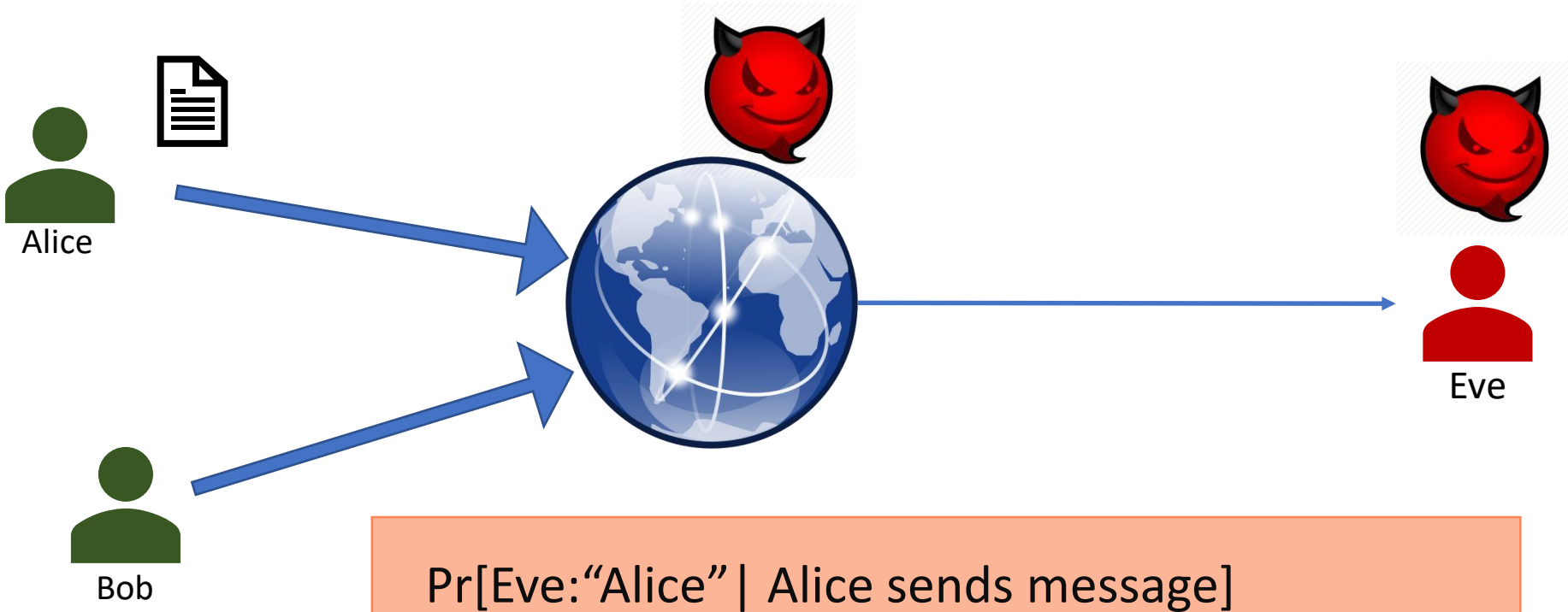
Not all is lost for anonymity – but quite a lot is.

Coordination among users can help with anonymity.

Debajyoti Das[1] Sebastian Meiser[2] Esfandiar Mohammadi[3] Aniket Kate[1]

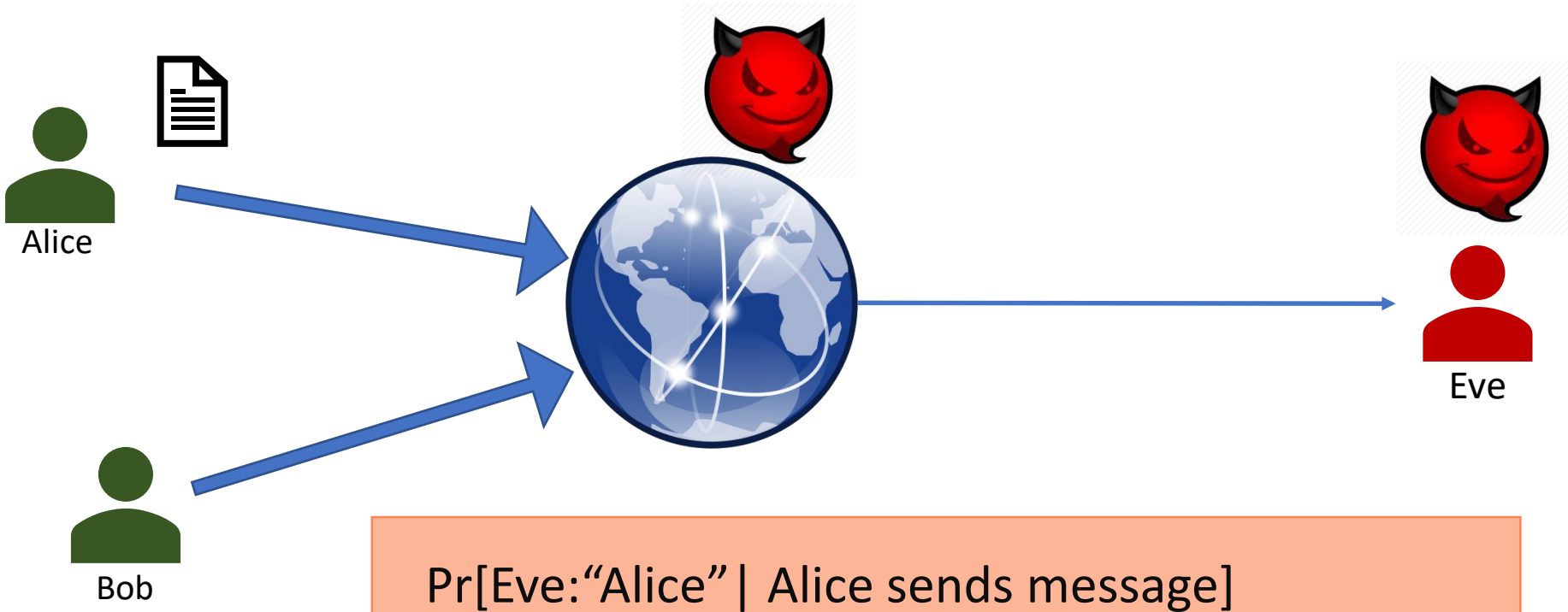
[1]Purdue University [2]Visa Research [3]ETH Zurich

Sender Anonymity (AnoA definition)



$$\Pr[\text{Eve:“Alice”} \mid \text{Alice sends message}] \leq \Pr[\text{Eve:“Alice”} \mid \text{Bob sends message}] + \delta(\eta)$$

Sender Anonymity (AnoA definition)

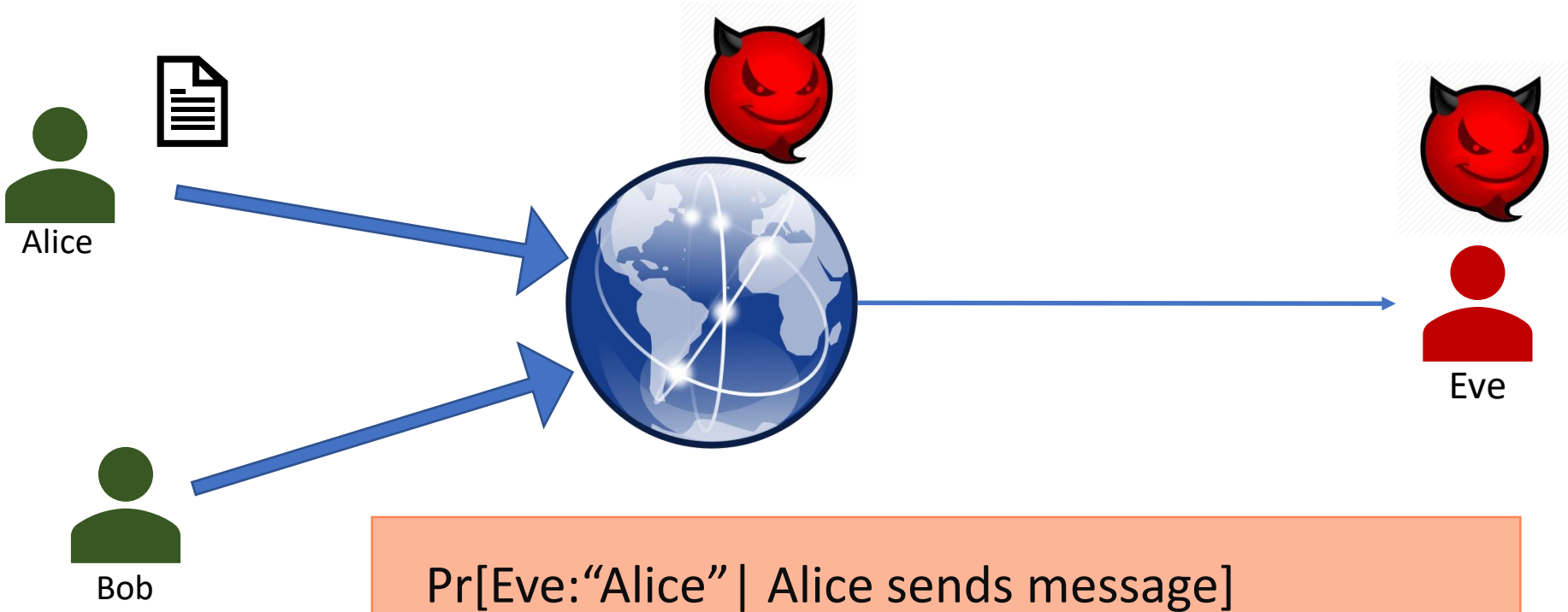


$$\Pr[\text{Eve:“Alice”} \mid \text{Alice sends message}] \leq \Pr[\text{Eve:“Alice”} \mid \text{Bob sends message}] + \delta(\eta)$$

strong: $\delta(\eta) \leq \text{negl}(\eta)$

strong

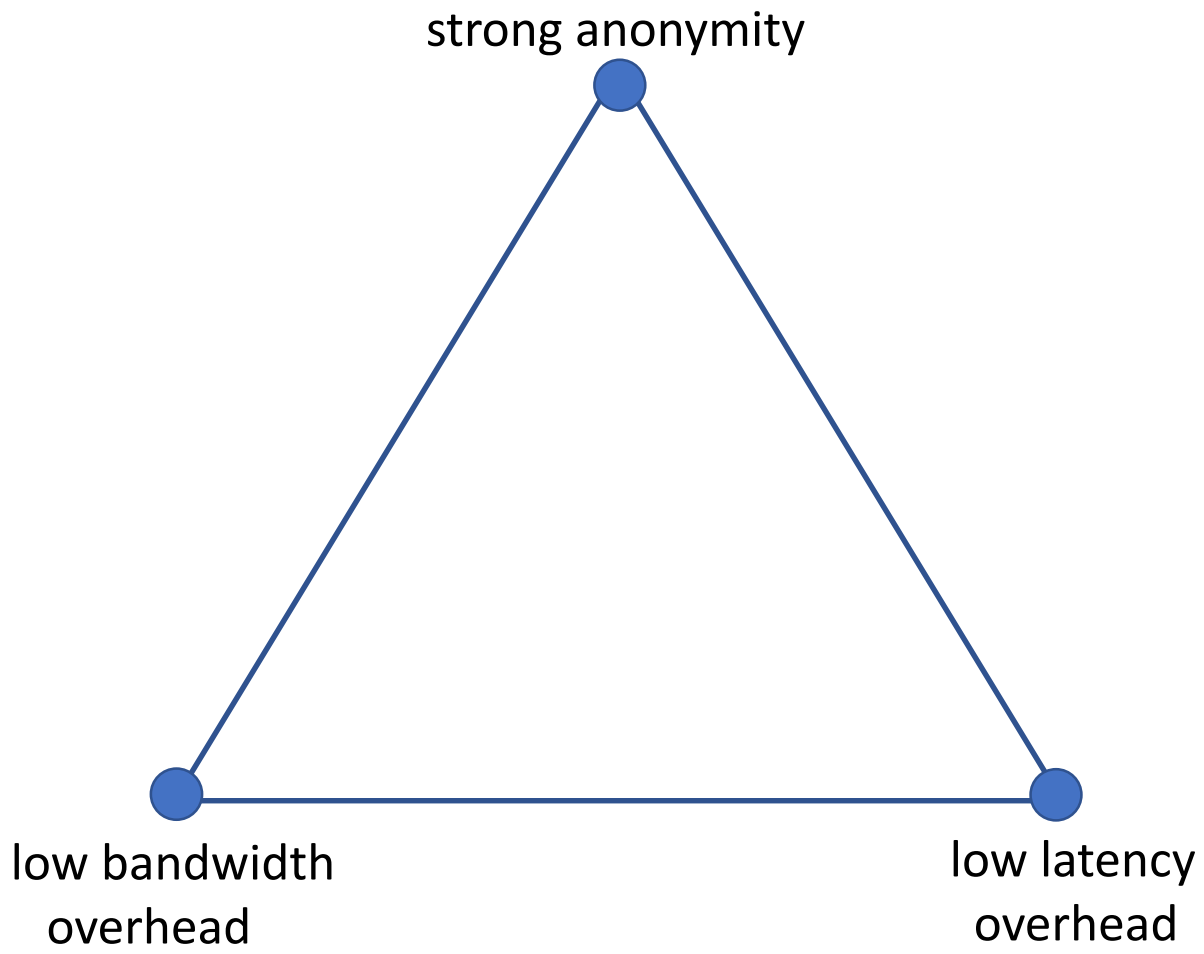
Sender Anonymity (AnoA definition)



$$\Pr[\text{Eve:“Alice”} \mid \text{Alice sends message}] \leq \Pr[\text{Eve:“Alice”} \mid \text{Bob sends message}] + \delta(\eta)$$

