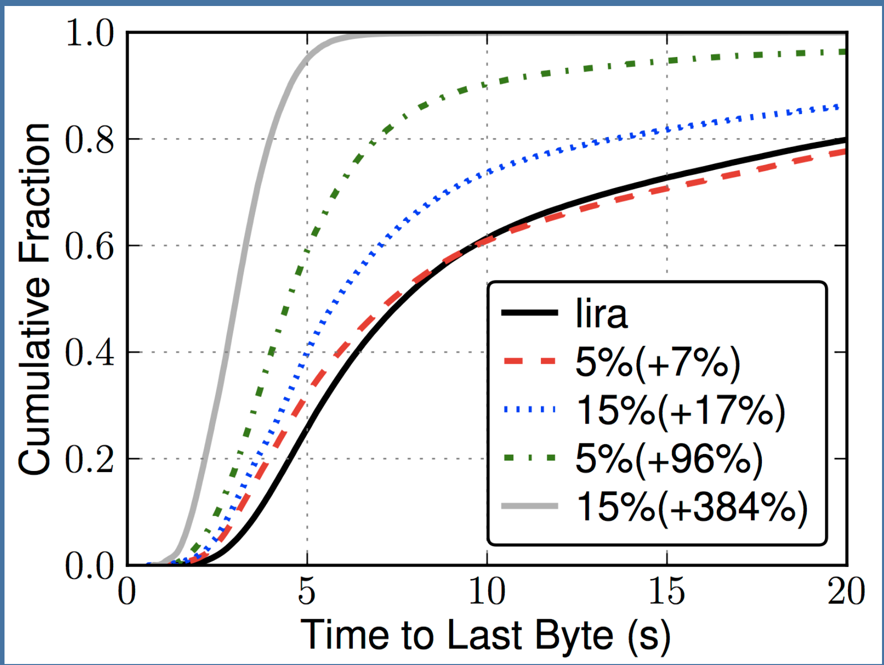


Bulk (5 MiB)

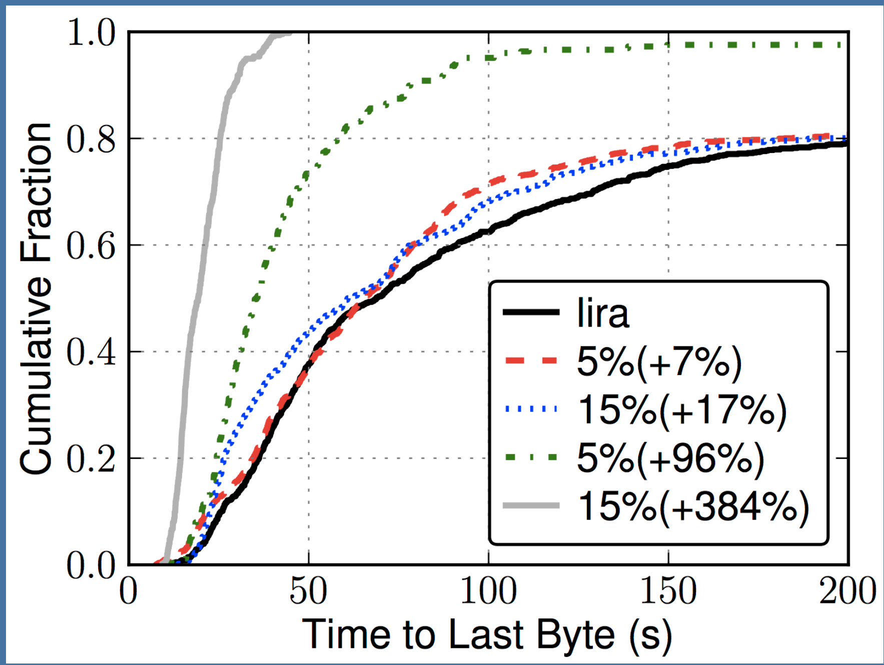


Performance, More Capacity

Web (320 KiB)