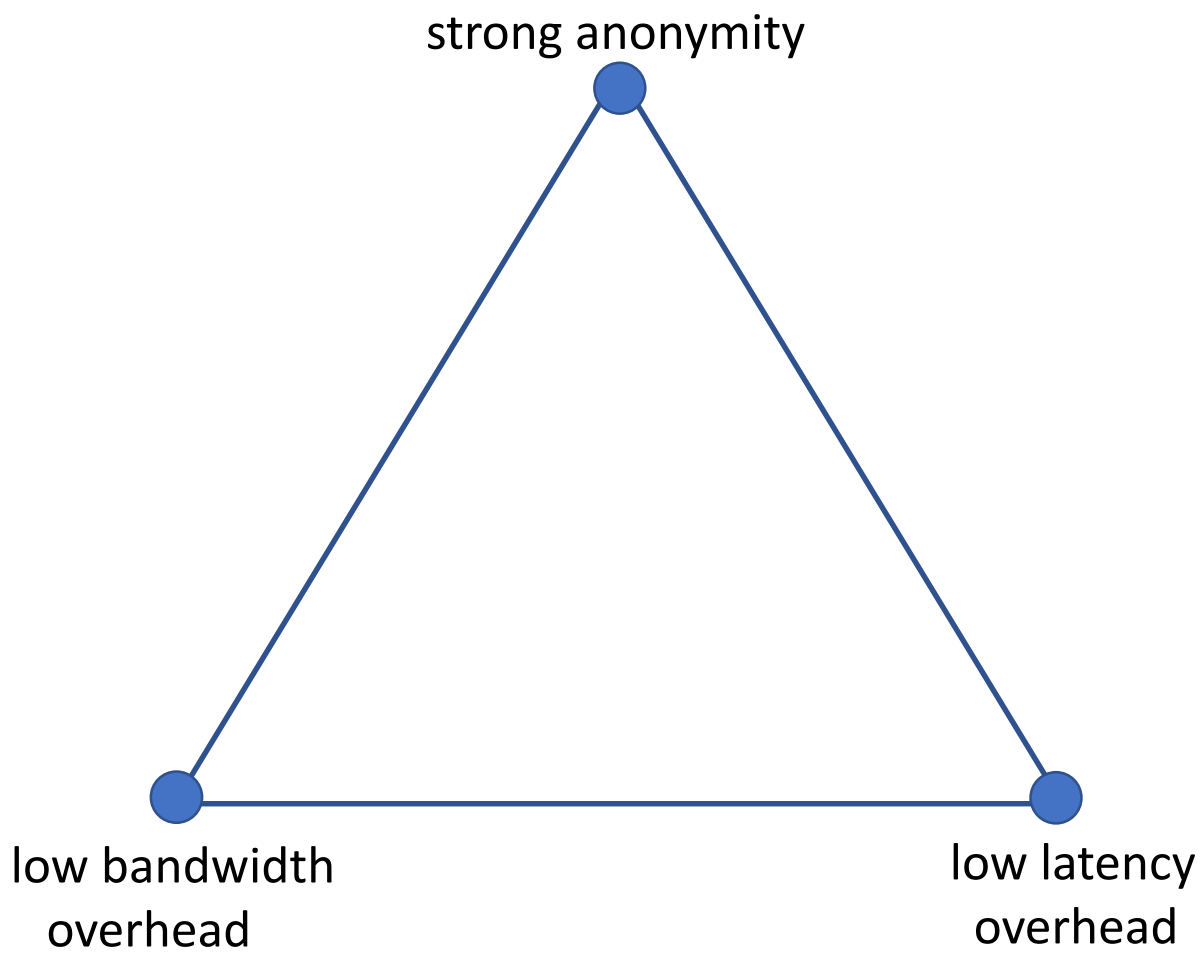
strong: $\delta(\eta) \leq \text{negl}(\eta)$

Anonymity Trilemma



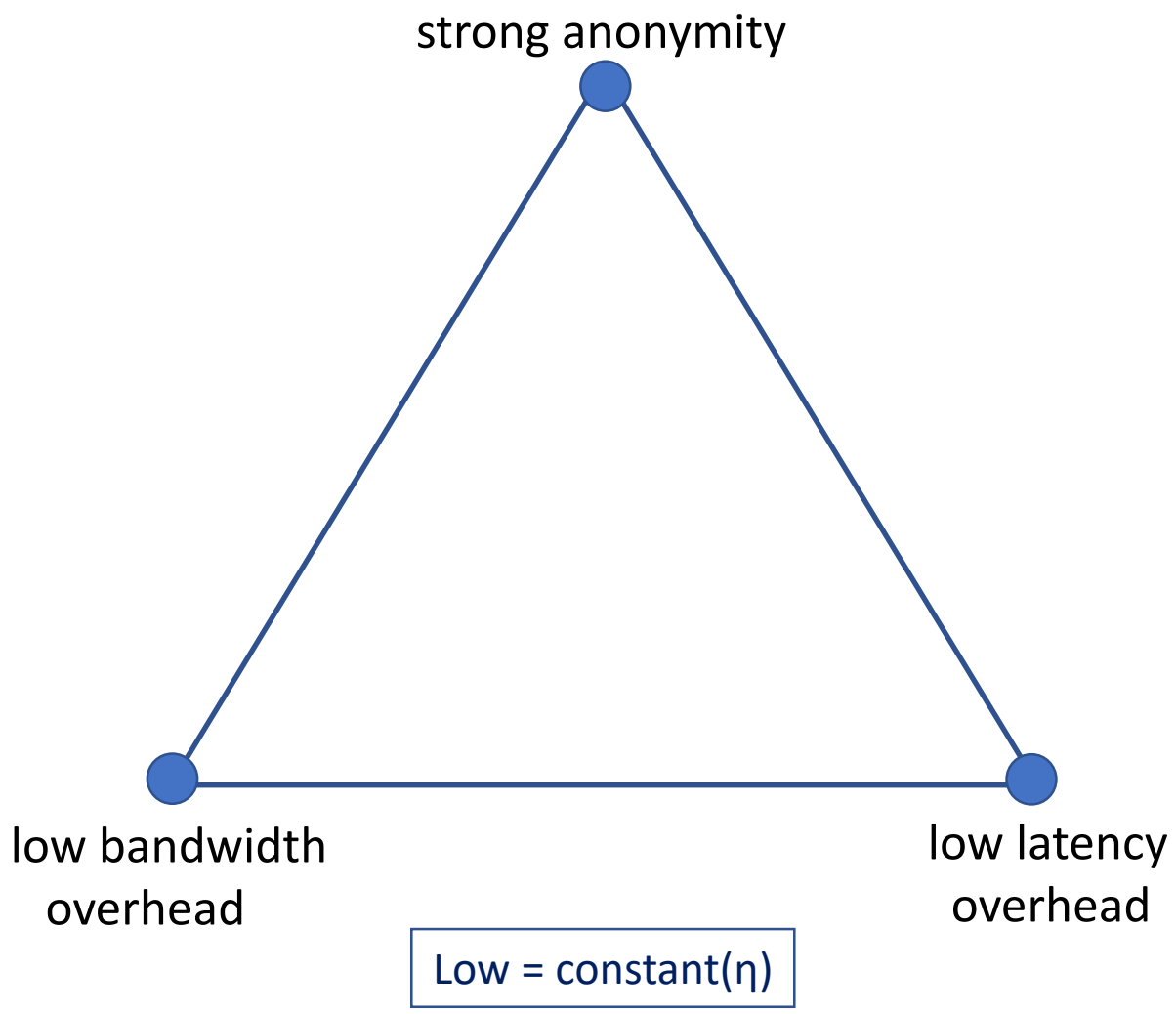
- Q1: Can we achieve strong anonymity without introducing large latency or bandwidth overhead?

Anonymity Trilemma



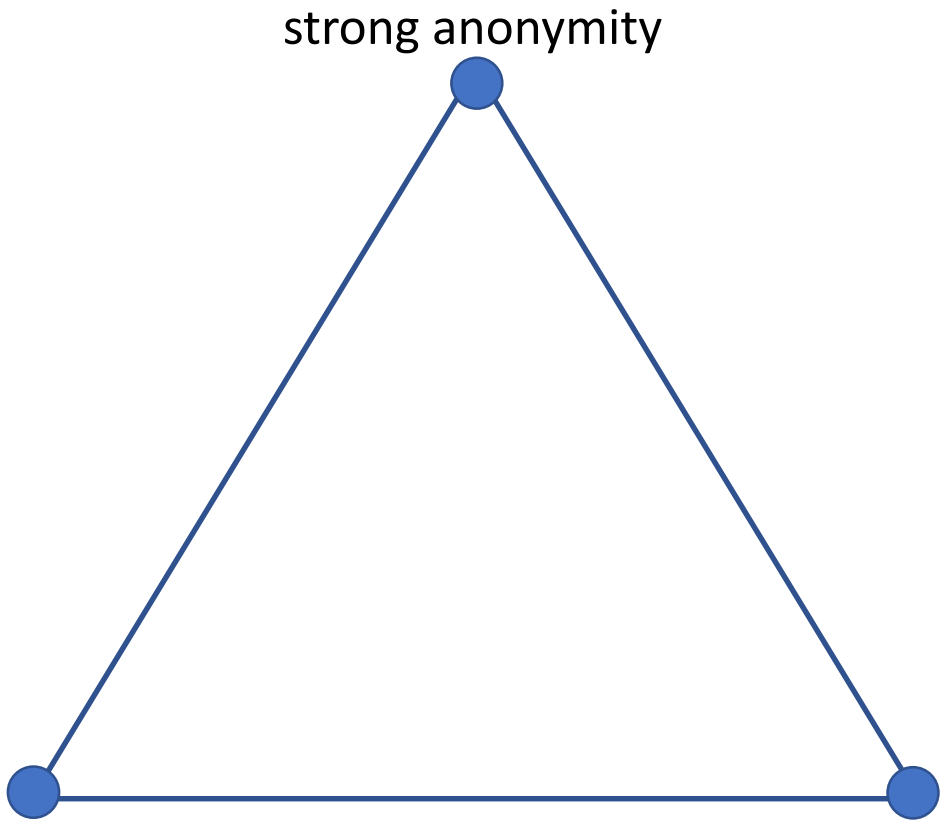
- Q1: Can we achieve strong anonymity without introducing large latency or bandwidth overhead?
  - **NO.**

Anonymity Trilemma



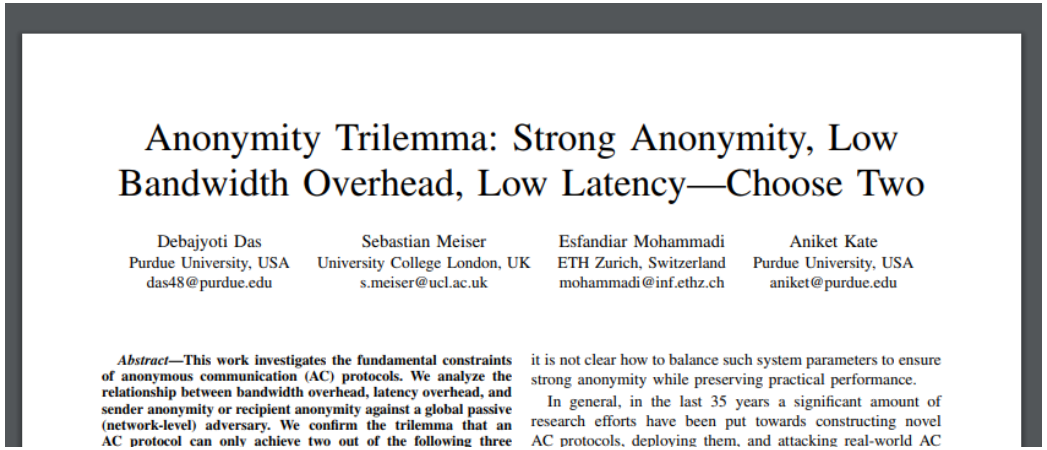
- Q1: Can we achieve strong anonymity without introducing large latency or bandwidth overhead?
  - **NO.**

Anonymity Trilemma



Low = constant(η)

- Q1: Can we achieve strong anonymity without introducing large latency or bandwidth overhead?
  - **NO.**



Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two

Debajyoti Das, Purdue University, USA, das48@purdue.edu
Sebastian Meiser, University College London, UK, s.meiser@ucl.ac.uk
Esfandiar Mohammadi, ETH Zurich, Switzerland, mohammadi@inf.ethz.ch
Aniket Kate, Purdue University, USA, aniket@purdue.edu

***Abstract*—This work investigates the fundamental constraints of anonymous communication (AC) protocols. We analyze the relationship between bandwidth overhead, latency overhead, and sender anonymity or recipient anonymity against a global passive (network-level) adversary. We confirm the trilemma that an AC protocol can only achieve two out of the following three**

it is not clear how to balance such system parameters to ensure strong anonymity while preserving practical performance.

In general, in the last 35 years a significant amount of research efforts have been put towards constructing novel AC protocols, deploying them, and attacking real-world AC

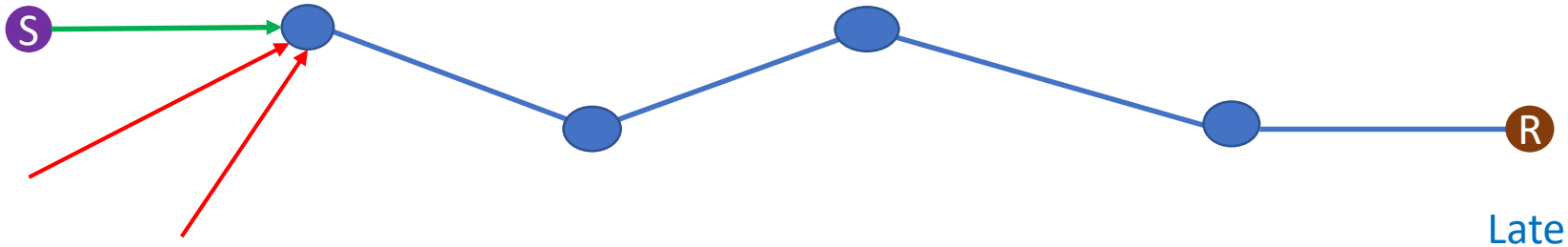
IEEE S&P 2018

Outline

- Prior Results on Anonymity Trilemma
- How coordination among users can help anonymity
- New impossibility results for anonymity
- Future direction of anonymity communication protocols

Bandwidth Overhead and Latency Overhead

- We consider one *communication round* as one time unit.
- Latency overhead ℓ is the number of rounds a message can be delayed by the protocol before being delivered.



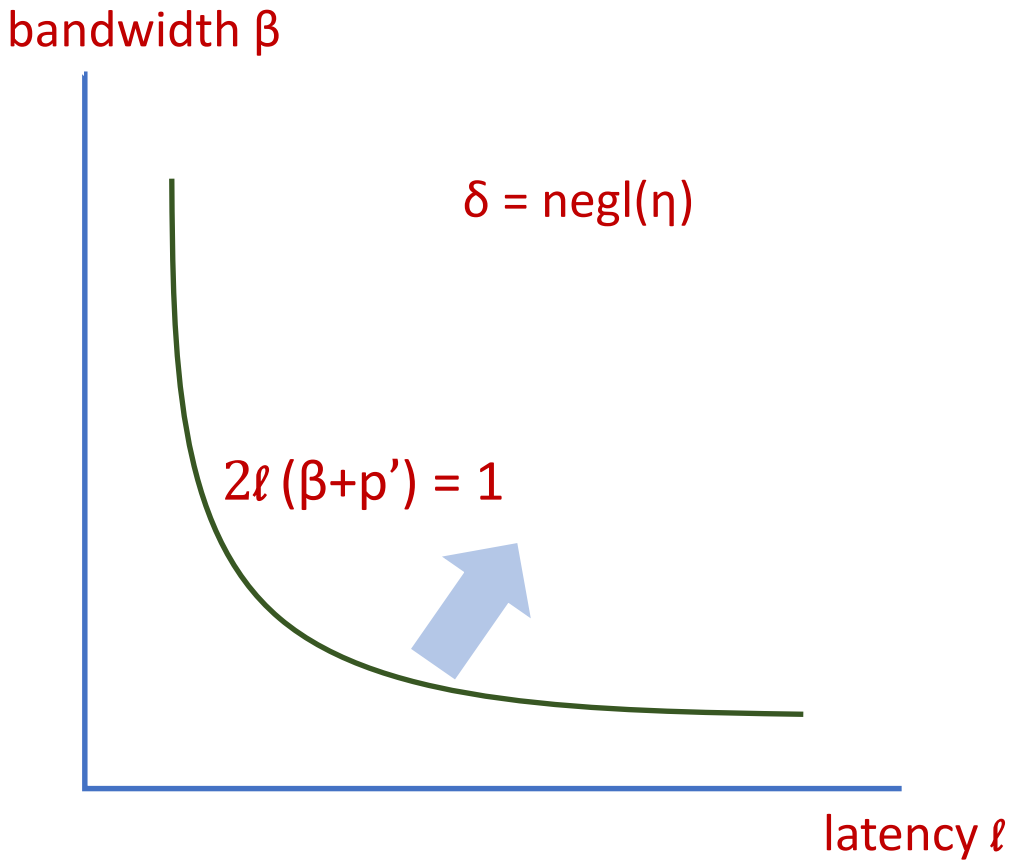
Latency overhead $\ell = 4$
Bandwidth overhead $\beta = 2$

- Bandwidth overhead β is the number of noise messages per user per round, i.e., the dummy message rate.

Prior Results for mix-nets (including onion routing)

- When users send messages at a rate of p' per user per round, To achieve strong anonymity:

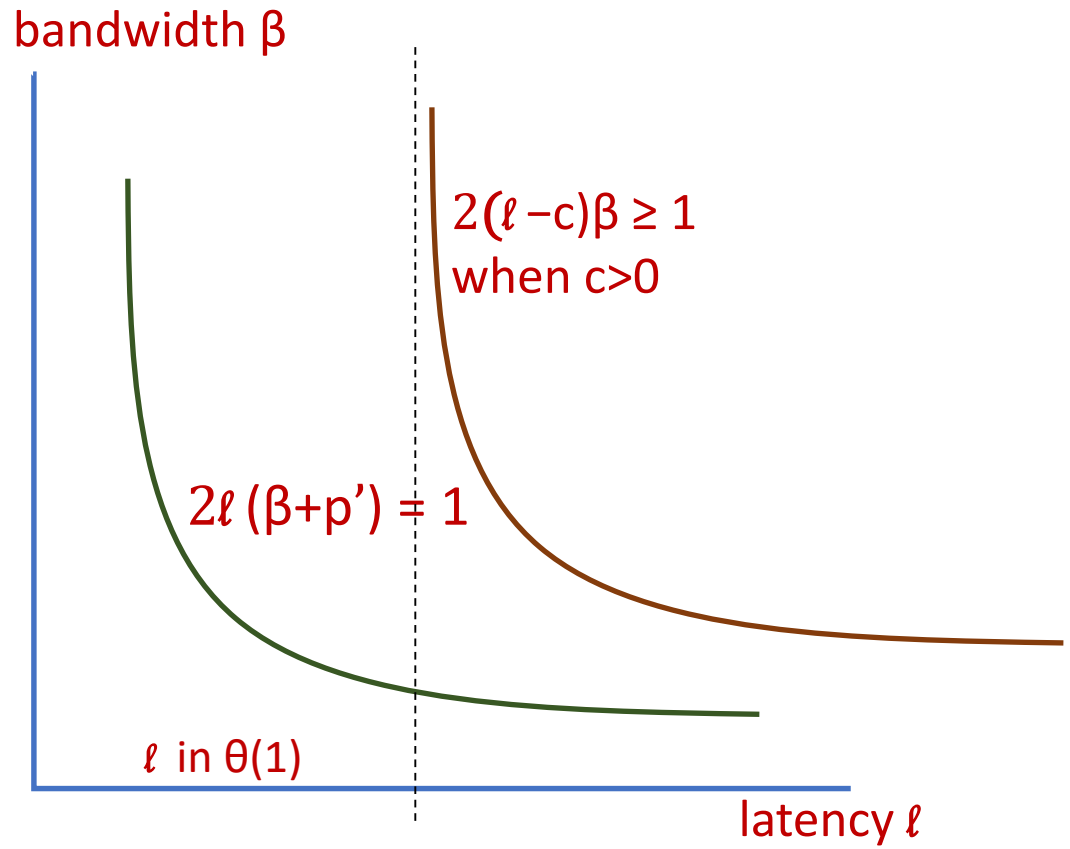
$$2\ell\,(\beta+p') \geq 1$$



When Adversary can compromise c protocol parties

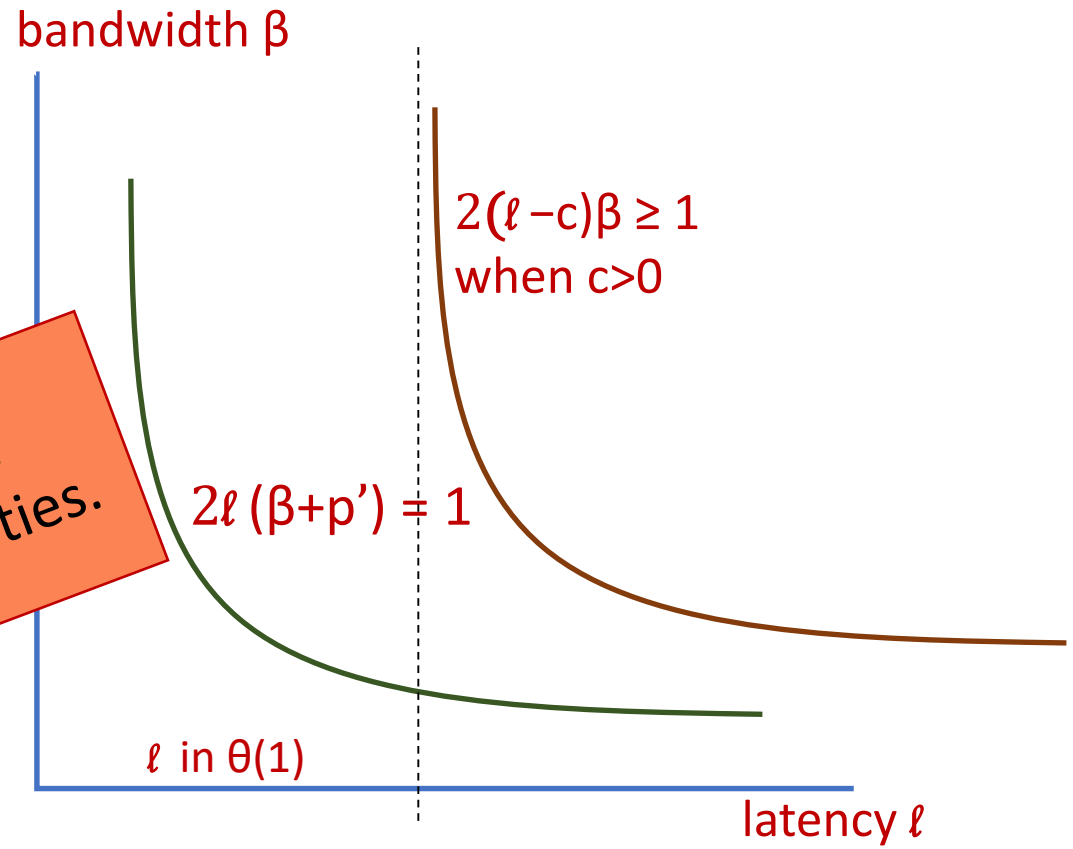
- to achieve strong anonymity:

- $\ell > \theta(1)$
- $2(\ell - c)\beta \geq 1$, when $\ell > c$.



When Adversary can compromise c protocol parties

- to achieve strong anonymity:
  - $\ell > \theta(1)$
  - $2(\ell - c)\beta \geq 1$, when



No strong anonymity with constant latency, in the presence of compromised protocol parties.

Is it impossible to achieve strong anonymity with constant latency overhead, when **c>0** ?

Is it impossible to achieve strong anonymity with constant latency overhead, when **c>0** ?

- NO.
- Example: DC-net with **user coordination**.

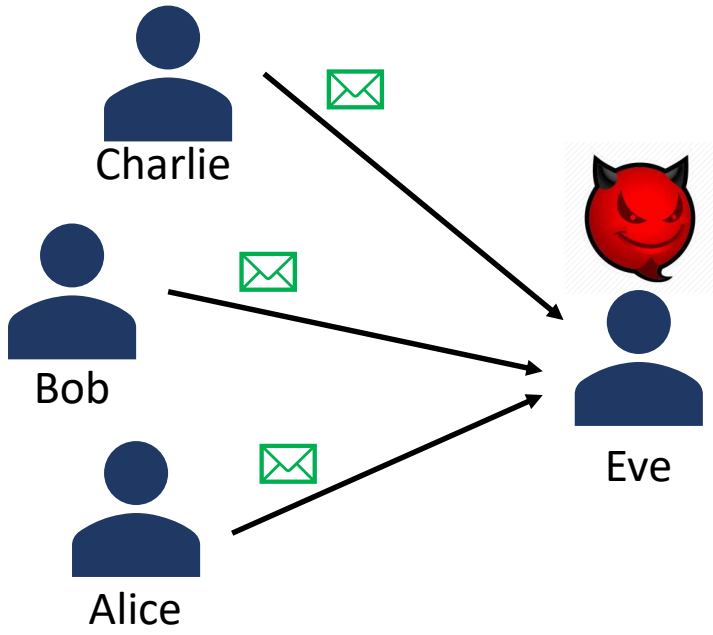
Is it impossible to achieve strong anonymity with constant latency overhead, when **c>0** ?

- NO.
- Example: DC-net with **user coordination**.

Our earlier protocol model did not assume any out-of-band user coordination.