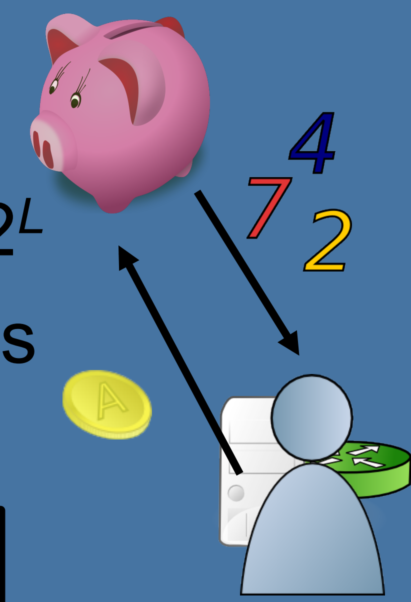
Bulk (5 MiB)



Conclusion

1. Volunteer-run Tor network is overloaded.
2. LIRA provides incentives to contribute by rewards with better network performance.
3. LIRA is more efficient than previous schemes while maintaining anonymity.
4. Full-network experiments demonstrate better performance and scalability.

Buying winning tickets



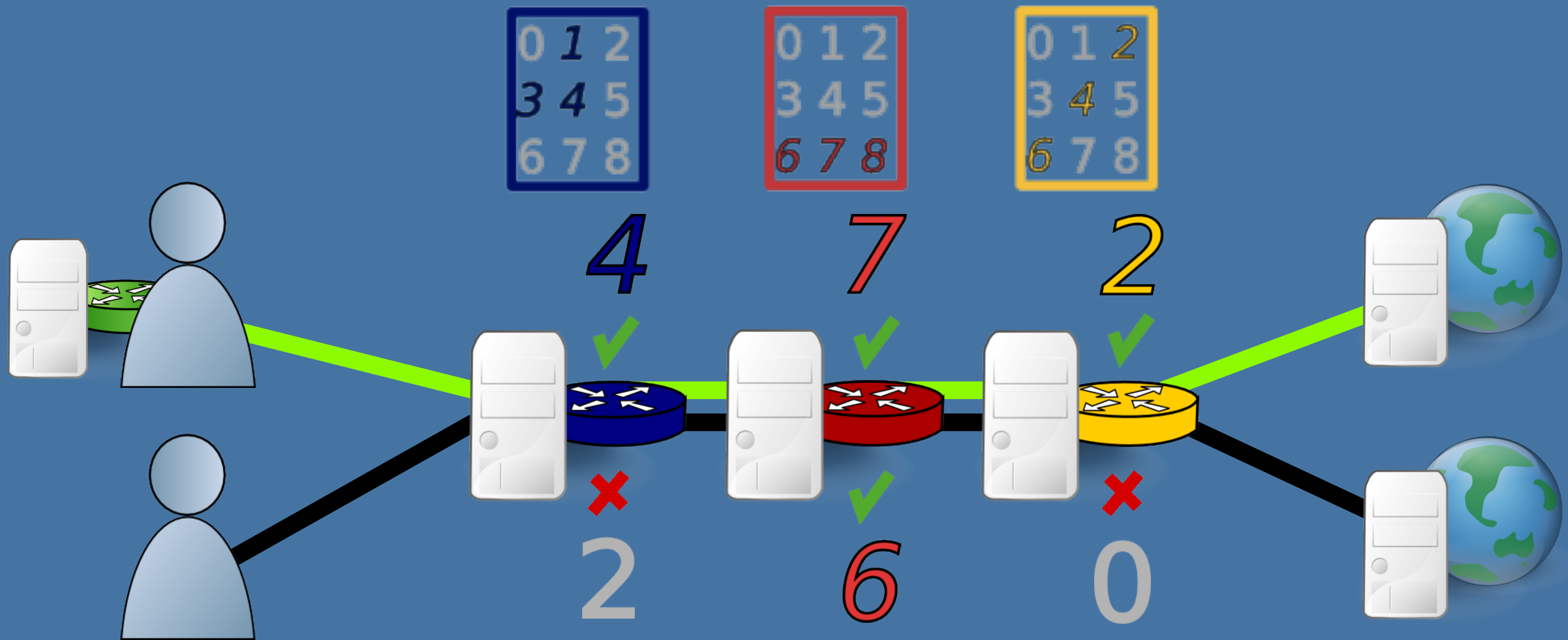
- Client chooses y_0, y_1, $0 \le y_0$ XOR $y_1 < p2^L$
- Using using PRF protocol, client reverses Luby-Rackoff process to get $g_r^{-1}(y_0 \,||\, y_1)$.