DC-net type protocols – user coordination

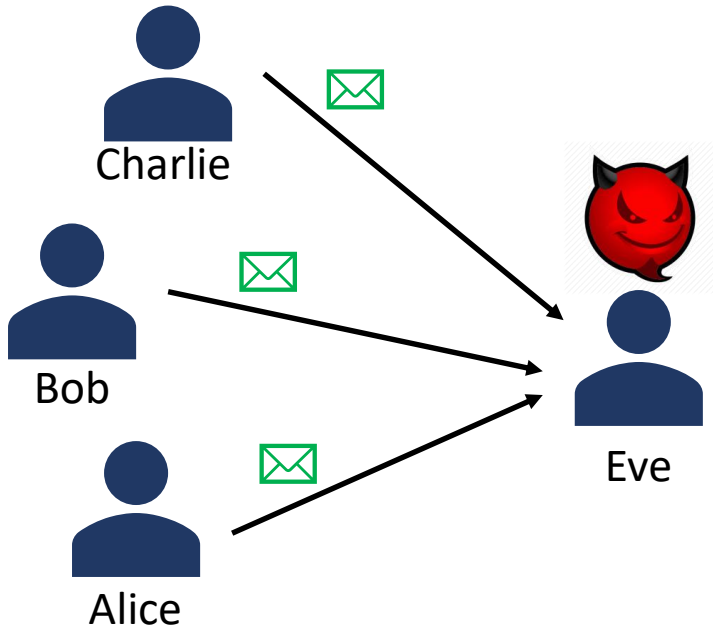
- Eve cannot point to a single packet to say the real message is only inside this packet.
- Another naïve way is to secret share the real message among several parties.
- Can provide strong anonymity even with constant latency.



Eve can retrieves the actual message only after combining all three packets.

DC-net type protocols – user coordination

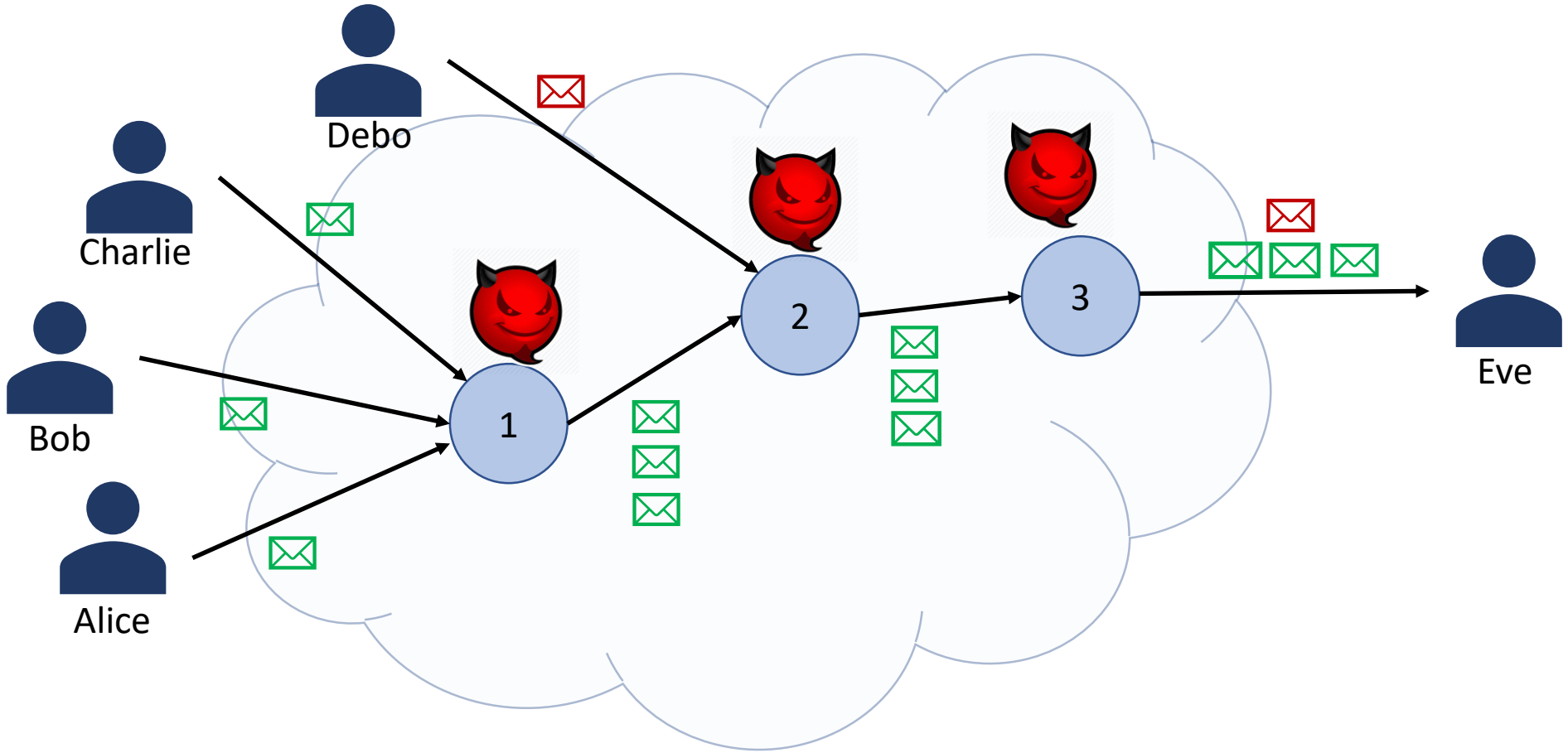
- Eve cannot point to a single packet to say the real message is only inside this packet.
- Another naïve way is to secret share the real message among several parties.
- Can provide strong anonymity even with constant latency.



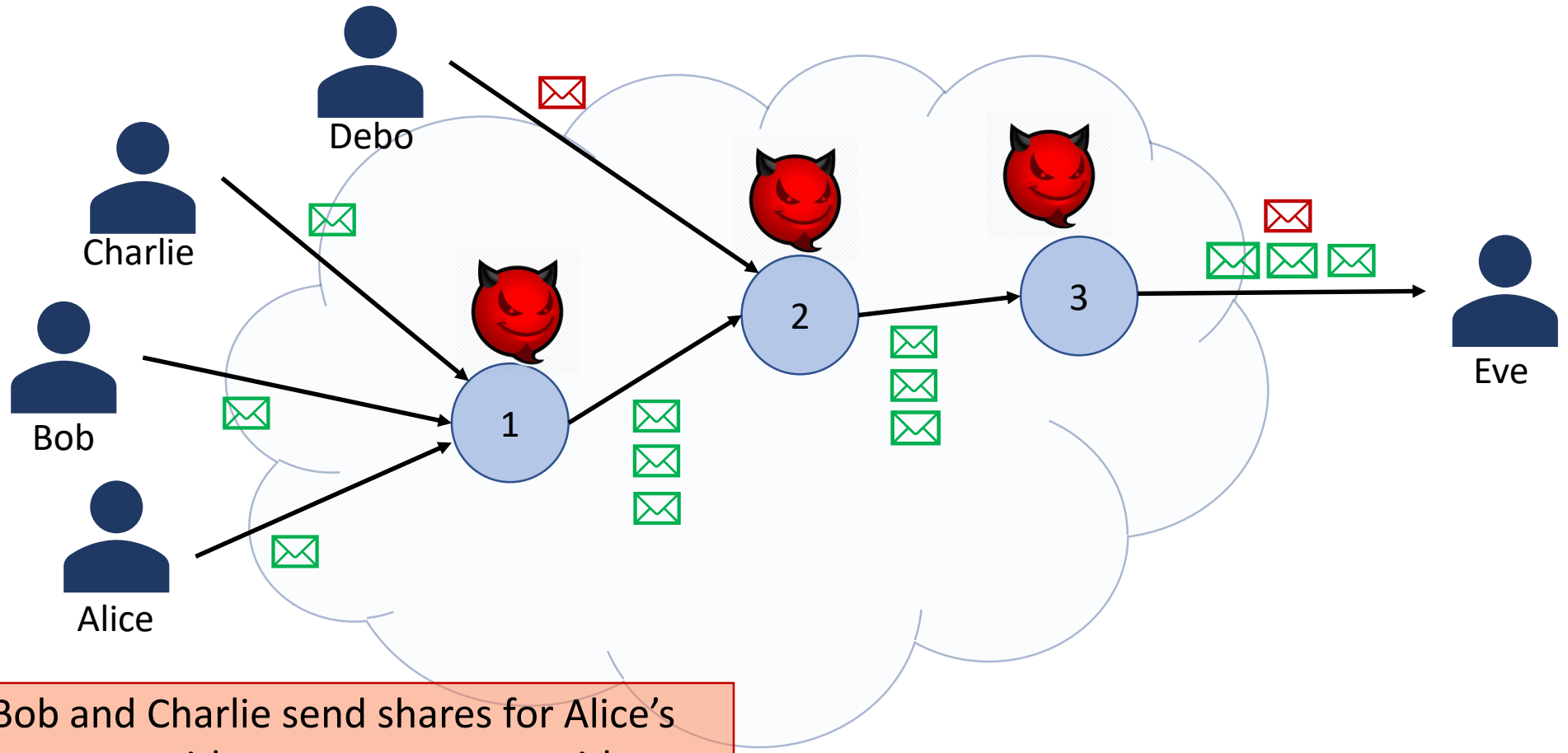
Eve can retrieves the actual message only after combining all three packets.

Issue: these protocols use very high bandwidth overhead. The overhead (number of dummy messages) per real message, B > (N-1), N = total users.

Protocols beyond mix-nets –hybrid protocols

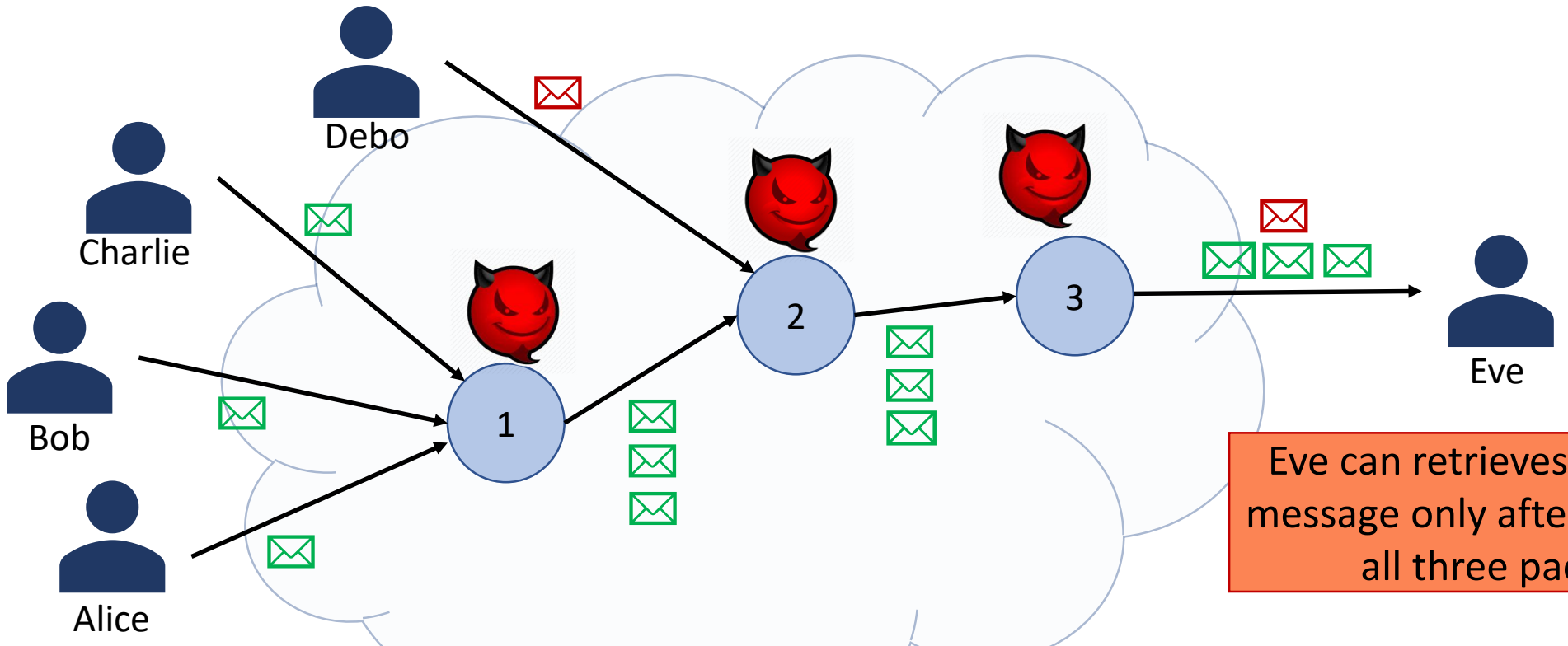


Protocols beyond mix-nets –hybrid protocols



Bob and Charlie send shares for Alice's message, with some pre-setup, without Alice communicating to them.

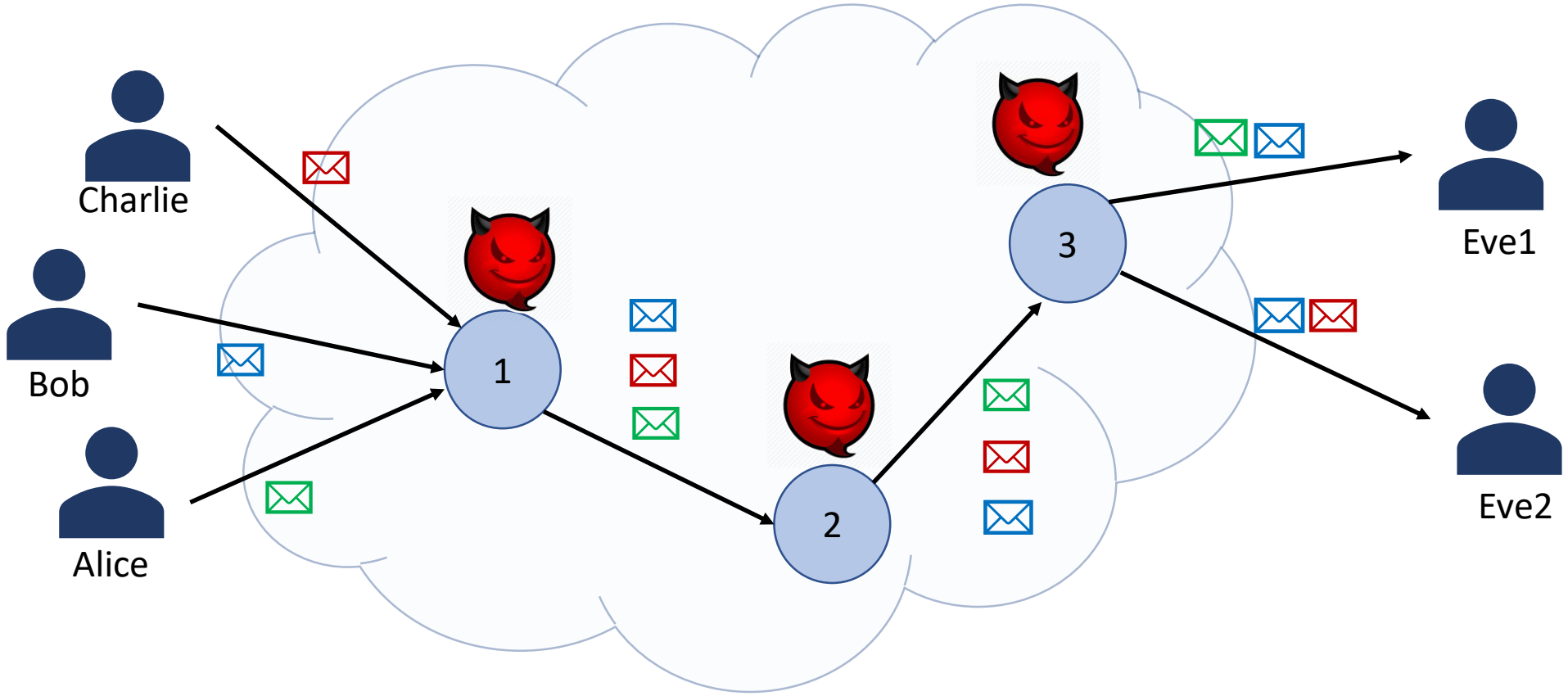
Protocols beyond mix-nets –hybrid protocols



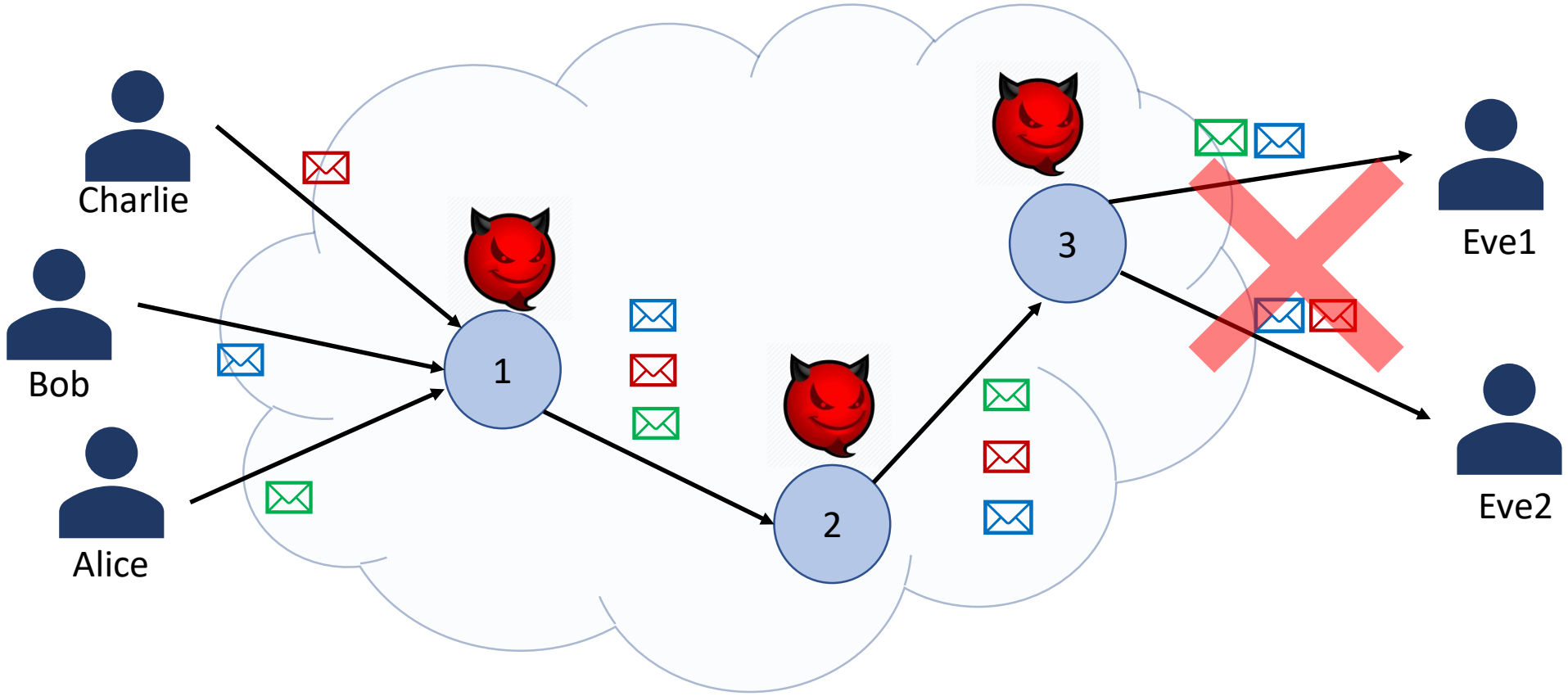
Eve can retrieves the actual message only after combining all three packets.

Bob and Charlie send shares for Alice's message, with some pre-setup, without Alice communicating to them.