Client *c* and bank *B* evaluate $f_r(x)$

1. *C* sends $a^e x_r^d$ to B, *a* random.
2. *B* returns abx_r^d, *b* random.
3. *c* sends *b* $H(x)x_r^d$ to *B*.
4. *B* returns $H(H(x)x_r^d)$ to *c*.
5. *c* outputs $f_r(x) = H(x\, H(H(x)x_r^d))$.

PRF Protocol

Winning circuits are prioritized

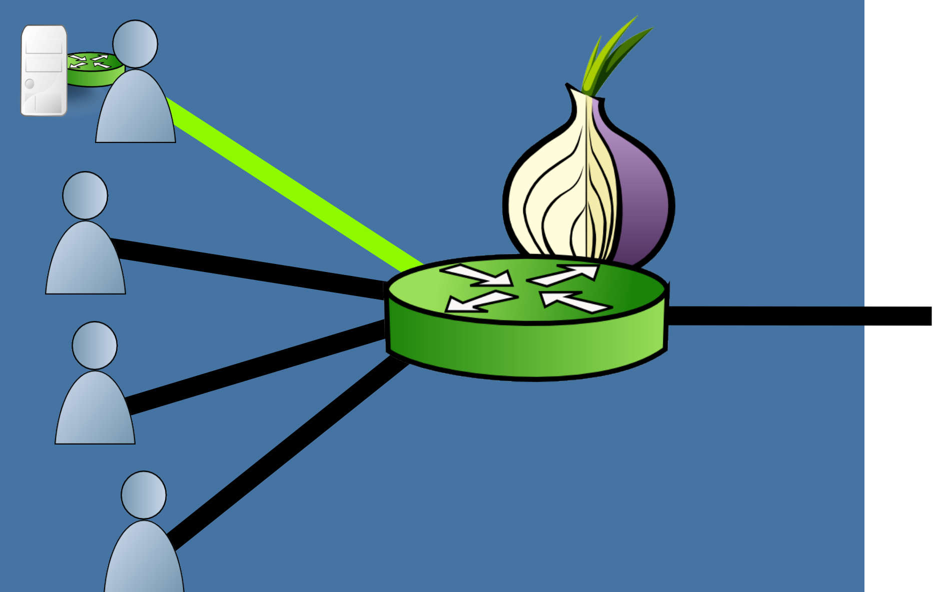


1. Client sends tickets to each relay in circuit.
2. Relays evaluate tickets. Winners must have unseen PRF inputs. Neighbors sent results.
3. If ticket wins and neighbors report wins, circuit is prioritized for next β bytes.

Priority Scheduling

- Proportional Differentiated Services
  - Split traffic into “paid” and “unpaid” classes
  - Prioritize classes using quality differentiation parameters p_i and quality measure Q (EWMA)

$$p_1/p_2 = Q_1(\Delta t) \,/\, Q_2(\Delta t)$$



Bank secrecy (honest-but-curious)

- Clients oblivious to x_r^d.
- B cannot produce *r*, input *x*, or output $f_r(x)$.
- Relay purchases are batched, preventing bank from knowing when prioritized circuits are constructed.

c and *B* evaluate $f_r(x)$

1. *c* obtains bx_r^d.
2. *c* sends *b* $H(x)x_r^d$ to *B*.
3. *B* sends $H(H(x)x_r^d)$ to *c*.
4. *c* outputs $H(x(H(H(x)x_r^d)))$.

PRF Protocol

Creating winning tickets

- f_r is random in ROM when x_r^d unknown.
- y_0 XOR y_1 is random. for y_0 or y_1 unknown
- One-time-use inputs to f_r prevent double spending.
- Tickets not fully purchased win with probability p.

$$f_r(x) = \mathrm{H}(x(\mathrm{H}(\mathrm{H}(x)\ x_r^d)))$$

$$y_0 = f_r(x_1) \oplus x_0$$
$$y_1 = f_r(y_0) \oplus x_1$$
$$g_r(x) = y_0 \mid\mid y_1$$

$$0 \leq y_0 \oplus y_1 < p\ 2^L$$

Cryptographic Lottery