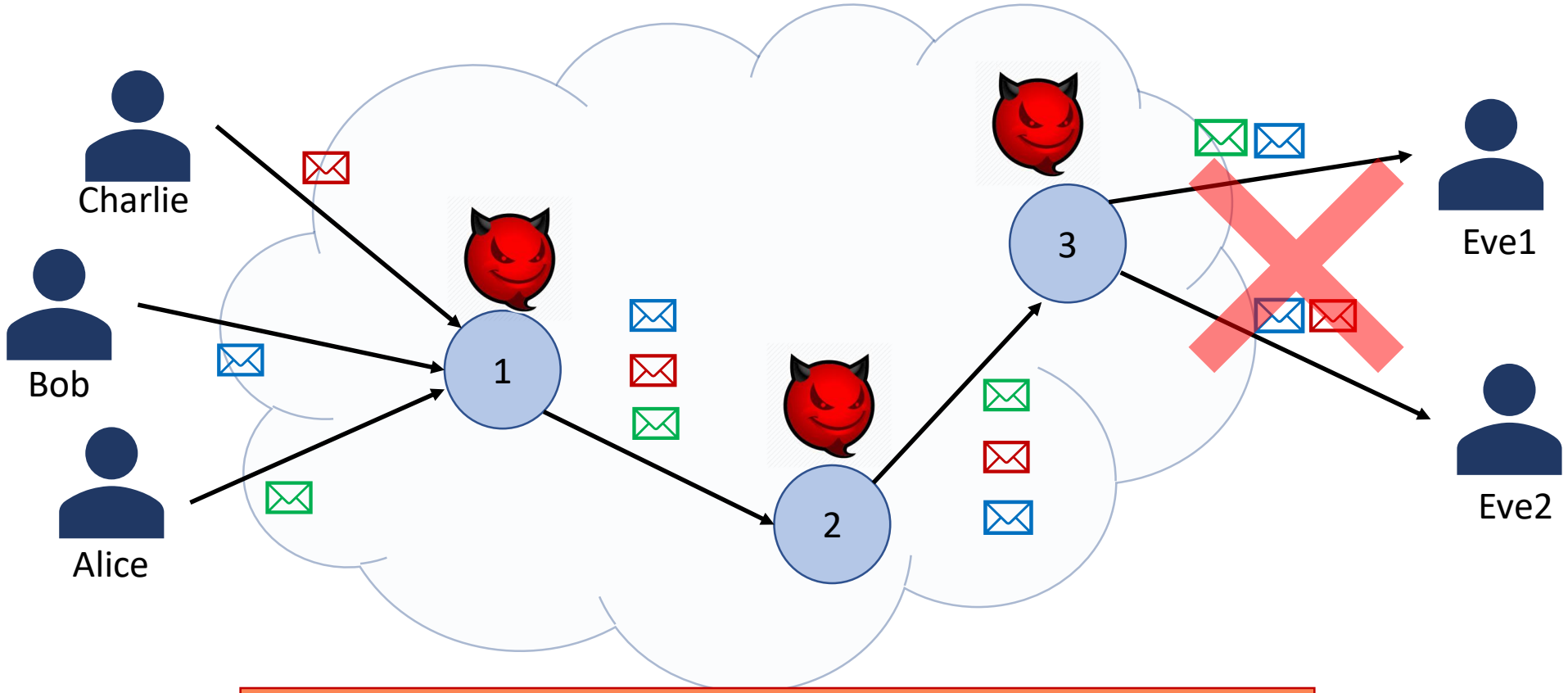
Assumptions on the protocols



Assumptions on the protocols

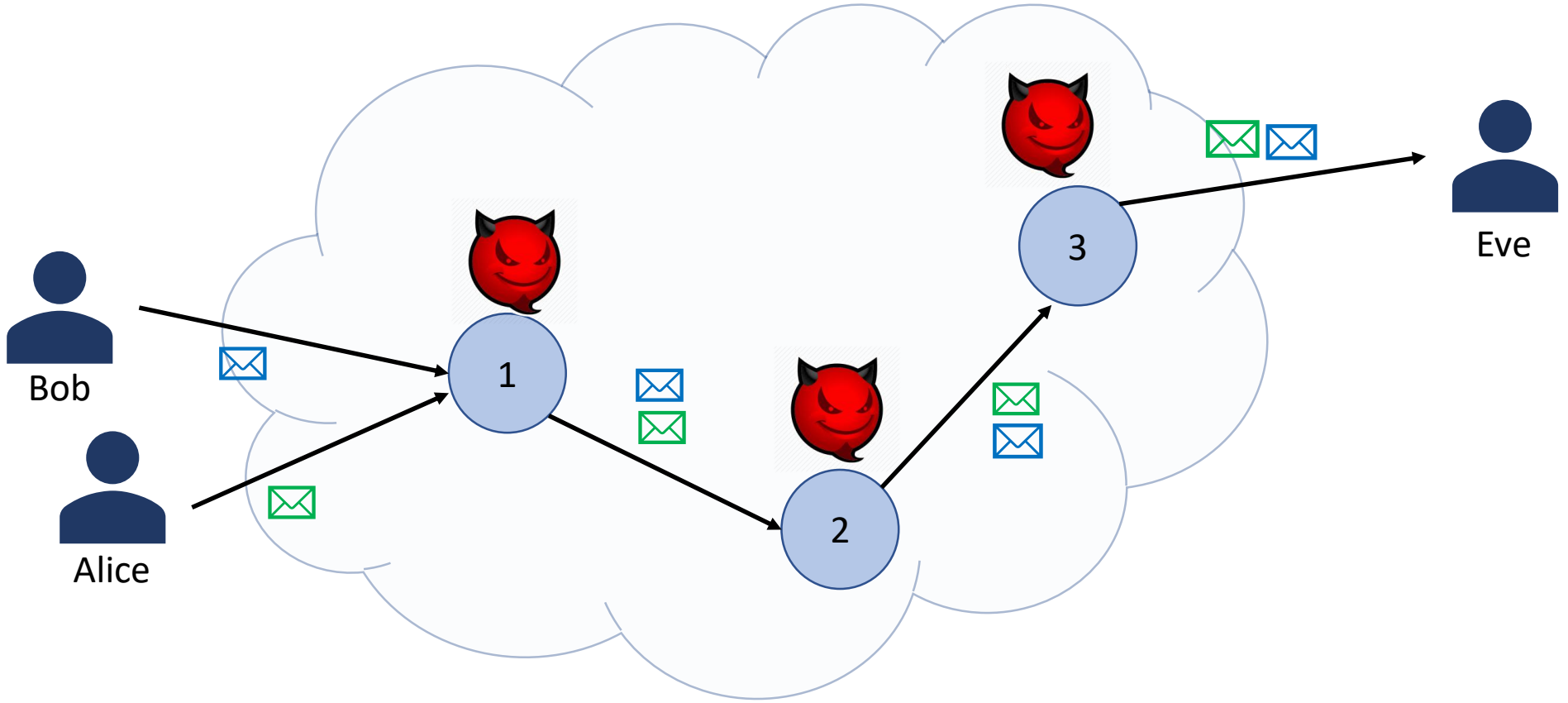


Assumptions on the protocols

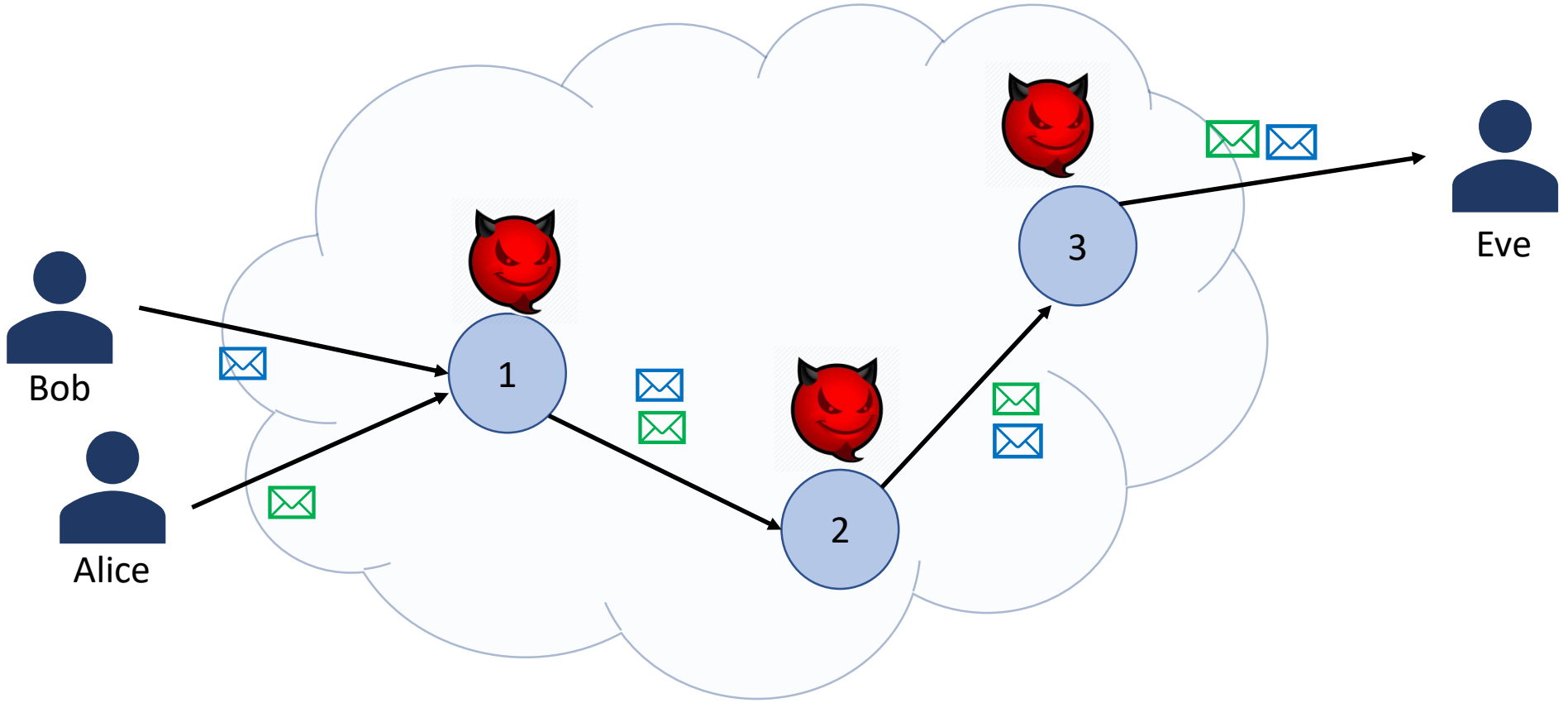


Assumption 1: One packet does not take part in the reconstruction of two separate messages.

Assumptions on the protocols

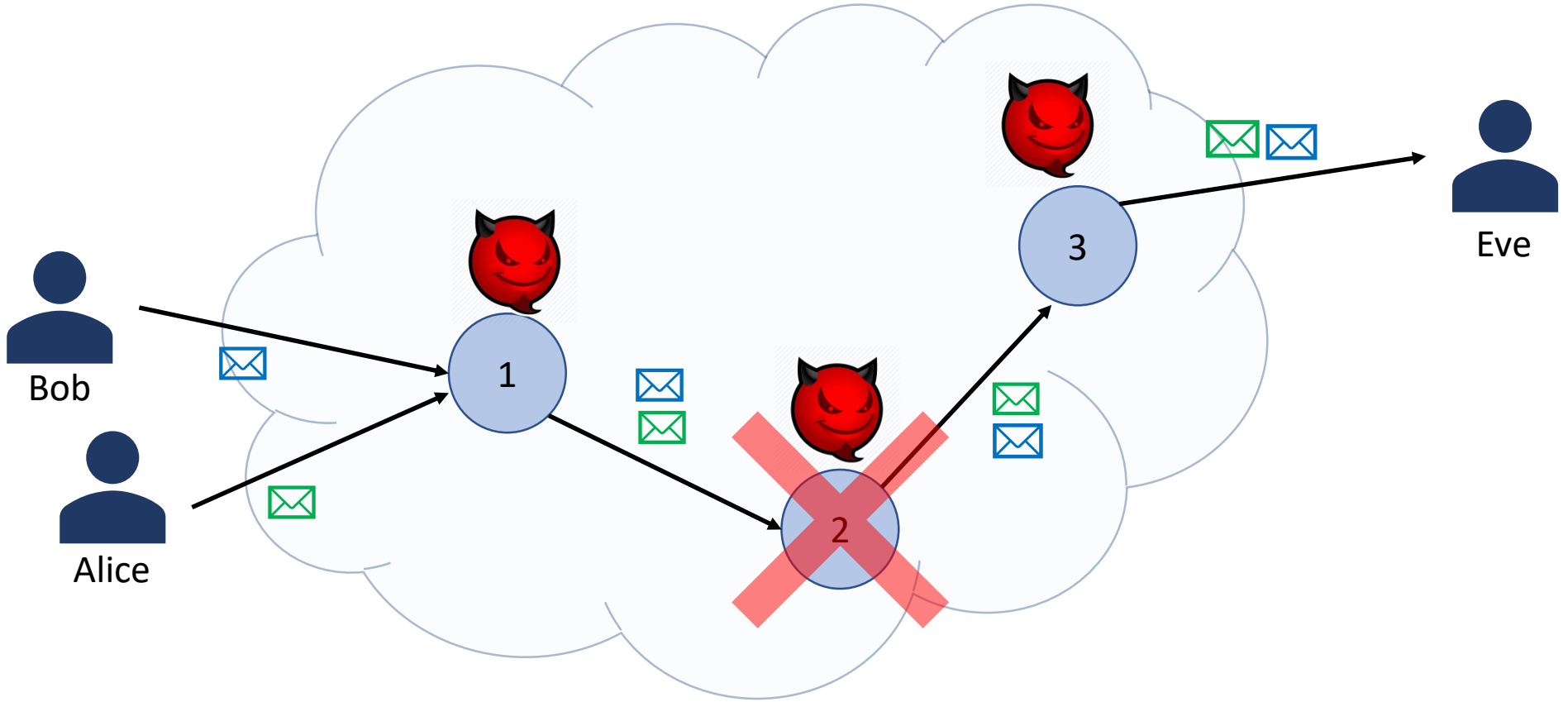


Assumptions on the protocols



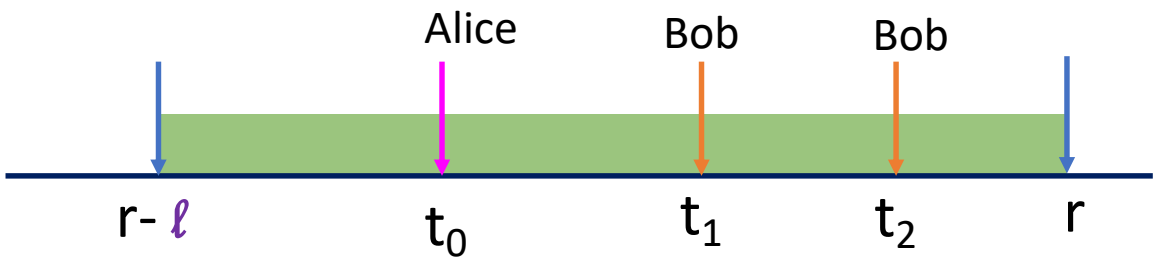
Assumption 2: Oblivious swapping is not possible.

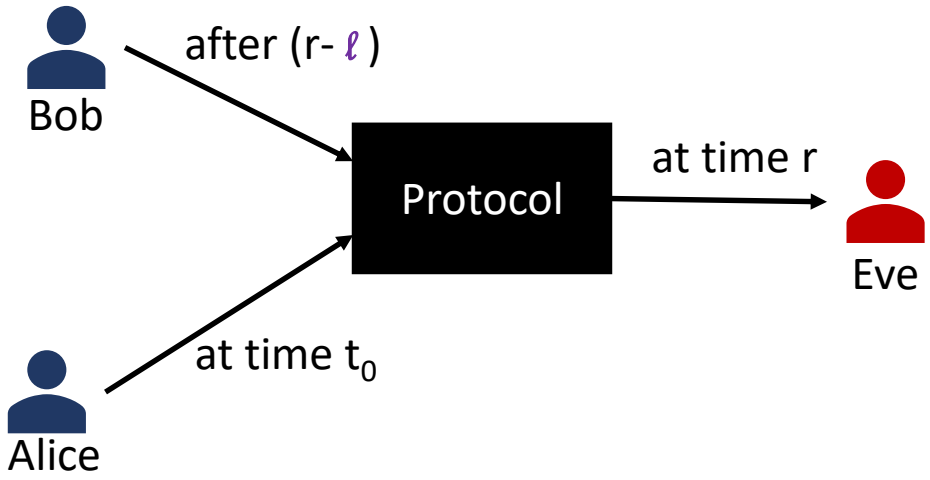
Assumptions on the protocols



Assumption 2: Oblivious swapping is not possible.

Necessary Invariant for Anonymity

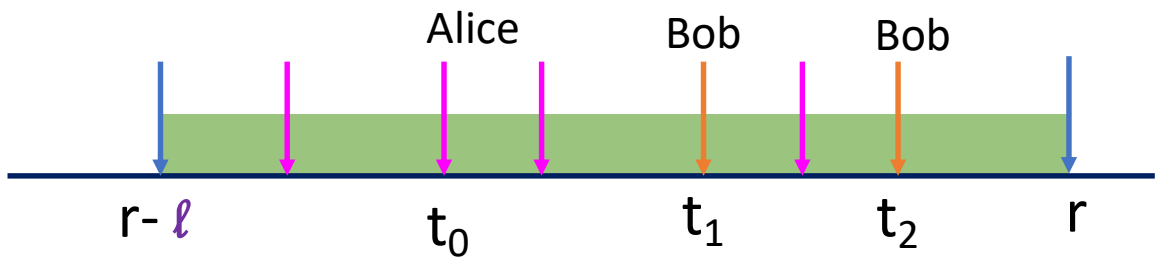


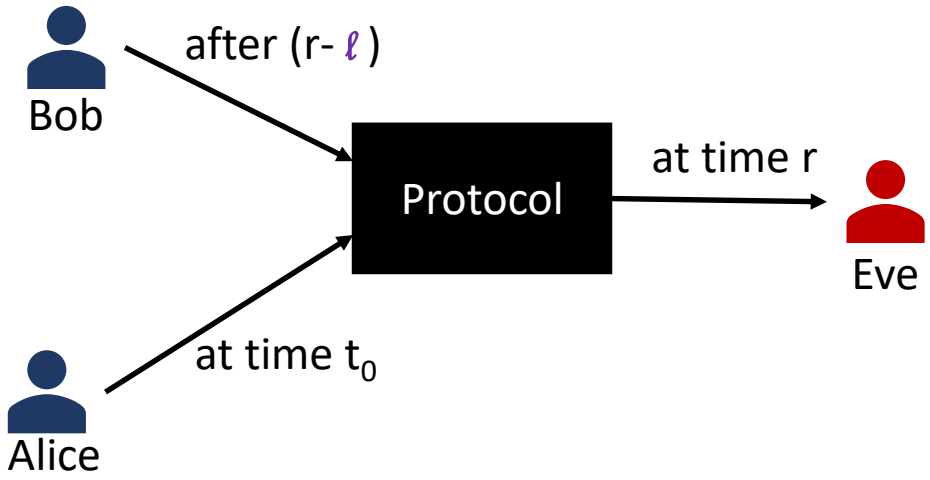


For anonymity we need:

- Bob sends at least one message within the time slice [r- ℓ , r).

Necessary Invariant for Anonymity

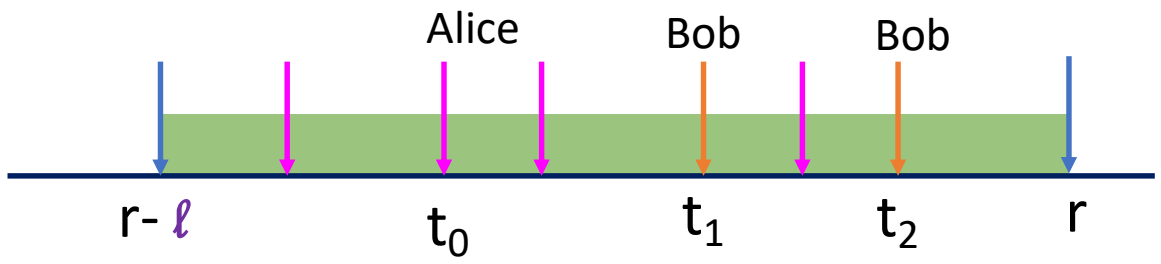


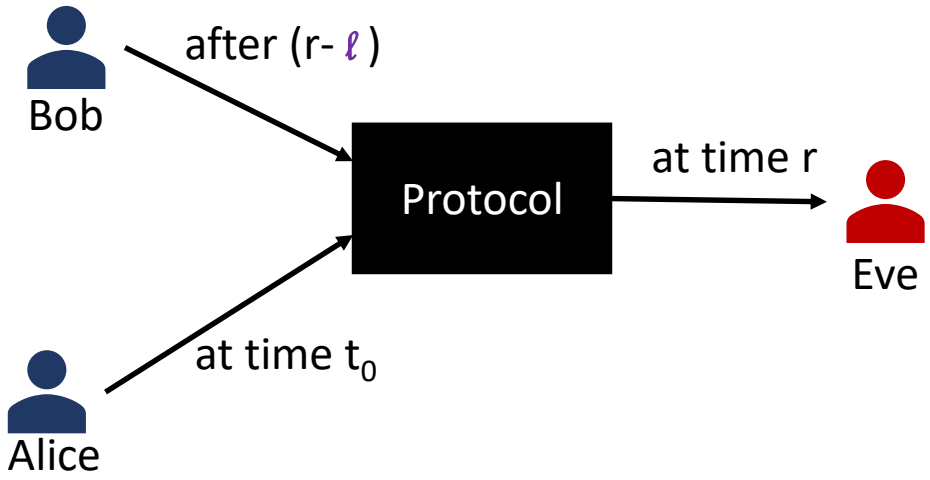


For anonymity we need:

- Bob sends at least one message within the time slice [r- ℓ , r).

Necessary Invariant for Anonymity





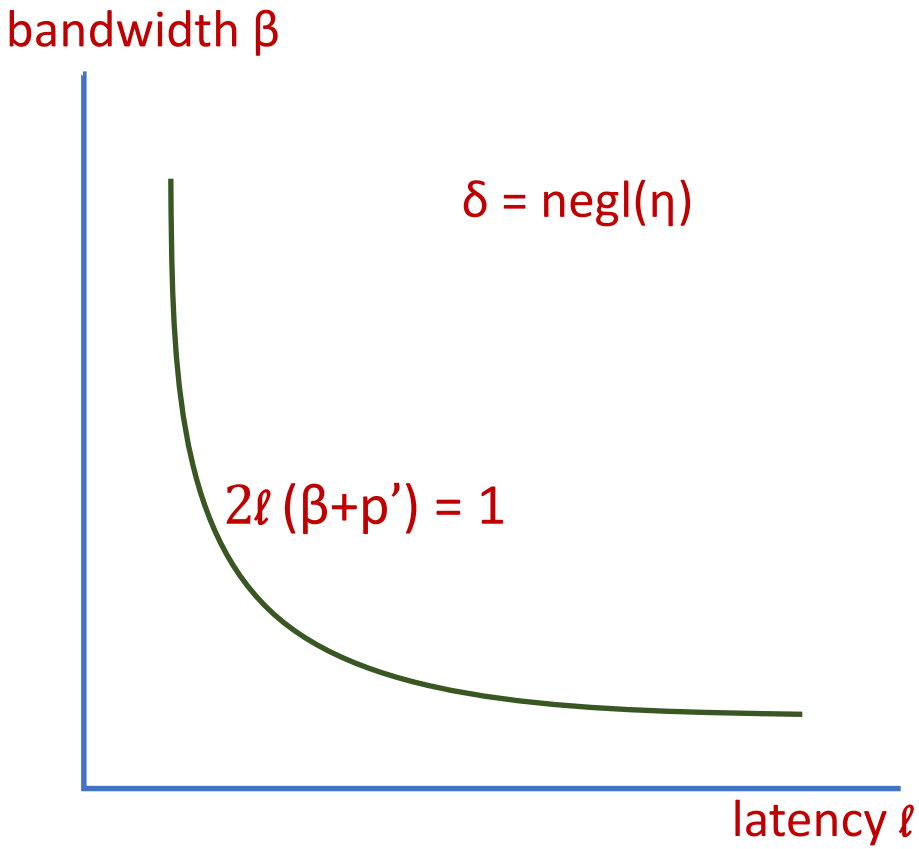
For anonymity we need:

- Bob sends at least one message within the time slice [r- ℓ , r).
- At least one of the packets helping the message from Alice meets a message from Bob at an honest node.

Results are same when no parties are compromised

- To achieve strong anonymity:

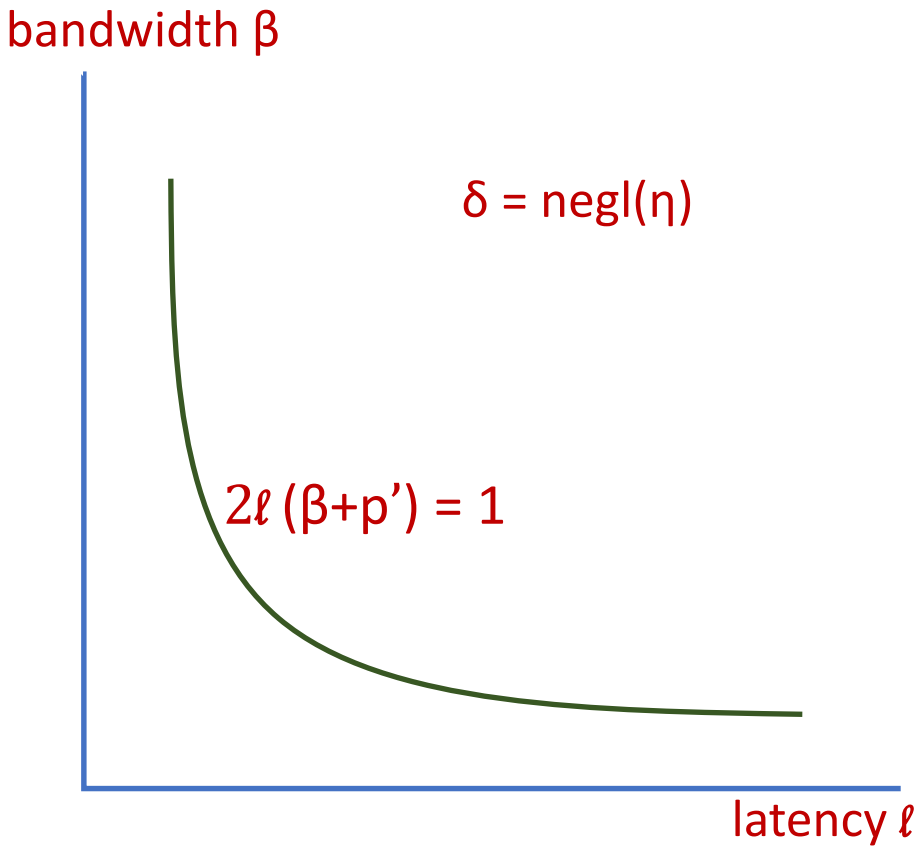
$$2\ell\,(\beta+p') \geq 1$$



Results are same when no parties are compromised

- To achieve strong anonymity:

$$2\ell\,(\beta+p') \geq 1$$



The basic trilemma still holds, except ℓ =0.

Quantum of Solace:
when protocol parties are compromised

Quantum of Solace:
when protocol parties are compromised

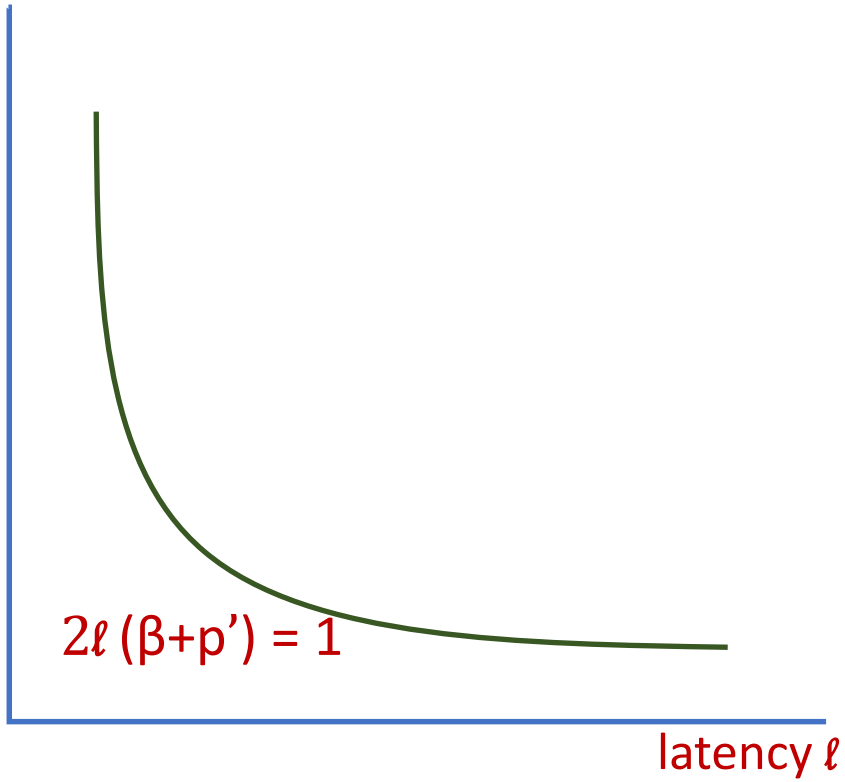
- If strong anonymity is not required, user coordination could allow better anonymity.

Quantum of Solace:
when protocol parties are compromised

- If strong anonymity is not required, user coordination could allow better anonymity.
- Better resistance against compromization.

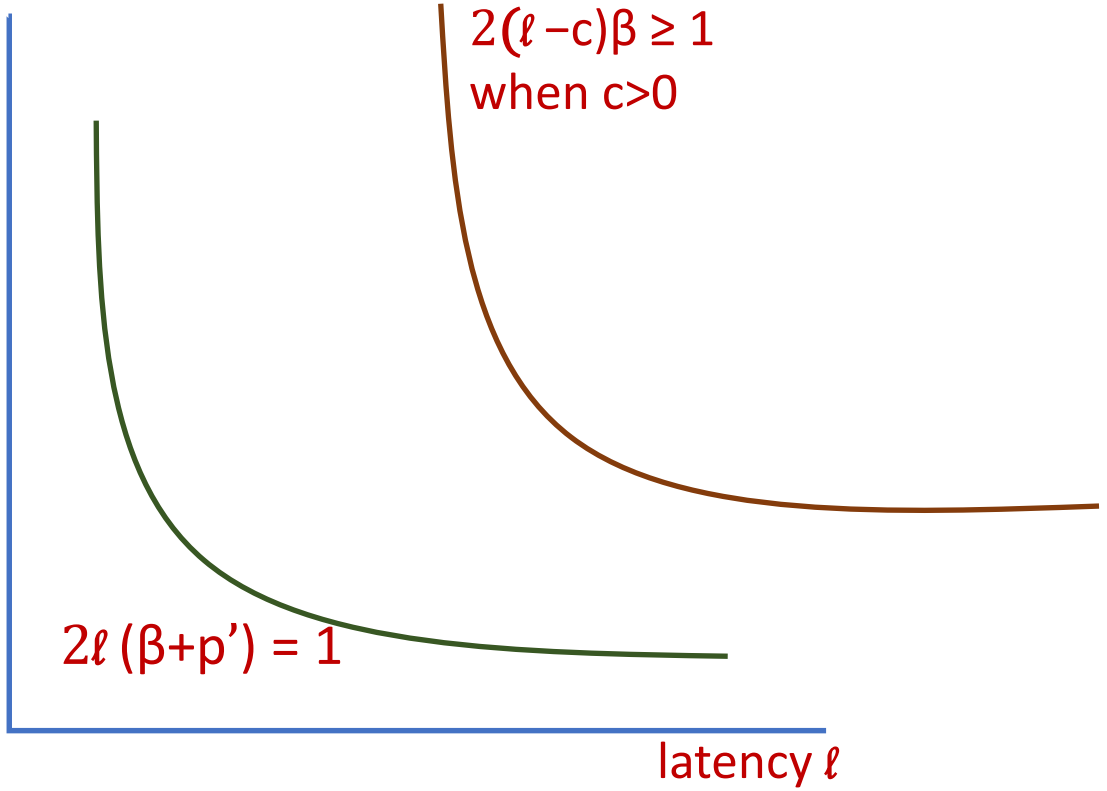
Quantum of Solace: when protocol parties are compromised

- If strong anonymity is not required, user coordination could allow better anonymity.
- Better resistance against compromization.



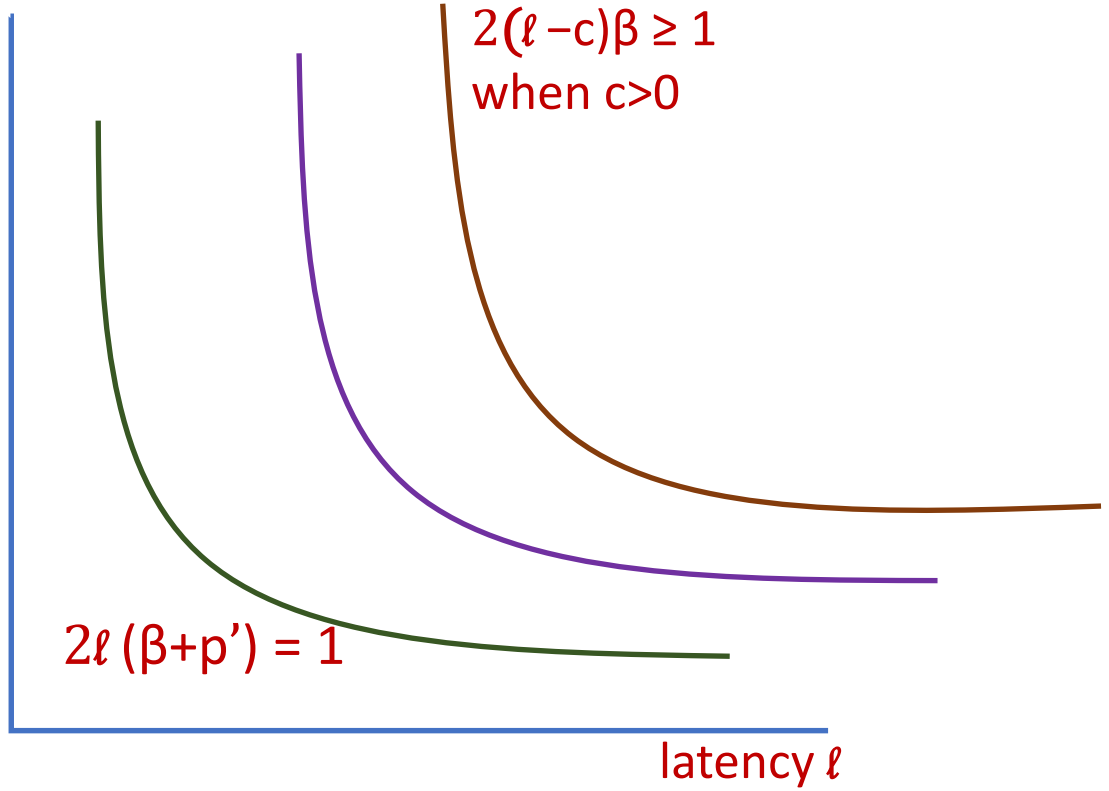
Quantum of Solace: when protocol parties are compromised

- If strong anonymity is not required, user coordination could allow better anonymity.
- Better resistance against compromization.



Quantum of Solace: when protocol parties are compromised

- If strong anonymity is not required, user coordination could allow better anonymity.
- Better resistance against compromization.



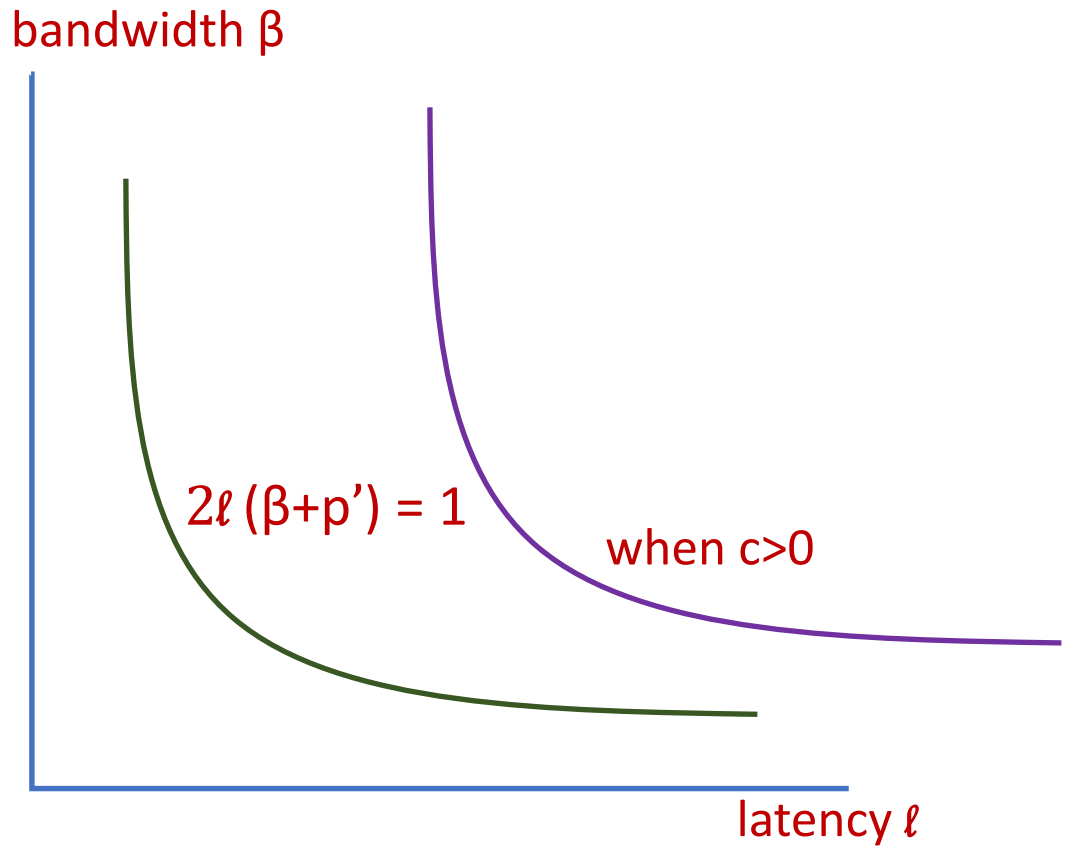
Effect of coordination: resistance against compromised protocol parties

Cases	mix-net	hybrid
$0 \leq \mathsf{c}$	$2\ell p < 1 - \epsilon(\eta)$	$p\ell < 1 - \epsilon(\eta)$
$0 < \mathsf{c} \leq \ell$	$2(\ell - \mathsf{c})p < 1 - \epsilon(\eta)$	$p(\ell - \mathsf{c}) < 1 - \epsilon(\eta)$
$\ell < \mathsf{c} \leq \ell^2$	$\ell \in O(1)$	-
$\ell^2 < \mathsf{c}$	$\ell \in O(1)$	$\ell \in O(1)$
$\mathsf{K}/\mathsf{c} \in O(1)$	$\ell \in log(\eta)$	$\ell \in \sqrt{log(\eta)}$

K: total number of intermediate protocol parties (routers/nodes),
c: total number of compromised parties out of K parties,
p: the probability that a user sends a message in a round,
η: security parameter, ℓ : latency overhead

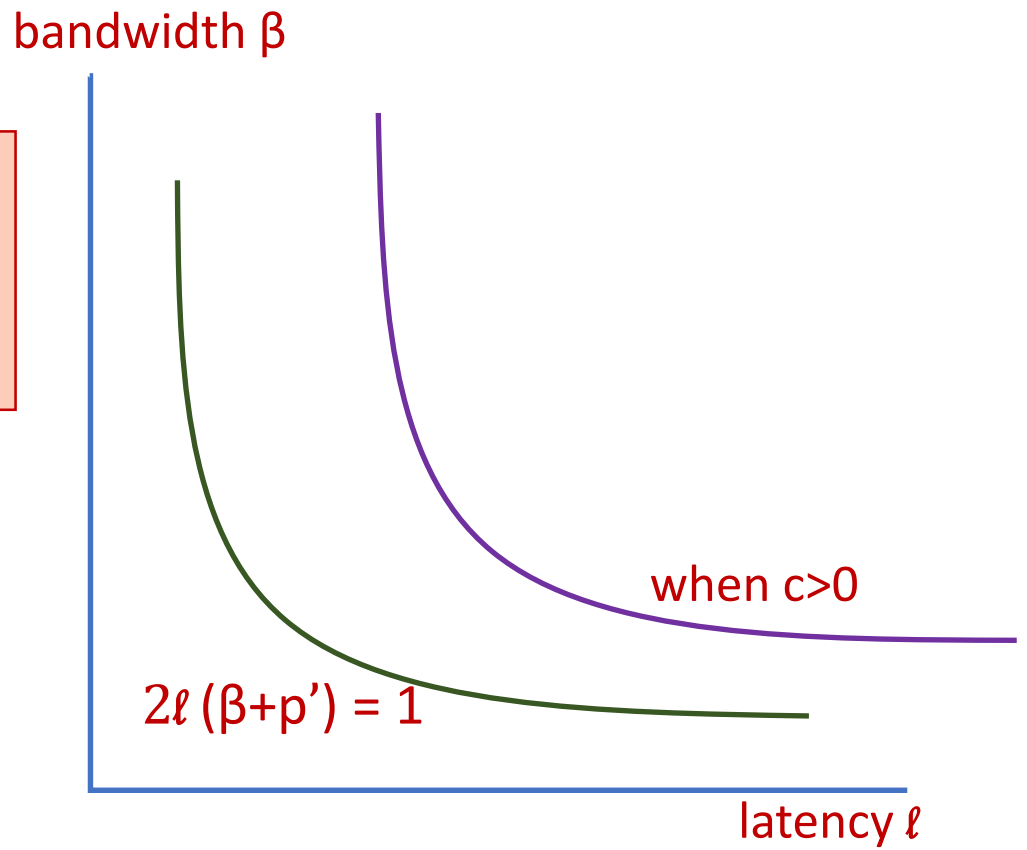
Takeaways

- Our work points protocol designers to focus on hybrid protocols, to at least achieve resistance against compromization.
- Still we can not do better than the limit specified by the trilemma: $2\ell\,(\beta+p') \geq 1$.
- If a protocol achieves strong anonymity for $2\ell\,(\beta+p') = 1$, then that will be the optimal ACN.



Leap of faith:

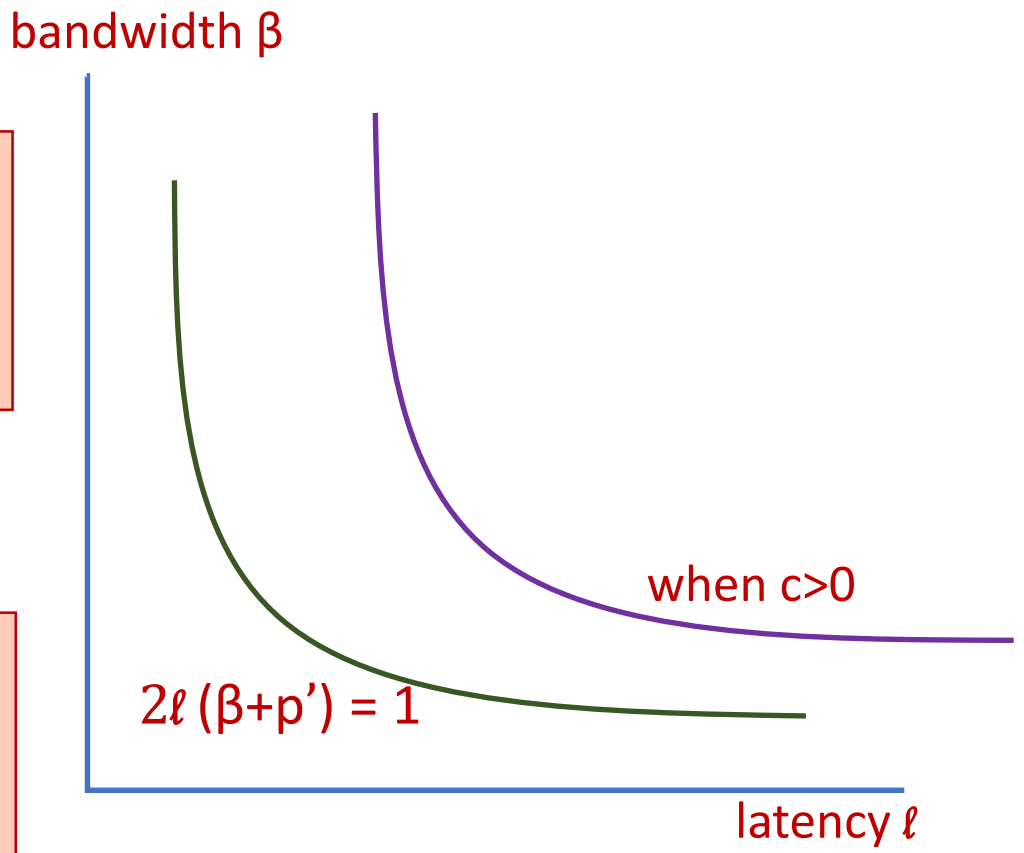
Challenge: Achieve oblivious swapping at a dishonest node.



Leap of faith:

Challenge: Achieve oblivious swapping at a dishonest node.

Still strong anonymity will be impossible for $2\ell\,(\beta+p') < 1$



A New Hope:

Challenge 2: Break Assumption 1.
If a protocol can use a secret sharing scheme that generates $w < k*n$ shares for n messages such that k shares are sufficient to reconstruct all the n messages correctly, without using any trusted third party, with a communication of O(n) and constant latency overhead, that protocol can break anonymity trilemma.

http://bit.ly/AnonymityTrilemma

Thank you. ☺


@tutaidas


das48@purdue.edu